



การออกแบบระบบตรวจสอบบุคคลเข้าสอบโดยใช้เทคโนโลยีชีวมิติด้วยใบหน้าและ
ลายพิมพ์นิ้วมือแบบหลายโปรโตคอลบนระบบสมองกลฝังตัว



คุณฐิณีพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตาม
หลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
วิทยาลัยนวัตกรรมการดิจิทัลเทคโนโลยี

บัณฑิตวิทยาลัย มหาวิทยาลัยรังสิต
ปีการศึกษา 2565



**DESIGNING EXAMINEE PERSONAL VERIFICATION SYSTEM USING
MULTIPROTOCOL FACE AND FINGERPRINT BIOMETRIC
TECHNOLOGIES BASED ON EMBEDDED SYSTEM**

**BY
SETHAPONG WONG-IN**

**A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY IN INFORMATION
TECHNOLOGY
COLLEGE OF DIGITAL INNOVATION TECHNOLOGY**

**GRADUATE SCHOOL, RANGSIT UNIVERSITY
ACADEMIC YEAR 2022**

คุษฎีนิพนธ์เรื่อง

การออกแบบระบบตรวจสอบบุคคลเข้าสอบโดยใช้เทคโนโลยีชีวมิติด้วยใบหน้าและลายพิมพ์
นิ้วมือแบบหลายโปรโตคอลบนระบบสมองกลฝังตัว

โดย

เศรษฐพงศ์ วงษ์อินทร์

ได้รับการพิจารณาให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาปรัชญาคุษฎีบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

มหาวิทยาลัยรังสิต
ปีการศึกษา 2565

รศ. อานนท์ สุขเสถียรวงศ์
ประธานกรรมการสอบ

ผศ. ดร.กวีวัฒน์ อำนาจโชติพันธุ์
กรรมการ

รศ. ดร.สิริพร ศุภราทิตย์
กรรมการ

ผศ. ดร.ธรรณพ อารีพรรค
กรรมการ

ผศ. ดร.มินนภา รัชัทธิ์
กรรมการและอาจารย์ที่ปรึกษาร่วม

รศ. ดร.ปณิธิ เนตินันท์
กรรมการและอาจารย์ที่ปรึกษา

บัณฑิตวิทยาลัยรับรองแล้ว

(ผศ. ร.ต.หญิง ดร.วรรณิ์ สุขสาตร)
คณบดีบัณฑิตวิทยาลัย
29 พฤษภาคม 2566

Dissertation entitled

**DESIGNING EXAMINEE PERSONAL VERIFICATION SYSTEM USING
MULTIPROTOCOL FACE AND FINGERPRINT BIOMETRIC
TECHNOLOGIES BASED ON EMBEDDED SYSTEM**

by

SETHAPONG WONG- IN

was submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Information Technology

Rangsit University
Academic Year 2022

Assoc. Prof. Anon Sukstrienwong
Examination Committee Chairperson

Asst. Prof. Kawiwat Amnatchotiphan, Ph.D.
Member

Assoc. Prof. Siriporn Supratid, D.Tech.Sci
Member

Asst. Prof. Thannob Aribarg, Ph.D.
Member

Asst. Prof. Meennapa Rukhiran, Ph.D.
Member and Co-Advisor

Assoc. Prof. Paniti Netinant, Ph.D.
Member and Advisor

Approved by Graduate School

(Asst. Prof. Plt. Off. Vanee Sooksatra, D.Eng.)

Dean of Graduate School

May 29, 2023

กิตติกรรมประกาศ

ขอกราบขอบพระคุณ รศ. ดร.ทองหล่อ วงษ์อินทร์ และ ผศ. ดร.นันทนา วงษ์อินทร์ บิดา มารดา และครอบครัววงษ์อินทร์ ที่คอยส่งเสริมสนับสนุนและเป็นแรงบันดาลใจที่ดีในการพัฒนาตนเองอย่างต่อเนื่อง ขอขอบคุณภรรยาและบุตรชาย ที่เป็นกำลังใจและสนับสนุนมาโดยตลอด

วิทยานิพนธ์ฉบับนี้สำเร็จได้เป็นอย่างดีเนื่องมาจากการอนุเคราะห์จาก รศ. ดร.ปณิธิ เนตินันท์ อาจารย์ที่ปรึกษา และ ผศ. ดร.มินนภา รักษ์หิรัญ ที่ปรึกษาร่วมที่ให้ความเอาใจใส่ช่วยเหลือ เป็นแบบอย่างที่ดีและคอยให้คำปรึกษาแนะนำเป็นอย่างดีมาโดยตลอด รศ. อานนท์ สุขเสถียรวงศ์ ประธานกรรมการสอบ ผศ. ดร.สิริพร ศุภราทิตย์ ผศ. ดร.กวีวัฒน์ อำนาจโชติพันธุ์ และ ผศ. ดร.ธรรณพ อารีพรรค กรรมการสอบทุกท่าน ที่กรุณาให้เกียรติมาเป็นกรรมการสอบ ปรินญาณินท์ และให้ความคิดเห็นอันเป็นประโยชน์ต่อวิทยานิพนธ์ฉบับนี้ให้สำเร็จโดยสมบูรณ์

ขอขอบพระคุณคณาจารย์ ที่ให้ความรู้ทางวิชาการ และเจ้าหน้าที่หลักสูตรปรัชญาดุษฎีบัณฑิตสาขาวิชาเทคโนโลยีสารสนเทศมหาวิทยาลัยรังสิตที่ให้ความอนุเคราะห์ในการประสานงานต่าง ๆ

ขอขอบพระคุณผู้บริหารคณะวิทยาศาสตร์และเทคโนโลยี เพื่อนคณาจารย์และนักศึกษา หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิศวกรรมดิจิทัลและวิศวกรรมซอฟต์แวร์ และเจ้าหน้าที่ทุกท่านของมหาวิทยาลัยราชภัฏวไลยอลงกรณ์ ในพระบรมราชูปถัมภ์ ที่การให้กำลังใจและสนับสนุนมาโดยตลอดการศึกษา

ขอขอบคุณ เพื่อน ๆ พี่ ๆ น้อง ๆ ในหลักสูตรปรัชญาดุษฎีบัณฑิตสาขาวิชาเทคโนโลยีสารสนเทศมหาวิทยาลัยรังสิตทุกท่านที่ช่วยเป็นแรงใจและร่วมสู้ฝ่าฟันมาด้วยกันทุก ๆ ท่าน

เศรษฐพงศ์ วงษ์อินทร์

ผู้วิจัย

6105824 : เสฐฐพงษ์ วงษ์อินทร์
 ชื่อคุณิพนธ์ : การออกแบบระบบตรวจสอบบุคคลเข้าสอบโดยใช้เทคโนโลยีชีวมิติด้วย
 ใบหน้าและลายพิมพ์นิ้วมือแบบหลายโปรโตคอลบนระบบสมองกลฝังตัว
 หลักสูตร : ปรัชญาคุณิพนธ์บัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
 อาจารย์ที่ปรึกษา : รศ. ดร.ปณิธิ เนดินันท์
 อาจารย์ที่ปรึกษาร่วม : ผศ. ดร.มินนภา รักษ์หิรัญ

บทคัดย่อ

วิธีการยืนยันตัวตนแบบดั้งเดิมในการสอบของนักเรียนโดยใช้กรรมการคุมสอบเป็นผู้ตรวจสอบตัวตนของผู้เข้าสอบอาจส่งผลให้เกิดการยืนยันตัวตนที่ไม่ถูกต้องแม่นยำและใช้เวลาในการดำเนินการมาก โดยเฉพาะอย่างยิ่งสำหรับนักเรียนกลุ่มใหญ่ ระบบการรู้จำชีวมิติสามารถติดตามผลแบบเรียลไทม์และเข้าถึงระบบจากระยะไกลได้ และเป็นวิธีการในการตรวจสอบความถูกต้องของนักเรียนที่ปลอดภัยและสะดวกยิ่งขึ้นในการสอบ งานวิจัยนี้ออกแบบและพัฒนากรอบโครงสร้างระบบยืนยันตัวบุคคลผู้เข้าสอบด้วยชีวมิติบนระบบสมองกลฝังตัว และนำเสนอเกณฑ์การประเมินคุณภาพของชีวมิติโดยเปรียบเทียบประสิทธิภาพและประสิทธิผลของระบบการรู้จำใบหน้าและลายนิ้วมือแบบหลายโปรโตคอลในการสอบจริง นอกจากนี้ ยังได้ประเมินการยอมรับเทคโนโลยีของระบบการรู้จำการตรวจด้วยชีวมิติควบคู่กันไป

งานวิจัยนี้เป็นการออกแบบกึ่งปฏิบัติกับกลุ่มตัวอย่างโดยเปรียบเทียบวิธีการยืนยันตัวตนแบบดั้งเดิมกับเทคนิคการรู้จำด้วยชีวมิติ โดยพัฒนาระบบรู้จำชีวมิติแบบ Unimodal และ Multimodal ผลลัพธ์จากงานวิจัยนี้ได้แก่ระบบสมองกลฝังตัวสำหรับการพัฒนาระบบจดจำชีวมิติแบบหลายโปรโตคอลซึ่งมีความยืดหยุ่นและวิธีการประเมินคุณภาพของระบบชีวมิติสำหรับการใช้งานด้านการสอบ ผลจากการวิจัยพบว่า เทคโนโลยีการรู้จำชีวมิติหลายรูปแบบได้รับคะแนนเชิงบวกมากกว่าเทคโนโลยีการรู้จำชีวมิติรูปแบบเดียวอย่างมีนัยสำคัญ การวิจัยเสนอให้มหาวิทยาลัยใช้เทคโนโลยีชีวมิติ โดยเฉพาะการจดจำใบหน้า เพื่อประเมินการยอมรับของระบบในหมู่ผู้ใช้ การศึกษายังใช้ทฤษฎีเพื่อการกระทำอย่างมีเหตุผลและรูปแบบการยอมรับเทคโนโลยี โดยใช้แบบสอบถามเพื่อตรวจสอบปัจจัยด้านการรับรู้ เช่น การรับรู้ว่าการใช้งานง่าย ความไว้วางใจ ความปลอดภัย และการรับรู้ถึงประโยชน์ ซึ่งส่งผลกระทบต่อความตั้งใจเชิงพฤติกรรมที่จะใช้ระบบจดจำชีวมิติที่ใช้อินเตอร์เน็ตของสรรพสิ่ง

(วิทยานิพนธ์มีจำนวนทั้งสิ้น 190 หน้า)

คำสำคัญ: ระบบการตรวจสอบผู้เข้าสอบ, เทคโนโลยีชีวมิติ, การวิเคราะห์และออกแบบซอฟต์แวร์, การยอมรับเทคโนโลยี

ลายมือชื่อนักศึกษา ลายมือชื่ออาจารย์ที่ปรึกษา
 ลายมือชื่ออาจารย์ที่ปรึกษาร่วม

6105824 : Sethapong Wong-In
 Dissertation Title : Designing Examinee Personal Verification System Using Multiprotocol
 Face and Fingerprint Biometric Technologies based on Embedded System
 Program : Doctor of Philosophy in Information Technology
 Dissertation Advisor : Assoc. Prof. Paniti Netinant, Ph.D.
 Dissertation Co-Advisor : Asst. Prof. Meennapa Rukhiran, Ph.D.

Abstract

Traditional methods of verifying the identity of students based on human proctoring can result in fraudulent identity verification and inefficient processing time, especially for large groups of students. Biometric recognition systems enable real-time monitoring and remote system access and deliver more secure and convenient methods of identifying and validating students during classes and exams in an educational setting. This research designed and developed a biometric personal verification framework based on an embedded system for exam takers. The proposed system was evaluated by a biometric quality metric comparing the efficiency and effectiveness of a multi-protocol facial and fingerprint biometric recognition system in an actual exam. In addition, the technology adoption of the biometric examination recognition system was assessed concurrently.

This study employs a quasi-practical design with sample groups to compare traditional methods of identity verification with biometric recognition techniques. Developing and deploying unimodal and multimodal biometric recognition methods yielded experimental outcomes. The study presents an embedded system for the development of flexible multi-protocol biometric recognition systems and a method for evaluating the quality of biometric systems for educational applications. According to the findings, multimodal biometric recognition technologies received significantly more positive ratings than unimodal biometric recognition technologies. This research aids that universities employ biometric recognition technology, specifically facial recognition. The study also adopts the Theory for Reasoned Action and the Technology Acceptance Model using questionnaires to examine perception factors such as perceived ease of use, trust, security, and perceived usefulness, which significantly impact behavioral intentions to use IoT-based biometric recognition systems.

(Total 190 pages)

Keywords: Examinee Personal Verification System, Biometric Technology, Software Analysis and Design, Technology Acceptance Model.

Student's Signature Dissertation Advisor's Signature
 Dissertation Co-Advisor's Signature.....

สารบัญ

	หน้า
กิตติกรรมประกาศ	ก
บทคัดย่อภาษาไทย	ข
บทคัดย่อภาษาอังกฤษ	ค
สารบัญ	ง
สารบัญตาราง	ช
สารบัญรูป	ซ
บทที่ 1	บทนำ
	1
1.1	ความเป็นมาและความสำคัญของปัญหา
	1
1.2	วิธีการ แนวทางในการแก้ปัญหา
	2
1.3	วัตถุประสงค์การวิจัย
	4
1.4	ขอบเขตการดำเนินการ
	4
1.5	ประโยชน์ที่คาดว่าจะได้รับ
	5
1.6	ผลลัพธ์ที่ได้
	5
1.7	สรุปโครงการวิจัย
	6
บทที่ 2	ทบทวนวรรณกรรมที่เกี่ยวข้อง / ทฤษฎีที่เกี่ยวข้อง
	7
2.1	การตรวจสอบบุคคลเข้าสอบ
	7
2.2	เทคโนโลยีชีวมิติ
	8
2.3	กรอบการทำงานของโอเพนซีวี
	23
2.4	อินเทอร์เน็ตสำหรับสรรพสิ่ง
	28
2.5	การวิเคราะห์และออกแบบระบบ
	33
2.6	การประกันคุณภาพของการออกแบบระบบเทคโนโลยีสารสนเทศ
	37
2.7	แบบจำลองการยอมรับเทคโนโลยี
	47
2.8	การวิเคราะห์แบบจำลองสมการโครงสร้าง
	48

สารบัญ (ต่อ)

	หน้า
2.9 งานวิจัยที่เกี่ยวข้อง	49
บทที่ 3 ระเบียบวิธีการวิจัย	55
3.1 การศึกษาและระบุปัญหา	55
3.2 การพัฒนากรอบแนวคิด	56
3.3 การทบทวนวรรณกรรม	58
3.4 การพัฒนากรอบการทำงาน	58
3.5 การออกแบบเครื่องมือที่ใช้ในการตรวจสอบบุคคลเข้าสอบ	62
3.6 การออกแบบการทดลอง	65
3.7 การประเมินระบบการตรวจสอบผู้เข้าสอบโดยเทคโนโลยีชีวมิติ	71
3.8 การประเมินการยอมรับการใช้ระบบการตรวจสอบผู้เข้าสอบโดยเทคโนโลยีชีวมิติ	72
3.9 สถิติที่ใช้ในงานวิจัย	76
บทที่ 4 ผลการวิจัย	79
4.1 ผลการประเมินประสิทธิภาพของระบบ	79
4.2 ผลการประเมินการยอมรับการใช้งานระบบตรวจสอบบุคคลเข้าสอบโดยใช้เทคโนโลยีชีวมิติ	85
บทที่ 5 สรุปผลและข้อเสนอแนะ	96
5.1 สรุปผลการวิจัย	96
5.2 อภิปรายผล	97
5.3 ข้อเสนอแนะในการนำผลการวิจัยไปใช้	98
5.4 ข้อเสนอแนะในการดำเนินงานในภายหน้า	98
บรรณานุกรม	99

สารบัญ (ต่อ)

	หน้า
ภาคผนวก	
ภาคผนวก ก แบบประเมินการยอมรับการใช้งานระบบตรวจสอบบุคคลเข้า สอบด้วยเทคโนโลยีชีวมิติ	109
ภาคผนวก ข การเผยแพร่ผลงานวิจัยในงานประชุมวิชาการระดับนานาชาติ ครั้งที่ 1	114
ภาคผนวก ค การเผยแพร่ผลงานวิจัยในงานประชุมวิชาการระดับนานาชาติ ครั้งที่ 2	129
ภาคผนวก ง การเผยแพร่ผลงานวิจัยในวารสารวิชาการระดับนานาชาติ ครั้งที่ 1	142
ภาคผนวก จ การเผยแพร่ผลงานวิจัยในวารสารวิชาการระดับนานาชาติ ครั้งที่ 2	165
ประวัติผู้วิจัย	190



สารบัญตาราง

ตารางที่	หน้า
2.1 แสดงข้อดีและข้อด้อยของทั้ง 3 อัลกอริทึม	27
2.2 แสดงคุณลักษณะของอุปกรณ์อินเทอร์เน็ตของสรรพสิ่ง	31
2.3 แสดงมุมมองการออกแบบตามมาตรฐานการออกแบบซอฟต์แวร์ของสถาบันวิชาชีพวิศวกรรมไฟฟ้าและอิเล็กทรอนิกส์	39
2.4 แสดงการสำรวจเกณฑ์ที่ใช้ในการประเมินประสิทธิภาพของระบบชีวมิติต่าง ๆ	43
4.1 แสดงผลการทดสอบการใช้งานของระบบตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติ	79
4.2 แสดงผลการทดสอบการใช้งานของระบบโดยการเทียบลำดับ	81
4.3 แสดงข้อมูลทั่วไปของผู้ตอบแบบสอบถาม	86
4.4 แสดงผลการประเมินเชิงตัวเลขสำหรับแต่ละตัวแปรด้านการสำรวจ	86
4.5 แสดงผลลัพธ์ความถูกต้องความตรงคู่สมบูรณ์	89
4.6 แสดงผลลัพธ์การแยกแยะความถูกต้องของโครงสร้าง	90
4.7 แสดงผลลัพธ์การวัดตัวบ่งชี้ความเหมาะสมสำหรับแบบจำลองการวัด	91
4.8 แสดงผลลัพธ์การวัดตัวบ่งชี้ความเหมาะสมสำหรับรูปแบบการวัดที่ปรับปรุงใหม่	93
4.9 แสดงผลสรุปการประเมินสมมติฐาน	94

สารบัญรูป

รูปที่		หน้า
2.1	แสดงขั้นตอนในการตรวจสอบบุคคลเข้าสอบโดยตรวจจากเอกสาร	7
2.2	แสดงขั้นตอนในการทำงานของการจดจำใบหน้า	9
2.3	แสดงหลักการทำงานของ Haar Cascade	10
2.4	แสดงภาพ คุณลักษณะของ Haar ประเภทต่าง ๆ	11
2.5	แสดงหลักการทำงานของ Adaboost	11
2.6	แสดงหลักการทำงานของ Feature Extraction โดยใช้ LBP	12
2.7	แสดงตัวอย่าง Feature Extraction โดยใช้ LBP	12
2.8	แสดงตัวอย่างการใช้หลักการต่าง ๆ ในการจดจำใบหน้า	14
2.9	แสดงประเภทของลายนิ้วมือ	15
2.10	แสดงขั้นตอนในการทำงานของการจดจำลายนิ้วมือ	15
2.11	แสดงขั้นตอนในการปรับปรุงคุณภาพลายนิ้วมือ	16
2.12	แสดง Gaussian Pyramid	17
2.13	แสดง SIFT Descriptor	18
2.14	แสดง Feature Factor โครงสร้างของ FLANN	19
2.15	แสดงขั้นตอนในการสร้างโครงสร้างต้นไม้ KD-Tree ของ Feature Vector	20
2.16	แสดงโครงสร้างต้นไม้ KD-Tree ของ Feature Vector	21
2.17	แสดงตัวอย่างภาพใบหน้าจากการใช้อัลกอริทึม Eigenface	25
2.18	แสดงตัวอย่างภาพใบหน้าจากการใช้อัลกอริทึม Fisherfaces	26
2.19	แสดงตัวอย่างภาพใบหน้าจากการใช้อัลกอริทึม LBPH	27
2.20	แสดงลักษณะและคำอธิบาย Raspberry Pi version 4 Model B	30
2.21	แสดงตัวอย่างการออกแบบระบบโดยใช้ IFD	37
2.22	แสดงหมวดหมู่ของ SQuaRE	42
2.23	แสดง Technology Acceptance Model (TAM)	47
3.1	แสดงขั้นตอนในการดำเนินงานวิจัย	55

สารบัญรูป (ต่อ)

รูปที่		หน้า
3.2	แสดง Biometric Examinee Personal Verification System (BEPVS) Conceptual Framework	57
3.3	แสดง Biometric Examinee Personal Verification System (BEPVS) Revised Framework	59
3.4	แสดงกรอบแนวคิดเชิงการออกแบบระบบการตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติ	61
3.5	แสดง Use-case Diagram ระบบการตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติ	62
3.6	แสดง Class Diagram ระบบการตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติ	63
3.7	แสดง Information Flow Diagram ระบบการตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติ	64
3.8	แสดงภาพรวมการทำงานของระบบชีวมิติทั้ง 8 กลุ่ม	68
3.9	แสดงขั้นตอนการทำงานของระบบ Unimodal Biometric	69
3.10	แสดงขั้นตอนการทำงานของระบบ Multimodal Biometric	70
3.11	แสดงขั้นตอนการทำงานของระบบ Semi-Multimodal Biometric	70
3.12	แสดงกรอบแนวคิดในการวิจัยด้านการยอมรับระบบตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติ	75
4.1	แสดงผลการเปรียบเทียบประสิทธิภาพและคะแนน Biometric Quality Metric ของระบบการตรวจสอบผู้เข้าสอบในแต่ละกลุ่ม	82
4.2	แสดงผลการเปรียบเทียบประสิทธิภาพของระบบการตรวจสอบผู้เข้าสอบแบบ Unimodal กับ Zero Biometric	82
4.3	แสดงผลการเปรียบเทียบประสิทธิภาพของระบบการตรวจสอบผู้เข้าสอบแบบ Multimodal กับ Zero Biometric	83
4.4	แสดงผลการเปรียบเทียบประสิทธิภาพของระบบการตรวจสอบผู้เข้าสอบแบบ Semi-Multimodal กับ Zero Biometric	83

สารบัญรูป (ต่อ)

รูปที่		หน้า
4.5	แสดงผลการเปรียบเทียบประสิทธิภาพของระบบการตรวจสอบผู้เข้า สอบแบบ Unimodal กับ Multimodal Biometric (Multiple Modalities)	84
4.6	แสดงผลการเปรียบเทียบประสิทธิภาพของระบบการตรวจสอบผู้เข้า สอบแบบ Unimodal กับ Multimodal Biometric (Multiple Sensors)	84
4.7	แสดงผลการเปรียบเทียบประสิทธิภาพของระบบการตรวจสอบผู้เข้า สอบแบบ Unimodal กับ Semi-multimodal Biometric	85
4.8	แสดงรูปแบบการวัดการรับรู้ของนักเรียนต่อการรู้จำทางชีวมิติ	92
4.9	แสดงการปรับปรุงรูปแบบการวัดการรับรู้ของนักเรียนต่อการจดจำทาง ชีวมิติ	93



บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันได้มีการนำเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการดำเนินงานหลายด้าน โดยเฉพาะการบริหารและการจัดการสถาบันการศึกษาเพื่อมุ่งให้เป็นสถาบันการศึกษาอัจฉริยะ ด้วยแพลตฟอร์มดิจิทัล (Smart School Digital Framework) (Phokajang & Netinant, 2021) สถาบันการศึกษาจำนวนมากได้พัฒนาระบบสารสนเทศ เพื่อใช้ในการดำเนินงานเฉพาะแต่ละสถาบัน ตัวอย่างระบบสารสนเทศสำหรับสถาบันการศึกษา เช่น ระบบลงทะเบียน ระบบการจัดตารางเรียน และระบบอื่น ๆ (Hamid, Mokhtar, Yusof, & Warland, 2020) นอกจากนี้ ระบบบริหารจัดการสอบเป็นหนึ่งในระบบสารสนเทศที่มีความสำคัญยิ่งในการประเมินความรู้ของผู้เรียน การประยุกต์ใช้เทคโนโลยีสารสนเทศเพื่อช่วยการบริหารการสอบให้สะดวกรวดเร็วและถูกต้องมากขึ้น การสอบด้วยระบบคอมพิวเตอร์ (Computer Based) สามารถนำมาใช้ทดแทนการสอบแบบกระดาษ ช่วยทำให้การตรวจผลการสอบของผู้เรียนสามารถทำได้รวดเร็วขึ้น และเริ่มมีการนำเทคโนโลยีสารสนเทศอื่น ๆ มาประยุกต์ใช้ เช่น การจัดการเรียนการสอนแบบออนไลน์ผ่านเว็บ (Abass, Olajide, & Samuel, 2017; Hamid et al., 2020) ระบบการจัดการตารางสอบ (Hameed & Abdullatif, 2017; Divya, Nandhini, Shobana, & Sujithra, 2021) ส่วนมากเป็นระบบสารสนเทศเพื่อสนับสนุนการบริหารจัดการ (Management Information System: MIS) สำหรับระบบดูแลหลังบ้าน (Back-end System) อย่างไรก็ตามหลายสถาบันศึกษามองข้ามองค์ประกอบของการตรวจสอบตัวตนผู้เข้าสอบ แม้จะมีกรณีที่ใช้บุคคลอื่นปลอมเข้าสอบแทน ซึ่งพบเห็นได้อยู่บ่อยครั้ง โดยเฉพาะในการสอบที่มีความสำคัญ เช่น การสอบบรรจุเข้าทำงาน การสอบเข้าเรียนในสถาบันการศึกษา

ในปัจจุบันของหลาย ๆ สถาบันการศึกษาใช้วิธีการตรวจสอบตัวตนผู้เข้าสอบ โดยตรวจดูจากเอกสารประจำตัวของผู้เข้าสอบ เช่น บัตรประจำตัวผู้เข้าสอบ บัตรประชาชน หรือเอกสารที่ออกโดยหน่วยงานของรัฐ ซึ่งพบปัญหาต่าง ๆ เช่น ผู้เข้าสอบทำบัตรหาย การทำหลักฐานปลอมมาใช้ในการเข้าสอบ บัตรประจำตัวประชาชนปลอม ใบขับขี่ปลอม รูปผู้เข้าสอบที่ปรากฏบนบัตรประจำตัวนักศึกษาไม่ได้มีการปรับปรุงให้ทันกับรูปลักษณะของผู้เข้าสอบตรงกับปัจจุบัน เมื่อเวลาผ่านไปหน้าตาของผู้เข้าสอบเปลี่ยนไปตามกาลเวลา รูปถ่ายติดบัตรประจำตัวนักศึกษาถูกถ่ายไว้ตั้งแต่ตอน

เข้าเรียนชั้นปีที่ 1 และนักศึกษาได้ใช้บัตรประจำตัวนักศึกษาเรื่อยมาจนกระทั่งชั้นปีที่ 4 ซึ่งใบหน้าของนักศึกษาอาจเปลี่ยนไปไม่ตรงกับรูปถ่ายในบัตรประจำตัวนักศึกษา ทำให้ผู้คุมสอบเกิดความไม่แน่ใจว่าตัวตนผู้เข้าสอบนั้นเป็นบุคคลผู้เข้าสอบตัวจริงตรงกับรูปถ่ายที่ปรากฏในบัตรประจำตัวนักศึกษาหรือไม่ นอกจากการตรวจสอบเอกสารประจำตัวนักศึกษาแล้วยังมีกระบวนการให้ผู้เข้าสอบต้องเซ็นชื่อเพื่อเป็นการยืนยันลายมือชื่อของผู้เข้าสอบได้เข้าสอบจริง การตรวจสอบลายเซ็นของผู้เข้าสอบนั้นไม่สามารถยืนยันได้ว่าเป็นลายเซ็นจริงของผู้เข้าสอบ อีกทั้งในกรณีที่มิให้ผู้เข้าสอบเป็นจำนวนมากจะทำให้การเซ็นชื่อในการเข้าสอบเพื่อระบุตัวบุคคลใช้เวลามากไปด้วย

การนำเทคโนโลยีชีวมิติ (Biometric Technology) มาประยุกต์ใช้ในการตรวจสอบตัวตนของผู้เข้าสอบ จึงเป็นทางเลือกที่มีประสิทธิภาพวิธีหนึ่ง โดยเทคโนโลยีชีวมิติสามารถจำแนกรูปแบบลักษณะชีวมิติบุคคลได้หลายรูปแบบ เช่น Kortli, Jridi, Falou, and Atri (2020) ใช้การตรวจสอบตัวตนโดยการตรวจสอบใบหน้า Shamsi and Andrews (2019) ใช้การตรวจสอบตัวตนโดยใช้ลายพิมพ์นิ้วมือในการลงชื่อเข้าออกสถานที่ทำงาน เป็นต้น นอกจากนี้ยังพบงานวิจัยที่ศึกษาการใช้ชีวมิติจากส่วนต่าง ๆ ของร่างกาย เช่น เสียง ม่านตา ใบหู ลายพิมพ์นิ้วมือ ฝ่ามือ รหัสดีเอ็นเอ (DNA) เป็นต้น ทั้งนี้การตรวจสอบตัวบุคคลขึ้นอยู่กับประเภทของการนำไปใช้งานและความเหมาะสมของกิจกรรมที่จะนำไปใช้ การนำไปประยุกต์ใช้ในแต่ละสถาบันการศึกษาเพื่อตรวจสอบผู้เข้าสอบสามารถทำได้หลายรูปแบบโดยขึ้นอยู่กับความพร้อมด้านเทคโนโลยีสารสนเทศของแต่ละสถาบัน

ในงานวิจัยนี้ได้ทำการออกแบบกรอบแนวคิดระบบการตรวจสอบตัวตนผู้เข้าสอบในสถาบันการศึกษาโดยใช้เทคโนโลยีชีวมิติ และออกแบบการทดสอบการทำงานของกรอบแนวคิดของเทคโนโลยีชีวมิติด้วยอินเทอร์เน็ตของสรรพสิ่ง (Internet of Things) โดยทดสอบเปรียบเทียบประสิทธิภาพของการใช้เทคโนโลยีชีวมิติหลายรูปแบบ ผลการทดสอบสามารถเป็นแนวทางให้นำไปประยุกต์ใช้งานต่อความเหมาะสม ความต้องการ และความพร้อมด้านเทคโนโลยีสารสนเทศของแต่ละสถาบัน

1.2 วิธีการ แนวทางการแก้ไข้ปัญหา

งานวิจัยที่ศึกษาถึงการนำเทคโนโลยีชีวมิติแบบทางเดียว (Unimodal Biometric Technology) นำไปใช้งานตรวจสอบตัวตน สามารถจำแนกตามชีวมิติรูปแบบต่าง ๆ เช่น การใช้ลายพิมพ์นิ้วมือ (Zainal, Sidek, Gunawan, Mansor, & Kartiwi, 2014; Zainal, Sidek, & Gunawan, 2016) การใช้ใบหน้า (Fenu, Marras, & Boratto, 2018; Mehta & Tomar, 2016; Sayeed, Hossen,

Kalaiarasi, Vaithiyashankar, Yusof, & Samraj, 2017; Traore, Nakkabi, Saad, Sayed, Ardigo, & Quinan, 2017; Ye, Shen, Lin, Xiang, Shao, & Hoi, 2020; Yusof, Nasir, Othman, Suliman, Shahbudin, & Mohamad, 2018) ในปัจจุบันยังไม่มีการนำเทคโนโลยีชีวมิติมาประยุกต์ใช้การตรวจสอบบุคคลเข้าสอบมากเท่าไรนัก ส่วนมากเป็นการนำเทคโนโลยีชีวมิติแบบทางเดียวมาใช้ เช่น Ahmed, Mohamed, and Noma (2018) ได้ใช้การรู้จำลายพิมพ์นิ้วมือมาใช้ในการสร้างกรอบการทำงานด้านความปลอดภัยสำหรับการสอบแบบออนไลน์ Emmanuel and Okonkwo (2019) ได้พัฒนาระบบการอนุญาตให้เข้าสอบโดยใช้เทคโนโลยีชีวมิติสำหรับนักเรียนในประเทศไนจีเรีย Mir, Balkhi, Lala, Sofi, Kirmani, Mir, and Hamid (2018) ทำการพัฒนาาระบบชีวมิติโดยใช้ม่านตาเพื่อตรวจสอบตัวตนนักเรียนที่เข้าห้องเรียน นอกจากนี้ยังมีงานวิจัยใช้เทคโนโลยีอินเทอร์เน็ตของสรรพสิ่ง (Internet of Things: IoT) เป็นแพลตฟอร์มประกอบกับการตรวจสอบชีวมิติของบุคคลแบบทางเดียว โดยใช้การรู้จำลายพิมพ์นิ้วมือ (Awojide, Awe, & Babatope, 2018; Jain, Tomar, Arora, & Jain, 2020; Zainal et al., 2016) การใช้การรู้จำใบหน้าในงานวิจัย Sunaryono, Siswantoro, and Anggoro (2021) และ Yusof et al. (2018) ซึ่งใช้การรู้จำใบหน้าแบบอัตโนมัติโดยบุคคลเดินผ่านกล้องก็สามารถตรวจสอบตัวตนได้เป็นต้น การใช้เทคโนโลยีชีวมิติแบบทางเดียว พบว่าการอ่านลายพิมพ์นิ้วมือหรือการตรวจสอบใบหน้าใช้เวลาในการประมวลผลค่อนข้างมาก หากผู้ใช้งานจำนวนมาก หรือความเข้ากันได้ของอุปกรณ์ที่ใช้ในการตรวจจับมีปัญหา การใช้เทคโนโลยีชีวมิตินั้นต้องคำนึงถึงความถูกต้องแม่นยำและต้องคำนึงถึงปัจจัยอื่น ๆ อีกด้วย เช่น ความสะดวกรวดเร็วในการทำงาน (Processing Time) การทนทานต่อความผิดพลาด (Fault Tolerance) การใช้เทคโนโลยีชีวมิติแบบทางเดียวในปัจจุบันยังทำงานได้ไม่เป็นที่พอใจ หลายงานวิจัยได้นำเสนอแนวคิดที่จะใช้เทคโนโลยีชีวมิติแบบหลายทาง (Multimodal Biometric Technology) มาใช้ในการทำงาน เพื่อเพิ่มประสิทธิภาพจากการใช้เทคโนโลยีชีวมิติแบบทางเดียว อาทิ (Raju & Udayashankara, 2018; Poria, Cambria, Bajpai, & Hussain, 2017; Singh, Singh, & Ross, 2019) โดยได้นำเสนอรูปแบบการใช้งานเทคโนโลยีชีวมิติทั้งสองแบบมาใช้ในการทำงานร่วมกัน

Wong-In and Netinant (2018) ได้เสนอกรอบการทำงานของระบบตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติ (Biometric Examinee Personal Verification System Framework: BEPVS Framework) เพื่อใช้เป็นตัวต้นแบบสำหรับผู้พัฒนาสามารถนำไปเป็นโครงร่างต้นแบบในการพัฒนาระบบการตรวจสอบผู้เข้าสอบสำหรับสถานศึกษา

ในงานวิจัยนี้ได้นำกรอบแนวคิด Wong-In and Netinant (2018) โดยเสนอแนวทางที่พัฒนาต้นแบบของระบบการตรวจสอบบุคคลเข้าสอบโดยใช้เทคโนโลยีชีวมิติแบบผสมสำหรับสถาบันการศึกษาด้วยเทคโนโลยีอินเทอร์เน็ตของสรรพสิ่ง ช่วยให้ผู้พัฒนาระบบสามารถนำไปต่อ

ยอดการพัฒนาระบบในสถานศึกษา โดยแต่ละสถานศึกษาย่อมมีความต้องการและความพร้อมที่แตกต่างกัน อีกทั้งยังนำเสนอเกณฑ์ที่ใช้ในการประเมินประสิทธิภาพของการใช้เทคโนโลยีชีวิตมิติในการตรวจสอบผู้เข้าสอบอีกด้วย

1.3 วัตถุประสงค์การวิจัย

1.3.1 เพื่อสร้างกรอบโครงสร้างระบบซอฟต์แวร์สำหรับการตรวจสอบตัวบุคคลเข้าสอบด้วยเทคโนโลยีชีวิตมิติบนอุปกรณ์สมองกลฝังตัว

1.3.2 เพื่อพัฒนาต้นแบบซอฟต์แวร์สำหรับการตรวจสอบตัวบุคคลเข้าสอบทางชีวิตมิติแบบหลายโปรโตคอล ซึ่งรองรับเทคโนโลยีชีวิตมิติแบบทางเดียวและแบบหลายทาง

1.3.3 เพื่อเปรียบเทียบประสิทธิภาพและประสิทธิผลของระบบหลายโปรโตคอลบนชีวิตมิติหลายแบบในการตรวจสอบบุคคลเข้าสอบ

1.4 ขอบเขตการดำเนินการ

ในงานวิจัยนี้ได้กำหนดขอบเขตในการวิจัยเป็นด้านต่าง ๆ ดังนี้

1.4.1 ด้านกระบวนการตรวจสอบบุคคลเข้าสอบ

การศึกษาเก็บรวบรวมข้อมูลความต้องการของกระบวนการจัดสอบ เพื่อนำไปพัฒนารอบการทำงานของการพัฒนาระบบซอฟต์แวร์ใช้ในการตรวจสอบผู้เข้าสอบ

1.4.2 ด้านเทคโนโลยีชีวิตมิติ

การศึกษาเทคโนโลยีชีวิตมิติโดยมุ่งเน้นการนำไปใช้งานด้านการตรวจสอบตัวบุคคลผู้เข้าสอบ

1.4.3 ด้านการออกแบบตัวต้นแบบกรอบการทำงาน

การออกแบบกรอบโครงสร้างการทำงาน เพื่อเป็นต้นแบบพัฒนานำไปใช้งานระบบการตรวจสอบผู้เข้าสอบ

1.4.4 ด้านการพัฒนากระบวนการตรวจสอบบุคคลเข้าสอบ

การพัฒนากระบวนการสารสนเทศตรวจสอบบุคคลเข้าสอบด้วยเทคโนโลยีชีวมิติ นำไปทดสอบใช้งานจริง โดยใช้ออกแบบตามหลักการพัฒนาเชิงวัตถุและการออกด้วยแบบแผนภูมิการไหลของข้อมูล

1.4.5 ด้านการทดลองเพื่อเปรียบเทียบประสิทธิภาพของระบบ

การทดสอบระบบสารสนเทศในการตรวจสอบบุคคลเข้าสอบด้วยเทคโนโลยีชีวมิติในการสอบเก็บคะแนนของนักศึกษาระดับปริญญาตรี คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏวไลยอลงกรณ์ ในพระบรมราชูปถัมภ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

ในการวิจัยนี้มุ่งเน้นการศึกษาและพัฒนาแนวทางในการพัฒนาระบบการตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติ ช่วยสนับสนุนเพิ่มความเชื่อมั่นการตรวจสอบผู้เข้าสอบว่าเป็นตัวบุคคลที่ตรงกับตัวตนจริง และเพิ่มความสะดวกรวดเร็วแม่นยำในการตรวจสอบตัวบุคคลผู้เข้าสอบของสถาบันการศึกษา ผลลัพธ์ที่ได้จากการวิจัยนี้ประกอบด้วย โครงร่างกรอบแนวคิดระบบสารสนเทศการตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติ ต้นแบบของระบบสารสนเทศ เพื่อใช้เป็นพิมพ์เขียวสำหรับนักพัฒนาสามารถนำไปต่อยอดการพัฒนาระบบภายนอกให้ตรงตามความต้องการและเหมาะสมกับสถาบันการศึกษา อีกทั้งผลการเปรียบเทียบประสิทธิภาพของระบบการตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติสามารถช่วยให้สถาบันการศึกษาเลือกรูปแบบที่เหมาะสมประยุกต์ใช้ได้อย่างมีประสิทธิภาพอีกด้วย

1.6 ผลลัพธ์ที่ได้

1.61 การค้นพบตัวต้นแบบการใช้เทคโนโลยีชีวมิติในระบบการตรวจสอบผู้เข้าสอบ (Biometric Examinee Personal Verification System Model: BEPVS Model) ซึ่งเป็นตัวต้นแบบเพื่อให้ผู้พัฒนาสามารถนำไปพัฒนาเป็นระบบตรวจสอบผู้เข้าสอบใช้งานในสถาบันการศึกษา โดยสามารถปรับเปลี่ยนรายละเอียดได้ตามความเหมาะสมของสถาบันการศึกษานั้น ๆ

1.6.2 ระบบซอฟต์แวร์สำหรับการตรวจสอบตัวบุคคลเข้าสอบด้วยเทคโนโลยีชีวมิติแบบหลายโปรโตคอลบนระบบสมองกลฝังตัว

1.6.3 ผลการเปรียบเทียบประสิทธิภาพและประสิทธิผลของระบบซอฟต์แวร์สำหรับการตรวจสอบตัวบุคคลเข้าสอบเทคโนโลยีชีวมิติแบบหลายโปรโตคอลบนระบบสมองกลฝัง

1.7 สรุปโครงการวิจัย

การสอบเป็นกระบวนการสำคัญยิ่งในการศึกษาเพื่อประเมินทักษะความรู้ของผู้เรียน การสอบในสถาบันการศึกษาควรนำเทคโนโลยีต่าง ๆ มาประยุกต์ใช้อย่างยิ่งโดยเฉพาะการตรวจสอบบุคคลผู้เข้าสอบช่วยเพิ่มประสิทธิภาพและความถูกต้องแม่นยำมากกว่าการตรวจสอบตัวบุคคลผู้เข้าสอบแบบเดิม อีกทั้งยังสามารถรองรับการสอบที่มีผู้เข้าสอบจำนวนมาก การนำเทคโนโลยีชีวมิติประยุกต์ใช้จึงเป็นทางเลือกที่เหมาะสม และทันต่อเทคโนโลยีปัจจุบัน การพัฒนาระบบสารสนเทศตรวจสอบตัวบุคคลผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติควรสามารถปรับเปลี่ยนตามเทคโนโลยีชีวมิติที่หลากหลายได้อย่างง่าย ทั้งต้องคำนึงถึงความพร้อมเชิงทรัพยากรบุคคลและเทคโนโลยีสารสนเทศของแต่ละสถาบันการศึกษาในการเลือกใช้รูปแบบของระบบตรวจสอบผู้เข้าสอบว่าควรใช้เทคโนโลยีชีวมิติแบบใด

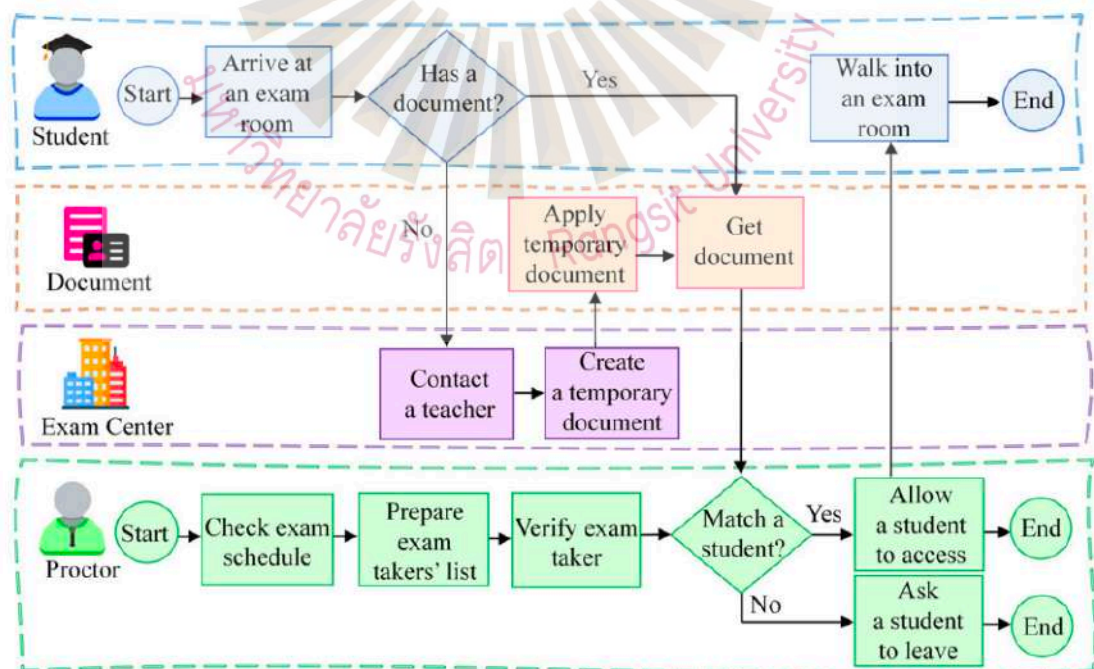
งานวิจัยนี้จึงได้ออกแบบและพัฒนาต้นแบบจากโครงร่างกรอบการทำงาน โดยใช้เกณฑ์การประเมินประสิทธิภาพและประสิทธิผลของระบบตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติ ตลอดจนผลการเปรียบเทียบประสิทธิภาพและประสิทธิผลของระบบตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติในรูปแบบต่าง ๆ เป็นแนวทางเลือกใช้และพัฒนาระบบสารสนเทศเทคโนโลยีชีวมิติให้เหมาะสมกับสถานศึกษาด้วยความพร้อมและความต้องการที่แตกต่างกันได้อย่างเหมาะสม

บทที่ 2

ทบทวนวรรณกรรมที่เกี่ยวข้อง / ทฤษฎีที่เกี่ยวข้อง

2.1 การตรวจสอบบุคคลเข้าสอบ

การตรวจสอบผู้เข้าสอบในปัจจุบันของหลาย ๆ สถาบันการศึกษา มักจะใช้วิธีการตรวจสอบจากเอกสารของผู้เข้าสอบ ได้แก่บัตรประจำตัวนักศึกษา ในกรณีที่นักศึกษาไม่มีบัตรทำบัตรหายหรือชำรุด ต้องทำการขอใบรับรองการเป็นนักศึกษาซึ่งต้องมีอาจารย์ผู้สอนหรืออาจารย์ที่ปรึกษาเซ็นชื่อรับรองให้ ในบางครั้งอาจมีการผ่อนปรนให้สามารถใช้เอกสารที่ออกโดยรัฐบาลมายืนยัน เช่น บัตรประชาชนหรือใบขับขี่ เป็นต้น จากการเก็บข้อมูลโดยใช้วิธีการสังเกตจากการสอบของนักศึกษาระดับปริญญาตรี คณะวิทยาศาสตร์และเทคโนโลยีของมหาวิทยาลัยราชภัฏวไลยอลงกรณ์ ในพระบรมราชูปถัมภ์ สามารถอธิบายขั้นตอนในการตรวจสอบบุคคลเข้าสอบ โดยแสดงในรูปที่ 2.1



รูปที่ 2.1 แสดงขั้นตอนในการตรวจสอบบุคคลเข้าสอบโดยตรวจสอบจากเอกสาร

ที่มา: Rukhiran, Wong-In, & Netinant, 2023

จากรูปที่ 2.1 จะเห็นได้ว่ากรณีที่ผู้เข้าสอบไม่มีเอกสารในการตรวจสอบมีขั้นตอนที่ซับซ้อนในการยืนยันตัวผู้สอบทำให้เกิดความล่าช้าและวุ่นวายซึ่งอาจส่งผลกระทบต่อสมาธิของผู้เข้าสอบได้

2.2 เทคโนโลยีชีวมิติ

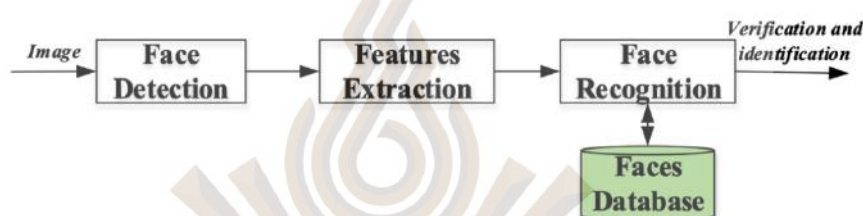
เทคโนโลยีชีวมิติ (Biometric Technology) คือเทคโนโลยีที่ใช้ในการจำแนกตัวบุคคลโดยนำชีวมิติที่บุคคลนั้น ๆ มี โดย Ahmed (2019) ได้ทำการจำแนกชีวมิติของบุคคลออกเป็นได้ 2 ประเภท ได้แก่ ชีวมิติทางกายภาพ (Physical Biometric) ได้แก่สิ่งบุคคลนั้นมี เช่น ใบหน้า ลายพิมพ์นิ้วมือ ฝ่ามือ ม่านตา และอื่น ๆ และชีวมิติทางพฤติกรรม (Behavior Biometric) ได้แก่พฤติกรรมหรือการกระทำของบุคคล เช่น เสียง ท่าทางการเดิน การเซ็นชื่อ และการเคลื่อนไหวแบบต่าง ๆ โดยการนำเทคโนโลยีชีวมิติไปประยุกต์ใช้มีวัตถุประสงค์หลักสองประการคือ เพื่อระบุตัวตนบุคคลและเพื่อควบคุมการเข้าถึงในระบบงานต่าง ๆ ประเด็นในการวิจัยค้นคว้าเกี่ยวกับเทคโนโลยีชีวมิติมีหลากหลายประเด็นที่แตกต่างกันออกไป อาทิเช่น การวิจัยเพื่อค้นหาอัลกอริทึมที่ดีที่สุดในการใช้เทคโนโลยีชีวมิติในรูปแบบต่าง ๆ การวิจัยเพื่อศึกษาโครงสร้างสถาปัตยกรรมของเทคโนโลยีชีวมิติ รวมถึงการค้นคว้าเพื่อหาคำตอบว่าควรใช้ชีวมิติแบบใดในการนำไปใช้กับเทคโนโลยีชีวมิติแล้วได้ประสิทธิภาพที่ดีที่สุด เป็นต้น

โดยทั่วไปการนำเทคโนโลยีชีวมิติไปพัฒนาเป็นระบบการตรวจสอบบุคคลสามารถแบ่งออกได้เป็น 2 แบบ ได้แก่ ระบบเทคโนโลยีชีวมิติแบบทางเดียว (Unimodal Biometric System) และระบบเทคโนโลยีชีวมิติแบบหลายทาง (Multimodal Biometric System) (Gawande & Golhar, 2018)

2.2.1 ระบบเทคโนโลยีชีวมิติแบบทางเดียว (Unimodal Biometric System)

2.2.1.1 การรู้จำใบหน้า (Face Recognition) คือ การจำแนกบุคคลโดยใช้ข้อมูลใบหน้าเป็นอีกหนึ่งชีวมิติที่มีการนำไปประยุกต์ใช้งานอย่างแพร่หลายมากที่สุด เช่น การตรวจจับใบหน้าที่ของอาชญากร ระบบรักษาความปลอดภัยในเขตที่อยู่อาศัย เป็นต้น เหตุผลที่การรู้จำบุคคลด้วยใบหน้าได้รับความนิยมมากเนื่องจากการจำแนกแบบพาสซีฟ (Passive Biometric) โดยผู้ใช้งานไม่จำเป็นต้องสัมผัสหรือกระทำใด ๆ ระบบจะสามารถจดจำใบหน้าโดยผู้ใช้งานผ่าน

กล้องที่เตรียมไว้เท่านั้น (Nguyen, Fookes, Sridharan, Tistarelli, & Nixon, 2018) การทำงานของระบบการรู้จำใบหน้าเป็นการทำงานด้วยหลักการปัญญาประดิษฐ์ที่ใช้การเรียนรู้เพื่อจดจำข้อมูลใบหน้าของบุคคลจำนวนหนึ่งและเก็บเอาไว้ในระบบฐานข้อมูลเพื่อที่จะถูกนำไปใช้ในการเปรียบเทียบกับข้อมูลบุคคลที่เข้ามาใช้งานระบบโดยใช้การวิเคราะห์จากรูปทรงและข้อมูลพื้นผิวบนใบหน้าเป็นหลัก ซึ่งการรู้จำข้อมูลใบหน้าประกอบด้วยการทำงาน 3 ขั้นตอนหลัก ได้แก่ การค้นหาใบหน้า (Face Detection) การสกัดข้อมูลใบหน้า (Face Extraction) และการรู้จำใบหน้า (Face Recognition) ดังแสดงในรูปที่ 2.2



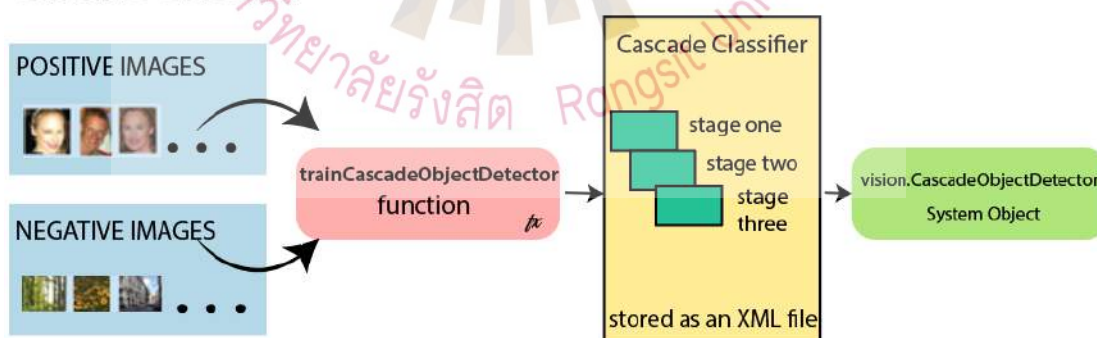
รูปที่ 2.2 แสดงขั้นตอนในการทำงานของการรู้จำใบหน้า

ที่มา: Kortli et al., 2020

1) การค้นหาใบหน้า (Face Detection) คือการหากรอบของใบหน้าจากภาพเพื่อที่จะกำหนดขอบเขตของใบหน้าของบุคคลนั้น ๆ โดยใช้วิธีการตรวจจับว่ามีพื้นที่ใดบ้างในภาพที่มีความเป็นไปได้ว่าเป็นใบหน้าของมนุษย์ วิธีการตรวจจับใบหน้าที่นิยมใช้กันอยู่ในปัจจุบันได้แก่การใช้อัลกอริทึมของ Haar Cascade ซึ่งเป็นวิธีการตรวจจับวัตถุที่นิยมใช้ในงานด้านคอมพิวเตอร์วิทัศน์และการประมวลผลภาพ โดยเฉพาะในการตรวจจับใบหน้า วิธีนี้คิดค้นโดย Paul Viola และ Michael Jones และตีพิมพ์บทความเมื่อปี พ.ศ. 2544 หลักการของ Haar Cascades คือการคำนวณความแตกต่างระหว่างพื้นที่ขาวและพื้นที่ดำภายในภาพ โดยมีขั้นตอนดังแสดงในรูปที่ 2.3 คุณลักษณะของ Haar มีหลายประเภท เช่น ขอบแนวนอน, ขอบแนวตั้ง, และสี่เหลี่ยม โดยมีขนาดและตำแหน่งที่แตกต่างกัน ดังแสดงในรูปที่ 2.4 จากนั้นใช้วิธีการ Adaboost ในขั้นตอนการเรียนรู้เพื่อที่จะเลือกคุณลักษณะของ Haar ที่สำคัญที่สุดสำหรับการตรวจจับวัตถุ ซึ่ง Adaboost (Adaptive Boosting) เป็นเทคนิคการเรียนรู้เชิงสถิติที่มีจุดมุ่งหมายในการรวมหลาย ๆ โมเดลอ่อน (Weak Classifiers) เข้าด้วยกันเพื่อสร้างโมเดลที่แข็งแกร่ง (Strong Classifiers) โดยมีขั้นตอน ได้แก่ สร้างโมเดลอ่อนจากข้อมูลฝึกอบรม คำนวณค่าความคลาดเคลื่อนของโมเดลอ่อน ปรับน้ำหนักตัวอย่างในชุดข้อมูลฝึกอบรม เน้นตัวอย่างที่ยากขึ้น คำนวณน้ำหนักของโมเดลอ่อน และรวมโมเดลอ่อนเพื่อสร้างโมเดลที่แข็งแกร่งการเรียนรู้ การใช้ Adaboost ช่วยให้โมเดลนั้น

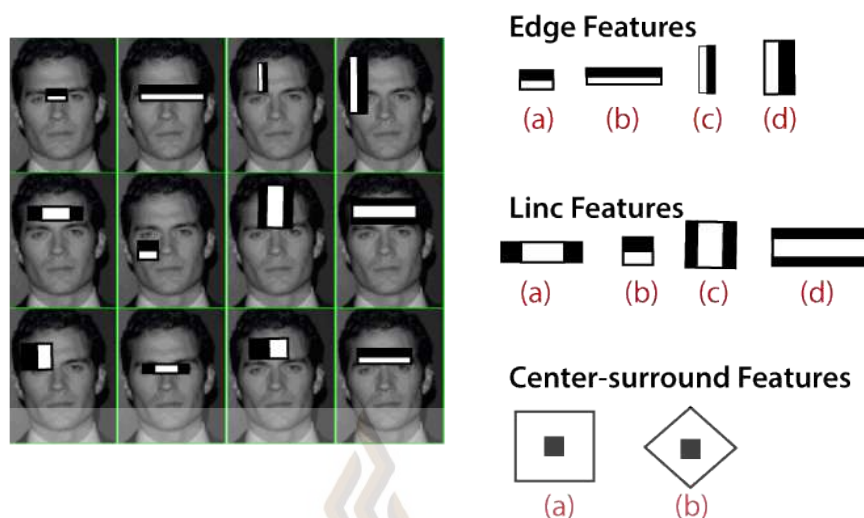
คุณลักษณะที่สามารถแยกวัตถุและพื้นหลังได้อย่างมีประสิทธิภาพ พร้อมทั้งลดขนาดของโมเดล ดังแสดงหลักการทำงานในรูปที่ 2.5 หลังจากเลือกคุณลักษณะของ Haar จากนั้นจะเป็นการสร้าง Cascade Classifier ซึ่งมีลักษณะเป็นขั้น ๆ ในการตัดสินใจ แต่ละขั้นของ Cascade Classifier จะมีคุณลักษณะของ Haar ที่สามารถตัดสินใจว่าบริเวณนั้นมีวัตถุที่สนใจหรือไม่ หากบริเวณนั้นผ่านการตรวจสอบจากขั้นแรก มันจะถูกส่งไปยังขั้นถัดไปของ Cascade Classifier ทำขั้นตอนนี้ไปเรื่อย ๆ จนกระทั่งผ่านขั้นสุดท้าย หากบริเวณนั้นผ่านการตรวจสอบจาก Cascade Classifier ทั้งหมด ระบบจะถือว่าบริเวณนั้นมีวัตถุที่สนใจอยู่ และเมื่อ Cascade Classifier ถูกสร้างขึ้น เราสามารถนำ Cascade Classifier มาใช้ในการตรวจจับวัตถุในภาพใหม่ เช่น การตรวจจับใบหน้า ระบบจะตรวจสอบภาพ และปรับขนาดของหน้าต่างตรวจจับให้เหมาะสมกับขนาดของวัตถุที่สนใจ โดยจะถือว่าตรวจพบเมื่อผ่านการตรวจสอบจาก Cascade Classifier ทั้งหมด โดยสรุป Haar Cascades มีข้อดีในเรื่องความเร็วในการตรวจจับวัตถุและตรวจจับใบหน้าได้ดีในกรณีที่มีการปรับเปลี่ยนเล็กน้อยในหน้าต่างรูป โดยเฉพาะในสถานะที่มีแสงสว่างเพียงพอ อย่างไรก็ตาม ข้อจำกัดของ Haar Cascades คือความไม่แม่นยำในกรณีที่มีการหมุนหน้าหรือมีการปิดหน้าเป็นส่วนหนึ่ง การใช้ Haar Cascades ในการตรวจจับใบหน้าเป็นเพียงขั้นตอนแรกในกระบวนการทำ Face Recognition การรวมกันกับวิธีการอื่น ๆ จะช่วยเพิ่มประสิทธิภาพและความแม่นยำในการรู้จำใบหน้า การเลือกใช้วิธีใดขึ้นอยู่กับความต้องการของแอปพลิเคชัน, ข้อจำกัดของทรัพยากร, และความซับซ้อนของโจทย์ที่ต้องการแก้ไข

Cascade Classifier



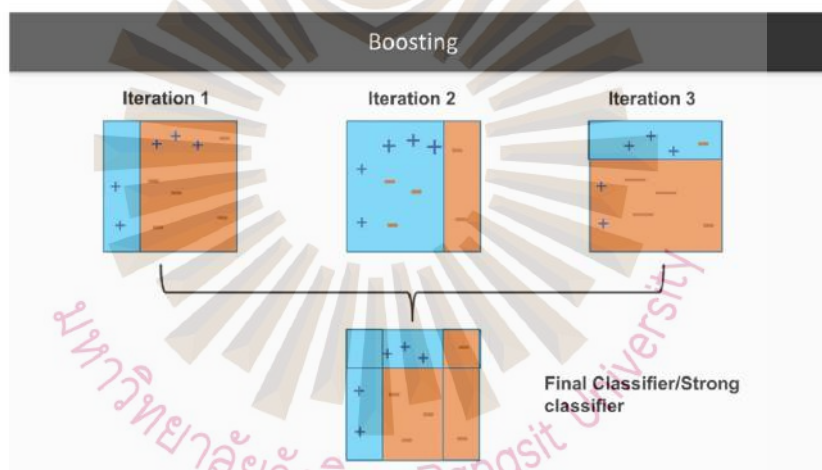
รูปที่ 2.3 แสดงหลักการทำงานของ Haar Cascade

ที่มา: OpenCV, 2023



รูปที่ 2.4 แสดงภาพ คุณลักษณะของ Haar ประเภทต่าง ๆ

ที่มา: JavaTPoint, 2021

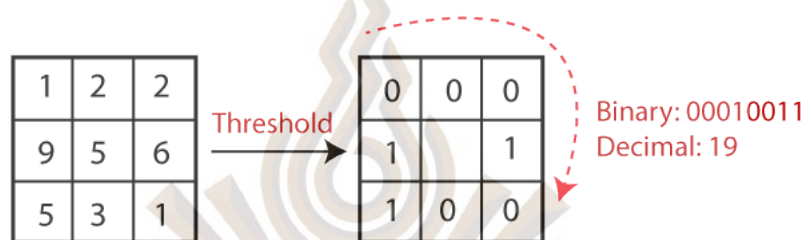


รูปที่ 2.5 แสดงหลักการทำงานของ Adaboost

ที่มา: OpenCV, 2023

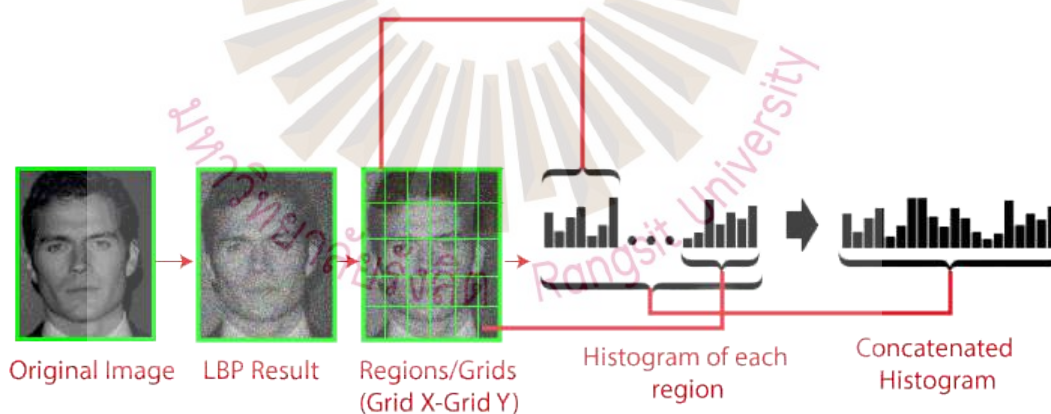
2) การสกัดลักษณะของใบหน้า (Feature Extraction) หมายถึงการแปลงภาพใบหน้าของบุคคลเป็นเวกเตอร์คุณลักษณะ (Feature Vector) ที่มีคุณสมบัติเฉพาะเจาะจงของแต่ละบุคคล ซึ่ง Feature Vector นี้จะใช้เป็นข้อมูลเข้าในระบบการเรียนรู้ของระบบต่อไป กระบวนการสกัดคุณลักษณะสำคัญของใบหน้าเพื่อใช้ในการจำแนกและระบุตัวตนของบุคคล ในปัจจุบันมีหลากหลายวิธีในการสกัดคุณลักษณะของใบหน้า ขึ้นอยู่กับวิธีการและขั้นตอนที่ใช้ โดยวิธีการที่ได้รับความนิยมในการทำการสกัดข้อมูลใบหน้า ได้แก่ (1) วิธีการ Eigenfaces โดยวิธีนี้ใช้การวิเคราะห์ส่วนประกอบหลัก (PCA) เพื่อลดขนาดของข้อมูลใบหน้า โดยสกัดคุณลักษณะที่สำคัญ

ที่สุดที่สามารถบ่งบอกความแตกต่างของใบหน้าแต่ละบุคคล (2) วิธีการ Fisherfaces โดยวิธีนี้ใช้การวิเคราะห์แบบเชิงเส้น (Linear Discriminant Analysis: LDA) เพื่อสกัดคุณลักษณะที่สามารถแยกแยะใบหน้าของคนต่างกันได้ดีที่สุดโดยให้ความสำคัญกับความแตกต่างของกลุ่มต่าง ๆ บนใบหน้า และ (3) วิธีการ Local Binary Patterns Histograms (LBPH) โดยวิธีการนี้สกัดคุณลักษณะของใบหน้าโดยเปรียบเทียบความสว่างของพิกเซลกับพิกเซลใกล้เคียง ทั้งสามวิธีการเป็นวิธีการในการสกัดคุณลักษณะของการรู้จำใบหน้าที่นิยมใช้กัน โดยใช้ OpenCV เป็นกรอบในการพัฒนา โดยงานวิจัยนี้ได้ใช้วิธีการ LBP ในการทดลอง ดังแสดงการทำงานของ LBPH ดังรูปที่ 2.6 และ 2.7 โดยอธิบายรายละเอียดใน ส่วนที่ 2.3 OpenCV Framework



รูปที่ 2.6 แสดงหลักการทำงาน Feature Extraction โดยใช้ LBP

ที่มา: JavaTPoint, 2021



รูปที่ 2.7 แสดงตัวอย่าง Feature Extraction โดยใช้ LBP

ที่มา: JavaTPoint, 2021

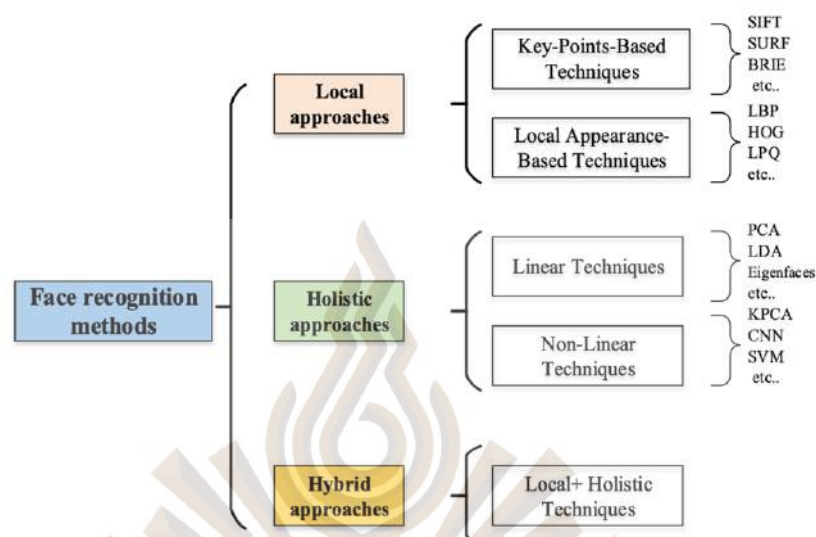
3) การรู้จำใบหน้า (Face Recognition) เป็นขั้นตอนที่ทำการสอน (Train) ให้ระบบสามารถจดจำใบหน้าของบุคคลได้ การทำการสอนสำหรับการทำรู้จำใบหน้า มีหลายวิธี วิธีที่ได้รับความนิยมมากที่สุดวิธีหนึ่ง ได้แก่การใช้งาน Convolutional Neural Networks (CNN) ในการเรียนรู้ลักษณะของใบหน้า และตรวจจับใบหน้าของบุคคลที่ต่างกัน โดยวิธีการทำการสอน

ด้วย CNN นั้นจะมีขั้นตอน คือ เตรียมข้อมูลรูปภาพใบหน้าที่จะนำมาทำการสอนให้ตัวต้นแบบ โดยภาพใบหน้าที่เตรียมมาต้องเป็นรูปภาพใบหน้าที่มีขนาดเท่ากัน มีการปรับแต่งรูปภาพใบหน้า เช่น การปรับแสง (Lighting), การปรับสี (Color) เป็นต้น เพื่อให้ได้ผลลัพธ์ที่ดีที่สุด จากนั้นแบ่งกลุ่มภาพใบหน้าโดยแบ่งเป็น 3 ชุด ได้แก่ Train set, Validation set และ Test set จากนั้นทำการสร้างโมเดล CNN ด้วย Framework ที่เหมาะสม เช่น TensorFlow, Keras หรือ PyTorch เมื่อสร้างโมเดล CNN แล้ว เริ่มทำการสอนตัวต้นแบบด้วยข้อมูลรูปภาพใบหน้าที่เตรียมไว้ โดยปรับค่าพารามิเตอร์ของโมเดลเพื่อให้มีผลลัพธ์ที่ดีขึ้น ขั้นตอนสุดท้ายคือการทดสอบโมเดลด้วยชุด Test Set เพื่อวัดประสิทธิภาพของโมเดลว่ามีความแม่นยำมากพอที่จะนำไปใช้งานได้หรือไม่ การเลือกใช้เทคนิคการ ทำการสอนสำหรับ การรู้จำใบหน้าขึ้นอยู่กับความต้องการและความซับซ้อนของงาน โดยมีปัจจัยหลายอย่างที่ต้องพิจารณา อาทิเช่น ปริมาณของข้อมูลใบหน้า, ระยะเวลาในการสอน, ประสิทธิภาพที่ต้องการ, ความซับซ้อนของโมเดล เป็นต้น (Krizhevsky, Sutskever, & Hinton, 2017)

การจับคู่คุณลักษณะ (Feature Matching) เป็นขั้นตอนสำคัญในกระบวนการทำ Face Recognition ซึ่งเป้าหมายคือการเปรียบเทียบความคล้ายคลึงระหว่างคุณลักษณะของใบหน้าที่ต้องการระบุตัวตนกับคุณลักษณะของใบหน้าที่มีอยู่ในฐานข้อมูล เพื่อระบุตัวตนของบุคคลนั้น ขั้นตอนการทำ Feature Matching ใน Face Recognition เป็นขั้นตอนต่อจากการสกัดคุณลักษณะของใบหน้า ซึ่งเริ่มตั้งแต่ขั้นตอนการตรวจจับใบหน้า เพื่อที่จะได้ภาพของใบหน้าที่ต้องการระบุตัวตนโดยทำการสกัดคุณลักษณะของใบหน้านั้น มีหลากหลายวิธีการ เช่น ใช้วิธี Local Binary Patterns Histograms (LBPH), Eigenfaces, หรือ Fisherfaces เป็นต้น จากนั้นทำการสร้างฐานข้อมูลคุณลักษณะจัดเก็บใบหน้าไว้ในฐานข้อมูล โดยให้สกัดคุณลักษณะของแต่ละใบหน้าและจัดเก็บไว้ในรูปแบบที่เหมาะสมสำหรับการค้นหาและเปรียบเทียบ จากนั้นจึงจะสามารถทำการเปรียบเทียบคุณลักษณะได้โดยนำคุณลักษณะที่สกัดจากใบหน้าที่ต้องการระบุตัวตนมาเปรียบเทียบกับคุณลักษณะของใบหน้าในฐานข้อมูล ซึ่งสามารถใช้วิธีการคำนวณระยะห่างยูคลิด (Euclidean Distance) หรือความคล้ายคลึงโคไซน์ (Cosine Similarity) เพื่อการเปรียบเทียบความคล้ายคลึงของใบหน้า ในการตัดสินใจเกี่ยวกับการจับคู่ใบหน้า เมื่อได้ผลการเปรียบเทียบความคล้ายคลึงของคุณลักษณะใบหน้าแล้ว ให้ทำการประเมินความคล้ายคลึงระหว่างใบหน้าที่ต้องการระบุตัวตนกับใบหน้าที่มีอยู่ในฐานข้อมูล หากความคล้ายคลึงอยู่ในเกณฑ์ที่ยอมรับ ก็ถือว่าการจับคู่ใบหน้าสำเร็จ

การทำงานทั้ง 3 ขั้นตอนที่กล่าวมานั้นมีการประยุกต์ใช้เทคนิคที่ต่างกัน และเป็นประเด็นที่หลากหลายในการทำวิจัยทางด้านเทคโนโลยีชีวมิติ ยกตัวอย่างเช่น ในขั้นตอน

การรู้จำใบหน้าในงานของ Kortli et al. (2020) ได้นำเสนอวิธีการในการรู้จำใบหน้า โดยนำเสนอวิธีการในการสกัดข้อมูลทั้ง 3 แบบ ได้แก่ Local Approach, Holistic Approach และ แบบ Hybrid Approach ดังแสดงในรูปที่ 2.8

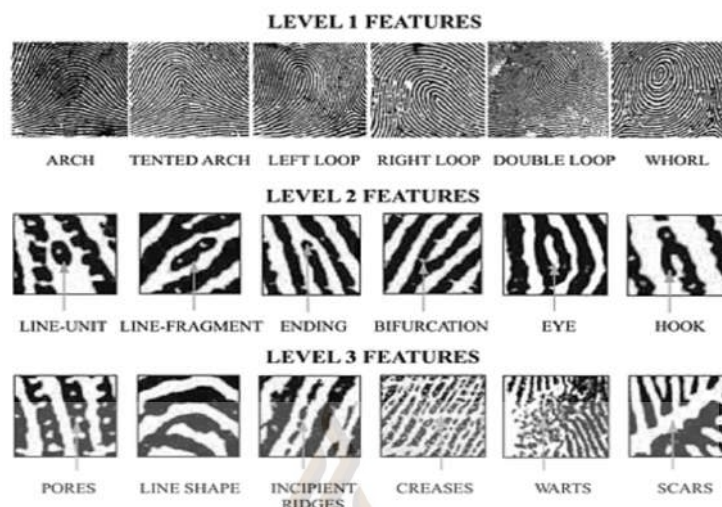


รูปที่ 2.8 แสดงตัวอย่างการใช้หลักการต่าง ๆ ในการรู้จำใบหน้า

ที่มา: Kortli et al., 2020

2.2.1.2 การรู้จำลายพิมพ์นิ้วมือ (Fingerprint Recognition) เป็นอีกวิธีที่ใช้ในการระบุตัวบุคคลโดยใช้ลายพิมพ์นิ้วมือ วิธีการนี้เป็นการระบุตัวบุคคลที่มีความแม่นยำสูงมากหรือน้อยขึ้นอยู่กับตัวอุปกรณ์ที่ใช้ในระบบ ซึ่งการใช้อุปกรณ์ที่ต่างกันอาจมีผลทำให้ได้ข้อมูลลายพิมพ์นิ้วมือในรูปแบบที่แตกต่างกัน บางครั้งระบบการจำแนกตรวจสอบบุคคลโดยใช้ลายพิมพ์นิ้วมือนั้นเป็นระบบปิดซึ่งสามารถใช้งานได้เฉพาะบางอุปกรณ์เฉพาะเท่านั้น เช่น การเก็บข้อมูลของโทรศัพท์มือถือที่ใช้ iOS เป็นระบบปฏิบัติการกับการเก็บข้อมูลลายพิมพ์นิ้วมือของโทรศัพท์มือถือที่ใช้ระบบปฏิบัติการ Android ก็มีเทคนิคในการทำงานที่ต่างกัน หลักการในการรู้จำลายพิมพ์นิ้วมือการใช้ลายพิมพ์นิ้วมือในการจำแนกมีความแม่นยำสูงและสามารถจำแนกได้แม่นยำกว่าการใช้ใบหน้าในการจำแนกในกรณีที่บุคคลที่มีใบหน้าใกล้เคียงกันหรือในกรณีแฝดซึ่งลายพิมพ์นิ้วมือของมนุษย์มีโอกาสที่จะคล้ายกันน้อยมาก

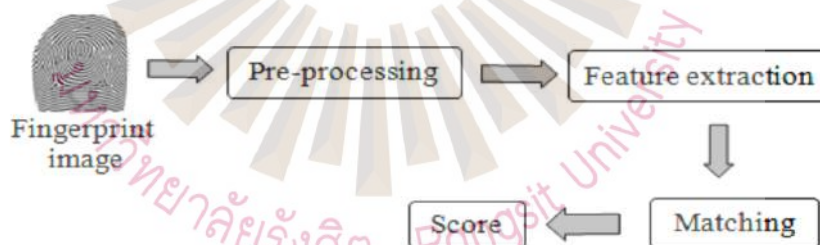
จากการศึกษาของ Soni and Goyani (2019) ได้จำแนกลักษณะของลายพิมพ์นิ้วมือได้ 3 แบบ ได้แก่ โดยแสดงดังรูปที่ 2.9



รูปที่ 2.9 แสดงประเภทของลายพิมพ์นิ้วมือ

ที่มา: Soni and Goyani, 2019

ขั้นตอนในการรู้จำลายพิมพ์นิ้วมือมีขั้นตอนคล้ายกับการรู้จำใบหน้า ได้แก่ การเตรียมการ (Pre-Processing) การสกัดส่วนประกอบ (Feature Extraction) การจับคู่ (Matching) และการให้คะแนน (Score) ดังแสดงในรูปที่ 2.10



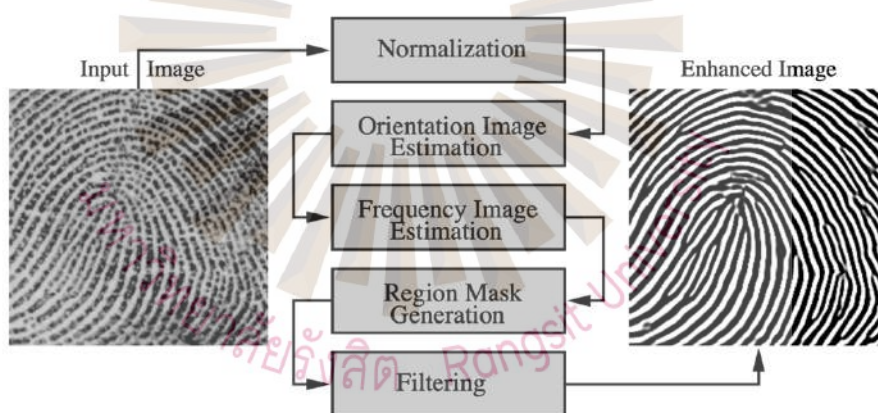
รูปที่ 2.10 แสดงขั้นตอนในการทำงานของการรู้จำลายพิมพ์นิ้วมือ

ที่มา: Soni and Goyani, 2019

จากรูปที่ 2.10 กระบวนการ Fingerprint Recognition ประกอบด้วยขั้นตอนดังนี้

- 1) การส่งสแกนลายพิมพ์นิ้วมือ (Fingerprint Image) โดยให้ผู้ใช้วางนิ้วที่เครื่องสแกนลายพิมพ์นิ้วมือ เพื่อส่งภาพลายพิมพ์นิ้วมือไปยังระบบ
- 2) การปรับปรุงคุณภาพภาพลายพิมพ์นิ้วมือ (Pre-processing หรือ Image Enhancement) เป็นการลบสัญญาณรบกวน ปรับความคมชัด และปรับปรุงความสว่างของภาพให้ภาพลายพิมพ์นิ้วมือมีคุณภาพที่เหมาะสมสำหรับการสกัดคุณลักษณะ Hong, Wan, & Jain (1998) ได้นำเสนอขั้นตอนในการปรับปรุงคุณภาพภาพลายพิมพ์นิ้วมือ โดยเริ่มจากการทำ Normalization

โดยใช้การหา Z-score Normalization, Min-Max Normalization หรือ Decimal Scaling Normalization การประมาณค่า Orientation Image Estimation คือเป็นวิธีการในการประมวลผลภาพดิจิทัลของรูปภาพลายพิมพ์นิ้วมือเพื่อหาค่ามุมหมุนของภาพนั้น ๆ โดยการหาค่ามุมหมุนจะช่วยให้สามารถแปลความหมายของรูปภาพนิ้วมือได้ถูกต้อง โดยส่วนใหญ่การหาค่ามุมหมุนจะใช้วิธีการหา และนำมาคำนวณเพื่อหาค่าความเอียงของแต่ละจุดในภาพ การประมาณค่า Frequency Image เป็นวิธีการในการประมวลผลภาพเพื่อหาความถี่ของแนวร่องของนิ้วมือ (Ridge Frequency) ซึ่งการหาความถี่ของแนวร่องนิ้วมือจะใช้วิธีการหา Gradient หรือเกรเดียนท์ในรูปของภาพเช่นเดียวกับการหาค่ามุมหมุนของภาพนิ้วมือ โดยจะนำค่า Gradient มาคำนวณเพื่อหาความถี่ของแนวร่องแต่ละจุดในภาพ จากนั้นทำการสร้าง Region Mask ซึ่งเป็นวิธีการในการสร้างแผนที่ของพื้นที่ที่สนใจเพื่อนำไปใช้ในการตรวจจับวัตถุหรือแยกแยะวัตถุในภาพ โดยการสร้าง Region Mask นั้นจะใช้ข้อมูลจากการวิเคราะห์ภาพ ซึ่งการสร้าง Region Mask นั้นสามารถทำได้หลายวิธี เช่น การใช้วิธีการแยกแยะเลเยอร์ (Layer Separation) หรือการใช้เทคนิคการกำหนดค่าความสนใจ (Interest Point Detection) และทำการ Filtering โดยใช้ Gabor Filter ดังแสดงในรูปที่ 2.11

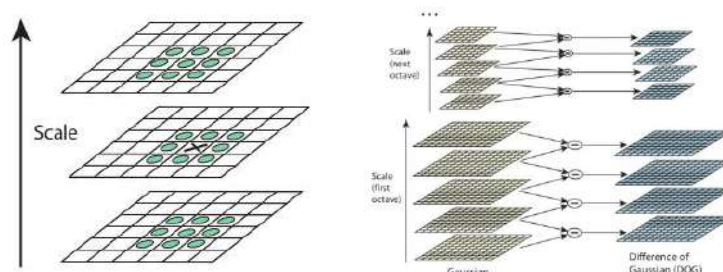


รูปที่ 2.11 แสดงขั้นตอนในการปรับปรุงคุณภาพลายพิมพ์นิ้วมือ

ที่มา: Hong et al., 1998

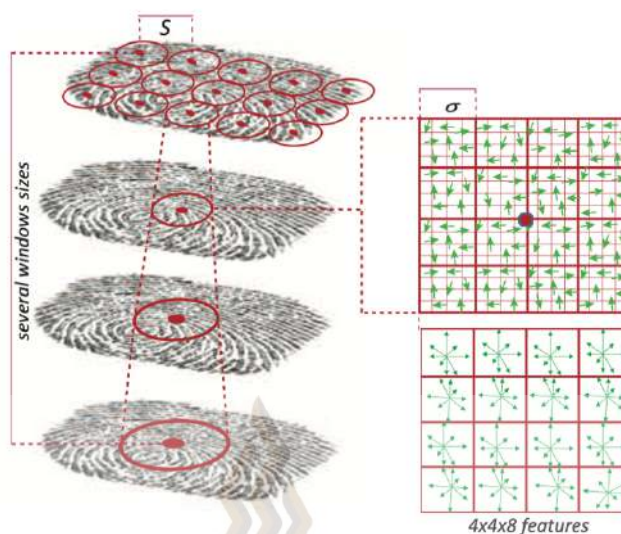
3) การสกัดคุณลักษณะของลายพิมพ์นิ้วมือ (Feature Extraction): สกัดคุณลักษณะที่สำคัญของลายพิมพ์นิ้วมือ เช่น Minutiae Points (Bifurcations และ Ridge Endings) หรือ Ridge Patterns และเก็บข้อมูลเหล่านี้ไว้ในรูปแบบที่เหมาะสม โดยอัลกอริทึมที่นิยมใช้ในการสกัดคุณลักษณะของลายพิมพ์นิ้วมือได้แก่ Scale-Invariant Feature Transform (SIFT) เป็นเทคนิคการประมวลผลภาพแบบคอมพิวเตอร์ที่ใช้สำหรับหาคุณลักษณะหรือสิ่งที่เป็เอกลักษณ์ในภาพ โดย SIFT จะสร้าง Feature Descriptor ซึ่งเป็นเวกเตอร์ที่แสดงลักษณะเฉพาะของภาพ เพื่อนำไปใช้

ในการจับคู่ระหว่างภาพ โดย SIFT มีขั้นตอนการทำงานดังนี้ (1) การหาจุดความสนใจในภาพ (Keypoint) โดย SIFT จะใช้วิธี Difference of Gaussians (DoG) ในการหาจุดความสนใจของภาพ โดยจะสร้าง Gaussian Pyramid ของภาพ และหา DoG ของระดับที่ต่ำกว่า โดยจุดความสนใจจะเป็นจุดที่มีความแตกต่างของค่า DoG รอบ ๆ กัน (2) การกำหนดทิศทางและขนาดของ Keypoint โดย SIFT จะกำหนดทิศทางและขนาดของ Keypoint โดยใช้ Gradient Orientation Histogram ซึ่งจะคำนวณค่าการกระจายของ Gradient ของภาพในบริเวณรอบ ๆ Keypoint เพื่อหาทิศทางที่สำคัญ และสร้าง Histogram ขึ้นมา (3) การสร้างเวกเตอร์ลักษณะ (Feature Descriptor) SIFT จะใช้ Local Image Descriptor ในการสร้าง Feature Descriptor โดยจะแบ่งบริเวณรอบ ๆ Keypoint เป็นหลายๆ บล็อก แล้วคำนวณ Gradient Orientation Histogram ของแต่ละบล็อก จากนั้น SIFT จะสร้างเวกเตอร์ลักษณะโดยใช้ข้อมูลจาก Gradient Orientation Histogram ของแต่ละบล็อก เพื่อสร้างเวกเตอร์ลักษณะที่มีขนาดคงที่ 128 ช่อง โดยใช้วิธีการ Normalize ให้มีค่าไม่เกิน 0.2 และป้องกันการเกิดสิ่งทีเรียกว่า Illumination Variance ซึ่งอาจเกิดจากความแตกต่างของความสว่างของภาพในแต่ละบริเวณ และใช้วิธีการหา Principal Component Analysis (PCA) เพื่อลดขนาดของเวกเตอร์ลักษณะให้เหลือเพียง 128 ช่อง โดยเลือกเฉพาะช่องที่มีค่าสูงสุดในแต่ละ Block เพื่อใช้เป็นค่าลักษณะของบล็อกนั้น ๆ (4) การจับคู่ระหว่าง Keypoint ในภาพที่แตกต่างกัน SIFT จะใช้ Euclidean Distance ในการหา Keypoint ที่มีค่าลักษณะที่ใกล้เคียงกัน ซึ่งจะเป็นการจับคู่ระหว่างภาพที่แตกต่างกัน สรุปได้ว่า SIFT ใช้การหา Keypoint จากการสร้าง Gaussian Pyramid และ DoG ของภาพ จากนั้นกำหนดทิศทางและขนาดของ Keypoint ด้วย Gradient Orientation Histogram และสร้าง Feature Descriptor จาก Local Image Descriptor และ PCA สุดท้ายคือการจับคู่ระหว่าง Keypoint ในภาพที่แตกต่างกัน ด้วย Euclidean Distance (Zhou, Zhong, & Han, 2013; González-Soler, Gomez-Barrero, Chang, Pérez-Suárez, & Busch, 2021) ดังแสดงในรูปที่ 2.12 และ 2.13



รูปที่ 2.12 แสดง Gaussian Pyramid

ที่มา: Zhou et al., 2013

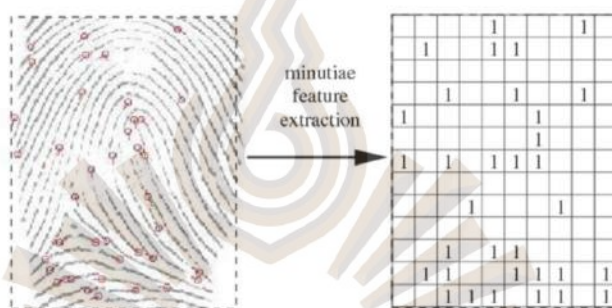


รูปที่ 2.13 แสดง SIFT Descriptor

ที่มา: González-Soler et al., 2021

4) การจับคู่คุณลักษณะ (Matching): เปรียบเทียบคุณลักษณะของลายพิมพ์นิ้วมือที่สแกนใหม่กับคุณลักษณะของลายพิมพ์นิ้วมือที่มีอยู่ในฐานข้อมูล ซึ่งสามารถใช้วิธีต่าง ๆ เช่น Euclidean Distance, Cosine Similarity, หรือ Fast Library for Approximate Nearest Neighbors (FLANN) ในการเปรียบเทียบความคล้ายคลึงของคุณลักษณะ หากความคล้ายคลึงของคุณลักษณะอยู่ในเกณฑ์ที่ยอมรับ สามารถพิจารณาว่าการจับคู่ลายพิมพ์นิ้วมือสำเร็จ และทำการระบุตัวตนของบุคคลนั้น โดย FLANN เป็นไลบรารีที่ใช้ในการค้นหาเพื่อนบ้านที่ใกล้เคียงที่สุด (Nearest Neighbors) แบบโดยประมาณอย่างรวดเร็ว โดยจะใช้วิธีการที่เรียกว่า Hierarchical Clustering ในการจัดเรียงข้อมูลเพื่อช่วยให้การค้นหาเพื่อนบ้านที่ใกล้เคียงมีประสิทธิภาพสูงสุด โดย FLANN สามารถใช้กับการรู้จำลายพิมพ์นิ้วมือ (Fingerprint Recognition) ได้โดยการนำลายพิมพ์นิ้วมือของผู้ใช้เป็นตัวอย่างแล้วนำไปสร้างเป็น Feature Vectors ด้วยวิธีการ PCA (Principal Component Analysis) หรือ LDA (Linear Discriminant Analysis) (Maltoni, Maio, Jain, & Prabhakar, 2009) ดังแสดงในรูปที่ 2.14 จากนั้น FLANN จะนำ Feature Vectors เหล่านี้มาสร้างเป็นโครงสร้างของต้นไม้ (Tree Structure) ที่ใช้ในการค้นหาเพื่อนบ้านที่ใกล้เคียง โดยที่ FLANN จะใช้วิธีการที่เรียกว่า KD-Tree (K-Dimensional Tree) ดังแสดงในรูปที่ 2.15 ในการสร้างโครงสร้างต้นไม้เพื่อช่วยให้การค้นหาเพื่อนบ้านที่ใกล้เคียงเป็นไปอย่างรวดเร็วและมีประสิทธิภาพสูงสุด หลังจากที่ FLANN ได้สร้างโครงสร้างต้นไม้จาก Feature Vectors ของลายพิมพ์นิ้วมือแล้ว จะสามารถใช้ต้นไม้เหล่านี้ในการค้นหาเพื่อนบ้านที่ใกล้เคียงที่สุดของลายพิมพ์นิ้วมือใหม่ได้ โดย FLANN จะเริ่มต้นค้นหาจาก Node แรกของต้นไม้ แล้วดูที่ Feature Vector ของ Node นั้น แล้วหา Feature Vector ที่ใกล้เคียง

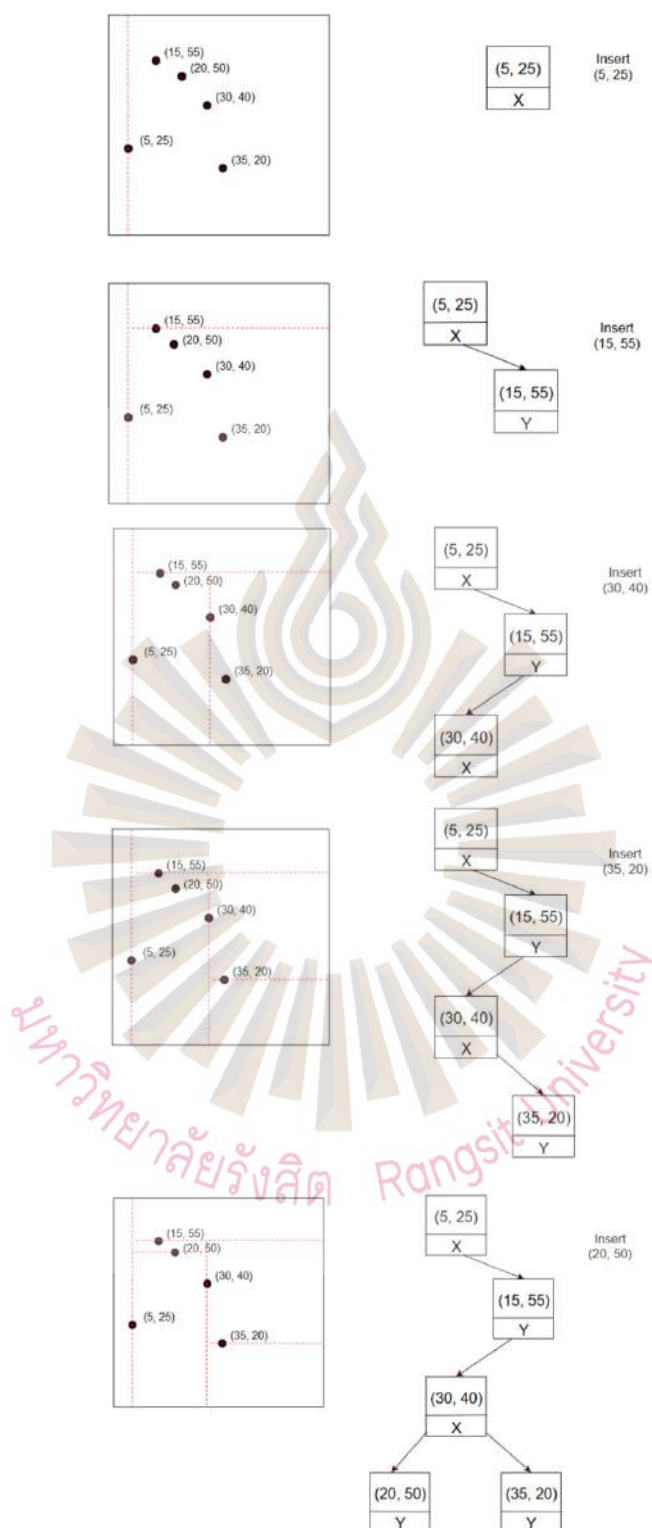
ที่สุด โดยการดูว่า Feature Vector ของ Node ปัจจุบันอยู่ในกลุ่มที่ใกล้เคียงกับ Feature Vector ของ Node ต่อไปหรือไม่ ถ้าใกล้เคียงกันมากพอ FLANN จะเดินทางไป Node ต่อไป และทำการค้นหาอีกครั้งจนกว่าจะเจอ LeafNode ซึ่งจะเก็บลายพิมพ์นิ้วมือที่ใกล้เคียงที่สุด โดย FLANN จะคืนค่า ID ของ LeafNode นี้กลับมาเพื่อบอกว่าลายพิมพ์นิ้วมือที่ใหม่นี้ตรงกับลายพิมพ์นิ้วมือใดในฐานข้อมูล ดังแสดงในรูปที่ 2.16 ด้วยวิธีการที่ FLANN ใช้ในการค้นหาเพื่อนบ้านที่ใกล้เคียงอย่างรวดเร็วและมีประสิทธิภาพสูง ทำให้ FLANN เป็นเครื่องมือที่น่าสนใจสำหรับการทำ Fingerprint Recognition โดยเฉพาะในกรณีที่มีจำนวนข้อมูลมาก หรือต้องการค้นหาข้อมูลที่ใกล้เคียงอย่างแม่นยำ



รูปที่ 2.14 แสดง Feature Factor โครงสร้างของ FLANN

ที่มา: Maltoni et al., 2009

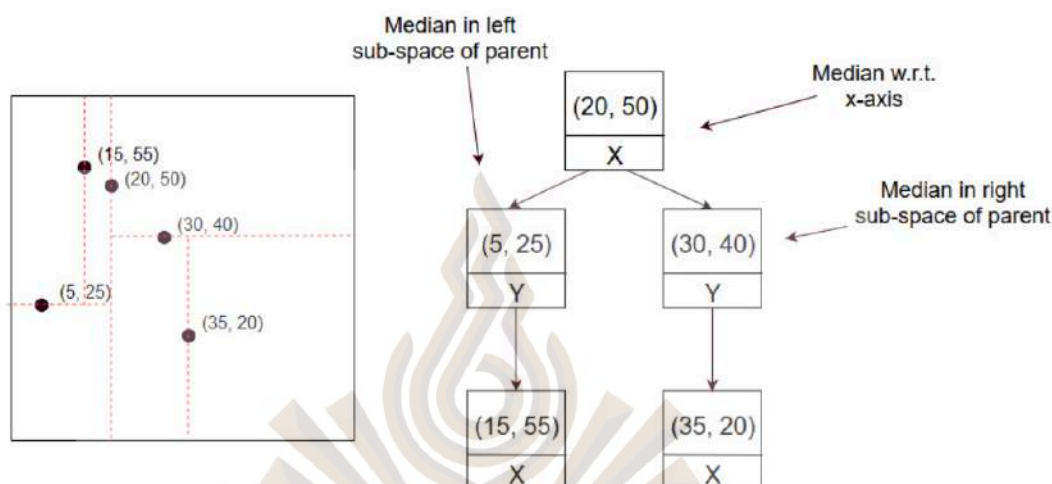
รูปที่ 2.15 แสดงโครงสร้างต้นไม้ KD-Tree ของ Feature Vector โดยทำการแปลงลายพิมพ์นิ้วมือให้เป็น Feature Vector โดยกำหนดให้แต่ละพิกัดเป็น ขั้นตอนทั่วไปในการสร้าง KD Tree คือการแบ่งพื้นที่แบบวนซ้ำเป็น 2 ส่วนตามแนวแกนที่มีการแผ่กว้างที่สุด ทุกโหนดในแผนผังต้นไม้ ระบุตามมิติที่พื้นที่ถูกแบ่งโดยโหนด ตัวอย่างในรูปที่ 2.15 ประกอบด้วย 5 พิกัด ได้แก่ (5, 25), (15, 55), (30, 40), (35, 20), และ (20, 50) ซึ่งเป็นตัวแทนของ Feature Vector ของลายพิมพ์นิ้วมือ และมีกระบวนการสร้างเริ่มจากค้นหาต้นไม้สำหรับค่า (x, y) จนกว่าจะถึงโหนดปลายทางสุด ถ้าต้นไม้ว่างเปล่า ให้เพิ่มโหนดใหม่เป็นรูทแทนจุด (x, y) โดย ซึ่งในจุดนี้สามารถแบ่งพื้นที่ตามแกนใดก็ได้ ระบุแกนที่แบ่งช่องว่างและสิ้นสุดการเพิ่มโหนด นั่นคือโหนดที่เป็นรูทคือ (5,25) จากนั้นแทรกโหนดใหม่ (15,55) ถ้าพารามิเตอร์แบ่งพื้นที่ตามแกน y ให้จุดแบ่งพื้นที่ตามแกน x ดังนั้นการเพิ่มพิกัด (15,55) จะใช้ค่าในแกน x ในการเปรียบเทียบ ถ้าค่า ในแกน x มากกว่า ให้ใส่โหนดใหม่ทางขวา แต่ถ้าน้อยกว่าให้ใส่ทางซ้าย ในกรณีนี้ค่า x ของโหนดใหม่มีค่ามากกว่า (5<15) จึงทำการใส่ค่า (15,55) ในโหนดทางขวา ทำแบบนี้ไปเรื่อย ๆ จนกระทั่งครบทุกพิกัด ดังแสดงขั้นตอนในรูปที่ 2.15



รูปที่ 2.15 แสดงขั้นตอนในการสร้างโครงสร้างต้นไม้ KD-Tree ของ Feature Vector

ที่มา: Aggarwal, 2020

เมื่อได้โครงสร้างต้นไม้ดังรูปที่ 2.15 แล้วต้องพิจารณาถึงความสมดุลทั้งสองฝั่งของโครงสร้างต้นไม้ ในกรณีที่โครงสร้างต้นไม้ขาดความสมดุล ให้ใช้ค่ามัธยฐานในการปรับสมดุลเมื่อปรับแล้วจะได้โครงสร้างต้นไม้ที่สมดุล ดังแสดงในรูปที่ 2.16 จะมีลักษณะดังนี้



รูปที่ 2.16 แสดงโครงสร้างต้นไม้ KD-Tree ของ Feature Vector

ที่มา: Aggarwal, 2020

ในการทำการค้นหาเพื่อเปรียบเทียบลายพิมพ์นิ้วมือ โดยวิธีการ FLANN ในโครงสร้าง KD-Tree ประกอบด้วย 3 ขั้นตอน ได้แก่ (1) ขั้นตอนที่ 1 ถ้าโหนดปัจจุบันเป็นจุด (x, y) ให้คืนค่าเป็นจริง (True), (2) ขั้นตอนที่ 2 ถ้าโหนดปัจจุบันไม่ใช่ LeafNode ให้เข้าไปทำตามขั้นตอนที่ 3 มิฉะนั้นให้คืนค่าเป็นเท็จ (False) และ (3) ขั้นตอนที่ 3 กำหนดให้โหนดปัจจุบันเป็นจุด (X, Y) ถ้าโหนดนี้แบ่งพื้นที่ตามแกน x , เปรียบเทียบ x กับ X ถ้า $x < X$ กำหนดโหนดปัจจุบันเป็นโหนดลูกด้านซ้าย (Left Child) มิฉะนั้นกำหนดโหนดปัจจุบันเป็นโหนดลูกด้านขวา (Right Child) หากโหนดนี้แบ่งพื้นที่ตามแกน y จากนั้นทำการเปรียบเทียบ y กับ Y กลับไปที่ขั้นตอนที่ 1

5) การตัดสินใจเกี่ยวกับการระบุตัวตน (Score) เป็นการให้คะแนนโดยให้ระบบตัดสินใจว่าภาพลายพิมพ์นิ้วมือที่สแกนเข้ามานั้น เป็นของบุคคลใดในฐานข้อมูล หรือไม่ตรงกับข้อมูลใดเลย ซึ่งขึ้นอยู่กับความคล้ายคลึงของคุณลักษณะและเกณฑ์ที่กำหนด

2.2.2 ระบบเทคโนโลยีชีวมิติแบบผสม (Multimodal Biometric System)

ในบางครั้งการใช้เทคโนโลยีชีวมิติต้องการระบบที่มีประสิทธิภาพสูง จึงมีแนวคิดใหม่ที่จะใช้เทคโนโลยีชีวมิติแบบผสมเพื่อเพิ่มประสิทธิภาพให้กับระบบชีวมิตินั้น ๆ โดยระบบเทคโนโลยีชีวมิติแบบผสมสามารถแบ่งย่อยได้เป็น 4 กลุ่ม ดังนี้

- 1) ใช้เครื่องมือมากกว่าหนึ่งประเภท (Multiple Modalities) เป็นการใช้เทคโนโลยีชีวมิติมากกว่า 1 ประเภทในการทำงานร่วมกัน เช่น การใช้การรู้จำใบหน้าร่วมกับ การรู้จำลายพิมพ์นิ้วมือ ยกตัวอย่างเช่น ในงานวิจัยของ Ammour, Boubchir, Bouden, and Ramdani (2020) ประยุกต์ใช้เทคโนโลยีชีวมิติทั้งใบหน้าและม่านตา และ งานวิจัยของ Gunasekaran, Jayamani, Ramasamy, and Pitchai (2019) ใช้ใบหน้า ลายพิมพ์นิ้วมือและม่านตาร่วมกันในการระบุตัวบุคคล
- 2) การใช้อุปกรณ์ตรวจจับประเภทเดียวกันมากกว่าหนึ่งชิ้น (Multiple Sensors) เป็นการใช้ชีวมิติรูปแบบเดียวกันแต่ใช้มากกว่า 1 ชิ้น เช่น การรู้จำใบหน้าที่ใช้กล้องมากกว่า 1 ตัว ยกตัวอย่างเช่น งานวิจัยของ Zhao, Xu, Wu, Hao, and Qian (2020) โดยได้ใช้กล้องบนอุปกรณ์มือถือจำนวน 2 เครื่องในการตรวจจับวัตถุ
- 3) การใช้วิธีการหรืออัลกอริทึมมากกว่าหนึ่งอย่าง (Multiple Features) เป็นระบบชีวมิติที่ใช้ทฤษฎีในการจำแนกมากกว่า 1 ทฤษฎีขึ้นไป
- 4) การทำซ้ำ (Multiple and Repeated Instants) เป็นระบบชีวมิติรูปแบบเดียวกันที่ใช้การทำซ้ำเพื่อให้ได้ข้อมูลเพิ่มขึ้น เช่น การสแกนม่านตาซ้ำและขวา การเก็บข้อมูลนิ้วมือหลาย ๆ นิ้ว เป็นต้น ยกตัวอย่างเช่น งานวิจัยของ Mathur, Mathur, Mathur, and Dadheech (2020) นำเสนอ งานวิจัย A Brief Survey of Deep Learning Techniques for Person Re-identification และ งานวิจัยของ Fenu, Marras, and Boratto (2018) นำเสนองานวิจัยที่ใช้ระบบชีวมิติแบบหลายทางในการตรวจสอบการเข้าชั้นเรียนของนักเรียนในการเรียนการสอน e-Learning โดยใช้ใบหน้าและลายพิมพ์นิ้วมือ และงานวิจัยของ Traore, Nakkabi, Saad, Sayed, Ardigo, Julibio, and Quinan (2017) นำเสนอกรอบการทำงานของระบบชีวมิติแบบหลายทางโดยในการสอบแบบออนไลน์และใช้การจับภาพหน้าจอแบบต่อเนื่องผ่านกล้องเว็บ (Web Camera)

2.3 กรอบการทำงานของโอเพนซีวี (OpenCV Framework)

โอเพนซีวี (Open-Source Computer Vision: OpenCV) เป็นไลบรารีซอฟต์แวร์สำหรับการทำคอมพิวเตอร์วิทัศน์ (Computer Vision) และเรียนรู้ของเครื่องจักร (Machine Learning) ซึ่งเป็นส่วนหนึ่งของปัญญาประดิษฐ์ (Artificial Intelligence: AI) โดย OpenCV ถูกสร้างขึ้นเพื่อช่วยให้การพัฒนาซอฟต์แวร์หรือระบบสามารถใช้งานการรับรู้ของเครื่องจักรนำไปใช้งานเป็นผลิตภัณฑ์ทางธุรกิจได้อย่างรวดเร็ว โดยเป็นผลิตภัณฑ์ที่มีใบอนุญาตของ Apache 2 ซึ่งทำให้ธุรกิจสามารถใช้งานและปรับแต่งโค้ดได้โดยง่าย โดยไลบรารีนี้ประกอบด้วยอัลกอริทึมมากกว่า 2,500 อัลกอริทึมที่ถูกปรับเพื่อให้ทำงานได้อย่างมีประสิทธิภาพ อัลกอริทึมเหล่านี้สามารถใช้สำหรับตรวจจับและรู้จำใบหน้า การระบุวัตถุ การจำแนกพฤติกรรมมนุษย์ในวิดีโอ การติดตามการเคลื่อนไหวของกล้อง การติดตามวัตถุที่เคลื่อนไหว การสกัดโมเดล 3 มิติของวัตถุ การสร้างสร้างรูป 3 มิติโดยใช้กล้องสเตอริโอบนคลาวด์ การกำหนดพิกัดรูปภาพเข้าด้วยกันเพื่อสร้างรูปภาพความละเอียดสูงของฉากหลังทั้งหมด การค้นหารูปภาพที่คล้ายกันจากฐานข้อมูลภาพ การลบตาแดงออกจากรูปภาพที่ถ่ายด้วยแฟลช การติดตามการเคลื่อนไหวของตา การรู้จำฉากทัศนศาสตร์และการสร้างเครื่องหมายสัญลักษณ์เพื่อใช้ทับภาพเชิงเสมือนเพิ่มเติม และอื่น ๆ อีกมากมาย ในปัจจุบัน OpenCV มีผู้ใช้งานกว่า 47,000 คนและจำนวนดาวน์โหลดประมาณ 18 ล้านครั้ง ไลบรารีนี้ได้ถูกนำไปใช้กันอย่างกว้างขวางในบริษัท กลุ่มวิจัยและองค์กรรัฐ พร้อมกับบริษัทชื่อดังอย่าง Google, Yahoo, Microsoft, Intel, IBM, Sony, Honda, และ Toyota ที่ใช้ไลบรารีนี้ ยังมี บริษัทสตาร์ทอัพที่หลากหลาย เช่น Applied Minds, VideoSurf, และ Zeitera ที่นำ OpenCV ไปใช้ในแบบกว้างขวาง การนำไลบรารี OpenCV ไปใช้ประยุกต์ใช้มีความหลากหลาย ตั้งแต่การต่อภาพถนนเข้าด้วยกันเพื่อสร้างภาพทั้งหมดของสถานที่ต่าง ๆ การตรวจจับการบุกรุกโดยใช้วิดีโอกล้องวงจรปิดในอิสราเอล การตรวจสอบอุปกรณ์ในเหมืองแร่ในจีน การช่วยให้หุ่นยนต์เดินทางและยกสิ่งของได้ที่โรงรถ Willow Garage การตรวจจับอุบัติเหตุการจมน้ำในสระว่ายน้ำในยุโรป การเปิดฉากศิลปะแบบโต้ตอบในสเปนและนิวยอร์ก การตรวจสอบทางลาดในตุรกี การตรวจสอบป้ายซื้อสินค้าในโรงงานทั่วโลก และการตรวจจับใบหน้าอย่างรวดเร็วในประเทศญี่ปุ่น นอกจากนี้ OpenCV มีอินเตอร์เฟซภาษา C++, Python, Java, และ MATLAB โดย OpenCV สามารถรองรับระบบปฏิบัติการ Windows, Linux, Android และ Mac OS ซึ่ง OpenCV มีอัลกอริทึมที่นิยมใช้กับมากที่สุด 3 แบบ ได้แก่ Eigenfaces, Fisherfaces, และ Local Binary Patterns Histograms (LBPH)

2.3.1 Eigenfaces

Eigenfaces เป็นเทคนิคการประมวลผลภาพและการจัดการกับภาพที่ใช้วิธีการ PCA (Principal Component Analysis) เพื่อหาคุณลักษณะหลักของภาพ (Principal Components) และจัดเก็บข้อมูลนี้เป็นโมเดลของภาพในรูปแบบของเวกเตอร์ Eigenface ซึ่งเวกเตอร์ Eigenface จะถูกสร้างขึ้นโดยการทำ PCA กับชุดของภาพที่ใช้สอนโมเดล โดยจะแปลงภาพทุกภาพในชุดข้อมูลเป็นเวกเตอร์ที่มีจำนวนมิติลดลงจนเหลือเพียงไม่กี่ตัวเท่านั้น แล้วจึงใช้เวกเตอร์ที่ได้เพื่อเป็น Eigenfaces ที่ใช้เป็นตัวแทนของภาพในชุดข้อมูล Eigenfaces สามารถนำไปใช้ในการจัดการกับภาพต่าง ๆ ได้ เช่น การระบุใบหน้าในภาพ (Face Recognition) โดยการเปรียบเทียบ Eigenfaces ของภาพที่ต้องการระบุใบหน้าที่กับ Eigenfaces ในโมเดล หรือใช้ในการเข้ารหัสภาพ (Image Compression) เพื่อลดขนาดของภาพให้เหมาะสมกับการจัดเก็บหรือส่งผ่านข้อมูลที่มีความจำกัในการเก็บรักษาหรือส่งผ่าน ขั้นตอนการทำ Eigenfaces ประกอบด้วยขั้นตอนหลัก ๆ ดังนี้

2.3.1.1 รวบรวมชุดข้อมูลภาพ: จัดเก็บภาพที่ต้องการสร้าง Eigenfaces ไว้ในชุดข้อมูลภาพ

2.3.1.2 แปลงภาพเป็นเวกเตอร์: แปลงภาพทุกภาพในชุดข้อมูลภาพเป็นเวกเตอร์ โดยใช้เทคนิคการแปลงภาพเป็นเวกเตอร์ เช่น PCA (Principal Component Analysis) โดย PCA จะแปลงภาพที่มีจำนวนมิติสูงเป็นเวกเตอร์ที่มีจำนวนมิติที่ต่ำลง ซึ่งเรียกว่า Principal Components หรือ Eigenvectors แล้วจึงจัดเก็บข้อมูลเหล่านี้เป็นแต่ละ Eigenfaces

2.3.1.3 สร้าง Eigenfaces: สร้าง Eigenfaces โดยใช้ข้อมูลจากขั้นตอนก่อนหน้า และจัดเก็บ Eigenfaces เป็นโมเดลของภาพในรูปแบบของเวกเตอร์ Eigenface

2.3.1.4 นำ Eigenfaces มาใช้: นำ Eigenfaces ที่ได้จากขั้นตอนก่อนหน้าไปใช้ในการประมวลผลภาพต่าง ๆ เช่น การระบุใบหน้าในภาพ หรือการเข้ารหัสภาพ

การสร้าง Eigenfaces จำเป็นต้องมีการใช้เทคนิค PCA และการปรับค่า Threshold เพื่อเลือกจำนวน Eigenfaces ที่เหมาะสม โดยทั่วไปแล้ว เราจะเลือกจำนวน Eigenfaces ที่เป็นไปได้น้อยที่สุดที่ยังคงความสามารถในการระบุใบหน้าหรือการเข้ารหัสภาพได้ดีและป้องกันการเกิด Overfitting ในการสร้างโมเดล Eigenface โดยแสดงตัวอย่างรูปใบหน้าที่ใช้อัลกอริทึม Eigenvalue ในรูปที่ 2.17

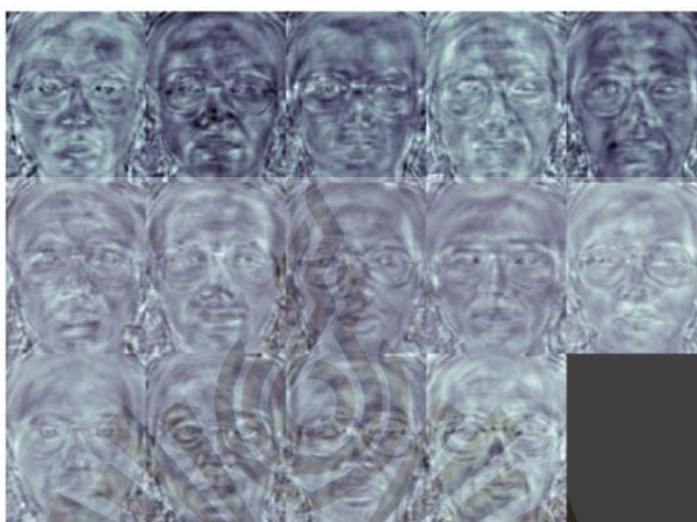


รูปที่ 2.17 แสดงตัวอย่างภาพใบหน้าจากการใช้อัลกอริทึม Eigenface
ที่มา: OpenCV, 2023

2.3.2 Fisherfaces

เป็นวิธีการในการจัดหมวดหมู่ใบหน้า ที่ใช้การวิเคราะห์หลักสูตร (Linear Discriminant Analysis: LDA) เพื่อเลือกแบบจำลองสำหรับการจำแนกใบหน้าในชุดข้อมูล โดย Fisherfaces เป็นการพัฒนามาต่อยอดจาก Eigenfaces ซึ่งเป็นวิธีการที่ใช้ PCA ในการลดมิติของข้อมูลใบหน้าและทำให้เป็นเวกเตอร์ลักษณะ (Feature Vectors) ก่อนจัดหมวดหมู่ใบหน้า แต่ Eigenfaces มีข้อจำกัดคือการเลือกแบบจำลองและวิธีการคำนวณความคล้ายคลึงที่ไม่ได้ใช้โครงสร้างของข้อมูลในการจัดหมวดหมู่ Fisherfaces จึงได้พัฒนาขึ้นมาเพื่อแก้ไขข้อจำกัดของ Eigenfaces โดยใช้ LDA เพื่อเลือกเฉพาะฟีเจอร์ที่มีความสำคัญต่อการจัดหมวดหมู่ ซึ่งสามารถช่วยลดความซับซ้อนของแบบจำลองและประสิทธิภาพในการจัดหมวดหมู่ใบหน้า ดังแสดงตัวอย่างในรูปที่ 2.18 นอกจากนี้ Fisherfaces ยังสามารถทำงานได้กับชุดข้อมูลที่มีขนาดใหญ่ขึ้นและมีประสิทธิภาพในการจัดหมวดหมู่ใบหน้าในเวลาอันสั้น โดย Fisherfaces จะใช้การคำนวณแบบ PCA เพื่อลดมิติของข้อมูลใบหน้าเหมือนกับ Eigenfaces และ จากนั้นจึงใช้ LDA เพื่อเลือกเฉพาะฟีเจอร์หลักที่แยกแยะความแตกต่างระหว่างกลุ่มของบุคคลได้ดีที่สุด และสร้าง Fisherfaces ที่เป็นเวกเตอร์ของภาพหน้าทั้งหมด ทำให้สามารถจัดกลุ่มแต่ละภาพหน้าของบุคคลได้อย่างแม่นยำ วิธีการ Fisherfaces เหมาะสำหรับการรู้จำหน้าของบุคคลโดยมีขนาดใหญ่และมีจำนวนของบุคคล

มาก ๆ เช่น ใช้ในระบบการตรวจสอบใบหน้าขณะผ่านเข้าออกจากโรงงานหรืออาคารสำนักงาน แต่วิธีการ Fisherfaces ก็มีข้อจำกัดในด้านการประมวลผลที่อาจใช้เวลานานและต้องมีการสอนใหม่หากมีการเพิ่มข้อมูลเข้ามา

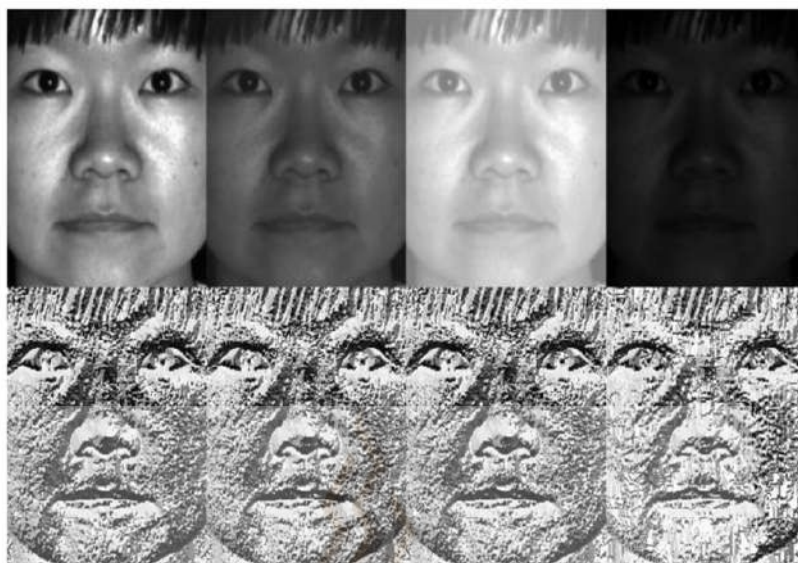


รูปที่ 2.18 แสดงตัวอย่างภาพใบหน้าจากการใช้อัลกอริทึม Fisherfaces

ที่มา: OpenCV, 2023

2.3.3 LBPH - Local Binary Patterns Histograms (LBPH)

เป็นอัลกอริทึมสำหรับการเข้ารหัส (Feature Extraction) ของภาพที่ใช้ในงานการตรวจจับ และตรวจจับวัตถุ (Object Detection) ซึ่งเป็นการแปลงภาพให้เป็นคุณลักษณะ (Feature) ที่แทนบุคคลหรือวัตถุในภาพได้อย่างความแม่นยำและเหมาะสม วิธีการทำงานของ LBPH จะทำการแบ่งภาพเป็นเซลล์ (Cell) ขนาดเล็ก ๆ แล้วใช้ Local Binary Pattern (LBP) ซึ่งเป็นการสร้างภาพใหม่โดยการเปรียบเทียบค่าความเข้มของพิกเซล (Pixel) รอบ ๆ กับค่าเซนเซอร์ (Threshold) แล้วแปลงผลลัพธ์เป็นตัวเลข 0 หรือ 1 ตามเงื่อนไขว่า ค่าพิกเซลรอบ ๆ มากกว่าเซนเซอร์หรือไม่ จากนั้นจะสร้าง Histograms ที่ใช้สรุปค่า LBP ของแต่ละเซลล์โดยแบ่งเป็นกลุ่มของค่า LBP ที่เป็นไปได้ทั้งหมด แล้วนำ Histograms ทั้งหมดมาเรียงต่อกันเป็น Feature Vector ซึ่งจะใช้สำหรับจดจำตัวบุคคลหรือวัตถุในภาพ ดังแสดงในรูปที่ 2.19 ซึ่ง LBPH มีข้อดีคือตรงไปตรงมาคือง่ายต่อการปรับแต่งพารามิเตอร์และทำงานได้รวดเร็ว นอกจากนี้ยังมีประสิทธิภาพในการรู้จำใบหน้าที่มีการเปลี่ยนแปลงเล็กน้อยของแสง แต่ก็มีข้อจำกัดที่ไม่สามารถจดจำใบหน้าได้อย่างแม่นยำในเงื่อนไข



รูปที่ 2.19 แสดงตัวอย่างภาพใบหน้าจากการใช้อัลกอริทึม LBPH

ที่มา: OpenCV, 2023

ในงานวิจัยของ Ahsan, Li, Zhang, Ahad and Gupta (2021) ได้ทำการทดลองเปรียบเทียบทั้ง 3 อัลกอริทึมในการทดลองจดจำใบหน้าในสภาวะอากาศที่ต่างกัน ผลลัพธ์ที่ได้คือกลุ่มที่ใช้ LBPH ในการรู้จำใบหน้ามีประสิทธิภาพมากที่สุด นอกจากนี้ยังสามารถสรุปข้อดีและข้อด้อยของทั้ง 3 อัลกอริทึม ดังแสดงในตารางที่ 2.1

ตารางที่ 2.1 แสดงข้อดีและข้อด้อยของทั้ง 3 อัลกอริทึม

อัลกอริทึม	ข้อดี	ข้อด้อย
Eigenfaces	- มีความเร็วในการประมวลผลที่ดีและเหมาะสำหรับการประมวลผลภาพแบบเวลาเรียลไทม์ - จัดการกับความแปรปรวนของภาพได้ - ไม่ต้องใช้ความละเอียดสูง	- ต้องใช้ชุดข้อมูลขนาดใหญ่ - การเปลี่ยนแปลงของแสงหรือมุมมองภาพ อาจจะทำให้มีปัญหาในการตรวจจับใบหน้า

ตารางที่ 2.1 แสดงข้อดีและข้อด้อยของทั้ง 3 อัลกอริทึม (ต่อ)

อัลกอริทึม	ข้อดี	ข้อด้อย
Fisherfaces	- สามารถจัดกลุ่มข้อมูลที่ซับซ้อนและมีความหลากหลายได้ดีกว่า Eigenfaces และ LBPH - เหมาะสำหรับจำแนกภาพที่มีความแตกต่างกันในมุมของแสงหรือมุมมอง	- มีความซับซ้อนและใช้เวลาในการประมวลผลมากกว่าแบบอื่น - หากข้อมูลไม่มีความแตกต่างกันมากพอ อาจจะไม่มีประสิทธิภาพมากพอในการจัดกลุ่มข้อมูล
LBPH	- ทำงานรวดเร็ว มีประสิทธิภาพสูง และใช้ทรัพยากรน้อยกว่า - มีความแม่นยำสูงเมื่อต้องการตรวจจับใบหน้าที่มีการเปลี่ยนแปลงเล็กน้อย - ไม่ต้องการการจัดเตรียมรูปภาพที่ซับซ้อน รูปภาพที่นำมาใช้งานสามารถเป็นภาพที่เก็บไว้แล้วก็ได้ - สามารถใช้งานได้ดีกับภาพที่มีแสงน้อยหรือเงามีได้	- การเปลี่ยนแปลงของแสงอาจทำให้ผลการตรวจจับใบหน้าไม่แม่นยำเท่าที่ควร - วิธีการ LBPH อาจทำงานได้ไม่ดีกับภาพที่มีขนาดเล็กหรือมากเกินไป - การถ่ายภาพ: ผลการตรวจจับใบหน้าอาจไม่แม่นยำถ้ารูปภาพถูกถ่ายในเงื่อนไขที่ไม่เหมาะสม เช่น ภาพที่ถูกถ่ายในมุมมองที่ไม่เหมาะสม

ที่มา: ผู้วิจัย, 2566

2.4 อินเทอร์เน็ตของสรรพสิ่ง (Internet of Things)

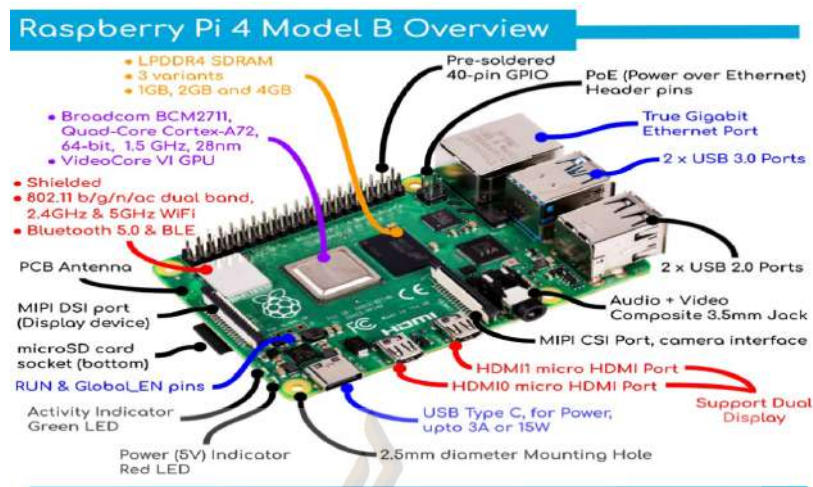
2.4.1 อินเทอร์เน็ตของสรรพสิ่ง

อินเทอร์เน็ตของสรรพสิ่ง หรือเรียกโดยย่อว่า IoT ย่อมาจาก Internet of Things ซึ่งหมายถึงการเชื่อมต่ออุปกรณ์ต่าง ๆ ให้สามารถสื่อสารกันผ่านอินเทอร์เน็ต โดยอุปกรณ์เหล่านี้มักเป็นอุปกรณ์ที่ใช้เซ็นเซอร์หรือตัววัดต่าง ๆ เช่น อุปกรณ์วัดอุณหภูมิ ความชื้น ค่าความเร็ว และอื่น ๆ ซึ่งสามารถเชื่อมต่อกับอินเทอร์เน็ตและแลกเปลี่ยนข้อมูลกับเครือข่ายได้อย่างอัตโนมัติ โดยในการเชื่อมต่อ IoT จะใช้เทคโนโลยีเครือข่ายแบบไร้สาย หรือ Wi-Fi เพื่อสื่อสารข้อมูลกับคอมพิวเตอร์หรือแพลตฟอร์มอื่น ๆ คำว่า Internet of Things ถูกใช้ครั้งแรกโดย Kevin Ashton ในปี 2552 โดยมีความหมายว่าการใช้เทคโนโลยี RFID (Radio Frequency Identification) เพื่อเชื่อมต่อ

สิ่งของต่าง ๆ ในโลกดิจิทัล เพื่อเพิ่มประสิทธิภาพในการดำเนินการและควบคุม ต่อมาในช่วงปี 2553 ถึง 2557 ได้มีการพัฒนาเทคโนโลยีต่าง ๆ ที่สามารถนำมาใช้งานในการเชื่อมต่ออุปกรณ์และสิ่งของต่าง ๆ ผ่านอินเทอร์เน็ตได้อย่างมีประสิทธิภาพ เช่น การใช้เซ็นเซอร์หรือตัววัดต่าง ๆ ที่สามารถอ่านและส่งข้อมูลผ่านอินเทอร์เน็ต การใช้เทคโนโลยีเครือข่ายแบบไร้สาย, Bluetooth หรือการสื่อสารสนามใกล้ (Near-field communication: NFC) เป็นต้น ผลกระทบของ IoT สามารถเห็นได้ในหลาย ๆ ด้าน เช่น การควบคุมการทำงานของเครื่องจักรแบบอัตโนมัติ การควบคุมและจัดการระบบเครือข่ายไฟฟ้า การติดตามและบริหารจัดการข้อมูลการใช้งานของอุปกรณ์ต่าง ๆ เช่น ตรวจสอบอุณหภูมิในห้องเย็น การจัดการอุปกรณ์อัจฉริยะในบ้าน เช่น ระบบควบคุมไฟสว่าง ประตู เครื่องปรับอากาศ และอื่น ๆ ซึ่งจะช่วยให้ชีวิตของเรามีความสะดวกสบายและปลอดภัยยิ่งขึ้น

2.4.2 Raspberry Pi

Raspberry Pi เป็นคอมพิวเตอร์เล็กที่มีขนาดไม่ใหญ่มาก แต่มีฟังก์ชันที่หลากหลาย โดยเฉพาะในการใช้งานเพื่อการเรียนรู้และพัฒนาโปรแกรม สำหรับผู้ที่ต้องการเริ่มต้นเรียนรู้การเขียนโปรแกรม หรือใช้งาน IoT ในโครงการของตนเอง และไม่ต้องใช้เครื่องคอมพิวเตอร์ที่มีขนาดใหญ่และมีราคาสูง Raspberry Pi เป็นพลังงานประหยัด มีขนาดเล็กและราคาไม่สูงมาก โดยมีพอร์ตต่อ USB HDMI Ethernet รวมถึง GPIO (General Purpose Input/Output) ซึ่งช่วยให้ผู้ใช้สามารถเชื่อมต่อกับอุปกรณ์ต่าง ๆ เช่น เซ็นเซอร์อุณหภูมิ, ตัวรับสัญญาณอินเทอร์เน็ตไร้, กล้อง, และอุปกรณ์ต่าง ๆ ที่สามารถเชื่อมต่อได้ผ่านพอร์ต GPIO นี้ได้ นอกจากนี้ ยังมีระบบปฏิบัติการ Raspbian ซึ่งเป็นเวอร์ชันของ Linux ที่เข้าถึงและควบคุมอุปกรณ์ต่าง ๆ ได้อย่างง่ายดาย Raspberry Pi ได้รับความนิยมมากในการใช้งานเพื่อการเรียนรู้และการพัฒนาโปรแกรม เช่น ใช้ในการสร้างโปรแกรมเบื้องต้นเพื่อควบคุมอุปกรณ์ต่าง ๆ เช่น ระบบควบคุมสัญญาณไฟฟ้า ระบบอัตโนมัติเปิดปิดหลอดไฟ การเขียนโปรแกรมเพื่อส่งข้อมูลเซ็นเซอร์อุณหภูมิไปยังคลาวด์ เพื่อควบคุมเครื่องปรับอากาศในบ้าน การสร้างเกม โปรแกรมสำหรับการทำงานและอื่น ๆ อีกมากมาย (กอบเกียรติ สระอุบล, 2561, น.379-381)



รูปที่ 2.20 แสดงลักษณะและคำอธิบาย Raspberry Pi version 4 Model B

ที่มา: Techmakers Innovation, n.d.

จากรูปที่ 2.20 แสดงภาพของ Raspberry Pi โมเดล B ซึ่งเป็นเสมือน Mainboard ในเครื่อง PC ซึ่ง Raspberry Pi 4 Model B เป็นรุ่นล่าสุดของบอร์ด Raspberry Pi ที่มีประสิทธิภาพสูง และมีฟีเจอร์ใหม่ ๆ เพิ่มเติม โดย Raspberry Pi 4 Model B มาพร้อมกับชิพ Broadcom BCM2711 ที่มีความเร็ว 1.5GHz และมีหน่วยประมวลผลกราฟิกแยกต่างหาก ที่เป็น Broadcom VideoCore VI ที่สามารถแสดงผลความละเอียดสูงสุดถึง 4K 60fps ได้ นอกจากนี้ ยังมีการอัปเดตหน่วยความจำ ไปยัง 4GB LPDDR4 RAM และมีทั้งเทคโนโลยีเครือข่ายแบบไร้สายและ Bluetooth หลายเวอร์ชัน ที่สามารถเชื่อมต่อได้ผ่าน Wi-Fi 5 (802.11ac) หรือ Bluetooth 5.0 ทำให้สามารถเชื่อมต่ออุปกรณ์ได้อย่างง่ายดาย อีกสิ่งที่น่าสนใจคือ บอร์ด Raspberry Pi 4 Model B มีพอร์ต USB จำนวนสามพอร์ต และมีพอร์ต USB 3.0 จำนวนสองพอร์ต เพื่อให้มีการถ่ายโอนข้อมูลได้อย่างรวดเร็ว และมีพอร์ต Gigabit Ethernet สำหรับเชื่อมต่อกับเครือข่ายได้ด้วยความเร็วสูงสุด 1 Gbps เนื่องจากการอัปเดตโดยมีรูปร่างเปลี่ยนแปลงไป โดยรุ่น Raspberry Pi 4 Model B มีขนาดที่ใหญ่กว่ารุ่นก่อน ๆ เพราะมีความยาว 88 มม. และกว้าง 58 มม. แต่ยังคงมีความพอร์ตพื้นฐานเช่น HDMI, GPIO, สาย Ethernet และสาย MicroSD ให้ใช้งานได้เช่นเดิม นอกจากนี้ยังมีฟีเจอร์ที่กล่าวมาแล้ว ยังมีการเพิ่มหน่วยความจำสำหรับการเก็บข้อมูลได้มากขึ้น ซึ่งมีหลายความจุให้เลือกตามต้องการ ได้แก่ 1GB, 2GB, 4GB, และ 8GB ซึ่งช่วยเพิ่มประสิทธิภาพในการทำงานและใช้งานได้อย่างยอดเยี่ยม นอกจากนี้ Raspberry Pi 4 Model B ยังมีฟีเจอร์การทำงานที่ปรับปรุงใหม่ เช่น มีการเพิ่มระบบ Dual-Display Support ที่สามารถเชื่อมต่อกับหน้าจอสองเครื่องได้พร้อมกัน มีการปรับปรุงการทำงานในส่วน of USB ทำให้สามารถเชื่อมต่อกับอุปกรณ์ USB หลายอย่างได้อย่างสมบูรณ์แบบ และมีการเพิ่มส่วนของช่องรับสัญญาณเสียง Digital Audio Output ในรูปแบบ HDMI หรือ Jack

Audio 3.5 mm ทำให้สามารถเชื่อมต่อกับเครื่องเสียงหรือลำโพงได้โดยตรงรวมถึงยังมีการอัปเดตที่ความเร็วของเครื่องด้วย ทำให้ Raspberry Pi 4 Model B มีความเร็วในการประมวลผลและการทำงานสูงขึ้นเป็นอย่างมาก และยังสามารถใช้งานได้กับระบบปฏิบัติการต่าง ๆ เช่น Raspbian, Ubuntu, Kali Linux, และอื่น ๆ ในงานวิจัยนี้ได้ใช้ Raspberry Pi 4 Model B เป็นอุปกรณ์ที่ใช้ในการทดลอง โดยได้ทำการเชื่อมต่อกับกล้อง Raspberry Pi Camera (8 Megapixels) คือกล้องถ่ายภาพที่ออกแบบมาเป็นพิเศษสำหรับบอร์ด Raspberry Pi ซึ่งเป็นเครื่องมือในการพัฒนาโปรแกรมและโครงการสำหรับนักพัฒนาและผู้สนใจในเทคโนโลยีการสร้าง IoT หรือระบบฝังตัว (Embedded System) การที่มีขนาดเล็กและน้ำหนักเบาทำให้เหมาะสำหรับการใช้งานในที่ต้องใช้หน่วยประมวลผลขนาดเล็ก เช่น การสร้างระบบวิดีโอกล้อง CCTV ระบบตรวจจับใบหน้า (Face Detection) โดยมีคุณลักษณะทางเทคนิค แสดงในตารางที่ 2.2

ตารางที่ 2.2 แสดงคุณลักษณะของอุปกรณ์ IoT

อุปกรณ์ชีวมิติ	ข้อมูลจำเพาะ	ราคา (USD)
	Raspberry Pi Camera (8mp) - Sensor: Sony IMX219 - Sensor Resolution: 32480 x 2464 (8 megapixels) - Sensor Image Area: 3.69 x 2.81 mm - Pixel Size: 1.12um x 1.12um - Optical Size: 1/4" - Video: Dimension: 25mm x 23mm x 9mm / 0.98" x 0.90" x 0.35": 1920 x 1080 (1080p), 30 fps/1280 x 720 (720p), 60 fps/640 x 480 (480p), 90 fps - Weight: (Camera board + attached cable): 3.4g	\$40
	Fingerprint reader Adafruit R305 - Fingerprint Imaging Time: less than 1 second - Match Mode: Compare Mode 1:1 - Search Mode: 1: N - Window Area: 14 mm. x 18 mm. - Signature File Size: 256 bytes	\$55

ตารางที่ 2.2 แสดงคุณลักษณะของอุปกรณ์ IoT (ต่อ)

อุปกรณ์ชีวมิติ	ข้อมูลจำเพาะ	ราคา (USD)
	- Template File Size: 512 bytes - Storage Capacity: 162 templates - Safety Ratings: 1 (low) to 5 (high) - False Acceptance Rate: less than 0.001% - False Reject Rate: less than 1% - Interface: Serial UART TTL - Baud Rate: 57600 by default (9600, 19200, 28800, 38400, 57600 configurable) - Working Temperature Rating: -20 to +50 Degree Celsius - Working Humidity: 40 to 85 %RH - Full Dimension: 56 mm. x 20mm x 21.5mm (H x W x L)	
	Raspberry Pi 4 Model B - BCM2711 SoC - 8GB DDR4 RAM - USB 3.0 - PoE Enabled	\$335
	LG 50 inches UQ8000PSC UHD 4K Smart TV	\$315
	Raspberry Pi Black - Grey QWERTY (UK) Raspberry Pi Keyboard	\$20
	256 GB MICRO SD Card	\$40
	Pair Wires - GPIO Extender cable male female 40 Pin - Jumper wire male to female	\$10

ที่มา: Rukhiran et al., 2023

Fingerprint reader Adafruit R305 เป็นอุปกรณ์สแกนลายพิมพ์นิ้วมือที่ออกแบบมาเพื่อใช้ในการรับรู้และตรวจสอบลายพิมพ์นิ้วมือของผู้ใช้งาน โดยอุปกรณ์นี้ใช้เทคโนโลยีการสแกนลายพิมพ์นิ้วมือด้วยวิธีออกแบบเป็นแบบออปติค (Optical Sensor) เพื่อทำการจับคู่และตรวจสอบลายพิมพ์นิ้วมือที่ถูkBันทึกไว้กับฐานข้อมูล Adafruit R305 มีขนาดเล็กและราคาไม่แพง และมีการติดตั้งและใช้งานได้ง่าย โดยสามารถเชื่อมต่อกับไมโครคอนโทรเลอร์หรือคอมพิวเตอร์ได้โดยใช้หน่วยประมวลผลที่อยู่ในตัวอุปกรณ์ และมีหน้าจอ LED แสดงผลสถานะการทำงาน รวมถึงมีเทคโนโลยีการป้องกันการถูกปลอมแปลงของลายพิมพ์นิ้วมือ (Fingerprint Spoofing) ด้วย การใช้งาน Fingerprint Reader Adafruit R305 สามารถนำมาใช้งานได้หลายสถานการณ์ เช่น การควบคุมการเข้าถึงระบบ (Access Control) การตรวจสอบตัวตนของผู้ใช้งาน (Authentication) หรือใช้ในการเก็บบันทึกเวลาการเข้างาน (Time Attendance) เป็นต้น

จากตารางที่ 2.2 แสดงคุณลักษณะของอุปกรณ์ที่ใช้ในการทดลอง ประกอบด้วย กล้อง Raspberry Pi Camera และ Fingerprint Scanner Adafruit R305 ซึ่งเป็นอุปกรณ์ IoT ที่หลายคนนำไปใช้ในการทดลองเนื่องจากสามารถเข้ากันได้ดีกับระบบปฏิบัติการของ Raspberry Pi และราคาไม่สูงมากนัก

2.5 การวิเคราะห์และออกแบบระบบ

การวิเคราะห์และออกแบบระบบในปัจจุบันสามารถทำได้หลายวิธีขึ้นอยู่กับความถนัดในการออกแบบและความเหมาะสมของงาน

2.5.1 การวิเคราะห์และออกแบบเชิงวัตถุ

หลักการออกแบบเชิงวัตถุ (Object-Oriented Analysis and Design) เป็นกลุ่มของหลักการและแนวคิดในการออกแบบซอฟต์แวร์ที่มุ่งเน้นในการเพิ่มประสิทธิภาพ ความยืดหยุ่น และความสามารถในการบำรุงรักษา โดยใช้วัตถุ (Object) และคลาส (Class) เป็นองค์ประกอบหลักในการออกแบบ ซึ่งหลักการออกแบบเชิงวัตถุประกอบด้วยหลักต่อไปนี้ (อัษฎาพร ทรัพย์สมบูรณ์, 2557, น.18-32)

2.5.1.1 Encapsulation (การบรรจุภัณฑ์): คือความสามารถในการสร้างวัตถุซึ่งเป็นการปกปิดข้อมูลและฟังก์ชันภายในวัตถุไว้ภายในวัตถุ โดยมีการกำหนดค่าของตัวแปรและสร้างเมธอดเพื่อเข้าถึงข้อมูลนั้น

2.5.1.2 Inheritance (การสืบทอด): คือความสามารถในการสร้างคลาสใหม่โดยใช้คลาสที่มีอยู่แล้วเป็นพื้นฐาน ซึ่งทำให้เราสามารถใช้งานโค้ดที่มีอยู่แล้วได้อย่างมีประสิทธิภาพ

2.5.1.3 Polymorphism (การหลายรูปแบบ): คือความสามารถในการให้วัตถุหนึ่ง ๆ ทำงานได้หลากหลายวิธี ขึ้นอยู่กับว่าวัตถุนั้นถูกสร้างขึ้นมาจากคลาสใด

2.5.1.4 Abstraction (การถอดรหัส): คือหลักการที่ช่วยให้เราสามารถซ่อนรายละเอียดที่ซับซ้อนและแสดงเฉพาะฟังก์ชันหรือคุณสมบัติที่สำคัญสำหรับผู้ใช้งานหรือผู้พัฒนาคนอื่น ๆ ได้นำไปใช้ประโยชน์ต่อไป

2.5.2 UML (Unified Modeling Language)

UML เป็นภาษาแบบกราฟิก (Graphic Language) ที่ถูกออกแบบมาเพื่อใช้ในการแสดงและอธิบายรูปแบบการออกแบบซอฟต์แวร์ โดยใช้แผนภาพในการแสดงผล UML ถูกพัฒนาขึ้นโดย Object Management Group (OMG) และมีเป้าหมายเพื่อให้โครงสร้างและพฤติกรรมของระบบซอฟต์แวร์มีความชัดเจน และเพิ่มความสามารถในการเข้าใจและออกแบบระบบโดยที่ผู้ใช้งานไม่จำเป็นต้องมีความรู้ทางเทคนิคเฉพาะเจาะจงในรายละเอียดการออกแบบ UML ประกอบด้วยแผนภาพ (Diagram) ต่าง ๆ ซึ่งแต่ละแผนภาพจะใช้ในการแสดงผลและอธิบายองค์ประกอบต่าง ๆ ในระบบซอฟต์แวร์ รวมถึงการแสดงผลลักษณะพฤติกรรมของระบบและความสัมพันธ์ระหว่างองค์ประกอบ ตัวอย่างของแผนภาพใน UML ประกอบด้วย สัญลักษณ์ (Notation) และแผนภาพ (Diagram) ต่าง ๆ ที่ใช้ในการแสดงและอธิบายรูปแบบการออกแบบซอฟต์แวร์ แต่ละแผนภาพมีจุดประสงค์ที่แตกต่างกัน ดังนี้

2.5.2.1 Use Case Diagram: แสดงการทำงานของระบบในรูปแบบการทำงานของผู้ใช้

2.5.2.2 Class Diagram: แสดงคลาสในระบบและความสัมพันธ์ระหว่างคลาส

2.5.2.3 Sequence Diagram: แสดงลำดับการทำงานขององค์ประกอบในระบบ โดยแสดงการเรียกใช้เมธอดระหว่างองค์ประกอบ

2.5.2.4 Activity Diagram: แสดงกระบวนการในระบบในรูปแบบแผนภาพกระบวนการ (Flow Chart)

2.5.2.5 Component Diagram: แสดงส่วนประกอบ (Component) และความสัมพันธ์ระหว่างส่วนประกอบในระบบ

2.5.2.6 Deployment Diagram: แสดงแหล่งที่มาและการกระจายโปรแกรม หรือการติดตั้งทางฮาร์ดแวร์ของโปรแกรม

2.5.2.7 Package Diagram: แสดงการแบ่งแพ็คเกจของโปรแกรม โดยแต่ละแพ็คเกจจะมีคลาสและองค์ประกอบของตัวเอง

2.5.2.8 Object Diagram: แสดงวัตถุในระบบและความสัมพันธ์ระหว่างวัตถุ

2.5.2.9 State Machine Diagram: แสดงสถานะของวัตถุและการเปลี่ยนสถานะของวัตถุ

2.5.2.10 Communication Diagram: แสดงวัตถุและการสื่อสารระหว่างวัตถุในระบบ

2.5.2.11 Timing Diagram: แสดงเวลาและการเกิดเหตุการณ์ของวัตถุในระบบ

ทั้ง 11 ประเภทของแผนภาพข้างต้นเป็นตัวอย่างของแผนภาพใน UML ซึ่งเป็นเพียงบางส่วนเท่านั้น นอกจากนี้ยังมีแผนภาพอื่น ๆ ที่ใช้ในการแสดงผลและอธิบายรูปแบบการออกแบบใน UML อีกมากมาย แต่ละแผนภาพจะมีจุดประสงค์และลักษณะที่แตกต่างกัน และคุณสมบัติของแต่ละแผนภาพสามารถเพิ่มเติมได้เพื่อตอบสนองความต้องการของโครงการและการออกแบบที่แตกต่างกันไป

2.5.3 การวิเคราะห์และออกแบบระบบโดยใช้แผนภาพการไหลของข้อมูล (Information Flow Diagram: IFD)

การวิเคราะห์และออกแบบระบบโดยใช้แผนภาพการไหลของข้อมูล หรือเรียกโดยย่อว่า IFD (Information Flow Diagram) เป็นเทคนิคที่ใช้ในการแสดงภาพของกระบวนการในระบบโดยใช้แผนภาพกระแสข้อมูล โดยที่แผนภาพกระแสข้อมูลจะแสดงให้เห็นถึงกระบวนการที่เกิดขึ้นในระบบโดยแยกออกเป็นกระแสข้อมูลแต่ละประเภท เพื่อให้ง่ายต่อการวิเคราะห์และพัฒนา

ระบบ โดยใช้เครื่องหมายเชื่อมโยงและสัญลักษณ์ต่าง ๆ เพื่อแสดงถึงการกระจายข้อมูลระหว่างแหล่งที่มาและปลายทางของข้อมูลในระบบ IFD มีโครงสร้างที่จะประกอบด้วย 3 ส่วนหลัก ๆ ได้แก่

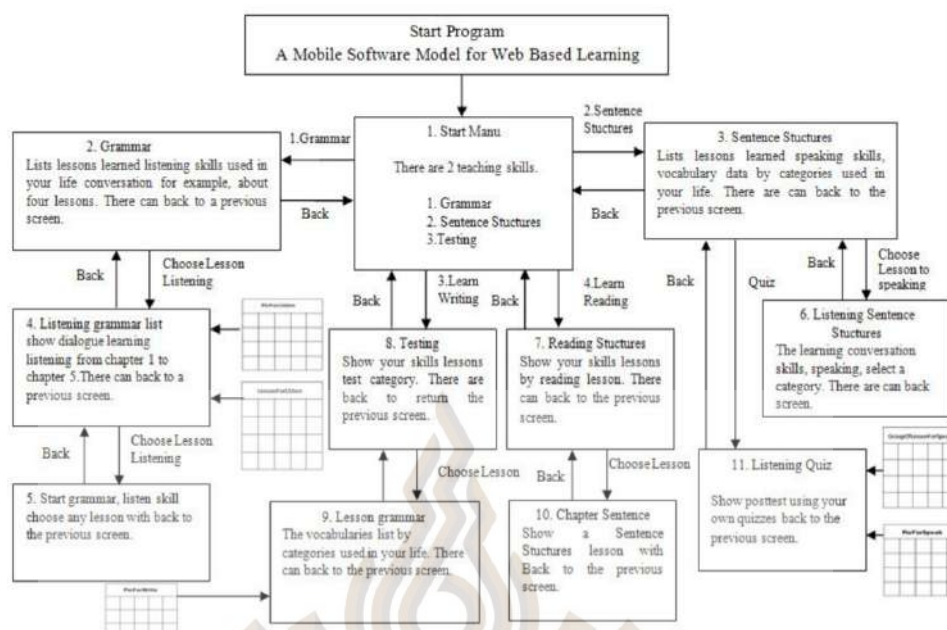
2.5.3.1 แหล่งที่มาของข้อมูล (Sources) เป็นส่วนที่แสดงถึงแหล่งที่มาของข้อมูล เช่น ผู้ใช้งาน ระบบฐานข้อมูล หรือระบบที่เชื่อมต่อกับระบบของเรา

2.5.3.2 กระแสข้อมูล (Flows) เป็นส่วนที่แสดงถึงการกระจายข้อมูลระหว่างแหล่งที่มาและปลายทางของข้อมูล โดยมีเครื่องหมายเชื่อมโยงแสดงถึงการเชื่อมโยงของกระแสข้อมูลระหว่างแหล่งที่มาและปลายทาง

2.5.3.3 ปลายทางของข้อมูล (Destinations) เป็นส่วนที่แสดงถึงปลายทางของข้อมูล เช่น การประมวลผล ระบบฐานข้อมูล หรือผู้ใช้งาน

โดย IFD ช่วยให้ผู้พัฒนาระบบสามารถวิเคราะห์กระบวนการของระบบได้อย่างชัดเจน มีการเข้าใจกันเป็นระบบ และลดความผิดพลาดในการพัฒนาระบบ IFD มีความสำคัญในการพัฒนาระบบเนื่องจากช่วยให้ผู้พัฒนาระบบสามารถวิเคราะห์และพัฒนาระบบได้อย่างมีประสิทธิภาพ นอกจากนี้ การใช้ IFD ยังช่วยให้ผู้ใช้งานเข้าใจระบบได้ง่ายขึ้น และสามารถนำไปใช้ในการเปลี่ยนแปลงและพัฒนาระบบในอนาคตได้อย่างมีประสิทธิภาพ

ตัวอย่างในงานวิจัยของ Chomngern and Netinant (2017) ได้นำเสนอการใช้งาน IFD ในการออกแบบระบบการสอนภาษาอังกฤษด้วย e-Learning ดังแสดงในรูปที่ 2.21



รูปที่ 2.21 แสดงตัวอย่างการออกแบบระบบโดยใช้ IFD

ที่มา: Chomngern and Netinant, 2017

2.6 การประกันคุณภาพของการออกแบบระบบเทคโนโลยีสารสนเทศ

2.6.1 Software Design Based on IEEE SDD

งานวิจัยนี้ได้ทำการออกแบบตามมาตรฐานการออกแบบของ IEEE Standard for Information Technology Systems Design Software Design Descriptions (IEEE-SDD) ซึ่ง เรียกอีกชื่อหนึ่งว่า IEEE 1016 คือมาตรฐานในการเขียน Software Design Descriptions (SDDs) ซึ่งตั้งอยู่ภายใต้การดำเนินงานของ IEEE (The Institute of Electrical and Electronics Engineers) มาตรฐานนี้ได้รับการออกแบบมาเพื่อให้แน่ใจว่าการออกแบบซอฟต์แวร์ที่อธิบายใน SDD มีความครอบคลุม, ความชัดเจน, และความเป็นระเบียบ เพื่อที่จะใช้ในการเขียนและอธิบายเอกสารการออกแบบซอฟต์แวร์ (Software Design Document: SDD) สิ่งที่จะต้องประกอบไปใน IEEE SDD มีดังนี้

2.6.1.1 Introduction: ระบุความต้องการที่เกี่ยวข้องกับซอฟต์แวร์ และรายละเอียดของซอฟต์แวร์ที่จะพัฒนา เช่น สิ่งที่ซอฟต์แวร์ต้องทำ ประโยชน์ของซอฟต์แวร์ และข้อจำกัดของซอฟต์แวร์

2.6.1.2 Overall Description: ระบุภาพรวมของซอฟต์แวร์ โดยระบุคุณลักษณะและคุณสมบัติทั่วไปของซอฟต์แวร์ รวมถึงข้อมูลเชิงลึกเกี่ยวกับผู้ใช้และระบบที่เกี่ยวข้องกับซอฟต์แวร์

2.6.1.3 Specific Requirements: ระบุคุณลักษณะและคุณสมบัติที่เกี่ยวข้องกับซอฟต์แวร์ โดยระบุฟังก์ชันหลักของซอฟต์แวร์ และรายละเอียดของฟังก์ชันที่รองรับการทำงานต่าง ๆ รวมถึงแผนการทดสอบ การติดตั้ง และการดูแลรักษา

2.6.1.4 System Features: ระบุรายละเอียดของคุณลักษณะและคุณสมบัติของระบบ ซึ่งรวมถึงฟังก์ชัน ส่วนประกอบ และระบบที่เกี่ยวข้องกับซอฟต์แวร์ รายละเอียดนี้จะช่วยให้ผู้ใช้งานและผู้พัฒนาเข้าใจว่าซอฟต์แวร์มีความสามารถอะไรบ้าง และสามารถทำงานอย่างไรได้บ้าง

2.6.1.5 External Interface Requirements: ระบุข้อมูลเกี่ยวกับส่วนติดต่อภายนอกของซอฟต์แวร์ เช่น การเชื่อมต่อกับฐานข้อมูล การเชื่อมต่อกับเครื่องมือต่าง ๆ และการเชื่อมต่อกับผู้ใช้งาน

2.6.1.6 Non-Functional Requirements: ระบุข้อกำหนดเชิงอนุพันธ์ของซอฟต์แวร์ เช่น ประสิทธิภาพ ความน่าเชื่อถือ ความปลอดภัย ความสามารถในการรองรับการเปลี่ยนแปลง เป็นต้น

2.6.1.7 Design Constraints: ระบุข้อจำกัดต่าง ๆ ที่ต้องเกี่ยวข้องกับการออกแบบซอฟต์แวร์ เช่น ระยะเวลาในการพัฒนา การใช้เครื่องมือที่กำหนดไว้ และการประยุกต์ใช้เทคโนโลยีที่แนะนำ

2.6.1.8 Software System Attributes: ระบุคุณลักษณะของระบบที่มีผลต่อการออกแบบซอฟต์แวร์ เช่น ความมั่นคง ความเสถียร และความสามารถในการตรวจสอบข้อผิดพลาด

2.6.1.9 Appendices: เป็นส่วนที่ใช้เก็บข้อมูลเพิ่มเติมที่เกี่ยวข้องกับซอฟต์แวร์ เช่น แผนผัง ER (Entity Relationship) และคุณลักษณะเฉพาะของซอฟต์แวร์ ซึ่งช่วยให้ผู้ใช้งานและผู้พัฒนาเข้าใจว่าซอฟต์แวร์ทำงานอย่างไรและมีรายละเอียดอะไรบ้าง

การออกแบบซอฟต์แวร์ตามมาตรฐาน IEEE SDD ช่วยให้ผู้ใช้งานและผู้พัฒนาเข้าใจและมีความสอดคล้องกันในเรื่องของฟังก์ชันและคุณลักษณะของซอฟต์แวร์ และช่วยให้การพัฒนาซอฟต์แวร์เป็นไปอย่างมีประสิทธิภาพและมีคุณภาพสูง นอกจากนี้ ได้แสดงการระบุมุมมองการออกแบบออกเป็น 12 มุมมอง (Viewpoint) โดยมีรายละเอียด ดังแสดงตารางที่ 2.3

ตารางที่ 2.3 แสดงมุมมองการออกแบบตามมาตรฐานการออกแบบซอฟต์แวร์ของสถาบันวิชาชีพ
วิศวกรไฟฟ้าและอิเล็กทรอนิกส์

มุมมองการ ออกแบบ	คำอธิบาย	ตัวอย่างภาษาที่ใช้ในการ ออกแบบ
Context	เป็นการเน้นไปที่บริบทของระบบซอฟต์แวร์ โดยที่เน้นเรื่องของผู้ใช้งาน ลูกค้า และผู้เกี่ยวข้องที่เกี่ยวข้องกับระบบ	IDEF0, UML Use Case diagram, และ Structured Analysis Context diagram
Composition	มุ่งเน้นไปที่การประกอบของระบบจากส่วนประกอบที่แตกต่าง ซึ่งอธิบายว่าแต่ละส่วนประกอบของระบบมีความสัมพันธ์กันอย่างไร	Logical: UML Package diagram, UML Component diagram, Architecture Description Languages, IDEF0, Structure chart, และ HIPO Physical: UML Deployment diagram
Logical	เป็นการเน้นไปที่ความสัมพันธ์ระหว่างผู้ใช้กับซอฟต์แวร์ โดยที่เน้นเรื่องการทำงานของระบบ การสร้างส่วนประกอบของระบบ การติดต่อกับฐานข้อมูล และเรื่องของการควบคุมผู้ใช้งาน	UML Class diagram, และ UML Object diagram
Dependency Viewpoint	เน้นในการบรรยายความสัมพันธ์ของการพึ่งพากันระหว่างส่วนประกอบต่าง ๆ ในระบบซอฟต์แวร์ มุมมองนี้ทำให้เราเข้าใจได้ถึงวิธีการที่ส่วนประกอบต่าง ๆ ในระบบสามารถส่งผลกระทบกันได้หรือทำงานร่วมกันได้อย่างไร	UML Package diagram และ Component diagram

ตารางที่ 2.3 แสดงมุมมองการออกแบบตามมาตรฐานการออกแบบซอฟต์แวร์ของสถาบันวิชาชีพ
วิศวกรไฟฟ้าและอิเล็กทรอนิกส์ (ต่อ)

มุมมองการ ออกแบบ	คำอธิบาย	ตัวอย่างภาษาที่ใช้ในการ ออกแบบ
Information Viewpoint	เป็นการอธิบายวิธีการที่ระบบจัดการข้อมูล และวิธีที่ข้อมูลเหล่านั้นได้รับการนำไปใช้ มันเป็นเครื่องมือสำคัญในการอธิบาย โครงสร้างข้อมูล รูปแบบข้อมูล และการ ไหลของข้อมูลในระบบ	IDEF1X, Entity-Relation diagram, และ UML Class diagram
Patterns Viewpoint	เป็นมุมมองที่เน้นไปที่การใช้และการ ประยุกต์ใช้ Patterns หรือรูปแบบที่เป็น แบบแผน ในการออกแบบและ สถาปัตยกรรมซอฟต์แวร์	UML Composite Structure diagram
Interface Viewpoint	เป็นมุมมองที่เน้นไปที่การออกแบบและ การจัดการกับส่วนประสานงานผู้ใช้ของ ระบบซอฟต์แวร์ใช้ในการสื่อสารระหว่าง ส่วนประกอบของระบบ และระหว่าง ระบบกับผู้ใช้ หรือระบบอื่น ๆ	Interface Definition Languages (IDL), และUML Component diagram
Structure Viewpoint	เน้นไปที่การอธิบายโครงสร้างพื้นฐานของ ระบบซอฟต์แวร์ นั่นคือ วิธีการที่ ส่วนประกอบต่าง ๆ ของระบบถูกจัดเรียง และมีความสัมพันธ์กันอย่างไร	UML Structure diagram, และ Class diagram
Interaction Viewpoint	เน้นไปที่การอธิบายวิธีการที่ส่วน ต่าง ๆ ของระบบซอฟต์แวร์ทำงานร่วมกัน	UML Sequence diagram, และ UML Communication diagram

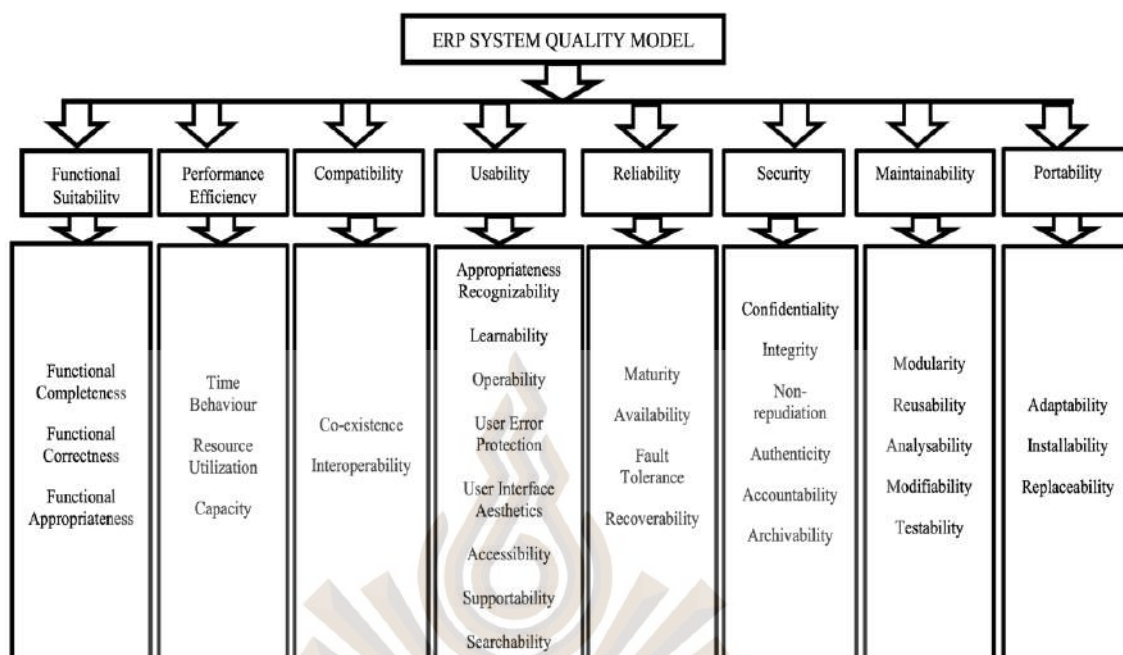
ตารางที่ 2.3 แสดงมุมมองการออกแบบตามมาตรฐานการออกแบบซอฟต์แวร์ของสถาบันวิชาชีพ
วิศวกรไฟฟ้าและอิเล็กทรอนิกส์ (ต่อ)

มุมมองการ ออกแบบ	คำอธิบาย	ตัวอย่างภาษาที่ใช้ในการ ออกแบบ
State dynamics Viewpoint	เน้นไปที่การอธิบายสถานะและการ เปลี่ยนแปลงสถานะของระบบซอฟต์แวร์ หรือส่วนประกอบภายในระบบ	UML State Machine diagram, Statechart (Harel's), State Transition Table (matrix), Automata, และ Petri Net
Algorithm Viewpoint	เน้นไปที่การอธิบายขั้นตอนการทำงาน หรือขั้นตอนวิธี (Algorithm) ที่ใช้ในระบบ ซอฟต์แวร์	Decision table, Warnier diagram, JSP, และ PDL
Resources Viewpoint	เน้นไปที่การอธิบายและจัดการทรัพยากรที่ ใช้ในระบบซอฟต์แวร์	UML Real-time Profile, UML class diagram, และ UML Object Constraint Language (OCL)

ที่มา: Wong-In and Netinant, 2018

2.6.2 การประกันคุณภาพของการออกแบบซอฟต์แวร์ (Software design model quality assurance based on ISO/IEC: SQuaRE)

ISO/IEC SQuaRE (Software Quality Requirements and Evaluation) เป็นชุดมาตรฐานที่พัฒนาโดยองค์กรมาตรฐานสากล (ISO) และสภาวิศวกรไฟฟ้าสากล (IEC) เพื่อการตรวจสอบและปรับปรุงคุณภาพซอฟต์แวร์ มีรูปแบบต่าง ๆ เช่น มาตรฐาน แนวปฏิบัติ และโมเดลต่าง ๆ สำหรับการพัฒนาซอฟต์แวร์ ซึ่งหนึ่งในส่วนประกอบสำคัญของ SQuaRE คือมาตรฐานการประกันคุณภาพโมเดลการออกแบบซอฟต์แวร์ ISO/IEC 25010 โดยมาตรฐานนี้จะอธิบายความต้องการและแนวปฏิบัติในการประเมินคุณภาพของโมเดลการออกแบบซอฟต์แวร์ และให้ Framework ในการประเมินประสิทธิภาพและความเหมาะสมสำหรับการใช้งาน ISO/IEC 25010 ได้กำหนดชุดคุณลักษณะและคุณลักษณะย่อยที่ควรพิจารณาเมื่อประเมินโมเดลการออกแบบซอฟต์แวร์ ซึ่งประกอบด้วยเกณฑ์ต่าง ๆ ดังแสดงในรูปที่ 2.22



รูปที่ 2.22 แสดงหมวดหมู่ของ SQuaRE

ที่มา: Febrero, Calero, & Moraga, 2016

จากรูปที่ 2.21 แสดงเกณฑ์ต่าง ๆ โดยประกอบด้วย

2.6.2.1 ความสามารถในการทำงาน การเติบโตของโมเดลการออกแบบซอฟต์แวร์ที่สามารถตอบสนองความต้องการและความจำเป็นของผู้ใช้ได้หรือไม่

2.6.2.2 ประสิทธิภาพ ระดับความเหมาะสมของโมเดลการออกแบบซอฟต์แวร์ในการใช้ทรัพยากรอย่างมีประสิทธิภาพเพื่อประสิทธิภาพการทำงานตามวัตถุประสงค์

2.6.2.3 ความเข้ากันได้ ความสามารถของโมเดลการออกแบบซอฟต์แวร์ในการทำงานร่วมกับซอฟต์แวร์และฮาร์ดแวร์ระบบอื่น ๆ โดยไม่เกิดข้อผิดพลาดหรือความขัดแย้ง

2.6.2.4 ความสะดวกในการใช้งาน ความง่ายในการใช้งานของผู้ใช้กับโมเดลการออกแบบซอฟต์แวร์ รวมถึงความสามารถในการเรียนรู้ ทำความเข้าใจ และใช้งานได้อย่างง่ายดาย

2.6.2.5 ความเชื่อถือได้ ความสามารถของโมเดลการออกแบบซอฟต์แวร์ในการทำงานตามปกติโดยไม่มีข้อผิดพลาดหรือความล้มเหลว

2.6.2.6 ความปลอดภัย ความสามารถในการป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต และความเข้าใจวิธีการใช้งานของผู้ใช้

2.6.2.7 ความสามารถในการบำรุงรักษา ความง่ายในการปรับปรุง ปรับเปลี่ยน แก้ไขโมเดลการออกแบบซอฟต์แวร์ตลอดเวลา

2.6.2.8 ความพหุภาพ ความสามารถของโมเดลการออกแบบซอฟต์แวร์ที่จะใช้ได้ในสภาพแวดล้อม แพลตฟอร์ม และระบบต่าง ๆ โดยไม่ต้องแก้ไข

ISO/IEC SQuaRE เป็นชุดมาตรฐานที่จะช่วยให้ผู้พัฒนาซอฟต์แวร์มี Framework ในการประเมินและปรับปรุงคุณภาพโมเดลการออกแบบซอฟต์แวร์ได้อย่างมีประสิทธิภาพ โดยมาตรฐานนี้จะช่วยให้เรารู้จักและเข้าใจคุณลักษณะต่าง ๆ ที่ต้องพิจารณาในการประเมินคุณภาพของโมเดลการออกแบบซอฟต์แวร์ เช่น ความสามารถในการทำงาน ความเชื่อถือได้ ประสิทธิภาพ ความสามารถในการบำรุงรักษา ความพหุภาพ ความเข้ากันได้ และความปลอดภัย

2.6.3 เกณฑ์ที่ใช้ในการประเมินคุณภาพของระบบชีวมิติ

หลักเกณฑ์ที่ใช้ในการวัดประสิทธิภาพของระบบชีวมิติ จากการศึกษการวิจัยที่ใช้ระบบชีวมิติต่าง ๆ สามารถทำการสรุปเกณฑ์ที่เหล่านักวิจัยนำมาใช้ในการวัดประสิทธิภาพของระบบชีวมิติของตนได้ดังแสดงในตารางที่ 2.4

ตารางที่ 2.4 แสดงการสำรวจเกณฑ์ที่ใช้ในการประเมินประสิทธิภาพของระบบชีวมิติต่าง ๆ

ผู้วิจัย	ชื่องานวิจัย	เกณฑ์ในการประเมิน
Dube, Singh, Rajesh and Gurjit (2020)	A Framework for Evaluation of Biometric Based Authentication System	- Performance - Privacy - Security
Kanak and Sogukpinar (2017)	BioTAM: a Technology Acceptance Model for Biometric Authentication Systems	TAM + Trust - Public willingness, Confident, Estimate Privacy, Estimated Security
Zhou et al. (2021)	Evaluation of biometric recognition in the Covid-10 period	Universality, Permanency, Uniqueness, Accuracy, Acquisition, Usability, Safety

ตารางที่ 2.4 แสดงการสำรวจเกณฑ์ที่ใช้ในการประเมินประสิทธิภาพของระบบชีวมิติต่าง ๆ (ต่อ)

ผู้วิจัย	ชื่องานวิจัย	เกณฑ์ในการประเมิน
Ammour et al. (2020)	Multimodal Biometric Identification System Based on the Face and Iris	Accuracy (FAR, FRR)
Siddique, Yasmin, Taher, and Alam (2021)	The Reliability and Acceptance of Biometric System in Bangladesh: Users Perspective	Reliability, Ease of use, Security, Cost
El-Abed and Charrier (2012)	Evaluation of Biometric Systems	Universality, Uniqueness, Permanency, Collectability, Acceptability
Ahsan et al. (2021)	Evaluating the Performance of Eigenface, Fisherface, and Local Binary Pattern Histogram-Based Facial Recognition Methods under Various Weather Conditions	Accuracy, Precision, Recall, F1 Score, Execution Time

ที่มา: Rukhiran et al., 2023

จากตารางที่ 2.4 แสดงหลักเกณฑ์ต่าง ๆ ที่นักวิจัยใช้ในการประเมินระบบชีวมิติของตน ซึ่งเกณฑ์ที่มักจะนำมาใช้ในการประเมินประสิทธิภาพของระบบชีวมิติได้แก่ ความแม่นยำ (Accuracy), เวลาที่ใช้ในการประมวลผล (Processing Time), ราคา (Cost), และอื่น ๆ

2.6.3.1 ค่าความแม่นยำ ในระบบชีวมิติ เป็นค่าที่ใช้วัดประสิทธิภาพของระบบในการตรวจสอบตัวตนของบุคคล ซึ่งจะบอกว่าระบบชีวมิติมีความแม่นยำเท่าใดในการระบุตัวตนของบุคคลจากข้อมูลที่ได้รับ เช่น สแกนลายพิมพ์นิ้วมือ, สแกนใบหน้า, หรือเสียงพูด ค่าความแม่นยำสามารถคำนวณค่าเฉลี่ยความแม่นยำในการจำแนก (Average Classification Accuracy: ACA) การใช้งานความแม่นยำในระบบชีวมิติจะต้องพิจารณากับสภาวะแวดล้อมและเงื่อนไขการใช้งานอย่างรอบคอบ เช่น ถ้าระบบมีความแม่นยำสูงแต่เมื่อผู้ใช้งานใช้งานในสภาวะแวดล้อมที่ซับซ้อนหรือใช้งานไม่ถูกต้อง เช่น ใช้งานเป็นช่วงเวลากลางคืน หรือมีแสงสว่างไม่เพียงพอ การระบุตัวตนอาจมีความผิดพลาดสูงขึ้นมีสูตรในการคำนวณ ดังนี้

$$\text{Accuracy} = \frac{(\text{TP} + \text{TN})}{(\text{TP} + \text{FP} + \text{TN} + \text{FN})} \quad (2-1)$$

True Positive (TP) คือ จำนวนของตัวอย่างที่ถูกต้องตามที่ระบบ Biometric ทำนายว่าเป็น Positive

True Negative (TN) คือจำนวนของตัวอย่างที่ถูกต้องตามที่ระบบ Biometric ทำนายว่าเป็น Negative

False Positive (FP) คือ จำนวนของตัวอย่างที่ระบบ Biometric ทำนายว่าเป็น Positive แต่จริง ๆ แล้วไม่ใช่ Positive

False Negative (FN) คือ จำนวนของตัวอย่างที่ระบบ Biometric ทำนายว่าเป็น Negative แต่จริง ๆ แล้วไม่ใช่ Negative

2.6.3.2 อัตราความผิดพลาด (Error Rate) หรือ (False Error Rate: FER) ในระบบชีวมิติเป็นอัตราส่วนของจำนวนการตรวจสอบตัวตนที่ผิดพลาด (False Accept Rate: FAR หรือ False Reject Rate: FRR) ต่อจำนวนการตรวจสอบตัวตนทั้งหมด โดยแต่ละระบบชีวมิติจะมีค่า FER ที่แตกต่างกันไป อย่างไรก็ตามค่า FER มักเป็นตัวบอกความสามารถในการระบุตัวตนของระบบ ค่า FER ยิ่งต่ำ แสดงว่าระบบมีความแม่นยำสูงในการระบุตัวตนของบุคคล ค่า FER สามารถแบ่งออกเป็นสองประเภทได้ คือ FAR และ FRR โดยเมื่อเทียบกับค่า Threshold ที่กำหนดขึ้นมา ค่า FAR จะบอกถึงอัตราส่วนของการตรวจสอบตัวตนที่ถูกต้องแต่ระบบชีวมิติกลับระบุว่าเป็นบุคคลอื่น (ส่วนที่ผิดพลาดเป็น False Positive) ในขณะที่ค่า FRR จะบอกถึงอัตราส่วนของการตรวจสอบตัวตนที่ไม่สามารถระบุตัวตนของบุคคลแต่จริง ๆ แล้วเป็นบุคคลนั้น (ส่วนที่ผิดพลาดเป็น False Negative) การใช้งานค่า FER ต้องพิจารณาพร้อมกับค่าความแม่นยำและความเหมาะสมของการใช้งานของระบบชีวมิติเพื่อประเมินประสิทธิภาพและความเป็นไปได้ในการใช้งานของระบบ โดยปกติแล้ว ค่า FER จะต้องต่ำกว่าค่าความแม่นยำเนื่องจากค่า FER นั้นเป็นส่วน of ค่าความแม่นยำ และมีอิทธิพลต่อการตัดสินใจในการรับประกันว่าระบบชีวมิติมีความเหมาะสมหรือไม่ เช่น การใช้งานระบบชีวมิติในการระบุตัวตนของบุคคลที่มีลักษณะหน้าตาคล้ายกันหลายคน หรือในสถานะแวดล้อมที่ซับซ้อน เช่น แสงสว่างไม่เพียงพอ ก็อาจทำให้ค่า FER สูงขึ้น โดยเฉพาะค่า FAR ซึ่งอาจทำให้มีการปลอมแปลงตัวตนได้ง่ายขึ้น ดังนั้นการใช้งานระบบชีวมิติต้องพิจารณาความเหมาะสมและความน่าเชื่อถือของผลการวิเคราะห์ทั้งหมดก่อนที่จะใช้งานในสถานการณ์จริง โดยสามารถคำนวณค่า FER ได้ดังสมการ ข้างล่าง (Precise Biometrics, 2014)

$$FER = \frac{(FAR+FRR)}{2} \quad (2-2)$$

ซึ่ง $FAR = FMR * (1 - FTA)$ (2-3)

และ $FRR = FTA + (FNMR) * (1 - FTA)$ (2-4)

โดยที่ ค่า False Match Rate (FMR) คือ โอกาสของการตรวจสอบตัวตนที่ระบบชีวมิติตรวจพบว่าเป็นตัวตนที่ไม่ถูกต้อง เช่น ผู้เข้าสอบไม่ได้ลงทะเบียนในระบบ แต่ระบบชีวมิติกลับระบุว่าบุคคลนั้นสามารถเข้าสอบได้ ค่า FMR สามารถคำนวณได้โดยการหาร้อยละของจำนวนการยอมให้ผู้เข้าสอบที่เป็นตัวปลอมเข้าสอบต่อจำนวนของผู้เข้าสอบตัวปลอมทั้งหมด

ค่า False Not Match Rate (FNMR) คือ โอกาสของการตรวจสอบตัวตนที่ระบบชีวมิติไม่สามารถระบุตัวตนของบุคคลได้ถูกต้อง เช่น ผู้เข้าสอบนี้ได้ลงทะเบียนในระบบ แต่ระบบชีวมิติกลับระบุว่าผู้เข้าสอบไม่สามารถเข้าสอบได้ ค่า FNMR สามารถคำนวณได้โดยการหาร้อยละของจำนวนการปฏิเสธไม่ให้ผู้เข้าสอบที่เป็นตัวจริงเข้าห้องสอบต่อจำนวนของผู้เข้าสอบตัวจริงทั้งหมด

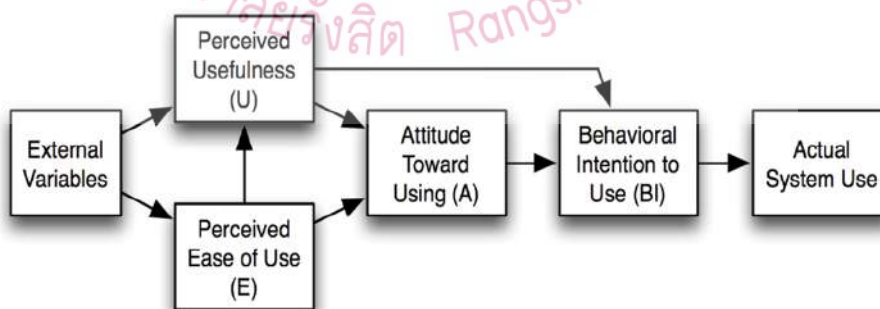
ค่า False to Acquire (FTA) คือ โอกาสของการที่อุปกรณ์ไม่สามารถเก็บข้อมูลชีวมิติได้ในการตรวจสอบ เช่น ไม่สามารถทำการสแกนลายพิมพ์นิ้วมือได้ด้วยหลากหลายสาเหตุ เป็นต้น

2.6.3.3 เวลาที่ใช้ในการตรวจสอบ (Processing Time) คือ เวลารวมของการตรวจสอบผู้เข้าสอบด้วยชีวมิติ ตั้งแต่เริ่มเข้าสู่กระบวนการตรวจสอบจนได้ผลลัพธ์ของการตรวจสอบ

2.6.3.4 ค่าใช้จ่าย (Cost) เนื่องจากทุกระบบมีค่าใช้จ่าย ซึ่งจะมากหรือน้อยขึ้นอยู่กับความต้องการของระบบนั้น ๆ เช่น กรณีที่ต้องใช้ระบบการตรวจสอบผู้เข้าสอบด้วยชีวมิติในการสอบที่มีผู้เข้าสอบจำนวนมาก ระบบนั้นย่อมต้องเน้นทางด้านความเร็ว ดังนั้นการเลือกใช้ประเภทของชีวมิติย่อมต้องสอดคล้องไปตามความต้องการของผู้ใช้งาน ค่าใช้จ่ายแบ่งได้ 2 ประเภท ได้แก่ ค่าอุปกรณ์ชีวมิติ (Sensor Cost) และค่าใช้จ่ายของระบบ (System Cost) เช่น ค่าจ้างผู้คุมสอบ ค่าอุปกรณ์ IOT อื่น ๆ เป็นต้น

2.7 แบบจำลองการยอมรับเทคโนโลยี (Technology Acceptance Model: TAM)

TAM (Technology Acceptance Model) เป็นแบบจำลองทฤษฎีที่ใช้ในการอธิบายกระบวนการที่ผู้ใช้เทคโนโลยีเข้าใจและยอมรับเทคโนโลยี โดยตัวทฤษฎีถูกพัฒนามาจากทฤษฎีการกระทำด้วยเหตุผล (Theory of Reasoned Action: TRA) โดยการใช้แบบสอบถามเพื่อเก็บข้อมูลและวิเคราะห์ผลของการใช้โมเดล TAM โดยผลลัพธ์จากการวิจัยพบว่า ปัจจัยที่ส่งผลต่อการยอมรับและการใช้งานเทคโนโลยีคือความคิดเห็นของผู้ใช้ที่มีความสัมพันธ์กับคุณค่าและความสะดวกในการใช้งานของเทคโนโลยี และนิสัยทางสังคมที่มีผลกระทบต่อการใช้งานเทคโนโลยี อีกทั้งยังพบว่า การควบคุมพฤติกรรมที่มีผลต่อความสามารถในการใช้งานเทคโนโลยีมีความสำคัญอย่างมากในการส่งเสริมการใช้งานเทคโนโลยีในองค์กร การวิจัยนี้ช่วยให้ผู้ประกอบการในองค์กรเข้าใจและตระหนักถึงความสำคัญของปัจจัยที่ส่งผลต่อการยอมรับและการใช้งานเทคโนโลยี การศึกษาตัวโมเดลนี้จะช่วยให้ผู้วิจัยและผู้พัฒนาเทคโนโลยีเข้าใจแนวโน้มในการใช้งานเทคโนโลยีของผู้ใช้ในองค์กร โดย TAM มีสองตัวแปรหลัก ได้แก่ ตัวแปรแรกคือความคุ้มค่าที่รู้สึก (Perceived Usefulness) หมายถึงความคุ้มค่าที่ผู้ใช้รู้สึกว่า การใช้เทคโนโลยีจะช่วยให้เขาประสบความสำเร็จหรือประโยชน์ในการทำงานได้มากขึ้นหรือไม่ ซึ่งการรับรู้ถึงประโยชน์และ คุณค่าของการใช้งานที่ได้ จะส่งผลโดยตรงต่อความตั้งใจในการใช้งานครั้งต่อไป และตัวแปรที่สองได้แก่ความสะดวกในการใช้งานที่รู้สึก (Perceived Ease of Use) หมายถึง ความสะดวกในการใช้งานที่ผู้ใช้รู้สึกว่า การใช้งานเทคโนโลยีจะง่ายและสะดวกแค่ไหน การรับรู้ความง่ายในการใช้งานนี้ยังส่งผลทางอ้อมต่อความตั้งใจในการใช้งานครั้งต่อไป ดังแสดงในรูปที่ 2.23



รูปที่ 2.23 แสดง Technology Acceptance Model (TAM)

ที่มา: Davis, 1989

2.8 การวิเคราะห์แบบจำลองสมการโครงสร้าง (Structural Equation Modeling: SEM)

การวิเคราะห์แบบจำลองสมการโครงสร้าง หรือ SEM เป็นเครื่องมือการวิเคราะห์ข้อมูลทางสถิติที่ใช้ในการทดสอบแบบจำลองที่มีการสัมพันธ์ระหว่างตัวแปรในระบบที่ซับซ้อน โดย SEM ทำการวิเคราะห์หลายตัวแปรพร้อมกันโดยใช้โครงสร้างแบบพารามิเตอร์ (Parameterized Model) เพื่อทำนายและทดสอบการสัมพันธ์ของตัวแปรเหล่านั้น โดย SEM จะทำการรวมการวิเคราะห์ของโมเดลการวิเคราะห์ต่างๆ เช่น การวิเคราะห์ปัจจัย (Factor Analysis) และการวิเคราะห์พื้นฐาน (Path Analysis) เป็นต้น หลักการของ SEM คือการสร้างโมเดลของระบบโดยใช้หลักการวิเคราะห์พื้นฐาน (Path Analysis) ซึ่งเป็นการวิเคราะห์การสัมพันธ์ของตัวแปรแบบหนึ่งเท่านั้น และสามารถสร้างโมเดลระดับสูงขึ้นได้โดยการรวมหลายๆ โมเดลพื้นฐานเข้าด้วยกัน โดยใช้การวิเคราะห์ปัจจัย (Factor Analysis) เพื่อหาตัวแปรที่เป็นตัวกลางในการสัมพันธ์ระหว่างตัวแปรที่ซับซ้อน และการกำหนดตัวแปรที่ต้องการวิเคราะห์เพื่อหาค่าพารามิเตอร์ (Parameter Estimation) เพื่อตรวจสอบและทดสอบแบบจำลองที่เกี่ยวข้องกับข้อมูล โดยการวิเคราะห์ SEM นั้นมีขั้นตอนวิธีการดังนี้

2.8.1 การวิเคราะห์ข้อมูล: ก่อนที่จะเริ่มต้นการวิเคราะห์ SEM จะต้องทำการเตรียมข้อมูลให้พร้อมก่อน โดยการตรวจสอบความถูกต้องของข้อมูล และทำการกำหนดข้อมูลเข้าสู่โปรแกรมวิเคราะห์ที่ใช้

2.8.2 การกำหนดโมเดล: การกำหนดโมเดล SEM จะต้องเลือกโมเดลที่เหมาะสมกับข้อมูล โดยการกำหนดตัวแปรที่ต้องการวิเคราะห์และตัวแปรที่เป็นตัวกลางในการวิเคราะห์

2.8.3 การกำหนดโครงสร้างของโมเดล: โดยทั่วไปจะใช้หลักการวิเคราะห์พื้นฐาน (Path Analysis) ในการกำหนดโครงสร้างของโมเดล โดยการวางแผนโครงสร้างและการกำหนดความสัมพันธ์ระหว่างตัวแปร

2.8.4 การปรับโมเดล: การปรับโมเดล SEM เพื่อให้โมเดลเข้ากับข้อมูลได้อย่างดีที่สุด โดยการปรับเปลี่ยนโครงสร้างของโมเดล หรือการเพิ่มหรือลดตัวแปรที่เกี่ยวข้อง

2.8.5 การประเมินโมเดล: การประเมินโมเดล SEM โดยใช้เทคนิคภาวะสารูปสนิทธิ (Goodness of Fit) ในการตรวจสอบว่าโมเดลเหมาะสมกับข้อมูลหรือไม่ โดยจะใช้ค่าทางสถิติต่างๆ เช่น การวิเคราะห์ค่าไคสแควร์ (Chi-Square), ดัชนีวัดระดับความสอดคล้องเปรียบเทียบ (Comparative Fit Index: CFI), ค่าความคลาดเคลื่อนในการประมาณค่าพารามิเตอร์ (Root Mean Squared Error of Approximation: RMSEA), ค่ารากของค่าเฉลี่ยกำลังสองของส่วนเหลือมาตรฐาน (Root Mean Squared Residual: SRMR) เป็นต้น

2.8.6 การทดสอบสมมติฐาน: การทดสอบสมมติฐาน (Hypothesis Testing) ในการตรวจสอบว่าความสัมพันธ์ของตัวแปรที่สรุปได้จากโมเดล SEM เป็นไปตามทฤษฎีหรือไม่ โดยจะใช้ค่าทางสถิติเช่น p-value เพื่อตรวจสอบความสำคัญของความสัมพันธ์นั้น ๆ

2.8.7 การแก้ไขโมเดล: หากพบว่าโมเดลไม่เหมาะสมหรือไม่สอดคล้องกับข้อมูล จะต้องทำการแก้ไขโมเดลด้วยการปรับค่าพารามิเตอร์ หรือเพิ่มหรือลดตัวแปรเพื่อให้โมเดลสอดคล้องกับข้อมูลมากขึ้น

2.8.8 การนำเสนอผลการวิเคราะห์: การนำเสนอผลการวิเคราะห์ SEM ต้องอธิบายการวิเคราะห์และผลที่ได้ในลักษณะที่เข้าใจง่าย เช่น การอธิบายความสัมพันธ์ระหว่างตัวแปร การตีความค่าทางสถิติ เป็นต้น

โดยการวิเคราะห์ SEM จะต้องใช้โปรแกรมสำเร็จรูปที่รองรับการวิเคราะห์ SEM เช่น AMOS, Mplus, LISREL, หรือ R ซึ่งให้ความสะดวกสบายในการทำงานและให้ผลลัพธ์ที่แม่นยำและถูกต้อง

2.9 งานวิจัยที่เกี่ยวข้อง

2.9.1 การประยุกต์ใช้งานเทคโนโลยีชีวมิติ

งานวิจัยของ Yadav and Virendra (2019) ได้ นำเสนอเทคนิคการระบุตัวตนในภาพโดยใช้เทคโนโลยีการแทนที่แบบหายาก (Sparse Representation) ร่วมกับการแบ่งช่วงค่าคงที่ (Interval Type-2) และการใช้ Kernel การแทนที่แบบหายาก เพื่อเพิ่มประสิทธิภาพในการระบุตัวตนในภาพหน้าผู้ใช้งาน การทดสอบใช้ชุดข้อมูลภาพหน้า LFW (Labeled Faces in the Wild) ซึ่งเป็นชุดข้อมูลที่ใช้ในการทดสอบเทคนิคการระบุตัวตนในภาพหน้าอย่างแพร่หลายในวงการวิจัยด้านนี้ ผลการทดสอบพบว่า เทคนิคที่นำเสนอมีประสิทธิภาพในการระบุตัวตนที่ดีกว่าการใช้เทคนิคการแทนที่แบบหายากแบบทั่วไปโดยเฉพาะเมื่อมีการใช้ Kernel ร่วมกับการแทนที่แบบหายาก และการแบ่งช่วงค่าคงที่ (Interval Type-2) เพื่อลดผลกระทบจากความไม่แน่นอนของข้อมูลในการระบุตัวตนในภาพโดยใช้ใบหน้า ผลการวิเคราะห์ทางประสิทธิภาพทางการทดลองพบว่าการปรับปรุงในความแม่นยำตั้งแต่ร้อยละ 2-10 สูงกว่าผลงานที่มีอยู่ในปัจจุบัน

งานวิจัยของ Kas, Merabet, Ruichek, and Messoussi (2018) นำเสนอเทคนิคการระบุตัวตนในโดยใช้ใบหน้าโดยใช้เทคโนโลยีการเรียนรู้เชิงลึก (Deep Learning) และการนำเข้ามิติ

ใหม่ (New Dimension Input) โดยใช้เทคนิค Cross Decoded Patterns (CDP) ร่วมกับ Topology of Mixed Neighborhood (TMN) ซึ่งเป็นการทำให้การระบุตัวตนด้วยใบหน้ามีประสิทธิภาพสูงขึ้นกว่าวิธีการที่มีในปัจจุบัน

งานวิจัยของ Yaddaden, Adda, Bouzouane, Gaboury, and Bouchard (2018) ได้นำเสนอบทความเกี่ยวกับระบบการรู้จำใบหน้าที่มีประสิทธิภาพและใช้โครงสร้าง Convolutional Neural Network (CNN) โดยได้นำเสนอระบบการใช้แท็ก RFID ที่มีโมดูลตรวจจับข้อผิดพลาด การทดลองนำไปใช้กับชุดข้อมูลใบหน้าประเภทสามารถให้ผลลัพธ์ที่มีประสิทธิภาพสูงกว่าร้อยละ 95 และมีการปรับปรุงผลลัพธ์อย่างสม่ำเสมอ โดยมีอัตราการตรวจจับผิดพลาดลดลงถึงร้อยละ 20 โดยระบบนี้จะมีการจัดเก็บข้อมูลใบหน้าของผู้ใช้ในแท็ก RFID เพื่อใช้ในการรู้จำใบหน้าของผู้ใช้ และการตรวจสอบความถูกต้องของผู้ใช้ก่อนอนุญาตให้เข้าใช้ระบบหรือเข้าสู่สถานที่ที่ต้องการตรวจสอบตัวบุคคล

งานวิจัยของ Awojide et al. (2018) ได้นำเสนอระบบช่วยตรวจสอบตัวตนของผู้สอบในสถาบันการศึกษาในประเทศไนจีเรีย โดยได้นำเสนอระบบช่วยตรวจสอบตัวตนด้วยการใช้ลายพิมพ์นิ้วมือที่มีความปลอดภัยสูง โดยการใช้ระบบรูปแบบการรู้จำรูปแบบออนไลน์ ระบบนี้สามารถรับประกันความปลอดภัยในการตรวจสอบตัวตนของผู้สอบได้ ผ่านการตรวจสอบลายพิมพ์นิ้วมือเพื่อยืนยันตัวตนของผู้ใช้งาน ทำให้การสอบในสถาบันการศึกษาเป็นไปอย่างเป็นระบบและมีประสิทธิภาพมากขึ้น โดยระบบนี้จะช่วยลดการทุจริตในการสอบและช่วยให้การทำชำนั้นเกิดขึ้นได้ยาก อีกทั้งยังช่วยป้องกันการทุจริตในการสอบ

งานวิจัยของ Taileb (2020) ได้นำเสนอระบบการรู้จำลายพิมพ์นิ้วมือและเทคโนโลยี RFID เพื่อใช้ในการยืนยันตัวตนของนักเรียน นอกจากนี้ ยังมีการวิจัยหลายฉบับที่ใช้ขั้นตอนวิธีอัลกอริทึมที่แตกต่างกัน เช่น Tatar (2017) ได้นำเสนออัลกอริทึมใหม่สำหรับการรู้จำลายพิมพ์นิ้วมือ โดยที่การวิจัยเหล่านี้มีเป้าหมายเดียวกันคือเพื่อที่จะพัฒนาระบบการรับรองตัวตนที่มีประสิทธิภาพสูงในการจัดการกับการเข้าห้องเรียนของนักเรียนในสถาบันการศึกษา ซึ่งช่วยเพิ่มความปลอดภัยและความถูกต้องแม่นยำในการยืนยันตัวตนในการเข้าถึงทรัพยากรและสิ่งของต่าง ๆ ในสถาบันการศึกษา

งานวิจัยของ Yang, Wang, Hu, Zheng, and Valli (2018) เกี่ยวกับระบบการรู้จำเส้นเลือดนิ้วมือ ซึ่งประกอบด้วยสองขั้นตอนหลัก คือ ขั้นตอนการลงทะเบียนและขั้นตอนการตรวจสอบตัวตน ในขั้นตอนแรก รูปภาพเส้นเลือดนิ้วมือจะถูกถ่ายขึ้นและทำการปรับปรุงคุณภาพ (Enhance) จากนั้นจึงแยกแยะลักษณะเด่นและเก็บเป็นแม่แบบ ในขั้นตอนการตรวจสอบตัวตน จะถูกนำเอาตัวอย่างเส้นเลือดนิ้วมือของผู้ใช้งานมาใช้ในการทดสอบ โดยมีการปรับปรุงขั้นตอนเบื้องต้นและการแยกแยะลักษณะเด่น สุดท้ายจึงนำผลลัพธ์การทดสอบเทียบกับแม่แบบที่เก็บไว้เพื่อทำการตรวจสอบและยืนยันตัวตนของผู้ใช้งาน

งานวิจัยของ Xi, Yang, and Yin (2016) นำเสนอโครงการสำหรับระบบช่วยรู้จำเชิงชีวภาพโดยใช้รูปแบบเส้นเลือดนิ้วมือ โดยใช้เทคนิค Discriminative Binary Code (DBC) เพื่อให้ระบบสามารถแยกแยะลักษณะเด่นได้ง่ายขึ้น และยังใช้ฐานข้อมูล PolyU และฐานข้อมูล MLA ในการทดสอบ นอกจากนี้ยังมีการใช้ข้อมูลที่ประกอบด้วยข้อมูลที่มีการกำกับดูแลและ SVM ที่ช่วยให้ DBC มีความแยกแยะและสั้นลง ระบบนี้สามารถช่วยในการรักษาความปลอดภัยในการเข้าถึงทรัพยากรของผู้ใช้งานได้อย่างมีประสิทธิภาพสูง โดยที่มีการลดเวลาในการรับรู้และตรวจสอบตัวตนของผู้ใช้งานด้วยวิธีการที่มีความแม่นยำและเร็ว

งานวิจัยของ Noma-Osaghae, Robert, Okereke, Okesola, and Okokpujie (2017) ได้นำเสนอการใช้ระบบยืนยันตัวตนด้วยการสแกนดวงตาเพื่อเข้าถึงประตู โดยได้นำเสนอวิธีการใช้ระบบรูปแบบดวงตา (Iris) ในการยืนยันตัวตนเพื่อเข้าถึงประตู ระบบนี้ใช้เทคโนโลยีสแกนดวงตาเพื่อจดจำและตรวจสอบตัวตนของผู้ใช้งาน ซึ่งช่วยเพิ่มความปลอดภัยในการเข้าถึงสถานที่ ระบบนี้สามารถระบุตัวตนของผู้ใช้งานได้อย่างแม่นยำและรวดเร็ว ทำให้ผู้ใช้งานไม่จำเป็นต้องใช้บัตรหรือรหัสผ่านเพื่อเข้าถึงสถานที่ และช่วยลดการเข้าถึงของบุคคลที่ไม่มีอำนาจหรือไม่ได้รับอนุญาตให้เข้าถึงสถานที่

งานวิจัยของ Gomez-Barrero, Maiorana, Galbally, Campisi, and Fierrez (2017) มุ่งเน้นวิธีการปกป้องข้อมูลตัวแทนช่วยระบุตัวตน (Template) ที่เกี่ยวกับการระบุตัวตนแบบหลายแบบ (Multimodal Biometric) อย่างมีประสิทธิภาพ โดยใช้เทคนิค Homomorphic Encryption ในการเข้ารหัสและปกป้องข้อมูลตัวแทนช่วยระบุตัวตนของผู้ใช้ซึ่งได้นำวิธีการใช้ Homomorphic Encryption เพื่อปกป้องข้อมูลตัวแทนช่วยระบุตัวตน (Template) ที่เกี่ยวกับการระบุตัวตนแบบหลายแบบ เช่น การระบุตัวตนด้วยลายพิมพ์นิ้วมือและใบหน้า โดยทำการแยกแยะและ

เข้ารหัสข้อมูลตัวแทนช่วยระบุตัวตน แล้วทำการปกป้องข้อมูลโดยใช้ Homomorphic Encryption ทำให้ไม่สามารถอ่านหรือเข้าถึงข้อมูลตัวแทนช่วยระบุตัวตนจนกว่าจะถูกถอดรหัส โดยมีการใช้เทคนิค homomorphic hash function เพื่อให้มีความปลอดภัยเมื่อมีการเก็บข้อมูลในระบบ ผลการทดลองแสดงให้เห็นว่าการใช้ Homomorphic Encryption สามารถปกป้องข้อมูลตัวแทนช่วยระบุตัวตนได้อย่างมีประสิทธิภาพและคงความลับของข้อมูลได้ดี โดยเฉพาะเมื่อเทียบกับการใช้เทคนิคที่มีอยู่ในปัจจุบันอย่าง Homomorphic Hash Function ที่มีความเสี่ยงต่อการรั่วไหลข้อมูล

งานวิจัยของ Walia, Singh, Singh, and Verma (2019) ได้นำเสนอการพัฒนา ระบบชีวมิติที่ทนทานและมีประสิทธิภาพ โดยใช้หลายตัวบ่งชี้ชีวมิติ เช่น ม่านตา (Iris), ลายพิมพ์ นิ้วมือ (Fingerprint) และต้นแบบการผสมผสานคะแนนระดับที่เหมาะสม โดยระบบนี้ใช้วิธีการ ค้นหาความเหมาะสมที่สุดแบบย้อนกลับ (Backtracking Search Optimization Method: BSA) และ กฎการกระจายความขัดแย้งแบบสัดส่วน (Proportional Conflict Redistribution Rules) ในการ ผสมคะแนนหลังจากใช้ลักษณะหลายอย่าง และใช้ Support Vector Machine สำหรับการจำแนก และรายงานอัตราความถูกต้อง ผลการทดลองแสดงให้เห็นว่าระบบนี้มีความแม่นยำสูงถึงร้อยละ 98.43 และอัตราความผิดพลาดร้อยละ 1.57 ดังนั้น บทความนี้นอกจากจะนำเสนอชีวมิติที่ทนทาน และมีประสิทธิภาพแล้วยังอธิบายวิธีการปรับแต่งและผสมคะแนนเพื่อเพิ่มประสิทธิภาพของระบบ ซึ่งจะช่วยให้ผู้ใช้งานทำความเข้าใจและเลือกใช้ชีวมิติที่เหมาะสมสำหรับงานของพวกเขา

งานวิจัยของ Dass, Sadrulhuda, Pasha, Nayan, and Nayak (2020) นำเสนอ บทความวิชาการ Real Time Face Recognition using Raspberry Pi โดย มุ่งเน้นการพัฒนา ระบบรูปภาพจำแนกใบหน้าแบบเรียลไทม์โดยใช้ Raspberry Pi โดยระบบนี้ใช้กล้องเว็บแคมและ ระบบปฏิบัติการ Raspbian ซึ่งเป็นระบบปฏิบัติการที่พัฒนามาสำหรับ Raspberry Pi ในการสกัด ลักษณะเชิงบริบทและคุณลักษณะของใบหน้าและจัดกลุ่มตามแต่ละบุคคล ระบบนี้ใช้เทคนิค Viola-Jones ในการตรวจจับใบหน้าและสกัดลักษณะเชิงบริบทและคุณลักษณะของใบหน้า และใช้ Local Binary Pattern (LBP) ในการสกัดคุณลักษณะของใบหน้า จากนั้นใช้ PCA (Principal Component Analysis) ในการลดมิติของข้อมูลและ SVM (Support Vector Machine) สำหรับการ จำแนกใบหน้า ผลการทดลองแสดงให้เห็นว่าระบบนี้มีความแม่นยำถึงร้อยละ 96.5 และสามารถ ทำงานในโหมดเรียลไทม์ได้ ซึ่งเหมาะสำหรับการนำไปใช้ในแอปพลิเคชันต่าง ๆ ที่ต้องการระบบ การรู้จำใบหน้าแบบเรียลไทม์

2.9.2 การวิเคราะห์และออกแบบระบบ

Pukdesree and Netinant (2016) นำเสนอบทความ Conceptual Framework: The Adaptive Biometrics Authentication for Accessing Cloud Computing Services using iPhone โดยมุ่งเน้นการพัฒนาระบบรักษาความปลอดภัยด้วยเทคโนโลยีชีวมิติสำหรับการเข้าถึงการให้บริการประมวลผลแบบก้อนเมฆ (Cloud Computing) ด้วยมือถือระบบปฏิบัติการ iOS โดยนำเสนอกรอบแนวคิดการทำงานแบบเชิงพื้นที่สำหรับระบบการพิสูจน์ตัวตนที่ปรับตัวให้เหมาะสมสำหรับผู้ใช้เพื่อเข้าถึงการให้บริการประมวลผลแบบก้อนเมฆ โดยระบบนี้ใช้ชีวมิติเพื่อตรวจสอบความถูกต้องของตัวตนของผู้ใช้ และการปรับตัวต้นแบบอัตโนมัติเพื่อเพิ่มประสิทธิภาพของระบบการพิสูจน์ตัวตน และยังได้นำเสนอการออกแบบและการพัฒนาระบบการพิสูจน์ตัวตนด้วยเทคโนโลยีชีวมิติสำหรับ iPhone ซึ่งรวมถึงการเลือกใช้ฟิเจอร์ชีวมิติที่เหมาะสมสำหรับผู้ใช้แต่ละคน นอกจากนี้ บทความยังอธิบายการใช้งานและการปรับตัวของระบบที่ช่วยให้ผู้ใช้สามารถเข้าถึงการให้บริการประมวลผลแบบก้อนเมฆได้อย่างปลอดภัย ในส่วนสุดท้าย บทความยอมรับว่าการพัฒนาระบบดังกล่าวยังต้องปรับปรุงและพัฒนาต่อไปในอนาคต

งานวิจัยของ Lee (2014) ได้นำเสนอบทความวิชาการเรื่อง Software Quality Factors and Software Quality Metrics to Enhance Software Quality Assurance โดยนำเสนอแนวคิดเกี่ยวกับปัจจัยคุณภาพของซอฟต์แวร์และการวัดคุณภาพของซอฟต์แวร์เพื่อเสริมความมั่นใจในคุณภาพของซอฟต์แวร์ บทความนี้ได้กล่าวถึงปัจจัยที่มีผลต่อคุณภาพของซอฟต์แวร์ โดยแบ่งออกเป็นหลายประเภทเช่น ประสิทธิภาพของซอฟต์แวร์ ความปลอดภัยของซอฟต์แวร์ การบำรุงรักษาและการแก้ไขข้อบกพร่องของซอฟต์แวร์ และการติดต่อสื่อสารระหว่างผู้ใช้และซอฟต์แวร์ นอกจากนี้ บทความยังเสนอการวัดคุณภาพของซอฟต์แวร์ด้วยการใช้ Software Quality Metrics ซึ่งเป็นเครื่องมือในการวัดคุณภาพของซอฟต์แวร์ ซึ่งแบ่งออกเป็นหลายประเภทเช่น ประสิทธิภาพของซอฟต์แวร์ ความปลอดภัยของซอฟต์แวร์ ความสะดวกในการใช้งาน และความเป็นไปได้ในการขยายขนาด

งานวิจัยของ Febrero et al. (2016) นำเสนอบทความหัวข้อ Software Reliability Modeling Based on ISO/IEC SQuaRE โดยเป็นการนำเสนอการวิเคราะห์และสร้างโมเดลความเชื่อถือของซอฟต์แวร์โดยใช้หลักการของมาตรฐาน ISO/IEC Systems and Software Quality Requirements and Evaluation (SQuaRE) ซึ่งเป็นมาตรฐานระดับสากลที่ใช้ในการประเมินคุณภาพ

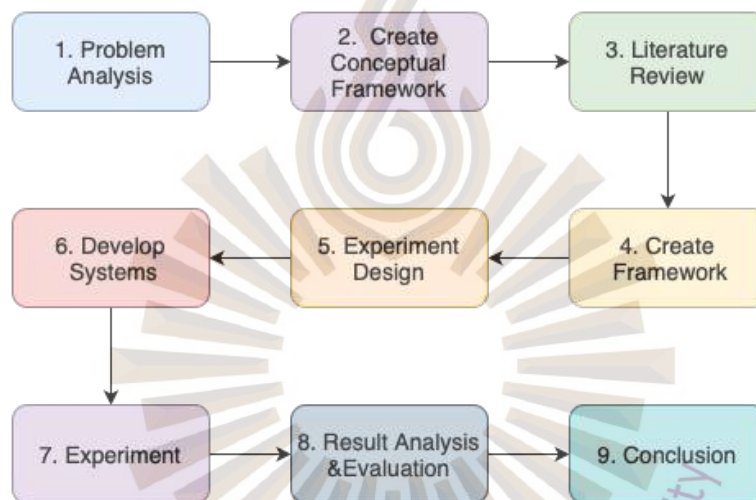
ของซอฟต์แวร์ ซึ่งบทความนี้แนะนำวิธีการใช้ SQuaRE เพื่อกำหนดและตรวจสอบคุณภาพของซอฟต์แวร์ด้วยการสร้างโมเดลความเชื่อถือโดยใช้ข้อมูลที่ได้จากการทดสอบและประเมินความเสี่ยง โดยการสร้างโมเดลความเชื่อถือจะช่วยให้ผู้พัฒนาซอฟต์แวร์สามารถประเมินความเสี่ยงและปรับปรุงซอฟต์แวร์ให้มีคุณภาพสูงขึ้น นอกจากนี้ ยังอธิบายวิธีการใช้งาน SQuaRE เพื่อวัดความเสี่ยงและการบำรุงรักษาซอฟต์แวร์โดยมีการอ้างอิงถึงแนวทางการสร้างโมเดลของ SQuaRE โดยเฉพาะอย่างยิ่ง ISO/IEC ซึ่งเป็นมาตรฐานของ SQuaRE ในการประเมินคุณภาพซอฟต์แวร์



บทที่ 3

ระเบียบวิธีการวิจัย

ขั้นตอนในการวิจัยแบ่งออกเป็น 9 ขั้นตอน ดังแสดงในรูปที่ 3.1 ดังนี้



รูปที่ 3.1 แสดงขั้นตอนในการดำเนินงานวิจัย

ที่มา: ผู้วิจัย, 2566

จากรูปที่ 3.1 แสดงขั้นตอนการดำเนินการของงานวิจัยฉบับนี้ โดยเริ่มจากขั้นแรกทำการระบุปัญหาของงานวิจัยนี้

3.1 การศึกษาและระบุปัญหา (Problem Analysis)

ปัญหาของงานวิจัยนี้เริ่มจากการมองเห็นปัญหาในการตรวจสอบผู้เข้าสอบในการสอบในปัจจุบันโดยมีประเด็นของปัญหาคือ เราจะมีความมั่นใจได้มากน้อยแค่ไหนว่าผู้เข้าสอบเป็นความจริง และระบบการตรวจสอบแบบดั้งเดิมนั้นมีประสิทธิภาพเพียงพอหรือไม่ในกรณีที่มีจำนวนผู้เข้าสอบเป็นจำนวนมาก ซึ่งเป็นที่มาของแนวคิดที่จะนำเทคโนโลยีชีวมิติมาประยุกต์ใช้ จากการศึกษาทฤษฎีและงานวิจัยที่เกี่ยวข้องเกี่ยวกับเทคโนโลยีชีวมิติเพื่อที่จะนำมาประยุกต์ใช้ในการตรวจสอบผู้เข้า

สอบ ทำให้เก็บเป็นประเด็นคำถามที่นำไปสู่การตั้งวัตถุประสงค์ในการทำวิจัย ซึ่งแบ่งออกเป็น 3 วัตถุประสงค์ ได้แก่

3.1.1 เพื่อสร้างกรอบโครงร่างระบบซอฟต์แวร์สำหรับการตรวจสอบตัวบุคคลเข้าสู่ระบบด้วยเทคโนโลยีชีวมิติบนอุปกรณ์สมองกลฝังตัว

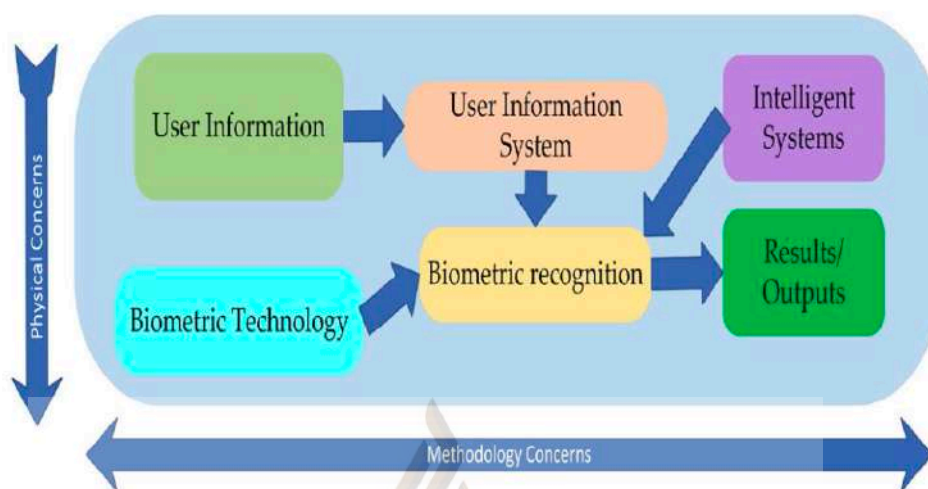
3.1.2 เพื่อพัฒนาต้นแบบซอฟต์แวร์สำหรับการตรวจสอบตัวบุคคลเข้าสู่ระบบทางชีวมิติแบบหลายโปรโตคอล ซึ่งรองรับเทคโนโลยีชีวมิติแบบทางเดียวและแบบหลายทาง

3.1.3 เพื่อเปรียบเทียบประสิทธิภาพและประสิทธิผลของระบบหลายโปรโตคอลบนชีวมิติหลายแบบในการตรวจสอบบุคคลเข้าสู่ระบบ

นอกจากนี้ยังมีประเด็นปัญหาในการยอมรับการเทคโนโลยีในการใช้งานระบบการตรวจสอบตัวบุคคลเข้าสู่ระบบทางชีวมิติ ซึ่งในปัจจุบันการนำใช้เทคโนโลยีชีวมิติเป็นเสมือนดาบสองคม เนื่องจากหากข้อมูลหลุดรั่วไหลออกไปย่อมทำให้เกิดความเสียหายหลายด้าน โดยเฉพาะการใช้ชีวมิติในการทำธุรกรรมต่าง ๆ เช่น การใช้ใบหน้าในการยืนยันการทำธุรกรรมทางการเงิน หรือการเข้าถึงข้อมูลที่เป็นส่วนตัว เป็นต้น ในงานวิจัยนี้ได้ทำการประเมินการยอมรับเทคโนโลยีเพื่อประเมินแนวโน้มในการยอมรับเทคโนโลยีชีวมิติเพื่อนำไปใช้ในอนาคตอีกด้วย

3.2 การพัฒนากอบแนวคิด (Create Conceptual Framework)

เพื่อที่จะตอบคำถามตามวัตถุประสงค์ในงานวิจัยในการพัฒนาต้นแบบซอฟต์แวร์สำหรับการตรวจสอบตัวบุคคลเข้าสู่ระบบทางชีวมิติ และเพื่อเป็นต้นแบบให้นักพัฒนาสามารถนำไปเป็นต้นแบบในการพัฒนาระบบตรวจสอบผู้เข้าสู่ระบบของสถาบันการศึกษาต่าง ๆ ได้ จึงได้ทำการพัฒนากอบแนวคิดของการประยุกต์ใช้งานเทคโนโลยีชีวมิติในการตรวจสอบผู้เข้าสู่ระบบ โดยงานวิจัยนี้ได้นำเสนอกรอบความคิดในการพัฒนาต้นแบบสำหรับการออกแบบระบบตรวจสอบผู้เข้าสู่ระบบด้วยเทคโนโลยีชีวมิติ โดยประกอบด้วยองค์ประกอบ 6 ด้าน ได้แก่ ด้านข้อมูลผู้เข้าสู่ระบบ (User Information) ระบบการจัดการการสอบ (User Information System) ผลลัพธ์ (Result/Output) เทคโนโลยีชีวมิติ (Biometric Technology) การตรวจสอบด้วยชีวมิติ (Biometric Recognition) และระบบอัจฉริยะ (Intelligent System) ดังแสดงในรูปที่ 3.2



รูปที่ 3.2 แสดง Biometric Examinee Personal Verification System (BEPVS) Conceptual Framework

ที่มา: Rukhiran et al., 2023

จากรูปที่ 3.2 กรอบแนวความคิดของการพัฒนาตัวต้นแบบการออกแบบระบบการตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติ ประกอบด้วย 6 องค์ประกอบ โดยมีรายละเอียด ดังนี้

3.2.1 ด้านข้อมูลผู้เข้าสอบ (User Information) หมายถึงองค์ประกอบที่เกี่ยวข้องกับข้อมูลของผู้เข้าสอบว่ามีข้อมูลแบบใดบ้าง รวมถึงวิธีการรวบรวมข้อมูล การเก็บบันทึกข้อมูล เช่น ข้อมูลทั่วไป ข้อมูลชีวมิติ

3.2.2 ด้านระบบการจัดการการสอบ (User Information System) หมายถึงองค์ประกอบที่เกี่ยวข้องกับการจัดสอบ เช่น ข้อมูลตารางสอบ สถานที่สอบ รายชื่อผู้เข้าสอบ กรรมการผู้คุมสอบ เป็นต้น

3.2.3 ด้านผลลัพธ์ (Result/Output) หมายถึงองค์ประกอบที่เกี่ยวข้องกับรูปแบบของผลลัพธ์ในการตรวจสอบผู้เข้าสอบ

3.2.4 ด้านเทคโนโลยีชีวมิติ (Biometric Technology) หมายถึงองค์ประกอบที่เกี่ยวข้องกับเทคโนโลยีชีวมิติที่นำมาใช้ เช่น การเชื่อมต่ออุปกรณ์ชีวมิติ การตั้งค่าสภาพแวดล้อม เป็นต้น

3.2.5 ด้านการตรวจสอบด้วยชีวมิติ (Biometric Recognition) หมายถึงองค์ประกอบที่เกี่ยวข้องกับวิธีการที่ใช้เทคโนโลยีในการตรวจสอบผู้เข้าสอบ เช่น ใช้อัลกอริทึมแบบใด ใช้ประเภทของชีวมิติแบบใด นำมาเชื่อมต่อกับระบบการจัดการข้อมูลในการสอบอย่างไร เป็นต้น

3.2.6 ด้านระบบอัจฉริยะ (Intelligent System) หมายถึงองค์ประกอบที่เกี่ยวข้องกับการใช้ระบบอัจฉริยะต่าง ๆ ที่อาจจะมีในอนาคตได้อย่างไร เช่น การนำไปใช้บน Smart School เป็นต้น

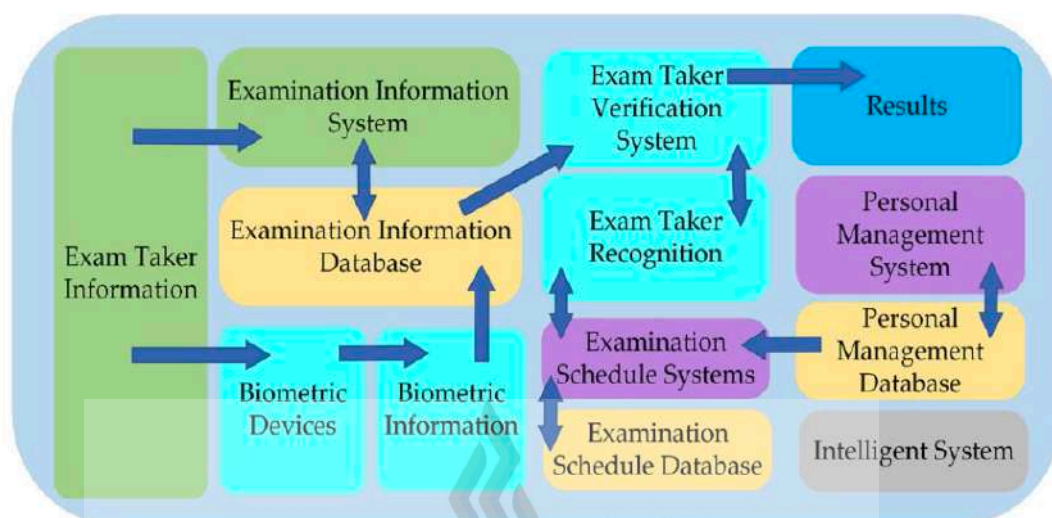
3.3 ทบทวนวรรณกรรม (Literature Review)

เมื่อได้วางกรอบแนวคิดในการวิจัยแล้ว ได้ทำการศึกษาทฤษฎีและงานวิจัยที่เกี่ยวข้อง โดยแบ่งเนื้อหาการศึกษาออกเป็น ส่วน ๆ ได้แก่ การศึกษาเทคโนโลยีชีวมิติ การศึกษาระบบการจัดการการสอบ และการประเมินประสิทธิภาพในการออกแบบ ซึ่งกล่าวไว้ในบทที่ 2 แล้ว

3.4 พัฒนารอบการทำงาน (Create Framework)

3.4.1 กรอบแนวคิดเชิงส่วนประกอบระบบการตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติ (Biometric Examinee Personal Verification System Component Framework)

การพัฒนารอบการทำงาน คือ การพัฒนาต้นแบบการในออกแบบเพื่อใช้ในการสร้างระบบการตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติโดยใช้กรอบความคิดเป็นต้นแบบ ซึ่งการพัฒนารอบการทำงานนี้ทำโดยการวิเคราะห์ สังเคราะห์ จากการทบทวนวรรณกรรมต่าง ๆ ที่เกี่ยวข้อง โดยใช้แนวทางการออกแบบตามมาตรฐานการออกแบบของ IEEE SDD และ ISO 25010 SQuaRE และอ้างอิงจากกรอบแนวคิดของการพัฒนาต้นแบบการออกแบบระบบการตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติ ดังแสดงรูปที่ 3.2 ผลลัพธ์ที่ได้คือกรอบแนวคิดเชิงส่วนประกอบเพื่อนำไปใช้เป็นต้นแบบในการพัฒนาระบบการตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติ ซึ่งสามารถแบ่งส่วนประกอบเป็น 13 ส่วน ดังแสดงใน รูปที่ 3.3 ซึ่งแสดงให้เห็นส่วนประกอบและความสัมพันธ์ระหว่างแต่ละส่วนประกอบ



รูปที่ 3.3 แสดง Biometric Examinee Personal Verification System (BEPVS) Revised Framework
ที่มา: Rukhiran et al., 2023

จากรูปที่ 3.3 แสดงส่วนประกอบย่อยทั้ง 13 ส่วน และความเชื่อมต่อระหว่างแต่ละองค์ประกอบ ซึ่งมีรายละเอียดดังนี้

3.4.1.1 Exam Taker Information หมายถึง องค์ประกอบที่เกี่ยวข้องกับข้อมูลทั่วไปของผู้เข้าสอบ โครงสร้างของข้อมูล รวมถึงวิธีการนำข้อมูลเข้าสู่ระบบ

3.4.1.2 Examination Information System หมายถึง องค์ประกอบที่เกี่ยวข้องกับระบบการจัดการข้อมูลผู้เข้าสอบ ในบางสถาบันการศึกษาที่ไม่มีความพร้อมด้าน ICT ที่ยังไม่มีระบบฐานข้อมูลในการเก็บข้อมูลผู้เข้าสอบ จำเป็นที่จะต้องมีการจัดการกับข้อมูลผู้เข้าสอบ ซึ่งบางสถาบันการศึกษาที่มีความพร้อมที่มีระบบการจัดการข้อมูลผู้เข้าสอบอยู่แล้วต้องสามารถทำการนำระบบที่มีมาทำการเชื่อมต่อกับส่วนอื่นได้

3.4.1.3 Examination Information Database หมายถึง ระบบฐานข้อมูลในการจัดเก็บข้อมูลผู้เข้าสอบทั้งในรูปแบบข้อมูลทั่วไป และข้อมูลชีวมิติ

3.4.1.4 Biometric Device หมายถึง อุปกรณ์ชีวมิติที่จะนำมาใช้ในระบบการตรวจสอบว่าเป็นแบบใด มีการเชื่อมต่อแบบใด สามารถทำงานบนระบบปฏิบัติการแบบใด

3.4.1.5 Biometric Information หมายถึง ข้อมูลชีวมิติที่ได้มาจากอุปกรณ์ชีวมิติ รูปแบบของข้อมูล ซึ่งจะถูกลำไปเก็บไว้ใน Examination Information Database ร่วมกับ Exam Taker Information

3.4.1.6 Exam Taker Verification System หมายถึง ตัวระบบการตรวจสอบผู้เข้าสอบ ซึ่งจะประกอบด้วยข้อมูลจากส่วนต่าง ๆ ได้แก่ รายชื่อผู้เข้าสอบในแต่ละวิชา รายวิชาที่สอบ

และสถานที่สอบ กรรมการคุมสอบ วิธีการในการตรวจสอบผู้เข้าสอบที่จะใช้ในสถาบันการศึกษานั้น ๆ รวมทั้งผลลัพธ์ที่ได้จากการตรวจสอบ กล่าวคือในส่วนประกอบนี้เป็นศูนย์กลางในการทำงานหลักของระบบนั่นเอง

3.4.1.7 Exam Taker Recognition หมายถึง วิธีการในการตรวจสอบผู้เข้าสอบว่าใช้วิธีการใด

3.4.1.8 Examination Schedule System หมายถึง ระบบการจัดการข้อมูลที่เกี่ยวข้องในการจัดการสอบ เช่น รายชื่อผู้สอบ รายวิชาที่สอบ เวลาที่สอบ สถานที่สอบ เป็นต้น

3.4.1.9 Examination Schedule Database หมายถึง ฐานข้อมูลที่เก็บข้อมูลในการจัดสอบ

3.4.1.10 Result หมายถึง ผลลัพธ์ที่ได้จากการตรวจสอบผู้เข้าสอบ ซึ่งแต่ละสถาบันการศึกษามีความต้องการที่แตกต่างกัน บางสถาบันอาจต้องรูปแบบของผลลัพธ์ที่เป็นภาพรวม บางที่อาจต้องการดูผลแบบเรียลไทม์ เป็นต้น

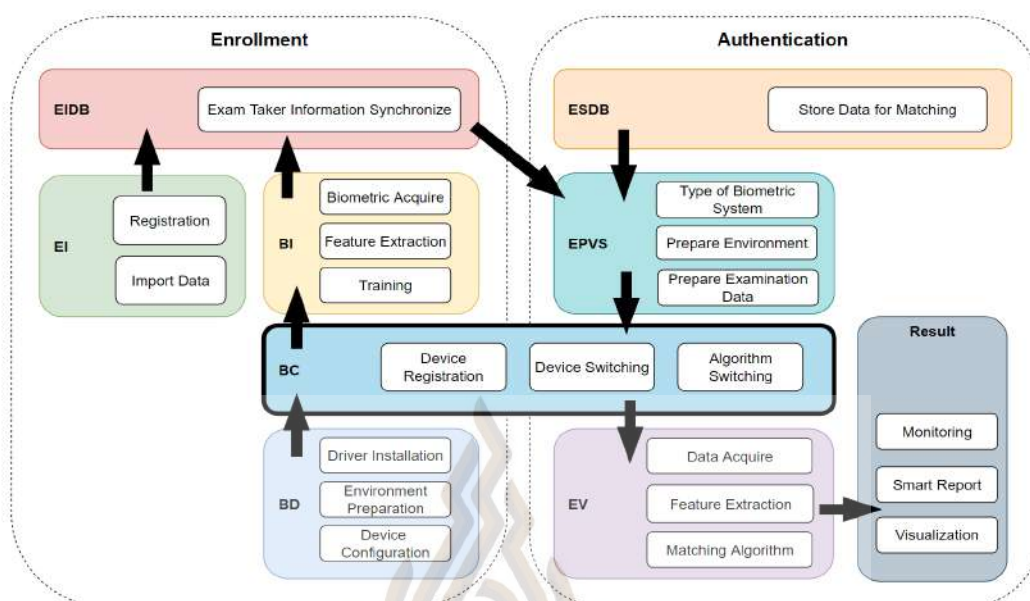
3.4.1.11 Personal Management System หมายถึง ระบบการจัดการข้อมูลกรรมการคุมสอบ ซึ่งในการจัดสอบบางครั้งจำเป็นต้องมีการเก็บข้อมูลของกรรมการคุมสอบด้วยเพื่อเป็นข้อมูลในการพิจารณาในด้านอื่น ๆ ต่อไป เช่น การประเมินภาระงาน เป็นต้น

3.4.1.12 Personal Management Database หมายถึง ฐานข้อมูลในการเก็บข้อมูลกรรมการคุมสอบ

3.4.1.13 Intelligent System ด้านระบบอัจฉริยะ (Intelligent System) หมายถึง องค์ประกอบที่เกี่ยวข้องกับการใช้ระบบอัจฉริยะต่าง ๆ ที่อาจจะมีในอนาคตได้อย่างไร เช่น การนำไปใช้บน Smart School เป็นต้น

3.4.2 กรอบแนวคิดเชิงออกแบบระบบการตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติ (Biometric Examinee Personal Verification System Design Framework)

ผลลัพธ์จากการพัฒนากกรอบแนวคิดเชิงการออกแบบโดยใช้ดังรูปที่ 3.3 เป็นพื้นฐานในการวิเคราะห์ แสดงในรูปที่ 3.4



รูปที่ 3.4 กรอบแนวคิดเชิงการออกแบบระบบการตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติ

ที่มา: Rukhiran et al., 2023

กรอบแนวคิดเชิงการออกแบบระบบการตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติ ดังแสดงในรูปที่ 3.4 เป็นการแสดงกระบวนการและขั้นตอนในการทำงานของระบบการตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติเพื่อเป็นต้นแบบให้นักพัฒนานำไปเป็นต้นแบบในการพัฒนาระบบการตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติของตนเองได้ โดยมีรายละเอียดดังนี้

3.4.2.1 การนำข้อมูลเข้า (Enrollment) ได้แก่การนำข้อมูลเข้าสู่ระบบ ขั้นตอนนี้ทำได้ในตอนที่ผู้เข้าสอบทำการลงทะเบียนเรียนหรือสมัครสอบ โดยแบ่งการนำเข้าข้อมูลเป็น 2 ส่วน ได้แก่ ข้อมูลทั่วไป (Exam Taker Information: EI) จากการกรอกข้อมูลหรือทำการดึงข้อมูลจากฐานข้อมูล (ถ้ามี) และข้อมูลชีวมิติ (Biometric Information: BI) จากอุปกรณ์ชีวมิติ (Biometric Device: BD) ที่ใช้ในระบบนั้น ๆ นำมาบันทึกไว้ในฐานข้อมูล (Examination Information Database: EIDB)

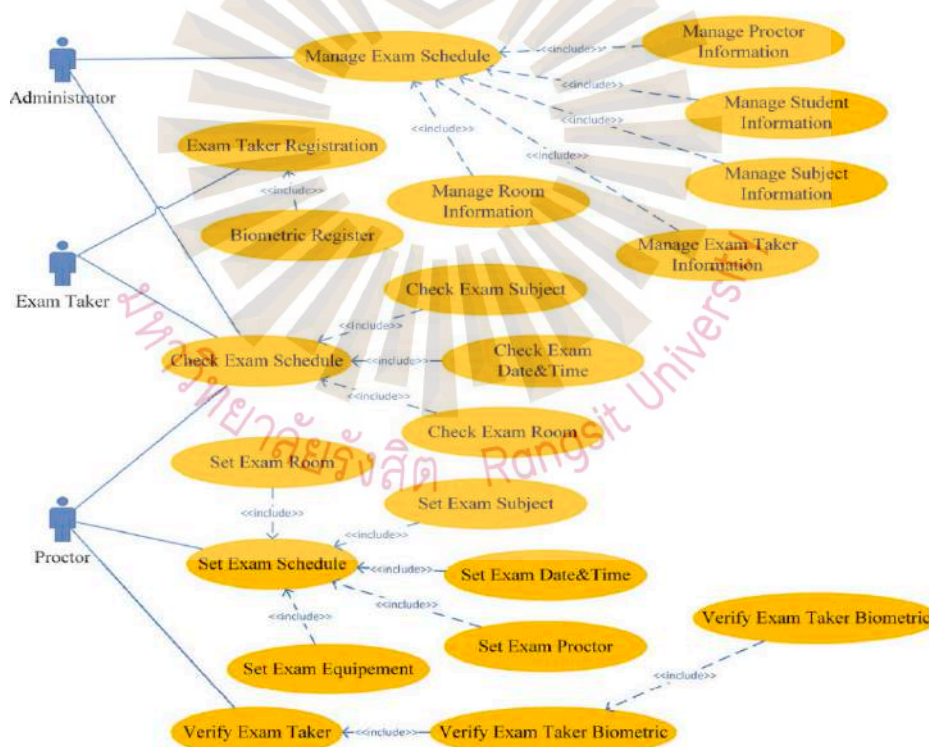
3.4.2.2 การตรวจสอบผู้เข้าสอบ (Authentication) ได้แก่ขั้นตอนในการตรวจสอบผู้เข้าสอบ โดยเริ่มจากผู้เข้าสอบทำการตรวจสอบข้อมูลการสอบ (Examination Schedule Database: ESDB) เช่นวิชาสอบ ห้องสอบ สถานที่สอบ จากนั้นเมื่อถึงเวลาเข้าสอบผู้เข้าสอบทำการตรวจสอบผ่านระบบตรวจสอบผู้เข้าสอบ (Exam Taker Personal Verification System: EPVS) โดยใช้อุปกรณ์ชีวมิติ (BD) และวิธีการตรวจสอบ (Exam Taker Verify) ของระบบนั้น ๆ และทำการบันทึกหรือแสดงผลลัพธ์ (Result) ตามรูปแบบที่สถาบันการศึกษานั้นกำหนด

3.4.2.3 ในส่วนของ Biometric Control (BC) เป็นส่วนควบคุมการเชื่อมต่อและใช้งานอุปกรณ์ชีวมิติ ซึ่งในกรณีที่มีการใช้งาน Multimodal Biometric จำเป็นต้องเตรียม BC ไว้ใช้ในการควบคุมการเพื่อสับเปลี่ยนอุปกรณ์ชีวมิติด้วย

3.5 การออกแบบเครื่องมือที่ใช้ในการตรวจสอบบุคคลเข้าสอบ

ในการออกแบบและพัฒนาเครื่องมือที่ใช้ในการทดลองนี้ ผู้วิจัยได้ใช้หลักการวิเคราะห์และออกแบบเชิงวัตถุร่วมกับการใช้ Information Flow Diagram (IFD) เป็นหลักการในการออกแบบ โดยระบบตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติ โดยได้ผลการออกแบบ ดังนี้

3.5.1 Use-case Diagram



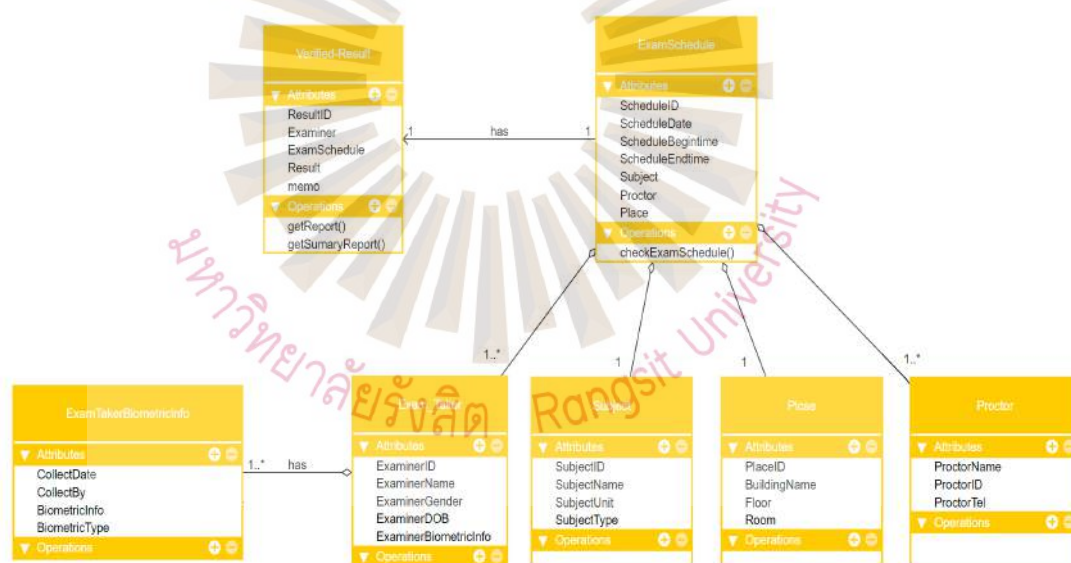
รูปที่ 3.5 แสดง Use-case Diagram ระบบการตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติ
ที่มา: Rukhiran et al., 2023

Use-case Diagram ในรูปที่ 3.5 ประกอบด้วยผู้ที่เกี่ยวข้องในการใช้ระบบ (Actor) และกิจกรรมที่ทำในระบบ (Use-case) ซึ่ง ผู้ใช้ระบบ ได้แก่ ผู้ดูแลระบบ (Admin) กรรมการคุมสอบ

(Proctor) และผู้เข้าสอบ (Examinee) โดยผู้ดูแลระบบสามารถทำกิจกรรมการนำข้อมูลผู้สอบเข้าระบบ (Examinee Registration) ซึ่งรวมทั้งข้อมูลชีวมิติ (Biometric Register) และจัดการข้อมูลการสอบ (Manage Exam Schedule) ซึ่งประกอบด้วยข้อมูลวิชาที่สอบ (Manage Exam Subject) สถานที่สอบ (Manage Room) กรรมการคุมสอบ (Manage Proctor Info) และรายชื่อผู้เข้าสอบ (Manage Examinee List) กรรมการคุมสอบสามารถตรวจสอบข้อมูลการสอบ (Check Exam Schedule) ตรวจสอบผู้เข้าสอบ และผู้เข้าสอบสามารถทำกิจกรรมการลงทะเบียนสอบ (Examinee Registration) และตรวจสอบข้อมูลการสอบ (Check Exam Schedule) ได้

3.5.2 Class Diagram

ในการออกแบบฐานข้อมูลเพื่อรองรับการทำงานของระบบตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติ ใช้ Class Diagram ในการออกแบบ โดยได้ผลลัพธ์ดังแสดงในรูปที่ 3.6



รูปที่ 3.6 แสดง Class Diagram ระบบการตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติ

ที่มา: Rukhiran et al., 2023

ข้อมูลที่ใช้ในระบบตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติประกอบด้วย 7 คลาสหลัก ประกอบด้วย

3.5.2.1 ExamSchedule เป็นคลาสที่เก็บข้อมูลการสอบ ประกอบด้วยคลาสย่อย ได้แก่ Exam_Taker, Subject, Place, Proctor, และ Verified-Result

3.5.2.2 Exam Taker เป็นคลาสที่เก็บข้อมูลทั่วไปของผู้สอบ เช่น ชื่อนามสกุล

รหัสสอบ เพศ ประกอบด้วยคลาสย่อย ExamTakerBiometricInfo

3.5.2.3 ExamTakerBiometricInfo เป็นคลาสที่เก็บข้อมูลชีวมิติ ซึ่งในคลาสนี้อาจมีโครงสร้างที่แตกต่างกันไปตามประเภทของข้อมูลชีวมิติ ซึ่งขึ้นอยู่กับประเภทของชีวมิติที่นำมาใช้

3.5.2.4 Subject เก็บข้อมูลรายวิชา

3.5.2.5 Place เก็บข้อมูลสถานที่ที่มีการจัดสอบ

3.5.2.6 Proctor เก็บข้อมูลกรรมการคุมสอบ

3.5.2.7 Verified-Result เก็บข้อมูลผลการตรวจสอบ

3.5.3 Information Flow Diagram (IFD)

ในการออกแบบระบบตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติ เพื่อแสดงมุมมองการออกแบบที่มากกว่า 1 มุมมองใน 1 แผนภาพการออกแบบ ซึ่งสามารถแสดงมุมมองของการออกแบบได้ดังนี้ มุมมองด้าน UX/UI มุมมองการไหลของข้อมูล มุมมองของกระบวนการทำงานของระบบ และมุมมองของข้อมูลที่ใช้ โดยได้ใช้ IFD เป็นกรอบในการพัฒนา ซึ่งผลลัพธ์ในการออกแบบระบบตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติ แสดงในรูปที่ 3.7



รูปที่ 3.7 แสดง Information Flow Diagram ระบบการตรวจสอบผู้เข้าสอบโดยใช้

เทคโนโลยีชีวมิติ

ที่มา: ผู้วิจัย, 2566

จากรูปที่ 3.7 แสดงให้เห็นการใช้งานระบบตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติ เริ่มจากกรรมการสอบทำการเข้าสู่ระบบ (Login) เข้าสู่ระบบจะเห็นข้อมูลการสอบที่ตนเป็น กรรมการคุมสอบทั้งหมด เมื่อทำการเลือกรายวิชาที่สอบ จะแสดงข้อมูลการสอบในรายวิชานั้น ๆ ซึ่งประกอบด้วย ห้องสอบ เวลาสอบ และรายชื่อผู้เข้าสอบ จากนั้นเมื่อถึงเวลาสอบให้ผู้เข้าสอบ ตรวจสอบผ่านอุปกรณ์ที่ละคน กรรมการคุมสอบสามารถดูผลลัพธ์การตรวจสอบบนหน้าจอ ซึ่งถ้า ตรวจสอบผ่านจะทำการบันทึกผลการมาเข้าสอบของผู้เข้าสอบคนนั้นในระบบได้เลย

3.6 การออกแบบการทดลอง (Experiment Design)

การทดลองในงานวิจัยนี้แบ่งออกเป็น 2 การทดลอง ได้แก่ (1) การทดลองการเปรียบเทียบ การใช้งานของระบบตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติในรูปแบบต่าง ๆ ที่ได้รับการ พัฒนาตามกรอบการทำงาน และ (2) การทดลองการยอมรับเทคโนโลยีการใช้งานระบบตรวจสอบ ผู้เข้าสอบด้วยเทคโนโลยีชีวมิติ โดยจะทำการทดลองแรกก่อน และอธิบายการทดลองที่สองใน หัวข้อ 3.8 โดยในการทดลองแรกแบ่งเป็น 3 ประเด็นหลัก ๆ ดังนี้

3.6.1 การเตรียมข้อมูล

ในการทดลองเพื่อทดสอบประสิทธิภาพและประสิทธิผลของระบบการตรวจสอบ ด้วยเทคโนโลยีชีวมิติมักใช้จำนวนภาพที่เหมาะสมในการทดสอบ เช่น Ahsan et al. (2021) ได้ใช้ ข้อมูลจำนวน 17 คน เป็นจำนวนใบหน้าคนละ 7 รูป ทั้งหมด 119 รูป ในการทดลองนี้ได้เตรียม นักศึกษาระดับปริญญาตรี คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏวไลยอลงกรณ์ ในพระบรมราชูปถัมภ์ จำนวน 30 คน เก็บข้อมูลใบหน้าจำนวนคนละ 10 รูป ซึ่งเพียงพอต่อการ ทดลองโดยการแบ่งกลุ่มผู้เข้าสอบเป็นผู้เข้าสอบตัวจริง 15 คน และตัวปลอม 15 คน ซึ่งผู้วิจัยได้ทำ การอธิบายวัตถุประสงค์ในการทดลอง เนื้อหาและกระบวนการในการทดลองให้กับกลุ่มนักศึกษาที่ ใช้ในการทดลอง อีกทั้งยังเปิดช่องทางในการติดต่อสอบถามทางออนไลน์กับผู้วิจัยในกรณีที่ นักศึกษามีข้อสงสัย ผู้วิจัยได้แจ้งให้นักศึกษาผ่านการยินยอมว่าพวกเขาจะให้ข้อมูลชีวมิติใบหน้า และลายพิมพ์นิ้วมือในการทำการทดลองด้วยความสมัครใจ โดยข้อมูลของนักศึกษาและข้อมูล ชีวมิติได้รับการปกป้องและใช้เพื่อยืนยันตัวตนที่หน้าห้องสอบในวันสอบที่กำหนดเท่านั้น ซึ่งนักศึกษาทุกคนได้ทำการยินยอมในการเข้าร่วมโครงการวิจัย เพื่อที่จะสร้างความมั่นใจในความ

แม่นยำของข้อมูลชีวมิติ ผู้วิจัยได้ทำขั้นตอนการเรียนรู้และทดสอบระบบและกำหนดความแม่นยำให้อยู่ในระดับร้อยละ 85

3.6.1.1 การเตรียมข้อมูลใบหน้าของผู้เข้าสอบ การเตรียมข้อมูลชีวมิติของผู้เข้าสอบ ประกอบด้วยข้อมูลใบหน้าและข้อมูลลายพิมพ์นิ้วมือของผู้เข้าสอบ การเตรียมข้อมูลใบหน้า ทำโดยการถ่ายรูปใบหน้าของผู้เข้าสอบในมุมที่ต่างกัน จำนวนคนละ 10 ภาพ โดยมีขนาดของภาพที่ 640 x 480 พิกเซล และมีระยะห่างจากกล้อง ประมาณ 1.12 เมตร จึงจะได้ข้อมูลที่เหมาะสมที่สุดในการทำการรู้จำใบหน้า (Rukhiran and Netinan, 2020) จากนั้นจึงทำตามขั้นตอนดังนี้

1) การค้นใบหน้า โดยเริ่มจากใช้วิธีการ Haar Cascade ในการค้นหารูปใบหน้าเพื่อสร้างกรอบรูปใบหน้า ในขั้นตอนนี้ได้พัฒนาโปรแกรมด้วยภาษา Python โดยใช้ OpenCV ในภาษา Python ด้วยฟังก์ชัน `cv2.CascadeClassifier()`

2) จากนั้นทำการสกัดคุณลักษณะของใบหน้า โดยใช้ วิธีการ LBPH เพื่อสกัดคุณลักษณะของใบหน้าเพื่อทำการเก็บคุณลักษณะลงในฐานข้อมูล ซึ่งเป็นวิธีการที่เหมาะสมที่สุดในการสกัดคุณลักษณะของใบหน้า (Ahsan et al., 2021) ในการทำชุดข้อมูลในการทดสอบเพื่อให้ระบบจดจำใบหน้าทำงานได้อย่างมีประสิทธิภาพ โดยใช้ OpenCV library ซึ่งเป็นไลบรารีที่ช่วยในการประมวลผลภาพดิจิทัลได้ง่ายขึ้น เมื่อได้คุณลักษณะที่ต้องการแล้วนำมาทำการสอนโดยใช้ Train Recognizer

3) เก็บคุณลักษณะลงในฐานข้อมูล ซึ่งในงานวิจัยนี้ได้ใช้ MySQL ติดตั้งบน Cloud Server เพื่อทำการเก็บข้อมูล

4) การตรวจสอบข้อมูลใบหน้า เมื่อถึงวันสอบ ระบบจะทำการจับคู่ข้อมูลคุณลักษณะใบหน้าของผู้เข้าสอบกับข้อมูลใบหน้าที่เก็บอยู่ในฐานข้อมูล เพื่อเปรียบเทียบว่าเป็นคน ๆ เดียวกันหรือไม่ โดยการจับคู่เพื่อเปรียบเทียบ

3.6.1.2 ในส่วนของการเตรียมข้อมูลลายพิมพ์นิ้วมือ ทำการเก็บข้อมูลลายพิมพ์นิ้วมือของผู้เข้าสอบจำนวน 2 นิ้ว ใช้ Raspberry Pi Fingerprint Library ในการสร้างข้อมูลทดสอบ (Martin, Koprda, & Lubor, 2018) โดยทำการสกัดคุณลักษณะของลายพิมพ์นิ้วมือ ด้วยวิธีการ Scale-Invariant Feature Transform (SIFT) ด้วยภาษา Python สามารถทำได้โดยใช้ OpenCV โดยทำการสร้าง SIFT Detector โดยใช้ฟังก์ชัน `cv2.xfeatures2d.SIFT_create()` และทำการหา Keypoints และ Descriptors จากรูปภาพ ซึ่ง Keypoints เป็นจุดโดดเด่นบนภาพที่ SIFT จับได้ และ Descriptors เป็นเวกเตอร์ที่เก็บข้อมูลคุณลักษณะของจุดโดดเด่นนั้น ๆ ซึ่งสามารถนำไปใช้ในการเปรียบเทียบภาพ จากนั้นทำการนำคุณลักษณะที่ได้ไปเก็บไว้ในฐานข้อมูล ในการจับคู่ลายพิมพ์นิ้วมือ (Fingerprint Matching) ผู้วิจัยได้ใช้วิธีการ FLANN (Fast Library for Approximate Nearest Neighbors) ด้วยภาษา

Python สามารถทำได้โดยใช้ OpenCV ซึ่งเป็น Python library โดยการเปรียบเทียบ Keypoints ระหว่างลายพิมพ์นิ้วมือของผู้เข้าสอบกับลายพิมพ์นิ้วมือที่เก็บในฐานข้อมูล

3.6.2 การเตรียมชุดอุปกรณ์

ชุดอุปกรณ์ที่ใช้ในการทดลองการตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติ ประกอบด้วยอุปกรณ์ ดังแสดงในรูปที่ 3.8 ดังนี้

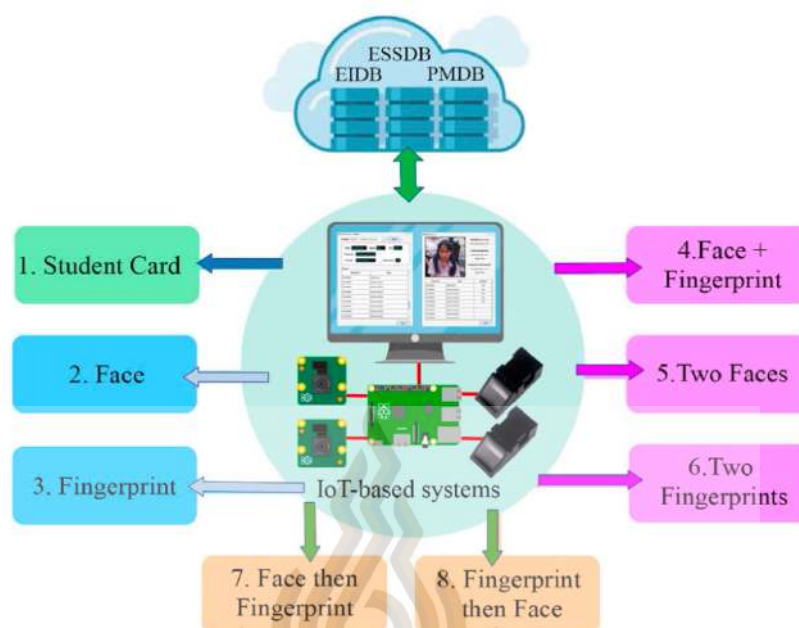
3.6.2.1 Raspberry Pi 4 Model B เป็น Mainboard ที่ใช้ในการประมวลผล เชื่อมต่อไปยัง Cloud Server และเป็นตัวกลางในการเชื่อมต่ออุปกรณ์ IoT ต่าง ๆ เช่น กล้อง เครื่องอ่านลายพิมพ์นิ้วมือ

3.6.2.2 Raspberry Pi Camera 8mp เป็นกล้องที่ใช้ในการเก็บข้อมูลใบหน้าของผู้เข้าสอบ โดยทำการตั้งค่าขนาดพื้นฐานที่กำหนดขนาดของภาพไว้ที่ 640 x 480 พิกเซล

3.6.2.3 Fingerprint Reader Adafruit R305 เป็นเครื่องอ่านลายพิมพ์นิ้วมือที่ใช้งาน และมีความแม่นยำสูง โดยเครื่องอ่านนี้ใช้การเชื่อมต่อผ่าน UART และใช้เทคโนโลยี Optical Sensor

3.6.2.4 Cloud Storage: MySQL ใช้ฐานข้อมูล MySQL ในการจัดเก็บฐานข้อมูล โดยทำการติดตั้งบน Cloud Platform

3.6.2.5 LG Monitor ขนาด 50 นิ้ว ใช้ในการแสดงผลการตรวจสอบผู้เข้าสอบทีละคน โดยแสดงคะแนนการจับคู่ความเหมือนในขณะที่ผู้สอบเดินผ่านกล้อง



รูปที่ 3.8 แสดงภาพรวมการทำงานของระบบชีวมิติทั้ง 8 กลุ่ม

ที่มา: Rukhiran et al., 2023

3.6.3 ขั้นตอนการทดลอง

จากรูปที่ 3.8 การทดลองได้แบ่งเป็น 8 กลุ่ม ซึ่งแต่ละกลุ่มจะมีขั้นตอนการดำเนินการที่แตกต่างกัน แบ่งออกเป็น 4 รูปแบบ ได้แก่ Zero-Biometric, Unimodal Biometric, Multimodal Biometric, และ Semi-Multimodal Biometric โดยมีรายละเอียดแต่ละกลุ่ม ดังนี้

3.6.3.1 กลุ่มที่ 1 ใช้การตรวจสอบแบบดั้งเดิม (Zero Biometric) เป็นการตรวจสอบผู้เข้าสอบจากการตรวจสอบเอกสารของผู้เข้าสอบเช่นบัตรประจำตัวผู้เข้าสอบ

3.6.3.2 กลุ่มที่ 2 ใช้การรู้จำใบหน้า เป็นระบบ Unimodal Biometric โดยใช้การรู้จำใบหน้าในการตรวจสอบผู้เข้าสอบ

3.6.3.3 กลุ่มที่ 3 ใช้การรู้จำลายพิมพ์นิ้วมือ เป็นระบบ Unimodal Biometric โดยใช้การรู้จำใบหน้าในการตรวจสอบผู้เข้าสอบ

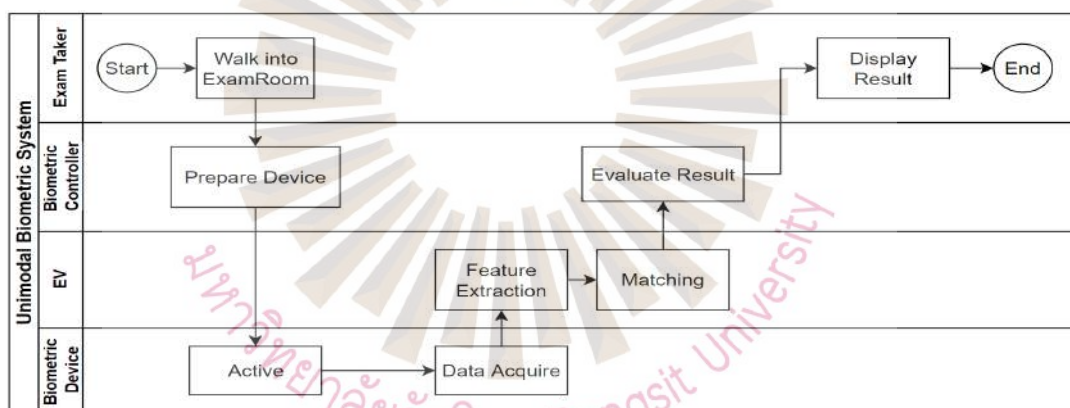
3.6.3.4 กลุ่มที่ 4 ใช้การรู้จำใบหน้า และใช้การรู้จำลายพิมพ์นิ้วมือ เป็นระบบ Multimodal Biometric แบบ Multiple Modalities โดยใช้การรู้จำใบหน้าและการรู้จำลายพิมพ์นิ้วมือในการตรวจสอบผู้เข้าสอบ

3.6.3.5 กลุ่มที่ 5 ใช้การรู้จำใบหน้าโดยใช้กล้อง 2 กล้องลายพิมพ์นิ้วมือ เป็นระบบ Multimodal Biometric แบบ Multiple Modalities โดยใช้ภาพจากกล้อง 2 กล้อง ในการตรวจสอบผู้เข้าสอบ

3.6.3.6 กลุ่มที่ 6 ใช้การรู้จำลายพิมพ์นิ้วมือ ใช้ 2 เครื่องสแกนนิ้วมือ เป็นระบบ Multimodal Biometric แบบ Multiple Modalities โดยใช้ลายพิมพ์นิ้วมือจากเครื่องสแกนลายพิมพ์นิ้วมือจำนวน 2 เครื่อง ในการตรวจสอบผู้เข้าสอบ

3.6.3.7 กลุ่มที่ 7 ใช้การรู้จำใบหน้าเป็นหลักร่วมกับใช้การลายพิมพ์นิ้วมือ เป็นระบบ Multimodal Biometric โดยใช้ใบหน้าในการตรวจสอบก่อน กรณีที่เกิดปัญหาจะใช้ลายพิมพ์นิ้วมือในการตรวจสอบเป็นลำดับต่อไป

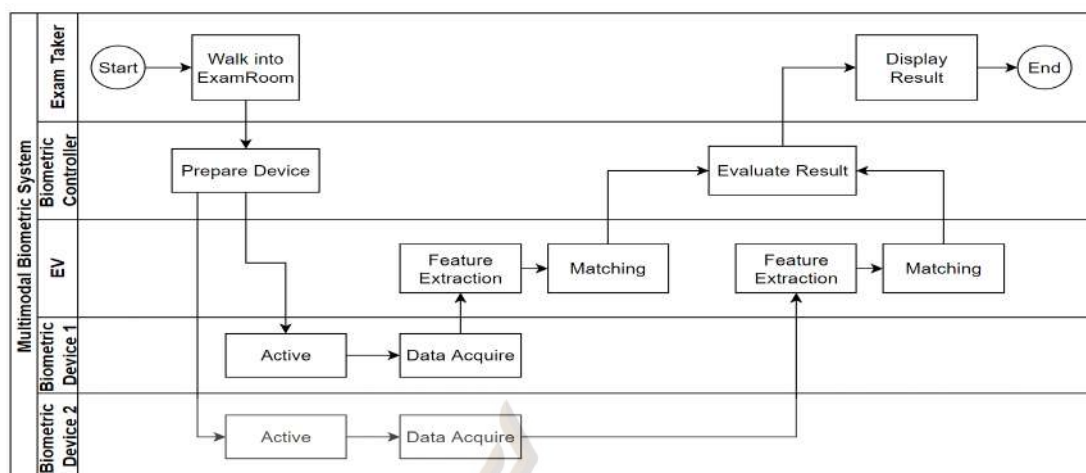
3.6.3.8 กลุ่มที่ 8 ใช้การรู้จำลายพิมพ์นิ้วมือเป็นหลักร่วมกับใช้การรู้จำใบหน้า เป็นระบบ Multimodal Biometric โดยใช้ลายพิมพ์นิ้วมือในการตรวจสอบก่อน กรณีที่เกิดปัญหาจะใช้ภาพจากกล้องในการตรวจสอบเป็นลำดับต่อไป



รูปที่ 3.9 แสดงขั้นตอนการทำงานของระบบ Unimodal Biometric

ที่มา: ผู้วิจัย, 2566

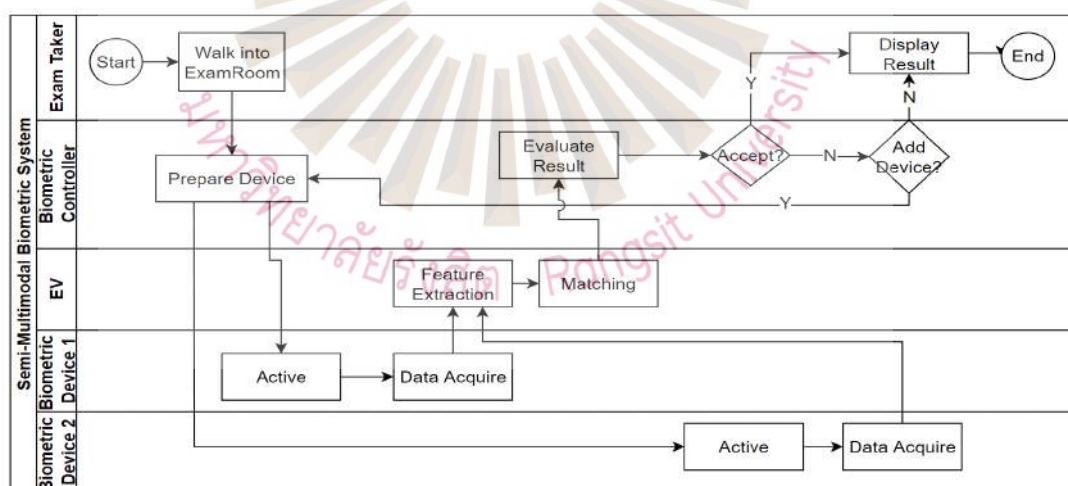
จากรูปที่ 3.9 เป็นขั้นตอนการทำงานของระบบตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติแบบทางเดียว ซึ่งประกอบด้วยกลุ่มทดลองที่ 2 และกลุ่มทดลองที่ 3 โดยเริ่มจากผู้เข้าสอบทำการตรวจสอบข้อมูลชีวมิติ โดยระบบจะทำการตรวจสอบข้อมูลชีวมิติแล้วแสดงผลการตรวจสอบบนหน้าจอ



รูปที่ 3.10 แสดงขั้นตอนการทำงานของระบบ Multimodal Biometric

ที่มา: ผู้วิจัย, 2566

จากรูปที่ 3.10 เป็นขั้นตอนการทำงานของระบบตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติแบบหลายทาง ซึ่งประกอบด้วยกลุ่มทดลองที่ 4 กลุ่มทดลองที่ 5 และกลุ่มทดลองที่ 6 โดยเริ่มจากผู้เข้าสอบทำการตรวจสอบข้อมูลชีวมิติ โดยระบบจะทำการตรวจสอบข้อมูลชีวมิติของผู้เข้าสอบโดยทำการเก็บข้อมูลทั้งสองอุปกรณ์พร้อม ๆ กัน จากนั้นจะแสดงผลการตรวจสอบบนหน้าจอ



รูปที่ 3.11 แสดงขั้นตอนการทำงานของระบบ Semi-Multimodal Biometric

ที่มา: ผู้วิจัย, 2566

จากรูปที่ 3.11 เป็นขั้นตอนการทำงานของระบบตรวจสอบผู้เข้าสอบโดยใช้เทคโนโลยีชีวมิติแบบหลายทาง ซึ่งประกอบด้วยกลุ่มทดลองที่ 7 และกลุ่มทดลองที่ 8 โดยเริ่มจากผู้เข้าสอบทำการตรวจสอบข้อมูลชีวมิติ โดยระบบจะทำการตรวจสอบข้อมูลชีวมิติของผู้เข้าสอบ โดยจะใช้

อุปกรณ์แรกก่อน ในกรณีที่เกิดปัญหาหรือความไม่ชัดเจนในการตรวจสอบจะทำการใช้อุปกรณ์ที่สองในการตรวจสอบแทน จากนั้นจะแสดงผลการตรวจสอบบนหน้าจอ

3.7 การประเมินระบบการตรวจสอบผู้เข้าสอบโดยเทคโนโลยีชีวมิติ

เกณฑ์ในการประเมินประสิทธิภาพสำหรับระบบการตรวจสอบผู้เข้าสอบโดยเทคโนโลยีชีวมิติในงานวิจัยนี้ได้นำเสนอ Biometric Quality Metric ในการประเมิน ซึ่งประกอบด้วยปัจจัยต่างๆ ในการประเมิน ประกอบด้วย ความแม่นยำ (Accuracy), อัตราความผิดพลาด (False Error Rate), เวลาในการประมวลผล (Processing Time), และค่าใช้จ่าย (Cost) เข้าไปด้วย โดยการคำนวณหาค่าความแม่นยำ อัตราความผิดพลาด เวลาในการประมวลผล สามารถคำนวณได้จากสูตรในบทที่ 2 โดยในส่วนของค่าใช้จ่ายในการใช้งานระบบต้องทำการประเมินจากค่าใช้จ่ายทุกรายการที่ใช้ ประกอบด้วย ราคาของอุปกรณ์ ค่าจ้างผู้คุมสอบ และอื่น ๆ เพื่อนำมาเป็นค่าใช้จ่ายโดยเฉลี่ย โดยเขียนเป็นสมการได้ดัง (3-1)

$$\text{Biometric Quality Metric} = \{\text{Accuracy, False Error Rate, Processing Time, Cost}\} \quad (3-1)$$

ในการประเมินด้านค่าใช้จ่าย ในงานวิจัยนี้ได้คำนวณค่าใช้จ่ายโดยพิจารณาจาก ค่าอุปกรณ์ในระบบ ค่าจ้างกรรมการคุมสอบ โดยคิดเป็นค่าใช้จ่ายต่อชั่วโมง โดยค่าจ้างกรรมการคุมสอบของมหาวิทยาลัยราชภัฏวไลยอลงกรณ์ ในพระบรมราชูปถัมภ์ อยู่ที่ 11.43\$ ต่อชั่วโมง และจากงานวิจัยของ Chen, Yang, Wang, and Park (2016) กล่าวว่าอุปกรณ์ IoT มีอายุการใช้งานโดยเฉลี่ยอยู่ที่ 500 ชั่วโมง ซึ่งราคาของชุดอุปกรณ์ IoT (ไม่รวมอุปกรณ์ Sensor) ที่กล่าวในบทที่ 2 อยู่ที่ 720\$ ต่อชุด ดังนั้นการคำนวณค่าใช้จ่าย สามารถคำนวณได้จาก (3-2)

$$\text{Total System Cost} = \frac{(\text{System Cost} + \sum_1^n \text{Sensor}_i)}{\text{age}} \quad (3-2)$$

โดย n คือ จำนวนอุปกรณ์ Sensor

age คือ อายุการใช้งานของอุปกรณ์

ในการคำนวณเพื่อหาค่า Biometric Quality Score สามารถทำได้โดยการปรับค่าคะแนนดั้งเดิมในแต่ละด้านของแต่ละกลุ่ม โดยใช้หลักการเทียบบัญญัติไตรยางค์ โดยกลุ่มที่มีคะแนนมาก

ที่สุดในด้านนั้น ๆ จะได้คะแนน 100 และจะนำคะแนนนั้นเป็นตัวตั้งเพื่อใช้ในการเปรียบเทียบเป็นคะแนนต่อ ๆ มา ยกตัวอย่างเช่น ในด้านความแม่นยำ กลุ่มที่ 6 มีค่าคะแนนสูงที่สุดเมื่อเปรียบเทียบกับกลุ่มอื่น ๆ เพราะฉะนั้น ค่าคะแนนที่ปรับใหม่ของกลุ่มที่ 6 ทางด้านความแม่นยำจะมีค่า 100 คะแนน ต่อมาทำการเปรียบเทียบค่าความแม่นยำของกลุ่มอื่น ๆ ก็จะใช้คะแนนดั้งเดิมของกลุ่มที่ 6 เป็นตัวตั้ง เพื่อนำไปคำนวณหาค่าคะแนนปรับใหม่ของแต่ละกลุ่ม โดยมีสูตรการคำนวณดัง (3-3)

$$\text{Transform Score} = \sum_1^n \frac{X_o * 100}{X_{\max}} \quad (3-3)$$

เมื่อ n คือ จำนวนด้านของปัจจัย

X_o คือ คะแนนดั้งเดิม

$X_{\max}$ คือ คะแนนปรับใหม่

เมื่อทำการปรับค่าคะแนนแล้ว ขั้นตอนถัดมาคือการกำหนดคะแนนอันดับ (Ranking Score) ในแต่ละด้าน เพื่อทำการหาคะแนนรวม (Total Score) โดยการจัดอันดับคะแนนในรูปแบบอันดับที่ ซึ่งการจัดอันดับของคะแนนขึ้นอยู่กับปัจจัยในแต่ละด้าน เช่นการจัดอันดับของความแม่นยำ ยิ่งมีค่าสูงจะมีคะแนนอันดับที่สูง อันดับคะแนนของเวลาที่ใช้ยิ่งใช้เวลามากยิ่งมีคะแนนอันดับน้อย เป็นต้น โดยการให้คะแนนจะเรียงลำดับจากคะแนนเต็ม 5 คะแนนสำหรับกลุ่มที่มีประสิทธิภาพเป็นอันดับแรก และ 4 คะแนนสำหรับกลุ่มที่มีอันดับรองลงมา การให้คะแนนเต็มสามารถกำหนดช่วงตามความต้องการของผู้ใช้งานได้ ในงานวิจัยนี้ผู้วิจัยจะใช้การจัดอันดับโดยแบ่งเป็น 5 อันดับ จากนั้น เมื่อได้ Total Score แล้ว ทำการปรับค่าเพื่อทำการเปรียบเทียบให้ชัดเจน โดยนำ Total Score ไปทำการเทียบบัญญัติไตรยางศ์อีกครั้งเพื่อ ได้ผลลัพธ์สุดท้ายเป็น Biometric Quality Metric

3.8 การประเมินการยอมรับการใช้ระบบการตรวจสอบผู้เข้าสอบโดยเทคโนโลยีชีวมิติ

3.8.1 ประชากรและกลุ่มตัวอย่าง

ในการประเมินการยอมรับการใช้งานระบบการตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติ ผู้วิจัยทำการทดลองจากกลุ่มตัวอย่าง จำนวน 161 คน โดยเลือกเป็นนักศึกษาระดับปริญญาตรี คณะวิทยาศาสตร์และเทคโนโลยี จำนวนทั้งหมด 483 คน โดยการคำนวณขนาดของ

กลุ่มตัวอย่างจากหลักการของ Yamane (1967) จากการคำนวณโดยการกำหนดความผิดพลาดที่ยอมรับได้ (กำหนด 0.075)

$$n = \frac{N}{(1 + NE^2)} \quad (3.4)$$

โดย

n คือ จำนวนกลุ่มตัวอย่าง

N คือจำนวนประชากรที่ใช้ในการศึกษา

E คือ ความผิดพลาดที่ยอมรับได้

เมื่อนำมาคำนวณ

$$n = 483 / (483 / (1 + (483 * (0.075)^2)))$$

$$n = 129.95$$

โดยออกแบบชุดคำถามตามแบบจำลองการยอมรับเทคโนโลยี (Technology Acceptance Model: TAM) ซึ่งในงานวิจัยนี้แบ่งออกเป็น 6 ด้าน ได้แก่ 1) ด้านการรับรู้ประโยชน์ (Perceived Usefulness: PU) จำนวน 4 ข้อ 2) ด้านการรับรู้ความง่ายในการใช้งาน (Perceived Ease of Use: PEU) จำนวน 6 ข้อ และ 3) การรับรู้ด้านความเชื่อมั่นและความปลอดภัย (Trust and Security: TS) จำนวน 5 ข้อ 4) การรับรู้ด้านทัศนคติในการใช้งาน จำนวน 4 ข้อ 5) การรับรู้ด้านพฤติกรรมการความตั้งใจที่จะงาน จำนวน 3 ข้อ 6) ด้านการรับรู้ข้อมูลด้านการใช้งานจริง จำนวน 2 ข้อ รวมข้อคำถามทั้งสิ้น จำนวน 24 ข้อ โดยแต่ละข้อของคำถามเป็นการเรียงลำดับตามมาตรวัดของลิเคิร์ท (Likert Scale) โดยเริ่มจากน้อยไปมาก เช่น 1 คือระดับน้อยที่สุด และ 5 คือระดับมากที่สุด โดยมีชุดคำถามดังนี้

3.8.1.1 การรับรู้ประโยชน์ (PU)

- 1) ท่านคิดว่าการรู้จำใบหน้าเพื่อเข้าสอบมีประโยชน์มากกว่าวิธีการแบบเดิม (บัตรนักเรียน)
- 2) ท่านคิดว่าการรู้จำใบหน้าหลายรูปแบบสำหรับการเข้าสอบมีประโยชน์มากกว่าการรู้จำใบหน้ารูปแบบเดียว
- 3) เทคโนโลยีชีวมิติมีประโยชน์สำหรับการเรียนประจำวันของท่าน
- 4) เทคโนโลยีชีวมิติช่วยให้ท่านเพิ่มประสิทธิภาพในระหว่างชั้นเรียนได้

3.8.1.2 การรับรู้ความง่ายต่อการใช้งาน (PEU)

- 1) ท่านคิดว่าการรู้จำใบหน้าเพื่อเข้าสอบนั้นง่ายกว่าวิธีการแบบเดิม (บัตรนักเรียน)
- 2) ท่านคิดว่าการรู้จำใบหน้าหลายรูปแบบสำหรับการเข้าสอบความง่ายในการใช้งานมากกว่าการรู้จำใบหน้ารูปแบบเดียว
- 3) เทคโนโลยีชีวมิติง่ายต่อการใช้งาน
- 4) เหตุผลหนึ่งที่ระบบนี้มีประโยชน์ก็เพราะการใช้งานง่าย
- 5) การรับรู้ที่มีต่อระบบชีวมิติของนักเรียนนั้นง่ายกว่าในการตรวจสอบวิธีการแบบดั้งเดิม
- 6) การรู้จำด้วยเทคโนโลยีชีวมิติไม่ต้องใช้ความพยายามมากนักในการระบุตัวเอง

3.8.1.3 การรับรู้ด้านความเชื่อมั่นและความปลอดภัย (TS)

- 1) ท่านคิดว่าการรู้จำด้วยเทคโนโลยีชีวมิติจะเป็นการรุกรานทางกายภาพ
- 2) ท่านจะเชื่อมั่นในระบบจดจำด้วยชีวมิติ
- 3) การระบุตัวนักเรียนโดยใช้การรู้จำชีวมิตินั้นเชื่อถือได้
- 4) การระบุตัวตนโดยใช้การรู้จำชีวมิติสามารถระบุตัวท่านได้อย่างถูกต้อง
- 5) การระบุตัวตนโดยใช้การรู้จำชีวมิติมีความแม่นยำสูง

3.8.1.4 การรับรู้ด้านทัศนคติในการใช้งาน

- 1) ท่านรู้สึกว่าการใช้ชีวมิติดีกว่าที่คาดไว้
- 2) ความคาดหวังส่วนใหญ่ของท่านในการใช้ระบบจดจำใบหน้าได้รับ
- 3) ท่านรู้สึกใช้เทคโนโลยีชีวมิติในการเรียนของท่านเป็นส่วนใหญ่
- 4) ท่านสามารถเชื่อมั่นในการรู้จำโดยใช้เทคโนโลยีชีวมิติเนื่องจากมีความแม่นยำสูง

3.8.1.5 การรับรู้ด้านด้านพฤติกรรมความตั้งใจที่จะงาน

- 1) ท่านชอบการรู้จำด้วยเทคโนโลยีชีวมิติสำหรับการเข้าสอบมากกว่าวิธีดั้งเดิม

2) ท่านจะใช้การรู้จำใบหน้าด้วยเทคโนโลยีชีวมิติเมื่อมีการเข้าสอบ

3) ท่านหวังว่าจะสามารถนำเทคโนโลยีชีวมิติมาประยุกต์ใช้ใน

มหาวิทยาลัยโดยเร็ว

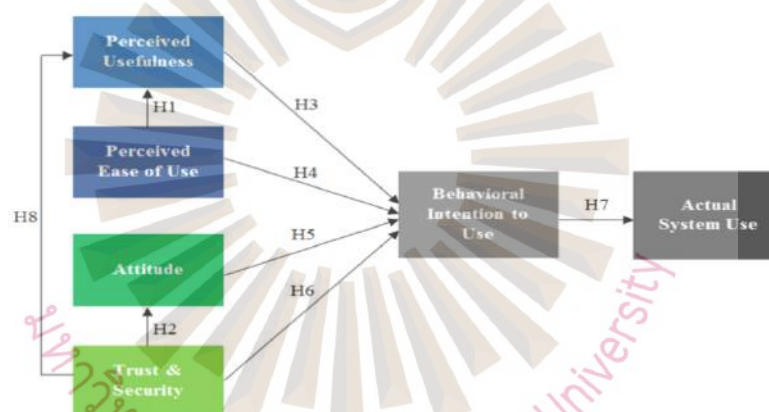
3.8.1.6 การรับรู้ด้านข้อมูลด้านการใช้งานจริง

1) ท่านจะใช้ระบบจดจำใบหน้าในการเข้าสอบ

2) ท่านอยากจะแนะนำให้มหาวิทยาลัยของท่านใช้ระบบจดจำใบหน้าเพื่อ

ยืนยันตัวนักเรียนในพื้นที่ตรวจสอบสิทธิ์ทั้งหมด

ในส่วนของการวิจัยด้านการยอมรับระบบตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติมีการออกแบบการวิจัยดังแสดงในรูปที่ 3.12



รูปที่ 3.12 แสดงกรอบแนวคิดในการวิจัยด้านการยอมรับระบบตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติ

ที่มา: Rukhiran, Wong-In, & Netinant , 2022

3.8.2 สมมติฐาน

1) สมมติฐานข้อที่ 1 (Hypothesis 1: H1) ความง่ายในการใช้งานที่รับรู้มีผลในเชิงบวกต่อการรับรู้ถึงประโยชน์

2) สมมติฐานข้อที่ 2 (Hypothesis 2: H2) ความไว้วางใจและความปลอดภัยมีผลดีต่อทัศนคติ

3) สมมติฐานข้อที่ 3 (Hypothesis 3: H3) การรับรู้ถึงประโยชน์มีผลดีต่อพฤติกรรมความตั้งใจที่จะใช้

4) สมมติฐานข้อที่ 4 (Hypothesis 4: H4) การรับรู้ว่าใช้งานง่ายมีผลดีต่อพฤติกรรมความตั้งใจที่จะใช้

5) สมมติฐานข้อที่ 5 (Hypothesis 5: H5) ทักษะดิจิทัลมีผลดีต่อพฤติกรรมความตั้งใจที่จะใช้

6) สมมติฐานข้อที่ 6 (Hypothesis 6: H6) ความไว้วางใจและความปลอดภัยส่งผลดีต่อพฤติกรรมการใช้งาน

7) สมมติฐานข้อที่ 7 (Hypothesis 7: H7) ความตั้งใจเชิงพฤติกรรมที่จะใช้มีผลดีต่อความเป็นจริง

3.9 สถิติที่ใช้ในงานวิจัย

การนำข้อมูลเข้ารวมถึงการประมวลผลข้อมูลในงานวิจัยนี้ได้ใช้โปรแกรมสำเร็จรูปเอสพีเอสเอส (SPSS) ในการดำเนินการ ดังนี้

3.9.1 สถิติพรรณนา (Descriptive Statistical)

เป็นการวิเคราะห์ข้อมูลที่ได้รับจากการสำรวจหรือการเก็บรวบรวมข้อมูล โดยเป็นการใช้เครื่องมือทางสถิติในการวิเคราะห์ข้อมูลเพื่อหาแนวโน้ม ความสัมพันธ์ ความสัมพันธ์ของตัวแปร และจุดมุ่งหมายอื่นๆ ในงานวิจัยนี้ ได้ใช้ค่าสถิติพรรณนา คือ ค่าเฉลี่ย (Mean) ค่าสูงสุด (Max) ค่าต่ำสุด (Min) และส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation)

3.9.2 การวิเคราะห์องค์ประกอบเชิงยืนยัน (Confirmatory Factor Analysis: CFA)

การวิเคราะห์ปัจจัยยืนยัน (Confirmatory Factor Analysis: CFA) เป็นวิธีการทางสถิติที่ใช้ในการทดสอบระดับที่โมเดลทางคณิตศาสตร์ที่เรามีอยู่แล้วสามารถอธิบายข้อมูลที่มีอยู่ได้ดีแค่ไหน โดยเฉพาะอย่างยิ่งในสถิติที่เกี่ยวข้องกับการวัดทางจิตวิทยา โดยทั่วไป CFA มักจะใช้กับข้อมูลที่มีความซับซ้อน เช่น ข้อมูลที่มีหลายมิติ หรือข้อมูลที่มีหลายตัวแปร โดยมีวัตถุประสงค์เพื่อที่จะประเมินว่าแบบจำลองการวัดมีความเหมาะสมกับสมมติฐานเหล่านั้นมากหรือน้อยเพียงใด CFA เป็นส่วนหนึ่งของโมเดลสมการโครงสร้าง (Structural Equation Modeling: SEM) ซึ่งใช้ใน

การทดสอบสมมติฐานเกี่ยวกับความสัมพันธ์ระหว่างตัวแปร ซึ่งแตกต่างจากการวิเคราะห์ปัจจัยสำรวจ (Exploratory Factor Analysis: EFA) ซึ่งใช้ในการค้นพบโครงสร้างที่อยู่ในข้อมูล โดย CFA จะใช้ในการยืนยันหรือปฏิเสธทฤษฎีหรือแบบจำลองที่มีอยู่ก่อนแล้ว การวิเคราะห์ปัจจัยยืนยัน (CFA) สามารถนำไปใช้ในหลายสาขาวิชา เช่น สังคมศาสตร์ และพฤติกรรมศาสตร์ เพื่อทดสอบความสอดคล้องของตัวบ่งชี้ทางจิตวิทยา นอกจากนี้ CFA ยังสามารถนำไปใช้ในการวิเคราะห์ข้อมูลในสาขาอื่นๆ เช่น การตลาดและเศรษฐศาสตร์ เพื่อทดสอบความสอดคล้องของเครื่องมือวัด หรือการประเมินโครงสร้างข้อมูลที่ซับซ้อน สำหรับการวิเคราะห์ปัจจัยยืนยัน นักวิจัยจำเป็นต้องมีความเข้าใจในหลักการและเทคนิคทางสถิติ และมีความชำนาญในการใช้ซอฟต์แวร์ทางสถิติ เพื่อเลือกเทคนิคที่เหมาะสมและปรับแก้ปัญหาในกรณีที่โมเดลไม่สอดคล้องกับแบบจำลอง นอกจากนี้ การตีความผลและการใช้ผลการวิเคราะห์ให้เหมาะสมกับวัตถุประสงค์ของการวิเคราะห์เป็นสิ่งสำคัญอีกด้วย

3.9.3 การวิเคราะห์ค่า CR และ AVE

การวิเคราะห์ค่า CR (Composite Reliability) และ AVE (Average Variance Extracted) เป็นการวิเคราะห์ความเชื่อถือและความถูกต้องของแบบจำลองการวัดที่ได้รับการสมมติในการวิเคราะห์ปัจจัยยืนยัน (Confirmatory Factor Analysis: CFA) โดยพารามิเตอร์ทั้งสองนี้มีความสำคัญในการประเมินคุณภาพของแบบจำลองการวัด โดยมีความหมายดังนี้

3.9.3.1 ค่า CR (Composite Reliability) หมายถึง ค่าเชื่อถือแบบส่วนประกอบ ซึ่งเป็นการวัดระดับความเชื่อถือของแต่ละตัวบ่งชี้ (Indicator) โดยเทคนิคการวิเคราะห์สำหรับคำนวณค่า CR คือ alpha reliability และ Dillon-Goldstein's rho โดยค่า CR จะเป็นไปในช่วง 0-1 และค่า CR ที่มีค่ามากกว่าหรือเท่ากับ 0.70 จะถือว่ามีความเชื่อถือสูง

3.9.3.2 ค่า AVE (Average Variance Extracted) หมายถึง ค่าความถูกต้องของการวัดที่วัดได้จากตัวบ่งชี้แต่ละตัว ซึ่งเป็นการวัดว่าตัวบ่งชี้แต่ละตัววัดอย่างไร โดยค่า AVE จะเป็นไปในช่วง 0-1 และค่า AVE ที่มีค่ามากกว่าหรือเท่ากับ 0.50 จะถือว่ามีความถูกต้องสูง

การวิเคราะห์ค่า CR และ AVE เป็นการวิเคราะห์สถิติที่สำคัญในการตรวจสอบคุณภาพของแบบจำลองการวัดใน CFA โดยค่า CR และ AVE ที่มีค่าสูงแสดงว่าแบบจำลองการวัดมีความเชื่อถือสูงและมีความถูกต้องในการวัด ส่วนค่า CR ที่ต่ำกว่า 0.70 และค่า AVE ที่ต่ำกว่า 0.50

อาจแสดงให้เห็นว่าแบบจำลองการวัดไม่สามารถอธิบายข้อมูลได้อย่างถูกต้องหรือมีความเชื่อถือต่ำ ซึ่งอาจจะเกิดจากการใช้ตัวบ่งชี้ที่ไม่เหมาะสม หรือโครงสร้างของแบบจำลองการวัดไม่เหมาะสมกับข้อมูลที่มีอยู่จริง การวิเคราะห์ค่า CR และ AVE นั้นมีความสำคัญในการตรวจสอบความเหมาะสมของแบบจำลองการวัด แต่ไม่สามารถใช้เพียงค่าเดียวเพื่อวิเคราะห์คุณภาพของแบบจำลองการวัดได้ ในการวิเคราะห์แบบจำลองการวัดจะต้องรวมถึงการวิเคราะห์อื่น ๆ เช่น การตรวจสอบค่าชี้วัดการแตกต่าง (Discriminant Validity) เพื่อตรวจสอบว่าตัวบ่งชี้ที่ต่างกันสามารถแยกแยะตัวแปรที่ต้องการตรวจสอบได้ หรือการวิเคราะห์การปรับแก้แบบจำลอง (Model Fit) เพื่อตรวจสอบว่าแบบจำลองการวัดเหมาะสมกับข้อมูลหรือไม่ (Fornell & Larcker, 1981)



บทที่ 4

ผลการวิเคราะห์ข้อมูล

4.1 ผลการประเมินประสิทธิภาพของระบบ

ผลจากการทดลองเพื่อเปรียบเทียบประสิทธิภาพของระบบตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติในรูปแบบที่ต่าง ๆ กันจำนวน 8 กลุ่ม กลุ่มที่ 1 (ตรวจจับบัตรประจำตัวนักเรียน), กลุ่มที่ 2 (ตรวจจับใบหน้าเท่านั้น), กลุ่มที่ 3 (ตรวจจับลายพิมพ์นิ้วมือเท่านั้น), กลุ่มที่ 4 (ตรวจจับใบหน้าและลายพิมพ์นิ้วมือ), กลุ่มที่ 5 (ใช้การรู้จำใบหน้าด้วยกล้องสองตัวในการตรวจจับ) กลุ่มที่ 6 (ใช้ลายพิมพ์นิ้วมือที่มีการตรวจจับด้วยเครื่องสแกนสองเครื่อง) กลุ่มที่ 7 (การตรวจจับใบหน้าเป็นตัวหลักและลายพิมพ์นิ้วมือเป็นตัวเสริม), และกลุ่มที่ 8 (การตรวจจับลายพิมพ์นิ้วมือเป็นตัวหลักและใบหน้าเป็นตัวเสริม) ผลลัพธ์แบ่งออกเป็นสี่ด้าน ดังแสดงในตารางที่ 4.1

ตารางที่ 4.1 แสดงผลการทดสอบการใช้งานของระบบตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติ

เกณฑ์ ประเมิน	1. บัตร นักเรียน	2. ใบหน้า	3. ลาย พิมพ์นิ้ว มือ	4. ใบหน้า +ลาย พิมพ์นิ้ว มือ	5. ใบหน้า 2 กล้อง	6. ลาย พิมพ์นิ้ว มือ 2 เครื่อง	7. ใบหน้า แล้วลาย พิมพ์นิ้ว มือ	8. ลาย พิมพ์นิ้ว มือแล้ว ใบหน้า
Accuracy	66.67%	86.78%	86.67%	93.33%	90.00%	96.67%	93.33%	93.33%
Error Rate	21.29%	11.28%	3.49%	2.76%	4.83%	1.82%	2.35%	1.94%
Time (sec.)	14.01	2.49	4.69	6.54	2.76	9.81	6.69	6.77
Sensor cost (USD)	-	\$40	\$55	\$95	\$80	\$110	\$95	\$95
Estimate cost (USD)	\$34.29	\$4.56	\$4.65	\$4.89	\$4.80	\$4.98	\$4.89	\$4.89

ที่มา: Rukhiran et al., 2023

จากตารางที่ 4.1 พบว่า ทางด้านความแม่นยำ กลุ่มที่ 6 มีอัตราความแม่นยำสูงสุดด้วยคะแนนร้อยละ 96.67 ขณะที่กลุ่มที่ 1 มีความแม่นยำน้อยที่สุดด้วยคะแนนร้อยละ 66.67 ด้านอัตราข้อผิดพลาด กลุ่มที่ 1 มีอัตราข้อผิดพลาดสูงสุด ที่ร้อยละ 21.29 ในขณะที่ กลุ่มที่ 6 มีอัตราความผิดพลาดน้อยที่สุดร้อยละ 1.82 ด้านเวลาที่ใช้ในการประมวลผล กลุ่มที่ 6 ใช้เวลาในการประมวลผลมากที่สุด 9.81 วินาที กลุ่มที่ 2 ใช้เวลาในการประมวลผลน้อยที่สุดด้วยเวลา 2.49 วินาที ในด้านค่าใช้จ่ายกลุ่มที่ 1 มีค่าใช้จ่ายรวมของระบบมากที่สุด \$34.29 หรือประมาณ 1,200 บาท กลุ่มที่ 2 มีค่าใช้จ่ายรวมของระบบน้อยที่สุด \$4.56 หรือประมาณ 3,400 บาท ในขณะที่กลุ่มที่ 1 มีค่าใช้จ่ายน้อยที่สุด 34.29 U.S. Dollar หรือประมาณ 160 บาทไทย ในส่วนของการคำนวณค่าใช้จ่ายรวมของระบบ เป็นการคิดค่าใช้จ่ายทั้งหมด ได้แก่ ค่าอุปกรณ์ IoT ค่าจ้างกรรมการคุมสอบ และค่าอุปกรณ์ Sensor โดยทำการคิดเป็นราคาเฉลี่ยต่อการใช้งาน (เวลาที่ใช้ในการสอบโดยเฉลี่ย 3 ชั่วโมง) โดยมีตัวอย่างการคำนวณ ดังนี้ ในกลุ่มที่ 2 ใช้ใบหน้าในการตรวจสอบ มีค่าอุปกรณ์ IoT ดังแสดงในตารางที่ 4.2 ซึ่งมีค่าใช้จ่ายรวม \$720 รวมกับกล้องจำนวน 1 กล้อง ราคา \$40 รวมเป็นราคาอุปกรณ์พร้อมกล้อง \$760 โดยมีอายุการใช้งาน 500 ชั่วโมง ดังนั้นค่าใช้จ่ายรวมของระบบในการใช้กล้อง 1 กล้อง คือ $\$4.56 ((\$760 / 500 \text{ ชั่วโมง}) * 3 \text{ ชั่วโมงในการสอบ})$

เพื่อทำการปรับเปลี่ยนข้อมูลเพื่อเปรียบเทียบคะแนนของแต่ละกลุ่มการทดสอบ ผู้วิจัยได้นำเสนอ Biometric Quality Metric โดยใช้กฎบัญญัติไตรยางศ์เพื่อปรับรูปแบบคะแนนใหม่ในแต่ละด้าน ตัวอย่างเช่น หากค่าสูงสุดของเวลาประมวลผลเฉลี่ยคือกลุ่มที่ 1 โดยมีค่าเฉลี่ย 14.01 วินาที ค่า Biometric Quality Metric จะถูกแปลงเป็น 100 คะแนน จากนั้นจะทำการคำนวณคะแนนของแต่ละกลุ่มโดยเทียบบัญญัติไตรยางศ์ เพื่อจัดอันดับประสิทธิภาพในแต่ละด้านของกลุ่มทดลองทั้ง 8 กลุ่ม

จากนั้นได้ทำการให้คะแนนในการจัดอันดับ (Ranking Score) โดยให้คะแนนที่มีประสิทธิภาพดีที่สุดในแต่ละด้านเป็น 5 คะแนน และอันดับรองลงมาให้คะแนนเป็น 4 คะแนน ในกรณีที่มียุทธวิธีเท่ากันคะแนนอันดับจะให้เท่ากัน ยกตัวอย่างการคิดคะแนนอันดับ เช่น ในด้านความแม่นยำกลุ่มที่ความแม่นยำมากที่สุดได้แก่กลุ่มที่ 6 ดังนั้นจะให้คะแนนอันดับ 5 คะแนน (ค่าคะแนนอันดับจะแสดงในวงเล็บ ต่อจากค่าคะแนน ดังแสดงในตารางที่ 4.2) ในกรณีของราคาและเวลาที่ใช้ในการประมวลผล ยังมีค่าสูงยิ่งแปลว่ามีประสิทธิภาพน้อย ดังนั้นในด้านทั้งสองนั้นจะมีคะแนนอันดับแบบผกผัน กล่าวคือยิ่งมีค่ามากจะยิ่งมีคะแนนอันดับน้อย จากนั้นทำการรวมคะแนนอันดับของแต่ละด้านในแต่ละกลุ่มจะได้เป็น Biometric Quality Metric โดยงานวิจัยนี้

ให้ความสำคัญกับ ความแม่นยำ (Accuracy), อัตราความผิดพลาด (Error Rate) , เวลาที่ใช้ (Time), และ ราคา (Cost) โดยมีน้ำหนักเท่าเทียมกัน ซึ่งในทางปฏิบัติ การคำนวณค่า Biometric Quality Metric จากปัจจัยทั้งสี่จะขึ้นอยู่กับสถานการณ์ที่ใช้ในการพิจารณา

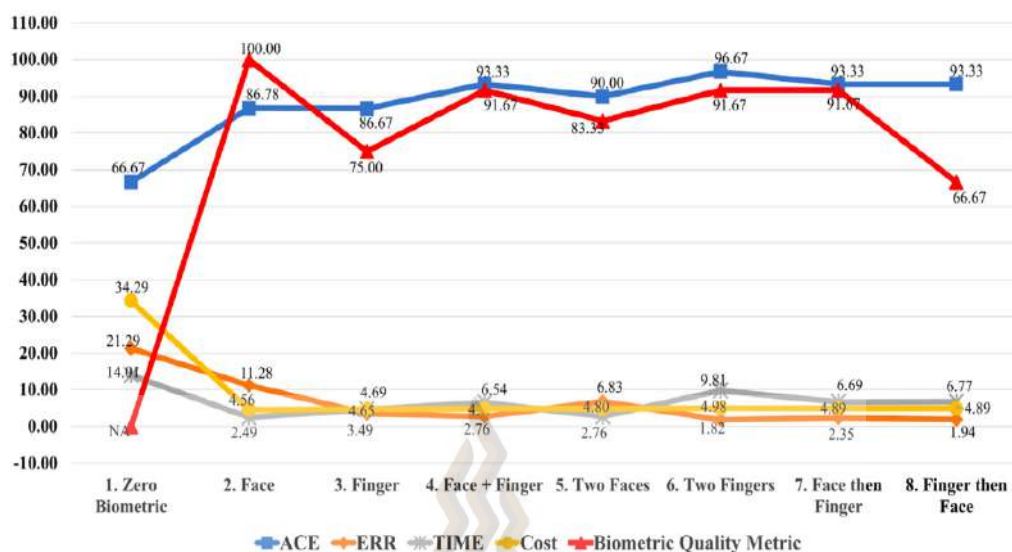
ตารางที่ 4.2 แสดงผลการทดสอบการใช้งานของระบบโดยการเทียบลำดับ

เกณฑ์ ประเมิน	1. บัตร นักเรียน	2. ใบหน้า	3. ลาย พิมพ์นิ้ว มือ	4. ใบหน้า +ลาย พิมพ์นิ้ว มือ	5. ใบหน้า 2 กล้อง	6. ลาย พิมพ์นิ้ว มือ 2 เครื่อง	7. ใบหน้า แล้วลาย พิมพ์นิ้ว มือ	8. ลายพิมพ์นิ้ว มือแล้ว ใบหน้า
Accuracy (%)	68.89	89.76 (2)	89.56 (1)	96.45 (4)	93.10 (3)	100.00 (5)	96.45 (4)	96.45 (4)
Error Rate (%)	100.00	52.97	16.39 (1)	12.97 (2)	32.09	8.55 (5)	11.04 (3)	9.11 (4)
Time (%)	100.00	17.75 (5)	33.46 (3)	46.67 (2)	19.70 (4)	70.04	47.76 (1)	48.31
System Cost (%)	-	91.57 (5)	93.37 (4)	98.19 (2)	96.39 (3)	100.00 (1)	98.19 (2)	98.19 (2)
Total Score	-	12.00	9.00	10.00	10.00	11.00	10.00	10.00
Biometric Quality Metric		100.00	75	83.33	83.33	91.67	83.33	83.33

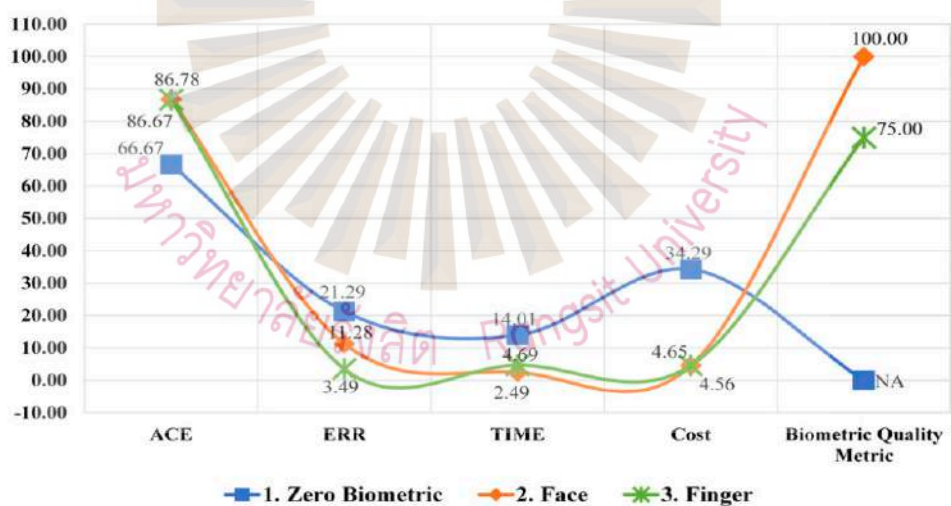
ที่มา: Rukhiran et al., 2023

จากตารางที่ 4.2 กลุ่มที่มี Biometric Quality Metric มากที่สุดได้แก่ กลุ่มที่ 2 โดยมีกลุ่มที่ 6 มีคะแนนเป็นอันดับที่สอง และกลุ่มที่มีคะแนนน้อยที่สุดได้แก่กลุ่มที่ 3

เพื่อให้เห็นการเปรียบเทียบที่ชัดเจนมากยิ่งขึ้นในรูปแบบกราฟแท่งร่วมกับกราฟเส้น โดยกราฟแท่งแสดงข้อมูลประสิทธิภาพของระบบตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติ ในขณะที่กราฟเส้นจะแสดงคะแนนลำดับประสิทธิภาพของระบบตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติของแต่ละกลุ่มทดลอง ดังแสดงในรูปที่ 4.1 – 4.7

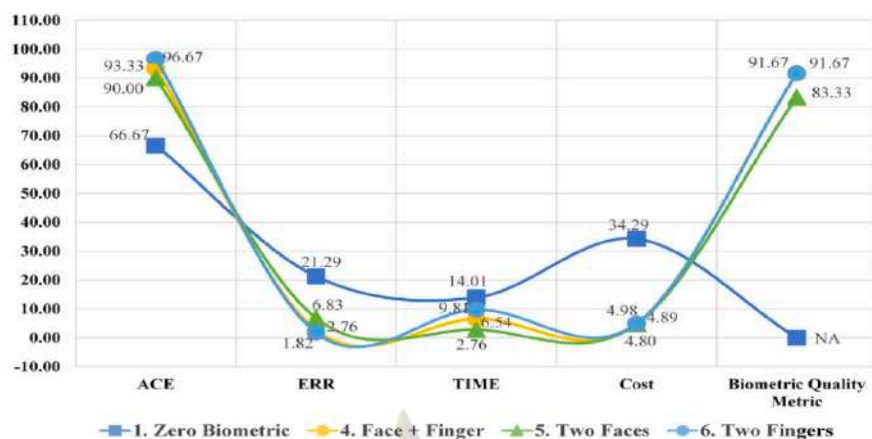


รูปที่ 4.1 แสดงผลการเปรียบเทียบประสิทธิภาพและคะแนน Biometric Quality Metric ของระบบการตรวจสอบผู้เข้าสอบในแต่ละกลุ่ม
ที่มา: Rukhiran et al., 2023



รูปที่ 4.2 แสดงผลการเปรียบเทียบประสิทธิภาพของระบบการตรวจสอบผู้เข้าสอบแบบ Unimodal กับ Zero Biometric
ที่มา: Rukhiran et al., 2023

จากรูปที่ 4.2 แสดงว่าประสิทธิภาพของการใช้ระบบการตรวจสอบผู้เข้าสอบแบบ Unimodal มีประสิทธิภาพเหนือกว่าแบบ Zero Biometric และการใช้การตรวจสอบใบหน้ามีประสิทธิภาพมากกว่าการใช้ลายพิมพ์นิ้วมือ

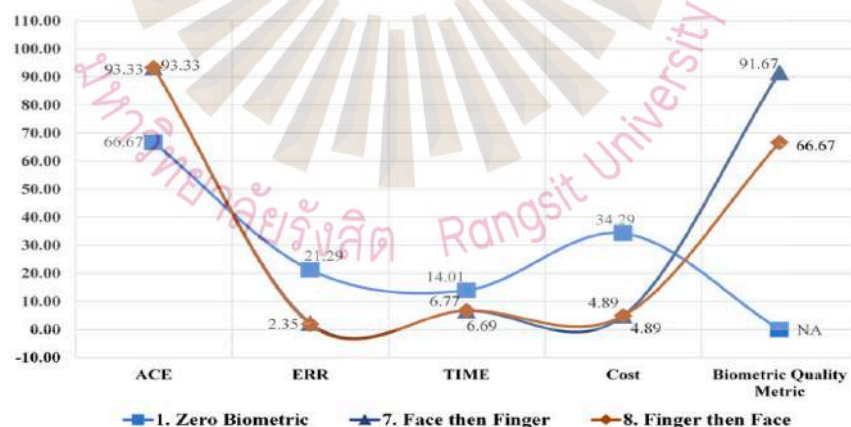


รูปที่ 4.3 แสดงผลการเปรียบเทียบประสิทธิภาพของระบบการตรวจสอบผู้เข้าสอบแบบ

Multimodal กับ Zero Biometric

ที่มา: Rukhiran et al., 2023

จากรูปที่ 4.3 สรุปได้ว่าประสิทธิภาพของระบบการตรวจสอบผู้เข้าสอบแบบ Multimodal มีประสิทธิภาพมากกว่าแบบ Zero Biometric โดยการใช้ลายพิมพ์นิ้วมือ 2 เครื่องและการใช้ใบหน้าพร้อมกับลายพิมพ์นิ้วมือมีประสิทธิภาพมากที่สุดเท่ากัน รองลงมาคือการใช้กล้อง 2 กล้องในการรู้จำใบหน้า

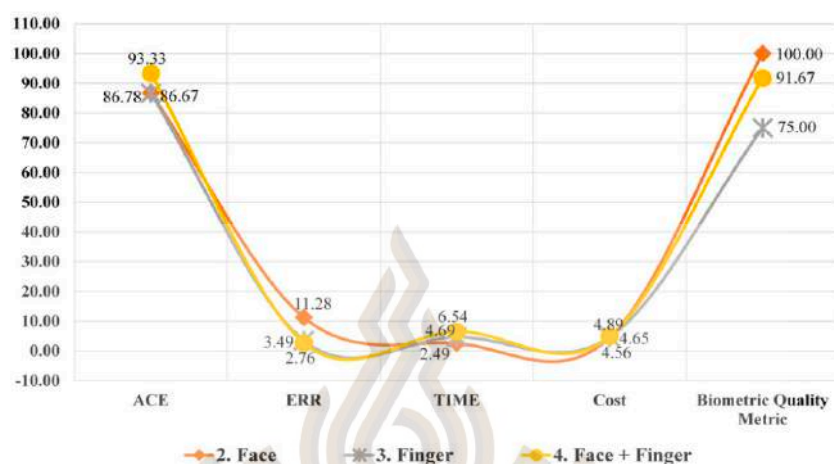


รูปที่ 4.4 แสดงผลการเปรียบเทียบประสิทธิภาพของระบบการตรวจสอบผู้เข้าสอบแบบ Semi-

Multimodal กับ Zero Biometric

ที่มา: Rukhiran et al., 2023

จากรูปที่ 4.4 สรุปได้ว่า ประสิทธิภาพของระบบการตรวจสอบผู้เข้าสอบแบบ Semi-Multimodal มีประสิทธิภาพมากกว่าแบบ Zero Biometric โดยการตรวจสอบโดยใช้ใบหน้าก่อน มีประสิทธิภาพมากกว่าการใช้ลายพิมพ์นิ้วมือในการตรวจสอบก่อน



รูปที่ 4.5 แสดงผลการเปรียบเทียบประสิทธิภาพของระบบการตรวจสอบผู้เข้าสอบแบบ Unimodal กับ Multimodal Biometric (Multiple Modalities)

ที่มา: Rukhiran et al., 2023

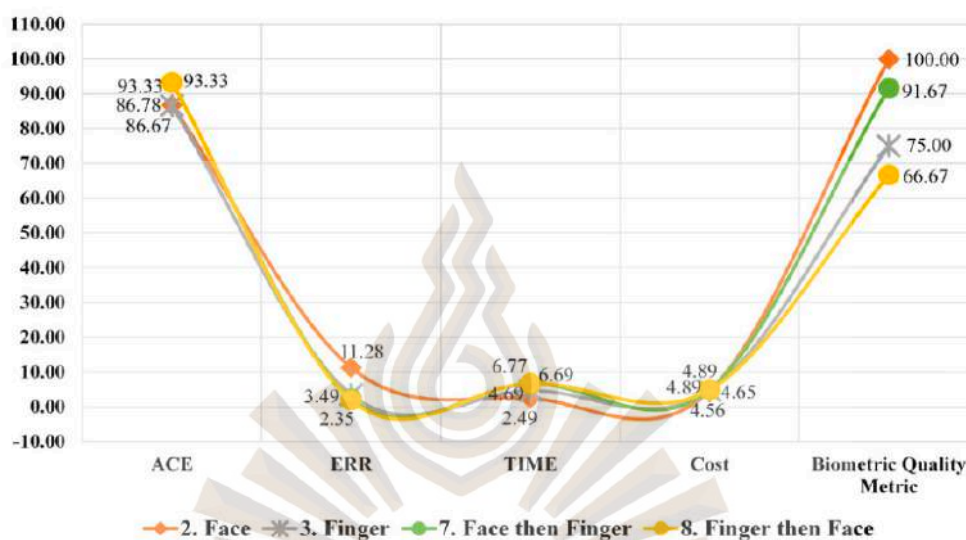
จากรูปที่ 4.5 สรุปได้ว่า ประสิทธิภาพของระบบการตรวจสอบผู้เข้าสอบแบบ Unimodal โดยใช้ใบหน้ามีประสิทธิภาพมากกว่าแบบ Multimodal Biometric (Multiple Modalities) แต่การใช้ลายพิมพ์นิ้วมือนี้อาจมีประสิทธิภาพน้อยกว่าการใช้ลายพิมพ์นิ้วมือกับใบหน้ารวมกัน



รูปที่ 4.6 แสดงผลการเปรียบเทียบประสิทธิภาพของระบบการตรวจสอบผู้เข้าสอบแบบ Unimodal กับ Multimodal Biometric (Multiple Sensors)

ที่มา: Rukhiran et al., 2023

จากรูปที่ 4.6 สรุปได้ว่า ประสิทธิภาพของระบบการตรวจสอบผู้เข้าสอบแบบ Unimodal โดยใช้ใบหน้ามีประสิทธิภาพมากกว่าแบบ Multimodal Biometric (Multiple Sensors) แต่การใช้ลายพิมพ์นิ้วมือนี้อมีประสิทธิภาพน้อยกว่าแบบ Multimodal Biometric (Multiple Sensors)



รูปที่ 4.7 แสดงผลการเปรียบเทียบประสิทธิภาพของระบบการตรวจสอบผู้เข้าสอบแบบ Unimodal กับ Semi-multimodal Biometric
ที่มา: Rukhiran et al., 2023

จากรูปที่ 4.7 สรุปได้ว่า ประสิทธิภาพของระบบการตรวจสอบผู้เข้าสอบแบบ Unimodal โดยใช้ใบหน้า มีประสิทธิภาพมากกว่าแบบ Semi-multimodal Biometric และการใช้ลายพิมพ์นิ้วมือนี้อมีประสิทธิภาพน้อยกว่าแบบ Semi-multimodal Biometric แบบใช้ใบหน้าที่ก่อนลายพิมพ์นิ้วมือ และการใช้ลายพิมพ์นิ้วมือนี้อ่อนใบหน้ามีประสิทธิภาพน้อยที่สุด

4.2 ผลการประเมินการยอมรับการใช้งานระบบตรวจสอบบุคคลเข้าสอบโดยใช้เทคโนโลยีชีวมิติ

ในการประเมินการยอมรับการใช้งานระบบตรวจสอบบุคคลเข้าสอบโดยใช้เทคโนโลยีชีวมิติ โดยใช้แบบสอบถามจำนวน 161 ชุด ได้ผลลัพธ์ ดังนี้

4.2.1 สถิติพรรณนา

ตารางที่ 4.3 แสดงข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

	คำอธิบาย	จำนวน	ร้อยละ
เพศ	ชาย	92	57.10
	หญิง	69	42.90
อายุ	18	107	66.50
	19	54	33.50
ระดับการศึกษา	ปริญญาตรี	161	100.00

ที่มา: Rukhiran et al., 2022

ตารางที่ 4.3 แสดงข้อมูลผู้ตอบแบบสอบถามในงานวิจัยนี้ โดยข้อมูลจากการประเมินด้วยแบบสอบถามจำนวน 161 ชุด พบว่า ผู้ตอบแบบสอบถามเป็นเพศชายเป็นผู้เข้าร่วมส่วนใหญ่ (ร้อยละ 57.10) อายุ 19 ปี (ร้อยละ 33.50)

ตารางที่ 4.4 แสดงผลการประเมินเชิงตัวเลขสำหรับแต่ละตัวแปรด้านการสำรวจ

โครงสร้าง	ชุดคำถาม	Mean	SD
การรับรู้ประโยชน์ (PU) (Davis, 1989; Rukhiran, Netinant, & Elrad, 2020; Song, 2021)	PU1: ท่านคิดว่าการรู้จำใบหน้าเพื่อเข้าสอบมีประโยชน์มากกว่าวิธีการแบบเดิม (บัตรนักเรียน)	2.84	0.766
	PU2: ท่านคิดว่าการรู้จำใบหน้าหลายรูปแบบสำหรับการเข้าสอบมีประโยชน์มากกว่าการรู้จำใบหน้ารูปแบบเดียว	3.19	0.818
	PU3. เทคโนโลยีชีวมิติมีประโยชน์สำหรับการเรียนประจำวันของท่าน	2.85	0.823
	PU4. เทคโนโลยีชีวมิติช่วยให้ท่านเพิ่มประสิทธิภาพในระหว่างชั้นเรียนได้	2.94	0.834

ตารางที่ 4.4 แสดงผลการประเมินเชิงตัวเลขสำหรับแต่ละตัวแปรด้านการสำรวจ (ต่อ)

โครงสร้าง	ชุดคำถาม	Mean	SD
การรับรู้ความ ง่ายต่อการใช้งาน (PEU) (Acosta-Medina, Torres-Barreto, & Cárdenas- Parga, 2021; Davis, 1989)	PEU1: ท่านคิดว่าการรู้จำใบหน้าเพื่อเข้าสอบนั้นง่ายกว่า วิธีการแบบเดิม (บัตรนักเรียน)	2.85	0.654
	PEU2: ท่านคิดว่าการรู้จำใบหน้าหลายรูปแบบสำหรับการ เข้าสอบความง่ายในการใช้งานมากกว่าการรู้จำใบหน้า รูปแบบเดียว	3.1	0.714
	PEU3: เทคโนโลยีชีวมิติช่วยต่อการใช้งาน	2.80	0.614
	PEU4: เหตุผลหนึ่งที่ระบบนี้มีประโยชน์ก็เพราะใช้งานง่าย	2.87	0.603
	PEU5: การรับรู้ที่มีต่อระบบชีวมิติของนักเรียนนั้นง่ายกว่า ในการตรวจสอบวิธีการแบบดั้งเดิม	2.92	0.642
	PEU6: การรู้จำด้วยเทคโนโลยีชีวมิติไม่ต้องใช้ความ พยายามมากนักในการระบุตัวเอง	2.74	0.657
การรับรู้ด้าน ความเชื่อมั่นและ ความปลอดภัย (TS) (Hassanein & Head, 2007; Wang, 2021)	TS1: ท่านคิดว่าการรู้จำด้วยเทคโนโลยีชีวมิติจะเป็นการ รุกรานทางกายภาพ	4.01	0.680
	TS2: ท่านเชื่อมั่นในระบบจดจำใบหน้า	4.01	0.652
	TS3: การระบุตัวนักเรียนโดยใช้การรู้จำชีวมิตินั้นเชื่อถือได้	4.04	0.660
	TS4: การระบุตัวตนโดยใช้การรู้จำชีวมิติสามารถระบุตัว ท่านได้อย่างถูกต้อง	3.99	0.707
	TS5: การระบุตัวตนโดยใช้การรู้จำชีวมิติมีความแม่นยำสูง	3.96	0.660
ทัศนคติในการ ใช้งาน (ATT) (Ajzen & Fishbein, 1980)	ATT1: ท่านรู้สึกว่าการรู้จำชีวมิติดีกว่าที่ฉันคาดไว้	3.89	0.707
	ATT2: ความคาดหวังส่วนใหญ่ของท่านในการใช้ระบบ จดจำใบหน้าได้รับการยืนยันแล้ว	3.89	0.689
	ATT3: ท่านรู้สึกใช้เทคโนโลยีชีวมิติในการเรียนของท่าน เป็นส่วนใหญ่	3.74	0.712
	ATT4: ท่านสามารถเชื่อมั่นในการรู้จำโดยใช้เทคโนโลยีชีว มิติเนื่องจากมีความแม่นยำสูง	3.77	0.700

ตารางที่ 4.4 แสดงผลการประเมินเชิงตัวเลขสำหรับแต่ละตัวแปรด้านการสำรวจ (ต่อ)

โครงสร้าง	ชุดคำถาม	Mean	SD
ด้านพฤติกรรม ความตั้งใจที่จะ งาน (BIU) (Ajzen & Fishbein, 1980; Ngugi, Kamis, & Tremaine, 2011)	BIU1: ท่านชอบการรู้จำด้วยเทคโนโลยีชีวมิติ สำหรับการเข้าสอบมากกว่าวิธีดั้งเดิม	3.20	0.593
	BIU2: ท่านจะใช้การรู้จำใบหน้าด้วยเทคโนโลยีชีว มิติเมื่อมีการเข้าสอบ	3.59	0.586
	BIU3: ท่านหวังว่าจะสามารถนำเทคโนโลยีชีวมิติมา ประยุกต์ใช้ในมหาวิทยาลัยโดยเร็ว	3.52	0.571
ข้อมูลด้านการใช้ งานจริง (ASU) (Norfolk & O'Regan, 2021)	ASU1: ท่านจะใช้ระบบจดจำใบหน้าในการเข้าสอบ	3.70	0.537
	ASU2: ท่านอยากจะแนะนำให้มหาวิทยาลัยของท่าน ใช้ระบบจดจำใบหน้าเพื่อยืนยันตัวตนนักเรียนในพื้นที่ ตรวจสอบสิทธิ์ทั้งหมด	3.78	0.559

ที่มา: Rukhiran et al., 2022

ผลการประเมินเชิงตัวเลขสำหรับแต่ละตัวแปรด้านการสำรวจแสดงในตารางที่ 4.4 ในทุกด้าน ตัวแปรสามตัวที่มีคะแนนเฉลี่ยสูงสุด (ตามลำดับ) คือ การระบุตัวนักเรียนโดยใช้การรู้จำชีวมิตินั้นเชื่อถือได้ (4.04) การรู้จำด้วยชีวมิติจะรุกรานทางกายภาพ และ ท่านจะเชื่อมั่นในระบบจดจำด้วยชีวมิติ มีคะแนนเฉลี่ยสูงเท่ากัน (4.01) ในทางกลับกัน ตัวแปรที่มีคะแนนเฉลี่ยต่ำสุด (ตามลำดับ) คือ การรับรู้ที่มีต่อระบบชีวมิติของนักเรียนนั้นง่ายกว่าในการตรวจสอบวิธีการแบบดั้งเดิม (2.74), เทคโนโลยีชีวมิติง่ายต่อการใช้งาน (2.80) และ ท่านคิดว่าการรู้จำใบหน้าเพื่อเข้าสอบมีประโยชน์มากกว่าวิธีการแบบเดิม (บัณฑิตนักเรียน) (2.84)

4.2.2 การทดสอบความน่าเชื่อถือ (Reliability Test)

ใช้เทคนิค Confirmatory Factor Analysis (CFA) เพื่อตรวจสอบความเชื่อถือได้ของการทดสอบความน่าเชื่อถือ โดย Hair, Black, Babin, and Anderson (2013) ได้นิยามความถูกต้องของแบบจำลองการวัดความสัมพันธ์ (Construct Validity) ว่าเป็นการวัดความสัมพันธ์ระหว่างตัวแปรที่สัมพันธ์กันได้อย่างถูกต้องตามทฤษฎีที่กำหนดไว้ นอกจากนี้ยังประเมินความสอดคล้องและความแตกต่างของตัวแปรตามเกณฑ์ที่กำหนดไว้ ผลการวิเคราะห์ยืนยันได้ทั้งหมด

24 รายการ และไม่มีรายการใดถูกลบออก เนื่องจากค่า Standardized Item Loading มีค่ามากกว่า 0.5 เช่นเดียวกับคำแนะนำของ Bagozzi and Yi (1964) นอกจากนี้ Factor Loadings มีค่ามากกว่า 0.50 และอยู่ในช่วง 0.622 ถึง 0.959 ซึ่งแสดงให้เห็นถึงความน่าเชื่อถือได้สูง นอกจากนี้ ได้ประเมินความน่าเชื่อถือของเครื่องมือวัดด้วยการวัดความเชื่อมั่น ความสอดคล้อง และความถูกต้อง ตามคำแนะนำค่าความน่าเชื่อถือรวม (Composite Reliability: CR) มีค่ามากกว่า 0.70 และอยู่ระหว่าง 0.823 ถึง 0.937 และ ค่า Average Extracted Variance (AVE) มีค่ามากกว่า 0.50 และอยู่ระหว่าง 0.520 ถึง 0.881 ซึ่งแสดงให้เห็นถึงความเชื่อถือได้สูง นอกจากนี้ค่า Alpha Coefficient ของ Cronbach มีค่ามากกว่า 0.70 และอยู่ระหว่าง 0.801 ถึง 0.934 ตามที่ Cronbach (1951) แนะนำ ดังเช่นที่แสดงในตาราง 4.5 ผลการวิเคราะห์ทั้งหมดและค่าเกณฑ์ที่แนะนำแสดงให้เห็นถึงการยอมรับความสอดคล้องกัน (Convergent Validity Acceptance) ($CR > 0.70$ และ $AVE > 0.50$)

ตารางที่ 4.5 แสดงผลลัพธ์ความถูกต้องความตรงผู้สมบูรณ์ (Convergent validity)

โครงสร้าง	รายการ	Factor loadings	CR	AVE	Cronbach's Alpha
		> 0.50	> 0.70	> 0.50	> 0.70
Perceived	PU1	0.799	0.850	0.589	0.846
Usefulness	PU2	0.915			
(PU)	PU3	0.818			
	PU4	0.759			
Perceived Ease	PEU1	0.622	0.864	0.520	0.859
of Use (PEU)	PEU2	0.750			
	PEU3	0.856			
	PEU4	0.781			
	PEU5	0.800			
	PEU6	0.789			
Trust &	TS1	0.790	0.932	0.735	0.932
Security (TS)	TS2	0.869			
	TS3	0.959			
	TS4	0.913			
	TS5	0.861			

ตารางที่ 4.5 แสดงผลลัพธ์ความถูกต้องความตรงสู่สมบูรณ์ (Convergent validity) (ต่อ)

โครงสร้าง	รายการ	Factor loadings > 0.50	CR > 0.70	AVE > 0.50	Cronbach's Alpha > 0.70
Attitude (ATT)	ATT1	0.853	0.902	0.699	0.903
	ATT2	0.888			
	ATT3	0.892			
	ATT4	0.828			
Behavioral	BIU1	0.679	0.823	0.623	0.801
Intention to	BIU2	0.900			
Use (BIU)	BIU3	0.925			
Actual System	ASU1	0.954	0.937	0.881	0.934
Use (ASU)	ASU2	0.946			

ที่มา: Rukhiran et al., 2022

การตรวจสอบการแยกแยะความถูกต้อง (Discriminant Validity) นี้สามารถแยกได้อย่างถูกต้อง เนื่องจากค่ารากที่สองของแต่ละโครงสร้างมีค่านัยสำคัญมากกว่าค่าสหสัมพันธ์ระหว่างโครงสร้างอื่น ๆ ซึ่งแสดงในตารางที่ 4.6 ดังนั้น ทุกโครงสร้างจึงได้รับการทดสอบความเชื่อมั่นและความถูกต้องและพบว่ามีความมีระดับมีนัยสำคัญ

ตารางที่ 4.6 แสดงผลลัพธ์การแยกแยะความถูกต้องของโครงสร้าง (Discriminant Validity)

โครงสร้าง	PU	PEU	TS	AT	BIU	ASU
PU	0.767					
PEU	-0.269**	0.721				
TS	0.280**	-0.059	0.858			
ATT	0.160†	-0.108	0.480***	0.836		
BIU	0.224*	-0.165†	0.175*	0.114	0.789	
ASU	0.042	-0.008	0.051	0.108	0.220*	0.939

† $p < 0.100$, * $p < 0.050$, ** $p < 0.010$, *** $p < 0.001$

ที่มา: Rukhiran et al., 2022

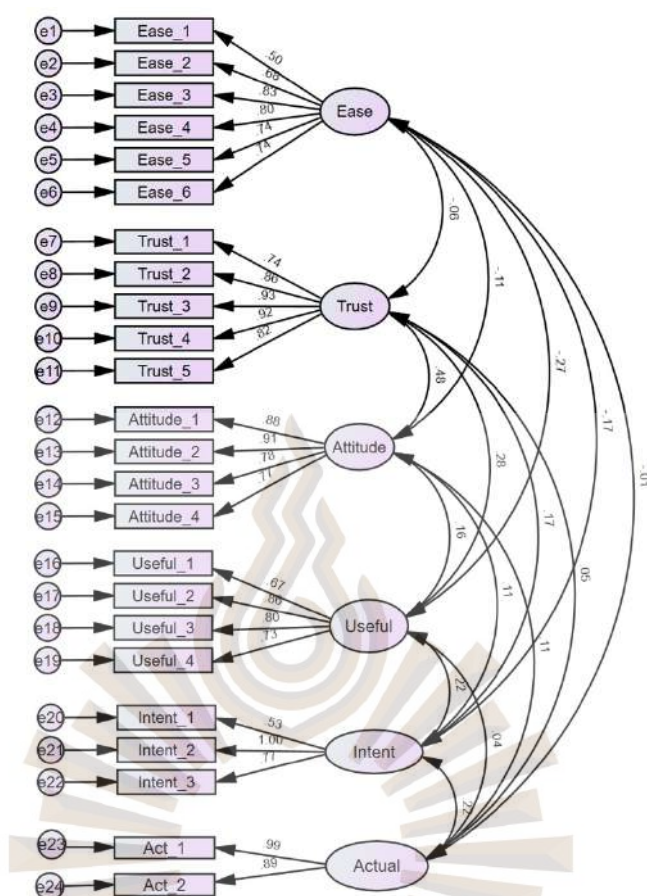
4.2.3 ผลการวิเคราะห์แบบจำลองในการวัด (Measurement Model Testing)

จากรูปที่ 4.8 แบบจำลองการวัดยืนยันว่าทั้ง 6 โครงสร้าง ได้แก่ PU, PEU, TS, ATT, BIU และ ASU เป็นตัวปัจจัยหลักในการศึกษาที่ได้รับการตรวจสอบด้วยแบบจำลอง EFA ผู้วิจัยไม่ลบรายการใดออกจากเครื่องมือเนื่องจากน้ำหนักของการถดถอยมีค่ามากกว่าค่าเกณฑ์การยอมรับขั้นต่ำ 0.60 เพื่อเป็นการยืนยันแบบจำลองการวัด ผู้วิจัยใช้ Confirmatory Factor Analysis โดยทดสอบค่า Model-Fit จากตัวชี้วัดความเหมาะสมของแบบจำลองที่แนะนำ (χ^2/df , GFI, RMSEA, RMR, NFI, CFI, IFI, และ TLI) เพื่อการยืนยันดัชนีความเหมาะสมทั้งหมด ผลลัพธ์พบว่าค่าทั้งหมดมีค่ามากกว่าค่าเกณฑ์ที่เกี่ยวข้อง (การยอมรับต่ำสุดทั่วไป) ตามคำแนะนำของ Hair et al. (2013) ดังที่แสดงในตาราง 4.7

ตารางที่ 4.7 แสดงผลลัพธ์การวัดตัวบ่งชี้ความเหมาะสมสำหรับแบบจำลองการวัด

Model	χ^2	Df	χ^2/df	GFI	RMSEA	RMR	NFI	CFI	IFI	TLI
Standards			$1 < \chi^2/df < 3$	≥ 0.90	$\leq 0.08 < .1$	$\leq 0.08 < .1$	≥ 0.90	≥ 0.90	≥ 0.90	≥ 0.90
Acquired	437.90	237	1.848	0.907	0.073	0.028	0.938	0.917	0.918	0.903

ที่มา: Rukhiran et al., 2022



รูปที่ 4.8 แสดงรูปแบบการวัดการรับรู้ของนักเรียนต่อการรู้จำทางชีวมิติ

ที่มา: Rukhiran et al., 2022

รูปที่ 4.8 แสดงแบบจำลองการวัดของมุมมองของนักศึกษาที่มีต่อการใช้งานระบบการรู้จำโดยใช้เทคโนโลยีชีวมิติ โดยใช้โปรแกรม AMOS ซึ่งโปรแกรม AMOS ย่อมาจาก Analysis of Moment Structures เป็นโปรแกรมวิเคราะห์ข้อมูลทางสถิติที่ใช้ในการวิเคราะห์โมเมนต์สตรัคเจอร์ ซึ่งเป็นเทคนิคการวิเคราะห์โมเดลสมการโครงสร้าง (Structural Equation Modeling: SEM) โดยโปรแกรม AMOS ใช้ตัวช่วยในการสร้างแบบจำลองทางสถิติและการประมวลผลข้อมูลที่มีความซับซ้อนต่าง ๆ ในการสร้างแบบจำลอง

4.2.4 การวิเคราะห์โมเดลสมการโครงสร้าง (Structural Model Estimation: SEM)

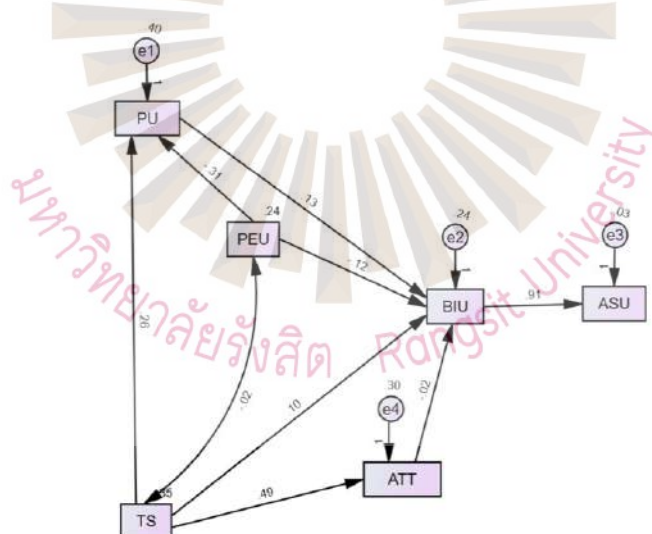
การวิเคราะห์โมเดลสมการโครงสร้าง (Structural Equation Modeling: SEM) เป็นเทคนิควิเคราะห์ข้อมูลทางสถิติที่ใช้ในการตรวจสอบและสร้างแบบจำลองที่เป็นไปได้ของความสัมพันธ์ระหว่างตัวแปรต่างๆ โดยใช้สมการทางคณิตศาสตร์เป็นพื้นฐาน โดย SEM มุ่งเน้น

การวิเคราะห์และให้ข้อมูลเกี่ยวกับโครงสร้างที่มีอยู่ของตัวแปรต่าง ๆ โดยการจัดกลุ่มตัวแปรเหล่านี้เข้าเป็นโครงสร้างหนึ่งและทำการวิเคราะห์ความสัมพันธ์ที่มีระหว่างตัวแปรเหล่านี้ SEM ถูกใช้เพื่อประเมินแบบจำลองการสำรวจที่เสนอของเราตามที่แสดงในรูปที่ 4.9 โดย Hair et al. (2013) อธิบายว่าเทคนิคการวิเคราะห์ปัจจัยการสำรวจแบบสำรวจและการยืนยันสามารถใช้ในการสำรวจความสัมพันธ์ที่หลากหลายพร้อมกันในลำดับขั้นต่อเนื่อง ซึ่งเป็นประโยชน์มากเมื่อโครงสร้างของแบบจำลองแสดงอิทธิพลต่อกันโดยตรงและโดยอ้อม ขั้นตอนแรกในการตีความผลลัพธ์ SEM คือตรวจสอบตัวชี้วัดความเหมาะสมของแบบจำลองเพื่อพิสูจน์ว่าข้อมูลเหมาะสมกับแบบจำลองที่เสนอไว้ตามที่แสดงในตาราง 4.8

ตารางที่ 4.8 แสดงผลลัพธ์การวัดตัวบ่งชี้ความเหมาะสมสำหรับรูปแบบการวัดที่ปรับปรุงใหม่

Model	χ^2	df	χ^2/df	GFI	RMSEA	RMR	NFI	CFI	IFI	TLI
Criteria			$1 < \chi^2/df < 3$	≥ 0.90	$\leq 0.08 < 1$	$\leq 0.08 < 1$	≥ 0.90	≥ 0.90	≥ 0.90	≥ 0.90
Obtained	7.776	6	1.296	0.984	0.043	0.008	0.940	0.996	0.996	0.996

ที่มา: Rukhiran et al., 2022



รูปที่ 4.9 แสดงการปรับปรุงรูปแบบการวัดการรับรู้ของนักเรียนต่อการจดจำทางชีวมิติ

ที่มา: Rukhiran et al., 2022

จากรูปที่ 4.9 แบบจำลอง SEM แสดงว่าตัวชี้วัดความเหมาะสมทั้งหมดตรงตามหลักการยอมรับขั้นต่ำ ค่าความสำคัญของเส้นทาง (Path Significances), ค่าสัมประสิทธิ์ (Coefficients) และค่าความแปรปรวน (Variances) ที่มีผลต่อตัวแปรทุกตัวถูกแสดงในรูป 4.9

4.2.5 ผลการทดสอบสมมติฐาน (Hypotheses Test Results)

โดยภาพรวมของการทดสอบสมมติฐานของการประเมินการยอมรับการใช้งานระบบ ตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติ รวมผลการวิจัยพิจารณาถูกต้อง จำนวน 5 จาก 8 สมมติฐานที่ทดสอบ ดัง แสดงในตารางที่ 4.9

ตารางที่ 4.9 แสดงผลสรุปการประเมินสมมติฐาน

Hypotheses	Relationship (Positive)	value	p-value	Results
H1	PEU → PU	-0.228	0.002**	Accepted
H2	TS → ATT	0.469	0.000***	Accepted
H3	PU → BIU	0.169	0.036**	Accepted
H4	PEU → BIU	-0.117	0.137	Rejected
H5	ATT → BIU	-0.024	0.780	Rejected
H6	TS → BIU	0.115	0.194	Rejected
H7	BIU → ASU	0.938	0.000***	Accepted
H8	TS → PU	0.230	0.002**	Accepted

*** $p < 0.001$, ** $p < 0.05$

ที่มา: Rukhiran et al., 2022

จากตารางที่ 4.9 พบว่า

4.2.5.1 ยอมรับ H1 โดยสรุปได้ว่า ความง่ายในการใช้งาน (PEU) มีผลกระทบที่สำคัญอย่างมากต่อการรับรู้ถึงประโยชน์ในการใช้งาน (PU) ($\beta = -0.288$, $P < 0.002$)

4.2.5.2 ยอมรับ H2 โดยสรุปได้ว่าความเชื่อมั่นและความปลอดภัย (TS) มีผลกระทบที่สำคัญอย่างมากต่อทัศนคติ (ATT) ($\beta = 0.469$, $P < 0.000$)

4.2.5.3 ยอมรับ H3 โดยสรุปได้ว่า การรับรู้ถึงควมมีประโยชน์ (PU) ผลกระทบที่มีนัยสำคัญต่อความตั้งใจในการใช้งาน (BIU) ($\beta = 0.169$, $P < 0.036$)

4.2.5.4 ปฏิเสธ H4 โดยสรุปได้ว่า การใช้งานได้ง่าย (PEU) ไม่มีผลที่มีนัยสำคัญต่อการใช้งาน (BIU) ($\beta = -0.117, P < 0.137$)

4.2.5.5 ปฏิเสธ H5 โดยสรุปได้ว่าทัศนคติ (ATT) ไม่มีผลที่มีนัยสำคัญต่อความตั้งใจในการใช้งาน (BIU) ($\beta = -0.024, P < 0.780$)

4.2.5.6 ปฏิเสธ H6 โดยสรุปได้ว่า ความเชื่อมั่นและความปลอดภัย (TS) ไม่มีผลที่มีนัยสำคัญต่อความตั้งใจในการใช้งาน (BIU) ($\beta = 0.115, P < 0.194$)

4.2.5.7 ยอมรับ H7 โดยสรุปได้ว่า ความตั้งใจในการใช้งาน (BIU) มีผลกระทบที่มีนัยสำคัญต่อการใช้งานจริง (ASU) ($\beta = 0.938, P < 0.000$)

4.2.5.8 ยอมรับ H8 โดยสรุปได้ว่า ความเชื่อมั่นและความปลอดภัย (TS) มีผลกระทบที่สำคัญอย่างมากต่อการรับรู้ถึงประโยชน์ในการใช้งาน (PU) ($\beta = 0.230, P < 0.002$)



บทที่ 5

สรุปผล อภิปรายผล และข้อเสนอแนะ

5.1 สรุปผลการวิจัย

งานวิจัยนี้มีวัตถุประสงค์ 3 ข้อ ได้แก่ เพื่อสร้างกรอบโครงสร้างระบบซอฟต์แวร์สำหรับการตรวจสอบตัวบุคคลเข้าสอบด้วยเทคโนโลยีชีวมิติบนอุปกรณ์สมองกลฝังตัว เพื่อพัฒนาต้นแบบซอฟต์แวร์สำหรับการตรวจสอบตัวบุคคลเข้าสอบทางชีวมิติแบบหลายโปรโตคอล ซึ่งรองรับเทคโนโลยีชีวมิติแบบทางเดียวและแบบหลายทาง และเพื่อเปรียบเทียบประสิทธิภาพและประสิทธิผลของระบบหลายโปรโตคอลบนชีวมิติหลายแบบในการตรวจสอบบุคคลเข้าสอบ โดยผลลัพธ์ที่ได้จากงานวิจัยนี้มีดังนี้

5.1.1 กรอบโครงสร้างระบบซอฟต์แวร์สำหรับการตรวจสอบตัวบุคคลเข้าสอบด้วยเทคโนโลยีชีวมิติบนอุปกรณ์สมองกลฝังตัว

วัตถุประสงค์ในข้อแรก ในการเพื่อได้แก่ เพื่อสร้างกรอบโครงสร้างระบบซอฟต์แวร์สำหรับการตรวจสอบตัวบุคคลเข้าสอบทางชีวมิติด้วยสมองกลฝังตัว ผู้วิจัยได้ทำการศึกษาจากงานวิจัยที่เกี่ยวข้อง ทำการเก็บรวบรวมข้อมูลต่างๆ ที่จำเป็นในการสร้างตัวต้นแบบซอฟต์แวร์ โดยการพัฒนารอบแนวคิดของระบบ ทำการวิเคราะห์และออกแบบตามมาตรฐานการออกแบบของ IEEE SDD และ ISO 25010 (SQuaRE) จนได้ผลลัพธ์เป็นกรอบแนวคิดเชิงออกแบบเพื่อเป็นตัวต้นแบบให้นักพัฒนานำไปใช้ต่อไป

5.1.2 ต้นแบบซอฟต์แวร์สำหรับการตรวจสอบตัวบุคคลเข้าสอบทางชีวมิติแบบหลายโปรโตคอล

วัตถุประสงค์ที่สอง เพื่อพัฒนาต้นแบบซอฟต์แวร์สำหรับการตรวจสอบตัวบุคคลเข้าสอบทางชีวมิติแบบหลายโปรโตคอล หลังจากผู้วิจัยได้กรอบแนวคิดการออกแบบแล้ว จึงนำมา

เป็นต้นแบบในการพัฒนาระบบการตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติ โดยใช้หลักการออกแบบเชิงวัตถุร่วมกับ Information Flow Diagram (IFD) ผลลัพธ์ที่ได้คือต้นแบบซอฟต์แวร์สำหรับการตรวจสอบตัวบุคคลเข้าสอบทางชีวมิติแบบหลายโปรโตคอล

5.1.3 ผลการเปรียบเทียบประสิทธิภาพและประสิทธิผลของระบบหลายโปรโตคอลบนชีวมิติในการตรวจสอบบุคคลเข้าสอบ

วัตถุประสงค์ที่สาม เพื่อเปรียบเทียบประสิทธิภาพและประสิทธิผลของระบบหลายโปรโตคอลบนชีวมิติในการตรวจสอบบุคคลเข้าสอบ ผู้วิจัยได้ทำการทดลองเพื่อเปรียบเทียบประสิทธิภาพของระบบชีวมิติ 8 รูปแบบ โดยทำการพัฒนาเครื่องมือชีวมิติเพื่อทดสอบและได้นำเสนอ Biometric Quality Metric ในการเปรียบเทียบประสิทธิภาพและประสิทธิผลของระบบชีวมิติแบบต่าง ๆ โดยผลลัพธ์ที่ได้คือ ระบบชีวมิติแบบ Unimodal และ Multimodal มีประสิทธิภาพและประสิทธิผลมากกว่าระบบการตรวจสอบแบบไม่มีชีวมิติ (Zero Biometric) และระบบชีวมิติแต่ละรูปแบบมีทั้งข้อดีและข้อด้อย ขึ้นอยู่กับว่าจะนำรูปแบบใดไปใช้ในการทำงานในลักษณะใด

นอกจากนี้ผู้วิจัยทำการประเมินการยอมรับเทคโนโลยี โดยใช้แบบจำลองการยอมรับเทคโนโลยี (Technology Acceptance Model: TAM) ในการประเมิน โดยมีสมมติฐานในการสำรวจ จำนวน 8 สมมติฐาน โดยสรุปแล้วส่วนใหญ่ผู้ใช้ในการยอมรับการใช้งานระบบตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติ โดยการยอมรับ 5 จาก 8 สมมติฐาน และสรุปได้ว่าการยอมรับการใช้ระบบตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติ ในด้านความรู้สึกที่ง่ายต่อการใช้งาน ประโยชน์ที่ได้รับ ทัศนคติ ความเชื่อมั่นและความปลอดภัย

5.2 อภิปรายผล

ผลลัพธ์ที่ได้จากการวิจัยนี้ พบว่า ระบบตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติแบบทางเดียวและแบบหลายทาง มีประสิทธิภาพและประสิทธิผลดีกว่าการใช้การตรวจสอบผู้เข้าสอบแบบใช้บัตรประจำตัวผู้เข้าสอบ ซึ่งผลลัพธ์ที่ได้เป็นไปในทิศทางเดียวกับงานวิจัยที่เกี่ยวข้อง เช่น Ammour et al. (2020) ในการประยุกต์ใช้ชีวมิติใบหน้าและม่านตาร่วมกันในการตรวจสอบบุคคล และ Zhao et al. (2020) ได้ใช้ชีวมิติแบบหลายทางด้วยกล้อง 2 กล้องในการตรวจสอบบุคคลด้วยใบหน้าได้ผลลัพธ์เชิงประสิทธิภาพทางด้านความแม่นยำในการตรวจสอบที่ดีขึ้นกว่าแบบใช้กล้อง

ตัวเดียว แต่ในการนำไปใช้ในการตรวจสอบผู้เข้าสอบในแต่ละสถาบันการศึกษาซึ่งมีปัจจัยในการให้ความสำคัญกับประสิทธิภาพที่ต่างกัน การใช้ชีวมิติที่เหมาะสมกับแต่ละสถานศึกษาจึงแตกต่างกันไป ในงานวิจัยนี้ได้กำหนดค่าความสำคัญของแต่ละปัจจัยให้มีค่าเท่า ๆ กัน ซึ่งผลลัพธ์ที่ได้จากการประเมินประสิทธิภาพของระบบตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติในงานวิจัยนี้ ได้แก่ การใช้ชีวมิติแบบใบหน้า

5.3 ข้อเสนอแนะในการนำผลการวิจัยไปใช้

ผลลัพธ์ที่ได้จากการวิจัยนี้ ได้แก่ ตัวต้นแบบในการพัฒนาระบบตรวจสอบผู้เข้าสอบด้วยเทคโนโลยีชีวมิติ สามารถนำไปต่อยอดเพื่อพัฒนาระบบการตรวจสอบผู้สอบด้วยเทคโนโลยีชีวมิติในรูปแบบต่าง ๆ ที่เหมาะสมตามความพร้อมและความต้องการของแต่ละสถาบันการศึกษา โดยงานวิจัยนี้ใช้การพัฒนานับอุปกรณ์ Raspberry Pi 4 ซึ่ง นักพัฒนาสามารถปรับเปลี่ยนไปใช้บนระบบอื่น ๆ ได้ตามความเหมาะสม

การหา Biometric Quality Metric ในงานวิจัยนี้ได้ตั้งค่าน้ำหนักของแต่ละปัจจัยในการประเมินประสิทธิภาพของระบบการตรวจสอบผู้เข้าสอบไว้ในระดับเท่ากัน ในกรณีที่สถาบันการศึกษาต้องการที่จะเน้นประสิทธิภาพในด้านใดด้านหนึ่ง สามารถทำการใส่ค่าน้ำหนักในการคำนวณได้ตามความเหมาะสม

5.4 ข้อเสนอแนะในการดำเนินงานในภายหน้า

ทั้งนี้ในการนำไปใช้เพื่อให้มีประสิทธิภาพมากขึ้น นักพัฒนาอาจทำการปรับเปลี่ยนรูปแบบของระบบชีวมิติเป็นแบบอื่นโดยต่อยอดจากต้นแบบซอฟต์แวร์สำหรับการตรวจสอบตัวบุคคลเข้าสอบทางชีวมิติ เช่น นำไปต่อยอดในประเด็นการนำไปใช้งานกับ Intelligent System หรือนำไปต่อยอดในกรณีที่มีการคิดค้นชีวมิติแบบใหม่ เช่น การตรวจจับความร้อนในร่างกาย หรือนำไปต่อยอดในการจับทุจริตในระหว่างที่ผู้สอบทำข้อสอบโดยการตรวจจับการเคลื่อนไหว เป็นต้น

บรรณานุกรม

- กอบเกียรติ สระอุบล. (2561). *พัฒนา iot บนแพลตฟอร์ม Arduino Raspberry Pi*. กรุงเทพฯ: อินเตอร์มีเดีย.
- อัยฎาพร ทรัพย์สมบูรณ์. (2557). *การวิเคราะห์และออกแบบเชิงวัตถุ*. กรุงเทพฯ: เคทีพี.
- Abass, O. A., Olajide, S. A., & Samuel, B. O. (2017). Development Of Web-Based Examination System Using Open-Source Programming Model. *Turkish Online Journal of Distance Education*, 18(2), 30-42. doi:10.17718/tojde.306555.
- Acosta-Medina, J. K., Torres-Barreto, M. L., & Cárdenas-Parga, A. F. (2021). Students' preference for the use of gamification in virtual learning environments. *Australasian Journal of Educational Technology*, 37(4), 145-148. doi:10.14742/ajet.6512.
- Aggarwal, Y. (2020). *K Dimensional Tree / (K D Tree)*. Retrieved from <https://iq.opengenus.org/k-dimensional-tree>.
- Ahmed, A. A. (2019). Future Effects and Impacts of Biometrics Integrations on Everyday Living. *Al-Mustansiriyah Journal of Science*, 29(3), 139-144. doi:10.23851/mjs.v29i3.642.
- Ahmed, I. B., Mohamed, M. A., & Noma, A. M. (2018). A Framework For Secure Online Exam Using Biometric Fingerprint And Steganography Techniques. *International Journal of Engineering & Technology*, 7, 32-35. doi:10.14419/ijet.v7i3.28.20961.
- Ahsan, M. M., Li, y., Zhang, J., Ahad, M. T., & Gupta, K. D. (2021). Evaluating the Performance of Eigenface, Fisherface, and Local Binary Pattern Histogram-Based Facial Recognition Methods under Various Weather Conditions. *Technologies 2021*, 9, 31. doi:10.3390/technologies9020031.
- Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ.: Prentice–Hall.
- Ammour, B., Boubchir, L., Bouden, T., & Ramdani, M. (2020). Face–Iris Multimodal Biometric Identification System. *Electronics*, 9(1), 1-18. doi:10.3390/electronics9010085.
- Awojide, S., Awe, O. S., & Babatope, T. S. (2018). Biometric Fingerprint System Using an Online Based Pattern Recognition for Candidates Authentication in Nigeria Institution Examinations. *The Design Perspective. International Journal of Scientific & Engineering Research*, 9(5), 1680-1694. doi:10.14299/ijser.2018.05.02.

บรรณานุกรม (ต่อ)

- Bagozzi, P. R., & Yi, Y. (1964). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, 16, 74-94. doi:10.1007/BF02723327.
- Chen, Y., Yang, J., Wang, C., & Park, D. (2016). Variational Bayesian Extreme Learning Machine. *Neural Comput & Applic*, 27, 185–196. doi:10.1007/s00521-014-1710-1.
- Chomngern , T., & Netinant, P. (2017). A Mobile Software Model for Web-Based Learning Using Information Flow Diagram (IFD). *ICIT 2017: 2017 International Conference on Information Technology Singapore Singapore December 27 - 29, 2017* (pp. 243-247. doi:10.1145/3176653.3176680).
- Dass, S., Sadrulhuda, M. Q., Pasha, N., Nayan, N., & Nayak, J. S. (2020). Real Time Face Recognition using Raspberry Pi. *International Journal of Computer Applications*, 176(33), 1-4. doi:10.5120/ijca2020920387.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319-339. doi:10.2307/249008.
- Divya, H., Nandhini, S., Shobana, S., & Sujithra, M. (2021). Examination Management System. *International Journal of Advanced Research*, 9(1), 920-923. doi:10.21474/ijar01/12370.
- Dube, A., Singh, D., Asthana, R., & Singh Walia, G. (2020). A framework for evaluation of biometric based Authentication System. *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, 925-932. 10.1109/iciss49785.2020.9315933.
- El-Abed, M., & Charrier, C. (2012). Evaluation of Biometric Systems. *New Trends and Developments in Biometrics*, 149-169. doi:10.5772/52084.
- Emmanuel, E., & Okonkwo, T. (2019). A Biometric Authentication Approach to Examination Conduct in Nigerian Universities. *International Journal of Innovative Research in Science, Engineering and Technology*, 8(3), 2176-2182. doi:10.15680/IJRSET.2019.0802072.
- Febrero, F., Calero, C., & Moraga, M. Á. (2016). Software reliability modeling based on ISO/IEC SQuaRE. *Information and Software Technology*, 70, 18-29. doi: 10.1016/j.infsof.2015.09.006.

บรรณานุกรม (ต่อ)

- Fenu , G., Marras , M., & Boratto , L. (2018). A multi-biometric system for continuous student authentication in e-learning platforms. *Pattern Recognition Letters*, 113, 83-92. doi:10.1016/j.patrec.2017.03.027.
- Fornell, C., Larcker, D.F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, 1(18), 39-50.
- Gawande, U., & Golhar, Y. (2018). Biometric security system: A rigorous review of unimodal and multimodal biometrics techniques. *International Journal of Biometrics*, 10(2), 142-175. doi:10.1504/ijbm.2018.10012749.
- Gomez-Barrero, M., Maiorana, E., Galbally, J., Campisi, P., & Fierrez, J. (2017). Multi-biometric template protection based on Homomorphic Encryption. *Pattern Recognition*, 67, 149-163. doi:10.1016/j.patcog.2017.01.024.
- González-Soler, L., J., Gomez-Barrero, M., Chang, L., Pérez-Suárez, A., & Busch, C. (2021). Fingerprint Presentation Attack Detection Based on Local Features Encoding for Unknown Attacks. *IEEE Access*, 9, 5806-5820, 2021. doi:10.1109/ACCESS.2020.3048756.
- Gunasekaran, K., Jayamani, R., & Ramasamy, P. (2019). Deep multimodal biometric recognition using contourlet derivative weighted rank fusion with human face, fingerprint and iris images. *Automatika*, 60(3), 253-265. doi:10.1080/00051144.2019.1565681.
- Hair, J. F., Black , W. C., Babin, B. J., & Anderson , R. E. (2013). *Multivariate data analysis* (7th ed.). USA: Pearson Education Limited.
- Hameed, M. R., & Abdullatif, F. A. (2017). Online Examination System. *International Advanced Research Journal in Science, Engineering and Technology*, 4(3), 106-110. doi:10.17148/iarjset.2017.4321.
- Hamid, R. A., Mokhtar, U. A., Yusof, M., & Warland, A. (2020). Electronic Records Management in Schools: The Case Study of School Examination Analysis System. *Journal Pengurusan*, 57, 1-13. doi:10.17576/pengurusan-2019-57-10.

บรรณานุกรม (ต่อ)

- Hassanein, K., & Head, M. (2007). Manipulating perceived social presence through the web interface and its impact on attitude towards online shopping. *International Journal of Human-Computer Studies*, 65(8), 689-708. doi:10.1016/j.ijhcs.2006.11.018.
- Hong, L., Wan, Y., & Jain, A. K. (1998). Fingerprint image enhancement: Algorithm and performance evaluation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 20(8), 777-789.
- Jain, T., Tomar, U., Arora, U., & Jain, S. (2020). IoT Based Biometric Attendance System. *International Journal of Electrical Engineering & Technology*, 11(2), 156-161.
- JavaTPoint. (2021). *Face recognition and Face detection using the OpenCV*. Retrieved from <https://www.javatpoint.com/face-recognition-and-face-detection-using-opencv>.
- Kanak, A., & Sogukpinar, I. (2017). BioTAM: A technology acceptance model for biometric authentication systems. *IET Biometrics*, 6(6), 457-467. doi:10.1049/iet-bmt.2016.0148.
- Kas, M., Merabet, Y. E., Ruichek, Y., & Messoussi, R. (2018). Mixed Neighborhood Topology Cross Decoded Patterns For Image-Based Face Recognition. *Expert Systems With Applications*, 114, 119-142. doi:10.1016/j.eswa.2018.07.035.
- Kortli, Y., Jridi, M., Falou, A. A., & Atri, M. (2020). Face Recognition Systems: A Survey. *Sensors* 2020, 20(2), 1-36. doi:10.3390/s20020342.
- Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2017). ImageNet Classification with Deep Convolutional Neural Networks. *Communications of the ACM*, 60(6), 84-90. doi:10.1145/3065386.
- Lee, M.-C. (2014). Software Quality Factors and Software Quality Metrics to Enhance Software Quality Assurance. *British Journal of Applied Science & Technology*, 4(21), 3069-3095. doi:10.9734/BJAST/2014/10548.
- Maltoni, D., Maio, D., Jain, A.K., & Prabhakar, S. (2009). *Fingerprint Matching*. In: *Handbook of Fingerprint Recognition* (2nd ed.). Switzerland: Springer. doi:10.1007/978-3-030-83624-5_4.

บรรณานุกรม (ต่อ)

- Martin, M., Koprda, S., & Lubor, F. (2018). Biometrics Authentication of Fingerprint with Using Fingerprint Reader and Microcontroller Arduino. *Telkomnika (Telecommunication Computing Electronics and Control)*, 16(2), 755-765.
doi:10.12928/TELKOMNIKA.v16i2.7572.
- Mathur, N., Mathur, S., Mathur, D., & Dadheech, P. (2020). A Brief Survey of Deep Learning Techniques for Person Re-identification. *3rd International Conference on Emerging Technologies in Computer Engineering: Machine Learning and Internet of Things (ICETCE)*, 129-138. doi: 10.1109/ICETCE48199.2020.9091747.
- Mehta, P., & Tomar, P. (2016). An efficient attendance management sytem based on face recognition using Matlab and Raspberry Pi 2. *International Journal of Engineering Technology Science and Research*, 3, 71-78.
- Mir, G. M., Balkhi, A., Lala, N. A., Sofi, N. A., Kirmani, M., Mir, I. A., & Hamid, H. A. (2018). The Benefits of Implementation of Biometric Attendance System. *Oriental Journal of Computer Science and Technology*, 11(1), 50-54. doi:10.13005/ojcs11.01.09.
- Ngugi, B., Kamis, A., & Tremaine, M. (2011). Intention to use biometric systems. *e-Service Journal*, 7(3), 20-46. doi:10.2979/eservicej.7.3.20.
- Nguyen, K., Fookes, C., Sridharan, S., Tistarelli, M., & Nixon, M. (2018). Super-Resolution for Biometrics: A Comprehensive Survey. *Pattern Recognition*, 78, 23-42.
doi:10.1016/j.patcog.2018.01.002.
- Noma-Osaghae, E., Okonigene, R. E., Okereke, C., Okesola, O., & Okokpujie, K. (2017). Design and Implementation of an Iris Biometric Door Access Control System. *International Conference on Computational Science and Computational Intelligence (CSCI)*, 590-593.
doi:10.1109/csci.2017.102.
- Norfolk, L., & O'Regan, M. (2021). Biometric technologies at music festivals: An extended technology acceptance model. *Journal of Convention & Event Tourism*, 22(1), 36-60.
doi:10.1080/15470148.2020.1811184.
- OpenCV. (2023). *Face Recognition with OpenCV*. Retrieved from
https://docs.opencv.org/3.4/da/d60/tutorial_face_main.html.

บรรณานุกรม (ต่อ)

- Phokajang, A., & Netinant, P. (2021). Developing Software Architecture for A Smart School Digital Framework. *ICSIM 2021: 2021 The 4th International Conference on Software Engineering and Information Management*, 22-27. doi:10.1145/3451471.3451475.
- Poria, S., Cambria, E., Bajpai, R., & Hussain, A. (2017). A review of affective computing: From unimodal analysis to multimodal fusion. *Information Fusion*, 37, 98-125. doi:10.1016/j.inffus.2017.02.003.
- Precise Biometrics. (2014). *Understanfing Biometric Performance Evaluation*. Retrieved from <https://precisebiometrics.com/wp-content/uploads/2014/11/White-Paper-Understanding-Biometric-Performance-Evaluation.pdf>.
- Pukdesree, S., & Netinant, P. (2016). Conceptual Framework: The Adaptive Biometrics Authentication for Accessing Cloud Computing Services Using iPhone. *Recent Advances in Information and Communication Technology 2016*, 463, 209-216. doi:10.1007/978-3-319-40415-8_20.
- Raju, A. S., & Udayashankara, V. (2018). A survey on unimodal, multimodal biometrics and its fusion techniques. *International Journal of Engineering & Technology*, 7(4), 689-695. doi:10.14419/ijet.v7i4.36.24224.
- Ratjeana Malatji, W., van Eck, R., & Zuva, T. (2020). Acceptance of Biometric Authentication Security Technology on Mobile Devices. *2020 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*. doi:10.1109/imitec50163.2020.9334082.
- Rukhiran, M., & Netinant, P. (2020). A practical model from multidimensional layering: Personal finance information framework using mobile software interface operations. *Journal of Information and Communication Technology*, 19(3), 321-349. doi:10.32890/jict2020.19.3.2.
- Rukhiran, M., Netinant, P., & Elrad, T. (2020). Effecting of environmental conditions to accuracy rates of face recognition based on IoT solution. *Journal of Current Science and Technology*, 10(1), 21-33. doi: 10.14456/jcst.2020.2.

บรรณานุกรม (ต่อ)

- Rukhiran, M., Wong-In, S., & Netinant, P, (2022). User acceptance factors related to biometric recognition technologies of examination attendance in higher education: TAM model. *Sustainability*, 15(4), 3092. doi:10.3390/su15043092.
- Rukhiran, M., Wong-In, S., & Netinant, P, (2023). IoT-Based Biometric Recognition Systems in Education for Identity Verification Services: Quality Assessment Approach. *IEEE Access*, 11, 22767-22787. doi: 10.1109/ACCESS.2023.3253024.
- Sayeed, S., Hossen, J., Kalaiarasi, S., Vaithiyashankar, J., Yusof, I., & Samraj, A. (2017). Realtime face recognition for attendance monitoring system. *Journal of Theoretical and Applied Information Technology*, 95, 24-30.
- Shamsi, S. V., & Andrews, J. V. (2019). A Survey Paper on Fingerprint Recognition and Cross Matching. *International Journal for Research in Applied Science and Engineering Technology*, 7(5), 573-575. doi:10.22214/ijraset.2019.5096.
- Siddique, S., Yasmin, M., Taher, T., & Alam, M. (2021). The Reliability and Acceptance of Biometric System in Bangladesh: Users Perspective. *International Journal of Computer Trends and Technology*, 69(6), 15-21. doi:10.14445/22312803/ijctt-v69i6p103.
- Singh, M., Singh, R., & Ross, A. (2019). A comprehensive overview of biometric fusion. *Information Fusion*, 52, 187-205. doi:10.1016/j.inffus.2018.12.003.
- Song, B. K. (2021). E-portfolio implementation: Examining learners' perception of usefulness, self-directed learning process and value of learning. *Australasian Journal of Educational Technology*, 37(1), 68-81. doi:10.14742/ajet.6126.
- Soni, U., & Goyani, M. (2018). A Survey on State of the Art Methods of Fingerprint Recognition. *International Journal of Scientific Research in Science, Engineering and Technology*, 4(2), 189-200.
- Sunaryono, D., Siswantoro, J., & Anggoro, R. (2021). An android based course attendance system using face recognition. *Journal of King Saud University - Computer and Information Sciences*, 33, 304-312. doi:10.1016/j.jksuci.2019.01.006.

บรรณานุกรม (ต่อ)

- Taileb, M. (2020). Design and Implementation of RFID and Fingerprint-Based Student Verification System. *Design and Implementation of RFID and Fingerprint-Based Student Verification System. nternational Journal of Recent Technology and Engineering Regular*, 8(5), 2084-2092. doi:10.35940/ijrte.e5788.018520.
- Tatar, F. D. (2017). Fingerprint Recognition Algorithm. *Computer Science & Information Technology (CS & IT)*, 85-100. doi:10.5121/csit.2017.70609.
- Techmakers Innovation. (n.d.). *Raspberry Pi 4 Model B*. Retrieved from <https://shop.techmakers.com.my/raspberry/raspberry-pi-4-model-b-2gb-ram>.
- Traore, I., Nakkabi, Y., Saad, S., Sayed, B., Ardigo, J. D., & Quinan, P. M. (2017). Ensuring Online Exam Integrity Through Continuous Biometric Authentication. *Information Security Practices*, 73-81. doi:10.1007/978-3-319-48947-6_6.
- Walia, G. S., Singh, T., Singh, K., & Verma, N. (2019). Robust multimodal biometric system based on optimal score level fusion model. *Expert Systems with Applications*, 116, 364-376. doi:10.1016/j.eswa.2018.08.036.
- Wang, J. S. (2021). Exploring biometric identification in FinTech applications based on the modified TAM. *Financial Innovation*, 7(42), 1-25. doi:10.1186/s40854-021-00260-2.
- Wong-In, S., & Netinant, P. (2018). Designing an examinee personal verification system using biometric technology. *Journal of Current Science and Technology. Journal of Current Science and Technology*, 8(2), 75-86. doi:10.14456/jcst.2018.9.
- Xi, X., Yang, L., & Yin, Y. (2016). Learning Discriminative Binary Codes for Finger Vein Recognition. *Pattern Recognition*, 66, 26-33. doi:10.1016/j.patcog.2016.11.002.
- Yadav, S., & Vishwakarma, V. P. (2019). Extended Interval Type-II and Kernel Based Sparse Representation Method for Face Recognition. *Expert Systems with Applications*, 116, 265-274. doi:10.1016/j.eswa.2018.09.032.
- Yaddaden, Y., Adda, M., Bouzouane, A., Gaboury, S., & Bouchard, B. (2018). User Action and Facial Expression Recognition for Error Detection System in an Ambient Assisted Environment. *Expert Systems With Applications*, 112, 173-189. doi:10.1016/j.eswa.2018.06.033.

บรรณานุกรม (ต่อ)

- Yamane, T., (1967). *Statistics, An Introductory Analysis* (2nd ed)., New York: Harper and Row.
- Yang, W., Wang, S., Hu, J., Guanglou, Z., & Valli, C. (2018). A Fingerprint and Finger-vein Based, Cancelable Multi-biometric System. *Pattern Recognition*, 78, 242-251.
doi:10.1016/j.patcog.2018.01.026.
- Ye, M., Shen, J., Lin, G., Xiang, T., Shao, L., & Hoi, S. C. (2020). Deep Learning for Person Re-identification: A Survey and Outlook. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 1, 1-20. doi:10.1109/TPAMI.2021.3054775.
- Yusof, Y. W., Nasir, M. A., Othman, K. A., Suliman, S. I., Shahbudin, S., & Mohamad, R. (2018). Real-time internet based attendance using face recognition system. *International Journal of Engineering & Technology*, 7(3), 174-178. doi:10.14419/ijet.v7i3.15.17524.
- Zainal, I., Sidek, K. A., Gunawan, T. S., Mansor, H., & Kartiwi, M. (2014). Design and development of portable classroom attendance system based on Arduino and fingerprint Biometric. *The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M)* The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M), 1-4.
doi:10.1109/ICT4M.2014.7020601.
- Zainal, N. I., Sidek, K. A., & Gunawan, T. S. (2016). Portable anti forgery recognition for attendance system using fingerprint based biometric. *ARPJ Journal of Engineering and Applied Sciences*, 11(1), 396-403.
- Zhao, Y., Xu, J., Wu, J., Hao, J., & Qian, H. (2020). Enhancing Camera-Based Multimodal Indoor Localization With Device-Free Movement Measurement Using WiFi. *IEEE Internet of Things Journal*, 7(2), 1024-1038. doi:10.1109/jiot.2019.2948605.
- Zhou, R., Zhong, D., & Han, J. (2013). Fingerprint Identification Using SIFT-Based Minutia Descriptors and Improved All Descriptor-Pair Matching. *Sensors* 2013, 13, 3142-3156.
doi:10.3390/s130303142.

ภาคผนวก



ภาคผนวก ก

แบบประเมินการยอมรับการใช้งานระบบตรวจสอบบุคคลเข้าสอบด้วยเทคโนโลยีชีวมิติ

มหาวิทยาลัยรังสิต Rangsit University



แบบประเมินการยอมรับการใช้งานระบบตรวจสอบบุคคลเข้าสอบด้วยเทคโนโลยีชีวมิติ

แบบสอบถามนี้เป็นส่วนหนึ่งของการศึกษาและวิจัยตามหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาเทคโนโลยีสารสนเทศ วิทยาลัยนวัตกรรมการจัดการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยรังสิต โดยข้อมูลที่ได้ จะนำไปใช้ประโยชน์ทางการศึกษาและการออกแบบระบบซอฟต์แวร์ต่อไป

แบบสอบถามประกอบด้วย 8 ส่วน ดังนี้

ส่วนที่ 1 ข้อมูลพื้นฐาน แบบไม่ระบุข้อมูลเฉพาะที่เป็นการระบุตัวตนของผู้ตอบ

ส่วนที่ 2 ข้อมูลด้านการรับรู้ประโยชน์

ส่วนที่ 3 ข้อมูลด้านการรับรู้ความง่ายในการใช้งาน

ส่วนที่ 4 ข้อมูลด้านการรับรู้ความเชื่อมั่นและความปลอดภัย

ส่วนที่ 5 ข้อมูลด้านทัศนคติในการใช้งาน

ส่วนที่ 6 ข้อมูลด้านพฤติกรรมความตั้งใจที่จะงาน

ส่วนที่ 7 ข้อมูลด้านการใช้งานจริง

ส่วนที่ 8 ข้อมูลความคิดเห็นและข้อเสนอแนะเกี่ยวกับตัวระบบ

ขอความอนุเคราะห์ผู้ตอบแบบสอบถามทุกท่านตอบแบบสอบถามตามความเป็นจริง ความคิดเห็นของท่านเป็นส่วนสำคัญต่อความสำเร็จของงานวิจัยนี้ โดยข้อมูลของท่านจะถูกเก็บเป็นความลับ

ขอขอบพระคุณ ผู้ตอบแบบสอบถามทุกท่านเป็นอย่างสูง

นายเศรษฐพงศ์ วงษ์อินทร์

นักศึกษาระดับปริญญาเอก สาขาเทคโนโลยีสารสนเทศ

มหาวิทยาลัยรังสิต

ตอนที่ 1: ข้อมูลพื้นฐาน

คำชี้แจง กรุณาทำเครื่องหมาย ✓ ลงใน ☐ หน้าข้อที่ตรงกับสภาพความเป็นจริงของท่าน

1. เพศ: 1) ชาย 2) หญิง
2. อายุ: 1) 18 ปี หรือน้อยกว่า 2) 19 ปี หรือมากกว่า

สำหรับส่วนที่ 2-7 มีคำชี้แจงดังนี้

คำชี้แจง กรุณาทำเครื่องหมาย ✓ ลงใน ☐ หน้าข้อที่ตรงกับสภาพความเป็นจริงของท่าน

ลำดับคะแนนที่ใช้มีความหมายดังนี้

- 5 คือ ระดับการยอมรับมากที่สุด 4 คือ ระดับการยอมรับมาก
3 คือ ระดับการยอมรับปานกลาง 2 คือ ระดับการยอมรับน้อย
1 คือ ระดับการยอมรับน้อยที่สุด

ส่วนที่ 2: ข้อมูลด้านการรับรู้ประโยชน์

ด้านการรับรู้ประโยชน์	ระดับการยอมรับ				
	5	4	3	2	1
1. ท่านคิดว่าการจดจำใบหน้าเพื่อเข้าสอบมีประโยชน์มากกว่าวิธีการแบบเดิม (บัตรนักเรียน)					
2. ท่านคิดว่าการจดจำใบหน้าหลายรูปแบบสำหรับการเข้าสอบมีประโยชน์มากกว่าการจดจำใบหน้ารูปแบบเดียว					
3. เทคโนโลยีชีวมิติมีประโยชน์สำหรับการเรียนประจำวันของท่าน					
4. เทคโนโลยีชีวมิติช่วยให้ท่านเพิ่มประสิทธิภาพในระหว่างชั้นเรียนได้					

ส่วนที่ 3 ข้อมูลด้านการรับรู้ความง่ายในการใช้งาน

ด้านการรับรู้ประโยชน์	ระดับการยอมรับ				
	5	4	3	2	1
1. ท่านคิดว่าการจดจำใบหน้าเพื่อเข้าสอบนั้นง่ายกว่าวิธีการแบบเดิม (บัตรนักเรียน)					

2. ท่านคิดว่าการจดจำใบหน้าหลายรูปแบบสำหรับการเข้าสอบความ ง่ายในการใช้งานมากกว่าการจดจำใบหน้ารูปแบบเดียว					
3. เทคโนโลยีชีวมิติง่ายต่อการใช้งาน					
4. เหตุผลหนึ่งที่ระบบนี้มีประโยชน์ก็เพราะการใช้งานง่าย					
5. การรับรู้ที่มีต่อระบบชีวมิติของนักเรียนนั้นง่ายกว่าในการสตรว จสอบวิธีการแบบดั้งเดิม					
6. การจดจำด้วยเทคโนโลยีชีวมิติไม่ต้องใช้ความพยายามมากนักในการ ระบุตัวเอง					

ส่วนที่ 4 ข้อมูลด้านการรับรู้ความเชื่อมั่นและความปลอดภัย

ด้านการรับรู้ประโยชน์	ระดับการยอมรับ				
	5	4	3	2	1
1. ท่านคิดว่าการจดจำด้วยเทคโนโลยีชีวมิติจะเป็นการรุกรานทาง กายภาพ					
2. ท่านจะเชื่อมั่นในระบบจดจำด้วยชีวมิติ					
3. การระบุตัวนักเรียนโดยใช้การรู้จำชีวมิตินั้นเชื่อถือได้					
4. การระบุตัวตนโดยใช้การรู้จำชีวมิติสามารถระบุตัวท่านได้อย่าง ถูกต้อง					
5. การระบุตัวตนโดยใช้การรู้จำชีวมิติมีความแม่นยำสูง					

ส่วนที่ 5 ข้อมูลด้านทัศนคติในการใช้งาน

ด้านการรับรู้ประโยชน์	ระดับการยอมรับ				
	5	4	3	2	1
1. ท่านรู้สึกว่าการใช้เทคโนโลยีชีวมิตินั้นดีกว่าที่คาดไว้					
2. ความคาดหวังของท่านส่วนใหญ่ในการใช้ระบบจดจำใบหน้า ได้รับการยืนยัน					
3. ท่านรู้สึกการใช้เทคโนโลยีชีวมิติในการเรียนของท่านเป็นส่วนใหญ่					
4. ท่านสามารถเชื่อมั่นในการจดจำโดยใช้เทคโนโลยีชีวมิติเนื่องจากมี ความแม่นยำสูง					

ส่วนที่ 6 ข้อมูลด้านพฤติกรรมความตั้งใจที่จะงาน

ด้านการรับรู้ประโยชน์	ระดับการยอมรับ				
	5	4	3	2	1
1. ท่านชอบการจดจำด้วยเทคโนโลยีชีวมิติสำหรับการเข้าสอบมากกว่าวิธีดั้งเดิม					
2. ท่านจะใช้การจดจำใบหน้าด้วยเทคโนโลยีชีวมิติเมื่อมีการเข้าสอบ					
3. ท่านหวังว่าจะสามารถนำเทคโนโลยีชีวมิติมาประยุกต์ใช้ไมหาวิทยาลัยโดยเร็ว					

ส่วนที่ 7 ข้อมูลด้านการใช้งานจริง

ด้านการรับรู้ประโยชน์	ระดับการยอมรับ				
	5	4	3	2	1
1. ท่านจะใช้ระบบจดจำใบหน้าในการเข้าสอบ					
2. ท่านอยากจะแนะนำให้มหาวิทยาลัยของท่านใช้ระบบจดจำใบหน้าเพื่อยืนยันตัวนักเรียนในพื้นที่ตรวจสอบสิทธิ์ทั้งหมด					

ส่วนที่ 5 ข้อมูลความคิดเห็นและข้อเสนอแนะเกี่ยวกับตัวระบบ

.....

.....

.....

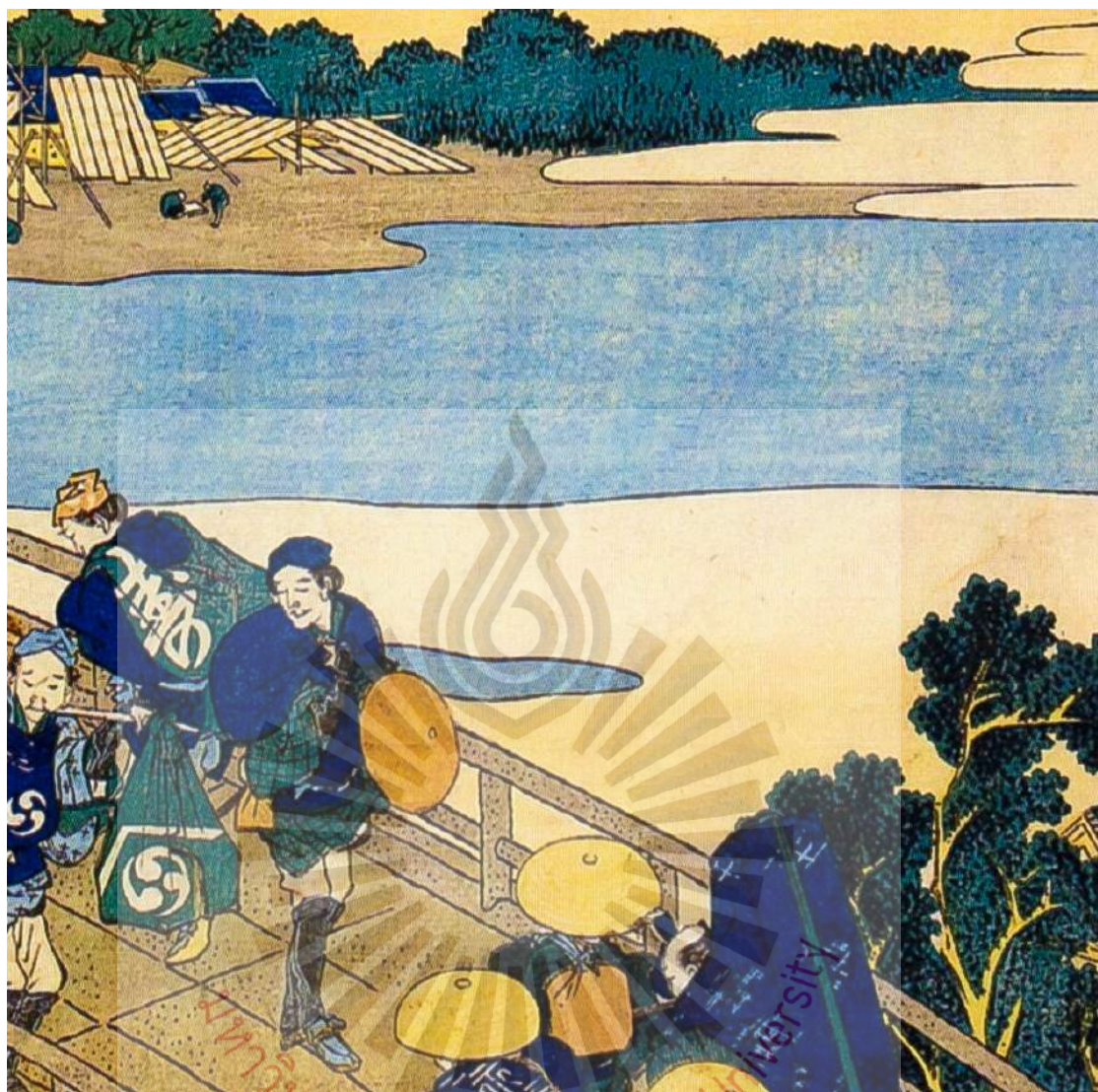
.....

.....

The logo of Rangsit University is a circular emblem. At the top is a stylized flame or sunburst. Below it, a circle is formed by numerous triangular rays of varying lengths, creating a sunburst effect. The text "มหาวิทยาลัยรังสิต Rangsit University" is written in a semi-circle at the bottom of the emblem.

ภาคผนวก ข

การเผยแพร่ผลงานวิจัยในงานประชุมวิชาการระดับนานาชาติ ครั้งที่ 1



The International Academic Forum

ACE/ACSET/AURS 2016

Art Center Kobe, Japan

iafor

The Asian Conference on Society, Education & Technology 2016

Official Conference Proceedings

ISSN: 2188-272X



© The International Academic Forum 2016
The International Academic Forum (IAFOR)
Sakae 1-16-26-201
Naka Ward, Nagoya, Aichi
Japan 460-0008
www.iafor.org

A Basic Study on a Task-based Style Foreign Language Learning Environment Using RFID and a 3DCG Character

Emi Shibuya

Min Kang

Kazuhiro Ohtsuki

Harumi Kashiwagi

pp. 123- 136

The Application of Analytic Hierarchy Process for the Evaluation of Imaginative Teaching Strategies

Shin Liao

Chao-Fu Yang

Chui-Chu Yang

Yi-Chen Pan

pp. 137 - 152

Development of an Introductory Programming Education System by Automatic Generation of Lecture Slides

Tatsuyuki Takano

Osamu Miyakawa

Takashi Kohama

pp. 153 - 158

A Reader of Gesture-Based Accessibility User Interface Design for Visually Impaired Children

Jin-Ting Jheng

Hsiao Ping Lee

Tzu-Fang Sheu

pp. 159 - 166

The Factors Affect Performance of Public Health Personnel Affiliated with Network Institute of Public Health and Medical Technology College toward ASEAN Communities

Tharin Sukanun

Hattaya Petcharoen

pp. 167 - 175

Measuring the Use of Twitter in Education

Fernando J. Garrigos-Simon

Juan Vicente Oltra-Gutiérrez

Yeamduan Narangajavana

Sofia Estellés Miguel

pp. 177 - 191

Software Model Design for Biometric Examiner Personal Verification

Sethapong Wong-In

Paniti Netinant

pp. 193 - 202

Conceptual Framework: A Mobile Software Model for Web Based Learning

Titiya Chomngern

Paniti Netinant

pp. 203 - 210

The Executive Council of the International Advisory Board

Mr Mitsumasa Aoyama
Director, The Yufuku Gallery, Tokyo, Japan

Lord Charles Bruce
Lord Lieutenant of Fife
Chairman of the Patrons of the National Galleries of Scotland
Trustee of the Historic Scotland Foundation, UK

Professor Donald E. Hall
Herbert J. and Ann L. Siegel Dean
Lehigh University, USA
Former Jackson Distinguished Professor of English and Chair of the Department of English

Professor Arthur Stockwin
Founding Director of the Nissan Institute for Japanese Studies & Emeritus Professor
The University of Oxford UK

Professor Chung-Ying Cheng
Professor of Philosophy, University of Hawai'i at Manoa, USA
Editor-in-Chief, The Journal of Chinese Philosophy

Professor Steve Cornwell
Professor of English and Interdisciplinary Studies, Osaka Jogakuin University, Osaka, Japan
Osaka Local Conference Chair

Professor A. Robert Lee
Former Professor of English at Nihon University, Tokyo from 1997 to 2011, previously long taught at the University of Kent at Canterbury, UK

Professor Dexter Da Silva
Professor of Educational Psychology, Keisen University, Tokyo, Japan

Professor Georges Depeyrot
Professor and Director of Research & Member of the Board of Trustees
French National Center for Scientific Research (CNRS) & L'Ecole Normale Supérieure, Paris, France

Professor Johannes Moenius
William R. and S. Sue Johnson Endowed Chair of Spatial Economic Analysis and Regional Planning
The University of Redlands School of Business, USA

Professor June Henton
Dean, College of Human Sciences, Auburn University, USA

Professor Michael Hudson
President of The Institute for the Study of Long-Term Economic Trends (ISLET)
Distinguished Research Professor of Economics, The University of Missouri, Kansas City

Professor Koichi Iwabuchi
Professor of Media and Cultural Studies & Director of the Monash Asia Institute, Monash University, Australia

Professor Sue Jackson
Professor of Lifelong Learning and Gender & Pro-Vice Master of Teaching and Learning, Birkbeck, University of London, UK

Professor Sir Geoffrey Lloyd
Senior Scholar in Residence, The Needham Research Institute, Cambridge, UK
Fellow and Former Master, Darwin College, University of Cambridge
Fellow of the British Academy

Professor Keith Miller
Orthwein Endowed Professor for Lifelong Learning in the Science, University of Missouri-St. Louis, USA

Professor Kuniko Miyana
Director, Human Potential Institute, Japan
Fellow, Reichsauer Institute, Harvard University, USA

Professor Dennis McInerney
Chair Professor of Educational Psychology and Co-Director of the Assessment Research Centre
The Hong Kong Institute of Education, Hong Kong SAR

Professor Brian Daizen Victoria
Professor of English
Fellow of the Oxford Centre for Buddhist Studies

Professor Michiko Nakano
Professor of English & Director of the Distance Learning Center, Waseda University, Tokyo, Japan

Professor Thomas Brian Mooney
Professor of Philosophy
Head of School of Creative Arts and Humanities
Professor of Philosophy and Head of School of Creative Arts and Humanities, Charles Darwin University, Australia

Professor Baden Offord
Professor of Cultural Studies and Human Rights & Co-Director of the Centre for Peace and Social Justice
Southern Cross University, Australia

Professor Frank S. Ravitch
Professor of Law & Walter H. Stowers Chair in Law and Religion, Michigan State University College of Law

Professor Richard Roth
Senior Associate Dean, Medill School of Journalism, Northwestern University, Qatar

Professor Monty P. Satiadarma
Clinical Psychologist and Lecturer in Psychology & Former Dean of the Department of Psychology and Rector of the University, Tarumanagara University, Indonesia

Mr Mohamed Salaheen
Director, The United Nations World Food Programme, Japan & Korea

Mr Lowell Sheppard
Asia Pacific Director, HOPE International Development Agency, Canada/Japan

His Excellency Dr Drago Stambuk
Croatian Ambassador to Brazil, Brazil

Professor Mary Stuart
Vice-Chancellor, The University of Lincoln, UK

Professor Gary Swanson
Distinguished Journalist-in-Residence & Mildred S. Hansen Endowed Chair, The University of Northern Colorado, USA

Professor Jiro Takai
Secretary General of the Asian Association for Social Psychology & Professor of Social Psychology
Graduate School of Education and Human Development, Nagoya University, Japan

Professor Svetlana Ter Minasova
President of the Faculty of Foreign Languages and Area Studies, Lomonosov Moscow State University

Professor Yozo Yokota
Director of the Center for Human Rights Affairs, Japan
Former UN Special Rapporteur on Myanmar

Professor Kensaku Yoshida
Professor of English & Director of the Center for the Teaching of Foreign Languages in General Education, Sophia University, Tokyo, Japan

Software Model Design for Biometric Examiner Personal Verification

Sethapong Wong-In, Rangsit University, Thailand
 Paniti Netinant, Rangsit University, Thailand

The Asian Conference on Society, Education & Technology 2016
 Official Conference Proceedings

Abstract

Nowadays the Examiner Personal Verification in most universities uses comparison methodology to match a physical appearance of examiner to a student ID card. This methodology is simple by it is easily lead to an examination cheating. For instances, some students' faces have been changed during study but their student ID cards are not up to date. Some students might hire another person to impersonate them for the examination. While some students may lost their student ID cards or student ID cards get damaged. By these, it is inevitable for the proctors to face the above problems. This paper proposes the applied Biometric Technology to the Examiner Personal Verification by using fingerprint to verify an identity. This paper tends to create a software model to solve the problem not specific to any university for general. Therefore, the software model is supposed to design to be the framework for a developer to develop software to suit each university standard in the future. To develop good and acceptable software, the software model should be designed based on a software design standard to ensure that our model shall follow and meet a quality standard. This paper is designed a software model based on IEEE standard for Information Technology-System Design-Software Design Descriptions (IEEE Std 1016TM-2009).

Keywords: Examiner Personal Verification System, Software Design, Biometric Technology.

iafor

The International Academic Forum
www.iafor.org

1. Introduction

Software model design for personal verification examiner of an examination using a biometric is a very important and essential process to every school, university, even institute or organization where there is a process to personal assessment. The only objective of examination is to assess competency of examiners or students. There are many processes in examination, for instances a preparing basic information, room, examiner list, proctors, data and time, etc. Besides, the one important process is an examiner personal verification that emphasizes on accuracy, clarity, convenience and speed.

Some academic institutes give a priority to an examiner personal verification, of which there are some problems and challenges. Raising up two problems are intentional cheating i.e. hiring another person to impersonate for the examination or forgery and unintentional cheating i.e. lost and damaged a student ID card, unmatching of a personal to a photo on card due to no update. The challenge in examiner personal verification is in case that there are such many examiners. Thus, it is a time consuming in a verification and may cause to some errors.

An examiner personal verification system (EPVS) is to cope with these problems and challenges, there is an idea to use IT to verify examiner personal identifications. The issue of problem can be divided into four levels: The infrastructure, managing, identifying, and reliability and by two points of view: non-IT, without information technology and IT views, with information technology as illustrates in figure 1.

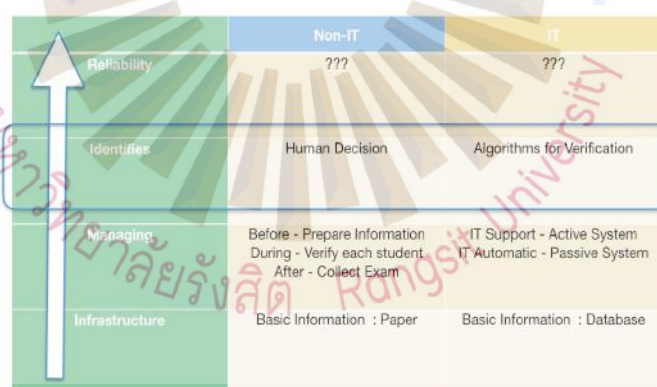


Figure 1: EPVS Problem issues

In an infrastructure level, this level concern about the infrastructure of Examiner Personal Verification System and basic information to verify examiners, the data preparation format are cared for. By the non-IT view, information is prepared in a paper base for an instance, a signed paper for examination participation while the IT view, a database is applicable. To transform non-IT view to IT view for this issue, have to prepare Information from every paper into computer base.

In a managing level, it is concern about how to control and manage the process in an examiner personal verification. By the non-IT view, proctors would verify a student ID card and a signed paper while the IT view can be verified in two ways: an active or a passive. Regarding of an active verification, an examiner has to react some activities to the system i.e. a finger scanning, a pressing, or any other activities depending on a specific IT system while a passive one, an examiner has no interaction with the system but the system itself will automatically verify, for instances, taking CCTVs to scan examiners' faces while queuing to enter the room. To transform non-IT view to IT view for this issue, have to analysis the non-IT process and reengineering it on term of computer process. This issue is very important because if the software designer understands every process of non-IT clearly they can design new system without mistake.

In an identifying level, it is concern about a methodology to verify examiners. By the non- IT view, proctors make decision by comparing a person with a photo affixed on a student ID card while in the IT view, various algorithms are applied for a decision making to verify the real examiner, and however it depends on a methodology in managing level. For non-IT identify examiner by human decision might have human error. Sometime the real examiner have the old student card, make the proctor confuse. To transform non-IT view to IT view for this issue will reduce the human error by using machine to make decision instead. Using machine for examiner verification have many methodologies such as: apply user and password, Smart card and biometric technology. Biometric technology is the good solutions to use what people have, the most biometric that used in many applications include: retina, fingerprint, palm, face, speech, iris, motion and others to the identified the real examiner (Uddin, N., et al., 2011).

In a reliability level, the accuracy and reliability of system are focused, as both non-IT and IT have to specify what index to be used and how reliable the index is. For biometric technology uses biometric error to measure the efficiency. Figure 1 show the issues that we could concern about in EPVS. Nowadays many University and school try to apply IT Solution into their work.IT Solution in the university have many system such as registration system, human resource system, account system, asset management system, class management system and the others. EPVS is sub-system of the University System but it more complicate than the other system.

2. Biometric Technology

An idea to bring Biometric Technology in verification and specifying identity is widespread used in many patterns and various organizations, for instances, security system, and people searching. BT is to use personal identity i.e. a fingerprint, a face, a hand geometry, an iris and a voice of which using BT in an examiner verifying can solve the problems such as a student ID card lost, a forgery, having an impersonate and verifying simultaneous of examiners.

Biometric technology can divide into 3 issues (Choudhary, J., 2012) include: physical biometric, behavior biometric and chemical biometric. Physical biometric is concern about physical measurement and include modalities such as face, fingerprints, iris-scans, hand geometry. Behavior biometric is concern about the way in which a user

performs such as speech, signature, gait, keystroke dynamics and other. Chemical biometric is concern about chemical cue measurement such as perspiration and smell.

An important question of a biometric technology is how the best we can use the biometric technology, regarding of a research (Prabhakar, S., Pankanti, S., & Anil J, 2003), there are a biometric technology in a comparison by five identities: a fingerprint, a face, a hand geometry, an iris and a voice as well as by seven indexes: barriers to an universality, a distinctiveness, a permanence, a collectability, a performance, an acceptability and a potential for a circumvention.

In figure 2, each biometric technology has different advantages and disadvantages. It is also stated that there is no a perfect biometric technology. The most efficiency to use a biometric technology depends on the methodology and the system characteristics, for instances, it is indicated that using a fingerprint and an iris can more identify a personal than using a voice. However, in tele-banking, the biometric technology by a voice is considered to use because a communication methodology is using a voice, for instance.

BIOMETRIC	FINGERPRINT	FACE	HAND GEOMETRY	IRIS	VOICE
					
Barriers to universality	Worn ridges; hand or finger impairment	None	Hand impairment	Visual impairment	Speech impairment
Distinctiveness	High	Low	Medium	High	Low
Permanence	High	Medium	Medium	High	Low
Collectability	Medium	High	High	Medium	Medium
Performance	High	Low	Medium	High	Low
Acceptability	Medium	High	Medium	Low	High
Potential for circumvention	Low	High	Medium	Low	High

Figure 2: Biometric Technology Comparison

The methodology to measure the biometric efficiency is biometric system error indicators that have 2 types of errors: False Match Rate (FMR), mistaking biometric measurements from two different persons to be from the same and False Non Match Rate (FMNR), mistaking two biometric measurements from the same person to be from two different persons. Both FMR and FMNR is less is more. Using FMR or FMNR to be the indicator is depending on what kind of application. For example the criminal Identified System use FMNR to identify the criminal, the security system might use FMR to identified person who have right to access.

To develop EPVS, with high quality, we have to develop software base on the standard. Software Development has life cycle call Software Development Life Cycle (SDLC) include: requirement collect, analysis, design, coding, testing, implement and evaluate. Each step has own standard and some standard is propose on different issue. The software development has many standards such as: European Space Agency (ESA), Institute of Electrical and Electronic Engineers (IEEE), and International Organization for Standardization (ISO), Capability Maturity Model Integration

(CMMI) by Software Engineering Institute Carnegie Mellon University USA, is focus on the document in software development process. ISO/IEC JTC 1/SC 7 Software and systems engineering have many standards and projects under the direct responsibility of ISO/IEC JTC 1/SC 7 such as: ISO 3535:1977 forms design sheet and layout chart, ISO 5806:1984 Information processing. ISO Standard has focus on the standard of international operator (Al-Qutaish, R., & Al-Sarayreh, K., 2008). Institute of Electrical and Electronics Engineers (IEEE) set the software development standard into many issue such as Standard of Software Requirement, Standard of Software Design, Standard of Software Testing, Standard of Software Quality Assurance and others. IEEE Software Standard is focus on the definition and concept of methodologies in software development. This paper is focus on software design methodology so we use Software & Systems Engineering Standards Committee to be standard.

Software design is very important, software designer have to create design model from user requirements. If the software design model have good quality it's easy to build software for the other rules in software development team. To develop the process view, the designer partitions the software into separate tasks (Kruchten, B., 1995).

Software design technique can divide into 3 techniques: process-oriented design technique, data-oriented design technique and object-oriented design technique (Yau, S., & JEFFERY, P., 1986).

The software design standard is to get an effective EPVS. It is necessary to develop a quality software. Nowadays the biggest problem in software development is what not developed to meet user's requirement. The cause of this problem is that there are various processes in software development which are information gathering, problem analysis, designing, coding, testing, installing, training including document making. It means to develop software, there need various personnel and roles whom possess different point of views in software development which sometime it is misinterpreted in communication and might cause the final results not meet users' requirement. Moreover, different roles may have their own views and might not be aware of the effect of other views which can cause to an error in software development.

Software Design by IEEE standard (Software & Systems Engineering Standards Committee, 2009) has specified view of software development as shown in figure 3 and indicated in different views in software development, a message conveying and giving an example of different charts.

Design viewpoint	Design concerns	Example design languages
Context (5.2)	Systems services and users	IDEF0, UML use case diagram, Structured Analysis context diagram
Composition (5.3) Can be refined into new viewpoints, such as: functional (logical) decomposition, and run-time (physical) decomposition.	Composition and modular assembly of systems in terms of subsystems and (pluggable) components, buy vs. build, reuse of components	Logical: UML package diagram, UML component diagram, Architecture Description Languages, IDEF0, Structure chart, HIPO Physical: UML deployment diagram
Logical (5.4)	Static structure (classes, interfaces, and their relationships) Reuse of types and implementations (classes, data types)	UML class diagram, UML object diagram
Dependency (5.5)	Interconnection, sharing, and parameterization	UML package diagram and component diagram
Information (5.6) with data distribution overlay and physical volumetric overlay	Persistent information	IDEFIX, entity-relation diagram, UML class diagram
Patterns (5.7)	Reuse of patterns and available Framework template	UML composite structure diagram
Interface (5.8)	Service definition, service access	Interface definition languages (IDL), UML component diagram
Structure (5.9)	Internal constituents and organization of design subjects, components and classes	UML structure diagram, class diagram
Interaction (5.10)	Object communication, messaging	UML sequence diagram, UML communication diagram
State dynamics (5.11)	Dynamic state transformation	UML state machine diagram, statechart (Harel's), state transition table (matrix), automata, Petri net
Algorithm (5.12)	Procedural logic	Decision table, Warmer diagram, JSP, PDL
Resources (5.13) May be refined into resource based viewpoints with possible overlays	Resource utilization	UML Real-time Profile, UML class diagram, UML Object Constraint Language (OCL)

Figure 3 : Software Design Viewpoint Standard by IEEE

From figure 3, there are many views in software development and current charts are unable to cover all views causing to the problems mentioned earlier. The research presents an idea to compile different views in software development to be closest to one chart by presenting with Information Flow Diagram (IFD). By IFD, it can present in view of Context Logical Dependency Information Interface State Dynamic Resource in one chart of which the advantages are: all roles can see an overview of software development, operation between modules or processes, and effect in changing some point in one chart. Example of IFD is indicated in figure 4.

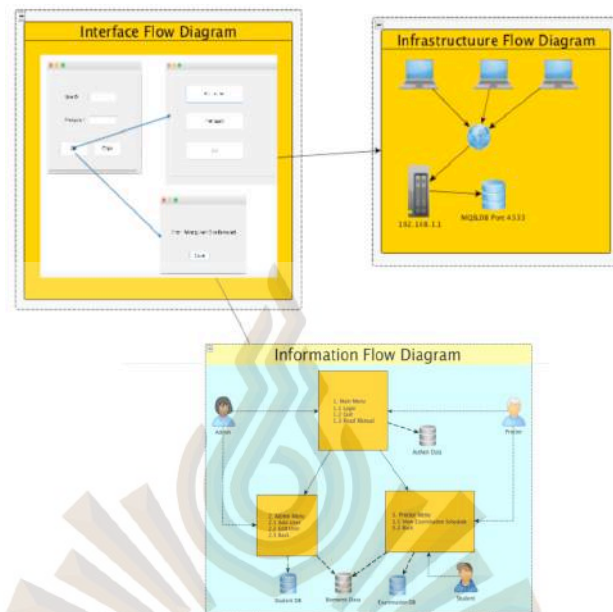


Figure 4: Example of IFD Figure

From figure 4, three diagrams include information flow diagram, interface flow diagram and infrastructure flow diagram show in one picture. The Information flow diagram show the information that use in each interface and show its flow to the next interface. It's also show the interactive between user and process. Interface flow diagram show the graphic user interface flow that can make user more understand how to use software than user manual in term of document. Interface flow diagram can reduce the gap of understand between user and software developer because user can see the final result of software development. The old school traditional software development uses the software prototype to show to the user. Software Prototype can make user see the final design of software but if user want to change something it's difficult to change in Prototype. Figure 4 also show the infrastructure flow diagram to make the implementer understand how to install the software into server and configuration the system and network. Three diagrams are the sample of multi-viewpoint in software design that can reduce the complex ability and gap of understand.

3.EPVS Framework

In order to develop the EPVS with the quality we not only focus on the software design but also concern on the whole picture of the examination system.

Framework in developing EPVS software system is comprised of 6 main issues and shown in figure 5 as horizontal axel stands for Physical Device while vertical axel stands for Methodology.

Issue 1: Examiner Information – considers information of examiner, method and process in data collection and storage. This issue is concern about what the examiner information is and how to gather them in to the system. Sometime the huge number of the examiner spent process time too much if we have not prepared the good methodology for gathering the data.

Issue 2: Examination Information System (EIS) – considers on an examination management system of which EPVS is part of this huge system. This system has to prepare exam room, exam schedule management and management in other issues. EIS also manage the examination both the examination room assignments and the examination proctor assignments in each room (Vasupongayya, S., Noodam, W., Kongyong, P., 2013). This issue concern about how to connect the EPVS with the legacy system in each university. Sometime the legacy system in the university is very old and closes system; sometime have non-IT system.

Issue 3: The Result/ Output – consider an outcome from EPVS system i.e. outcome format, quality and reliability. This issue concern about the output that sent out from the EPVS, Some university concentrates on the accuracy to be the first priority and processing time is the second. Some university focuses on the ease of use.

Issue 4: Biometric Technology – considers about format and algorithm. This issues concern about which algorithm applied in EVPS. It's depends on what type of biometric that EPVS use. In the same biometric technology also have many algorithm such as: Face recognition use neural network, Eigenfaces, Independent Component Analysis and the others, fingerprint use the correlation-based techniques and minutiae for alignment (Mir, A. ,H. , Rubab, S. , Jhat, Z. 2011).

Issue 5: EPVS – consider how to connect BT with EIS and how it works together in each process. This issue concern about how to connect the biometric device with the examination information system. Each type of biometric has many devices and many vendors.

Issue 6: Intelligence System – considers applying intelligence system using high technology equipment. This issue concerns about how to make the EPVS to be the intelligence system or expert system by make it more automatic and passive system. For example, apply new model of CCTV with facial recognition function while the examiner walk into the examination room CCTV will verify each examiner automatically, apply mobile with fingerprint scan function to be the device instead signing name on paper. The Intelligence System issue can applied into remote access for online testing (Rodchua, S., Yiadom-Boakye, G., Woolsey, R. ,2011) for online learning student.

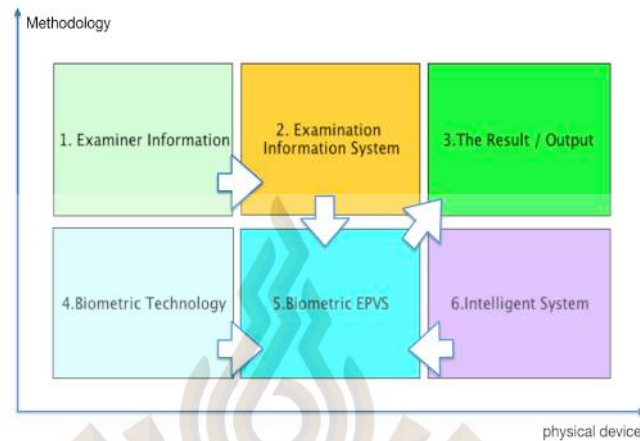


Figure 5: Framework in developing EPVS software system

Conclusion

In conclusion, solution to solve the problem in identifying the examiner by using Biometric, need a model framework in development. To develop good software to meet users' requirement, it is necessary to meet the standard, in which here is referred to IEEE Software Design Standard that be specified many points of view in design. Efficient Software Design may lead to an efficient System Development. Therefore, to make the Design more efficient, this research presents a way in software design by using Information Flow Diagram which presenting many points of view to make the relevant personnel to see the same view in order to reduce any misunderstanding in software design.

IFD in this paper is just the example of using multi-viewpoint for software model design. It still has to complete the notations and rules in the future. The IFD has the concept of using diagrams based on the interoperate information between modules, user and anything in term of information.

References

- Mir, A. ,H. , Rubab, S. , Jhat, Z., A. (2011), Biometrics Verification: a Literature Survey , *Journal of Computing and ICT Research*, 5(2), 67-80.
- Prabhakar, S. , Pankanti, S. , Anil, J. (2003) , Biometric Recognition: Security and Privacy Concerns, *IEEE SECURITY & PRIVACY MARCH/APRIL* , 1(2) , 33-42.
- IEEE Standard for Information Technology—Systems Design— Software Design Descriptions, *IEEE Standard 1016*, 2009.
- Rodchua ,S ., Yiadom-Boakye, G., Woolsey,R. (2011), Student Veri cation System for Online Assessments: Bolstering Quality and Integrity of Distance Learning, *Journal of Industrial Technology* , 27(3), 1-8.
- Vasupongayya, S., Noodam, W., Kongyong, P. (2013), Developing Examination Management System : Senior Capstone Project, a Case Study, *World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Information Engineering* , 7(7), 1046-1052.
- Philippe, B. Kruchtenr (1995) , The4+1View Model of Architecture , *IEEE Software*, vol. 12 (6), 45-50.
- Choudhary ,J. (2012), Survey of Different Biometrics Techniques, *International Journal of Modern Engineering Research (IJMER)*, 2(5), 3150-315,.
- Uddin,M.,N., Sharmin,S., Shohel,H.,A. , Hasan,E., Hossain,S., Muniruzzaman (2011), A Survey of Biometrics Security System, *IJCSNS International Journal of Computer Science and Network Security*, 11(10) , 16-23.
- Yau, S., S., JEFFERY, J.,P. (1986),A Survey of Software Design Techniques , *IEEE Transactions on software Engineering*, 12(6), 713-721.
- Al-Qutaish,E.,R., Al-Sarayreh,K.(2008), Software Process and Product ISO Standards: A Comprehensive Survey, *European Journal of Scientific Research*, 19(2),289-303.

Contact email: sethapongw@tmail.com, netinant1@gmail.com

ภาคผนวก ค
การเผยแพร่ผลงานวิจัยในงานประชุมวิชาการระดับนานาชาติ ครั้งที่ 2



**PROCEEDINGS OF
2017 International Conference
on Information Technology
(ICIT 2017)**



มหาวิทยาลัยรังสิต Rangsit University

**Singapore
December 27-29, 2017**



Proceedings of

The International Conference on Information Technology

ICIT 2017

Singapore

December 27-29, 2017





The Association for Computing Machinery
2 Penn Plaza, Suite 701
New York New York 10121-0701

ACM COPYRIGHT NOTICE. Copyright © 2017 by the Association for Computing Machinery, Inc. Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Publications Dept., ACM, Inc., fax +1 (212) 869-0481, or permissions@acm.org.

For other copying of articles that carry a code at the bottom of the first or last page, copying is permitted provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, +1-978-750-8400, +1-978-750-4470 (fax).

ACM ISBN: 978-1-4503-6351-8



Nattika Chunsuttiwat, Nithinant Thammakoranonta

Multidimensional Application Grade of Interconnected and Locally Administered Services (MAGILAS): A Management Information System of Ifugao State University.....195

Roger S. Tamargo, Domingo Junior P. Ngipol, Thelma D. Palaoag, DIT

Comparison BER with the Different Stack-up PCB of KOSMOS Micro-server System Interconnection Module Supporting 800Gbps Bandwidth.....201

Hyukje Kwon, Ziho Shin, Won-ok Kwon, Hag-Young Kim, Dongjae Kang

Event Management Solution Using Web Application Platform206

Maria Rona L. Perez, Ace C. Lagman, Rossana T. Adao

Software engineering and multimedia technology

Empirical Study of Multimedia Learning Object to Enhance Introductory Programming Learning212

Matthews, R, Hew, S.H, Koo, A.C

Exploring Facebook for Sharing Crime Experiences Using Selenium and Support Vector Machine.....218

Ken D. Gorro, Mary Jane G. Sabellano, Christian V. Maderazo, Angie M. Ceniza, Kim Gorro

The study for Early warning mechanism of public opinion for emergency based on the new media field effect223

Longbao Mei, Libin Cai, Hao Zhang

Spatio-Temporal Visualization Model for Movie Success Prediction Based on Tweets227

A. W. M. K. S. A. Wijekoon, T. C. Sandanayake, K. D. A. A. Jayawardena, A. L. Y. Buddhini,

U. K. D. G. S. Ariyawansa

The Concept Design of House Bookkeeping Software Using Aspect Oriented Approach232

Meennapa Rukhiran, Paniti Netinant

Revised Software Model Design for Biometric Examiner Personal Verification System.....237

Sethapong Wong-In, Paniti Netinant

A Mobile Software Model for Web-Based Learning Using Information Flow Diagram (IFD)243

Titiya Chomngern and Paniti Netinant

Path Coverage Information for Adaptive Random Testing248

Arnaldo Marulitua Sinaga, Oscar Daniel Hutajulu, Ruth Tabita Hutahaeen, Ida Christy Hutagaol

Kids Menu Care: An Application for Food Menu Scheduling with Caloric Balance253

Syefrida Yulina, Dewi Hajar

Cultural characteristics of architectures in the Game Scenic Design258

Wei Wang

Committees

Advisory Board

Prof. Chin-Chen Chang, IEEE and IET Fellow, Feng Chia University, Taiwan

Conference Chair

Prof. Maode Ma, Nanyang Technological University, Singapore

Organizing Committee Chair

Prof. Lipo Wang, Nanyang Technological University, Singapore

Program Chairs

Prof. Xudong Jiang, Nanyang Technological University, Singapore

Assoc. Prof. Xuefeng Liang, Kyoto University, Japan

Technical Program Committee

Prof. Mary Mehrnoosh Eshaghian-Wilner, University of Southern California, USA

Dr. Feiyun ZHU, University of Texas, USA

Dr. P. Raviraj, Kalaingar Karunanidhi Institute of Technology, India

Assoc. Prof. Dr. Ismail Rakip Karas, Karabük University, Turkey

Prof. Karbhari V. Kale, Babasaheb Ambedkar Marathwada University, India

Prof. Surekha Kamath, Manipal Institute of Technology Manipal, India

Prof. Mohammad Shorif Uddin, Jahangirnagar University, Bangladesh

Senior Lecturer Hamid A. Jalab, University of Malaya, Malaysia

Assoc. Prof. J. Jennifer Ranjani, SASTRA University, India

Dr. Teodoro Macaraeg Jr., University of Caloocan City (UCC), Philippines

Assoc. Prof. Dr. Zarinah Binti Mohd Kasirun, University of Malaya, Malaysia

Prof. G. Raju, Kannur University, India

Assoc. Prof. Dr. V. Santhi, VIT University, India

Dr. Yumnam Jayanta Singh, Director, National Institute of Electronics & Information Technology, India

Dr. Prasenjit Sen, Symbiosis Centre for IT, India

Dr. Rochelle D. Pacio, PKFokam Institute of Excellence, Philippines
 Assoc. Prof. Omaira Nomir, Mansoura University, Egypt
 Lecturer Supaporn Chairungsee, Walailak University, Thailand
 Dr. Ramya M, Coimbatore Institute of Technology, India
 Prof. Priyanka Sharma, Raksha Shakti University, India
 Asst. Prof. Dr. Pu-Tai Yang, Tunghai University, Taiwan
 Prof. Rajeswari A, Coimbatore Institute of Technology, India
 Dr. Charoenchai Wongwatkit, Mae Fah Luang University, Thailand
 Asst. Prof. Ramya M, Coimbatore Institute of Technology, India
 Asst. Prof. Chung Yung, National Dong Hwa University, Taiwan
 Prof. Gaurav Tejpal, shri venkateshwara university gajraula, India
 Prof. Guoyue Chen, Akita Prefectural University, Japan
 Asst. Prof. Nithinant Thammakoranonta, National Institute of Development Administration, Thailand
 Assoc. Prof. Dr. Deok-Joo Lee, Seoul National University, Korea
 Assoc. Prof. Vijay Kale, Visvesvaraya National Institute of Technology, India
 Asst. Prof. Dr. DARICHA SUTIVONG, Chulalongkorn University, Thailand
 Prof. G. ANJAN BABU, Sri Venkateswara University, India
 Assoc. Prof. Dr. Gurdal Ertek, Abu Dhabi University, UAE
 Dr. Sonal Sharma, Uttaranchal University, India
 Prof. Jean Paul Van Belle, University of Cape Town, South Africa
 Dr. Reginamary Matthews, The University of Nottingham, Malaysia
 Prof. Dr. Gaurav Tejpal, Amritsar College of Engineering & Technology, India
 Asst. Prof. Dr. Chung Yung, National Dong Hwa University, Taiwan
 Dr. Iskandar Bin Ishak, Universiti Putra Malaysia, Malaysia

Revised Software Model Design for Biometric Examiner Personal Verification System

Sethapong Wong-In

College of Information and Communication
Technology, Rangsit University, Phaholyothin Road,
Lak-Hok, Mueng, Phatumthani 12000, Thailand
sh1nes@hotmail.com

Paniti Netinant

College of Information and Communication
Technology, Rangsit University, Phaholyothin Road,
Lak-Hok, Mueng, Phatumthani 12000, Thailand
paniti.n@rsu.ac.th

ABSTRACT

Nowadays educational institutes use information technology in administration and management in various ways. One of activities is to verify examiners. The current verification of examiner identity is to check documents for instances: identification cards, student cards, and signatures. Concepts to apply biometric technology are more efficient options. It is necessary to design the software comprehensively and evidently for an efficient system. Our conceptual framework of the examiner personal verification system is to adapt biometric technology for Biometric Examiner Personal Verification System (BEPVS). Our system design is divided into six components. This paper presents deeply of these six components to be used as a software design model for BEPVS software design and development. The revised software model design for BEPVS can also be divided into thirteen sub-component. This paper also presents the semantic and workflow of each revised BEPVS component.

CCS Concepts

- Software and its engineering → Software system models
- Software and its engineering → Software system structures
- Software and its engineering → Abstraction, modeling and modularity.

Keywords

Examiner Personal Verification System, Biometric Technology, Software Model Design, IEEE Systems Design.

1. INTRODUCTION

Even though information technology systems is applied to use in many activities in educational institutes such as financial systems or back-end systems, verifying examiners of each class in university still has some challenges to concern about. The examiner verification problems can be divided into three main issues: how to check examiners identification, how to manage the verification processes, and how to cope with appropriated technology. The first issue concerns about the precision of

verification, for example, how can proctors ensure whether the examiner is the right person for each student identification. Especially in case of the proctors are third party, they can't be able to identified examiners. The second issue is to manage verification process. There are many tasks in the verification processes. Some educational institutes verify examiners by checking their documents such as student card, personal card, sometime driven license card and passports. In some case, when some examiners lose their documents or their documents are unclear, it might take time to use an optional plan to verify. It can cause to make queuing problem. Moreover having many verification steps are time consuming. The last issue is no appropriated technology applied in an examiner verification at present. There is some technology to applied in the verification such as RFID and smart card to reduce the processing time but the precision issue still has questionable.

This paper presents concept to apply biometric technology to verify examiners by developing the software design of Biometric Examiner Personal Verification System (BEPVS). The output is the BEPVS design model that can be used in general education institute to verify examiners. The BEPVS developing is based on IEEE Standard for Information Technology—Systems Design—Software Design Descriptions (SDD) to make sure that our model is based on standard and meet an efficiency system.

The remainder issues are shown as follows. In section 2, IEEE Standard for Information Technology - Systems Design--Software Design Descriptions [1], explains the software design standard to use as a design framework in this paper. The examiner verification methodology in education institute explains the methodology of examiner personal verification in education institutes. A biometric technology explains the biometric technology use in the examiner personal verification. Section 3 introduces the biometric examiner personal verification system conceptual framework (BEPVS Conceptual framework). Section 4 describes the revised BEPVS framework in two issues include the semantic and workflow of BEPVS. Section 5 presents the conclusions and future work.

2. RELATED WORK

2.1 Software Model Design

To develop good quality software developers must have a good design model. At present, Bhuvaneswari [2] survey the software development life cycle model and present many SDLC models such as waterfall model, incremental model, object-orient model and etc. Sarker [3] 's papers surveys the SLDC models and describes the advantages and disadvantages of each model however it's difficult to decision which model is the best. The

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

ICIT 2017, December 27–29, 2017, Singapore, Singapore

© 2017 Association for Computing Machinery.

ACM ISBN 978-1-4503-6351-8/17/12...\$15.00

DOI: <https://doi.org/10.1145/3176653.3176678>

methodology to measure the quality of software is complicated and hard to measure. Lee [4] presents the software measurement and software metrics in software quality to be the methodology in order to measure the quality of software.

This paper concentrates on software model designing for BEPVS. The output is the BEPVS model to be used in general education institute.

Valiallah [5] presents the software architecture viewpoint surveys and explain the meaning of each viewpoint for software design. Using the right viewpoint is very important in software design thus this paper uses the design viewpoint in IEEE to standard. IEEE Standard for Information Technology--Systems Design--Software Design Descriptions (IEEE SDD) has been developed to be a framework of the software designer to use as a standard for design the efficiency software that meets the requirements. IEEE SDD presents twelve design viewpoints, each viewpoint indicates each semantic in software design as shown in Table 1. Each design viewpoint has own a design concern to describe the semantic of the viewpoint. The Table 1 also presents the example of the designed tools use to show each viewpoint. The BEPVS software design model uses IEEE SDD as a framework to the design in each viewpoint in order to ensure the model is efficient.

2.2 Examiner Verification Methodology in Education Institute

In the most education institutes use an information system in a term of personal management or a back-end system management such as e-SMS (electronics School Management System) in Macedonia [6]. It uses e-SMS to manage subject, schedule, inventory, library, and personal management but not have any function for any examiner verification. The Examination scheduling system in school in Malaysia, Danlami [7], is developed for arranging examination for student. E-School, the school management system in Malaysia [8], also uses them to help many tasks in school. However, it can't verify the examiner. Most school management software in the market also has the similar functions but none of them has any function to verify examiners. In Thailand, the methodology in verifying the examiner is still non-IT and semi-IT function. Semi-IT means institutes have information system to manage examiners information but have no function for examiners verification. The system will provide the proctor the examiner information such as the examination schedule and the examiner list. On the other hand, non-IT means institutes have no information system.

2.3 Rapid Applications Development

RAD is the software development life cycle that faster than the others and gives a high-quality software. Naz [9] compare RAD with the other software development method, such as CBD mode, RepoGuard, Dynamic addition in agile, Framework for agile SOA development, and others models. According to Naz 's work, even though RAD uses less time and less requirement but the quality of software form RAD is a high quality. The BEPVS model design use a RAD as a framework to save time and still keep a good quality.

2.4 Biometric Technology

Nowadays, many tasks use biometric technology for many purposes to authenticate, to verify, and to classify by using individual identity such as facial, palm, voice, retina, iris, and

motion. The most advantage of biometric technology is hard to counterfeit and to fail. The popular question for using biometric technology is which one be the best biometric. Sruthy [10] mentioned in his paper that no a single biometric can effectively meet the requirements of all applications. That means each biometric technology has its strength and weakness. In Table 2, show the comparison of the biometric technologies efficiency in three issues including: security level, user acceptance and hardware.

Table 1. IEEE systems design--software design descriptions(SDD) viewpoint.

Design viewpoint	Design concerns	Example design languages
Context	Systems services and users	IDEF0, UML use case diagram, Structured Analysis context diagram
Composition (Can be refined into new viewpoints, such as: functional (logical) decomposition, and run- time (physical) decomposition.	Composition and modular assembly of systems in terms of subsystems and (pluggable) components, buy vs. build, reuse of components	Logical: UML package diagram, UML component diagram, Architecture Description Languages, IDEF0, Structure chart, HIPO Physical: UML deployment diagram
Logical	Static structure (classes, interfaces, and their relationships) Reuse of types and implementations (classes, data types)	UML class diagram, UML object diagram
Dependency	Interconnection, sharing, and parameterization	UML package diagram and component diagram
Information with data distribution overlay and physical volumetric overlay	Persistent information	IDEF1X, entity-relation diagram, UML class diagram
Patterns	Reuse of patterns and available Framework template	UML composite structure diagram
Interface	Service definition, service access	Interface definition languages (IDL), UML component diagram
Structure	Internal constituents and organization of design subjects, components and classes	UML structure diagram, class diagram
Interaction	Object communication, messaging	UML sequence diagram, UML communication diagram
State dynamics	Dynamic state transformation	UML state machine diagram, state chart (Harel's), state transition table (matrix), automata, Petri net
Algorithm	Procedural logic	Decision table, Warnier diagram, JSP, PDL

Resources May be refined into resource based viewpoints with possible overlays	Resource utilization	UML Real-time Profile, UML class diagram, UML Object Constraint Language (OCL)
--	----------------------	---

Table 2. The comparison of the 3 issues of biometric technology in a different method

Method	Security level	User Acceptance	Hardware
Fingerprint	High	Medium	Special, cheap
Facial	Medium	Medium	Common, cheap
Hand geometry	Medium	Medium	Special, mid-price
Voice	Medium	Medium	Common, cheap
Iris scan	High	Medium	Special, expensive
Signature	Medium	Medium	Special, mid-price
Keystroke	Medium	Medium	Special, cheap
Machine vision based gait	Medium	Medium	Special, cheap
Floor sensor based gait	High	Medium	Expensive
Wearable sensor based gait	High	Medium	Special, cheap

According to Table 2, using biometric technology in the examiner personal verification system for each educational institute might be different methods depend on some criteria of each institute. Hence the software design model of BEVPS should be flexible to adapt biometric methods.

3. OUR APPROACH

The main propose of our approach is to create the software design model for any educational institute in order to verify the examiner with a biometric technology.

3.1 BEPVS Conceptual Framework

The conceptual framework of BEPVS by Sethapong [11] is developed by showing general tasks in many education institutes and focus on the task that concerns about the examination. Using biometric technology to verify person is widely spread but not famous in the examination system. Thus this framework is present the brand new concept to use a biometric technology in the examination information management system.

BEPVS conceptual framework can be divided into six important components that show in Figure 1.

3.1.1 Examiner Information (EI component)

This component focuses on the information of examiner and the methodology to acquire. EI component focuses on the definition of examiner information. EI also concentrates how to collect the examiner information.

3.1.2 Examination Information System (EIS component)

This component focuses on the system to manage information of examination. In the semi-IT System institute is hard to define the boundary of their system, some institute have only back-end system without examiner manage system. EIS component concentrates only the systems that manage the examiner information.

3.1.3 Result/Output component

This component focuses on the output from verification system. Sometime educational institutes want different result from verification system, some institute want only final result while others need to view the detail.

3.1.4 Biometric Technology (BT Component)

This component focuses on biometric technology that applies in the system. BT component concerns about how to connect the biometric device, what the type of information come from the biometric device.

3.1.5 Biometric EVPS (BEPVS)

This component focuses on the methodology to apply the biometric into the system. BEPVS component is the main component which focuses on the examiner verification using biometric technology. This component concerns about how to verify the examiner with the biometric information from BT component and which algorithm.

3.1.6 Intelligent System component

This component focuses on the future work that concentrates on the way to apply new technology into the system such as new smart device or new CCTV.

Below figure, Y and X axis are stand for methodology and physical device respectively.

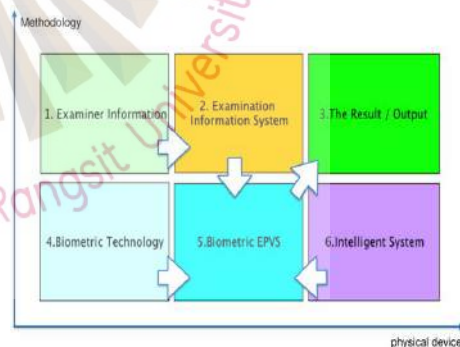


Figure 1. BEPVS conceptual framework.

3.2 Using Biometric for Examiner Personal Verification System

The use of biometric technology to verify the person is a tool that is extremely high performance and widely used in the current. To apply the biometric technology to use in the system for the examination task of educational institutions needs to be aware of the elements of the task in the education institutions. The issue to

apply the biometric technology is divided into two parts: Select the biometric method and choose the right algorithm.

3.2.1 Select the Biometric Method

To select the biometric method, it can be used any part of the body such as fingerprint, iris, facial, palm or human behavior such as motion and keystroke. Hence selecting the biometric method be related to biometric data stored in the system and the connection of the devices to the computer system, it is important to consider carefully.

3.2.2 Choose Biometric Algorithm

After selecting the biometric method, it is then needed to choose right algorithm to verify the biometric information. Uddin [12] explains how each biometric method works and also explain its process which includes input process, feature extraction process, and recognition process. As a process of each biometric method has different algorithms, our model is designed to provide various algorithms.

4. REVISED BEPVS MODEL

To revise BEPVS conceptual framework as shown in Figure 1 base on IEEE SDD, the revised framework of BEPVS presents the design model in term of context design viewpoint. Our concerns are the system services, structure design viewpoint, internal constituents, and organization of design subjects of the system. This revised framework also presents some piece of the interaction design viewpoints that concern about the communication between components. The revised BEPVS can be divided into thirteen components as shown in Figure 2.

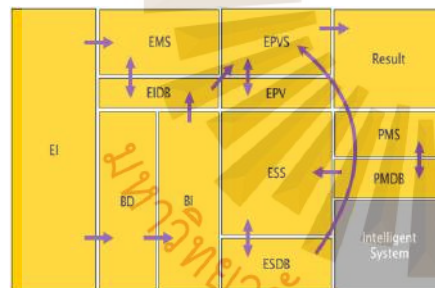


Figure 2. Revised BEPVS Diagram.

4.1 Revised Semantic

From figure 2 presents revised a BEPVS diagram divided into thirteen components. The diagram shows the connection between each component.

4.1.1 EI (Examiner Information)

This component explains the methodology of information collection and identifies the detail and format of the basic of examiner information. The basic examiner information includes prefix, first name, last name, gender, examiner id and etc.

4.1.2 EMS (Examiner Management System)

This component is the System that manages the examiner's information. Main function of this component is to manipulate information with examiner information database component (EIDB). Normally education institutes have their own EMS but some places still use manual system. For example, Vasupongayya [13] presents the Examiner Management System

(EMS) that provides examination schedule management services using in Prince of Songkla University in Thailand.

4.1.3 EIDB (Examiner Information Database)

This component describes about database that contains the examiner data.

4.1.4 BD (Biometric Device)

This component explains the biometric devices or tools to collect biometric information from the examiner. For example, some education institutes uses facial image for biometric information, so they will identify which device will apply to the system. Biometric device developments go very fast, Blasco [14] survey report shows the several of wearable biometric device that mean BD component have to follow the current biometric device technology to work with BEPVS.

4.1.5 BI (Biometric Information)

This component explains the format and biometric information from the biometric device. For example if education institutes decides to use facial image, they need to identify the format of facial image such as the resolution and the dimension of the facial image. BI and EI are needed to complete examiner information for BEPVS.

4.1.6 EPVS (Examiner Personal Verify System)

This component explains functions of the verification system such as information preparation before verification, verification processing result and report summarizing of verification result.

4.1.7 EPV (Examiner Personal Verification)

This component explains how the biometric technology works in BEPVS. It also explains which algorithm is used to verify biometric information in the system.

4.1.8 ESS (Examiner Schedule System)

This component explains the functions of the examination schedule system.

4.1.9 ESDB (Examiner Schedule Database)

This component describes the database which contains examination schedule information.

4.1.10 PMS (Proctor Management System)

This component explains functions of proctor management system.

4.1.11 PMSDB (Proctor Management Database)

This component explains the proctor management database

4.1.12 Result

This component explains the format of verified-output from EPVS.

4.1.13 Intelligent System

This component explains the future work and how to apply intelligent technology into BEPVS.

4.2 Revised Work Flow

From the revised BEPVS diagram in Figure 2, it shows the BEPVS revised framework can be divided into thirteen components. This Revised framework begins with Examiner Information (EI) component containing the examiner information to use in the system and methodology to collect the examiner information. There are two types of examiner's information be used in our model. The first type is basic information, i.e. prefix,

first name, last name, gender, examiner id, etc., which will be provided by Examiner Management System (EMS) component. The second type is biometric information, i.e. fingerprint, facial image, iris voice, palm, etc., can be collected via biometric device which provide by Biometric Device (BD) component. BD component describes the biometric device that be used in the system such as fingerprint scanner for examiner fingerprint, digital camera for examiners facial image, and etc. The Biometric Information (BI) component from BD is similar to EI which explains examiners information in term of basic information while BI explains examiner information in term of biometric information. If some education institutes have only basic information of examiner they can develop only BD component to collect complete examiner information for BEPVS. Both EI and BI are stored in EIDB.

The essential information for examination is the examination schedule that provides in Examiner Schedule System (ESS) component. ESS focuses on how to manage the examination schedule, such as examination room, and examination schedule. Examination schedule Information will be stored in Examination Schedule Database (ESDB) component. Proctor Management System (PMS) component is the system that manages proctors. Some education institutes hire external proctors, so PMS is needed to manage their information and store proctors information in Proctor Management Database (PMDb) component. To verify examiner using BEPVS, Examiner Personal Verification System (EPVS) component will prepare a basic information including examination schedule from ESSDB and examiner list from EIDB. Before the examiners access the examination room, the proctor will use biometric device to verify biometric information of each examiner and send it to Examiner Personal Verification (EPV) component. EPV of each system may have different methodology to extract biometric information. However, it depends on the appropriateness of each education institute. EPV will verify each examiner's biometric information and send back the result to EPVS component. Then EPVS will collect the result, summarize and then send it to Result component.

5. FUTURE WORK AND CONCLUSION

The revised BEPVS's purpose is to develop the software model design to use in BEPVS in general education institute. Our model can be divided into thirteen components which are explicitly and clearly explained how each component is about and how it works. This model also indicates the workflows of BEPVS showing the connection among components. For actual implementation of BEPVS in any education institute based on IEEE SDD standard, the developers can adapt components of the model to optimize the BEPVS for their own system. For example, some institutes want to use a facial recognition to verify examiners, they can change only the EPV component while the other components are remained the same. Our future work is to complete the software model design by create the rest of the design viewpoint such as user interface, and database systems. Implement the BEPVS design model in various educational institutes is still the challenge to prove that our model meets a sufficiently efficiency.

6. REFERENCES

- [1] IEEE Standard for Information Technology--Systems Design--Software Design Descriptions. (n.d.). doi:10.1109/ieeestd.2009.5167255.
- [2] Bhuvaneswari, T., Prabakaran, S. (2013). A Survey on Software Development Life Cycle Models. *International Journal of Computer Science and Mobile Computing*, 2(5), 262 - 267.
- [3] Sarker, I. H., Faruque, F., Hossen, U., & Rahman, A. (2015). A Survey of Software Development Process Models in Software Engineering. *International Journal of Software Engineering and Its Applications*, 9(11), 55 - 70. doi:10.14257/ijseia.2015.9.11.05.
- [4] Lee, M. (2014). Software Quality Factors and Software Quality Metrics to Enhance Software Quality Assurance. *British Journal of Applied Science & Technology*, 4(21), 3069-3095. doi:10.9734/bjast/2014/10548.
- [5] Valiollah, O., Seyyed, A., Razavi, E. (2013). Software Architecture Viewpoint Models: A Short Survey. *ACSIJ Advances in Computer Science: an International Journal*, 2(5), 55 - 62.
- [6] Majlinda, F., Bekim, F., & Mirlinda, E. (2013). Devising a model of electronic School Management System based on web services for secondary schools in Macedonia, *Proceedings of the ITI 2013 35th International Conference on Information Technology Interfaces, Cavtat, 2013*, 187 - 192.
- [7] Danlami, M., Fadhilah, A., Zarina, M., Hasni, H., & Aznida, H.Z. (2014). Examination Scheduling System Based on Quadratic Assignment, *Proceedings of the Third International Conference on Informatics & Applications*, 64 - 71.
- [8] Al-hayek, A., Hijazi, F., Mualiq, J. A. (2016). E- School – School Management System. Retrieved September 15, 2017, from <http://dspace.up.edu.ps/xmlui/handle/123456789/209>
- [9] Naz, R., Khan, M. N. (2015). Rapid Applications Development Techniques: A Critical Review. *International Journal of Software Engineering and Its Applications*, 9(11), 163 - 176. doi:10.14257/ijseia.2015.9.11.15
- [10] Sruthy S. (2013). Literature Survey on Automated Person Identification Techniques, *International Journal of Computer Science and Mobile Computing - IJCSMC*, 2(5), 232 - 237.
- [11] Wong-In, S., Netinant, P. (2016). Software Model Design for Biometric Examiner Personal Verification, *The Asian Conference on Society, Education & Technology*, 193 - 202.
- [12] Uddin, M.N., Sharmin, S., Shohel, H.A., Hasan, E., & Hossain, S., Muniruzzaman. (2011). A Survey of Biometrics Security System, *IJCSNS International Journal of Computer Science and Network Security*, 11(10), 16 - 23.
- [13] Vasupongayya, S., Noodam, W., & Kongyong, P. (2013). Developing Examination Management System: Senior Capstone Project, a Case Study, *World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Information Engineering*, 7(7), 1046 - 1052.
- [14] Blasco, J., Thomas, M.C., Tapiador, J., Peris-Lopez, P. (2016). A Survey of Wearable Biometric Recognition Systems. *ACM Computing Surveys (CSUR)*, 49(3), 43: 1 - 43: 35. doi:10.1145/2968215.
- [15] Netinant, P. (2015). Design adaptability for multilingual mobile application software, presented at the 24th

- International Conference on Software Engineering and Data Engineering, SEDE, California, USA, Oct. 12-14, 189 - 193.
- [16] Pukdesree, S., Netinant, P. (2016). Conceptual framework: The adaptive biometrics authentication for accessing cloud computing services using iPhone, Advances in Intelligent Systems and Computing, 463, 209 - 216.



ภาคผนวก ง

การเผยแพร่ผลงานวิจัยในวารสารวิชาการระดับนานาชาติ ครั้งที่ 1

มหาวิทยาลัยรังสิต Rangsit University


[Journals](#)
[Topics](#)
[Information](#)
[Author Services](#)
[Initiatives](#)
[About](#)
[Profile](#)
[Sign Out](#)
[Submit](#)

Search for Articles:

[Advanced](#)

[Journals](#) / [Sustainability](#) / [Journal Statistics](#)


sustainability

[Submit to Sustainability](#)

[Review for Sustainability](#)

Journal Menu

- * Sustainability Home
- * Aims & Scope
- * Editorial Board
- * Reviewer Board
- * Topical Advisory Panel
- * Instructions for Authors
- * Special Issues
- * Topics
- * Sections & Collections
- * Article Processing Charge
- * Indexing & Archiving
- * Editor's Choice Articles
- * Most Cited & Viewed
- **Journal Statistics**
- * Journal History
- * Journal Awards
- * Society Collaborations
- * Conferences
- * Editorial Office

Journal Browser

Sustainability Statistics

Overview

Sustainability in Numbers

Sustainability (ISSN: 2071-1050)

Founded: 2009 (Volumes: 15)

63,139 articles published so far

17510 articles have been cited 10 times or more

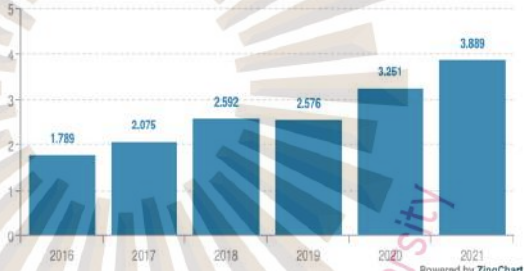
H5-Index: 103 (Sustainable Development)

Impact Factor

Current Impact Factor: 3.889

5-year Impact Factor: 4.089

JCR category rank: Q2: Environmental Sciences (SCIE) | Q2: Environmental Studies (SSCI) | Q3: Green & Sustainable Science & Technology (SCIE) | Q4: Green & Sustainable Science & Technology (SSCI)

Impact Factor


Year	Impact Factor
2016	1.789
2017	2.075
2018	2.592
2019	2.576
2020	3.251
2021	3.889

Powered by ZingChart

IMPACT FACTOR
3.889

CITESCORE
5.0

Sustainability Statistics from Scopus

CiteScore: 5.0

[view Scopus page](#)

[SJR data](#), [view statistics from SCImago](#)



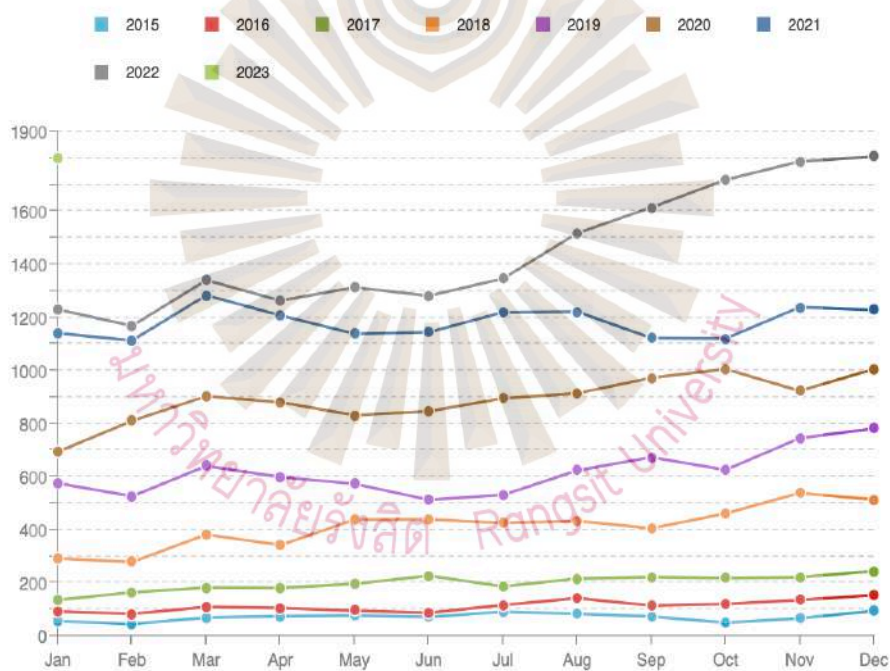
Sustainability Statistics

[Papers Monthly](#)

[Papers Yearly](#)

[Papers per country / territory](#)

[More Statistics From Scilit](#)



3,889 5.0

Share

Alert



[Submit to Sustainability](#)

[Review for Sustainability](#)

Journal Menu

- [Sustainability Home](#)
- [Aims & Scope](#)
- [Editorial Board](#)
- [Reviewer Board](#)
- [Topical Advisory Panel](#)
- [Instructions for Authors](#)
- [Special Issues](#)
- [Topics](#)
- [Sections & Collections](#)
- [Article Processing Charge](#)
- [Indexing & Archiving](#)
- [Editor's Choice Articles](#)
- [Most Cited & Viewed](#)
- [Journal Statistics](#)
- [Journal History](#)
- [Journal Awards](#)
- [Society Collaborations](#)
- [Conferences](#)
- [Editorial Office](#)

Journal Browser

Go

> Forthcoming issue

> Current issue

Editorial Board

- Environmental Sustainability and Applications Section
- Social Ecology and Sustainability Section
- Economic and Business Aspects of Sustainability Section
- Sustainable Engineering and Science Section
- Energy Sustainability Section
- Sustainable Urban and Rural Development Section
- Sustainable Agriculture Section
- Sustainable Education and Approaches Section
- Tourism, Culture, and Heritage Section
- Sustainable Chemical Engineering and Technology Section
- Sustainable Transportation Section
- Geography and Sustainability Section
- Psychology of Sustainability and Sustainable Development Section
- Resources and Sustainable Utilization Section
- Air, Climate Change and Sustainability Section

- Sustainability, Biodiversity and Conservation Section
- Sustainable Food Section
- Health, Well-Being and Sustainability Section
- Hazards and Sustainability Section
- Sustainable Materials Section
- Sustainable Management Section
- Green Building Section
- Soil Conservation and Sustainability Section
- Sustainable Forestry Section
- Waste and Recycling Section
- Sustainable Oceans Section
- Sustainable Water Management Section
- Pollution Prevention, Mitigation and Sustainability Section
- Bioeconomy of Sustainability Section
- Sustainable Products and Services Section

Members (2322)

Prof. Dr. Marc A. Rosen [Website](#) [SciProfiles](#)

Editor-in-Chief

Faculty of Engineering and Applied Science, University of Ontario Institute of Technology, Oshawa, ON L1G 0C5, Canada

Interests: sustainability; sustainable development; energy; efficiency; environmental impact; economics; ecology; sustainable engineering and design

Special Issues, Collections and Topics in MDPI journals



Dr. Sarah Holdsworth [Website](#)

Associate Editor

Lecturer, School of Property, Construction and Project Management, RMIT University, 78 Roseneath St. Clifton Hill, VIC 3068, Australia

Interests: sustainability; higher education; urban planning resilience

Special Issues, Collections and Topics in MDPI journals



Vol. 15 (2023)

Vol. 7 (2015)

► Show Figures

Open Access Article

How Do House Prices and Financial Expenditure Affect Birth Rate? New Evidence from the Dynamic Threshold Panel Model

by Lifang Yan and Wenzhong Ye

Sustainability 2023, 15(4), 3093; <https://doi.org/10.3390/su15043093> - 08 Feb 2023

Viewed by 154

Abstract Owing to low birth rate, the demographic dividend in China is disappearing. It is thus of great significance to study the regional differences and influencing factors of the birth rate, further proposing political advices on how to raise birth rate. In this study, [...] Read more.

(This article belongs to the Special Issue Sustainable Human Development versus Sustainable Personal Development)

► Show Figures

Open Access Article

User Acceptance Factors Related to Biometric Recognition Technologies of Examination Attendance in Higher Education: TAM Model

by Meennapa Rukhiran, Sethapong Wong-In and Paniti Netinant

Sustainability 2023, 15(4), 3092; <https://doi.org/10.3390/su15043092> - 08 Feb 2023

Viewed by 178

Abstract Identity recognition is influenced at all educational levels by biometric technology. The invention of facial recognition technology has added new efficiencies to the traditional method of tracking student examination attendance. This study aims to determine whether biometric recognition technologies could be utilized to [...] Read more.

► Show Figures

Open Access Article

Evaluating the Effects of Logistics Center Location: An Analytical Framework for Sustainable Urban Logistics

by Yanxia Wang, Yisong Li and Changxiang Lu

Sustainability 2023, 15(4), 3091; <https://doi.org/10.3390/su15043091> - 08 Feb 2023

Viewed by 156

Abstract Sustainable urban logistics require support of sustainable logistics center location planning. Nevertheless, urban public authorities generally experience difficulties in choosing a successful planning scheme, due to the lack of a rigorous analytical tool designed to help understand how logistics center location affects sustainability [...] Read more.

(This article belongs to the Special Issue Sustainable Urban Freight Transport, City Logistics and Transportation)

► Show Figures

Article

User Acceptance Factors Related to Biometric Recognition Technologies of Examination Attendance in Higher Education: TAM Model

Meennapa Rukhiran ¹, Sethapong Wong-In ² and Paniti Netinant ^{2,*}

¹ Faculty of Social Technology, Rajamangala University of Technology Tawan-OK, Chanthaburi 22210, Thailand

² College of Digital Innovation Technology (DIT), Rangsit University, Pathum Thani 12000, Thailand

* Correspondence: paniti.n@rsu.ac.th

Abstract: Identity recognition is influenced at all educational levels by biometric technology. The invention of facial recognition technology has added new efficiencies to the traditional method of tracking student examination attendance. This study aims to determine whether biometric recognition technologies could be utilized to enhance undergraduate examination attendance systems. The study examined the perceptions of first-year college students regarding the system's use of face recognition technologies. Based on the proposed framework, experimental results were obtained by developing and deploying unimodal and multimodal face recognition methods. Using a quasi-practical design with sample groups, undergraduate students' perceptions of traditional and biometric examination attendance were compared. Adopting the Theory for Reasoned Action and the Technology Acceptance Model, a questionnaire was distributed and analyzed to determine perception factors. The findings reveal that perceived ease of use, and trust and security significantly impact perceived usefulness. It was discovered that perceived usefulness significantly affects behavioral intention to use a system. According to the research findings, multimodal biometric recognition receives significantly more positive ratings than unimodal biometric recognition. This study proposes that universities utilize biometric technology, particularly facial recognition, to assess users' acceptance of the system.

Keywords: biometric; examination attendance; face recognition; user perception; framework



Citation: Rukhiran, M.; Wong-In, S.; Netinant, P. User Acceptance Factors Related to Biometric Recognition Technologies of Examination Attendance in Higher Education: TAM Model. *Sustainability* **2023**, *15*, 3092. <https://doi.org/10.3390/su15043092>

Academic Editor: Diego Monferrer

Received: 28 December 2022

Revised: 18 January 2023

Accepted: 6 February 2023

Published: 8 February 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Universities have a significant requirement that students participate in class examinations. Student examinations are essential to students' academic success at all educational levels [1,2]. Traditionally, students are required to present identification to proctors before entering the examination room to verify their identities. The signature of each student is required on an examination attendance list. The traditional method of identity verification examines identification cards, driver's licenses, and passports. This method is insufficient in terms of accuracy and efficiency, which can lead to class discipline, monitoring, and fraud [3], especially in a large examination classroom [4]. Student identification is susceptible to forgery, loss, obsolescence, and damage. Students could sign the examination attendance list on behalf of classmates who could not attend. In large examination rooms, proctors may take longer to verify students' identities, which may negatively affect students' cognitive psychology [5]. Due to human error, proctors need technological tools to ensure the accuracy of student verification [6]. A modern university uses information technology extensively in a variety of areas, including admissions, registration, surrounding information, schedule management, learning, exams, and web-based exams [7–10]. The well-known online systems are made to handle important information and general tasks [11], and students use a username and password to log in and verify their identity [12].

Utilizing biometric technology to verify students is a reasonable solution. A student is not required to carry any identification with them. Numerous biometric techniques

are being used at present in various applications, involving fingerprint authentication for check-in and check-out [13] and face recognition for granting access to cloud services [14]. To ensure system accuracy and efficiency, some propose using unimodal and multimodal biometric techniques [15–18]. At present, no proposed verification system utilizes multimodal biometrics to verify student attendance on examinations. The hard work of figuring out how to use information technology to verify a student's identity is crucial to helping students with exam attendance verification.

Several identification and verification systems based on biometric recognition have been proposed, such as fingerprint [19,20] and facial recognition [21–26]. The other proposed verification system made use of barcodes [27], QR codes [28], Near-Field Communication (NFC) [29], and Radio Frequency Identification (RFID) [30–32]. Ahmed et al. [33] used fingerprint recognition to establish a security framework for online examination. Emmanuel and Okonkwo [34] also developed a biometric authentication system for Nigerian students. The other reason an educational institution might use a biometric system [35] is to create a biometric system that can use the iris to check if a student is in class.

Biometric technology's advantages, made possible by the Internet of Things (IoT), have resulted in its widespread use as a verification device in various applications. While Awojide et al. [36], Jain et al. [37], and Zainal et al. [20] have proposed an IoT user attendance system based on fingerprint recognition, the issue to date of a high number of users may result in a long queue and require a significant amount of time to verify each student. Facial recognition is an effective technique that requires a large amount of personal data. Numerous studies on unimodal face recognition have been investigated to allow students to verify a student's classroom attendance automatically [26,38].

Our previous work designed and explained a framework and architecture for student biometric recognition [39]. The authors developed an IoT-based student biometric recognition system for examination attendance in this work. As such, this system examines students' perceptions of the examination attendance system using facial biometric technologies compared to traditional and biometric approaches, particularly unimodal and multimodal biometric recognition. There are several critical concerns to be addressed in this study to improve student recognition and simplify the operational practice of facial recognition. The research questions were developed to support the study's objectives as follows:

Q1: What affects students' perceptions of using biometric technology for identity verification of examination attendance?

Q2: Which biometric technology, based on unimodal or multimodal face recognition, do students desire to use for the purpose of attendance verification during examinations?

2. Literature Review

2.1. Biometric Technology

Biometric technology is widely used for two primary purposes: identification and access control [40]. Numerous biometric technology studies are underway, at present, in various recent areas, including algorithms, architectures, modalities, and empirical studies. Three broad categories of biometric studies exist. Physical biometric verification entails the examination of physical characteristics of the human body, including the face, fingerprints, palm, hand geometry, retina, and iris. Behavioral biometrics studies human operations, such as speech, signature, posture, keystroke dynamics, and other behavioral biometric authentication activities on smartphones [41]. Chemical biometrics is the study of chemical cues associated with humans, such as personal odor. The human face is the most important biometric feature, as it is used in various applications, including felon recognition, security systems, forensics, observation systems, and credit card verification.

Generally, biometric systems are classified into two types [42]: unimodal and multimodal [43,44]. A unimodal system uses a single biometric source, such as the face, iris, fingerprint, palm, or other human body parts. By enhancing the performance of a biometric recognition system known as multimodal biometric recognition, multiple physical characteristics of humans can be identified. Four subcategories of multimodal biometric

recognition systems exist, including (1) multiple modalities: the recognition of a subject using more than two types of biometric technologies, such as a face and fingerprint. Ammour et al. [45] used facial and iris recognition to identify individuals in the system. Gunasekaran et al. [46] identified individuals through face, fingerprint, and iris blending. (2) Multiple sensors employ the same inspection pattern, for example, by combining images from two cameras. Zhao et al. [47] detected objects using two cameras on a mobile phone. (3) Multiple features: employ multiple algorithms to extract features from images or data, for instance, fingerprint extraction is to be used in conjunction with the first and second algorithms. (4) Multiple and repeated instances: using one or more biometric forms, such as left- and right-iris images for iris recognition, or using the same biometrics in recognition processes. Ye et al. [25] presented a concise overview of deep learning techniques for the re-identification of individuals. Additionally, numerous recent research papers discussed the multimodal biometric approach. Fenu et al. [21] described a multi-biometric recognition system for continuous learner validation in e-learning systems. The system authenticates and authorizes students' entries using their faces and fingerprint. Traore et al. [24] proposed a framework for an online examination that incorporates a multimodal biometric system that utilizes the continuous capture of images via a web camera.

Numerous published articles on contemporary biometric research discuss multimodal biometric technologies. Chen et al. [48] proposed a multimodal framework in their pioneering Variational Bayesian Extreme Learning Machine (VBELM). They created a block using facial images and fingerprint templates generated from a feature-image matrix. The proposed approach retrieved the core layer semantic aspects of local features, resulting in increased characterization capabilities, element reduction, and improved correctness for multimodal biometrics. In terms of generalization, testing accuracy, efficiency, and stability, the VBELM outperforms traditional methods. Gomez-Barrero et al. [49] described a technique for improving a multimodal biometric approach based on the homomorphic encoding technique, which encrypts all database data. Multimodal biometric fusion is a term that refers to the combination of features, scores, and decision levels. The experiments were performed using an online signature and fingerprint recognition database. The system complies with the ISO/IEC 24745. Biometric technology demonstrates that the biometric approach is applicable in a wide variety of fields. As a result, this study focused on the applications of unimodal and multimodal biometric recognitions that can be used to determine a student's examination attendance in place of the traditional method.

2.2. Related Face Recognition

Face recognition is the most widely used method for identifying and verifying individuals in person. A face recognition system's three critical processes are detection, feature extraction, and facial similarity. Face recognition applies to a broad range of research fields. For instance, Dass et al. [50] concentrated on face recognition techniques and real-time face recognition on the Raspberry Pi. Yadav and Vishwakarma [51] proposed a novel, advanced, efficient framework based on interval type-II fuzzy membership and a kernel-based sparse method. They quantified the pixels in a participation image using type-II fuzzy logic and a membership function for type-II extended intervals. When K-nearest neighbor and Euclidean distance metrics were used for sparse representation, the experimental analysis revealed a 10% increase in accuracy. According to Nguyen et al. [52], the human face is a passive biometric. Face images work well when combined with the individual's interaction, including blinking, nodding, and turning the face. The facial recognition system is an artificial intelligence system that identifies individuals through image patterns derived from the textures and shapes of their faces. Temperatures and wrinkles do not affect the visible imagery of facial biometrics. Yaddaden et al. [53] demonstrated the effectiveness of a facial recognition system built on a convolutional neural network architecture and equipped with an error detection module. The experiment used five benchmark facial expression datasets with promising results. For example, the accuracy was higher than 95%, and the number of false positives was cut by 20%.

2.3. User Perception Model

The Technology Acceptance Model (TAM) was adopted and developed to examine the use of system acceptance [54]. The principal keys of TAM influenced users' intention to use technology by assembling perceived usefulness and perceived ease of use. BioTAM was a new resolution for a biometric authentication system's technology acceptance model [55]. BioTAM proposed that factors, such as user interfaces, biometric enrollment or verification procedures, devices, and other auxiliary tools, were used to study the end-behavioral user's intention toward using a biometric system. The questionnaire was statistically evaluated based on confounding variables. Wang [56] extended a modified TAM to investigate financial biometric identification applications. The study suggested that perceived privacy and perceived trust were added as modified TAM variables for biometric identification, which includes the face, fingerprint, iris, and voice.

Additionally, TAM is not limited to the study of user perception. Ajzen and Fishbein [57] proposed the Theory for Reasoned Action (TRA) as a framework for forecasting and describing actions across a range of domains, including attitude, intention [58], and motivation. TRA is a very broad concept intended to describe essentially any aspect of human actions. To summarize, the proper determination of user perception is contingent upon the users' intention to use technology. Buabeng-Andoh [59] proposed a model for predicting students' intentions regarding mobile learning adaptation. A combination of TAM and TRA was used to ascertain students' intentions regarding m-learning usage in the classroom. Banga and Pillai [60] discussed the factors that should be considered. Biometric systems for mobile payments should include accuracy, capability, acceptability, cost-effectiveness, and hygiene factors. Behavioral biometrics measure how an activity was carried out rather than the outcome of the activity. For example, the login system is responsive to the speed with which a user enters a username and password. TAM and TRA were used in this study to establish a practical biometric relationship between six significant factors: perceived usefulness and ease of use, as well as users' trust and security, attitudes, intention to use, and actual system use.

3. Materials and Methods

This research employed the Internet of Things (IoT) and facial recognition to propose a student biometric recognition system for exam attendance. Comparing biometric technology to the conventional method enables the replacement of student identification cards with face recognition technology in examination rooms. Creating a fake student identification card is simple. Each semester, students are subject to traditional verification using student identification cards. During the midterm exam for the spring semester of 2020, a sampling group of 161 first-year students was subjected to the biometric examination attendance system. Students were separated into four classes for digital intelligence and software science. The unimodal biometric recognition system was used in a single examination session to examine student perception. The multimodal biometric recognition system was also tested on the same test subjects during a later examination session.

3.1. Proposed Face Recognition Framework

In order to develop a prototype software system for exam attendance, our framework outlined the specifics of biometric student recognition. The extension of the previous framework in this study made possible the deployment and investigation of a student examination attendance system based on the Internet of Things (IoT) in its present state for unimodal biometric recognition with a single camera and multimodal biometric recognition with two cameras, as illustrated in Figure 1. The student examination attendance system ran on a Raspberry Pi 4 with 8GB of RAM and was linked to cameras and a monitor displayed in front of the exam room. Our experiment utilized OpenCV and Python 3.9 to train and test data. There were two primary system users (proctors and students). Teachers and other staff members were assigned as proctors to monitor student examination attendance. A proctor must authenticate with the system and enter the examination session to gain access.

Figure 2a shows the home page of our examination attendance system. As depicted in Figure 2b, each examination session includes information about the examination, including the date, subject, time, student list, and proctors. Before entering the examination session, students must register their faces and personal information in the system. The real-time database system contained the facial templates of students from which the OpenCV face recognition technology-trained system. Prior to entering the examination room, when a student approaches, the proctor uses the verification mode to identify the student's face. The student examination attendance system can detect students' faces, validate their identity accuracy, and report on a student's rate of accurate face recognition.

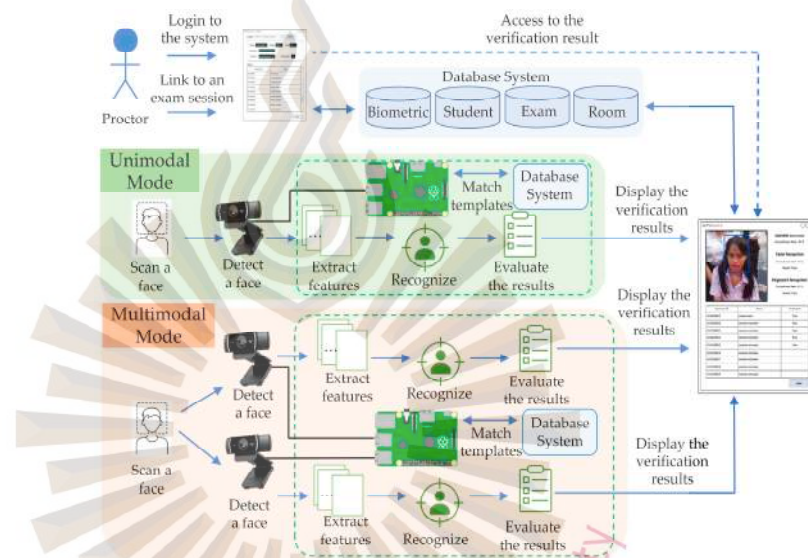


Figure 1. Proposed student biometric recognition framework for examination attendance system.

In addition, as shown in Figure 2c, a single camera was used to identify and verify the student's face, a technique known as unimodal biometric recognition. Multimodal biometric recognition requires two cameras to identify and verify the student's face; the system then calculates the average matching score, as shown in Figure 2d. Students gain practical experience with a cutting-edge face recognition system. The educational repercussion of biometric technology is the most challenging to implement. Therefore, in this study, the authors compared how people planned to make decisions based on how they used and satisfied biometric technologies in education.

3.2. Instrument

The questionnaire was separated into two major sections. The primary section examined the respondents' demographic characteristics (age and gender) in our experimental study. The secondary section of the study examined student perceptions using the Technology Acceptance Model (TAM) and Theory for Reasoned Action (TRA). The following five components were assigned to students: perceived usefulness (4 items), perceived ease of use (6 items), trust and security (5 items), attitude (4 items), behavioral intention to use (3 items), and actual system use (2 items). The survey respondents evaluated every item on a 5-point Likert scale, varying from 1 (strongly disagree) to 5 (strongly agree). This study included a total of twenty-three items. After the multimodal biometric verification was completed and the students completed their examinations, the participants were surveyed.

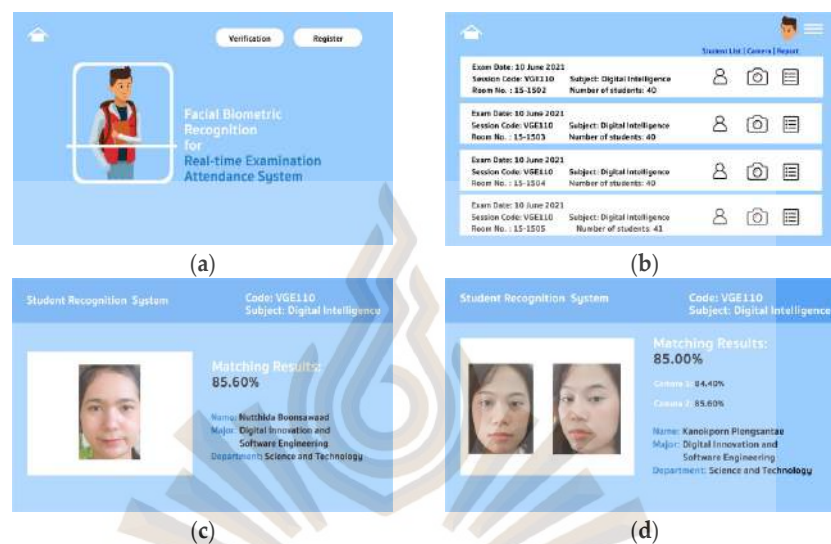


Figure 2. Samples of biometric recognition interfaces for examination attendance system: (a) the home page of the system; (b) examination information sessions; (c) the screen of a unimodal recognition result; (d) the screen of a multimodal recognition results.

3.3. Instrument Validation and Analysis

This study's methodology was quantitative. A questionnaire was initially developed to elicit student perceptions and test hypotheses. Perceptions and hypotheses were developed in accordance with DeVellis and Thorpe's guidelines [61]. The proposed method generated a list of components to evaluate, defined the items within each element, specified the measurement scale, and validated the model's reliability and validity. Cronbach's alpha [62], compound reliability (CR), convergent validity (AVE), and item analysis were used as indicators in the final step. SPSS was used to perform Exploratory Factor Analysis (EFA) and construct validity checks on the biometric recognition processes. Additionally, using the constructs' covariance matrix, the Confirmatory Factor Analysis (CFA) designed on Structural Equation Modeling (SEM) was assessed. Following that, one hundred and sixty-one students were asked to assess the end-user perception of facial biometric recognition with a 100% of response rate.

In addition, all study participants were given informed consent to ensure their contribution was anonymized and voluntary. The information presented was especially for the purpose of research. Justice, respect, autonomy, compassion, and confidentiality were all guaranteed as ethical values.

3.4. Hypotheses

Figure 3 depicts the proposed hypothesis model based on TAM and TRA. The authors labeled the following hypothesis about student perceptions of biometric recognition for examination attendance: Perceived ease of use has a positive effect on perceived usefulness (H1); trust and security have a positive effect on attitude (H2); perceived usefulness has a positive effect on behavioral intention to use (H3); perceived ease of use has a positive effect on behavioral intention to use (H4); attitude has a positive effect on behavioral intention to use (H5); trust and security have a positive effect on behavioral intention to use (H6); and behavioral intention to use has a positive effect on actual system use (H8).

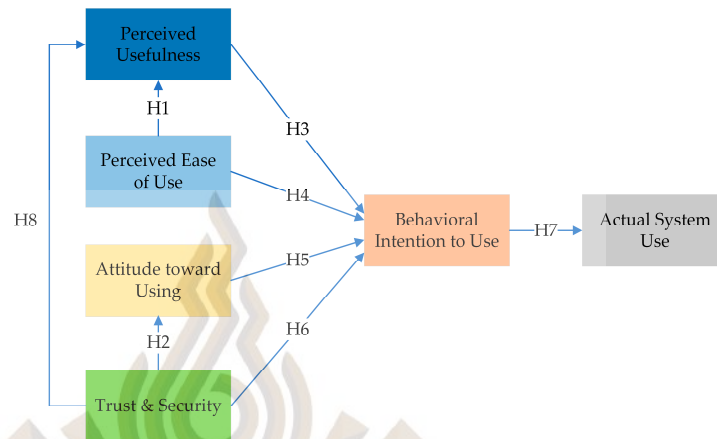


Figure 3. Proposed hypothesis model.

3.5. Evaluation Design and Data Collection

Using the extended TAM model, this study investigated the factors influencing the acceptance of face recognition technologies. The SEM model validated and verified the proposed hypothesis [63]. According to [64–66], at least 200 participants were required for an acceptable SEM analysis or at least 5 cases per parameter for a simple SEM model. Since this study contained 24 observable variables, the minimum sample size was $24 \times 5 = 120$. Students were used to selecting 161 user samples voluntarily. This research did not involve hazardous chemicals, equipment, procedures, animal or human testing, or the use of animals. However, this study obtained informed consent from individuals before collecting biometric data using and handling their facial biometric data. A consent form for facial biometric collection outlined the introduction, purpose, use, handling, rights, and contact information. As a part of the ethical research, the authors respected the participants' voluntariness, anonymity, freedom, and confidentiality. Students could make an informed decision about providing consent and then accept an individual's consent signature for collecting and using their facial biometric data.

3.6. Biometric Data Management

The management of collected biometric data is a crucial aspect of protecting the privacy and safety of individuals. Biometric data must be stored securely, using encryption and other security measures to prevent unauthorized access or data breaches. Administrators and authorized personnel must be the only ones with access to biometric data. Biometric information should be kept only as long as necessary for the purpose for which it was collected and should not be shared with third parties. When the data are no longer required, they should be deleted or anonymized to protect the privacy of individuals in accordance with all applicable laws and regulations, data protection and privacy laws, and to ensure that individuals have the right to access, correct, or delete their personal information. This study was conducted in accordance with all the applicable data protection laws and regulations, including the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, and Thailand's Personal Data Protection Act BE 2562. (PDPA).

4. Result and Discussion

Experiments were used to determine student perceptions of facial recognition for the examination attendance system, followed by a survey of 161 students to collect the data.

Students were exposed to the conventional method of identifying students with a student card, unimodal face recognition with a single camera, and multimodal face recognition with two cameras. Each participant completed a survey questionnaire at the conclusion of the three examination sessions. This section provides a summary of the study of the perceptions performed.

4.1. Descriptive Statistic

Males were the majority of participants (57.10%). The ages were 19 years old (33.50%). Table 1 shows the student demographic information in this research. The numerical assessment results for each aspect variable in the survey are shown in Table 2. In all the aspects, the three variables with the highest mean score (in order) were “The student identification using biometric recognition is reliable” (4.04). “The biometric recognition would be physically invasive” and “I would trust the face recognition system” had the same high mean score (4.01). On the other hand, the variables with the lowest mean score (in order) were “The biometric recognition does not require much effort to identify me.” (2.74), “The biometric recognition is easy to use” (2.80), and “I think the face recognition for examination attendance is more useful than the traditional method (student card)” (2.84).

Table 1. Student demographic information.

Item	Description	Sample	%
Gender	Male	92	57.10
	Female	69	42.90
Age	18	107	66.50
	19	54	33.50
Education level	Freshman student	161	100.00

Table 2. Mean and SD of constructs and items.

Construct	Description	Mean	SD
Perceived Usefulness (PU) [54,67,68]	PU1: I think face recognition for examination attendance is more useful than the traditional method (student card).	2.84	0.766
	PU2: I think multimodal face recognition for examination attendance is more useful than unimodal face recognition.	3.19	0.818
	PU3: The biometric technology is useful for my daily studies.	2.85	0.823
	PU4: The biometric technology helps me increase my productivity during my class.	2.94	0.834
Perceived Ease of Use (PEU) [54,69]	PEU1: I think face recognition for examination attendance is easier than the traditional method (student card).	2.85	0.654
	PEU2: I think multimodal face recognition for examination attendance is easier than the unimodal face recognition.	3.12	0.714
	PEU3: The biometric recognition is easy to use.	2.80	0.614
	PEU4: One of the reasons this system is useful is because of its ease of use.	2.87	0.603
	PEU5: The student recognition is simpler to identify than the traditional method.	2.92	0.642
	PEU6: Biometric recognition does not require much effort to identify myself.	2.74	0.657
Trust and Security (TS) [56,70]	TS1: The biometric recognition would be physically invasive.	4.01	0.680
	TS2: I would trust the face recognition system.	4.01	0.652
	TS3: Student identification using biometric recognition is reliable.	4.04	0.660
	TS4: The system can identify me correctly.	3.99	0.707
	TS5: The system has high recognition accuracy.	3.96	0.660

Table 2. Cont.

Construct	Description	Mean	SD
Attitude (ATT) [57]	ATT1: I feel that using biometric technology better than I expect.	3.89	0.707
	ATT2: Most of my expectations of using face recognition system were confirmed.	3.89	0.689
	ATT3: I feel pretty much use biometric technology in my study.	3.74	0.712
	ATT4: I can trust the biometric recognition system because of high security.	3.77	0.700
Behavioral Intention to Use (BIU) [57,71]	BIU1: I prefer biometric recognition for examination attendance than the traditional method.	3.20	0.593
	BIU2: I will use facial biometric recognition when I have an examination attendance.	3.59	0.586
	BIU3: I hope that biometric technology can be applied in university as soon as possible.	3.52	0.571
Actual System Use (ASU) [72]	ASU1: I would use a face recognition system for examination attendance.	3.70	0.537
	ASU2: I would recommend my university use a face recognition system for student identification in all authentication areas.	3.78	0.559

4.2. Reliability Test

Confirmatory Factor Analysis (CFA) was utilized to validate the reliability test. Hair et al. [73] defined construct validity so that the degree to which a collection of observed variables correctly signified the theoretically quantifiable latent variables. Additionally, they assessed the convergent and discriminant validity of postulated criteria. The findings confirm a total of 23 items. As Bagozzi and Yi [74] suggested, no items were removed because the standardized item loading exceeded 0.5. The factor loadings were more significant than 0.50 and ranged from 0.606 to 0.992, indicating their high reliability. Additionally, the instrument's reliability, consistency, and validity were evaluated. As suggested, the composite reliability (CR) value was greater than 0.70 and fell between 0.773 and 1.000 [75]. The average extracted variance (AVE) was greater than 0.50 and ranged between 0.533 and 0.999, indicating that the data are highly reliable. Cronbach's alpha coefficient values were greater than 0.70 and ranged between 0.774 and 0.932, as Cronbach [62] suggested. As shown in Table 3, all achieved and recommended measures and values demonstrate convergent validity acceptance (CR > 0.70 and AVE > 0.50).

Table 3. Convergent validity and reliability of constructs.

Construct	Item	Factor Loadings >0.50	CR >0.70	AVE >0.50	Cronbach's Alpha >0.70
Perceived Usefulness (PU)	PU1	0.799	0.850	0.589	0.846
	PU2	0.915			
	PU3	0.818			
	PU4	0.759			
Perceived Ease of Use (PEU)	PEU1	0.622	0.864	0.520	0.859
	PEU2	0.750			
	PEU3	0.856			
	PEU4	0.781			
	PEU5	0.800			
	PEU6	0.789			
Trust and Security (TS)	TS1	0.790	0.932	0.735	0.932
	TS2	0.869			
	TS3	0.959			
	TS4	0.913			
	TS5	0.861			

Table 3. Cont.

Construct	Item	Factor Loadings >0.50	CR >0.70	AVE >0.50	Cronbach's Alpha >0.70
Attitude (ATT)	ATT1	0.853	0.902	0.699	0.903
	ATT2	0.888			
	ATT3	0.892			
	ATT4	0.828			
Behavioral Intention to Use (BIU)	BIU1	0.679	0.823	0.623	0.801
	BIU2	0.900			
	BIU3	0.925			
Actual System Use (ASU)	ASU1	0.954	0.937	0.881	0.934
	ASU2	0.946			

The discriminant's validity was established because the square root of each construct was more significant than their corresponding inter-construct correlation estimates, as illustrated in Table 4. Therefore, all of the constructs were tested for their reliability and validity, which also showed a significant level.

Table 4. Discriminant validity.

Construct	PU	PEU	TS	AT	BIU	ASU
PU	0.767					
PEU	−0.269 **	0.721				
TS	0.280 **	−0.059	0.858			
ATT	0.160 †	−0.108	0.480 ***	0.836		
BIU	0.224 *	−0.165 †	0.175 *	0.114	0.789	
ASU	0.042	−0.008	0.051	0.108	0.220 *	0.939

† $p < 0.100$, * $p < 0.050$, ** $p < 0.010$, *** $p < 0.001$.

4.3. Measurement Model Testing

According to Figure 4, the measurement model confirms that all six constructs (PU, PEU, TS, ATT, BIU, and ASU) are the primary factors in the study that were examined using the EFA model. The authors removed no items from the instrument to achieve the best fit for the measurement model because their regression weights were larger than the bare minimum acceptance measure of 0.60. To validate the measurement model, confirmatory factor analysis was used. The authors tested the model-fit determines against the model's advised fit indicators (χ^2/df , GFI, RMSEA, RMR, NFI, CFI, IFI, and TLI) to validate the overall goodness of the fit index. The results show that all values are significantly greater than their relevant measures' (conventional least acceptance) quantities [73]. The model measurement of suitability indicators is shown in Table 5.

Table 5. Measurement of suitability indicators for the measurement model.

Model	χ^2	df	χ^2/df	GFI	RMSEA	RMR	NFI	CFI	IFI	TLI
Standards			$1 < \chi^2/df < 3$	≥ 0.90	$\leq 0.08 < 0.1$	$\leq 0.08 < 0.1$	≥ 0.90	≥ 0.90	≥ 0.90	≥ 0.90
Acquired	437.90	237	1.848	0.907	0.073	0.028	0.938	0.917	0.918	0.903

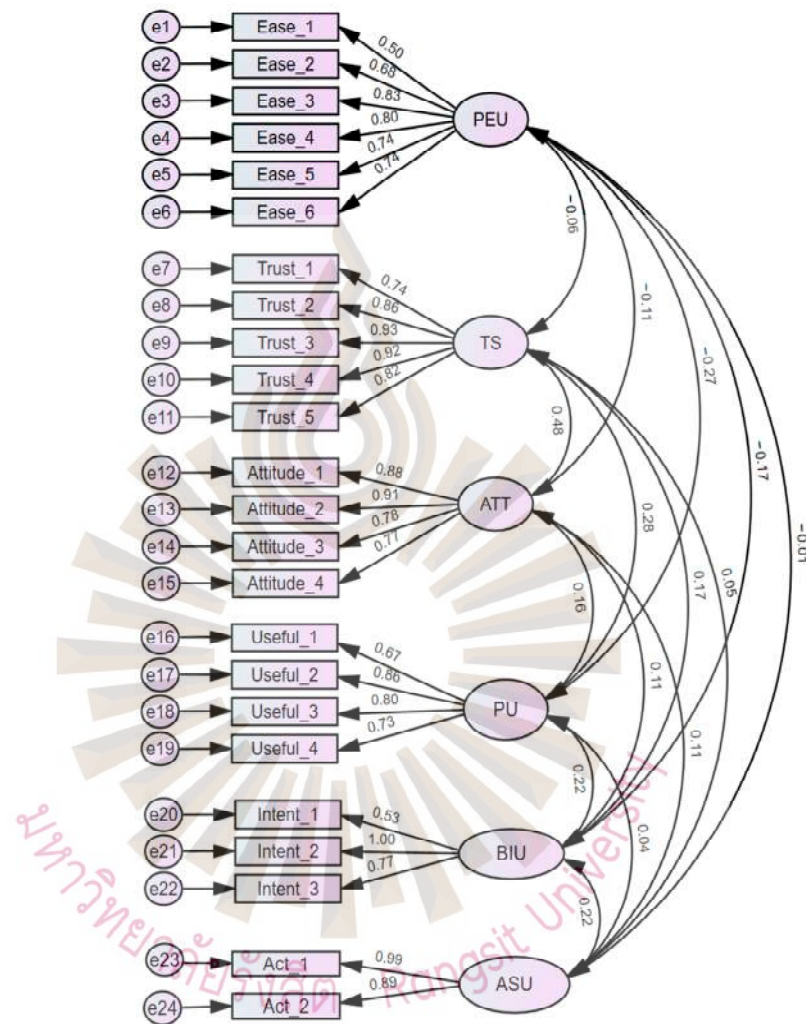


Figure 4. Measurement model of student perception toward biometric recognition.

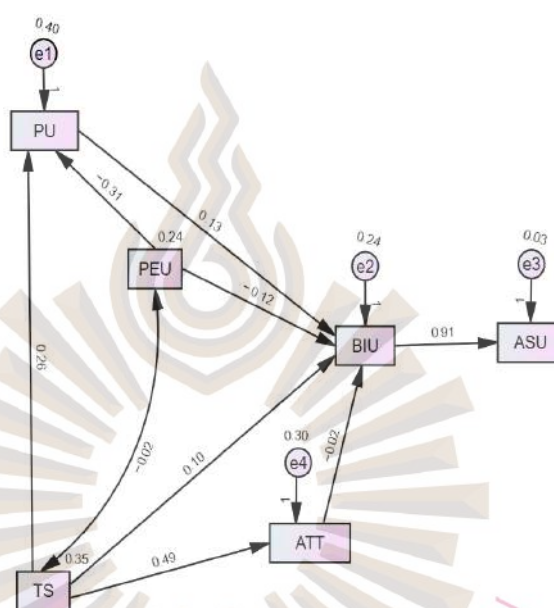
4.4. Structural Model Estimation

As shown in Figure 5, our proposed exploration model was evaluated using SEM. Hair et al. [73] explained how exploratory and confirmatory factor analysis techniques could simultaneously examine multiple dependence relations. When the model's constructs have direct and indirect effects on one another, this analysis method is particularly useful. The initial step in interpreting SEM results is to examine the model-fit indicator, which demonstrates that the data perfectly fit the proposed model.

As shown in Table 6, the SEM model demonstrates that all fit indicators meet the bare minimum acceptable standards. Figure 5 depicts the path significances, coefficients, and variances justified for each affected variable.

Table 6. Measurement of suitability indicators for the revised measurement model.

Model	χ^2	df	χ^2/df	GFI	RMSEA	RMR	NFI	CFI	IFI	TLI
Criteria			$1 < \chi^2/df < 3$	≥ 0.90	$\leq 0.08 < 0.1$	$\leq 0.08 < 0.1$	≥ 0.90	≥ 0.90	≥ 0.90	≥ 0.90
Obtained	7.776	6	1.296	0.984	0.043	0.008	0.940	0.996	0.996	0.996

**Figure 5.** Revised measurement model of student perception toward biometric recognition.

4.5. Hypotheses Test Results

Overall, the results support five of the eight hypotheses tested. As shown in Table 7, the findings account for the following positive relationships: TS ($\beta = 0.469$, $p < 0.000$) has a highly significant positive impact on ATT, supporting hypothesis H2; PEU ($\beta = -0.288$, $p < 0.002$) and TS ($\beta = 0.230$, $p < 0.002$) have a highly significant positive impact on PU, supporting hypothesis H1 and H8; PU ($\beta = 0.169$, $p < 0.036$) has a significantly positive impact on BIU, supporting hypothesis H3, while PEU ($\beta = -0.117$, $p < 0.137$), ATT ($\beta = -0.024$, $p < 0.780$), and TS ($\beta = 0.115$, $p < 0.194$) do not have a positive result for BIU; and BIU ($\beta = 0.938$, $p < 0.000$) has a positive influence on ASU, supporting hypothesis H7. However, TS exerts the greatest influence on PU's decision to use facial recognition for the examination attendance system, confirming hypothesis H3.

4.6. Discussion

According to our findings from the first research question, perceived usefulness is significantly predicted by trust and security (H8) and perceived ease of use (H1). Our accuracy factor was indicated in our item questions under the trust and security construct. This study is consistent with Sidharta's, Priadana's, and Affandi's [76], and Norfolk's and O'Regan's [72] findings on trust and security based on biometric technology. They asserted that a strong correlation existed between accuracy and perceived usefulness. Kanak and Sogukpinar [55] discovered that perceived ease of use of biometric authentication systems had a significant relationship with perceived usefulness in a situational relationship. Our findings support the notion that students' experiences with biometric technology have a strong correlation with perceived ease of use and usefulness for identifying and verifying

examination attendance. Students expressed a concern that using a face recognition system would be more convenient than the traditional approach.

Table 7. Summary of results for hypotheses assessment.

Hypotheses	Relationship (Positive)	Value	p-Value	Results
H1	PEU → PU	−0.228	0.002 **	Accepted
H2	TS → ATT	0.469	0.000 ***	Accepted
H3	PU → BIU	0.169	0.036 **	Accepted
H4	PEU → BIU	−0.117	0.137	Rejected
H5	ATT → BIU	−0.024	0.780	Rejected
H6	TS → BIU	0.115	0.194	Rejected
H7	BIU → ASU	0.938	0.000 ***	Accepted
H8	TS → PU	0.230	0.002 **	Accepted

*** $p < 0.001$, ** $p < 0.05$.

In this study, a construct of trust and security (H2) had a positive effect on attitude. However, Norfolk and O'Regan [72] discovered an unexpected relationship between accuracy and attitude toward use. On the other hand, this study discovered that trust and security (H6) had no positive effect on behavioral intention to use. Our findings imply that students involved in biometric technology can be trusted to maintain a high level of security while minimizing identity fraud. For various reasons, students consider the employment of biometric technology as an intelligent tool for examination attendance.

The findings indicate that perceived usefulness (H3) positively affects behavioral intention to use. Additionally, behavioral intention (H7) was associated with a beneficial effect on actual system use, as previously mentioned [77,78]. This evidence demonstrates the numerous benefits of biometric technology for actual biometric recognition systems in universities. Surprisingly, the results show that students' perceptions of perceived ease of use (H4) and attitude (H5) have no positive effect on their behavioral intention to use, which is supported by Norfolk and O'Regan [72].

The results of the second research question indicate that multimodal biometric recognition receives significantly more favorable ratings than unimodal biometric recognition. Student perceptions of perceived usefulness and perceived ease of use received the highest scores compared to other factors in the same constructs. According to Labayen et al. [79], students are positively affected by multimodal biometric recognition.

5. Conclusions

5.1. Theoretical Contributions

Biometric technology has several potential applications, including K-12 education, higher education, teacher education, and training. The empirical findings of this study demonstrate that the application of biometric technology can transform traditional examination approaches, challenge established approaches to biometric examination attendance, and enable exam aspects to improve security, reliability, and efficiency. Additionally, this study discovered that when conservative and biometric identifications were compared, they resulted in significantly different experience outcomes. Students preferred the face recognition system over the conservative approach for examination attendance, which is attributed to concerns about trust and security. Biometric recognition enables students to easily and accurately identify and verify themselves. The results produced the following conclusions as the study's primary contribution:

- The framework for biometric examination attendance recognition was proposed and a prototype application was developed. The study demonstrates the educational biometric recognition framework's practical outcomes, emphasizing unimodal and

multimodal face recognition for first-year undergraduate students. Additionally, the proposed architecture and system provide real-time face recognition of students for examination attendance, information, and accuracy rates of face recognition.

- To investigate students' actual system use, this research adopted a Model of Technology Acceptance (TAM) and a Theory of Reasoned Action (TRA). The educational biometric recognition factors considered student perceptions of ease of use, usefulness, attitude, trust, and security.
- Trust and security are significantly related to IoT-based face recognition for class attendance because they are essential to protect individuals' rights and privacy, ensure compliance with laws and regulations, maintain the integrity and security of the system, and build trust with individuals.
- In comparison to traditional and biometric recognition for examination attendance, multimodal face recognition is significantly more useful than unimodal face recognition.

5.2. Practical Implications

The biometric recognition framework of the examination attendance system can be used to enhance the proctoring approach for student identification and verification in elementary, secondary, and higher education. This study can provide new perspectives and techniques for administrators, educators, and instructors with perception into an innovative biometric recognition system for educational examinations and enhance security, reliability, and efficiency.

At present, users increasingly accept biometric technologies in their daily lives, owing to the convenience and speed with which they can be identified and verified. The authors exclusively focused on face recognition for examination attendance in this study. Biometric recognition can track students' movement between areas and eliminate the need for identification in various other ways, such as no student cards. Since 2019, due to the spread of coronavirus disease, universities worldwide have adopted distance education, considered the best solution for social isolation, less contact, and disease prevention.

Several steps can be taken to prevent errors in recognizing a specific image of a student and any significant changes to their appearance in facial recognition systems used for class attendance. One potential solution is to periodically update the stored images of students in the system to reflect any changes in their appearance. This approach could involve regularly scheduled re-enrollments or updates to the system, where students would be required to provide updated images of their current appearance. Another solution is to use more robust multimodal facial recognition systems that use multiple modalities, such as thermal, depth, and 3D images, to improve the system's accuracy and make it more resistant to changes in appearance. Another approach could be to use a combination of facial recognition technology with other forms of identification, such as a student ID card, a password, or a PIN. To ensure that even if the facial recognition system cannot recognize a student due to changes in their appearance, they will still be able to prove their identity and access the class. It is also important to communicate with students about the potential impact of changes in their appearance on the system's accuracy and to provide guidance on how they can update their data in the system in case of significant changes.

5.3. Limitations and Future Work

The limited use of facial recognition technology raises ethical concerns from different perspectives, such as privacy, bias, transparency, surveillance, discrimination, misuse of data, and lack of proper regulations. These ethical concerns must be carefully considered and addressed to ensure that the technology is used responsibly and ethically that respects individuals' rights and dignity. It is important to have clear guidelines, regulations, and oversight mechanisms in place to govern the use of facial recognition technology to minimize any negative impacts.

Future research on IoT-based face recognition for class attendance systems should detail potential areas that can be undertaken to improve accuracy and performance. These

include using multimodal systems, deep learning algorithms, data privacy and security, addressing biases in the system, integration with other technologies, and real-time monitoring. Researchers and educators could elucidate additional factors influencing individuals' preferences for biometric recognition in their examination approaches. The university may announce biometric recognition for student examination attendance without obtaining permission. However, university administrators would be sensible to obtain consent from students and research their perceptions before biometric recognition is used to replace traditional processes. Thus, researchers and educators could further elucidate the factors influencing individuals' preference for biometric recognition in their examination approaches. Moreover, student biometric recognition can integrate online learning and assessment systems, ensuring that students remain focused during their study sessions. These trends are likely to persist in subsequent research.

Author Contributions: Conceptualization, P.N. and M.R.; methodology, S.W.-I. and P.N.; software evaluation and modeling, S.W.-I.; validation, P.N., M.R., and S.W.-I.; formal analysis, P.N. and M.R.; investigation, S.W.-I.; resources, S.W.-I.; data curation, P.N., M.R., and S.W.-I.; writing—original draft preparation, M.R. and S.W.-I.; writing—review and editing, P.N. and M.R.; visualization, P.N., M.R., and S.W.-I.; supervision, P.N. and M.R.; project administration, P.N., M.R., and S.W.-I. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Ethical review and approval were waived for this study because this research does not involve hazardous chemicals, equipment, procedures, animal or human testing, or the use of animals and human as a subject experiment. Rangsit University granted ethical approval, and the actual protocol number is RSU-GRAD 537/2561.

Informed Consent Statement: Informed consent was obtained from all study participants. Participants were at least 18 years old. As part of the ethical research, the authors respect the voluntariness, anonymity, freedom, and confidentiality of the participants. The provided data contained no information that could be used to determine the participants' identities.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Constantinou, C.; Wijnen-Meijer, M. Student evaluations of teaching and the development of a comprehensive measure of teaching effectiveness for medical schools. *BMC Med. Educ.* **2022**, *22*, 113. [\[CrossRef\]](#) [\[PubMed\]](#)
2. Banwarith, R.; Basuhail, A.; Fattouh, A.; Gamalel-Din, S. E-exam cheating detection system. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, 176–181.
3. Vučković, D.; Peković, S.; Blečić, M.; Đoković, R. Attitudes towards cheating behavior during assessing students' performance: Student and teacher perspectives. *Int. J. Educ. Integr.* **2020**, *16*, 13. [\[CrossRef\]](#)
4. Roshan, A.S.; Gurbaz, M.Q.; Rahmani, S. The effects of large classes on English language teaching. *Integr. J. Res. Arts Humanit.* **2022**, *2*, 38–41. [\[CrossRef\]](#)
5. Lee, J.W. Impact of proctoring environments on student performance: Online vs offline proctored exams. *J. Asian Financ. Econ. Bus.* **2020**, *7*, 653–660. [\[CrossRef\]](#)
6. Anu, V.; Walia, G.; Bradshaw, G. Incorporating human error education into software engineering courses via error-based inspections. In Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education, Seattle, WA, USA, 8–11 March 2017; pp. 39–44. [\[CrossRef\]](#)
7. Abass, O.A.; Olajide, S.A.; Samuel, B.O. Development of web-based examination system using open-source programming model. *Turk. Online J. Distance Educ.* **2017**, *18*, 30–42. [\[CrossRef\]](#)
8. Hameed, M.R.; Abdullatif, F.A. Online examination system. *Int. Adv. Res. J. Sci. Eng. Technol.* **2017**, *4*, 106–110. [\[CrossRef\]](#)
9. Hamid, R.A.; Mokhtar, U.A.; Yusof, M.; Warland, A. Electronic records management in schools: The case study of school examination analysis system. *J. Pengur.* **2020**, *57*, 1–13. [\[CrossRef\]](#)
10. Rukhiran, M.; Napasorn, P.; Netinant, P. Adoption of environmental information chatbot services based on the internet of educational things in smart schools: Structural equation modeling approach. *Sustainability* **2022**, *14*, 15621. [\[CrossRef\]](#)
11. Divya, H.; Nandhini, S.; Shobana, S.; Sujithra, M. Examination management system. *Int. J. Adv. Res. Publ.* **2021**, *9*, 920–923. [\[CrossRef\]](#)

12. Rukhiran, M.; Pukdesree, S.; Netinant, P. Biometric cloud services for web-based examinations: An empirical approach. *Int. J. Inf. Technol.* **2022**, *17*, 22. [\[CrossRef\]](#)
13. Shamsi, S.V.; Andrews, J.V. A survey paper on fingerprint recognition and cross matching. *Int. J. Res. Appl. Sci. Eng. Technol.* **2019**, *7*, 573–575. [\[CrossRef\]](#)
14. Kortli, Y.; Jridi, M.; Falou, A.A.; Atri, M. Face recognition systems: A survey. *Sensors* **2020**, *20*, 342. [\[CrossRef\]](#)
15. Raju, A.S.; Udayashankara, V. A survey on unimodal, multimodal biometrics and its fusion techniques. *Int. J. Eng. Technol.* **2018**, *7*, 689–695. [\[CrossRef\]](#)
16. Rukhiran, M.; Netinant, P. A practical model from multidimensional layering: Personal finance information framework using mobile software interface operations. *J. Inf. Commun. Technol.* **2020**, *19*, 321–349. [\[CrossRef\]](#)
17. Poria, S.; Cambria, E.; Bajpai, R.; Hussain, A. A review of affective computing: From unimodal analysis to multimodal fusion. *Inf. Fusion* **2017**, *37*, 98–125. [\[CrossRef\]](#)
18. Singh, M.; Singh, R.; Ross, A. A comprehensive overview of biometric fusion. *Inf. Fusion* **2019**, *52*, 187–205. [\[CrossRef\]](#)
19. Zainal, I.; Sidek, K.A.; Gunawan, T.S.; Mansor, H.; Kartiwi, M. Design and development of portable classroom attendance system based on Arduino and fingerprint Biometric. In Proceedings of the 5th International Conference on Information and Communication Technology for The Muslim World, Sarawak, Malaysia, 17–19 November 2014. [\[CrossRef\]](#)
20. Zainal, N.I.; Sidek, K.A.; Gunawan, T.S. Portable anti forgery recognition for attendance system using fingerprint based biometric. *ARPN J. Eng. Appl. Sci.* **2016**, *11*, 396–403.
21. Fenu, G.; Marras, M.; Boratto, L. A multi-biometric system for continuous student authentication in e-learning platforms. *Pattern Recognit. Lett.* **2018**, *113*, 83–92. [\[CrossRef\]](#)
22. Mehta, P.; Tomar, P. An efficient attendance management system based on face recognition using Matlab and Raspberry Pi 2. *Int. J. Eng. Res. Technol.* **2016**, *3*, 71–78.
23. Sayeed, S.; Hossen, J.; Kalaiarasi, S.; Vaithiyashankar, J.; Yusof, I.; Samraj, A. Real-time face recognition for attendance monitoring system. *J. Theor. Appl. Inf. Technol.* **2017**, *95*, 24–30.
24. Traore, I.; Nakkabi, Y.; Saad, S.; Sayed, B.; Ardigo, J.D.; Quinan, P.M. *Ensuring Online Exam Integrity through Continuous Biometric Authentication*; Springer: New York, NY, USA, 2017; pp. 73–81. [\[CrossRef\]](#)
25. Ye, M.; Shen, J.; Lin, G.; Xiang, T.; Shao, L.; Hoi, S.C. Deep learning for person re-identification: A survey and outlook. *IEEE Trans. Pattern Anal. Mach. Intell.* **2022**, *44*, 2872–2893. [\[CrossRef\]](#) [\[PubMed\]](#)
26. Yusof, Y.M.; Nasir, M.M.; Othman, K.A.; Suliman, S.I.; Shahbudin, S.; Mohamad, R. Real-time internet-based attendance using face recognition system. *Int. J. Eng. Technol.* **2018**, *7*, 174–178. [\[CrossRef\]](#)
27. Khan, R.U.; Wee, V.C.; Lui, V.W.; UIHaq, M.I.; Khan, Y.; Barawi, M.H. Mobile barcode based examination attendance system. *Int. J. Eng. Technol.* **2018**, *7*, 49–54. [\[CrossRef\]](#)
28. Rahni, A.A.; Zainal, N.; Adna, M.Z.; Othman, N.E.; Bukhori, M.F. Development of the online student attendance monitoring system (SAMSTTM) based on QR-codes and mobile devices. *J. Eng. Sci. Technol.* **2015**, *10*, 28–40.
29. Mohandes, M.A. Class attendance management system using NFC mobile devices. *Intell. Autom. Soft Comput.* **2016**, *23*, 251–259. [\[CrossRef\]](#)
30. Bhalla, V.; Singla, T.; Gahlot, A.; Gupta, V. Bluetooth based attendance management system. *Int. J. Innov. Eng. Technol.* **2013**, *3*, 227–233.
31. Rjeib, H.D.; Ali, N.S.; Farawn, A.A.; Al-Sadawi, B.; Alsharqi, H. Attendance and information system using RFID and web-based application for academic sector. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 266–274. [\[CrossRef\]](#)
32. Taileb, M. Design and implementation of RFID and fingerprint-based student verification system design and implementation of RFID and fingerprint-based student verification system. *Int. J. Recent. Technol. Eng.* **2020**, *8*, 2084–2092. [\[CrossRef\]](#)
33. Ahmed, I.B.; Mohamed, M.A.; Noma, A.M. A framework for secure online exam using biometric fingerprint and steganography techniques. *Int. J. Eng. Technol.* **2018**, *7*, 32–35. [\[CrossRef\]](#)
34. Emmanuel, E.; Okonkwo, T. A biometric authentication approach to examination conduct in Nigerian universities. *Int. J. Innov. Res. Technol. Sci. Eng.* **2019**, *8*, 2176–2182. [\[CrossRef\]](#)
35. Mir, G.M.; Balkhi, A.; Lala, N.A.; Sofi, N.A.; Kirmani, M.; Mir, I.A.; Hamid, H.A. The benefits of implementation of biometric attendance system. *Oriental J. Comput. Sci. Technol.* **2018**, *11*, 50–54. [\[CrossRef\]](#)
36. Awojide, S.; Awe, O.S.; Babatope, T.S. Biometric fingerprint system using an online based pattern recognition for candidate's authentication in Nigeria institution examinations. The Design Perspective. *Int. J. Sci. Eng.* **2018**, *9*, 1680–1694. [\[CrossRef\]](#)
37. Jain, T.; Tomar, U.; Arora, U.; Jain, S. IoT based biometric attendance system. *J. Electr. Eng. Technol.* **2020**, *11*, 156–161.
38. Sunaryono, D.; Siswantoro, J.; Anggoro, R. An android-based course attendance system using face recognition. *J. King Saud Univ.—Comput. Inf. Sci.* **2021**, *33*, 304–312. [\[CrossRef\]](#)
39. Wong-In, S.; Netinant, P. Designing an examinee personal verification system using biometric technology. *J. Curr. Sci. Technol.* **2018**, *8*, 75–86. [\[CrossRef\]](#)
40. Ahmed, A.A. Future effects and impacts of biometrics integrations on everyday living. *Al-Mustansiriyah J. Sci.* **2019**, *29*, 139–144. [\[CrossRef\]](#)
41. Mahfouz, A.; Mahmoud, T.M.; Eldin, S.A. A survey on behavioral biometric authentication on smartphones. *J. Inf. Secur. Appl.* **2017**, *37*, 28–37. [\[CrossRef\]](#)

42. Gawande, U.; Golhar, Y. Biometric security system: A rigorous review of unimodal and multimodal biometrics techniques. *Int. J. Biom.* **2018**, *10*, 142–175. [\[CrossRef\]](#)
43. Walia, G.S.; Singh, T.; Singh, K.; Verma, N. Robust multimodal biometric system based on optimal score level fusion model. *Expert Syst. Appl.* **2019**, *116*, 364–376. [\[CrossRef\]](#)
44. Yang, W.; Wang, S.; Hu, J.; Guanglou, Z.; Valli, C. A fingerprint and finger-vein based cancelable multi-biometric system. *Pattern Recognit.* **2018**, *78*, 242–251. [\[CrossRef\]](#)
45. Ammour, B.; Boubchir, L.; Bouden, T.; Ramdani, M. Face-Iris multimodal biometric identification system. *Electronics* **2020**, *9*, 85. [\[CrossRef\]](#)
46. Gunasekaran, K.; Jayamani, R.; Ramasamy, P. Deep multimodal biometric recognition using contourlet derivative weighted rank fusion with human face, fingerprint and iris images. *Automatika* **2019**, *60*, 253–265. [\[CrossRef\]](#)
47. Zhao, Y.; Xu, J.; Wu, J.; Hao, J.; Qian, H. Enhancing camera-based multimodal indoor localization with device-free movement measurement using WiFi. *IEEE Internet Things J.* **2020**, *7*, 1024–1038. [\[CrossRef\]](#)
48. Chen, Y.; Yang, J.; Wang, C.; Park, D. Variational Bayesian extreme learning machine. *Neural Comput. Appl.* **2014**, *27*, 185–196. [\[CrossRef\]](#)
49. Gomez-Barrero, M.; Maiorana, E.; Galbally, J.; Campisi, P.; Fierrez, J. Multi-biometric template protection based on homomorphic encryption. *Pattern Recognit.* **2017**, *67*, 149–163. [\[CrossRef\]](#)
50. Dass, S.; Sadruhluda, M.Q.; Pasha, N.N.; Nayan, N.; Nayak, J.S. Real time face recognition using Raspberry Pi. *Int. J. Comput. Appl.* **2020**, *176*, 1–4. [\[CrossRef\]](#)
51. Yadav, S.; Vishwakarma, V.P. Extended interval type-II and kernel based sparse representation method for face recognition. *Expert Syst. Appl.* **2019**, *116*, 265–274. [\[CrossRef\]](#)
52. Nguyen, K.; Fookes, C.; Sridharan, S.; Tistarelli, M.; Nixon, M. Super-resolution for biometrics: A comprehensive survey. *Pattern Recognit.* **2018**, *78*, 23–42. [\[CrossRef\]](#)
53. Yaddaden, Y.; Adda, M.; Bouzouane, A.; Gaboury, S.; Bouchard, B. User action and facial expression recognition for error detection system in an ambient assisted environment. *Expert Syst. Appl.* **2018**, *112*, 173–189. [\[CrossRef\]](#)
54. Davis, F.D. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q.* **1989**, *13*, 319–339. [\[CrossRef\]](#)
55. Kanak, A.; Sogukpinar, I. BioTAM: A technology acceptance model for biometric authentication systems. *IET Biom.* **2017**, *6*, 457–467. [\[CrossRef\]](#)
56. Wang, J.S. Exploring biometric identification in FinTech applications based on the modified TAM. *Financ. Innov.* **2021**, *7*, 42. [\[CrossRef\]](#)
57. Ajzen, I.; Fishbein, M. *Understanding Attitudes and Predicting Social Behavior*; Prentice-Hall: Hoboken, NJ, USA, 1980.
58. Sheppard, B.H.; Hartwick, J.; Warshaw, P.R. The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research. *J. Consum. Res.* **1988**, *15*, 325–343. [\[CrossRef\]](#)
59. Buabeng-Andoh, C. Predicting students' intention to adopt mobile learning: A combination of theory of reasoned action and technology acceptance model. *J. Res. Innov. Technol. Learn.* **2018**, *11*, 178–191. [\[CrossRef\]](#)
60. Banga, L.; Pillai, S. Impact of behavioural biometrics on mobile banking system. *J. Phys. Conf. Ser.* **2021**, *1964*, 062109. [\[CrossRef\]](#)
61. DeVellis, R.F.; Thorpe, C.T. *Scale Development: Theory and Applications*, 5th ed.; Sage Publications: Washington, DC, USA, 2021.
62. Cronbach, L.J. Coefficient alpha and the internal structure of tests. *Psychometrika* **1951**, *16*, 297–334. [\[CrossRef\]](#)
63. Molnar, G.; Szuts, Z. The role of chatbot in formal education. In Proceedings of the 16th International Symposium on Intelligent Systems and Informatics, Subotica, Serbia, 13–15 September 2018; pp. 197–200. [\[CrossRef\]](#)
64. Anderson, J.C.; Gerbing, D.W. Structural equation modeling in practice: A review and recommended two-step approach. *Psychol. Bull.* **1988**, *103*, 411–423. [\[CrossRef\]](#)
65. Bentler, P.M.; Chou, C.P. Practical issues in structural modeling. *Sociol. Methods Res.* **1987**, *16*, 78–117. [\[CrossRef\]](#)
66. Huang, Y.C. Integrated concepts of the UTAUT and TPB in virtual reality behavioral intention. *J. Retail. Consum. Serv.* **2023**, *70*, 103127. [\[CrossRef\]](#)
67. Rukhiran, M.; Netinant, P.; Elrad, T. Effecting of environmental conditions to accuracy rates of face recognition based on IoT solution. *J. Curr. Sci. Technol.* **2020**, *10*, 21–33. [\[CrossRef\]](#)
68. Song, B.K. E-portfolio implementation: Examining learners' perception of usefulness, self-directed learning process and value of learning. *Australas. J. Educ. Technol.* **2021**, *37*, 68–81. [\[CrossRef\]](#)
69. Acosta-Medina, K.K.; Torres-Barreto, M.L.; Cárdenas-Parga, A.F. Students' preference for the use of gamification in virtual learning environments. *Australas. J. Educ. Technol.* **2021**, *37*, 145–148. [\[CrossRef\]](#)
70. Hassanein, K.; Head, M. Manipulating perceived social presence through the web interface and its impact on attitude towards online shopping. *Int. J. Hum. Comput.* **2007**, *65*, 689–708. [\[CrossRef\]](#)
71. Ngugi, B.; Kamis, A.; Tremaine, M. Intention to use biometric systems. *e-Serv. J.* **2011**, *7*, 20–46. [\[CrossRef\]](#)
72. Norfolk, L.; O'Regan, M. Biometric technologies at music festivals: An extended technology acceptance model. *J. Conv. Event Tour.* **2021**, *22*, 36–60. [\[CrossRef\]](#)
73. Hair, J.F.; Black, W.C.; Babin, B.J.; Anderson, R.E. *Multivariate Data Analysis*, 7th ed.; Prentice-Hall: Hoboken, NJ, USA, 2010.
74. Bagozzi, P.R.; Yi, Y. On the evaluation of structural equation models. *J. Acad. Mark. Sci.* **1964**, *16*, 74–94. [\[CrossRef\]](#)

75. Hair, J.F.; Hult, T.G.; Ringle, C.M.; Sarstedt, M. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*; Sage Publications: Washington, DC, USA, 2014.
76. Sidharta, I.; Priadana, S.; Affandi, A. Extending end-user computing satisfaction on academic information systems. *Indian J. Sci. Technol.* **2016**, *9*, 1–5. [[CrossRef](#)]
77. Ko, C.H. Exploring employees perceptions of biometric technology adoption in hotels. *Biotechnol. Indian J.* **2014**, *10*, 13242–13246.
78. Morosan, C. Theoretical and empirical considerations of guests' perceptions of biometric systems in hotels: Extending the technology acceptance model. *J. Hosp. Tour. Res.* **2012**, *36*, 52–84. [[CrossRef](#)]
79. Labayen, M.; Vea, R.; Flórez, J.; Aginako, N.; Sierra, B. Online student authentication and proctoring system based on multimodal biometrics technology. *IEEE Access* **2021**, *9*, 72398–72411. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.



ภาคผนวก จ

การเผยแพร่ผลงานวิจัยในวารสารวิชาการระดับนานาชาติ ครั้งที่ 2

มหาวิทยาลัยรังสิต Rangsit University

IEEE.org | IEEE Xplore | IEEE SA | IEEE Spectrum | More Sites SUBS

IEEE Xplore® Browse ▾ My Settings ▾ Help ▾ Institutional Sign In

All Q

☐ Search within Publication ADVANCED SEARCH

Browse Journals & Magazines > IEEE Access [?](#)

IEEE Access [🔗](#)



Submit
Manuscript



Add Title
To My Alerts



Add to
My Favorites



Home	Topics	Popular	Early Access	Current Volume	All Volumes	About Journal
------	--------	---------	--------------	----------------	-------------	---------------

3.476

Impact
Factor

0.24936

Eigenfactor

0.613

Article
Influence
Score

6.7

CiteScore

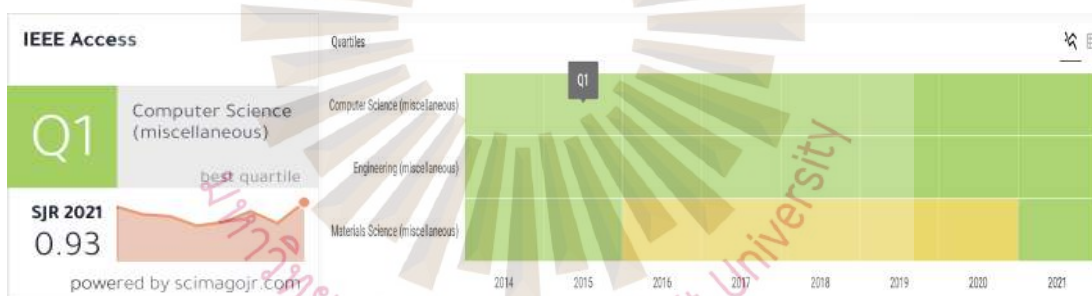
Powered by Scopus



Read the article again: 2015 IEEE Donald G. Fink Award Recipient



Millimeter Wave Mobile Communications for 5G Cellular: It Will Work!
T.S. Rappaport



IEEE Access Editorial Board

▶ **ALPHABETICALLY**



Sonia Aissa
Institut National de la
Recherche Scientifique
(INRS),
Montreal, Canada



**Anuradha
Annaswamy**
MIT,
Cambridge,
Massachusetts, USA



Nirwan Ansari
New Jersey Institute of
Technology,
Newark, New Jersey,
USA



Jun Cai
Concordia University,
Canada,
Montreal, Quebec,
Canada



Kun-Shan Chen
Guilin University of
Technology,
Guangxi, China



J.-C. Chiao
Southern Methodist
University,
Dallas, TX, USA



John W. Evans
NASA,
Washington, DC, USA



**Shaikh Anowarul
Fattah**
Bangladesh University
of Engineering and
Technology (BUET),
Dhaka, Bangladesh



Maya Gokhale
Lawrence Livermore
National Laboratory,
Livermore, California,
USA



Chih-Lin I
China Mobile Research
Institute,
Beijing, China



Giuseppe Iannaccone
University of Pisa,
Pisa, Italy



Yumi Iwashita
NASA-JPL California
Institute of Technology,
Pasadena, CA, USA



Bruce Jacob
Florida Polytechnic
University,
Lakeland, Florida USA



Abbas Jamalipour
University of Sydney,
Sydney, Australia



Bahram Javid
University of
Connecticut,
Storrs, CT USA



Weihua Jiang
Nagaoka University of
Technology,
Nagaoka, Niigata,
Japan



Okay Kaynak
Bogazici University,
Istanbul, Turkey



**Germano Lambert-
Torres**
Gnarus Institute,
Itajuba, Brazil



Joy Laskar
Maja Systems,
Milpitas, California,
USA



Victor Leung
The University of British
Columbia,
Vancouver, British
Columbia, Canada



Shengtao Li
Xi'an Jiaotong
University,
China



Qilian Liang
University of Texas at
Arlington,
Arlington, Texas, USA



Leda Lunardi
North Carolina State
University,
Raleigh, NC, USA



Michal Mrozowski
Gdansk University of
Technology,
Gdansk, Poland



Michele Nappi
University of Salerno,
 Fisciano, Italy

Volume 11: 2023

Showing 1-6 of 6

Refine

Author

Affiliation

Supplemental Items

Subject Category

☐ Select All on Page
 Sort By

Newest

☐ **IoT-Based Biometric Recognition Systems in Education for Identity Verification Services: Quality Assessment Approach**
 Meennapa Rukhiran; Sethapong Wong-In; Paniti Netinant
 Publication Year: 2023 , Page(s): 22767 - 22787
 ▶ Abstract HTML

☐ **The Use of Digital Peer Assessment in Higher Education—An Umbrella Review of Literature**
 Gitte Van Helden; Vivian Van Der Werf; Gillian N. Saunders-Smits; Marcus M. Specht
 Publication Year: 2023 , Page(s): 22948 - 22960
 ▶ Abstract HTML

☐ **Impact of Electrical Engineering Didactic Videos During Emergency Remote Learning**
 Ruben Lijo; Eduardo Quevedo; Jose Juan Castro; Ricard Horta
 Publication Year: 2023 , Page(s): 19622 - 19634
 ▶ Abstract HTML

☐ **Educational Recommendation System Utilizing Learning Styles: A Systematic Literature Review**
 Vivat Thongchotchai; Yasuo Kudo; Yoshifumi Okada; Kazuhiko Sato
 Publication Year: 2023 , Page(s): 8988 - 8999
 ▶ Abstract HTML

☐ **Learning Software Project Management From Analyzing Q&A's in the Stack Exchange**
 Alireza Ahmadi; Fatemeh Delkhosh; Gouri Deshpande; Raymond A. Patterson; Guenther Ruhe
 Publication Year: 2023 , Page(s): 5429 - 5441
 ▶ Abstract HTML

☐ **The Effectiveness of a Technology-Based Isometrical Transformation Flipped Classroom Learning Strategy in Improving Students' Higher Order Thinking Skills**
 Kalaarasi Nadarajan; Abdul Halim Abdullah; Najua Syuhada Ahmad Alhassora; Nor Hasniza Ibrahim; Johari Surif; Dayana Farzeeha Ali; Norasykin Mohd Zaid; Mohd Hilmi Hamzah
 Publication Year: 2023 , Page(s): 4155 - 4172
 ▶ Abstract HTML

Received 26 January 2023, accepted 1 March 2023, date of publication 6 March 2023, date of current version 9 March 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3253024



RESEARCH ARTICLE

IoT-Based Biometric Recognition Systems in Education for Identity Verification Services: Quality Assessment Approach

MEENNAPA RUKHIRAN¹, SETHAPONG WONG-IN², AND PANITI NETINANT¹¹Faculty of Social Technology, Rajamangala University of Technology Tawan-ok, Chanthaburi 22210, Thailand²College of Digital Information Technology, Rangsit University, Lak Hok, Pathum Thani 12000, Thailand

Corresponding author: Paniti Netinant (paniti.n@rsu.ac.th)

ABSTRACT Traditional identity verification of students based on the human proctoring approach can cause a scam identity verification and ineffective processing time, particularly among vast groups of students. Most student identification cards outdated personal information. Several biometric recognition approaches have been proposed to strengthen students' identity verification. Most educational adoption technologies struggle with evaluation and validation techniques to ensure that biometric recognition systems are unsuitable for utilization and implementation for student identity verification. This study presents the internet of things to develop flexible biometric recognition systems and an approach to assess the quality of biometric systems for educational use by investigating the effectiveness of identity verification of various biometric recognition technologies compared to the traditional verification method. The unimodal, multimodal, and semi-multimodal biometric technologies were tested using the developed internet of things-base biometric recognition systems examined by applying the proposed quality metrics of scoring factors based on accuracy, error rate, processing time, and cost. Hundreds of undergraduate exam takers were a sample group. Key findings indicate that the designed and presented systems suitably attain identity verification of exam students using a unimodal biometric. The unimodal facial biometric system promises excellent support. A unimodal fingerprint biometric system ensures second excellent aid for student identity verification. However, multimodal and semi-multimodal biometric systems provide better accuracy with fewer handling times and higher costs. This study contributes significantly to the knowledge of utilizing biometric recognition for identity verification in smart educational applications.

INDEX TERMS Biometrics, recognition, identity, verification, Internet of Things, quality assessment.

I. INTRODUCTION

The internet of things (IoT) has ushered in a new era of connectedness, allowing numerous objects and systems to communicate and share data effortlessly [1]. This has resulted in various applications, including biometrics [2]. In recent years, considerable advances have been in the IoT research. Incorporating IoT technology into biometric recognition systems enables real-time monitoring and remote system access [3], thereby increasing system accessibility and flexibility. Moreover, IoT technology can improve the

accuracy and efficiency [4] of biometric recognition systems by enabling the integration of several biometric modalities, such as facial recognition and fingerprint identification [5]. These systems can leverage physiological or behavioral characteristics to identify individuals uniquely, lower the chance of cheating, and enhance educational security [6]. IoT-based biometric recognition systems can provide a more secure and convenient method of identifying and confirming students during classes and exams in the educational setting. However, these studies also identify key implementation issues, such as assuring the accuracy and dependability of the identification process, protecting students' privacy, and controlling implementation costs.

The associate editor coordinating the review of this manuscript and approving it for publication was Rebecca Strachan.

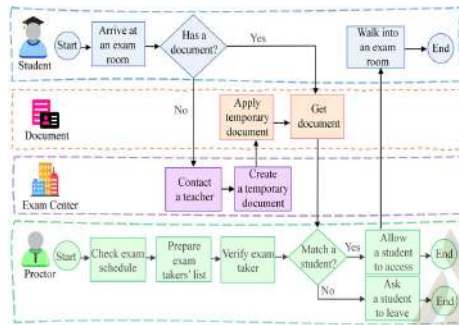


FIGURE 1. Traditional approach of examination takers' identification verification.

Moreover, information technology is a widely used in a variety of educational tasks. To become a smart school digital framework [7], numerous schools implement systems such as registration systems, and schedule management systems in their institutions [8]. However, the examination system is one of the most important factors in determining each student's academic achievement. Although many educational institutions have incorporated an electronic system into examination tasks, such as web-based examinations [9], online testing [10], and online examination systems [11], previous research has focused primarily on how to manage basic information and general tasks [12]. Student verification is the examination's most important and primary procedure for identifying the correct candidate for school, class, and examination authentications. Numerous educational institutions continue to use the conventional method, which includes personal documentation (e.g., student card and ID card), to verify exam takers. One of the most prominent issues with the conventional examination approach is that the proctor must be confident, and the student is the actual exam taker. No technological tools are available to the proctor to verify student identity. Even if a student's photograph appears on a personal document, it may not be possible to identify the actual exam taker using the photo. The student's personal document is also susceptible to lose or damage.

Checking a student's identification documents, such as a personal identification card, a student identification card, and a driver's license card is the standard procedure for confirming a student's eligibility to take an exam. Numerous complexities associated with this approach. At Valaya Rajabhat University in Thailand, for instance, the conventional approach to verifying student identity documents prior to entering an examination room is depicted in Fig. 1.

As shown in Fig. 1, verifying the identity of each exam candidate involves multiple steps and considerations. A student must present his/her document to a proctor prior to taking an exam. The proctor must then verify and match the information as well as the photo on the identification document to the specific student. There are multiple potential

causes for student verification, the first of which is how the proctor determines that the student is the actual exam taker. The student is granted access to the examination room if the student and the identification document match. The second scenario addresses the proctor's actions in the absence of an identification document. The proctor must contact the administrator of the registrar office at the university. The administrator must then provide the students with a one-day temporary identification card. In the third scenario, if the proctor suspects an exam taker, the student may request additional documentation or leave the examination room. Typically, proctors walk around the examination room to collect each student's signature. Consequently, this action may disturb the concentration of other test-takers during the exam.

An automated verification system is a contemporary method of identifying the correct individual. Several automated verification systems that employ biometric technologies have been proposed. The use of biometric technology in identity verification systems has several advantages over traditional identity verification. Access control using fingerprint recognition [13], face recognition to grant access [14], healthcare [15], citizen identification [16], [17], security systems [18], finance [19], airport [20], canteen management systems [21], visitor management systems [22] and parking management systems [23], [24], [25] have addressed the advantages of implementing biometric technologies. Biometric technology is a practical and useful alternative for verifying exam takers. Students were not required to provide or present identification during the examination. However, automated student verification requires extensive research into personal information technology verification design and development. Certain researchers have implemented a unimodal biometric technique as a face or voice-only biometric technology. Multiple biometric modalities are utilized in multimodal biometrics to ensure system quality and prevent biometric systems from having a single point of failure [26]. The biometric protocol gaps between unimodal and multimodal biometrics for identity verification in education are primarily concerned with the cost and accuracy of identity verification [27], [28]. The system evaluation is a crucial stage when standard objectives are evaluated to compare the new system's performance to those of the existing system [29]. There has never been a system that uses multimodal biometrics to verify the identity of students taking exams. Therefore, this research proposes an education-based biometric recognition system for identity verification services that focuses on a quality assessment metric.

This study makes three contributions to the scientific community as follows:

- The authors propose a system design and software development for examination management and biometric recognition systems using the IoT technology named biometric examinee personal verification system (BEPVS). The proposed system can support face and fingerprint recognition using many verification protocols.

- The authors compare the system quality of unimodal, semi-multimodal, and multimodal biometric examination verification systems. The quality measurement metrics for the proposed system are a pioneer investigation. The practical application's quality measurement metrics of biometric verification systems consisted of accuracy rate, error rate, response time, and cost.

- A relevant evaluation result for measuring the quality of each biometric verification protocol is analyzed to summarize the optimal biometric technology of IoT-based development.

The rest of the paper is organized as follows: Section II presents the literature review and theoretical background. The methodology used in this paper is deliberated in Section III. The experimental evaluation is described in Section IV. Section V reports the results and presents the discussion. Finally, Section VI summarizes the conclusions of this research.

II. LITERATURE REVIEW

This section summarizes the biometric technology principles, unimodal and multimodal biometric technologies, biometric verification systems in education, Internet of Things platforms for biometrics, and open-source computer vision (OpenCV) image processing for application development. The following section describes the works mentioned in this article.

A. BIOMETRIC TECHNOLOGY

Surveillance, identification, and access control are the three most prevalent biometric technology uses [30]. Numerous types of biometric technology-related research include algorithms, architecture, modalities, and applications. Physical biometrics focuses on human physical measurements such as the face, fingerprints, palm, retina, iris scans, and hand geometry. Behavior biometrics focuses on human operations, including voice, signature, gait, keystroke dynamics, and other activities (for instance, behavioral biometric authentication on smartphones [31]). Chemical biometrics are concerned with chemical identifiers, such as a person's scent. The biometric system can be classified as either unimodal or multimodal [32].

B. UNIMODAL BIOMETRIC TECHNOLOGY

The unimodal system uses a single biometric verification source, such as the face, iris, fingerprint, palm, or other distinctive human body parts.

Face recognition - The unimodal system employs a single biometric verification source, such as the face, iris, fingerprint, palm, or other distinctive human body parts. The human face is a well-known biometric characteristic utilized in various applications, including criminal identification, security systems, forensics, surveillance systems, credit card verification, etc. According to [33], the face is a passive biometric, and face images are used for effective development regardless of the individual's participation. The facial recognition system is a biometric artificial intelligence

system that identifies individuals by analyzing patterns of facial texture and shape patterns. Face biometrics primarily rely on visible imagery because temperature and eyewear have no effect on face verification.

Face recognition is a commonly used method for identifying or validating a person, and it is utilized in a variety of scientific disciplines. The three primary aspects of face biometrics are face recognition, feature extraction, and face matching. Recent studies [34], [35] focused on face recognition techniques and implemented real-time face recognition systems using Raspberry Pi, internet of things device. Yadav and Vishwakarma [36] proposed a novel, sophisticated, and efficient framework based on the interval type-II fuzzy membership with the kernel-based sparse method. The percentage of pixels contributing to the image was determined using interval type-II fuzzy logic, specifically an extended interval type-II membership function. Using the K nearest neighbor and Euclidean distance metric for sparse representation, the experimental analysis revealed a two to ten percent increase in accuracy over the current standard.

Kas et al. [37] presented a novel method for developing a feature descriptor called mixed neighborhood topology cross decoded patterns (MNTCDP) that can be combined across platforms to produce robust, computationally affordable, and simple solutions. MNTCDP depends on the pattern encoding scheme and neighborhood topology to produce a stable and discriminative face representation. Face alignment and detection supervised image classification, and the K-Nearest Neighbor classifier can improve precision rates. Experiments were conducted on the YALE, ORL, FERET, and AR datasets under various illumination conditions, and it was determined that the proposed MNTCDP descriptor exhibits outstanding performance. Yaddaden et al. [38] presented an efficient facial recognition system based on a Convolutional Neural Network architecture and radio-frequency identification (RFID) tags equipped with an error detection module. The experiment was conducted on five benchmark facial expression datasets and yielded promising results above 95 percent, with a false positive detection rate that was decreased by 20 percent and consistently improved results.

Fingerprint recognition - Fingerprint recognition is a well-established biometric technique. Hardware is used to collect and scan fingerprint data by the development system. Each fingerprint recognition technique utilizes a unique fingerprint data format. Awojide et al. [39] developed a biometric fingerprint system for candidate authentication in Nigeria Institution Examinations using online-based pattern recognition. Taileb [40] provided fingerprint recognition and RFID technology to verify students. Tatar [41] presented a novel algorithm for fingerprint recognition to illustrate research employing a novel algorithm. A finger vein recognition system has two primary phases: enrollment and verification, according to Wencheng et al. [42]. First, finger vein images are captured and enhanced for quality.

The extracted features are then saved as templates. In the second authentication phase, a vein sample is extracted from the user's finger for testing, followed by preprocessing and feature extraction techniques. The testing features were compared to the stored templates to display the verification result. In their study, Xi et al. [43] proposed a framework for a biometric system based on the finger vein modality, employing the discriminative binary code method and the PolyU and MLA databases. Moreover, they use supervised information and support vector machines (SVM) to make discriminative binary codes (DBC) more discriminatory and shorter. Various biometric systems, including Noma-Osaghae et al. [44], have granted door access using an iris and fingerprint verification.

C. MULTIMODAL BIOMETRIC TECHNOLOGY

Numerous researchers have examined multimodal biometric verification to improve the performance of the biometric recognition systems used to verify exam takers. Emmanuel and Ogadimma [45] created a multimodal cloud-based biometric service for online examinations. The proposed system uses face and voice recognition to access cloud services so students can access web-based examinations. Mir et al. [46] designed a novel framework for multimodal systems. The system utilized face and fingerprint images with block-based and feature-image matrices. The proposed method retrieved the semantic features of the middle layer of local biometric features, resulting in improved characterization capabilities, reduced dimension, and high accuracy rates for multimodal biometrics. They achieved highly stable and generalizable outcomes using the variational bayesian extreme learning machine (VBELM). The experimental results demonstrated greater precision, efficiency, and consistency in testing than conventional techniques.

Gomez-Barrero et al. [47] presented a method for developing a multimodal biometric system based on the homomorphic encryption method, with all encrypted database information. Multimodal fusion utilized the characteristics, scores, and decision levels. On Biosecurity identification's online signature and fingerprint database, experiments were conducted. The system complied with the ISO/IEC 24744 requirements. Walia et al. [48] proposed a robust biometric system based on the optimal score-level fusion model and multiple identifiers. The system considered iris, finger vein, and fingerprint biometric modalities. The backtracking search optimization technique and proportional conflict redistribution rules were utilized in this study. Using multiple traits and a fusion approach to biometric scores produced better results than a single biometric. The multimodal system can be divided into the following four subcategories:

- **Multiple modalities:** the examination uses more than two types of biometric technology, such as face image and fingerprint verification. For instance, Ammour et al. [49] utilized the face and iris to identify a system user. Gunasekaran et al. [50] fused the face, fingerprint, and iris for the purpose of identifying individuals.

- **Multiple sensors:** the same inspection pattern is utilized with multiple sensors, such as images from two cameras. For instance, Zhao et al. [35] utilized two mobile phone cameras to detect the objects.

- **Multiple features:** multiple algorithms are used to extract images or data from the source [51], such as extracting fingerprint images using the first and second methods.

- **Multiple and repeated occurrences:** multiple biometric forms are used, such as left and right iris images for iris recognition, or the same biometrics are used multiple times. A brief overview of deep learning techniques for the re-identification of individuals. Fenu et al. [52] and various publications on multimodal biometrics presented a multibiometric system for continuous student authentication in e-learning platforms that uses face, voice, touch, mouse, and keystroke verification to authenticate students for e-learning. Traore et al. [53] designed a framework for a multimodal biometric system for online examinations via continuous image capture with a webcam.

D. BIOMETRIC EXAM TAKER VERIFICATION SYSTEM

Many obstacles are involved in the biometric verification of test-takers in higher learning. To support the biometric verification technology, a number of factors, including the integration of an existing system, the developers' skills, and the technology's maturity, must be considered. Using fingerprint recognition [54] provided a safety infrastructure for the online examination. The biometric system developed to authenticate examinees in Nigeria was created by [45]. Another reason for utilizing biometric technology in educational institutions, such as those researched by [46]. The objective of Okokpuije et al. [55] was to develop an iris-based biometric system for verifying the student's attendant. A smart door using biometric development enhanced a security system [22]. The BEPVS [56] was presented with the conceptual design model for verifying exam takers, which included components for developing a biometric system. The six components of an examinee biometric information system are illustrated in Fig. 2 of the BEPVS conceptual model. The purpose of this framework is to demonstrate the creation and implementation of the biometric exam-taker verification system. Examiner information, the examination information system, the result and output, biometric technology, the biometric examinee personal verification system, and the intelligence system are the six principal components of the system development framework.

The BEPVS conceptual framework also presented the specifics of a revised software design model created software for use in an educational institution. Fig. 3 depicts the BEPVS architecture, consisting of thirteen system components demonstrating the design and development of a biometric exam-taker verification system.

Exam taker information is provided by examiner information (EI) component. The examination information system (EMS) component provides an examination information

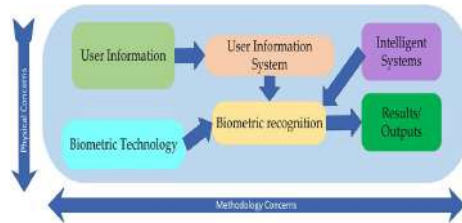


FIGURE 2. Revised BEPVS conceptual framework.

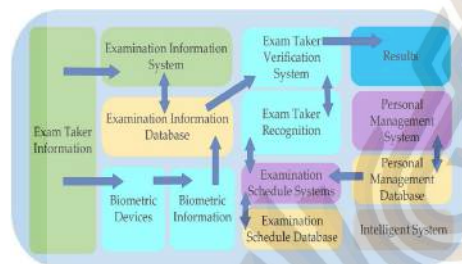


FIGURE 3. Biometric recognition framework in education.

management system. A component of the examination information database (EIDB) manages the student database by communicating with a component of biometric information (BI) stored on a component of the biometric device (BD). Exam taker verification system (ETVS) component responds to detect and identify students using exam taker verification (ETV), examination schedule database (ESSDB), and examination schedule system (ESS). A Personal Management System (PMS) and personal management database (PMDB) components oversee student data creation, retrieval, modification, and deletion. A personal management system (PMS) is an administration system of faculty in the educational institute. A result component provides feedback on a student's system identification. An intelligent component of the system prepares for a future support system for artificial intelligence.

E. BIOMETRIC TECHNOLOGY ON INTERNET OF THINGS PLATFORM

The IoT is currently the most popular platform for human life support, particularly in education [1], [7], [8]. Utilizing biometric technology on IoT platforms has the advantages of being economical, compact, and mobile. Recent studies have demonstrated various biometric applications utilizing the Internet of Things to create systems and applications. Emerging internet of things services in smart cities, industry, smart homes, and personal assistants, among others, require security at multiple stages. Intruders may inject fabricated data into the communications of the internet of things. Applying security to IoT devices makes it possible to realize mobility, portability, and multiple services. These issues are

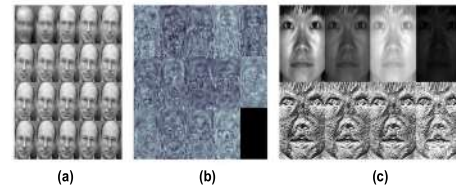


FIGURE 4. (a) Eigenfaces, (b) Fisherfaces, and (c) LBPH in OpenCV.

circumvented by utilizing biometric security, which does not require action or memory. Biometric authentications are popular, more reliable, and user-friendly than conventional methods. The previous research has discussed IoT issues and challenges regarding biometric security and application, including where biometrics can be integrated into IoT infrastructure [26], [51], [57].

F. OPENCV FACE RECOGNITION DEVELOPMENT

OpenCV is a well-known artificial intelligence library for image processing founded in 1999 by Intel. The cross-stage library emphasizes continuous image processing and includes non-patent-protected implementations of the latest computer vision calculations. OpenCV now includes a programming interface for the C, C++, Python, and Android programming languages. OpenCV is distributed under the BSD license, which is used for academic projects and commercial products. Fig. 4 illustrates OpenCV's three primary algorithms.

Eigenfaces - The image depiction is rendered with a high degree of dimension. Two-dimensional PQ grayscale images span PQ-dimensional vector space, so a 100×100 pixel image resides in a 10,000-dimensional image space. A developer can settle on any variation in relevant data and search for information. Pearson [58] and Hotelling [59] independently proposed the Principal Component Analysis (PCA) to transform a large number of possibly related factors into a more compact arrangement of uncorrelated factors. Frequently, associated factors represent a high-dimensional dataset. The majority of the data is comprised of a handful of significant aspects. The PCA technique tracks down the bearings with the best difference in information called the head parts. Fig. 4 (a) illustrates the Eigenfaces of OpenCV image processing.

Fisherfaces - Principal component analysis (PCA), the core of the Eigenfaces method, identifies a direct mixture of components. The method accentuates the extreme fluctuation in data. Although this is an unquestionably excellent method for addressing data, it does not consider classes. As a result, many discriminative data could be lost when discarding parts. Imagine a scenario in which an external source modifies the information of a user. Let there be no darkness. The components distinguished by a PCA lack discriminative data, so the projected examples are dispersed, making it impossible to characterize the population. The fisherfaces of OpenCV image processing are depicted in Fig. 4 (b).

Local binary pattern histogram (LBPH) - Eigenfaces and fisherfaces are adaptable to support a comprehensive acknowledgment strategy. Information is represented as a vector in high-dimensional image space. High-dimensionality is awful, so a lower-dimensional subspace is distinguished and (presumably) utilized to store useful information. The Eigenfaces strategy expands the total dissipate, which can cause issues if an external source fluctuates since parts with the greatest difference in overall classes are not useful for arrangement. The authors have utilized a linear discriminant analysis to safeguard some discriminative data, which was enhanced according to the fisherfaces method.

Numerous types and techniques have been investigated by analyzing the development performance of biometric systems. Under various weather conditions, Ahsan et al. [60] compared the performance of three facial recognition algorithms in OpenCV, including eigenface, fisherface, and local binary pattern histogram-based methods. In their research, the evaluation criteria were the accuracy, precision, recall, F1 score, and execution time. According to the findings of their study, LBPH had better outcomes than other treatments. Fig. 4(c) depicts the LBPH of the OpenCV image processing. The factors used to assess biometric efficiency in the various domains are presented in Table 1.

III. RESEARCH MODEL AND HYPOTHESES

This primary objective of this study was to experimentally investigate a biometric recognition system for education. This investigation commences with a framework design for IoT-based biometric technologies, which consists of designing and developing a biometric exam-taker management system and biometric verification architecture. The authors developed an IoT-based biometric verification system that supports various biometric technologies, including face and fingerprint-based unimodal, multimodal, and semi-multimodal biometrics. The developed system's effectiveness and efficiency have been evaluated. The accuracy rate, error rate, response time, and cost are used to compare the effectiveness and efficiency of using a biometric verification system for exam takers. Four biometric approaches involve the experimental study of the system's evaluation: zero-biometric (Z), unimodal biometric system (U), multimodal biometric system (M), and semi-multimodal biometric system (S). Using face and fingerprint experiments, the authors implement a biometric verification system for each testing group. Identifying the sampling group, testing the system, and collecting data for each testing group are the three aspects of each experiment. This study has compared each experimental outcome by determining which biometric protocol best suits the biometric verification system for educational applications.

A. RESEARCH OBJECTIVES AND HYPOTHESES

The authors have adopted the BEPVS conceptual framework [56] depicted in Fig. 3. To investigate the research

TABLE 1. Survey of performance evaluation criteria in biometric system usages.

References	Evaluation Criteria	Factors
Dube <i>et al.</i> [61]	A framework for evaluation of biometric based authentication system	- Performance - Privacy - Security
Kanak and Sogukpinar [62]	BioTAM: A technology acceptance model for biometric authentication systems	TAM + Trust - Public willingness - Confident - Estimate Privacy - Estimated Security
Zhou [63]	Evaluation of biometric recognition in the Covid-10 period	Universality, Permanency, Uniqueness, Accuracy, Acquisition, Usability, Safety
Oh <i>et al.</i> [64]	Usability evaluation model for biometric system considering privacy concern based on MCDM model	- Technical aspect (Effectiveness, Efficiency) - Ergonomic aspect (Anthropometry-fit, Accessibility, Affordance Psychological aspect) - Psychological aspect (privacy concern, Satisfaction)
Malatji <i>et al.</i> [65]	Acceptance of biometric authentication security technology on mobile devices	Performance, User Acceptance, Acquisition Device
Ammour <i>et al.</i> [48]	Multimodal biometric identification system based on the face and iris	Accuracy (FAR, FRR)
Siddique <i>et al.</i> [66]	Reliability and acceptance of biometric system in Bangladesh: Users perspective	Reliability, Ease of use, Security, Cost
El-Abed <i>et al.</i> [67]	Evaluation of biometric systems	Universality, Uniqueness, Permanency, Collectability, Acceptability
Ahsan <i>et al.</i> [60]	Evaluating the performance of eigenface, fisherface, and local binary pattern histogram-based facial recognition methods under various weather conditions	Accuracy, Precision, Recall, F1 Score, Execution Time

objectives, the practical implementation of an IoT-based biometric system for exam taker verification is also created. This section describes the design and development of the experimental system in accordance with the IEEE systems design—software design descriptions (SDD) standard [68] and systems and software engineering - Systems and software quality requirements and evaluation (SQuaRE) [69]. Use-case diagrams represent the context viewpoint, class diagrams represent the information viewpoint, deployment diagrams show the composition viewpoint, and graphical user interface (GUI) diagrams represent the interface viewpoint, and sequence diagrams represent the interaction

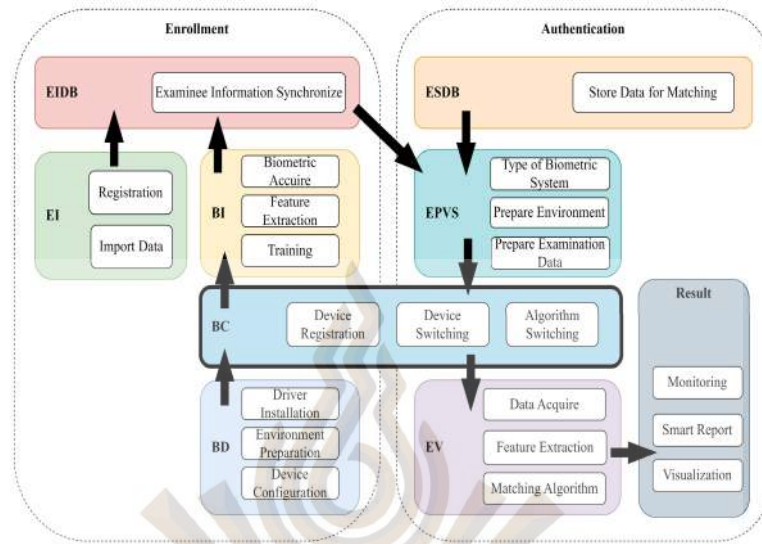


FIGURE 5. Biometric verification processing framework.

viewpoint. Using this study's quality assessment metric approach, the following are the primary concerns for confirming and evaluating the practical use of the IoT-based biometric recognition system for identity verification services.

Using IoT technology, the first objective is to propose software design and development for examination management and biometric recognition systems with face and fingerprint. IoT-based biometric examination verification systems can utilize unimodal, semi-multimodal, or multimodal biometrics. Consequently, the feasibility and promise of biometric technologies used for student identity verification can be evaluated by effectiveness and efficiency to determine if the IoT-based biometric system for verifying exam takers could adequately replace traditional proctoring for student identity verification.

The secondary objective is to examine quality measurement metrics for the biometric verification system by analyzing biometric effectiveness in an actual exam environment. The proposed quality metric for biometric verification of students in actual examination classrooms could evaluate and ensure biometric quality assurance of accuracy rate [49], error rate [23], [70], response time [46], and cost [66].

The hypotheses of this study are identified as contributing to biometric assessment quality assurances for educational applications. The following are the answers to the questions posed by the hypothesis:

Hypothesis 1 (H1): The quality of the unimodal biometric system for verifying exam candidates is superior to that of a conventional system.

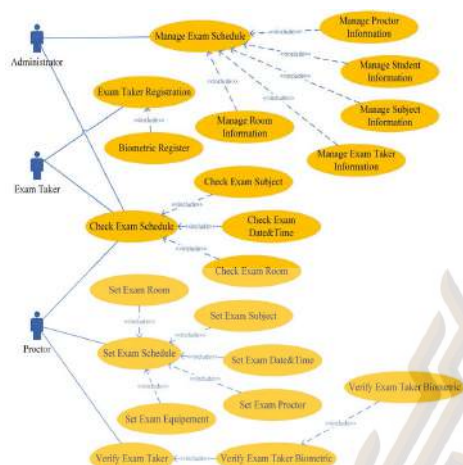
Hypothesis 2 (H2): The quality of the multimodal biometric system for verifying exam takers is superior to that of a conventional system.

Hypothesis 3 (H3): The multimodal biometric system for verifying exam takers is of a higher quality than the unimodal biometric system.

B. BIOMETRIC DATA ENROLLMENT

Fig. 5 depicts the system architecture derived from the revised design model of a biometric examinee personal verification system as illustrated in Fig. 3. Examinee registration, biometric collection, biometric verification, biometric databases, and verification results are components of the biometric verification processing framework. The framework comprises two major components: exam taker enrollment and authentication.

The data enrollment or training phase involves collecting test-takers biometric information into a database. The information about the exam taker is typically personal information, including biometric data. The system can collect personal information from existing data by accessing student identification numbers. However, biometrics collection is contingent on the biometric trait and devices used. This study employs the face and fingerprint as biometric system characteristics. Face and fingerprint biometrics share similar data collection procedures. By implementing an IoT-based biometric verification system in front of the examination room, the biometric registration device must install drivers, set the verification environments, and configure parameters to function correctly. After acquiring a student's face and fingerprint, the feature extraction processes commence, and



the system registers students' biometrics and information as a training set in a database. Face and fingerprint-based multimodal biometric systems have been investigated in this study. Therefore, two biometric scanners are configured to support dynamic manners. Each scanner device can seamlessly switch between unimodal and multimodal modes. The IoT-based biometric verification system box is developed as a biometric system controller. The smart box can scan facial and fingerprint biometrics and manage biometric recognition algorithms for experimental data enrollment.

C. EXAMINATION MANAGEMENT SYSTEM DESIGN

Fig. 6 depicts a use-case diagram that describes the system's actors and their respective responsibilities. Beginning with a user needs survey, the authors analyzed and designed the exam taker biometric verification system using a use-case diagram containing three actors: the exam taker, the administrator, and proctor. The test-taker biometric verification system consists of twenty-two key processes. Administrators

D. INFRASTRUCTURE DEVICES

The IoT-based biometric verification system consists of the hardware of the system, face images and fingerprint template-based biometric technologies. This research uses two biometric devices: an 8-megapixel Raspberry Pi camera for face recognition and a fingerprint scanner (Arduino compatible). Raspberry Pi cameras can capture 1080p images with a high resolution and can be completely programmed. A Raspberry Pi 4 8GB is connected to a camera, fingerprint scanner, and monitor in front of an exam room. This research uses two Raspberry Pi Camera (8-megapixel) biometric devices for face recognition. The Raspberry Pi camera can capture high-resolution images, 1080p video in full HD, and programmable code. Fingerprint scanners compatible with Arduino are used for fingerprint recognition. In Table 2, the specifics of each device are listed.

E. IOT-BASED BIOMETRIC VERIFICATION SYSTEM DESIGN AND DEVELOPMENT.

Fig. 8 represents an overview of the experiment's IoT-based biometric verification system architecture. EDIB, ESSDB, and PMDB were developed using MySQL server as a centralized biometric database to support web-based application programs for exam taker verification systems. Students face images, and fingerprint templates were collected and stored in a centralized database. Each training dataset for an IoT-based biometric verification system must be used to train the two biometrics listed below:

- **Face recognition training:** The system is developed using the OpenCV library with Python and the LBPH model as a face recognition algorithm to recognize a student's face.
- **Fingerprint recognition training:** The OpenCV library and Python programming language, in conjunction with the scale-invariant feature transform (SIFT) algorithm, are used to extract key points and detect descriptors for the best-retained features.

After receiving the examination room's student roster, the proctor logs into the system during the verification phase. The students formed a single line in front of the examination room, awaiting verification. Each student requires to use face

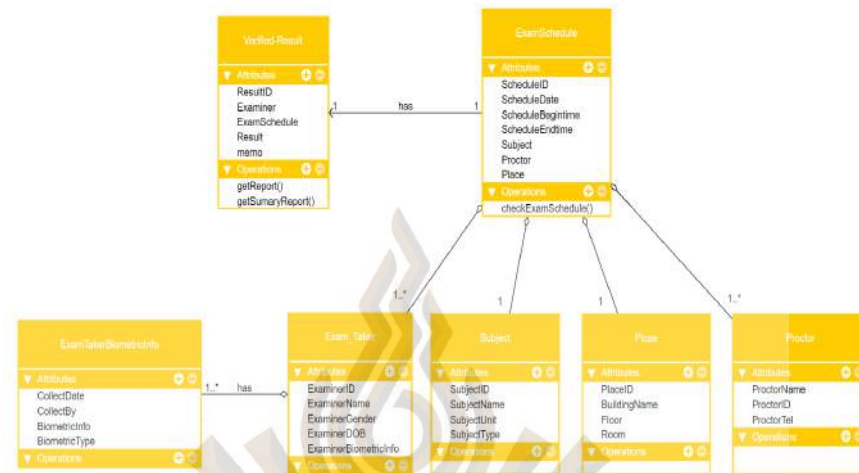


FIGURE 7. Class diagram of exam taker biometric verification system.

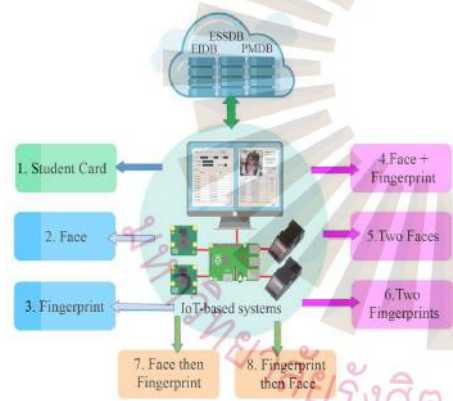


FIGURE 8. Overview of experimental scenarios of IoT-based biometric identity recognitions system.

and fingerprint biometric verification to identify the identity phase as follows:

- Face recognition matching algorithm: The system matches biometric data utilizing the LBPH model within the OpenCV framework.
- Fingerprint recognition matching algorithm: The authors used feature matching with the fast library for approximate nearest neighbors (FLANN) algorithm to match the fingerprint image of the exam taker with the pattern from the database.

The quality scores and scanning times for student recognition were recorded in a database log and displayed on an LCD screen after biometric verification.

This study categorizes the potential biometric verification case studies into eight identity verification approaches. The first method employs identification cards. Other approaches rely on biometrics for identification. The second method employs facial biometrics, while the third method employs fingerprint biometrics. The fourth method employs face and fingerprints. The fifth method uses a face captured by two cameras, while the sixth method uses fingerprints captured by two scanners. The seventh method uses the face, then the fingerprint, while the eighth method uses the fingerprint, then the face. Each biometric protocol's configuration is handled by a single-board computer (Raspberry Pi 4). Over a wireless network, the Raspberry Pi 4 connected to biometric devices captures a student's identity and retrieves the student's biometric from the database system to determine whether the student is authentic or fraudulent.

IV. METHODOLOGY

The experimental methodology includes collecting and analyzing datasets, training and testing datasets, comparing various biometric verification approaches, and evaluating biometric quality criteria for effectiveness and efficiency.

A. DATA COLLECTION AND ANALYSIS

The preparation and conduct of this study occurred between January and October of 2022. This research meeting was open to sixty undergraduates from three examination classrooms at the Valaya Alongkorn Rajabhat University, Thailand. The authors explained the research's objectives, contents, and methodology to the students. When students had questions, the authors provided online contact information to the researcher and research assistant. The authors informed the students through consent that they would provide facial and

TABLE 2. Biometric device specification in development.

Biometric Device	Specification	Cost
	Raspberry Pi Camera (8mp) - Sensor: Sony IMX219 - Sensor Resolution: 32480 x 2464 (8 megapixels) - Sensor Image Area: 3.69 x 2.81 mm - Pixel Size: 1.12um x 1.12um - Optical Size: 1/4" - Video: Dimension: 25mm x 23mm x 9mm / 0.98" x 0.90" x 0.35" 1920 x 1080 (1080p), 30 fps 1280 x 720 (720p), 60 fps 640 x 480 (480p), 90 fps - Weight: (Camera board + attached cable): 3.4g	\$40
	Fingerprint reader Adafruit R305 - Fingerprint Imaging Time: less than 1 second - Match Mode: Compare Mode 1:1 - Search Mode: 1: N - Window Area: 14 mm. x 18 mm. - Signature File Size: 256 bytes - Template File Size: 512 bytes - Storage Capacity: 162 templates - Safety Ratings: 1 (low) to 5 (high) - False Acceptance Rate: less than 0.001% - False Reject Rate: less than 1% - Interface: Serial UART TTL - Baud Rate: 57600 by default (9600, 19200, 28800, 38400, 57600 configurable) - Working Temperature Rating: -20 to +50 Degree Celsius - Working Humidity: 40 to 85 %RH - Full Dimension: 56 mm. x 20mm x 21.5mm (H x W x L)	\$55
	Raspberry Pi 4 Model B - BCM2711 SoC - 8GB DDR4 RAM - USB 3.0 - PoE Enabled	\$335
	LG 50 inches UQ8000PSC UHD 4K Smart TV	\$315
	Raspberry Pi Black - Grey QWERTY (UK) Raspberry Pi Keyboard	\$20
	256 GB MICRO SD Card	\$40
	Pair wires - GPIO Extender cable male female 40 Pin - Jumper wire male to female	\$10

fingerprint biometric data voluntarily. Students' information confidentiality and biometric information were safeguarded and only used to verify their identity in front of examination rooms on scheduled examination dates. All the students consented to participate in the research project. To ensure the accuracy of the biometric data, each student's face and fingerprint recognition during the training and testing phases must reach an accuracy score of 85 percent. The study

recruited thirty students by dividing each sample group into two types of exam takers: five fake exam takers and twenty-five real exam takers. The first sample group confirmed each student's identity using an IoT-based biometric verification system. A second sample group was subjected to traditional examination proctoring in which an identification document verified each student's identity.

By comparing zero-biometric, unimodal, multimodal, and semi-multimodal biometrics, the data analysis measured the quality of an IoT-based biometric verification system. As depicted in Fig. 9, the metric performance of the quality measurement could be assessed using a combination of conventional and biometric verification techniques. The protocols for detecting student identification consisted of 1) student identification for a traditional method of verification as a zero-biometric. 2) The facial unimodal biometric system recognizes only the face. 3) Only fingerprint recognition is supported for the unimodal biometric system. 4) Face and fingerprint verifications for a multimodal biometric system. 5) Face recognition through two cameras for a multimodal facial biometric system. 6) Fingerprint examinations utilizing two scanners for the multimodal fingerprint biometric system. 7) Face and then fingerprint verification for the semi-multimodal biometric system. 8) For the semi-multimodal biometric system, fingerprint verification is followed by face verification. Comparing traditional and biometric verification methods, the system then calculates the exam-identity taker's recognition results for quality scoring.

B. TRAINING AND TESTING DATASET

This experiment's dataset preparation consisted of two distinct phases: preparation for facial recognition and preparation for fingerprint recognition. The development of the biometric recognition system utilized OpenCV and Python to train and test a portion of the training and testing datasets. According to the findings of Ahsan et al. [60], the LBPH algorithm is the simplest and most effective face recognition method. In this experiment, system development utilized the LBPH algorithm. To optimize the environment for face recognition with the camera, experimentation was conducted by [51] to determine the optimal distance between the camera and the subject for a 640 × 480 resolution. This experiment replicates their findings by limiting the camera-to-subject distance to 1.12 meters and employing the Python face recognition package to calculate the bounding box around each face, facial embedding, and face comparisons in the encoding dataset.

The authors took ten photos of each exam taker's face without eyeglasses from various angles for the training dataset and then used the LBPH method to train and store the biometric pattern of each exam taker in the database. Each participant collected their faces in a single round. Ten images were captured by the IoT camera for each student using the same camera angle and distance.

The training and testing datasets of students' faces were collected under the same environmental conditions of

ambient daylight with two fluorescence in open areas from 8:00 a.m. to 9:00 a.m. A digital multimeter measured the lux level of illumination for a light meter as 197.

The authors captured two images of each finger as part of the biometric fingerprint training and testing dataset. Using cloud computing, one exam candidate enrolled and remained in the database using two fingers. Proctors applied alcohol every time fingerprints were collected. A fingerprint reader's glass must be wiped clean for each student scanned. This study configured the fingerprint reader Adafruit R305 and Arduino libraries using the solution from [71] to match the fingerprint image to the examinee.

C. COMPAIRISON OF DIFFERENT VERIFICATION SCENARIOS

This experiment compared four testing technologies of biometric approaches to evaluate the quality of an IoT-based biometric verification system for the identity verification of exam takers in a higher education institution: Zero-Biometric System (Z), Unimodal Biometric System (U), Multimodal Biometric System (M), and Semi-Multimodal Biometric System (S). Therefore, the experimental results can be divided into eight protocols.

1) ZERO BIOMETRIC (Z)

The zero-biometric system is a conventional method of identity verification that employs human proctors. A proctor verifies the students' identities by examining the photographs on their identification documents, such as student ID cards, personal ID cards, driver's licenses, and passports. Consider a student who appears to lack identification. In such a case, a proctor will request that a student obtains a day temporary identification card from the registrar's office or contacts the instructor of a specific examination subject to confirm a student's status. The instructor can verify the student's identity. As depicted in Fig. 1, a proctor will then permit the student to sign a temporary identification form for entry into the examination room.

2) UNIMODAL BIOMETRIC (U)

A unimodal biometric system includes only a single biometric. This experimental protocol utilizes facial or fingerprint biometrics. This study chose facial and fingerprint biometrics because examination verification systems require speed and convenience, and numerous exam candidates are available in the exam room. The study utilizes biometrics with universally high acceptance, reasonable costs, and experimentation suitability.

Algorithm 1 depicts the verification procedure for exam takers utilizing facial or fingerprint biometrics in conjunction with an IoT-based verification system. The examination results indicate that the examinee's biometric information does not match the biometric data in the database. In such a circumstance, the examinee will be denied entry into the

Algorithm 1 Pseudocode of Unimodal Biometric Verification

Input A student's face or fingerprint

Output The verification result of each student

Start Algorithm

A biometric verification system sets active

A biometric device is activated with configuration

A student walks into an examination room

Foreach data acquire on training dataset

For each biometric data captures, n data

 Biometric area detection

 Biometric preprocessing

 Biometric feature extraction

 Store a biometric feature as a biometric template on the database

 Display storing information

 Display results

End

For each data acquire on testing dataset

 Biometric area detection

 Biometric preprocessing

 Biometric feature extraction

 Match a biometric feature to biometric templates on the database

 Return the verification result

If the accuracy matching result is more than 0.85

 Accepted result of identity verification

Else

 Unaccepted result of identity verification

 Display results

End

End Algorithm

examination room. The rejected candidate must contact the subject instructor or other instructors who can verify the candidate's eligibility to take the examination. A proctor will then permit the student to sign a temporary identification form for entry into the examination room.

3) MULTIMODAL BIOMETRICS (M)

A multimodal biometric system incorporates at least two biometrics. This experiment requires two facial and fingerprint biometrics to detect and verify the identity of students.

Algorithm 2 represents the identity verification workflow of the multimodal biometric method. There are three possible verification outcomes. The system accepts two biometric protocols for the student to enter the exam room. The system accepts either protocol but denies access to the examination room if neither is presented. A proctor requests that the student undergo verification multiple times until the system can confirm his/her face and fingerprints. The system rejects all biometric protocols, denies the student access to the examination room, and flags him or her as a fraud student.

Algorithm 2 Pseudocode of Multimodal Biometric Verification**Input**A student's faces and fingerprints**Output**The verification result of each student**Start Algorithm**

A biometric verification system sets active

First biometric devices are activated with configuration

Second biometric devices are activated with configuration

A student walks into an examination room

For each data acquire on training dataset **For** each of the first biometric data captures, n data

First biometric area is detection

Second biometric area detection

Both biometric data preprocessing

Both biometric features extraction

Store biometric features as biometric templates on the database

Display storing information

Display results

End**For** each data acquire on testing dataset

First biometric area detection

Second biometric area preprocessing

Both biometric data extraction

Both biometric feature extraction

Match first biometric feature to biometric templates on the database

Match second biometric feature to biometric templates on the database

Return both verification results

Accuracy fusion calculation of first and second biometric recognition

If the fusion biometric recognition of accuracy matching result is more than 0.70

Accepted result of identity verification

Elseif the accuracy matching of first result is more than 0.85

Accepted result of identity verification

Elseif the accuracy matching of second result is more than 0.85

Accepted result of identity verification

Else

Unaccepted result of identity verification

Display results

End**End Algorithm**

Face and fingerprint - Upon student entry into the examination room, the multimodal biometric method can simultaneously apply face and fingerprint recognition. A web camera focuses on a test-taker as they enter a fingerprint-scanning device and sends the data to a database. Only examination candidates accepted by both biometric devices may enter the examination room. If a candidate were accepted by only one

biometric device, he or she would be denied access to the examination room.

Face with two cameras - Using multiple sensors and two cameras, this experimental group has verified exam takers. The brand and quality of the first and second cameras are identical, but their positions differ. Consequently, the images captured by the two cameras have distinct perspectives. The proctor admits only examination candidates who are approved by both cameras. If only one camera accepts an exam candidate, that individual will not be allowed into the examination room.

Fingerprint with two scanners - This experimental group has implemented a technique involving multiple sensors and two fingerprint scanners to verify exam takers. The quality and brand of the first and second fingerprint scanners are identical. Examinees must scan their fingerprints simultaneously on two fingerprint scanners. The proctor admits only exam candidates who both scanners have approved. If either scanner permitted the examinee to enter the exam room, the examinee would be denied entry.

4) SEMI-MULTIMODAL BIOMETRICS (S)

A single biometric system incorporates two biometrics. Face biometrics and fingerprints are sequentially required by semi-multimodal biometrics to detect and confirm student identity.

This experimental method sequentially verifies the face and fingerprint biometric identifiers. In our research, face recognition precedes or follows fingerprint recognition or vice versa. For instance, a genuine student may walk past a camera sensor or scan a fingerprint. Consider that the first biometric recognition using the camera sensor, or the fingerprint scanner captures the student's biometrics, and then the biometric database management system identifies biometric extraction. In this instance, the student's identification is accepted for entry into the examination room if the biometric templates captured match the biometric templates contained in the biometric database. If the initial biometric recognition during biometric scanning fails, a proctor asks the student to rescan the biometric until a result is obtained.

Alternatively, if the student's first biometric is rejected, he or she must scan a second biometric device to confirm his or her identity. If the student is scanned by a second biometric, the scanned biometric template is located on the biometric database management system. Then, the student is permitted to enter the examination room after his or her identity has been confirmed.

The biometric database management system cannot confirm the student's identity if the second biometric scan fails. A proctor will then be alerted by the system notification. Suppose that the student continues to be rejected by both types of biometrics. In such a scenario, a proctor requests that the student contact an instructor of the exam subject, who can verify the student's identity to verify student identity. If an instructor of the exam subject can verify the student, a proctor will provide a temporary identification

Algorithm 3 Pseudocode of Semi-Multimodal Biometric Verification**Input** A student's faces then fingerprints, or vice versa**Output** The verification result of each student**Start Algorithm**

A biometric verification system sets active

First biometric devices are activated with configuration

Second biometric devices are activated with configuration

A student walks into an examination room

For each data acquire on training dataset **For** each of the first biometric data captures, n data

First biometric area is detection

Second biometric area detection

Both biometric data preprocessing

Both biometric features extraction

Store biometric features as biometric templates on the database

Display storing information

Display results

End**For** each data acquire on testing dataset

First biometric area detection

First biometric data extraction

First biometric feature extraction

Match first biometric feature to biometric templates on the database

Return verification results

If the accuracy matching result is more than 0.85

Accepted result of identity verification

Else

Second biometric area preprocessing

Second biometric data extraction

Second biometric feature extraction

Match second biometric feature to biometric templates on the database

Return verification results

If the accuracy matching of second result is more than 0.85

Accepted result of identity verification

Else

Unaccepted result of identity verification

Display results

End**End Algorithm**

form with the student's signature. This method's workflow is represented by Algorithm 3.

D. BIOMETRIC QUALITY METRIC OF EFFECTIVENESS EVALUATION CRITERIA

Numerous researchers evaluate the biometric system and determine its quality based on various factors [24], [71], [72]. The essential aspects of a biometric system's quality investigation involve measuring its performance, accuracy, precision, recall, and execution time. Cost is also taken into

account when assessing biometric quality. Using a set of evaluation criteria, the authors compare biometric approaches. The biometric quality metric evaluates quantitative factors, including accuracy, error rate, processing time, and cost, as indicated by (1), the biometric quality metric.

Biometric quality metric

$$= \{Accuracy, ErrorRate, ProcessingTime, Cost\} \quad (1)$$

The average classification accuracy (ACE) formula has been utilized by Accuracy to evaluate and compare verification performance. ACE can be calculated using (2).

$$ACE = 100 \frac{(FMR + FNMR)}{2} \quad (2)$$

The error rate is a numerical score that indicates the proportion of potential genuine cases. False exam-takers have been permitted to enter a room titled false accept rate (FAR). Genuine exam candidates were denied entry to the examination room named false reject rate (FRR). The error rate indicator score should ideally be nearly zero, meaning that FAR and FRR are equal to zero. FAR can be expressed as (3).

$$FAR = FMR * (1 - FTA) \quad (3)$$

In addition, False match rate (FMR) is the percentage at which biometric processing incorrectly identifies biometric signals from two distinct individuals originating from the same individual. FMR is designated as (4).

$$FMR = \frac{\text{Number of false acceptance}}{\text{Number of impostor attempts}} * 100 \quad (4)$$

False reject rate (FRR) is the inverse of the false acceptance rate (FAR), which is the error rate score when the system denies the real examinee access to the examination room. FRR can be computed using (5). In addition, False to acquire (FTA) is the percentage of attempts in which the system fails to acquire a sample of adequate quality. FNMR can be computed using (6).

Time (T) is the duration of an exam-taker verification's execution. When the system cannot acquire an examinee detection result, the exam taker must re-verify his or her face or fingerprint until the system can acquire the biometric information. As (7) summarizes that each examinee is subject to multiple checks.

$$FRR = FTA + (FNMR) * (1 - FTA) \quad (5)$$

$$FNMR = \frac{\text{Number of false rejection}}{\text{Number of genuine exam taker attempts}} * 100 \quad (6)$$

$$T = \sum_{i=1}^n T_n \quad (7)$$

where n is a number of verifications for a student

Cost (C) is the cost of equipment for the IoT-based biometric system used to verify exam candidates. While the multimodal biometric system is more efficient than the

unimodal biometric system, the Internet of Things-based multimodal biometric system has a higher budget.

V. RESULTS AND DISCUSSION

The experimental verification results of eight testing protocols were as follows: first protocol (student identification card detection), second protocol (face detection only), third protocol (fingerprint detection only), fourth protocol (face and fingerprint detection), fifth protocol (face with two- cameras detection), sixth protocol (fingerprints with two- scanners detection), seventh protocol (face then fingerprint detection), and eighth protocol (fingerprint then face detection). For each testing protocol, the outcome is subdivided into five criteria of verification result: the average accuracy rate, the average error rate, the effective response times, the cost of biometric devices, and the estimated cost of 500 hours of usage. The verification results of eight testing protocols are summarized in Table 3 in terms of average precision, average error rate, average processing time, and the average cost of biometric devices.

According to Table 3, the sixth testing protocol (two fingerprints) has the highest average rate of identity recognition accuracy at 96.67 percent. In contrast, the initial testing protocol received the lowest score of 66.67 percent. The sixth testing protocol has the lowest average error rate for identity recognition at 1.82 percent, while the first testing protocol has the highest average error rate at 21.29 percent. The second testing protocol has the best average response time for identity verification at 2.49 seconds, while the first testing protocol has the worst average response time at 14.01 seconds. The cost of the biometric device is the subject of this study. Due to the absence of biometric devices in the first testing protocol, the device cost is unavailable. Therefore, the sixth testing protocol has the highest cost of biometric devices, at \$110, while the second testing protocol has the lowest cost, at \$40.

Valaya Alongkorn Rajabhat University proctor was estimated to cost US\$11.43 per hour. The estimated cost of IoT usage is based on the mean time before the failure of Raspberry Pi (MTBF). It has been estimated that Raspberry Pi could operate reliably for five to seven years [73]. The authors assume that the minimally functional hardware will continue to operate reliably for 1.5 years (approximately 500 hours). The IoT-based biometric verification system costs \$720 (according to Table 2), and biometric sensors are excluded. Using these formulas, the price of the IoT-based biometric verification system with biometric sensors was determined (8).

$$\text{Total system cost} = \text{System cost} + \sum_{i=1}^n \text{Sensor}_i \quad (8)$$

where n is the number of biometric sensors

For instance, a facial biometric verification system based on IoT was estimated to cost a total of US\$760 (US\$720 + US\$40). Therefore, the cost per hour was calculated to be \$1.52 (US\$760 / 500 hours).

Therefore, the first testing protocol has the highest estimated cost per examination class (three hours), at US\$34.29. In contrast, the second testing protocol costs the least at \$4.56.

To rank-compare the scores of each testing protocol in Table 3, the authors reformat the result using the triangular law. Consider the maximum value of the average processing time to be 14.01 seconds. In this instance, the value is converted to 100 percent, and the new score is computed using the triangular law, as shown in Table 4. The total score for each of the eight testing protocols was determined by using the category rankings. The values for each category range from five to zero. The same proportion of ranks and scores in each category are identical. The highest possible score in each category is 5 for the category winner. In contrast, the lowest position receives no points. Each group was responsible for determining the sum of their scores. The highest total scores are converted to 100 percent using the triangular law, and a new score is calculated. Table 4 displays the revised score.

Table 4 and Fig. 9 detail the biometric quality metric scores for each testing protocol, excluding the traditional proctoring system, also known as a zero biometric system, which received no score. Fig. 9 demonstrates that the best scoring system was the unimodal face biometric system. The multimodal face and fingerprint biometric system, the multimodal fingerprint biometric system with two scanners, and the semi-multimodal face then fingerprint biometric system received the second-highest scores. The two-camera, multimodal face biometric system received the third-highest score.

To prove the research hypotheses H1 and H2, it was determined that the unimodal and multimodal biometric approaches' accuracy, error rate, and processing time are superior to the conventional verification method.

H1: The quality of the unimodal biometric system is superior to the quality of the conventional system for exam-taker verification.

Fig. 10 (A) displays the outcomes of the zero and unimodal biometric approaches utilized in the experiment. The results of the biometric quality metric were calculated and reported to compare the biometric techniques. The biometric quality metric employs identity verification factors to assess the quality scores of biometric devices (1). The traditional method yielded the highest scores for error rate, processing time, and cost but the worst performance in terms of accuracy rate for exam-taker identity verification.

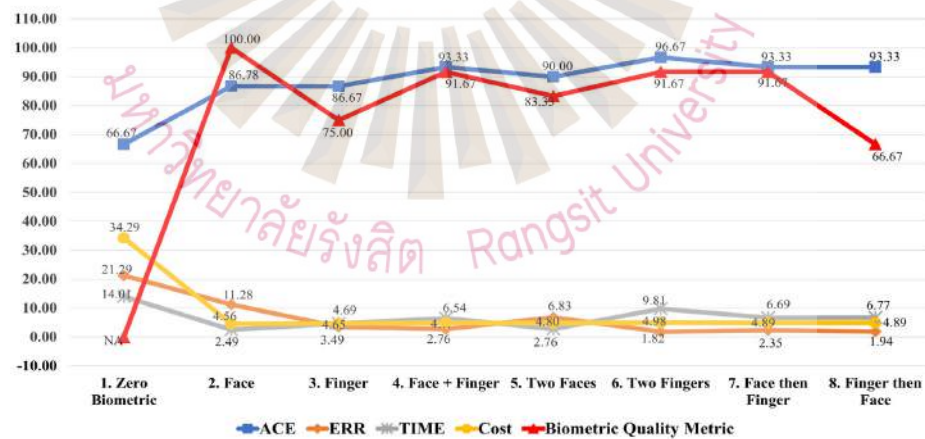
However, the conventional approach's biometric quality metric is not calculated. On the other hand, the results indicate that the unimodal face or fingerprint has greater accuracy, processing speed, and effectiveness while maintaining a lower error rate and cost. The biometric quality metric of the unimodal face biometric system is the highest-ranked metric. The unimodal fingerprint biometric verification system ranks second. Therefore, the overall quality of unimodal biometric verification systems is superior to that of a biometric verification system with no biometric features.

TABLE 3. Results of biometric quality metric for traditional and biometric verification approaches.

Criteria	1. Zero Biometric	2. Face	3. Finger	4. Face + Finger	5. Two Faces	6. Two Fingers	7. Face then Finger	8. Finger then Face
Accuracy	66.67%	86.78%	86.67%	93.33%	90.00%	96.67%	93.33%	93.33%
Error Rate	21.29%	11.28%	3.49%	2.76%	4.83%	1.82%	2.35%	1.94%
Time (sec.)	14.01	2.49	4.69	6.54	2.76	9.81	6.69	6.77
Sensor cost	-	\$40	\$55	\$95	\$80	\$110	\$95	\$95
Estimate cost (3 hrs.)	\$34.29	\$4.56	\$4.65	\$4.89	\$4.80	\$4.98	\$4.89	\$4.89

TABLE 4. Transformation scores for each testing group.

Criteria	1. Zero Biometric	2. Face	3. Finger	4. Face + Finger	5. Two Faces	6. Two Fingers	7. Face then Finger	8. Finger then Face
Accuracy (%)	68.97	89.76 (2)	89.65 (1)	96.54 (4)	93.10 (3)	100.00 (5)	96.55 (4)	96.55 (4)
Error Rate (%)	100.00	52.97	16.39 (1)	12.97 (3)	32.09	8.55 (5)	11.04 (4)	9.11 (2)
Time (%)	100.00	17.75 (5)	33.46 (3)	46.67 (2)	19.70 (4)	70.04	47.76 (1)	48.31
System cost (%)	-	91.57 (5)	93.37 (4)	98.19 (2)	96.39 (3)	100 (1)	98.19 (2)	98.19 (2)
Total Score	-	12.00	9.00	11.00	10.00	11.00	11.00	8.00
Biometric Quality Metric	-	100.00	75.00	91.67	83.33	91.67	91.67	66.67

**FIGURE 9.** Comparison testing scores of biometric quality metric for different verification approaches.

H2: The multimodal biometric approach is superior to the conventional approach in terms of quality. Fig. 10 (B) and (C) depict the experimental outcomes of the conventional verification approach and multimodal biometric approaches. The results of the biometric quality metric calculation revealed that the traditional approach yields the

highest scores for error rate, processing time, and cost but the worst performance in terms of accuracy rate for exam taker identity verification. However, the conventional approach's biometric quality metric is not calculated. The results of multimodal verification systems indicate, however, that face and fingerprint biometrics, face biometrics with two cameras,

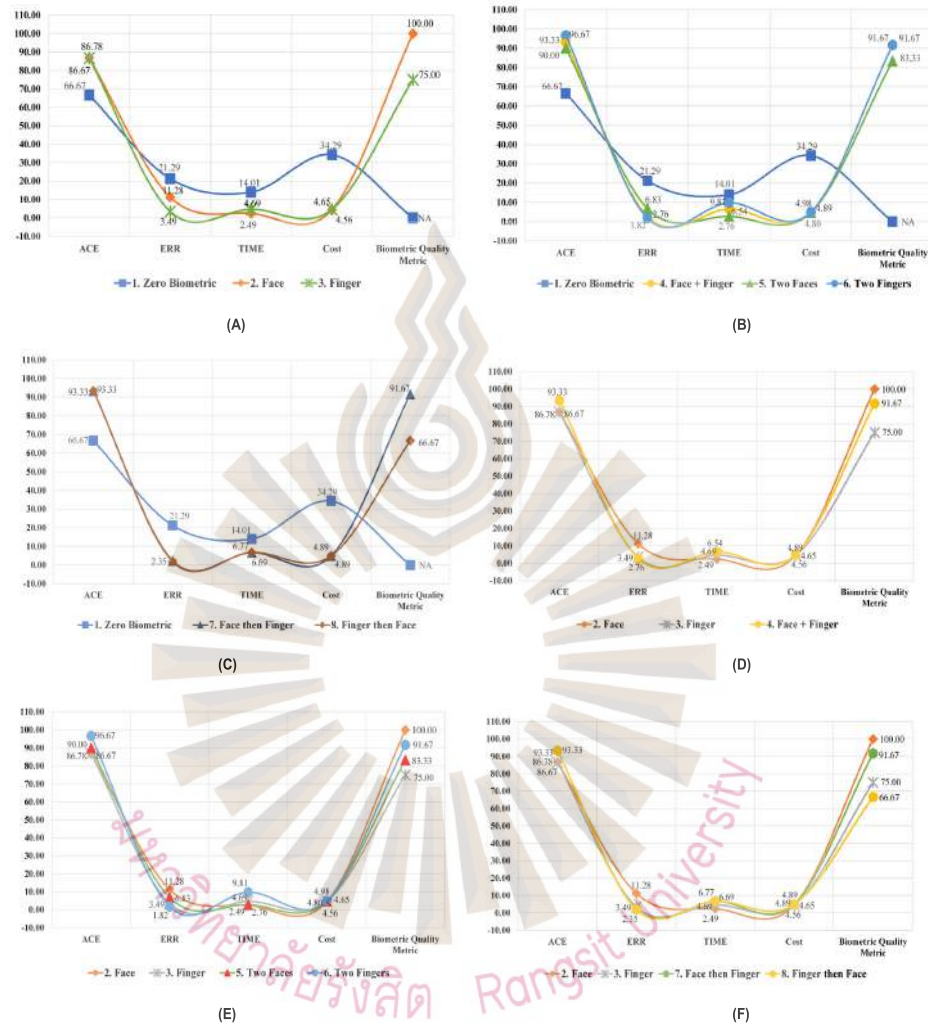


FIGURE 10. Each biometric verification approaches ranking by biometric quality metric.

and fingerprint biometrics with two scanners are more effective and efficient in terms of accuracy, processing time, and cost while maintaining a lower error rate and expense. In addition, the results of semi-multimodal verification systems indicate that face verification followed by fingerprint verification and fingerprint verification followed by face verification is more effective and efficient in terms of accuracy, processing time, and cost while maintaining a lower error rate. Face and fingerprints are utilized in the biometric quality metric of multimodal verification systems. The two fingerprints and the semi-multimodal face are ranked highest, followed by the fingerprint biometric verification system. Consequently, the overall quality of

multimodal and semi-multimodal biometric verification systems surpasses that of the zero biometric verification system.

H3: The multimodal biometric approach is superior to the unimodal biometric system for exam-taker verification in terms of quality. Fig. 10 (D), (E), and (F) illustrate that the biometric quality scores of unimodal face biometrics are the most effective and efficient overall. Multimodal biometric recognition systems employing face and fingerprint biometrics, face biometrics with two cameras or two fingerprints, have improved accuracy and a lower error rate at the expense of a significantly slower processing speed and a rising price. Multimodal biometric verification systems produce identical

TABLE 5. Comparative analysis of approaches.

Criteria	Contributions	Limitations
Zero Biometric	- Simple to use, as it only requires a physical card to be presented and verified. - Cost depends on the number of proctors and exam takers, as no additional hardware or software is required.	- Vulnerable to fraud and errors, as cards can be lost, stolen, or duplicated, and there is no updated information on an exam taker. - Limited to one form of identification and a proctor-to-examinee ratio.
Face	- Non-intrusive and user-friendly, requiring only a camera to capture the image. - Can be used for real-time identification and verification with the quickest response time and lowest cost for unimodal recognition. - Simply perform implementation and maintenance.	- Is sensitive to focusing ranges, lighting conditions, facial expressions, and aging. - Requires capturing a clear image of the face, which is not always possible. - Face recognition with eyeglasses and face variations requires complex algorithms.
Finger	- Non-intrusive and user-friendly, requiring only a fingerprint sensor to capture the image. - Capable of real-time identification and verification with the highest accuracy and lowest error rate for unimodal recognition. - Require fairly implementation and maintenance.	- Finger and scanner can be affected by factors such as dryness, moisture, and dirt. - Requires capturing a clear fingerprint image, which is not always possible. - Fingerprint scanners for capturing and verifying must be identical.
Face + Finger	- Provides a higher level of security due to the use of multiple forms of identification. - Improve the accuracy of the identification and verification process at the lowest cost for multimodal recognition. - Adapt to unimodal recognition.	- More complex and costly than using a single form of identification. - Subject to the same limitations as the individual face and fingerprint recognition methods. - Require an additional complicated implementation, recognition techniques, and maintenance.
Two Faces	- Provides a higher level of security due to the use of multiple forms of identification. - Multimodal recognition can achieve the highest level of identification and verification accuracy at the same cost as face and fingerprint recognition. - Support fault-tolerant cameras.	- More complex and costly than using a single form of identification. - Subject to the same limitations as the individual face recognition methods. - Additional expenses for an additional camera, implementation, recognition techniques, and maintenance are necessary.
Two Fingers	- Provides a higher level of security, as it employs multiple forms of identification. - Increase the accuracy of the identification and verification process, as multimodal recognition has the lowest error rate. - Support fault-tolerant scanners.	- More complicated and costly than using a single form of identification. - Subject to the same limitations as individual methods of finger recognition. - Require an additional scanner cost, implementation, recognition techniques, and maintenance.
Face then Finger	- Provides a higher level of security due to the use of multiple forms of identification. - Improve the accuracy of the identification and verification process with the quickest response time for semi-multimodal recognition. - Offer a quicker response time than multimodal recognition.	- More complex and costly than using a single form of identification. - Subject to the same limitations as face and fingerprint recognition alone. - Require complex implementation, recognition techniques, and maintenance.
Finger then Face	- Provides a higher level of security due to the use of multiple forms of identification. - Improve the accuracy of the identification and verification process with the lowest error rate for semi-multimodal recognition. - Multimodal recognition is somewhat more expensive.	- More complicated and costly than using a single form of identification. - Subject to the same limitations as fingerprint and face recognition methods. - Require complex implementation, recognition techniques, and maintenance.

results to semi-multimodal biometric verification systems. Thus, out of eight testing protocols, unimodal face recognition is an excellent factor for verifying the identity of exam candidates. These experimental results demonstrate that unimodal biometric technologies are superior to multimodal ones. However, the performance of the multimodal biometric approach in the IoT-based biometric system used to verify exam candidates is superior to that of the unimodal biometric approach. Regarding cost and processing time, it was determined that the performance of the unimodal biometric system was superior to that of the multimodal biometric method. In contrast, the multimodal biometric system has superior reliability.

Therefore, hypotheses H1 and H2 are accepted. The biometric quality scores of unimodal and multimodal face recognition systems indicate that unimodal face recognition is marginally superior to multimodal face recognition and finger recognition systems. Numerous researchers [47], [74] have confirmed the experimental findings that biometric verification techniques are more accurate, efficient, and stable than conventional methods.

Contrary to the results of this study, hypothesis H3 is rejected. A multimodal biometric system is more expensive than a unimodal system. Several studies have demonstrated that multimodal protocols are superior to unimodal protocols in terms of complex human verification and

security [75], [76], regarding those studies showing that multimodal protocols are superior to unimodal protocols. The multimodal biometric system is superior to the unimodal biometric system in terms of reliability criteria. Employing the IoT-based biometric system to verify exam candidates in educational institutions presents constructive challenges depending on the institution's existing systems. Some higher education institutions have extensive information and communication technology. Others, however, were unable to afford IoT-based biometric systems to verify exam candidates.

This research aims to not only compare the effectiveness of various unimodal and multimodal biometric technologies for identity verification systems of exam candidates but also to provide a methodology for developing an IoT-based biometric system used by higher education institutions to verify exam candidates. The biometric quality metric may employ a variety of criteria to implement the exam taker verification system in accordance with institution-specific requirements. Table 5 illustrates the comparative analysis of proposed identity verification methods based on this practical evaluation of IoT-based biometric recognition systems. Face + Finger, Two Faces, Two Fingers, and Face then Finger or Finger then Face approaches have the potential to increase the security of the identification and verification process, as indicated by the comparative results. However, they are more complex and costly than a single form of identification. In contrast, the single form of recognition is user-friendly, inexpensive, and susceptible to a few errors.

Nevertheless, the biometric quality metrics have demonstrated that unimodal, multimodal, and semi-multimodal biometric verifications depend on numerous factors, including accuracy, error rate, reliability, processing time, and cost.

Because the proposed factors are calculable, the unimodal approach to face recognition has the highest overall score compared with the alternatives. This study strongly suggests that contemporary universities should at least offer the unimodal biometric approach as an alternative to traditional methods of verifying the identity of exam-taking students.

VI. CONCLUSION

The IoT hardware, system development, and evaluation of the actual use of examination management and identity verification for exam candidates in education were among the most significant findings of this empirical study. Utilizing face and fingerprint biometric devices, an IoT-based biometric verification system has been developed to facilitate the collection, storage, detection, and verification of student information, including examination details, identification, identity, and biometric data. The proposed system design and development can recognize test-takers identities without identification documents using multiple biometric recognition techniques. In addition, this study describes different algorithms for IoT-based biometric verification of exam takers. A novel biometric quality metric is proposed for scoring biometric exam taker verification systems based on ISO/IEC 25000

and software quality models. By investigating and evaluating the biometric quality metric in the IoT-based biometric verification system, the findings of this study could have a direct impact on whether biometric technologies are used in education. Using the proposed architecture and system, this study compared the biometric technologies of unimodal, semi-multimodal, and multimodal approaches for recognizing exam-takers identities. Using the biometric quality metric to compare a combination of traditional proctoring and several biometric verification protocols, the effectiveness and efficiency criteria are defined as accuracy rate, error rate, processing time, and cost.

The results revealed that the two-fingers multimodal biometric system had the highest average accuracy of 96.67 percent and the lowest error rate of 1.9 percent. The traditional proctoring system, known as a zero biometric system, had the lowest average accuracy of 66.67 percent, resulting in the highest average error rate of 21.29 percent. With an average processing time of 2.49 seconds, the face unimodal biometric system was the most responsive, while the traditional proctoring system was the least responsive. The face unimodal biometric system had the lowest estimated cost for a 3-hour examination class at \$4.56, while the conventional proctoring system had the highest estimated cost at \$34.29.

To summarize the optimal IoT-based biometric systems, the triangular law was used to reformat the results of all system testing comparisons. The findings indicated that the unimodal face biometric is the most effective scoring system. The multimodal face and fingerprint biometric system, the multimodal fingerprint biometric system with two scanners, and the semi-multimodal face then fingerprint biometric system received the second-highest scores. The two-camera, multimodal face biometric system received the third-highest score.

A biometric system based on the Internet of Things promises to verify exam candidates accurately and could replace the traditional proctoring method for student identity verification. In addressing the research hypothesis, the evaluation results of the quality metrics demonstrate that unimodal, multimodal, and semi-multimodal biometric verification systems outperform the conventional proctoring system in terms of reliability, validity, processing time, and investment. In education, the unimodal face biometric system exhibited the highest overall system quality for examiner identity verification.

This study has several implications and applications. The findings enable educational institutions to more effectively use biometric technologies for the identity verification of exam takers by selecting a biometric technology suited to their objectives. Comparing the outcomes of various biometric technologies aided organizations in determining their preferred trade-offs between the number of resources and the consideration factors of desired accuracy, error rate, processing time, and cost to meet requirements. This research not only conserves time, resources, risk, and investment

but also demonstrates a greater understanding of biometric recognition for identity verification to reduce application failures. In addition, the results of this study can serve as recommendations for implementing biometric technologies in educational settings.

The study of an IoT-based biometric verification system demonstrates the proposed design and development, compares various biometric techniques, and determines the efficacy and efficiency of each biometric technique. This study has some limitations that can be addressed in future studies, including system development (hardware and software), user behavioral intentions (sociodemographic factors), and biometric quality metrics for varying biometric recognition. This study is based on Raspberry Pi 4, biometric devices, OpenCV, and wireless networks, whereas other researchers may use different hardware, software libraries, implementation strategies, and networks. Thus, future development systems should investigate the effects of changes. In addition, it is necessary to validate and analyze the impact of technology acceptance factors on user perceptions of actual system use. In addition, the biometric quality metric can be adapted to support additional biometric recognition.

REFERENCES

- [1] M. Rukhiran, N. Phaothla, and P. Netinant, "Adoption of environmental information chatbot services based on the Internet of Educational things in smart schools: Structural equation modeling approach," *Sustainability*, vol. 14, no. 23, p. 15621, Nov. 2022, doi: 10.3390/su142315621.
- [2] D. Shah and V. Haradi, "IoT based biometrics implementation on Raspberry Pi," *Procedia Comput. Sci.*, vol. 79, pp. 328–336, 2016, doi: 10.1016/j.procs.2016.03.043.
- [3] M. Rukhiran and P. Netinant, "IoT architecture based on information flow diagram for vermiculture smart farming kit," *TEM J.*, vol. 9, no. 4, pp. 1330–1337, Nov. 2020, doi: 10.18421/TEM94-03.
- [4] A. George, A. Ravindran, M. Mendieta, and H. Tabkhi, "MEZ: An adaptive messaging system for latency-sensitive multi-camera machine vision at the IoT edge," *IEEE Access*, vol. 9, pp. 21457–21473, 2021, doi: 10.1109/ACCESS.2021.3055775.
- [5] S. Taheri and J.-S. Yuan, "A cross-layer biometric recognition system for mobile IoT devices," *Electronics*, vol. 7, no. 2, p. 26, Feb. 2018, doi: 10.3390/electronics7020026.
- [6] P. Bellmann, P. Thiam, and F. Schwenker, "Person identification based on physiological signals: Conditions and risks," in *Proc. ICPRAM*, Valletta, Malta, 2020, pp. 373–380, doi: 10.5220/000865503730380.
- [7] A. Phokjang and P. Netinant, "Developing software architecture for a smart school digital framework," in *Proc. ICSIM*, Yokohama, Japan, 2021, pp. 22–27, doi: 10.1145/3451471.3451475.
- [8] R. A. Hamid, U. A. Mokhtar, M. M. Yusof, and A. Warland, "Electronic records management in schools: The case study of school examination analysis system," *J. Pengurusan*, vol. 57, pp. 142–154, May 2019, doi: 10.17576/pengurusan-2019-57-10.
- [9] O. A. Abass, S. A. Olajide, and B. O. Samuel, "Development of web-based examination system using open source programming model," *Turk. Online J. Distance Educ.*, vol. 18, no. 2, pp. 30–42, 2017, doi: 10.17178/TOJDE.306555.
- [10] C. Bohmer, N. Feldmann, and M. Ibsen, "E-exams in engineering education—Online testing of engineering competencies: Experiences and lessons learned," in *Proc. IEEE Global Eng. Educ. Conf. (EDUCON)*, Santa Cruz de Tenerife, Spain, Apr. 2018, pp. 571–576, doi: 10.1109/educon.2018.8363281.
- [11] M. R. Hameed and F. A. Abdullatif, "Online examination system," *IJARSET*, vol. 4, no. 3, pp. 106–110, Mar. 2017, doi: 10.17148/iar-jset.2017.4321.
- [12] M. Rukhiran, S. Buaroong, and P. Netinant, "Software development for educational information services using multilayering semantics adaptation," *Int. J. Service Sci., Manage., Eng., Technol.*, vol. 13, no. 1, pp. 1–27, Sep. 2022, doi: 10.4018/IJSSMET.307153.
- [13] V. S. Shamsi, "A survey paper on fingerprint recognition and cross matching," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 7, no. 5, pp. 573–575, May 2019, doi: 10.22214/ijraset.2019.5096.
- [14] Y. Kortli, M. Jridi, A. A. Falou, and M. Atri, "Face recognition systems: A survey," *Sensors*, vol. 20, no. 2, p. 342, Jan. 2020, doi: 10.3390/s20020342.
- [15] T. Kalisky, S. Saggese, Y. Zhao, D. Johnson, M. Azarova, L. E. Duarte-Vera, L. A. Almada-Salazar, D. Perales-Gonzalez, E. Chacon-Cruz, J. Wang, R. Graham, A. Hubenko, D. A. Hal, and E. Aronoff-Spencer, "Biometric recognition of newborns and young children for vaccinations and health care: A non-randomized prospective clinical trial," *Sci. Rep.*, vol. 12, Dec. 2022, Art. no. 22520, doi: 10.1038/s41598-022-25986-6.
- [16] L. Y. Yugai, "The use of biometric identification in countering crime," *Berlin Stud. Transnational J. Sci. Humanities*, vol. 2, nos. 1–4, pp. 3–14, 2022, doi: 10.5281/zenodo.5831922.
- [17] J. Żywiolek, A. Sarkar, and M. S. Sial, "Biometrics as a method of employee control," in *Proc. IMCOM*, Seoul, South Korea, 2022, pp. 1–5, doi: 10.1109/IMCOM53663.2022.9721809.
- [18] M. A. Hossain and M. A. Al Hasan, "Improving cloud data security through hybrid verification technique based on biometrics and encryption system," *Int. J. Comput. Appl.*, vol. 44, no. 5, pp. 455–464, May 2022, doi: 10.1080/1206212X.2020.1809177.
- [19] M. Zhang and Q. Luo, "A systematic literature review on the influence mechanism of digital finance on high quality economic development," *J. Risk Anal. Crisis Response*, vol. 12, no. 1, pp. 45–54, Apr. 2022, doi: 10.54560/jracr.v12i1.321.
- [20] O. Tomohide, I. Kazuo, I. Atsushi, T. Satoshi, H. Noriyuki, and T. Risa, "Fast travel: Using face recognition to improve airport services with a view towards wide scale implementation," *Intell. Logistics Mobility*, vol. 15, no. 1, pp. 52–56, Jan. 2021.
- [21] A. Karagianni and V. Papakonstantinou, "Surveillance in schools across Europe: A new phenomenon in light of the COVID-19 pandemic? The cases of Greece and France," *Eur. J. Educ. Res.*, vol. 11, no. 2, pp. 1219–1229, Apr. 2022, doi: 10.12973/eu-jer.11.2.1219.
- [22] K. N. Goud and K. Sindhuri, "Enhanced security for smart door using biometrics and OTP," in *Studies in Computational Intelligence*, Cham, Switzerland: Springer, 2022, pp. 517–526, doi: 10.1007/978-3-030-96634-8_47.
- [23] I. Anikin and E. Anisimova, "Framework for biometric user authentication based on a dynamic handwritten signature," in *Cyber-Physical Systems: Intelligent Models and Algorithms*, vol. 417, Cham, Switzerland: Springer, 2022, pp. 219–231, doi: 10.1007/978-3-030-95116-0_18.
- [24] N. M. Raharja, M. A. Pathansyah, and A. N. N. Chamim, "Vehicle parking security system with face recognition detection based on eigenface algorithm," *J. Robot. Control*, vol. 3, no. 1, pp. 78–85, Oct. 2021, doi: 10.18196/jrc.v3i1.12681.
- [25] O. Shlyakhetko, A. Braibant, E. Czechowska, M. Fryczka, and R. Hadrich, "IoT project: Smart parking," in *Developments in Information & Knowledge Management for Business Applications*, vol. 42, Cham, Switzerland: Springer, 2022, pp. 37–58, doi: 10.1007/978-3-030-95813-8_2.
- [26] V. Singh and C. Kant, "Biometric-based authentication in Internet of Things (IoT): A review," *Adv. Inf. Commun. Technol. Comput.*, vol. 392, pp. 309–317, May 2022, doi: 10.1007/978-981-19-0619-0_27.
- [27] L. Calderoni and A. Magnani, "The impact of face image compression in future generation electronic identity documents," *Forensic Sci. International, Digit. Invest.*, vol. 40, Mar. 2022, Art. no. 301345, doi: 10.1016/j.fsidi.2022.301345.
- [28] R. Srivastava, D. Singh, R. Tomar, and Sarishma, "Three-layer multimodal biometric fusion using SIFT and SURF descriptors for improved accuracy of authentication of human identity," in *EAI/Springer Innovations in Communication and Computing*, Cham, Switzerland: Springer, 2022, pp. 119–142, doi: 10.1007/978-3-030-78284-9_6.
- [29] M. A. Khan, I. Ud Din, S. U. Jadoon, M. K. Khan, M. Guizani, and K. A. Awan, "G-RAT: A novel graphical randomized authentication technique for consumer smart devices," *IEEE Trans. Consum. Electron.*, vol. 65, no. 2, pp. 215–223, May 2019, doi: 10.1109/TCE.2019.2895715.
- [30] A. A. Ahmed, "Future effects and impacts of biometrics integrations on everyday living," *Al-Mustansiriyah J. Sci.*, vol. 29, no. 3, pp. 139–144, Mar. 2019, doi: 10.23851/mjs.v29i3.642.

- [31] A. Mahfouz, T. M. Mahmoud, and A. S. Eldin, "A survey on behavioral biometric authentication on smartphones," *J. Inf. Secur. Appl.*, vol. 37, pp. 28–37, Dec. 2017, doi: [10.1016/j.jisa.2017.10.002](#).
- [32] U. Gawande and Y. Golhar, "Biometric security system: A rigorous review of unimodal and multimodal biometrics techniques," *Int. J. Biometrics*, vol. 10, no. 2, pp. 142–175, 2018, doi: [10.1504/ijbm.2018.091629](#).
- [33] K. Nguyen, C. Fookes, S. Sridharan, M. Tistarelli, and M. Nixon, "Super-resolution for biometrics: A comprehensive survey," *Pattern Recognit.*, vol. 78, pp. 23–42, Jun. 2018, doi: [10.1016/j.patcog.2018.01.002](#).
- [34] S. Dass, M. Sadruhluda, N. Pasha, N. Nayan, and J. S. Nayak, "Real time face recognition using raspberry Pi," *Int. J. Comput. Appl.*, vol. 176, no. 33, pp. 1–4, Jun. 2020, doi: [10.5120/ijca2020920387](#).
- [35] Y. Zhao, J. Xu, J. Wu, J. Hao, and H. Qian, "Enhancing camera-based multimodal indoor localization with device-free movement measurement using WiFi," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 1024–1038, Feb. 2020, doi: [10.1109/jiot.2019.2948605](#).
- [36] S. Yadav and V. P. Vishwakarma, "Extended interval type-II and kernel based sparse representation method for face recognition," *Exp. Syst. Appl.*, vol. 116, pp. 265–274, Feb. 2019, doi: [10.1016/j.eswa.2018.09.032](#).
- [37] M. Kas, Y. El Merabet, Y. Ruichek, and R. Messoussi, "Mixed neighborhood topology cross decoded patterns for image-based face recognition," *Exp. Syst. Appl.*, vol. 114, pp. 119–142, Dec. 2018, doi: [10.1016/j.eswa.2018.07.035](#).
- [38] Y. Yaddaden, M. Adda, A. Bouzouane, S. Gaboury, and B. Bouchard, "User action and facial expression recognition for error detection system in an ambient assisted environment," *Exp. Syst. Appl.*, vol. 112, pp. 173–189, Dec. 2018, doi: [10.1016/j.eswa.2018.06.033](#).
- [39] S. Awojide, O. S. Awe, and T. S. Babatope, "Biometric fingerprint system using an online based pattern recognition for candidates authentication in Nigeria institution examinations. The design perspective," *Int. J. Sci. Eng. Res.*, vol. 9, no. 5, pp. 1680–1694, May 2018, doi: [10.14299/ijser.2018.05.02](#).
- [40] M. Taibab and S. Arabia, "Design and implementation of RFID and fingerprint-based student verification system," *Int. J. Recent Technol. Eng.*, vol. 8, no. 5, pp. 2084–2092, Jan. 2020, doi: [10.35940/ijrte.e5788.018520](#).
- [41] F. D. Tatar, "Fingerprint recognition algorithm," in *Proc. Comput. Sci. Inf. Syst.*, 2017, pp. 85–100, doi: [10.5121/csit.2017.70609](#).
- [42] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "A fingerprint and finger-vein based cancelable multi-biometric system," *Pattern Recognit.*, vol. 78, pp. 242–251, Jun. 2018, doi: [10.1016/j.patcog.2018.01.026](#).
- [43] X. Xi, L. Yang, and Y. Yin, "Learning discriminative binary codes for finger vein recognition," *Pattern Recognit.*, vol. 66, pp. 26–33, Jun. 2017, doi: [10.1016/j.patcog.2016.11.002](#).
- [44] E. Noma-Osaghae, R. Okonigene, C. Okereke, O. J. Okesola, and K. O. Okokpuije, "Design and implementation of an Iris biometric door access control system," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Las Vegas, NV, USA, 2017, pp. 590–593, doi: [10.1109/csci.2017.102](#).
- [45] E. Emmanuel and O. T. Ogadimma, "A biometric authentication approach to examination conduct in Nigerian universities," *Int. J. Innov. Res. Sci., Eng. Technol.*, vol. 8, no. 3, pp. 2176–2182, Mar. 2019.
- [46] G. M. Mir, A. A. Balkhi, N. A. Lala, N. A. Sofi, M. M. Kirmani, I. A. Mir, and H. A. Hamid, "The benefits of implementation of biometric attendance system," *Oriental J. Comput. Sci. Technol.*, vol. 11, no. 1, pp. 50–54, Mar. 2018, doi: [10.13005/ojcs11.01.09](#).
- [47] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on homomorphic encryption," *Pattern Recognit.*, vol. 67, pp. 149–163, Jul. 2017, doi: [10.1016/j.patcog.2017.01.024](#).
- [48] G. S. Walia, T. Singh, K. Singh, and N. Verma, "Robust multimodal biometric system based on optimal score level fusion model," *Exp. Syst. Appl.*, vol. 116, pp. 364–376, Feb. 2019, doi: [10.1016/j.eswa.2018.08.036](#).
- [49] B. Ammour, L. Boubchir, T. Bouden, and M. Ramdani, "Face-iris multimodal biometric identification system," *Electronics*, vol. 9, no. 1, p. 85, Jan. 2020, doi: [10.3390/electronics9010085](#).
- [50] K. Gunasekaran, J. Raja, and R. Pitchai, "Deep multimodal biometric recognition using contourlet derivative weighted rank fusion with human face, fingerprint and iris images," *Automatika*, vol. 60, no. 3, pp. 253–265, Jul. 2019, doi: [10.1080/00051144.2019.1565681](#).
- [51] M. Rukhiran, P. Netinant, and T. Elrad, "Effecting of environmental conditions to accuracy rates of face recognition based on IoT solution," *J. Current Sci. Technol.*, vol. 10, no. 1, pp. 21–33, 2020, doi: [10.14456/jcst.2020.2](#).
- [52] G. Fenu, M. Marras, and L. Boratto, "A multi-biometric system for continuous student authentication in e-learning platforms," *Pattern Recognit. Lett.*, vol. 113, pp. 83–92, Oct. 2018, doi: [10.1016/j.patrec.2017.03.027](#).
- [53] I. Traore, Y. Nakkabi, S. Saad, B. Sayed, J. D. Ardigo, and P. M. Quinan, "Ensuring online exam integrity through continuous biometric authentication," in *Information Security Practices*. Cham, Switzerland: Springer, 2017, pp. 73–81, doi: [10.1007/978-3-319-48947-6_6](#).
- [54] I. B. Ahmed, M. A. Mohamed, and A. M. Noma, "A framework for secure online exam using biometric fingerprint and steganography techniques," *Int. J. Eng. Technol.*, vol. 7, no. 3, pp. 32–35, 2018, doi: [10.14419/ijet.v7i3.28.20961](#).
- [55] K. O. Okokpuije, E. Noma-Osaghae, O. J. Okesola, S. N. John, and O. Robert, "Design and implementation of a student attendance system using iris biometric recognition," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Las Vegas, NV, USA, 2017, pp. 563–567, doi: [10.1109/csci.2017.96](#).
- [56] S. Wong-In and P. Netinant, "Revised software model design for biometric examiner personal verification system," in *Proc. ICIT*, Singapore, 2017, pp. 237–242, doi: [10.1145/3176653.3176678](#).
- [57] M. Moradi, M. Moradkhani, and M. B. Tavakoli, "Security-level improvement of IoT-based systems using biometric features," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–15, Feb. 2022, doi: [10.1155/2022/8051905](#).
- [58] K. Pearson, "On lines and planes of closest fit to systems of points in space," *Philos. Mag.*, vol. 2, no. 6, pp. 559–572, 1901.
- [59] H. Hotelling, "Analysis of a complex of statistical variables into principal components," *J. Educ. Psychol.*, vol. 24, no. 6, pp. 417–441, Sep. 1933, doi: [10.1037/h0071325](#).
- [60] M. M. Ahsan, Y. Li, J. Zhang, M. T. Ahad, and K. D. Gupta, "Evaluating the performance of eigenface, fisherface, and local binary pattern histogram-based facial recognition methods under various weather conditions," *Technologies*, vol. 9, no. 2, p. 31, Apr. 2021, doi: [10.3390/technologies9020031](#).
- [61] A. Dube, D. Singh, R. K. Asthana, and G. S. Walia, "A framework for evaluation of biometric based authentication system," in *Proc. ICISS*, Thoothukudi, India, 2020, pp. 925–932, doi: [10.1109/iciss49785.2020.9315933](#).
- [62] A. Kanak and I. Sogukpinar, "BioTAM: A technology acceptance model for biometric authentication systems," *IET Biometrics*, vol. 6, no. 6, pp. 457–467, Nov. 2017, doi: [10.1049/iet-bmt.2016.0148](#).
- [63] Y. Zhou, "Evaluation of biometric recognition in the COVID-19 period," in *Proc. 2nd Int. Conf. Comput. Data Sci. (CDS)*, Stanford, CA, USA, Jan. 2021, pp. 243–248, doi: [10.1109/cds52072.2021.00049](#).
- [64] J. Oh, U. Lee, and K. Lee, "Usability evaluation model for biometric system considering privacy concern based on MCDM model," *Secur. Commun. Netw.*, vol. 2019, pp. 1–14, Mar. 2019, doi: [10.1155/2019/8715264](#).
- [65] W. R. Malatji, R. Eck, and T. Zuva, "Acceptance of biometric authentication security technology on mobile devices," in *Proc. IMITEC*, Kimberley, South Africa, 2020, pp. 1–5, doi: [10.1109/imitec50163.2020.9334082](#).
- [66] S. Siddique, M. Yasmin, T. B. Taher, and M. Alam, "The reliability and acceptance of biometric system in Bangladesh: Users perspective," *Int. J. Comput. Trends Technol.*, vol. 69, no. 6, pp. 1–6, Jun. 2021, doi: [10.14445/22312803/ijctt-v69i6p103](#).
- [67] M. El-Abed, C. Charrier, and C. Rosenberger, "Evaluation of biometric systems," in *New Trends and Developments in Biometrics*, vol. 7. London, U.K.: IntechOpen, 2012, pp. 149–169, doi: [10.5772/52084](#).
- [68] *IEEE Standard for Information Technology—Systems Design—Software Design Descriptions*, Standard IEEE 1016-2009, 2009, doi: [10.1109/IEEESTD.2009.5167255](#).
- [69] *Systems and Software Engineering—Systems and Software Quality Requirements and Evaluation (SQuaRE)—Guide to SQuaRE*, Standards ISO/IEC 25000, 2014.
- [70] P. Kumari and P. Thangaraj, "A fast feature selection technique in multi modal biometrics using cloud framework," *Microprocessors Microsystems*, vol. 79, Nov. 2020, Art. no. 103277, doi: [10.1016/j.micpro.2020.103277](#).

- [71] A. Alshbhat, N. Zanoon, and M. Alfraheed, "A novel secure fingerprint-based authentication system for student's examination system," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 9, pp. 515–519, 2019, doi: [10.14569/IJACSA.2019.0100968](https://doi.org/10.14569/IJACSA.2019.0100968).
- [72] M. Rukhiran, S. Pukdesree, and P. Netinant, "Development and evaluation of biometric authentication system based on facial and voice recognition," *ICIC Exp. Lett.*, vol. 16, no. 10, pp. 1027–1035, Oct. 2022, doi: [10.24507/icieel.16.10.1027](https://doi.org/10.24507/icieel.16.10.1027).
- [73] R. Pi, *MTBF Values of the Revolution Pi Modules*, Jan. 14, 2021. [Online]. Available: <https://revolutionpi.com/mtbf-revolution-pi-modules>
- [74] Y. Chen, J. Yang, C. Wang, and D. Park, "Variational Bayesian extreme learning machine," *Neural Comput. Appl.*, vol. 27, no. 1, pp. 185–196, Jan. 2016, doi: [10.1007/s00521-014-1710-1](https://doi.org/10.1007/s00521-014-1710-1).
- [75] A. S. Raju and V. Udayashankara, "A survey on unimodal, multimodal biometrics and its fusion techniques," *Int. J. Eng. Technol.*, vol. 7, no. 4, pp. 689–695, 2018, doi: [10.14419/ijet.v7i4.36.24224](https://doi.org/10.14419/ijet.v7i4.36.24224).
- [76] S. Poria, N. Majumder, R. Mihalcea, and E. Hovy, "Emotion recognition in conversation: Research challenges, datasets, and recent advances," *IEEE Access*, vol. 7, pp. 100943–100953, 2019, doi: [10.1109/ACCESS.2019.2929050](https://doi.org/10.1109/ACCESS.2019.2929050).



MEENNAPA RUKHIRAN received the B.Sc. degree in computer information systems from Burapha University, Thailand, in 2006, and the M.S. degree in information technology management and the Ph.D. degree in information technology from Rangsit University, Thailand, in 2014 and 2020, respectively. She is currently an Assistant Professor of information technology with the Faculty of Social Technology, Rajamangala University of Technology Tawan-ok, Chanthaburi, Thailand. Her research interests include multidimensional software design, system software framework, technology acceptance models, the Internet of Things, aspect orientation, information systems with chatbots, web-based development, mobile development, implementation, data mining, and theory of computation.



SETHAPONG WONG-IN received the B.S. degree in applied statistics from the King Mongkut's University of Technology North Bangkok, Thailand, in 1997, and the M.S. degree in information technology from the King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand, in 2000. He is currently pursuing the Ph.D. degree in information technology with Rangsit University, Pathum Thani, Thailand. He is also an Assistant Professor of information technology with Valaya Rajabhat University, Pathum Thani. His current research interests include software design, biometrics, the Internet of Things, data analysis, and software engineering.



PANITI NETINANT received the B.S. degree (Hons.) in computer science from Bangkok University, Thailand, in 1994, and the M.S. and Ph.D. degrees in computer science from the Illinois Institute of Technology, Chicago, IL, USA, in 1996 and 2001, respectively. He is currently an Associate Professor of computer science of the doctoral program in information technology and an Associate Dean with the Graduate School, Rangsit University, Thailand, where he is responsible for information technology and international affairs. His research interests include adaptive software architecture, operating systems, bot information systems, mobile development, the Internet of Things, compilers, object-oriented approach, aspect-oriented approach, and cloud computing services. He is a member of the international technical committee and a reviewer of IEEE and ACM conference papers.

...

ประวัติผู้วิจัย

ชื่อ	เศรษฐพงศ์ วงษ์อินทร์
วัน เดือน ปีเกิด	7 สิงหาคม 2518
สถานที่เกิด	จังหวัดกรุงเทพฯ ประเทศไทย
ประวัติการศึกษา	สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ ปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาสถิติประยุกต์, 2540 สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยี สารสนเทศ, 2543
ที่อยู่ปัจจุบัน	77/889 ซอย 9/3 หมู่บ้านดวงแก้ว ถ.ติวานนท์ ต.บ้าน ใหม่ อ.ปากเกร็ด จ.นนทบุรี
สถานที่ทำงาน	คณะวิทยาศาสตร์ มหาวิทยาลัยราชภัฏวไลยอลงกรณ์ ใน พระบรมราชูปถัมภ์
ตำแหน่งปัจจุบัน	ประธานหลักสูตรนวัตกรรมดิจิทัลและวิศวกรรม ซอฟต์แวร์