ระบบตรวจสอบใบหน้าด้วยปัญญาประดิษฐ์จากบัตรประชาชน

กรี สมุทรพูนไพศาล

ธชรัฐ ช้างมงคล

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตร์บัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2560

ระบบตรวจสอบใบหน้าด้วยปัญญาประดิษฐ์จากบัตรประชาชน

นายกรี สมุทรพูนไพศาล 60010019
นายธชรัฐ ช้างมงคล 60010376
รศ.ดร เจริญ วงษ์ชุ่มเย็น อาจารย์ที่ปรึกษา
ปีการศึกษา 2563

บทคัดย่อ

โดยทั่วไปแล้วขั้นตอนการยืนยันตัวบุคคลในธนาคารจะทำได้โดยเจ้าหน้าที่เปรียบเทียบภาพถ่ายในบัตรประชาชนกับใบหน้าจริงของบุคคลนั้น กระบวนการนี้มีแนวโน้มที่จะผิดพลาดเนื่องจากเจ้าหน้าที่มักจะต้องให้บริการคนหลายคนในเวลาอันสั้น

บทความนี้เสนอระบบการยืนยันตัวบุคคลโดยใช้บัตรประชาชนและรูปถ่ายใบหน้าโดยใช้การตรวจจับใบหน้าและการเปรียบเทียบใบหน้า มีการใช้ระบบที่ใช้ไลบรารีโอเพนซอร์สหลายตัวสำหรับการจดจำใบหน้ารวมถึง Dlib, Facenet และ ArcFace

การวิเคราะห์ทดลองแสดงให้เห็นว่าระบบที่ใช้ ArcFace ให้ความแม่นยำสูงสุดที่ 99.06% สำหรับการตรวจจับใบหน้าและ 96.09% สำหรับการเปรียบเทียบใบหน้า ArcFace มีประสิทธิภาพเหนือกว่าวิธีการอื่น ๆ เนื่องจากไม่เพียง แต่ใช้ MTCNN แต่ยังปรับภาพใบหน้าให้อยู่ในทิศทางตรงรวมทั้งแก้ไขตำแหน่งคิ้วจมูกตาและปากเพื่อให้ภาพทั้งหมดมีการอ้างอิงที่คล้ายคลึงกัน

Face Recognition To Identify And Verify System With ID Card

Mr. Kree	Samutpoonpaisan	60010113
Mr. Tacharat	Changmongkol	60010376
Assoc. Prof. Dr. Charoen	Vongchumyen	Advisor

Academic Year 2020

ABSTRACT

Abstract—Generally, the process of verifying a person's identification in a bank is accomplished by an officer comparing a photo in an ID card with the actual face of the person. This process is prone to mistake as officers usually need to serve several people in a short time.

This article proposes the personal verification system using an ID card and face photo by applying face detection and face comparison. A system based on several open source libraries for face recognition including Dlib, Facenet, and ArcFace is implemented.

The experimental analysis shows that the system based on ArcFace yields the highest accuracy at 99.06% for face detection and 96.09% for face comparison. ArcFace outperforms other methods because it not only uses MTCNN but also adjusts face image to be in a straight direction as well as fixes the positions of eyebrows, eyes nose, and mouth so that all images have similar references.

กิตติกรรมประกาศ

กิตติกรรมประกาศ เป็นการกล่าวขอบคุณบุคคลที่มีส่วนร่วมให้ความช่วยเหลือจนปริญญานิพนธ์สำเร็จลงได้ด้วยดี

นายกรี สมุทรพูนไพศาล

นายธชรัฐ ช้างมงคล

สารบัญ

หน้า

สารบัญ(ต่อ)

สารบัญตาราง

สารบัญรูป

รูป **หน้า**

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญ

ในปัจจุบันการพิสูจน์ตัวตนนั้นมีหลากหลายวิธี ไม่ว่าจะเป็นการใช้เอกลักษณ์ของแต่ละบุคคลในการพิสูจน์ตัวตนเช่น การสแกนลายนิ้วมือหรือการสแกนม่านตาเป็นตน แต่การพิสูจน์ตัวตนที่เป็นที่นิยมและเป็นมาตรฐานที่ได้รับการยอมรับ นั่นคือการพิสูจน์ตัวตนด้วยบัตรประชาชน ซึ่งบัตรประชาชนนั้นเป็นเอกสารทางราชการออกให้กับประชาชนผู้มีสัญชาติไทยเพื่อพิสูจน์ทราบและยืนยันตัวบุคคลในการขอให้สิทธิ หรือประกอบธุรกรรมต่าง ๆที่เกี่ยวข้องกับภาครัฐและเอกชนและเอกสารลำดับแรกที่ก่อให้เกิดสิทธิอื่น ๆตามมา

จากประโยชน์และความสำคัญของบัตรประจำตัวประชาชนที่กล่าวมานั้นทำให้ผู้ไม่ประสงค์ดีต้องการบัตรจำตัวประชาชนของผู้อื่น เพื่อไปดำเนินการด้านธุรกรรมต่าง ๆ โดยมิชอบ เช่น นำไปเปิดบัญชีธนาคาร ทำให้เกิดความเดือดร้อน และเสียหายต่อผู้เป็นเจ้าของบัตร หรืออาจนำมาซึ่งข้อมูลอันเป็นเท็จที่เกิดจากการปลอมแปลงบัตรประชาชน ซึ่งส่งผลต่อควบคุมข้อกำหนดต่าง ๆ เช่น การห้ามจำหน่ายสุราแก่ผู้ที่มีอายุต่ำกว่า 20 ปี

โดยการพิสูจน์ตัวตนโดยปกติแล้ว จะใช้เครื่องอ่านบัตรประชาชนอ่านข้อมูลจากชิปการ์ดในบัตรประชาชน ก็จะได้ข้อมูลภายในชิปการ์ดที่จะประกอบไปด้วย เลขบัตรประชาชน, ชื่อ, นามสกุล, วันเกิดและวันหมดอายุบัตร แล้วให้เจ้าหน้าที่นั้นจะเป็นผู้ตรวจสอบใบหน้าในบัตรประชาชนกับเจ้าของบัตรซึ่งการทำงานในรูปแบบนี้อาจเกิดข้อผิดพลาดขึ้นได้

โครงงาน “ระบบตรวจสอบใบหน้าด้วยปัญญาประดิษฐ์จากบัตรประชาชน(Face recognition to identify and verify system with id card)” นี้จึงถูกจัดทำขึ้นเพื่อสามารถพิสูจน์ตัวตนด้วยรูปจากบัตรประชาชนและใบหน้าผู้เข้าใช้บริการ เพื่อลดและหลีกเลี่ยงการพิสูจน์ตัวตนที่ผิดพลาด อีกทั้งเพื่อไม่ให้เกิดการละเมิดกฎต่าง ๆ

1.2 วัตถุประสงค์ของโครงงาน

1) เพื่อเก็บข้อมูลการเข้าใช้บริการตามสถานที่ เพื่อนำไปติดตามเฝ้าระวังผู้มีโอกาสติดเชื้อไวรัสโคโรนา(contact tracing)
2) เพื่อสร้างเครื่องเก็บข้อมูลบุคคลจากข้อมูลบัตรประชาชน โดยยืนยันความถูกต้องผ่านการเปรียบเทียบข้อมูลใบหน้า
3) เพื่อศึกษาระบบตรวจสอบและเปรียบเทียบใบหน้า
4) เพื่อนำข้อมูลบัตรประชาชนมาใช้ในการติดตามบุคคลในภายหลัง

1.3 ขอบเขตของโครงงาน

1) สร้างอุปกรณ์ทำการอ่านข้อมูลบัตรประชาชน ดึงเอาข้อมูล รูปภาพ วันเกิด ชื่อ นามสกุล เพศ รหัสประชาชนมาแสดงผลผ่านบนหน้าจอ
2) สร้างอุปกรณ์ทำการถ่ายรูปบุคคลเพื่อเอามาเปรียบเทียบจากรูปภาพในบัตรประชาชน แสดงผลความเหมือนกันของใบหน้าภายในระยะเวลาไม่เกิน 10 วินาที และมีความแม่นยำแล้วแสดงผลผ่านหน้าจอ
3) สร้างอุปกรณ์เก็บข้อมูลเมื่อเปรียบเทียบใบหน้า ได้แก่ ช่วงเวาตอนใช้งานอุปกรณ์ ความเหมือนกันของใบหน้า และข้อมูลในบัตรประชาชน รองรับจำนวนผู้ใช้ 10,000 คน โดยซ้ำกันได้
4) สร้างอุปกรณ์สามารถดูข้อมูลทั้งหมดที่เก็บมาได้ตลอดเวลา โดยแสดงผลเป็น datasheet สามารถเลือกแสดงผลสรุปข้อมูลเป็นวัน หรือเดือน
5) สร้างอุปกรณ์สามารถดึงข้อมูลใช้ค้นหาผู้ป่วย ผู้ที่อาศัย คนทำงาน หรือใช้ชีวิตประจำวัน อยู่ในชุมชน หรือในบริเวณเดียวกับผู้ป่วย เช่น แผนก ชั้นที่ทำางาน โรงเรียน ที่พัก (ค่ายทหาร เรือนจำ) ตึกคอนโดมิเนียม สถานบันเทิง

1.4 วิธีการดำเนินการ

1) สืบค้นข้อมูลและเอกสารการตรวจจับใบหน้า และการอ่านข้อมูลจากบัตรประชาชน
2) ออกแบบเครื่องในการตรวจจับใบหน้าด้วยกล้องไอพี(IP Camera) และอ่านข้อมูลบัตรประชาชน
3) ออกแบบระบบการตรวจจับใบหน้าจากข้อมูลบัตรประชาชน
4) สร้างเครื่องและระบบตามการออกแบบ
5) เขียนโปรแกรมให้เครื่องทำงานกับระบบตรวจสอบใบหน้า
6) ทดสอบการออกแบบระบบและเครื่องทุกฟังก์ชันหลัก
7) ปรับปรุงการออกแบบระบบและเครื่องทุกฟังก์ชันหลัก
8) ทดสอบออกแบบระบบและฟังก์ชันรวม
9) ปรับปรุงการออกแบบระบบและฟังก์ชันรวม
10) ทดสอบ เก็บลายละเอียด และเก็บข้อมูลที่ได้จากทำโครงงาน
11) สรุปปัญหาและแนวทางการพัฒนาต่อ

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1) เก็บข้อมูลการเข้า
   ใช้บริการตามสถานที่เพื่อนำไปติดตามเฝ้าระวังผู้มีโอกาสติดเชื้อไวรัสโคโรนา (contact tracing)
2) สร้างเครื่องเก็บข้อมูลบุคคลจากข้อมูลบัตรประชาชน โดยยืนยันความถูกต้องผ่านหาเปรียบเทียบข้อมูลใบหน้า
3) นำข้อมูลบัตรประชาชนมาใช้ในการติดตามบุคคลในภายหลัง

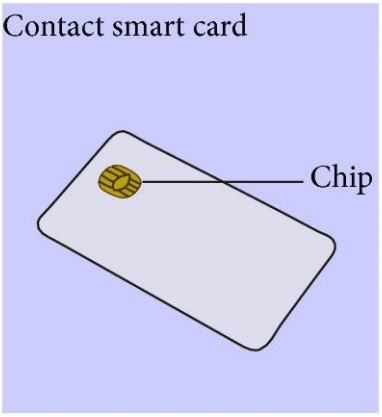
บทที่ 2
อุปกรณ์ ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 อุปกรณ์ที่เกี่ยวข้อง

2.1.1 สมาร์ทการ์ด[1]

2.1.1.1 สมาร์ทการ์ดแบบสัมผัส

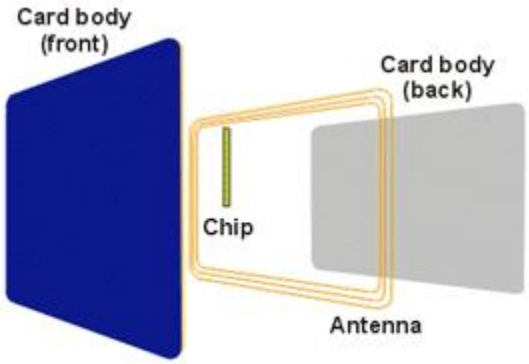
สมาร์ตการ์ดแบบสัมผัส (contact smart card) ตัวบัตรมีการฝังชิปใต้หน้าสัมผัสที่เป็นแผ่นโลหะสีทองขนาดเล็ก เส้นผ่าศูนย์กลางประมาณครึ่งนิ้วไว้ที่ด้านหน้าของบัตร ตอนใช้งานต้องสอดบัตรเข้าในเครื่องอ่านให้หน้าสัมผัสของบัตรได้แตะกับหน้าสัมผัสภายในเครื่องอ่านบัตร ส่วนใหญ่จะเป็นกับบัตรเครดิตหรือบัตรเอทีเอ็ม ปัจจุบันประเทศไทยได้ใช้สมาร์ตการ์ดชนิดนี้ทำบัตรประจำตัวประชาชนหรือซิมการ์ดของโทรศัพท์มือถือ ปัจจุบันมีการทำบัตรเครดิตที่เป็นสมาร์ทการ์ดแบบสัมผัสด้วยเป็นบัตรวีซ่า pay wave เช่น บัตรบลูการ์ด



รูปที่ 1 Contact smart card[1]

2.1.1.2 สมาร์ทการ์ดแบบไร้สัมผัส

สมาร์ตการ์ดแบบไร้สัมผัส (contactless smart card) ตัวบัตรจะมีการฝังชิปและขดลวดสายอากาศเอาไว้ภายในซึ่งอาจมองด้วยตาเปล่าไม่เห็น สามารถติดต่อกับเครื่องอ่านบัตรที่รับส่งสัญญาณผ่านคลื่นวิทยุได้ในระยะที่กำหนด ซึ่งอาจเป็นระยะที่ใกล้ชิด (proximity card) หรือระยะที่ใกล้เคียง (vicinity card) แล้วแต่มาตรฐานของบัตร โดยไม่จำเป็นต้องให้บัตรสัมผัสกับเครื่องอ่านดังกล่าว ส่วนใหญ่จะใช้กับบัตรเก็บเงินทางด่วน บัตรโดยสารของรถไฟฟ้า บีทีเอสและรถไฟฟ้าใต้ดิน และบัตรชำระเงินย่อยเช่นบัตร Smart Purse เป็นต้น



รูปที่ 2 Contactless Smart card[2]

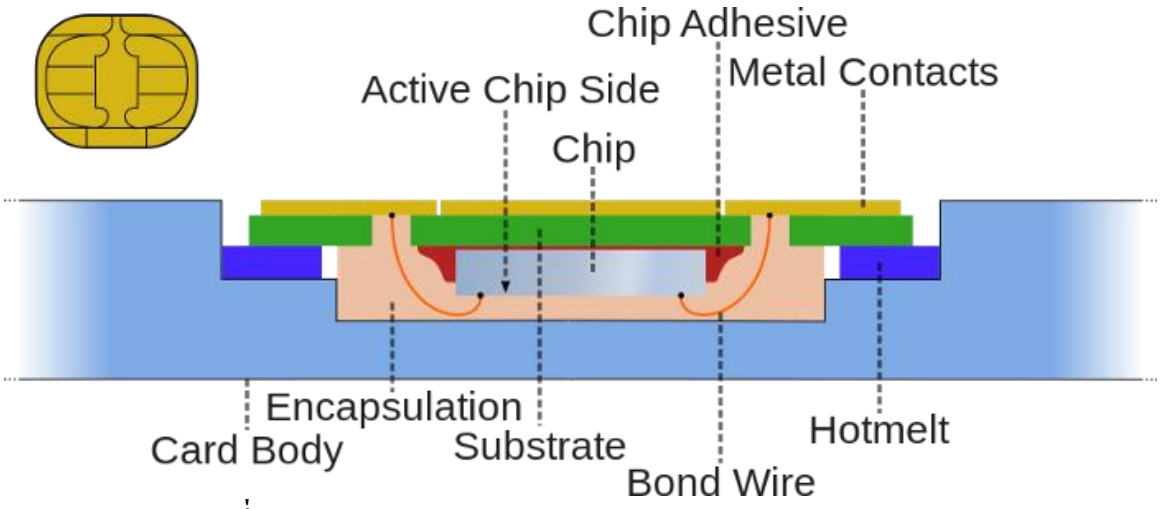
2.1.2 บัตรประชาชน[2]

บัตรประจำตัวประชาชน เป็นเอกสารที่ทางราชการออกให้กับประชาชนผู้มีสัญชาติไทย เพื่อพิสูจน์ทราบและยืนยันตัวบุคคลในการขอให้สิทธิ หรือประกอบธุรกรรมต่างๆ ที่เกี่ยวข้องกับภาครัฐและเอกชนและเป็นเอกสารสำคัญที่สุด และ ณ ปัจจุบันที่ได้พัฒนาระบบการบริการประชาชน โดยใช้บัตรประจำตัวประชาชนเพียงใบเดียวเป็นหลักฐานในการขอรับบริการต่างๆ จากภาครัฐ

รูปที่3 ตัวอย่างบัตรประชาชน [3]

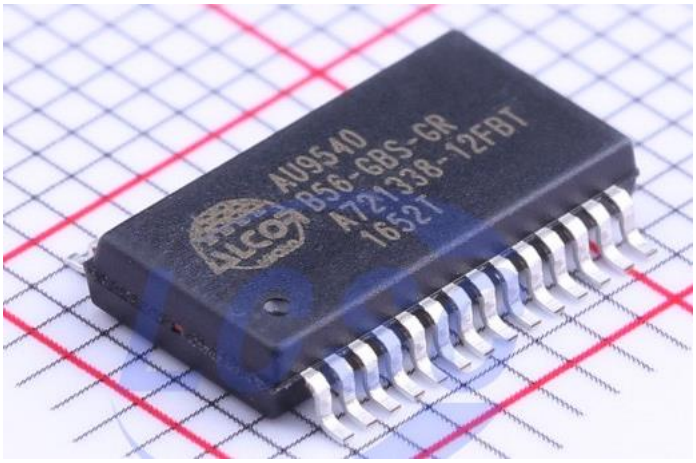
2.1.3 ชิป[3]

คือ ส่วนของพื้นที่ในบัตรมีพื้นที่สัมผัสประมาณ 1 ตารางเซนติเมตร (0.16 ตร.ว.) ประกอบด้วยแผ่นสัมผัสเคลือบทองหลายแผ่น แผ่นอิเล็กโทรดเหล่านี้ให้การเชื่อมต่อเมื่อเสียบเข้ากับเครื่องอ่าน



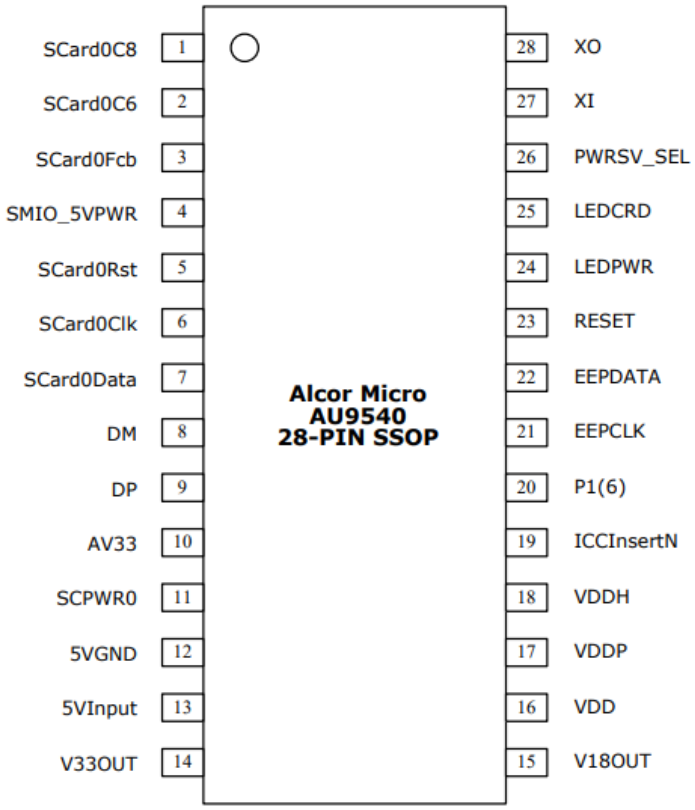
รูปที่4 Illustration of smart-card structure and packaging[4]

2.1.4 AU 9540[4]



รูปที่ 5 IC AU9540 [5]

AU9540 เป็นคอนโทรลเลอร์ USB Smart Card reader แบบชิปเดี่ยว การผสานรวมที่สูง ช่วยให้ต้นทุน BOM ต่ำที่สุดสำหรับเครื่องอ่านสมาร์ทการ์ด AU9540 รองรับมาตรฐานสากลหลาย มาตรฐานรวมถึง ISO7816 สำหรับมาตรฐาน IC card, PC / SC 2.0 สำหรับมาตรฐานสมาร์ทการ์ดของ windows, Microsoft WHQL, EMV สำหรับมาตรฐาน Europay MasterCard Visa และมาตรฐาน USB-IF CCID โดยทั่วไปแอปพลิเคชัน AU9540 สามารถใช้กับอุปกรณ์ปลายทางสำหรับอ่าน / เขียนบัตร สมาร์ทการ์ดเช่น ATM เครื่อง POS โทรศัพท์สาธารณะอีคอมเมิร์ซการใช้งานส่วนบุคคลบน อินเทอร์เน็ตการรับรองส่วนบุคคล ระบบชำระเงินล่วงหน้า ระบบที่มีความสม่ำเสมอ



รูปที่ 6 AU9540 Pin Assignment Diagram [6]

2.2 ทฤษฎีที่เกี่ยว

2.2.1 ISO/IEC 7816[5]

มาตรฐานผลิตภัณฑ์อุตสาหกรรมบัตรชี้บ่งลักษณะเฉพาะตัว-บัตรวงจรรวมมีตัวสัมผัส เป็นมาตรฐานที่กำหนดบัตรเรื่องการมีการเชื่อมโยงทางกายภาพด้วยตัวสัมผัสไฟฟ้า(chip) ในไทย ประกาศโดยกระทรวงอุตสาหกรรรม วันที่ 1 กันยายน พ.ศ. 2552

2.2.2 APDU (Application Protocol Data Unit) [6]

มาตราฐานในการสื่อสารของ smart card ที่ถูกกำหนดใน ISO/IEC 7816–4 โดยมี 2 ประเภท

2.2.2.1 APDU command

เป็นคำสั่งส่งไปเพื่อให้ smart card ทำงานตามที่ต้องการ ชุดคำสั่งมี 2 ส่วน คือ header และ body (header เป็นส่วนที่ต้องมี แต่ body ไม่มีก็ได้)

Command APDU		
Field name	**Length (bytes)**	**Description**
CLA	1	Instruction class - indicates the type of command, e.g. interindustry or proprietary
INS	1	Instruction code - indicates the specific command, e.g. "write data"
P1-P2	2	Instruction parameters for the command, e.g. offset into file at which to write the data
L_c	0, 1 or 3	Encodes the number (N_c) of bytes of command data to follow 0 bytes denotes N_c=0 1 byte with a value from 1 to 255 denotes N_c with the same value 3 bytes, the first of which must be 0, denotes N_c in the range 1 to 65 535 (all three bytes may not be zero)
Command data	N_c	N_c bytes of data
L_e	0, 1, 2 or 3	Encodes the maximum number (N_e) of response bytes expected 0 bytes denotes N_e=0 1 byte in the range 1 to 255 denotes that value of N_e, or 0 denotes N_e=256 2 bytes (if extended L_c was present in the command) in the range 1 to 65 535 denotes N_e of that value, or two zero bytes denotes 65 536 3 bytes (if L_c was not present in the command), the first of which must be 0, denote N_e in the same way as two-byte L_e

ตารางที่ 1 **Command APDU**

2.2.2.2 APDU response

เป็นข้อมูลที่ส่งกลับมาโดย smart card และ data field คือข้อมูลที่บัตรส่งกลับมา ขนาดไม่แน่นอน หรือไม่มีเลย ส่วนของ SW1 และ SW2 มีขนาด 1 byte เป็นข้อมูลบอกสถานะการทำงานของ APDU command ที่ส่งไป

Response APDU		
Response data	N_r (at most N_e)	Response data
SW1-SW2 (Response trailer)	2	Command processing status, e.g. 90 00 (hexadecimal) indicates success

ตารางที่ 2 Respponse APDU

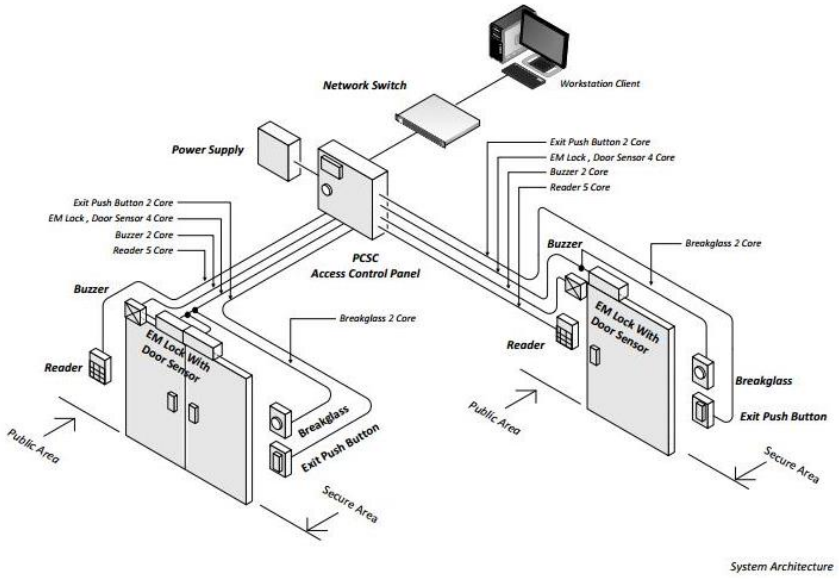
ตารางด้านล่างนี้ใช้อ้างอิงเวลาเขียนโปรแกรมรับส่งข้อมูลบัตร ปกติแล้วคำสั่งจะมาในรูปของ array ของ command ส่งไปก่อน 1 รอบเพื่อบอก smart card ว่ากำลังจะรับส่งข้อมูลอะไร รอบ 2 ที่ส่ง เป็นการขอข้อมูลจากบัตร ก็จะทำเหมือนรอบที่ 1 แต่ส่ง array ของ get response และมี le ต่อท้าย โดยที่ le เป็น byte สุดท้ายของข้อมูล

Description	CLA	INS	P1	P2	Lc	Data	Le
Select	0x00	0xA4	0X04	0x00	0x08	0xA0, 0X00, 0x00, 0x00, 0x54, 0x48, 0x00, 0x01	
GET RESPONSE	0X00	0XC0	0x00	0x00			
CID	0x80	0xB0	0x00	0x04	0x02	0x00	0x0D
TH Fullname	0x80	0xB0	0x00	0x11	0x02	0x00	0x64
EN Fullname	0x80	0xB0	0x00	0x75	0x02	0x00	0x64
Date of birth	0x80	0xB0	0x00	0xD9	0x02	0x00	0x08
Gender	0x80	0xB0	0x00	0xE1	0x02	0x00	0x01
Card Issuer	0x80	0xB0	0x00	0xF6	0x02	0x00	0x64
Issue Date	0x80	0xB0	0x01	0x67	0x02	0x00	0x08
Expire Date	0x80	0xB0	0x01	0x6F	0x02	0x00	0x08
Address	0x80	0xB0	0x15	0x79	0x02	0x00	0x64
Photo_Part1/20	0x80	0xB0	0x01	0x7B	0x02	0x00	0xFF
Photo_Part2/20	0x80	0xB0	0x02	0x7A	0x02	0x00	0xFF
Photo_Part3/20	0x80	0xB0	0x03	0x79	0x02	0x00	0xFF
Photo_Part4/20	0x80	0xB0	0x04	0x78	0x02	0x00	0xFF
Photo_Part5/20	0x80	0xB0	0x05	0x77	0x02	0x00	0xFF
Photo_Part6/20	0x80	0xB0	0x06	0x76	0x02	0x00	0xFF
Photo_Part7/20	0x80	0xB0	0x07	0x75	0x02	0x00	0xFF
Photo_Part8/20	0x80	0xB0	0x08	0x74	0x02	0x00	0xFF
Photo_Part9/20	0x80	0xB0	0x09	0x73	0x02	0x00	0xFF
Photo_Part10/20	0x80	0xB0	0x0A	0x72	0x02	0x00	0xFF
Photo_Part11/20	0x80	0xB0	0x0B	0x71	0x02	0x00	0xFF
Photo_Part12/20	0x80	0xB0	0x0C	0x70	0x02	0x00	0xFF
Photo_Part13/20	0x80	0xB0	0x0D	0x6F	0x02	0x00	0xFF
Photo_Part14/20	0x80	0xB0	0x0E	0x6E	0x02	0x00	0xFF
Photo_Part15/20	0x80	0xB0	0x0F	0x6D	0x02	0x00	0xFF
Photo_Part16/20	0x80	0xB0	0x10	0x6C	0x02	0x00	0xFF
Photo_Part17/20	0x80	0xB0	0x11	0x6B	0x02	0x00	0xFF
Photo_Part18/20	0x80	0xB0	0x12	0x6A	0x02	0x00	0xFF
Photo_Part19/20	0x80	0xB0	0x13	0x69	0x02	0x00	0xFF
Photo_Part20/20	0x80	0xB0	0x14	0x68	0x02	0x00	0xFF

ตารางที่ 3 **APDU ประเทศไทย**

2.2.3 Access Control System [7]

ระบบควบคุมการเข้าออกแบบอัตโนมัติ ถูกออกแบบขึ้นเพื่อใช้กำหนดสิทธิ์ในการเข้าออก ให้กับบุคลากรภายในที่เกี่ยวข้อง และป้องกันเหตุร้ายที่อาจเกิดจากบุคคลภายนอก มีการบริหารจัดการระบบอย่างมีประสิทธิภาพสามารถกำหนดช่วงเวลา ที่อนุญาตให้ผ่านเข้าออก และกำหนดสิทธิ์ในการเข้าออกแต่ละประตูแยกกันได้อย่างอิสระมีทั้งระบบ Standalone สำหรับทางเข้าออกเดี่ยว หรือสำหรับ อาคารขนาดเล็ก และระบบ Network ที่สามารถใช้ควบคุมทางเข้าออกทั้งหมด จากจุดควบคุมเพียงจุดเดียวหรือหลายจุดก็ตาม ซึ่งเหมาะสำหรับอาคารขนาดใหญ่ ทั้งนี้สามารถเลือกใช้ให้เหมาะสมกับสถานที่ต่าง ๆ ตามความต้องการ ปรับใช้ได้กับองค์กรทั่วไป เลือกรูปแบบการขออนุญาตเข้าออกได้หลายวิธี ซึ่งอาจตรวจสอบสิทธิ์ โดยใช้รหัส, บัตร หรือลายนิ้วมือ อย่างใดอย่างหนึ่งหรือเลือกใช้ร่วมกันเพื่อเพิ่มความปลอดภัยยิ่งขึ้น นอกจากใช้เพื่อควบคุมการเข้าออก ยังสามารถประยุกต์ใช้เพื่อ ประโยชน์ในด้านต่าง ๆ ได้อีกมากมาย เช่น ใช้สำหรับรายงานการปฏิบัติงานของเจ้าหน้าที่รักษาความปลอดภัย ที่จะต้องไปตรวจสอบความปลอดภัยยังจุดต่าง ๆ ของอาคาร, ใช้เชื่อมต่อกับระบบ Time Attendance ระบบรายงานการเข้าออกและคำนวณเวลาปฏิบัติงานของพนักงาน หรือการใช้งานด้านอื่น ที่จะต้องอาศัยข้อมูล การผ่าน เข้าออกยังจุดต่าง ๆ



รูปที่ 7 Access control system architecture [7]

2.2.4 Time Attendance[8]

เป็นชื่อเรียกของระบบลงเวลา เช่น การเข้างาน ออกงาน โดยในอดีต เป็นการใช้การตอกบัตร หรือ การลงลายมือชื่อ เพื่อยืนยันการเข้างาน และในปัจจุบันเปลี่ยนมาเป็นการใช้เครื่องลงเวลา เพื่อป้องกันการทุจริต และ เป็นการอำนวยความสะดวกให้กับพนักงาน โดยเป็นเพียงเครื่องที่มีระบบเพียงแค่ การดูการเข้าออกของพนักงาน บอกเวลาในการเข้างาน ออกงานของพนักงานเพียงเท่านั้น

2.2.5 Face detection [9]

การตรวจจับใบหน้า (รูปที่ 8) คือกระบวนการในการหาพื้นที่ของใบหน้าบนรูปภาพในปัจจุบันมีแอพพลิเคชั่นมากมายที่ต้องการใช้รูปใบหน้าเพื่อนำไปพัฒนาระบบเช่นระบบรู้จำใบหน้า (Face Recognition) ระบบรู้จำอารมณ์บนใบหน้า (Facial Expression Recognition) ระบบรู้จำองค์ประกอบบนใบหน้า (Facial Attribute Recognition) และระบบการประกอบโครงสร้างใบหน้าขึ้นมาใหม่ (Facial Shape Reconstruction) โดยทุกระบบจะต้องใช้การตรวจจับใบหน้าเป็นขั้นตอนแรกในการประมวลผลทำให้การตรวจจับใบหน้านั้นจะต้องมีประสิทธิภาพที่ดีที่สุดกล่าวคือความผิดพลาดในการตรวจจับสิ่งอื่นที่ไม่ใช่ใบหน้าต้องน้อย (False Positive) ความถูกต้องในการตรวจจับใบหน้าต้องสูง (True Positive) และการประมวลผลต้องไวเพื่อให้การประมวลผลในขั้นตอนต่อ ๆ ไปให้ผลลัพธ์ที่ดีที่สุด

รูปที่ 8 ตัวอย่างของการตรวจจับใบหน้า [8]

ในช่วงแรกของการศึกษาการตรวจจับใบหน้านั้นวิธีที่ใช้ในการตรวจจับใบหน้าถูกแบ่งออกเป็น 4 กลุ่มหลัก [10] คือ 1) การใช้กฎเกณฑ์พื้นฐานของมนุษย์ (Knowledge-based Method) 2) การค้นหาลักษณะ

เด่น (Feature Invariant Method) 3) การใช้แม่แบบมาตรฐาน (Template Matching Method) และ 4) การใช้วิธีทางสถิติ (Statistical-based Method)

1) การใช้กฎเกณฑ์พื้นฐานของมนุษย์ (Knowledge-based Method) นั้นจะหาความสัมพันธ์ขององค์ประกอบต่าง ๆบนใบหน้าโดยใช้ระยะทางและตำแหน่งตามกฎเกณฑ์ที่ตั้งไว้ซึ่งมีอุปสรรคคือการหากฎเกณฑ์ที่เฉพาะเจาะจงที่ใช้ในการจำแนกใบหน้าของมนุษย์นั้นทำได้ยากหากกฎเกณฑ์นั้นระบุรายละเอียดมากเกินไปจะทำให้ตรวจจับใบหน้าได้ยาก (เพราะไม่มีภาพใดผ่านเกณฑ์เลย) หรือหากกฎเกณฑ์น้อยเกินไปผลที่ได้อาจจะตรวจจับสิ่งอื่นที่ไม่ใช่ใบหน้ามาด้วยอีกทั้งเมื่อนำไปใช้ตรวจจับใบหน้าที่หันในทิศทางอื่นกฎเกณฑ์ในการตรวจจับใบหน้าในทิศทางนั้น ๆ จะทำได้ยากเนื่องจากมีความซับซ้อนและไม่คงที่

2) การค้นหาลักษณะเด่น (Feature Invariant Method) จะใช้การวิเคราะห์ใบหน้าด้วยการหาองค์ประกอบบนใบหน้าเบื้องต้นเช่นตาคิ้วจมูกและปากจากนั้นจึงใช้แบบจำลองทางสถิติ (Statistical Model) ในการอธิบายถึงความสัมพันธ์เพื่อยืนยันการตรวจพบใบหน้าซึ่งมีข้อเสียคือเมื่อมีเงาและสภาพแสงที่ไม่คงที่องค์ประกอบดังกล่าวอาจถูกบดบังจากเงาทำให้ระบบไม่เจอใบหน้านั้น ๆ

3) การใช้แม่แบบมาตรฐาน (Template Matching Method) จะใช้แม่แบบมาตรฐานของใบหน้าที่ถูกกำหนดขึ้นเองด้วยมือเช่นการกำหนดแม่แบบของใบหน้าซึ่งประกอบด้วย 16 พื้นที่และ 23 ความสัมพันธ์ภาพที่ถูกรับเข้ามาจะนำมาถูกหาค่าสหสัมพันธ์ (Correlation Value) กับใบหน้าที่เป็นรูปแบบมาตรฐานในส่วนขององค์ประกอบบนใบหน้าเช่นโครงหน้าดวงตาจมูกและปากซึ่งมีข้อดีคือสามารถทำได้ค่อนข้างง่าย แต่ประสิทธิภาพในการตรวจจับใบหน้านั้นยังไม่ดีเท่าที่ควรซึ่งเกิดจากผลของขนาดตำแหน่งการวางและรูปทรงของใบหน้าที่แตกต่างจากตัวแม่แบบมาตรฐาน

4) การใช้วิธีทางสถิติ (Statistical-based Method) จะเรียนรู้ความสัมพันธ์จากองค์ประกอบบนใบหน้าจากกลุ่มตัวอย่างภาพในฐานข้อมูลเพื่อหารูปแบบของใบหน้าและส่วนที่ไม่ใช่ใบหน้าวิธีการนี้มีความแม่นยำและความไวในการตรวจสูงและยังสามารถรับมือกับใบหน้าที่หันข้างได้ แต่มีข้อเสียคือต้องใช้เวลาในการสอนให้กับระบบและต้องใช้จำนวนภาพในฐานข้อมูลเยอะเพื่อให้ผลลัพธ์ออกมามาเป็นที่น่าพอใจ

ในปัจจุบันมีฐานข้อมูลที่เก็บภาพใบหน้าออกมาให้ใช้มากมายซึ่งช่วยสนับสนุนการใช้วิธีทางสถิติอย่างมากในปัจจุบันวิธีการตรวจจับใบหน้าจึงได้ถูกแบ่งใหม่ออกเป็น 3 ประเภทคือ 1) Boosting-Based Method 2) Deep Convolutional Neural Networks (DCNNs) lax 3) Deformable Parts-based Models (DPM) methods [11]

1) Boosting-Based Method จะใช้ตัวอย่างข้อมูลจำนวนมากของภาพใบหน้าและภาพที่ไม่ใช่ใบหน้าเพื่อนำมาสร้างเป็นแบบจำลองเพื่อใช้ในการแยกใบหน้าโดยจะหาค่าตัวจำแนกแบบอ่อนแอ (Weak Classifier) ที่มีความผิดพลาดของน้ำหนักน้อยที่สุดนำไปปรับน้ำหนักในรอบถัดไปโดยเลือกส่งเสริมน้ำหนักให้กับตัวที่ไม่ผ่านการจำแนก แต่ลดน้ำหนักตัวที่ผ่านการจำแนกจนได้ตัวจำแนกที่แข็งแรง (Strong Classifier) ซึ่งจะนำตัวจำแนกนี้ไปใช้ในการหาใบหน้า

2) DCNNs จะสร้างชั้นข้อมูลที่ทำหน้าที่เรียนรู้ความเป็นไปได้ของมุมมองบนใบหน้าด้วยการขยายข้อมูลโดยการสร้างมุมมองของใบหน้าสมมติขึ้นมาซึ่งมีประสิทธิภาพในการทำงานสูง แต่ต้องใช้ฐานข้อมูลภาพใบหน้าที่หันในมุมมองต่าง ๆจำนวนมาก

3) DPMs จะใช้ส่วนประกอบต่าง ๆบนใบหน้าหรือวัตถุที่เราสนใจเพื่อใช้ในการตรวจจับซึ่งส่วนประกอบที่ถูกตรวจเจอนั้นจะถูกนำมารวมกันเป็นส่วนประกอบใหญ่ซึ่งวิธีนี้สามารถใช้กับภาพใบหน้าหันข้างได้เช่นเดียวกับ DCNNs แต่ใช้ข้อมูลในการสอนระบบน้อยกว่า

2.2.6 Face recognition[12]

การจดจำใบหน้าเริ่มต้นด้วยการแยกพิกัดของคุณสมบัติต่าง ๆบนใบหน้าเช่น ความกว้างของปาก, ดวงตา, ม่านตา และนำมาเปรียบเทียบกับรูปที่เก็บไว้ในฐานข้อมูล แล้วจึงส่งบันทึกที่ใกล้เคียงที่สุดกลับไป ปัจจุบันมีเทคนิคและอัลกอริทึมการจดจำใบหน้าจำนวนมากที่พบและพัฒนาขึ้นทั่วโลก การจดจำใบหน้ากลายเป็นหัวข้อวิจัยที่น่าสนใจโดยได้รับการพิสูจน์จากเอกสารเผยแพร่จำนวนมากที่เกี่ยวข้องกับการจดจำใบหน้ารวมถึงการดึงคุณลักษณะใบหน้าการปรับปรุงอัลกอริทึมใบหน้าและการประยุกต์ใช้การจดจำใบหน้า

2.3 งานวิจัยที่เกี่ยวข้อง

2.3.1 Personal Verification System Using ID Card and Face Photo [13]

บทความนี้ศึกษาและดำเนินการระบบด้วยการตรวจจับใบหน้าและการเปรียบเทียบใบหน้าโดยใช้สามวิธีที่ได้รับการยอมรับอย่างกว้างขวาง ได้แก่ Dlib, Facenet และ ArcFace การวิเคราะห์เชิงทดลองของเราแสดงให้เห็นว่า ArcFace เป็นโซลูชันที่เหมาะสมที่สุดโดยมีความแม่นยำสูงสุดถึง 96% เนื่องจากหน้าตรงของ ArcFace สามารถเปรียบเทียบคุณสมบัติที่โดดเด่นบนใบหน้าได้ดีกว่าวิธีอื่น ๆ นอกจากนี้ ArcFace ยังตรวจจับใบหน้าบนภาพที่มีรอยขีดข่วนและสะท้อนแสงได้ดีกว่าวิธีอื่น ๆ สำหรับการทำงานในอนาคตการเปรียบเทียบใบหน้าโดยคำนึงถึงอายุของใบหน้าเป็นสิ่งที่

น่าสนใจเนื่องจากบัตรประจำตัวประชาชนหลายใบมีอายุการใช้งานที่แน่นอน ระยะเวลามากกว่าหนึ่งปีเป็นเวลาที่ยาวนานเพียงพอสำหรับการเปลี่ยนแปลงใบหน้าของใครบางคนและด้วยเหตุนี้จึงอาจเกิดข้อผิดพลาดในการเปรียบเทียบใบหน้าได้

บทที่ 3
การออกแบบและพัฒนาระบบ

การออกแบบและพัฒนาระบบตรวจสอบใบหน้าด้วยปัญญาประดิษฐ์จากบัตรประชาชนนั้นต้องอาศัยการทำงานของฮาร์ดแวร์และซอฟต์แวร์ซึ่งมุ่งเน้นในเรื่องของความถูกต้องในการพิสูจน์ตัวตนเป็นหลัก โดยจะรับข้อมูลมาจากรูปภาพจากกล้องและข้อมูลจากบัตรประชาชนเพื่อนำมาเปรียบเทียบในการพิสูจน์ตัวตน

การออกแบบนั้นต้องรู้ถึงความต้องการของระบบ

3.1 ความต้องการของระบบ

3.1.1 ความต้องการของฮาร์ดแวร์

3.1.1.1 ระบบกล้อง

โดยตัวกล้องนั้นต้องมีความละเอียดของภาพสูง (Network Camera) โดยที่ความละเอียดไม่น้อยกว่า 3MP หรือดีกว่า สามารถปรับเปลี่ยนระยะของเลนส์ได้ เพื่อให้ได้ระยะของภาพที่ต้องการ มีเทคโนโลยี Low pass Filter สำหรับตัดแสงที่สว่างจ้า (แสงไฟหน้ารถ) เพื่อให้ได้ภาพที่ชัดเจน มีชุดอินฟาเรด สำหรับส่องภาพในเวลากลางคืน กล้องรองรับมราตฐานการใช้งานระดับ IP66 กรณีติดตั้งใช้งานภายนอก

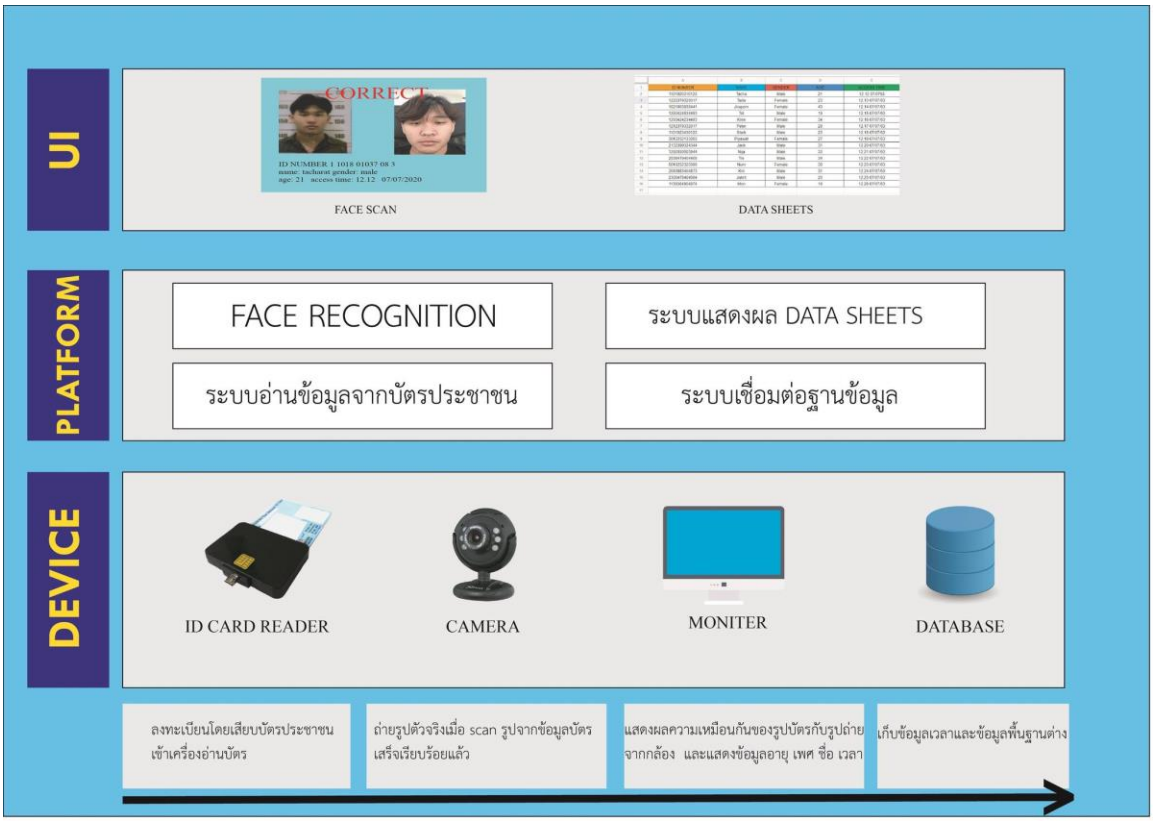
3.1.1.2 ระบบอ่านบัตรประชาชน

การใช้เครื่องอ่านบัตรประชาชนหลังจากเสียบบัตรตัวเครื่องจะนำข้อมูลที่ได้จากการอ่านส่งมายังระบบโดยจะได้รับข้อมูลที่ประกอบไปด้วย เลขประจำตัวประชาชน คำนำหน้า ชื่อ ชื่อสกุล วันเกิด และรายละเอียดที่อยู่

3.1.2 ความต้องการของซอฟต์แวร์

3.1.2.1 ระบบตรวจจับใบหน้า

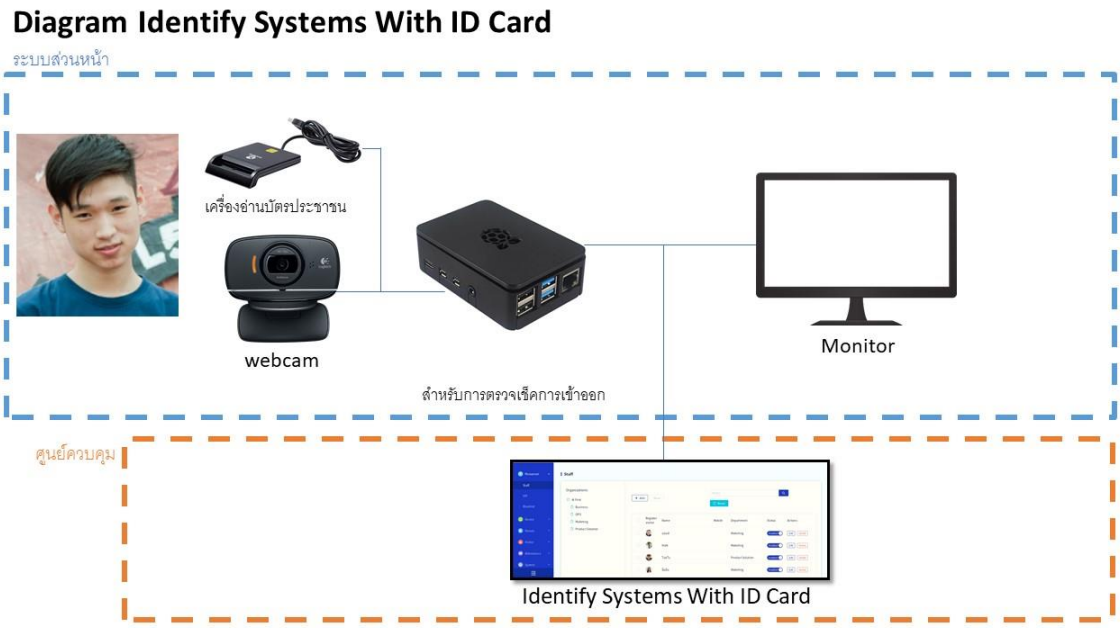
สามารถวิเคราะห์การตรวจจับใบหน้าและสามารถทำการเปรียบเทียบใบหน้าโดยระบบจะวิเคราะห์จากลักษณะเฉพาะต่าง ๆ บนใบหน้า ประกอบไปด้วย โครงหน้า ความกว้างของจมูก ระยะห่างระหว่างตาทั้งสองข้าง ขนาดของโหนกแก้ม ความลึกของเบ้าตา และ พื้นผิวใบหน้าเป็นต้น



3.2 ภาพรวมของระบบ

ระบบตรวจสอบใบหน้าด้วยปัญญาประดิษฐ์จากบัตรประชาชนถูกอออกแบบมาเพื่อตอบสนองการพิสูจน์ตัวตนด้วยบัตรประชาชน

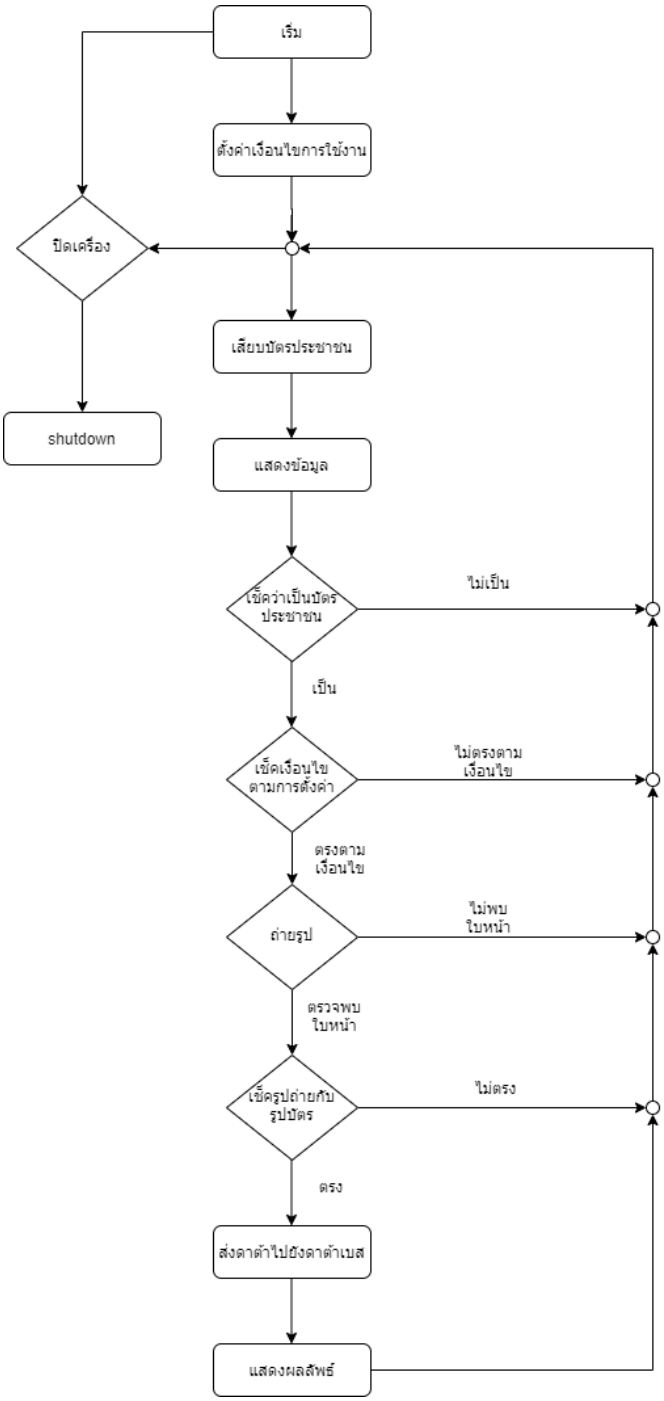
สำหรับการนำข้อมูลจากบัตรประชาชนมาใช้งานมีอุปกรณ์อ่านข้อมูลจากชิพบัตรประชาชนเพื่อดึงข้อมูลผู้ใช้งาน ต่อมาหลังจากทำงานดึงข้อมูลแล้วทำงานจับภาพของผู้ใช้งานด้วยกล้อง ข้อมูลผู้ใช้งานจะถูกเก็บและประมวลผลในโปรแกรมโดยตั้งค่าเงื่อนไขต่างๆได้



3.3 การทำงานภายในระบบ

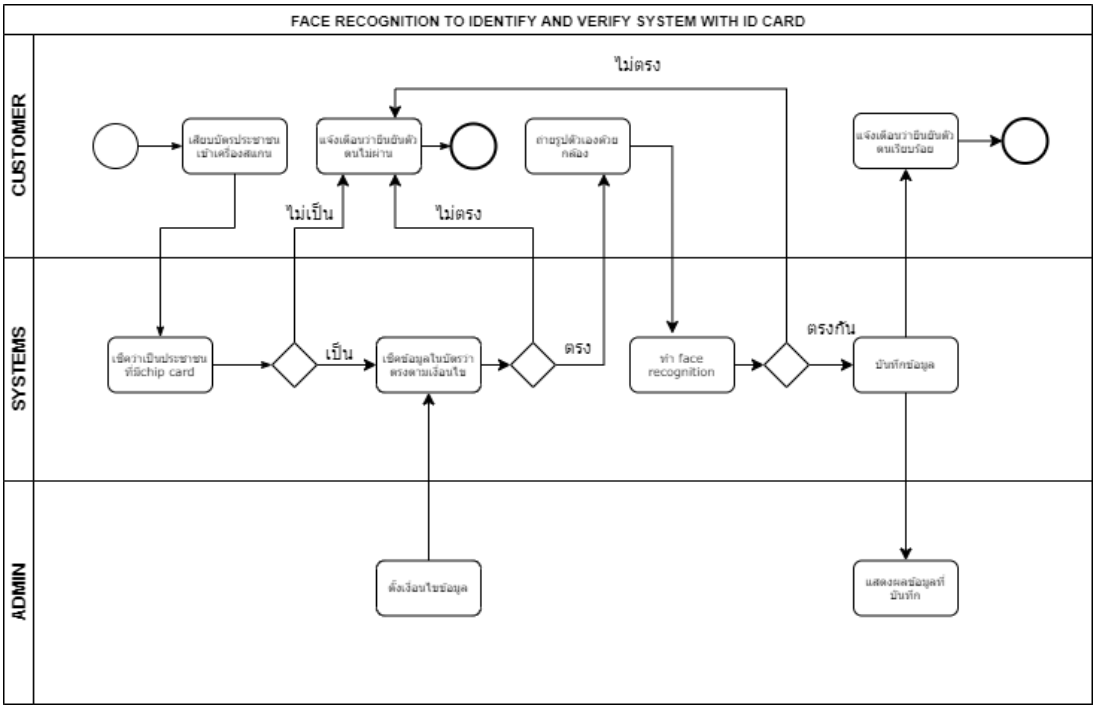
3.3.1 ขั้นตอนการทำงานของระบบตรวจสอบใบหน้าด้วยปัญญาประดิษฐ์จากบัตรประชาชน

1) ผู้ดูแลตั้งค่าอายุของผู้ใช้งาน โดยต้องการให้อายุเท่าไหร่ถึงจะสามารถเข้าใช้งานได้
2) ผู้ใช้งานนำบัตรประชาชนเสียบเข้าเครื่องอ่านข้อมูลบัตรประชานโปรแกรมดึงข้อมูลจากบัตร ถ้าอ่านบัตรไม่ได้จะขึ้นแจ้งเตือน
3) โปรแกรมจะแสดงข้อมูลของบัตรประชาชนที่ประกอบด้วย รูป ชื่อ นามสกุล อายุ เพศ และเช็คอายุว่าถึงตามเงื่อนไขหรือไม่ ถ้าไม่ถึงขึ้นแจ้งเตือนว่าผ่านไม่ได้ แต่ถ้าถึงไม่ต้องขึ้นแจ้งเตือน
4) ผู้ใช้งานยืนอยู่หน้ากล้องให้กล้องจับภาพใบหน้าได้
5) โปรแกรมจะนำรูปผู้ใช้งานที่จับภาพได้ มาทำการเปรียบเทียบใบหน้ารูปจากบัตรประชาชน ว่ามีความตรงกันหรือไม่ ถ้าตรงกันขึ้นแจ้งเตือนว่าผ่านได้ แต่ถ้าไม่ตรงกันขึ้นแจ้งเตือนว่าผ่านไม่ได้
6) ผู้ใช้งานถอดบัตรออกจากเครื่องอ่านบัตร
7) โปรแกรมจะเก็บข้อมูลผู้ใช้งานเพื่อสามารถเรียกกลับมาดูได้อีกครั้ง

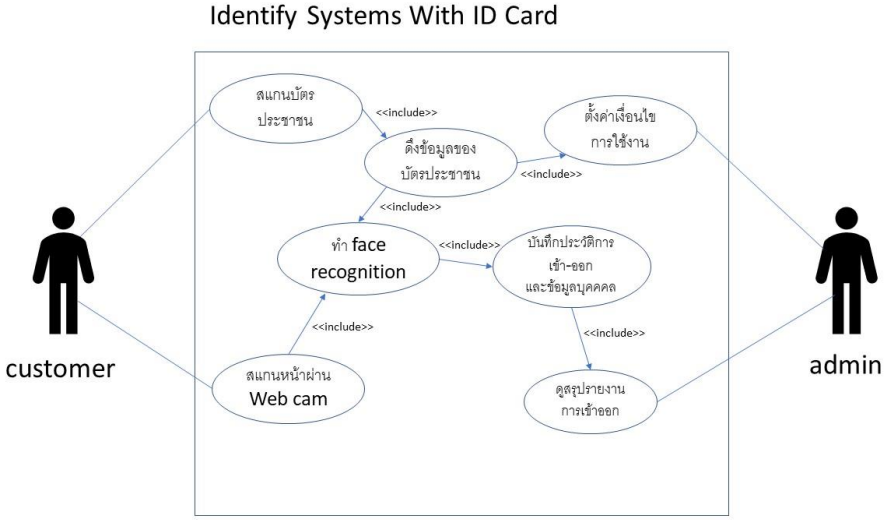

เริ่ม
ตั้งค่าเงื่อนไขการใช้งาน
ปิดเครื่อง
shutdown
เสียบบัตรประชาชน
แสดงข้อมูล
เช็คว่าเป็นบัตรประชาชน
ไม่เป็น
เป็น
เช็คเงื่อนไขตามการตั้งค่า
ไม่ตรงตามเงื่อนไข
ตรงตามเงื่อนไข
ถ่ายรูป
ไม่พบใบหน้า
ตรวจพบใบหน้า
เช็ครูปถ่ายกับรูปบัตร
ไม่ตรง
ตรง
ส่งดาต้าไปยังดาต้าเบส
แสดงผลลัพธ์

3.4 การออกแบบส่วนติดต่อผู้ใช้งาน

จากการทำงานของส่วนระบบตรวจสอบใบหน้าด้วยปัญญาประดิษฐ์จากบัตรประชาชน ทำให้ระบบได้ออกแบบส่วนติดต่อผู้ใช้งานเพื่อนำไปใช้ในการพัฒนาการทำงานของอุปกรณ์ให้รับคำสั่งและตอบสนองกับผู้ใช้งานได้ตามส่วนการออกแบบภายในระบบ



3.4.1 Use case



บทที่ 4

การทดลองระบบ

4.1 ทดลองการไหลเวียนของน้ำระหว่างบ่อเลี้ยงและถังกรอง

4.2 ทดลองการเก็บอุณหภูมิตามช่วงเวลา

4.3 ทดลองการให้อาหารอัตโนมัติโดยการตั้งเวลา

4.4 ทดลองการเลี้ยงกุ้งขาว

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

5.2 ปัญหาและอุปสรรคที่พบ

5.3 แนวทางการแก้ไข

5.4 แนวทางการพัฒนาต่อ

บรรณานุกรม