

ระบบบีนยันต์วัตนอัจฉริยะ (Intelligent Verification System)

กิตติศักดิ์ สุขกาญจนा ณัฐพงษ์ อินทร์ประดับ

ชยุต ศิริพรภูดิช

ทรงพล สายพิน

สุนันทา บุญตัน

ระบบบีนยันต์วัตนอัจฉริยะ

Intelligent Verification System

นาย กิตติศักดิ์ สุขกาญจนा
สาขา เทคโนโลยีดิจิทัลเมดิคัล
คณะ เทคโนโลยีอุตสาหกรรม
มหาวิทยาลัยราชภัฏหมู่บ้านจอมบึง
Kittisak.oomsin@gmail.com

นาย ณัฐพงษ์ อินทร์ประดับ
สาขา เทคโนโลยีดิจิทัลเมดิคัล
คณะ เทคโนโลยีอุตสาหกรรม
มหาวิทยาลัยราชภัฏหมู่บ้านจอมบึง
jj.nattpong11@gmail.com

นาย ทรงพล สายพิน
สาขา เทคโนโลยีดิจิทัลเมดิคัล
คณะ เทคโนโลยีอุตสาหกรรม
มหาวิทยาลัยราชภัฏหมู่บ้านจอมบึง
Kittisak.oomsin@gmail.com

นางสาว สุนันทา บุญตัน
สาขา เทคโนโลยีดิจิทัลเมดิคัล
คณะ เทคโนโลยีอุตสาหกรรม
มหาวิทยาลัยราชภัฏหมู่บ้านจอมบึง
Sunanthabuytan@gmail.com

นาย ชยุต ศิริพรภูดิช
สาขา เทคโนโลยีดิจิทัลเมดิคัล
คณะ เทคโนโลยีอุตสาหกรรม
มหาวิทยาลัยราชภัฏหมู่บ้านจอมบึง
chayut.glory@gmail.com

อาจารย์ที่ปรึกษา อาจารย์ ดร.นฤมล ชูเมือง
สาขา เทคโนโลยีดิจิทัลเมดิคัล คณะ เทคโนโลยีอุตสาหกรรม
มหาวิทยาลัยราชภัฏหมู่บ้านจอมบึง
อีเมล์ Lecho20@hotmail.com

1. ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันการถอนเงินจากตู้เอทีเอ็มมีเพียงแค่เลขที่บัญชีและบัตรเอทีเอ็ม ก็สามารถถอนเงินจากตู้ได้ ทันที การถอนเงินจากตู้เอทีเอ็มถึงต้องเป็นส่วนตัวและห้ามให้ผู้อื่นเห็นเลขบัญชีเด็ดขาด แต่การโจกรกรรมไม่จำเป็นต้องรับรู้ถึงเลขบัตรก็สามารถแฮกเข้าระบบธนาคารได้ ผู้ที่โจกรกรรมทางการเงินจากตู้เอทีเอ็มนี้เราจะเรียกว่า สกิมเมอร์ (Skimmer) [1] โดยวิธีการโจกรั้นนี้หัวขโมยจะนำอุปกรณ์ สกิมเมอร์ มาใช้ในการขโมยข้อมูลจากผู้ใช้บริการตู้เอทีเอ็ม ซึ่งจะทำการคัดลอกข้อมูลอิเล็กทรอนิกส์ในบัตรเอทีเอ็ม คนร้ายจะนำข้อมูลส่วนตัวของผู้เสียหายไปลักลอบเข้าบัญชี เพื่อโอนเงินไปยังบัญชีที่คนร้ายได้เตรียมไว้ การถูกโจกรั้นข้อมูลผ่านตู้เอทีเอ็ม ส่วนมากจะเกิดขึ้นภายในตึกสำนักงาน หรือตู้เอทีเอ็มที่อยู่ในที่มีด เพราะที่เหล่านี้คนไม่ค่อยปลูกพลา่น ทำให้ง่ายต่อการติดตั้งอุปกรณ์



รูปที่ 1 การถอนเงินจากตู้เอทีเอ็มในปัจจุบัน



รูปที่ 2 เครื่องมือในการโจกรั้นของ สกิมเมอร์

ในปี 2016 อัตราการโจกรั้นผ่านตู้เอทีเอ็มกลับยังคงขยายตัวทั่วโลก เช่นเดียวกับในสหราชอาณาจักร มีสถิติเพิ่มขึ้นถึง 546% จากปี 2014-2015 หรือสูงสุดเป็นประวัติการณ์จากการเก็บข้อมูลของบริษัทซอฟต์แวร์การเงินพิโก และเริ่มขยายไปยังเมืองเล็กทั่วประเทศมากขึ้นจากเดิมที่มักเกิดขึ้นในเมืองใหญ่ทางชายฝั่งตะวันออกและตะวันตกมากกว่า จากการตรวจสอบของบริษัทความมั่นคงไซเบอร์หลายแห่ง ระบุว่าวิธีการใช้โจรติดตู้เอทีเอ็มทั่วโลกมีหลายวิธีสมมตานกันไป ตั้งแต่รูปแบบเดิมๆ ที่ชื่อว่า Blackbox หรือการตัดการเชื่อมต่อของตู้กับระบบหลักแล้วใช้บัตรปลอมผ้างมัลแวร์ดูดเงินออกมาก ไปจนถึงการพัฒนามัลแวร์สกิมเมอร์ ให้มีความเข้มข้นและยากต่อการ

ตรวจจับมากขึ้น โดยเปลี่ยนจากการมุ่งเป้าข้อมูลลูกค้ารายคน เป็นการผังตัวเพื่อเก็บข้อมูลรวมของแบบกิ๊ฟมากที่สุด จากนั้นจึงเริ่มลงทะเบียนมืออย่างมืออาชีพ [2]

2. วัตถุประสงค์

- 2.1 เพื่อป้องกันการโจรมรรมาของตู้เอกสารที่อัมมและ การล่วงรู้ข้อมูลส่วนตัวในบัญชีธนาคาร
- 2.2 เพื่อยืนยันตัวตนของผู้ใช้บัญชีนั้น ๆ
- 2.3 เพื่อให้ทราบถึงใบหน้าของอาชญากร หากการยืนยันตัวตนล้มเหลว

3. ขอบเขต และ ข้อจำกัดของงาน

- 3.1 ระบบทำงานได้เฉพาะเวลากลางวัน หรือสถานที่ที่มีแสงสว่างทั่วถึง
- 3.2 หากผู้ที่ยืนยันตัวตนมีอาการป่วย หรือมีเหตุที่ทำให้เสียงของผู้ใช้เกิดการเปลี่ยนแปลง ระบบจะไม่สามารถยืนยันตัวตนได้

4. บททวนงานวิจัยที่เกี่ยวข้อง

4.1 Speech recognition คือ การทำให้คอมพิวเตอร์สามารถที่จะฟังคำพูดและตัดสินใจได้ว่าคำพูดนั้นเป็นคำว่าอะไรหรืออีกความหมายคือการนำ File Audio ที่บรรจุเสียงพูดนำมาแปลงเป็น Text ได้ Automatic Speech Recognition (ASR) เป็นเทคโนโลยีที่เกิดขึ้นเพื่อที่จะให้คอมพิวเตอร์สามารถแยกแยะคำพูดต่าง ๆ ที่มนุษย์สามารถพูดได้ อุปกรณ์ไมโครโฟนหรือเครื่องโทรศัพท์หรืออื่น ๆ เท่าที่จะเป็นไปได้ “Holy grail” of ASR Search เป็นโปรแกรมที่อนุญาตให้คอมพิวเตอร์เข้าใจคำศัพท์ทุกคำอย่างถูกต้อง 100% ซึ่งมีความสามารถเข้าใจถึงคำพูดได้ไม่จำกัดเป็นคำพูดของครรภ์ตามเป็นอิสระจากขนาดของกลุ่มคำศัพท์ , ความดัง , ลักษณะของผู้พูด และการออกเสียง หรือเงื่อนไขของช่องทางต่าง ๆ ที่เป็นไปได้ [3]

4.2 เทคโนโลยีรู้จำเสียงพูดหรือ Automatic Speech Recognition หรือ Automatic Voice Recognition เป็นเทคโนโลยีที่ใช้เวลาในการพัฒนาค่อนข้างนาน สาเหตุเนื่องจาก เป็นเทคโนโลยีที่ต้องการความสามารถในการประมวลผลจากเครื่องคอมพิวเตอร์ค่อนข้างสูง แต่ในปัจจุบันโปรแกรมการรู้จำเสียงพูดมีความสามารถสูงและเริ่มเป็นที่ยอมรับมากขึ้น มีการนำมายังในเชิงพาณิชย์ เช่น บริษัท Apple นำมาพัฒนาเป็น

โปรแกรมสนทนาร้อตตอบ ระหว่างผู้ใช้ ภายใต้ชื่อโปรแกรม SIRI โดยทั่วไปเทคโนโลยีการรู้จำเสียงพูดจะมีองค์ประกอบสำคัญ 3 ส่วน คือ

4.2.1 Acoustic Model เป็นโมเดลเก็บคุณสมบัติต่าง ๆ ของเสียงของภาษาที่เกี่ยวข้อง

4.2.2 Phonetic Dictionary เป็นพจนานุกรมเสียงที่คอมพิวเตอร์ใช้ตรวจสอบการออกเสียง

4.2.3 Language Model เป็นโมเดลช่วยให้คอมพิวเตอร์สามารถตัดสินใจเลือกคำ

ที่ต้องการ เพื่อให้การรู้จำเสียงมีความแม่นยำและมีความรวดเร็วขึ้นเนื่องจากคอมพิวเตอร์จะใช้เวลาในการเปรียบเทียบเสียงน้อยลง ยกตัวอย่างเช่น เมื่อป้อนข้อมูลด้วยประโยชน์ว่า “ฉันหิวข้าว” เมื่อคอมพิวเตอร์พยายามรู้จำเสียงพูดของคำว่า “หิว” ก็จะตรวจสอบว่ามีคำว่า “ข้าว” หรือ “น้ำ” อยู่ หรือไม่ ถ้ามีแล้วได้ยินเสียงคำถัดมา ก็จะเลือกได้โดยไม่ต้องย้อนกลับไปเปรียบเทียบกับคำอื่น ๆ ที่เหลือ [4]

4.3 ระบบการจดจำใบหน้าของมนุษย์เป็นหนึ่งในเทคโนโลยีปัญญาประดิษฐ์ หรือ AI (Artificial Intelligence) ในส่วนของ Machine Perception หรือ การรับรู้ของเครื่อง นั้นเอง โดยทั่วไปประกอบไปด้วย 2 ขั้นตอนหลัก คือ

4.2.1 การตรวจจับใบหน้า (Face Detection) คือ กระบวนการค้นหาใบหน้าของบุคคลจากภาพหรือวีดีโอ หลังจากนั้นก็ทำการประมวลผลภาพใบหน้าที่ได้สำหรับขั้นตอนถัดไป

4.3.2 การรู้จำใบหน้า (Face Recognition) คือ กระบวนการที่นำภาพไปตรวจจับประมวลผลแล้ว จากขั้นตอนการตรวจจับใบหน้า แล้วนำมาเปรียบเทียบกับฐานข้อมูลของใบหน้า เพื่อระบุว่าใบหน้านั้นตรงกับบุคคลใด [5]

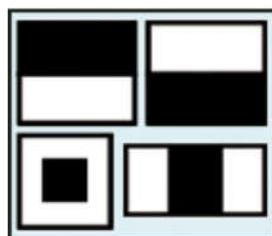
4.4 ระบบรู้จำใบหน้า (Face Recognition) ถูกออกแบบมาให้ทำการเปรียบเทียบใบหน้าบุคคลที่เราสนใจกับฐานข้อมูลใบหน้าที่มีอยู่โดยอัลกอริทึมที่ใช้ในขั้นตอนการสร้างแม่แบบและขั้นตอนการเปรียบเทียบอาจแตกต่างกันไปเล็กน้อยแต่การออกแบบระบบของแต่ละระบบ จะไม่ว่าจะมี อัลกอริทึมในการทำงานในขั้นตอนการสร้างแม่แบบและขั้นตอนการเปรียบเทียบยังไง แต่ขั้นตอนการทำงานโดยรวมของระบบก็ยังคงเหมือนกันอยู่ โดยทั่วไประบบรู้จำใบหน้าจะประกอบไปด้วย 2 ขั้นตอนหลักคือ การตรวจจับใบหน้า (Face Detection) และ การรู้จำใบหน้า (Face Recognition) [6]

4.4.1 การตรวจจับใบหน้า (Face Detection)คือกระบวนการค้นหาใบหน้าของบุคคลจากภาพหรือวิดีโอลังจกนั้นก็จะทำการประมวลผลภาพใบหน้าที่ได้สำหรับขั้นตอนถัดไปเพื่อให้ภาพใบหน้าที่ตรวจจับได้ง่ายต่อการจำแนก และอัลกอริทึมที่ใช้ในการตรวจจับใบหน้าในปัจจุบันก็มีอยู่ด้วยกันหลายวิธีซึ่งอัลกอริทึมในการตรวจจับใบหน้าที่ดีนั้นมีส่วนช่วยในการจำแนก

วิธีการหนึ่งที่ใช้ในการตรวจจับใบหน้าที่มีความสามารถในการประมวลผลได้รวดเร็วและมีอัตราความถูกต้องในการตรวจหาสูงซึ่ง Paul Viola และ Michael J. Jones ได้คิดค้นและพิมพ์ ในปี ค.ศ. 2001 โดยทั่วไปมักจะเรียกว่า Viola-Jones method ซึ่งอัลกอริทึมที่ได้นำเสนอั้นมีการนำเสนอบริการแทนรูปภาพที่เรียกว่า "Integral Image" ซึ่งช่วยให้การคำนวณfeatureทำได้รวดเร็วขึ้นและได้มีการปรับปรุงอัลกอริทึมการเรียนรู้โดยมีพื้นฐานจาก AdaBoost ซึ่งเลือกเอาเฉพาะ critical features ที่ให้ classifiers ที่มีประสิทธิภาพสูงสุด) นอกจากนี้ยังได้อธิบายถึงการรวม classifiers แบบ cascade ซึ่งช่วยให้ส่วนพื้น หลังของภาพถูกปฏิเสธได้เร็วและเน้นการคำนวนไปที่บริเวณที่มีลักษณะคล้ายวัตถุที่สนใจมากขึ้น

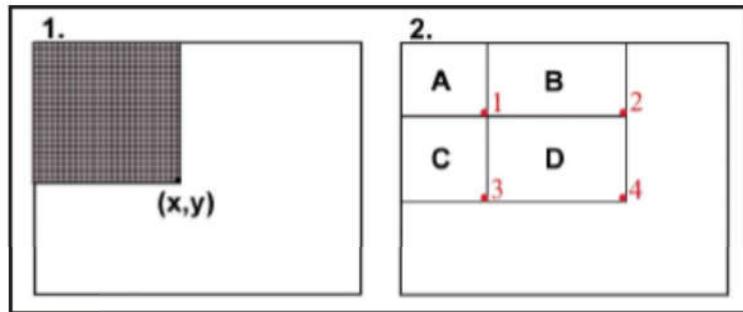
หลักการพื้นฐานของอัลกอริทึมของ Viola-Jones คือการสแกน sub-window เพื่อตรวจหาใบหน้าจากรูปภาพอินพุต การประมวลผลภาพแบบทั่วไปจะใช้การปรับขนาดภาพเข้าແຕกต่างกันหลายขนาด และใช้ตัวตรวจหา (Detector) ที่มีขนาดคงที่คันหารัตถุ ซึ่งวิธีนี้กินเวลาในการคำนวนมากเนื่องมาจากการคำนวนบนรูปภาพที่มีขนาดแตกต่างกัน Viola-Jones ได้เสนอวิธีใหม่โดยการปรับขนาดตัวตรวจหาแทนที่จะปรับขนาดภาพเข้า และใช้ตัวตรวจหากันหารัตถุหลายๆรอบ (แต่ละรอบใช้ขนาดแตกต่างกัน) ซึ่งทั้งสองวิธีน่าจะใช้เวลาในการคำนวนไม่ต่างกันมากนัก แต่ Viola-Jones ได้คิดคันตัวตรวจหาที่ใช้จำนวนครั้งในการคำนวนคงที่แม้จะมีขนาดของภาพแตกต่างกัน โดยตัวตรวจหาดังกล่าวมีร่างขึ้นโดยใช้ features ของ Haar wavelets (รูปที่ 1.1) และ Integral Image (รูปที่ 1.2)

รูปที่ 1.1 Examples of the Haar features



Example of The Haar Features

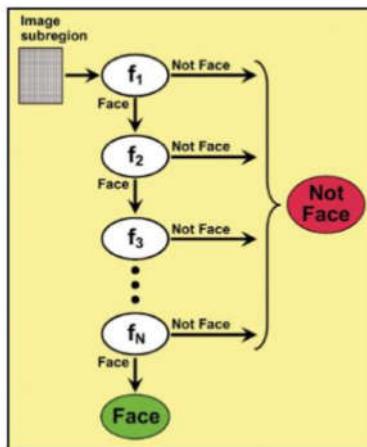
รูปที่ 1.2 The Integral Image trick



The Integral Trick

หลักการของอัลกอริทึมค้นหน้าของ Viola-Jones คือการใช้ตัวตรวจหา สแกนหลายๆ ครั้งบนภาพเดิม แต่ด้วยขนาดที่แตกต่างกัน ถึงแม้ว่าจะมีใบหน้ามากกว่าหนึ่งหน้า ผลลัพธ์ของ sub-window จำนวนมากยังคงเป็นลบ (negative non-faces) ซึ่งปัญหานี้แก้ได้โดยใช้หลักการ “ปฏิเสธสิ่งที่ไม่ใช่ใบหน้า” แทนการค้นหาใบหน้า” เพราะการตัดสินใจว่าบริเวณใด ๆ ไม่ใช่ใบหน้านั้น ทำได้เร็วกว่าการค้นหาใบหน้า และได้มีการสร้างตัวจำแนกประเภทแบบ cascaded (Cascaded classifier) คือเป็น Classifier หลายตัวต่อ กันเป็นลำดับดังแสดงในรูปที่ 1.3 ซึ่งเมื่อ sub-window ถูกจัดประเภทเป็น “ไม่ใช่ใบหน้า (non-face)” จะถูกปฏิเสธทันที แต่ในทางตรงกันข้าม ถ้า sub-window นั้น ถูกจำแนกเป็น มีโอกาสเป็นใบหน้า (maybe-face) จะถูกส่งต่อไปยัง Classifier ตัวถัดไปตามลำดับ และกล่าวได้ว่ายิ่งมีจำนวนชั้น ของ Classifier มากเท่าใด โอกาสที่ sub-window จะเป็นใบหน้าจะยิ่งมีมากขึ้น

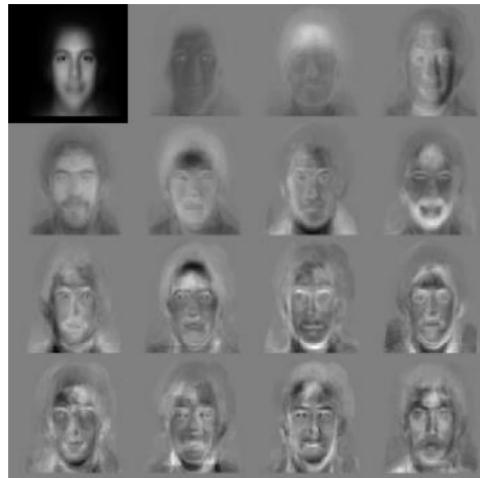
รูปที่ 1.3 The classifier cascade is a chain of filters. Image sub-regions that make it through the entire cascade are classified as “Face.” All others are classified as “Not Face.”



4.4.2 การรู้จำใบหน้า (Face Recognition) คือกระบวนการที่ได้นำภาพใบหน้าที่ตรวจจับได้และประมวลผลแล้วจากขั้นตอนการตรวจจับใบหน้ามาเปรียบเทียบกับฐานข้อมูลของใบหน้าเพื่อระบุว่าใบหน้าที่ตรวจจับได้ตรงกับบุคคลใด ตัวอย่างของอัลกอริทึมการรู้จำใบหน้าได้แก่ ๕ Principal Component Analysis (PCA)

PCA หรือ Principal Component Analysis หรือภาษาไทยเรียกว่า การวิเคราะห์องค์ประกอบหลักคือเทคนิคในการผสานลักษณะเด่นในเวคเตอร์นำเข้าเพื่อสร้างเวคเตอร์ใหม่ที่อยู่ในปริภูมิ (subspace) ที่มีดินอยกว่าเวคเตอร์เดิมโดยการผสานที่เราใช้นั้นจะเป็นการผสานเชิงเส้นตรง หรือ linear combination นั่นคือการเอาลักษณะเด่นมาคูณค่าคงที่บางอย่างแล้วค่อยบวกกัน

การนำ PCA มาใช้ในการพัฒนาระบบรู้จำใบหน้าก็จะทำได้โดยการแปลงภาพถ่ายใบหน้าบุคคลสองมิติไปเป็นเวคเตอร์หนึ่งมิติ และเก็บไว้ในฐานข้อมูล และเมื่อต้องการนำรูปภาพใบหน้าบุคคลที่ส่งเข้ามาเปรียบเทียบก็จะทำการแปลงภาพใบหน้านั้นเป็นเวคเตอร์หนึ่งมิติด้วย แล้วนำเวคเตอร์ไปเปรียบเทียบกับภาพในฐานข้อมูลเพื่อหาผลลัพธ์



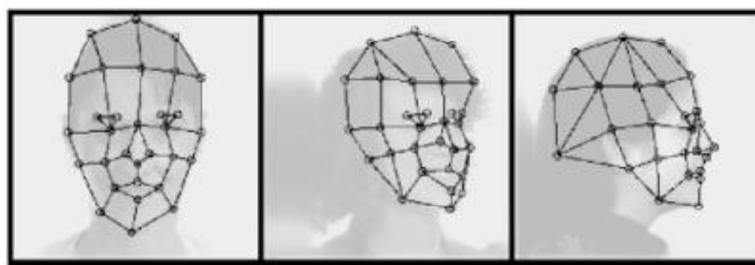
รูปที่ 1.4 ตัวอย่างของใบหน้าไอกเนน (Eigenfaces)

LDA นั้นก็จะมีวิธีการทำงานที่คล้ายกับ PCA ซึ่งใน PCA เราต้องหาปริภูมิoyerที่เมื่อฉาย (project) ข้อมูลลงไปแล้ว มีการกระจายตัวสูงสุด แต่ใน LDA เราต้องการปริภูมิoyerที่เมื่อฉายข้อมูลลงไปแล้ว ข้อมูลจาก class เดียวกันเข้าใกล้กันมากขึ้น และข้อมูลจากต่าง class กันจะอยู่ห่างกันมากขึ้นดังในรูปที่ 1.5 แต่ละบล็อกคือคลาสหรือภาพบุคคลที่มีความแตกต่างกันน้อยจะถูกจัดให้อยู่ในคลาสเดียวกัน



รูปที่ 1.5 ตัวอย่างของคลาสที่ถูกจัดกลุ่ม (Classified) โดยใช้ LDA

Elastic Bunch Graph Matching (EBGM) EBGM ตั้งอยู่บนพื้นฐานที่ว่ารูปใบหน้าของคนเรา นั้นมีส่วนที่ไม่เป็นเส้นอยู่มาก (non-linear) และไม่สามารถที่จะวิเคราะห์โดยใช้กรอบวนการเชิงเส้นอย่างวิธีที่กล่าวมาก่อนหน้านี้ได้อย่างเช่นในเรื่องของแสงที่ตัดกรอบใบหน้า, ตำแหน่งของใบหน้า และ การแสดงอารมณ์โดย EBGM จะใช้ Gabor Wavelet และ Gabor filter ในการประมวลผลและสร้างภาพใบหน้าโดยการกำหนดจุดที่สนใจบนใบหน้าหลังจากนั้นก็เก็บภาพใบหน้าที่สร้างขึ้นไว้เป็นฐานข้อมูลเมื่อต้องการที่จะทำการรู้จำกันนำภาพนำเข้ามาผ่านกระบวนการเดียวกันและเปรียบเทียบระยะห่างของแต่ละจุดของทั้งสองภาพว่ามีความใกล้เคียงเพียงพอที่จะเป็นรูปคนเดียวกันหรือไม่ซึ่งความยากของวิธีการนี้คือการกำหนดจุดที่สนใจบนใบหน้าต้องมีความแม่นยำเป็นอย่างมาก

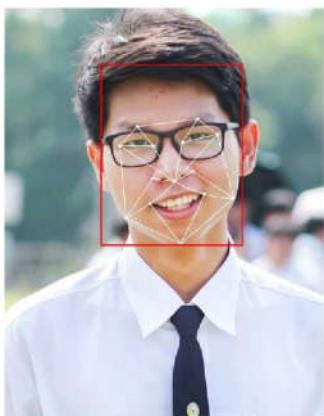


รูปที่ 1.6 Elastic Bunch Map Graphing

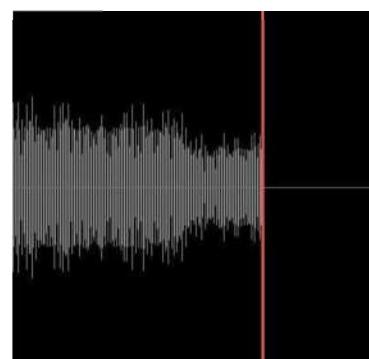
5. วิธีการพัฒนาและเทคนิคที่ใช้

ระบบยืนยันตัวตนอัจฉริยะ อุปกรณ์จะถูกติดตั้งภายในตู้เขียว ซึ่งภายในตู้เขียวที่อิมจะติดตั้งกล้องเว็บแคม เพื่อนำเข้าข้อมูลใบหน้าและเสียงของผู้ใช้ ซึ่งข้อมูลที่ได้รับมาจะถูกประมวลผลด้วยระบบ Face Recognition ระบบจะทำการตรวจหาใบหน้าของผู้ใช้และปรับภาพใบหน้าโดยอัตโนมัติ กรอบจะปรากฏขึ้นบนใบหน้าที่ถูกตรวจจับ และไฟกัล สี และค่าการวัดแสงจะถูกปรับโดยอัตโนมัติ นอกเหนือนั้นเมื่อบันทึกด้วยคุณภาพแบบ HD เทคโนโลยีการบีบอัดจะจัดสรรความจุของข้อมูลให้ลดลง แต่ได้ข้อมูลที่เป็นประโยชน์มากขึ้น เพื่อปรับคุณภาพของภาพ ข้อมูลที่ได้จะถูกนำไปเปรียบเทียบกับข้อมูลใบหน้าที่เก็บบันทึกไว้ในฐานข้อมูล อาจจะต้องใบหน้า หรือเสียงบางส่วน ขึ้นกับชนิดของวิธีแยกเอกลักษณ์ใบหน้า และข้อมูลเสียงจะถูกประมวลผลด้วยระบบ Speech Recognition ข้อมูลจะถูกทำให้อยู่ในรูปแบบของพิมพ์เสียง (Voice Print) และเพิ่มความปลอดภัยในรูปแบบไบนาリโคด (Binary Code) และนำไปเปรียบเทียบกับข้อมูลเสียงที่ได้บันทึกไว้ในฐานข้อมูล

เมื่อปีที่แล้วได้มีการประชุมผลทั้งในหน้าและเสียงได้ หากข้อมูลใบหน้าและเสียงตรงกับผู้ใช้ ระบบจะทำการส่งรหัส OTP (One Time Password คือชุดรหัสผ่านใช้ครั้งเดียวที่ระบบสร้างขึ้นเพื่อความปลอดภัยในการทำธุกรรมทางอินเทอร์เน็ต โดยเป็นตัวเลขจำนวน 6 หลัก) ไปยังโทรศัพท์เคลื่อนที่ของผู้ใช้ และเมื่อระบบได้รับรหัส OTP จากผู้ใช้ ระบบจะทำการยืนยันตัวตนกับเจ้าของบัญชีผู้ใช้ในนั้นให้ทำธุกรรมทางการเงินได้ทันที หากระบบยืนยันว่าข้อมูลใบหน้าและเสียงที่ได้รับไม่ตรงกับเจ้าของบัญชีผู้ใช้ ระบบจะทำการส่งข้อมูลใบหน้าและเสียง ซึ่งอาจจะเป็นผู้ต้องสงสัยไปยังฐานข้อมูลของสำนักงานตำรวจน้ำท่าฯ เพื่อสืบหาประวัติของผู้ที่อาจจะเป็นอาชญากรต่อไป

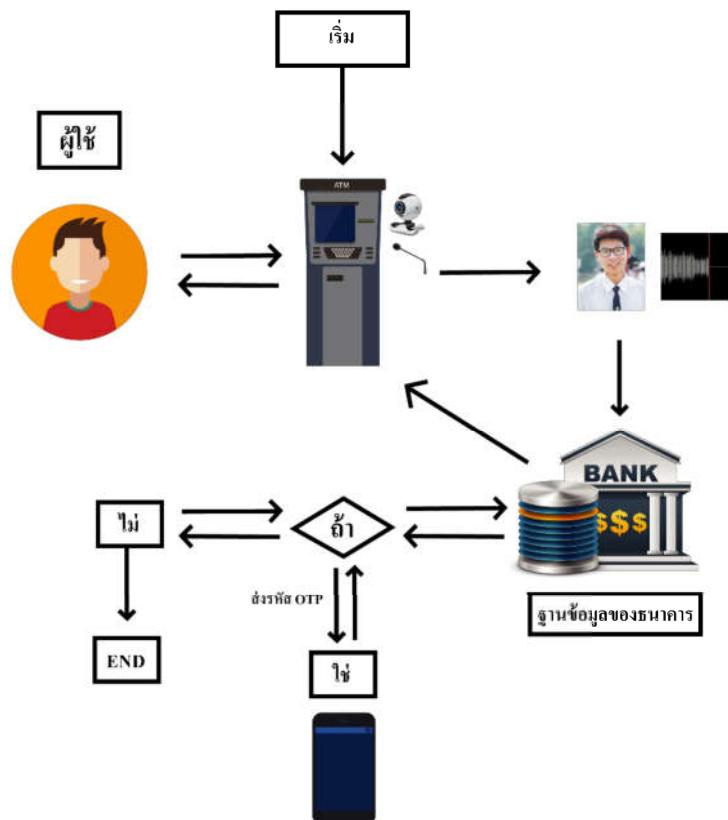


ภาพที่ประมวลผลด้วยระบบ Face Recognition



คลื่นเสียง Voice Print

ระบบการทำงาน



6. จุดเด่นของงาน และ ประโยชน์ในการนำไปใช้

- 6.1 ป้องกันบุคคลที่อาจจะแอบอ้างเป็นเจ้าของบัญชี
- 6.1 สามารถสืบหาแหล่งกบดานของอาชญากรจากสถานที่ที่ติดตั้งตู้เอทีเอ็ม
- 6.2 ป้องกันช่องเสียบบัตรเอทีเอ็มปลอมและอุปกรณ์โจมตีรุนแรงอื่น ๆ

7. อ้างอิงและเอกสารที่เกี่ยวข้อง

- [1] rabbit finance MAGAZINE, (2015). 5 เทคนิค กันขโมย โจกรรมผ่านเอทีเอ็ม, สืบค้นเมื่อวันที่ 30 ตุลาคม 2561, จากเว็บไซต์ <https://bit.ly/2ABr7uW>
- [2] โพสต์ทูเดย์, (2016). โจรไหเทคโนโลยี เป้า เจาะเอทีเอ็มทั่วโลก, สืบค้นเมื่อวันที่ 30 ตุลาคม 2561, จากเว็บไซต์ <https://bit.ly/2DcSU7h>
- [3] ภูวดล ศิริกองธรรม, (2013). เทคนิคสำหรับการควบคุมอินเทอร์เน็ตทีวีโดยคืนค่าด้วยการผสมผสานระหว่างการรู้จำเสียงและการตรวจสอบการเคลื่อนไหว, สืบค้นเมื่อวันที่ 30 ตุลาคม 2561, จากเว็บไซต์ <https://bit.ly/2Od5Jja>
- [4] รองศาสตราจารย์ ดร. สมบัติ เครือทอง, (2014). การทดสอบประสิทธิภาพโปรแกรมรู้จำเสียงพูดของโทรศัพท์มือถือไอโฟน เพื่อส่งเสริมการเรียนรู้ภาษาพูด : กรณีศึกษาภาษาอังกฤษ ฝรั่งเศส และจีน, สืบค้นเมื่อวันที่ 30 ตุลาคม 2561, จากเว็บไซต์ <https://bit.ly/2yIOMs5>
- [5] ศูนย์วิจัยยุทธศาสตร์ไทย – จีน สำนักงานคณะกรรมการวิจัยแห่งชาติ, (2018). การพัฒนาเครือข่ายเทคโนโลยีการจดจำใบหน้า (Facial Recognition Technology : FRT) ของจีน ที่ได้นำมาใช้ทั้งในด้านกิจการความมั่นคงและธุรกิจเชิงพาณิชย์, สืบค้นเมื่อวันที่ 30 ตุลาคม 2561, จากเว็บไซต์ <https://bit.ly/2ACEmLN>
- [6] mns-smartpro, (2015). ระบบวิเคราะห์ใบหน้า, สืบค้นเมื่อวันที่ 30 ตุลาคม 2561, จากเว็บไซต์ <https://bit.ly/2OXOeZe>