SUT7-709-52-12-62

รายงานการวิจัย

การตรวจสอบยืนยันแบบออนไลน์ด้วยลายเซ็นล่องหน

Online Verification Using Invisible Handwriting Signature

ได้รับทุนอุดหนุนการทำวิจัยจาก
มหาวิทยาลัยเทคโนโลยีสุรนารี

ผลงานวิจัยเป็นความรับผิดชอบของหัวหน้าโครงการวิจัยแต่เพียงผู้เดียว

SUT7-709-52-12-62

รายงานการวิจัย

การตรวจสอบยืนยันแบบออนไลน์ด้วยลายเซ็นล่องหน

Online Verification Using Invisible Handwriting Signature

คณะผู้วิจัย

หัวหน้าโครงการ

ผู้ช่วยศาสตราจารย์ ดร. พีระพงษ์ อุฑารสกุล

สาขาวิชาวิศวกรรมโทรคมนาคม

สำนักวิชาวิศวกรรมศาสตร์

มหาวิทยาลัยเทคโนโลยีสุรนารี

ได้รับทุนอุดหนุนการวิจัยจากมหาวิทยาลัยเทคโนโลยีสุรนารี ปีงบประมาณ พ.ศ. 2552

ผลงานวิจัยเป็นความรับผิดชอบของหัวหน้าโครงการวิจัยแต่เพียงผู้เดียว

เมษายน 2554

กิตติกรรมประกาศ

ขอขอบคุณมหาวิทยาลัยเทคโนโลยีสุรนารีที่ได้ให้การสนับสนุนทุนวิจัยสำหรับโครงการวิจัยนี้ ขอขอบคุณนักศึกษาในที่ปรึกษาของผู้วิจัยที่ช่วยเก็บผลการทดลองดังรายนามต่อไปนี้ นายปิยะพัทธ์ โสนันทะ นายณัฐวุฒิ พจน์ปริญญา นางสาวนลพรรณ สารีสุข และขอขอบคุณ ผู้ช่วยศาสตราจารย์ ดร. มนต์ทิพย์ ภา อุฑารสกุล สำหรับคำแนะนำในเชิงวิชาการที่เป็นประโยชน์

ผู้วิจัย

เมษายน 2554

บทคัดย่อ

การเพิ่มขึ้นอย่างมากของบริการแบบพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) สามารถสังเกตุได้ผ่านบริการต่างๆของโลกอินเตอร์เน็ต อย่างไรก็ตามวิธีที่ใช้เพื่อตรวจสอบยืนยันความเป็นเจ้าของยังใช้เพียงแค่ระบบตัวเลขหรือตัวอักษรเท่านั้น ทำให้การค้นหาวิธีการอื่นๆที่มีประสิทธิภาพจึงเป็นหัวข้อที่ได้รับความสนใจมากอยู่ในขณะนี้ สำหรับโครงการวิจัยนี้ได้เสนอวิธีการใหม่ในการตรวจสอบยืนยันด้วยเทคนิคการแปลงลายเซ็นให้เป็นข้อมูลเชิงมุม ค่าหน่วงเวลาที่เลื่อนไปสามารถวัดได้เมื่อมีการเซ็นลายเซ็นนี้ด้วยเวลาที่ไม่เท่ากัน ด้วยเทคนิคที่พัฒนาขึ้นนี้สามารถนำไปแยกองค์ประกอบของลายเซ็นได้ด้วยการพิจารณาจุดไม่ต่อเนื่องของข้อมูลเชิงมุม จากนั้นการประมาณค่าหน่วงเวลาของลายเซ็นที่ต้องการถูกตรวจสอบ นำไปเทียบกับลายเซ็นอ้างอิงที่อยู่ในฐานข้อมูล ระดับการตัดสินใจนั้นสามารถคำนวณได้จากคุณลักษณะของ FRR (False Rejection Rate) และ FAR (False Acceptance Rate) ซึ่งจะถูกปรับให้ค่าทั้งสองนี้เท่ากัน จากรายละเอียดดังกล่าวโครงการนี้จึงประดิษฐ์คำว่า ล่องหน เพราะลายเซ็นที่ส่งผ่านเครือข่ายนั้นไม่ใช่ภาพลายเซ็นที่จะมองเห็นได้ หากเป็นข้อมูลที่แปลงรหัสเชิงมุมแล้วทำให้การตรวจจับข้อมูลระหว่างทางไม่สามารถทำได้โดยง่าย และการปลอมแปลงนั้นยิ่งเป็นไปไม่ได้โดยทันที เสมือนว่าลายเซ็นนั้นหายไประหว่างการส่งข้อมูลนั้นเอง สำหรับผลการทดสอบพบว่าจากตัวอย่างลายเซ็นที่ทำการบันทึก และทำการตรวจสอบยืนยันผ่านอินเตอร์เน็ตด้วยโปรแกรมที่พัฒนาขึ้นเองนั้น ระบบที่เสนอในโครงการนี้มีความแม่นยำถึง 95.39% ซึ่งดีกว่าวิธีการตรวจสอบแบบเปรียบเทียบ 25% นอกจากนี้การตรวจสอบยืนยันลายเซ็นด้วยการแยกองค์ประกอบเชิงมุมที่เสนอนั้นยังทำให้ผลที่ได้มีความน่าเชื่อถือมากกว่าการไม่แยกองค์ประกอบอีกด้วย

Abstract

The rapid growth of e-Commerce services is significantly observed in the past decade. However, the method to verify the authenticated users still widely depends on numeric approaches. A new search on other verification methods suitable for online e-Commerce is an interesting issue. In this research project, a new online signature-verification method using angular transformation is presented. Delay shifts existing in online signatures are estimated by the estimation method relying on angle representation. In the proposed signature-verification algorithm, all components of input signature are extracted by considering the discontinuous break points on the stream of angular values. Then the estimated delay shift is captured by comparing with the selected reference signature and the error matching can be computed as a main feature used for verifying process. The threshold offsets are calculated by two types of error characteristics of the signature verification problem, False Rejection Rate (FRR) and False Acceptance Rate (FAR). The level of these two error rates depends on the decision threshold chosen whose value is such as to realize the Equal Error Rate (EER; FAR = FRR). As described above, this research project names a “invisible” signature because there is no image of signature transmitted through the internet. It is hardly possible to see or immediately remake the signature from signature feature due to angular transformation. The experimental results show that through the simple programming, employed on Internet for demonstrating e-Commerce services, the proposed method can provide 95.39% correct verifications and 25% better than basic matching based signature-verification method. In addition, the signature verification with extracting components provides more reliable results than using a whole decision making.

สารบัญ

หน้า

สารบัญรูปภาพ

หน้า

บทที่ 1 บทนำ

1.1 ความสำคัญ ที่มาของปัญหาที่ทำการวิจัย

ตั้งแต่ในอดีตถึงปัจจุบันการตรวจสอบและยืนยันความเป็นตัวตนของบุคคลในทางธุรกรรมนั้นไม่ว่าจะเป็นการเบิกเงินจากบัญชีธนาคาร การใช้บัตรเครดิต การถ่ายโอนกรรมสิทธิ์ที่ดิน การซื้อขายสังหาริมทรัพย์และอสังหาริมทรัพย์ จะใช้ลายเซ็นที่เขียนด้วยมือเพื่อบ่งบอกความถูกต้อง แต่เนื่องจากในปัจจุบันนี้การทำธุรกรรมผ่านทางระบบสื่อสารสมัยใหม่ หรือที่เรียกว่าพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) ได้รับความนิยมมาก จึงจำเป็นต้องหาวิธีการแสดงความเป็นตัวตันอื่นๆ ทดแทนลายเซ็น อาทิเช่น การกำหนดเลขรหัสลับสิบหลัก หรือการใช้ข้อมูลส่วนตัวประกอบการยืนยัน ทั้งนี้วิธีการยืนยันอื่นๆ ที่พัฒนาตามเทคโนโลยีคุณลักษณะทางกายภาพของแต่ละบุคคล (Biometrics) ยังถูกนำมาใช้งานด้วย เช่น การจดจำเสียงพูด การใช้ลายนิ้วมือ หรือการใช้ดีเอ็นเอ เพื่อตรวจสอบและยืนยันความถูกต้องด้วย อย่างไรก็ตามวิธีการต่างๆ ก็มีขีดจำกัดในการประยุกต์ใช้งานสำหรับพาณิชย์อิเล็กทรอนิกส์ กล่าวคือ การใช้รหัสลับหรือข้อมูลสามารถปลอมแปลงและจดจำได้ง่าย ส่วนการใช้เสียงพูดนั้นหากไม่สบายหรือเสียงเพี้ยนก็จะใช้ไม่ได้ การใช้ลายนิ้วมือจะเปลี่ยนตามอายุและห้ามมีรอยขีดข่วนที่นิ้วมือ สำหรับการตรวจสอบดีเอ็นเอนั้นจะต้องใช้วัสดุอุปกรณ์ที่มีราคาแพง ดังนั้นการใช้ลายเซ็นจึงดูเหมือนว่าจะเป็นวิธีการตรวจสอบที่สะดวกและมีประสิทธิภาพมากที่สุดวิธีหนึ่ง หากแต่จะต้องมีการปรับปรุงและพัฒนาให้เหมาะสมและมีความน่าเชื่อถือมากขึ้น

ปัญหาสำคัญของการใช้ลายเซ็นคือการลอกเลียนแบบ ซึ่งเกิดขึ้นเพราะมีการนำลายเซ็นมาเปรียบเทียบกันในภายหลัง ทำให้มีระยะเวลาในการปลอมแปลง และบุคคลอื่นสามารถเห็นต้นแบบลายเซ็นได้ ดังนั้นในโครงการนี้จึงเสนอวิธีการตรวจสอบลายเซ็นโดยที่ไม่ทิ้งร่องลอยของลายเซ็นไว้ หรือเรียกว่าลายเซ็นล่องหนซึ่งจะทำให้ป้องกันการปลอมแปลงได้อย่างมีประสิทธิภาพ เพราะเจ้าของลายเซ็นเท่านั้นที่ทราบวิธีการเขียน วิธีการนี้เป็นการป้องกันการทุจริตและสร้างภูมิคุ้มกันทางเศรษฐกิจให้กับประเทศซึ่งสอดคล้องกับยุทธศาสตร์การพัฒนาประเทศตามแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 10 (พ.ศ. 2550-2554) ตามยุทธศาสตร์การปรับโครงสร้างเศรษฐกิจให้สมดุลและยั่งยืน โครงการนี้ยังสามารถนำผลสำเร็จที่ได้ไปประยุกต์เพื่อใช้งานทางธุรกรรมต่างๆ รวมไปถึงพาณิชย์อิเล็กทรอนิกส์ได้ทันทีอีกด้วย จึงเป็นการเพิ่มสมรรถนะและพัฒนาศักยภาพขีดความสามารถทางเทคโนโลยีสารสนเทศและการสื่อสารของ

ประเทศซึ่งสอดคล้องกับนโยบายและยุทธศาสตร์การวิจัยของชาติ (พ.ศ. 2551-2553) ยุทธศาสตร์การวิจัยที่ 1 การสร้างศักยภาพและความสามารถเพื่อการพัฒนาทางเศรษฐกิจ นอกจากนี้ผลสำเร็จที่ได้จากโครงการถือว่าเป็นเทคโนโลยีใหม่ที่สามารถพัฒนาไปแข่งขันกับภาคอุตสาหกรรมอื่นๆในต่างประเทศได้ จึงสอดคล้องอย่างยิ่งต่อกลุ่มเรื่องที่ควรวิจัยเร่งด่วนตามนโยบายและยุทธศาสตร์การวิจัยของชาติ (พ.ศ. 2551-2553) ในเรื่องเทคโนโลยีใหม่และเทคโนโลยีที่สำคัญเพื่ออุตสาหกรรม

1.2 วัตถุประสงค์ของโครงการวิจัย

เพื่อสร้างระบบการตรวจสอบยืนยันแบบออนไลน์ด้วยลายเซ็นล่องหน สามารถตรวจสอบเจ้าของลายเซ็นล่องหนได้ โดยที่ผู้อื่นไม่สามารถเห็นหรือลอกเลียนวิธีการเขียนลายเซ็น
เพื่อป้องกันการปลอมแปลงลายเซ็น ทำให้สังคมมีคุณภาพชีวิตดีขึ้น และส่งผลต่อการสร้างภูมิคุ้มกันให้กับระบบเศรษฐกิจไทย
เพื่อสร้างเทคโนโลยีใหม่ที่มีศักยภาพในการแข่งขันกับต่างประเทศได้

1.3 แนวทางการดำเนินการวิจัย

1. ศึกษาและออกแบบอุปกรณ์ฮาร์ดแวร์สำหรับการเขียนลายเซ็นล่องหน
2. พัฒนาโปรแกรมประยุกต์เพื่อเก็บค่าสัญญาณลายเซ็น และเก็บในฐานข้อมูล
3. ศึกษาหลักการจดจำและตรวจสอบยืนยันรูปแบบ และนำหลักการนี้มาประยุกต์ใช้ในโปรแกรม
4. เก็บข้อมูลของลายเซ็นล่องหน และทดสอบการใช้งานของโปรแกรม
5. ปรับปรุงและพัฒนาระบบเพื่อให้บรรลุวัตถุประสงค์ของโครงการ
6. สรุปผลสำเร็จของโครงการและทำรายงานโครงการ

1.4 ผลสำเร็จของโครงการ

ผลสำเร็จของโครงการนี้จะมีประโยชน์ในเรื่องความปลอดภัยของการทำธุรกรรมต่างๆ และการดำเนินกิจการพาณิชย์อิเล็กทรอนิกส์ หรือประยุกต์ใช้ในการตรวจสอบยืนยันความเป็นเจ้าของในเรื่องอื่นๆ โครงการนี้มีเป้าหมายที่จะนำผลสำเร็จที่ได้ออกมาในสองลักษณะคือ

1. ตีพิมพ์บทความและเผยแพร่องค์ความรู้ทางเทคนิคบางส่วนของโครงการที่เป็นประโยชน์ต่อนักวิจัยอื่นๆ ในงานประชุมวิชาการระดับนานาชาติ อย่างน้อย 1 บทความ

2. หาแนวทางการพัฒนาผลสำเร็จนี้เพื่อการจดสิทธิบัตร ซึ่งจะสามารถนำไปสู่การผลิตในเชิงพาณิชย์ได้ในอนาคต

1.5 การสำรวจปริทรรศน์วรรณกรรมที่เกี่ยวข้องกับโครงการวิจัย

ในปัจจุบันนี้การเติบโตเชิงพาณิชย์ในเครือข่ายอินเตอร์เน็ตมีอัตราที่สูงมาก ซึ่งธุรกรรมในลักษณะนี้เรียกว่าพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) อย่างไรก็ตามเมื่อพิจารณาวิธีการตรวจสอบ ยืนยัน และกำหนดสิทธิ์ในการเข้าใช้ธุรกรรมดังกล่าวพบว่ายังคงเป็นแบบเดิมอยู่ คือใช้ตัวเลขและตัวอักษรเป็นรหัสผ่านเพื่อยืนยันการเป็นตัวตนของบุคคลนั้นๆ ตัวอย่างที่เห็นโดยทั่วไปคือ การกำหนดรหัสของอีเมลล์ การกำหนดรหัสผ่านของบัตรเครดิต เป็นต้น ทั้งนี้วิธีการดังกล่าวได้รับความนิยมเพราะง่ายในการใช้งาน แต่ก็ง่ายต่อการปลอมแปลงเช่นกัน ทำให้มีการพิจารณาแนวทาง หรือวิธีการอื่นๆ ที่สามารถให้ความน่าเชื่อถือของการตรวจสอบยืนยันความเป็นตัวตนได้มากขึ้น ในการสำรวจปริทรรศน์วรรณกรรมที่ผ่านมาพบว่ามีวิธีการหลากหลายรูปแบบที่จะนำมาประยุกต์กับการตรวจสอบออนไลน์สำหรับธุรกรรมอิเล็กทรอนิกส์ได้ วิธีการหนึ่งที่กำลังเป็นที่สนใจคือการใช้ลักษณะทางชีวภาพเป็นรหัสผ่าน เพราะลักษณะทางชีวภาพของแต่ละคนแตกต่างกันอย่างเห็นได้ชัด อาทิเช่น ลายมือ รูปหน้า ม่านในตา เสียงพูด เป็นต้น [1]-[2] ลักษณะทางชีวภาพเหล่านี้มีข้อได้เปรียบเหนือวิธีการที่ใช้ตัวเลขหรือตัวอักษรเป็นรหัสผ่านคือปราศจากการจดจำและไม่ต้องกังวลเรื่องการลืมรหัสที่กำหนดไว้ ทำให้ไม่ต้องห่วงเรื่องการขอรหัสใหม่ หรือการสูญหายของความทรงจำ แต่สิ่งที่เป็นดาบสองคมคือลักษณะทางชีวภาพเหล่านี้ส่วนมากไม่สามารถเปลี่ยนแปลงได้ หากถูกลักลอบปลอมแปลงก็จะไม่สามารถทำการเปลี่ยนรหัสใหม่ได้ ดังนั้นแนวทางอื่นๆ ที่น่าสนใจยังคงเปิดกว้างอยู่

ในโครงการวิจัยนี้ได้พิจารณาลายเซ็นมือว่ามีความเหมาะสมที่จะนำมาใช้ตรวจสอบยืนยันการเป็นตัวตนของเจ้าของเพราะลายเซ็นมือมีความซับซ้อนกว่า ตัวเลขและตัวอักษรมาก เพราะรูปแบบการสร้างลายเซ็นเป็นจินตนาการของเจ้าของเท่านั้นทำให้สามารถมีรูปแบบลายเซ็นได้ไม่จำกัด นอกจากนี้ยังสามารถเปลี่ยนแปลงได้ตามต้องการเมื่อคิดว่าลายเซ็นเก่าไม่ปลอดภัยแล้ว ซึ่งดีกว่าการใช้ลัษณะทางชีวภาพมาก [3]-[5] ในงานวิจัยด้านการตรวจสอบลายเซ็นมือนั้นสามารถแยกได้เป็นสองกลุ่มใหญ่ๆ คือแบบออนไลน์ และแบบไม่ออนไลน์ สำหรับแบบไม่ออนไลน์นั้นหมายถึงการตรวจสอบและยืนยันลายเซ็นหลังจากที่มีการเซ็นไปเรียบร้อยแล้ว ทำให้เทคนิคที่ใช้ในการตรวจสอบจะเสมือนการพิจารณาเฉพาะภาพลายเซ็นเท่านั้นไม่สามารถทราบความเร็ว จังหวะการเซ็น การหยุดของลายเซ็นได้ ซึ่งวิธีการตรวจสอบไม่ต่างอะไรกับการใช้เทคนิคการตรวจสอบภาพทั่วๆไป ซึ่งโครงงานนี้พิจารณาว่าไม่เหมาะที่จะนำมาใช้ในการตรวจสอบยืนยัน

สำหรับระบบพาณิชย์อิเล็กทรอนิกส์เพราะเป็นระบบที่ต้องการการตอบเสนอแบบในเวลาจริง (Real Time) ทำให้โครงการนี้พิจารณาเฉพาะการตรวจสอบยืนยันลายเซ็นมือแบบออนไลน์เท่านั้น

สำหรับลักษณะพิเศษของการตรวจสอบยืนยันลานเซ็นมือแบบออนไลน์คือการรับรู้ช่วงเวลาของการลากเส้นตั้งแต่ต้นจนจบ ระยะเวลาที่แตกต่างนี้เป็นอีกหนึ่งปัจจัยที่ต้องนำมาพิจารณาด้วย เพราะการปลอมลายเซ็นสามารถทำได้โดยง่ายถ้าค่อยๆ ลากเส้น ผู้ชำนาญแล้วเท่านั้นจึงจะทำให้ระยะเวลาในการเซ็นสม่ำเสมอเท่ากันทุกครับ อันนี้ถือว่าเป็นข้อดีที่ทำให้ผู้ลักลอบดูขอมูลลายเซ็นไม่สามารถปลอมแปลงได้ง่ายโดยทันที โดยทั่วไปแล้วมีแนวคิดเรื่องการตรวจสอบลายเซ็นมือออนไลน์สองกลุ่มคือกลุ่มแรกเรียกว่า Parametric Approaches (PA) [6] ซึ่งเป็นการใช้ลักษณะของลายเซ็นทั้งหมดเงื่อนไขในการพิจารณายืนยันตัวตน โดยจะไม่นำลายเซ็นที่ได้ไปแปลงเป็นรูปแบบอื่น วิธีการนี้ง่ายไม่ซับซ้อนแต่ก็มีความผิดพลาดสูง สำหรับแนวคิดที่สองนั้นเป็นการนำลักษณะของลายเซ็นแปลงเป็นความสัมพันธ์ทางเวลาเรียกว่า Functional Approaches (FA) ซึ่งแนวคิดนี้พิจารณาค่าหน่วงเวลาในการสร้างลายเซ็นร่วมด้วย เทคนิคที่ใช้แนวคิดนี้มีด้วยกันหลายเทคนิค เช่น วิธีการเปรียบเทียบด้วย Dynamic Programming (DP) [7] และวิธีการใช้ Hidden Markov Models (HMMs) [8]-[12] เป็นต้น สำหรั้บวิธีเปรียบเทียบด้วยดีพีนั้นเป็นวิธีที่สามารถทำได้เองโดยหาตำแหน่งหรือจุดหรือค่าต่างๆ ที่ได้จากการประมวลลายเซ็นในฐานข้อมูล เพื่อใช้เป็นค่าเปรียบเทียบกับลายเซ็นมือที่กำลังพิจารณาอยู่ ส่วนวิธีเอชเอ็มเอ็มจะใช้การวิเคราะห์ทางคณิตศาสตร์ขั้นสูงด้วยแบบจำลอง Markov models ทำให้วิธีนี้ต้องใช้การประมวลผลที่ยุ่งยากและซับซ้อน มีกระบวนการตรวจสอบหลายขั้นตอน ถึงแม้ว่าจะมีความแม่นยำสูงแต่วิธีการนี้ใช้เวลาในการประมวลผลนานมาก จึงไม่เหมาะที่จะนำไปใช้กับฐานข้อมูลที่มีผู้ใช้งานจำนวนมาก

สำหรับโครงการวิจัยนี้ได้เสนอวิธีการตรวจสอบยืนยันลายเซ็นแบบใหม่ตามแนวคิดแบบเอฟเอโดยจะทำการแยกองค์ประกอบของลายเซ็นตามการพิจารณาเชิงมุมในเวลาจริง วิธีการนี้จะแยกค่าหน่วงเวลาที่เกิดขึ้นตลอดลายเซ็นออกเป็นค่าหน่วงเวลาหลายๆ ค่าในแต่ละองค์ประกอบ ดังนั้นวิธีการแยกองค์ประกอบนี้จะสามารถช่วยลดความผิดพลาดลงได้ ข้อดีอีกอย่างของการพิจารณาเชิงมุมคือเมื่อมีการแปลงเชิงมุมข้อมูลของตำแหน่งพิกัดลายเซ็นเดิมจาก 2 แกนจะถูกยุบให้เหลือค่ามุมแค่มุมเดียวทำให้ประหยัดขนาดของข้อมูลที่ใช้ในการส่งผ่านเครือข่ายอินเตอร์เน็ตได้ ผลการทดสอบทั้งหมดในโครงงานนี้ถูกทดสอบผ่านเครือข่ายอินเตอร์เน็ตจริง ด้วยโปรแกรมที่พัฒนาขึ้นเองด้วย Java Servlet สรุปโดยรวมแล้วโครงงานนี้มีผลสำเร็จใหม่ 3 อย่างดังนี้ อย่างแรกเป็นการเสนอแนวคิดใหม่ที่จะนำการแปลงเชิงมุมเข้ามาร่วมในการตรวจสอบยืนยันลายเซ็นแบบออนไลน์ อย่างที่สองคือการเสนอแนวคิดใหม่เรื่องการแยกองค์ประกอบของลายเซ็นในการตรวจสอบทำให้มีความผิดพลาดลดลง และสุดท้ายคือการพัฒนาโปรแกรมและทดสอบผลเปรียบเทียบวิธีการที่เสนอมากับวิธีอื่น

บทที่ 2 การตรวจสอบยืนยันด้วยลายเซ็นมือ

2.1 กล่าวนำ

เนื้อหาในบทนี้จะกล่างถึงวิธีการตรวจสอบยืนยันลายเซ็นล่องหน โดยเริ่มด้วยการเกริ่นนำเกี่ยวกับวิธีการตรวจสอบยืนยันแบบต่างๆ ที่พบเห็นโดยทั่วไป และจากนั้นจะเป็นวิธีการตรวจสอบยืนยันลายเซ็นด้วยเทคนิคการเปรียบเทียบ ซึ่งใช้แนวคิดการเปรียบเทียบจากงานอื่นๆ มาประยุกต์เข้ากับลายเซ็นมือ และสุดท้ายเป็นการตรวจสอบยืนยันด้วยลายเซ็นล่องหนที่เสนอขึ้นในโครงการ โดยอาศัยกรรมวิธีการแปลงเชิงมุม และการแยกองค์ประกอบของลายเซ็นด้วยการพิจารณาเชิงมุม

2.2 การตรวจสอบยืนยันแบบต่างๆ

2.2.1 การตรวจสอบยืนยันตัวตนโดยใช้รหัสผ่าน

รหัสผ่านเป็นวิธีการที่ใช้มานานและนิยมใช้กันแพร่หลาย รหัสผ่านควรจำกัดให้เฉพาะผู้ใช้ที่มีสิทธิเท่านั้นที่ทราบแต่ว่าในปัจจุบันนี้ การใช้แค่รหัสผ่านไม่มีประสิทธิภาพมากพอที่จะรักษาความมั่นคงปลอดภัยให้กับระบบคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ เนื่องจากการตั้งรหัสผ่านที่ง่ายเกินไปและวิทยาการและความรู้ที่ก้าวหน้าทำให้รหัสผ่านอาจจะถูกขโมยโดยระหว่างการสือสารผ่านเครือข่ายได้

2.2.2 การตรวจสอบยืนยันตัวตนโดยใช้ PIN

PIN (Personal Identification Number) เป็นรหัสลับส่วนบุคคลที่ใช้เป็นรหัสผ่านเพื่อเข้าสู่ระบบ ซึ่ง PIN ใช้อย่างแพร่หลายโดยเฉพาะการทำธุรกรรมทางด้านธนาคาร เช่นบัตร ATM และเครดิตการ์ดต่างๆ การใช้ PIN ทำให้มีความปลอดภัยในการสื่อสารข้ามระบบเครือข่ายสาธารณะมากขึ้น เนื่องจาก PIN จะถูกเข้ารหัสเอาไว้และจำเป็นต้องมีเครื่องมือที่สามารถถอดรหัสนี้ออกมาได้ เช่นฮาร์ดแวร์ที่ออกแบบมาโดยเฉพาะ และถูกติดตั้งไว้ในเครื่องของผู้รับและผู้ส่งเท่านั้น

2.2.3 การตรวจสอบยืนยันตัวตนโดยใช้ Password Authenticators หรือ Tokens

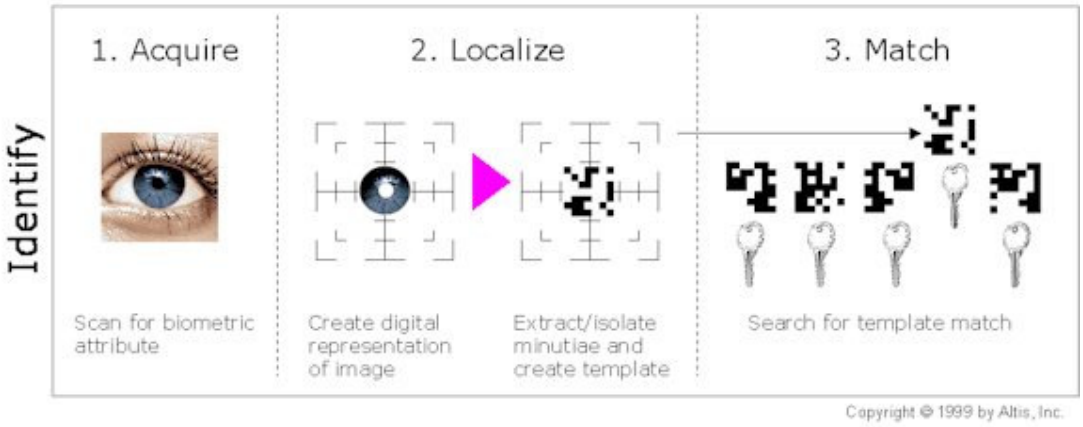
Authenticator หรือ Token เป็นฮาร์ดแวร์พิเศษที่ใช้สร้าง "รหัสผ่านซึ่งเปลี่ยนแปลงได้ (dynamic password)" ในขณะที่กำลังเข้าสู่ระบบเครือข่าย มี 2 วิธี คือ ซิงโครนัส และ อะซิงโครนัส

การตรวจสอบยืนยันตัวตนแบบซิงโครนัส แบ่งออกเป็น 2 ประเภทตามลักษณะของการใช้งาน คือ
การตรวจสอบยืนยันตัวตนแบบซิงโครนัสโดยขึ้นอยู่กับสถานการณ์ (Event-synchronous authentication) เมื่อผู้ใช้ต้องการที่จะเข้าสู่ระบบ ผู้ใช้จะต้องกด Token เพื่อให้ Token สร้างรหัสผ่านให้ จากนั้นผู้ใช้นำรหัสผ่านที่แสดงหลังจากกด Token ใส่ลงในฟอร์ม เพื่อเข้าสู่ระบบ ระบบจะทำการตรวจสอบกับเซิร์ฟเวอร์ก่อน ว่ารหัสผ่านที่ใส่มีอยู่ในเซิร์ฟเวอร์จริง จึงจะยินยอมให้ผู้ใช้เข้าสู่ระบบการตรวจสอบยืนยันตัวตนแบบซิงโครนัสโดยขึ้นอยู่กับเวลา (Time-synchronous authentication) เป็นวิธีการที่สร้างรหัสผ่านโดยมีการกำหนดช่วงระยะเวลาการใช้งาน โดยปกติแล้วรหัสผ่านจะถูกเปลี่ยนทุกๆ หนึ่งนาที การสร้างรหัสผ่านจะเป็นไปอย่างต่อเนื่อง ทำให้บางครั้งรหัสผ่านที่สร้างออกมาอาจจะซ้ำกันกับรหัสผ่านตัวอื่นที่เคยสร้างมาแล้วก็ได้ เมื่อผู้ใช้ต้องการเข้าสู่ระบบก็ใส่รหัสผ่านและเวลาที่รหัสผ่านตัวนั้นถูกสร้างขึ้นมา (รหัสผ่านจะถูกสร้างขึ้นมาจาก Token) ลงในฟอร์ม เพื่อเข้าสู่ระบบ ระบบจะทำการตรวจสอบเวลาและรหัสผ่านที่ผู้ใช้ใส่ลงไป กับเซิร์ฟเวอร์ว่ารหัสผ่านที่ใส่ตรงกับเวลาที่ Token สร้าง และมีอยู่ในเซิร์ฟเวอร์จริง จึงยินยอมให้ผู้ใช้เข้าสู่ระบบ
การตรวจสอบยืนยันตัวตนแบบอะซิงโครนัส หรือเรียกอีกอย่างหนึ่งว่า "challenge-response" ถูกพัฒนาขึ้นเป็นลำดับแรกๆ ของระบบการใช้ "รหัสผ่านซึ่งเปลี่ยนแปลงได้" ซึ่งถือได้ว่าเป็นการป้องกันการจู่โจมที่ปลอดภัยที่สุด เพราะเนื่องจากว่าเมื่อผู้ใช้ต้องการจะเข้าสู่ระบบ ผู้ใช้จะต้องทำการร้องของไปยังเซิร์ฟเวอร์ จากนั้นเซิร์ฟเวอร์ก็จะส่ง challenge string มาให้ผู้ใช้ เพื่อให้ผู้ใช้ใส่ลงใน Token ที่ผู้ใช้ถืออยู่ จากนั้น Token จะทำการคำนวณรหัสผ่านออกมาให้ผู้ใช้ ผู้ใช้จึงสามารถนำรหัสผ่านนั้นใส่ลงในฟอร์มเพื่อเข้าสู่ระบบได้ การตรวจสอบยืนยันตัวตนแบบซิงโครนัสทั้งไคลเอ็นต์และเซิร์ฟเวอร์จะมีรหัสผ่านเก็บเอาไว้ แต่แบบอะซิงโครนัส ไคลเอ็นต์จะต้องติดต่อเซิร์ฟเวอร์ก่อน ก่อนจะได้รับรหัสผ่านจริง ทำให้การตรวจสอบยืนยันตัวตนแบบอะซิงโครนัสมีขั้นตอนที่ซับซ้อนกว่าแบบซิงโคนัส

รูปที่ 2-1 ตัวอย่างของฮาร์ดแวร์พิเศษที่ใช้ในการสร้างรหัสผ่านซึ่งเปลี่ยนแปลงได้ ของการตรวจสอบยืนยันตัวตนโดยใช้ Password authenticator หรือ token [15]

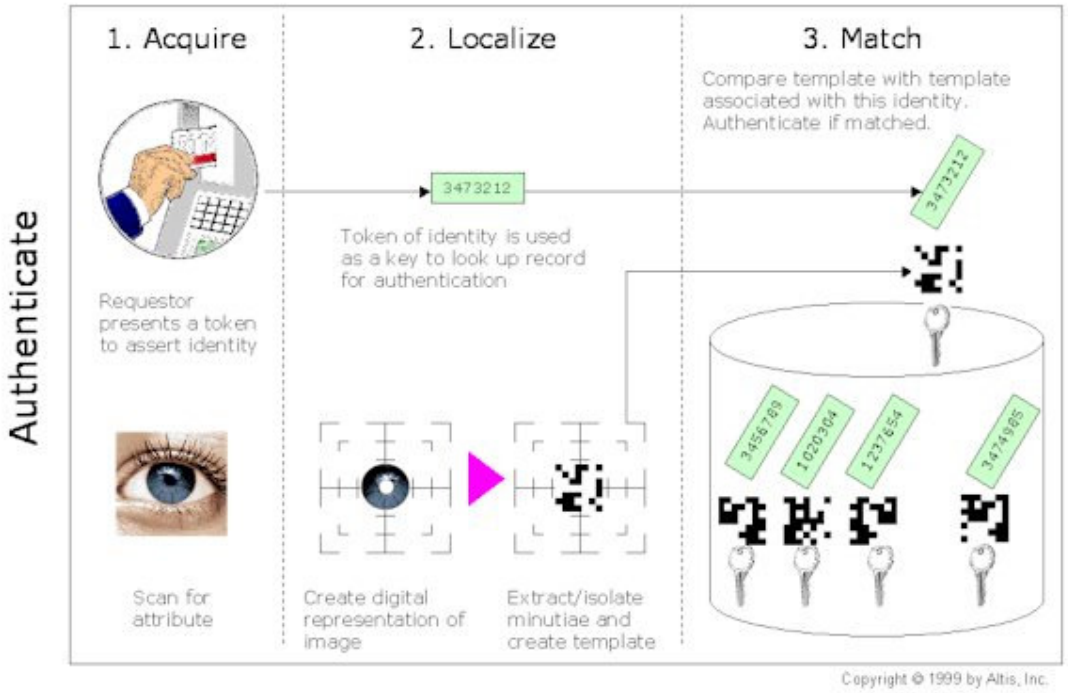
2.2.4 การตรวจสอบยืนยันตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล

ลักษณะทางชีวภาพของแต่ละบุคคลเป็นลักษณะเฉพาะและลอกเลียนแบบกันไม่ได้ การนำมาใช้ในการตรวจสอบยืนยันตัวตนจะเพิ่มความน่าเชื่อถือได้มากขึ้นเช่นการใช้ลายนิ้วมือ เสียง ม่านตา เป็นต้น จึงมีการนำเทคโนโลยีนี้มาช่วยในการตรวจสอบยืนยันตัวตน เพื่อเพิ่มความปลอดภัยก่อนเข้าสู่ระบบ เช่นการใช้ควบคู่กับการใช้รหัสผ่าน token การ์ด หรือสมาร์ทการ์ด



รูปที่ 2-2 ขั้นตอนของการเก็บหลักฐานทางชีวภาพ [16]

ในขั้นตอนของการเก็บหลักฐานทางชีวภาพ จากตัวอย่างของรูปที่ 2-2 ในขั้นแรกระบบจะทำการเก็บภาพของเรตินาจากบุคคลที่ถือ token การ์ดหรือสมาร์ทการ์ด จากนั้นจะนำภาพเรตินาที่ได้มาแยกแยะเพื่อหาลักษณะเด่นของแต่ละบุคคลเพื่อไม่ให้ซ้ำกับบุคคลอื่น แล้วเก็บไว้เป็น template ซึ่ง template ที่ได้จะถูกบันทึกเป็นกุญแจคู่กับรหัสผ่านที่มีอยู่ใน token การ์ด หรือสมาร์ทการ์ดของแต่ละบุคคล



รูปที่ 2-3 ขั้นตอนของการตรวจสอบหลักฐานทางชีวภาพ [16]

ในขั้นตอนของการตรวจสอบหลักฐาน ผู้ใช้ที่ถือ Token การ์ด หรือสมาร์ทการ์ด จะนำบัตรมาผ่านเครื่องอ่านบัตรและแสดงเรตินาให้เครื่องเก็บภาพ เมื่อเครื่องอ่านบัตร อ่านค่าเลขที่ได้จากบัตรแล้ว ก็จะนำไปหากุญแจ ซึ่งในขณะเดียวกันภาพเรตินาที่เครื่องเก็บไว้ได้ ก็จะนำไปแยกแยะเพื่อหาลักษณะเด่น แล้วเก็บค่าไว้เป็น template และนำ template ที่ได้ไปตรวจสอบกับ template ที่เก็บไว้เพื่อหากุญแจ และนำกุญแจที่ได้มาเปรียบเทียบกันว่าตรงกันหรือไม่ ถ้าตรงกันก็แสดงว่าผู้ที่ถือบัตรกับผู้ใช้เป็นคนเดียวกัน จึงอนุญาตให้เข้าสู่ระบบได้

ตัวอย่างการใช้งานของลายม่านตาเป็นดังนี้ นายดำจะเข้าไปในห้องพิเศษขององค์กรหนึ่ง ซึ่งต้องห้ามสำหรับบุคคลที่ ไม่เกี่ยวข้องที่ประตูห้องจะมีอุปกรณ์คล้ายเครื่องตรวจวัดสายตาเหมือนร้านแว่นตา นายดำต้องมายืนที่จุดกำหนดแล้วยื่นหน้าเข้าไปอยู่ในตำแหน่งพอเหมาะติดกับอุปกรณ์คล้ายกล้องส่องตา สักครู่นายดำก้าวถอยหลังออกมาอีกเพียง 5 วินาทีมีไฟเขียวสว่างขึ้นที่เครื่อง ตัวอักษรจะปรากฏชื่อนายดำให้เห็น แล้วประตูจะเลื่อนเปิดออก เมื่อนายดำเดินผ่านประตู เข้าไปประตูจะเลื่อนปิด การตรวจสอบลายม่านตาของบุคคลต่าง ๆ เป็นเทคโนโลยีใหม่ที่พัฒนาขึ้นมาโดยคณะนักวิทยาศาสตร์ที่ห้องปฏิบัติการแห่งชาติลอสอลา มอส (Los Alamos National Laboratory) ในประเทศสหรัฐอเมริกามี โรเจอร์ จอห์นสตัน (Roger Johnston) และ เคลวิน เกรช (Kevin Grace) ร่วมทีมอยู่ด้วย เทคโนโลยีการตรวจสอบบุคลลากรโดยอาศัย

ลาย ม่านตาระบบแรกที่ใช้งานได้จริง มีชื่อเรียกว่า BATAS ประกอบด้วยอุปกรณ์สำคัญคือ กล้องวีดีทัศน์ที่มีกำลังขยายสูงสามารถตรวจ จับลักษณะของลายม่านตาได้อย่างละเอียดแล้วส่งข้อมูลเกี่ยวกับลายม่านตาให้ไมโครคอมพิวเตอร์วิเคราะห์ เก็บเป็นรหัสทางคณิตศาสตร์ เป็นรหัส ลายม่านตาของแต่ละคนเอาไว้ในคลังลายม่านตา (ลักษณะคล้ายแฟ้มลายนิ้วมือ หรือแฟ้มดีเอ็นเอของตำรวจ) ในทางปฏิบัติการใช้ลายม่านตา มีขั้นตอนคล้ายฉากสมมติเกี่ยวกับนายดำคือผู้ที่ ถูกตรวจสอบต้องให้ระบบเป็นกล้องวิดิทัศน์อ่านลายม่านตาโดยใช้คอมพิวเตอร์วิเคราะห์ออกมาเป็นรหัสลายม่านตา แล้วระบบก็จะเปรียบเทียบกับรหัสลายม่านตาของเจ้าตัว ในคลังลายม่านตานั่นเอง การตรวจสอบยืนยันหลักฐานโดยลายม่านตาเป็นวิธีที่ดีกว่าลายนิ้วมือคือปลอมแปลงไม่ได้เพราะลายนิ้วมือสามารถปลอมแปลงได้ และยังดีกว่าดีเอนเอคือวิธีการตรวจสอบง่ายกว่าและสามารถตรวจสอบได้ทันที ปัจจุบันเทคโนโลยีการใช้ลายม่านตายังอยู่ในระยะแรก ๆ ของการพัฒนาความแม่นยำจากการทดสอบ แต่ก็ปรากฏว่าแม่นยำถึง 96-98% นับว่าสูงมาก และนักวิทยาศาสตร์ก็ยังมีการปรับปรุงวิธีการนี้อยู่ตลอดเพื่อให้ได้ประสิทธิภาพการทดสอบที่สูงกว่านี้ เพราะฉะนั้นในอนาคตอันใกล้การตรวจสอบบุคคลากรในวงการต่าง ๆ คงจะใช้เทคโนโลยีใหม่โดยการตรวจลายม่านตาเข้ามาแทนหรือเสริมลายนิ้วมือและลายดีเอ็นเอ

2.2.5 การตรวจสอบยืนยันตัวตนโดยใช้รหัสผ่านที่ใช้เพียงครั้งเดียว

รหัสผ่านที่ใช้เพียงครั้งเดียว (One-Time Password) ถูกพัฒนาขึ้นเพื่อหลีกเลี่ยงปัญหาที่เกิดจากการใช้รหัสผ่านเพียงตัวเดียวซ้ำๆกัน OTP จะทำให้ระบบมีความปลอดภัยมากขึ้น เพราะรหัสผ่านจะถูกเปลี่ยนทุกครั้งก่อนที่ผู้ใช้จะเข้าสู่ระบบ การทำงานของ OTP คือเมื่อผู้ใช้ต้องการจะเข้าใช้ระบบ ผู้ใช้จะทำการร้องขอไปยังเซิร์ฟเวอร์ จากนั้นเซิร์ฟเวอร์จะส่ง challenge string กลับมาให้ผู้ใช้ จากนั้นผู้ใช้จะนำ challenge string และรหัสลับที่มีอยู่กับตัวของผู้ใช้นำไปเข้าแฮชฟังก์ชันแล้วออกมาเป็นค่า response ผู้ใช้ก็จะส่งค่านั้นกลับไปยังเซิร์ฟเวอร์ เซิร์ฟเวอร์จะทำการตรวจสอบค่าที่ผู้ใช้ส่งมาเปรียบเทียบกับค่าที่เซิร์ฟเวอร์เองคำนวณได้ โดยเซิร์ฟเวอร์ก็ใช้วิธีการคำนวณเดียวกันกับผู้ใช้ เมื่อได้ค่าที่ตรงกันเซิร์ฟเวอร์ก็จะยอมรับให้ผู้ใช้เข้าสู่ระบบ

2.2.6 การตรวจสอบยืนยันตัวตนโดยการเข้ารหัสโดยใช้กุญแจสาธารณะ

เป็นการรักษาความปลอดภัยของข้อมูลระหว่างการส่งข้ามเครือข่ายวิธีหนึ่งที่นิยมใช้กันอยู่ในปัจจุบัน การเข้ารหัสแบบคู่รหัสกุญแจนี้จะมีความปลอดภัยมากกว่าการเข้ารหัสข้อมูลแบบธรรมดา แต่ก็

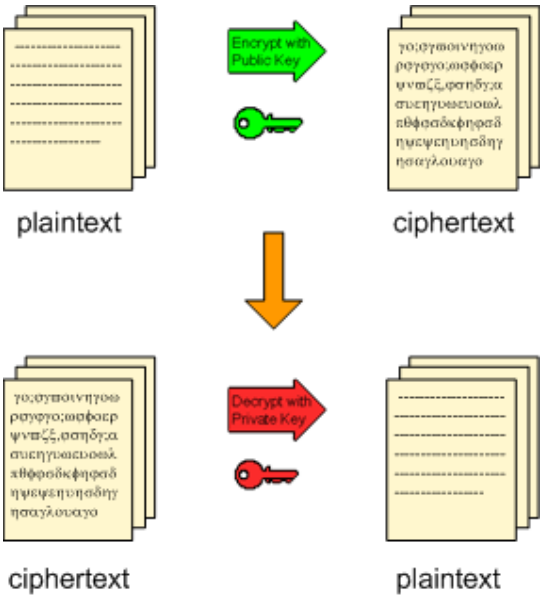
ไม่ได้หมายความว่าการเข้ารหัสแบบคู่รหัสกุญแจนี้จะเป็นวิธีที่เหมาะสมที่สุดของวิธีการเข้ารหัส ทั้งนี้ขึ้นอยู่กับประเภทงานของแต่ละองค์กรหรือบุคคล การเข้ารหัสโดยใช้กุญแจสาธารณะ ประกอบไปด้วยกุญแจ 2 ชนิด ที่ต้องใช้คู่กันเสมอในการเข้ารหัสและถอดรหัสคือ

- กุญแจสาธารณะ (public key) เป็นกุญแจที่ผู้สร้างจะส่งออกไปให้ผู้ใช้อื่นๆ ทราบหรือเปิดเผยได้
- กุญแจส่วนตัว (private key) เป็นกุญแจที่ผู้สร้างจะเก็บไว้ โดยไม่เปิดเผยให้คนอื่นรู้

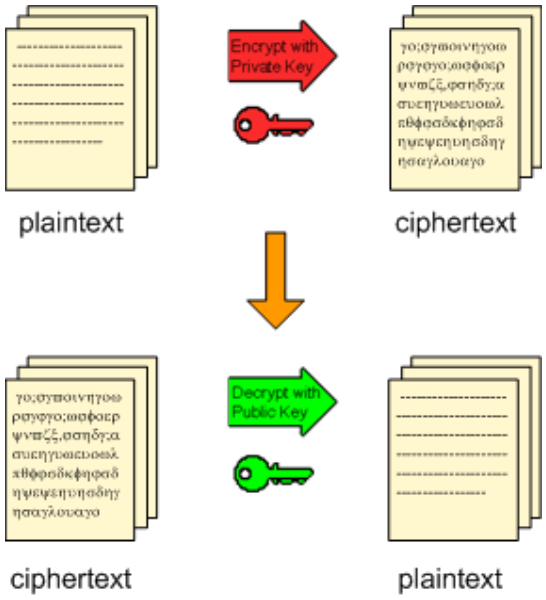
กระบวนการของการเข้ารหัสแบบคู่รหัสกุญแจ มีดังนี้

1. ผู้ใช้แต่ละคนจะสร้างคู่รหัสกุญแจของตัวเองขึ้นมา เพื่อใช้สำหรับการเข้ารหัสและการถอดรหัส
2. กุญแจสาธารณะจะถูกส่งออกไปยังผู้ใช้คนอื่นๆ แต่กุญแจส่วนตัวจะถูกเก็บที่ตนเอง
3. เมื่อจะส่งข้อมูลออกไปหาผู้ใช้คนใด ข้อมูลที่ส่งจะถูกเข้ารหัสด้วยกุญแจสาธารณะ ก่อนถูกส่งออกไป
4. เมื่อผู้รับได้รับข้อความแล้วจะใช้กุญแจส่วนตัวซึ่งเป็นคู่รหัสกันถอดรหัสออกมา

การเข้ารหัสโดยใช้กุญแจสาธารณะสามารถใช้ได้ทั้งในการเข้ารหัส (Encryption) และการตรวจสอบยืนยันตัวตน (Authentication) การประยุกต์ใช้ในการเข้ารหัสข้อมูล (Encryption) เป็นการนำข้อมูลที่จะส่งไปยังผู้รับมาเข้ารหัสด้วยกุญแจสาธารณะของผู้รับ และเมื่อผู้รับได้รับข้อความนั้นแล้วจะถอดรหัสออกมาด้วยกุญแจส่วนตัว จึงจะเห็นได้ว่ามีเพียงผู้รับเท่านั้นที่จะสามารถถอดรหัสออกมาได้



รูปที่ 2-4 ระบบของการเข้ารหัสแบบใช้คู่รหัสกุญแจ [15]



รูปที่ 2-5 ระบบของการเข้ารหัสแบบใช้คู่รหัสกุญแจเพื่อการตรวจสอบยืนยันตัวตน [15]

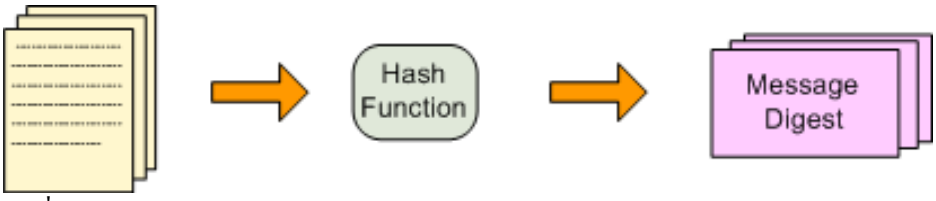
จากรูปที่ 2-4 และรูปที่ 2-5 การประยุกต์ใช้ในการตรวจสอบยืนยันตัวตน (Authentication) เป็นการนำข้อมูลที่ผู้ส่งต้องการส่งมาเข้ารหัสด้วยกุญแจส่วนตัวของผู้ส่ง แล้วนำข้อมูลนั้นส่งไปยังผู้รับ ซึ่งผู้รับจะใช้กุญแจสาธารณะซึ่งเป็นคู่รหัสกันถอดรหัสออกมา ผู้รับก็สามารถรู้ได้ว่าข้อความนั้นถูกส่งมาจากผู้ส่งคนนั้นจริง ถ้าสามารถถอดรหัสข้อมูลได้อย่างถูกต้อง

2.2.7 การตรวจสอบยืนยันตัวตนโดยการใช้ลายเซ็นอิเล็กทรอนิคส์ (Digital Signature)

เป็นการนำหลักการของการทำงานของระบบการเข้ารหัสแบบใช้คู่รหัสกุญแจเพื่อการตรวจสอบยืนยันตัวตนมาประยุกต์ใช้ ลายเซ็นนี้ไม่ใช่ลายเซ็นมือแต่อย่างใดเพียงแต่มีลักษณะจำเพาะของการเข้ารหัสและถอดรหัสตามแต่ผู้เป็นตัวตนกำหนดไว้ จึงเสมือนมีการเซ็นยืนยัน แต่ไม่เกี่ยวข้องกับการใช้ลายเซ็นมือที่ทางโครงการวิจัยนี้ศึกษา

ระบบของลายเซ็นดิจิตอลสามารถแบ่งเป็นขั้นตอนได้ดังนี้

1. เมื่อผู้ใช้ต้องการจะส่งข้อมูลไปยังผู้รับ ข้อมูลนั้นจะถูกนำไปเข้าฟังก์ชั่นทางคณิตศาสตร์ที่เรียกว่า "แฮชฟังก์ชัน" ได้เมสเซสไดเจสต์ (Message Digest) ออกมา

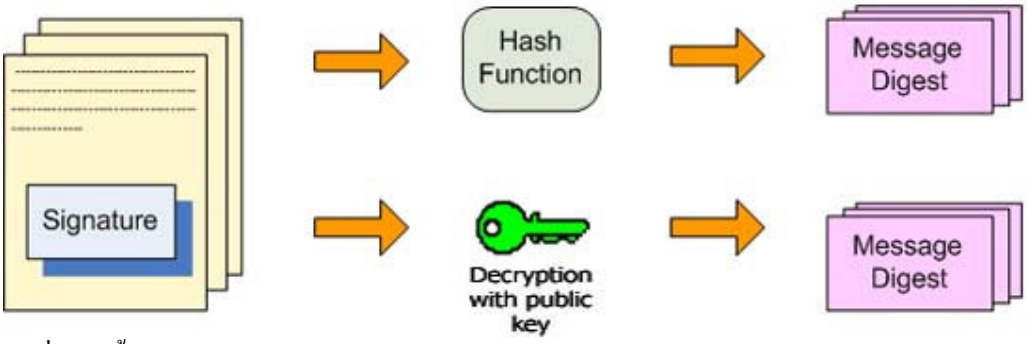


รูปที่ 2-6 การส่งข้อมูลเข้าไปใน Hash function [15]

2. การใช้กุญแจส่วนตัวเข้ารหัสข้อมูล หมายถึงว่าผู้ส่งได้ลงลายเซ็นดิจิตอล ยินยอมที่จะให้ผู้รับ สามารถทำการตรวจสอบด้วยกุญแจสาธารณะของผู้ส่งเพื่อตรวจสอบยืนยันตัวตนของผู้ส่งได้

รูปที่ 2-7 การเข้ารหัสเมสเซสไดเจสต์ด้วยกุญแจส่วนตัวเพื่อเป็นการลงลายเซ็น [15]

3. การตรวจสอบข้อมูลว่าถูกส่งมาจากผู้ส่งคนนั้นจริงในด้านผู้รับ โดยการนำข้อมูลมาผ่านแฮชฟังก์ชันเพื่อคำนวณหาค่าเมสเซจไดเจสต์ และถอดรหัสลายเซ็นอิเล็กทรอนิคส์ด้วยกุญแจสาธารณะของผู้ส่ง ถ้าสามารถถอดได้อย่างถูกต้อง จะเป็นการยืนยันข้อมูลจากผู้ส่งคนนั้นจริง และถ้าข้อมูลเมสเซจไดเจสต์ที่ได้จากการถอดรหัสเท่ากันกับค่าเมสเซจไดเจสต์ในตอนต้นที่ทำการคำนวณได้ จะถือว่าข้อมูลดังกล่าวนั้นถูกต้อง



รูปที่ 2-8 ขั้นตอนการเปรียบเทียบความถูกต้อง [15]

2.2.8 การตรวจสอบยืนยันตัวตนโดยใช้การถาม - ตอบ

เป็นวิธีการตรวจสอบยืนยันตัวตนโดยใช้การถาม - ตอบ เมื่อผู้ใช้เข้ามาในระบบแล้ว ระบบจะแน่ใจได้อย่างไรว่าผู้ใช้คนนั้น เป็นคนที่ได้รับอนุญาตให้เข้ามาใช้ระบบได้จริง การใช้ชื่อผู้ใช้และรหัสผ่าน ในปัจจุบันนี้ไม่มีความปลอดภัยเพียงพอต่อการเข้าใช้ระบบ เนื่องจากความรู้และวิทยาการที่ก้าวหน้า ทำให้เกิดผู้ที่ต้องการจะเข้ามาละเมิดระบบต่างๆมีมากขึ้น ทำให้ชื่อผู้ใช้และรหัสผ่าน อาจจะถูกลักลอบดักข้อมูลระหว่างการสื่อสารกันได้

การที่จะทำให้ระบบมั่นใจได้ว่า ผู้ที่เข้าไปในระบบผู้นั้นเป็นผู้ที่ได้รับอนุญาตจริง นั่นก็คือ ระบบจะใช้การถาม - ตอบ ซึ่งคำถามและคำตอบเหล่านี้ ผู้ใช้จะเป็นคนสร้างคำถามและคำตอบขึ้นมาเอง จากนั้นจะส่งให้กับเซิร์ฟเวอร์ ซึ่งคำถาม - คำตอบที่ผู้ใช้สร้างขึ้นมา ผู้ใช้เท่านั้นจะเป็นคนที่ทราบคำตอบของแต่ละคำถามที่ถูกสร้าง และเมื่อผู้ใช้คนนั้นๆเข้าสู่ระบบได้ ระบบจะถามสุ่มคำถามเหล่านั้นที่ผู้ใช้คนนั้นๆ สร้างขึ้นมา ถามผู้ใช้คนนั้นๆก่อนที่จะยอมให้เข้าใช้ระบบได้จริง การให้ใช้ระบบได้จริงจะได้รับการยินยอมก็ต่อเมื่อการตอบคำตอบที่ผู้ใช้ตอบ นั้นสัมพันธ์กับคำตอบที่มีอยู่ในเซิร์ฟเวอร์ ยกตัวอย่างเช่น นาย ก. กับ นาย ข. รู้จักกันมานานละสนิทกัน นาย ก. และ นาย ข. ย่อมมีความสนิทกันเป็นส่วนตัวเมื่อนาย ก. และนาย ข. เล่น MSN กัน ต่างฝ่ายต่างจะแน่ใจได้อย่างไรว่า คนที่ตนคุยอยู่เป็นบุคคลเดียวกันกับที่ตนรู้จัก เพราะว่านาย ก. หรือ นาย ข. อาจจะทำการเข้าระบบทิ้งไว้ หรือ อาจจะมีบุคคลอื่นสามารถดักจับหลักฐานและข้อมูลที่สามารถเข้าสู่ระบบของคนใดคนหนึ่งไว้ได้ แล้วทำการสวมรอยแทน นั่นก็คือการใช้คำถามและคำตอบที่มีเพียงนาย ก. และ นาย ข. เท่านั้นที่ทราบ

วิธีการตรวจสอบยืนยันตัวตนวิธีนี้ เป็นวิธีการที่ต้องใช้ความรู้ขั้นสูงในการนำมาใช้ เนื่องจากระบบจะใช้การเรียนรู้จากข้อมูลที่ได้รับ อาจจะเรียกระบบนี้ได้ว่าเป็นการนำความรู้ด้าน AI (Artificial Intelligence) มาใช้นั่นเอง

2.2.9 การตรวจสอบยืนยันตัวตนโดยการใช้ลายเซ็นมืออิเล็กทรอนิคส์ (Digital Handwriting Signature)

เป็นวิธีการตรวจสอบยืนยันตัวตนโดยใช้ลายเซ็นมือจริงของเจ้าของ ซึ่งเป็นลายเซ็นที่ปกติจะใช้อยู่เป็นประจำในการทำธุรกรรมต่างๆ เพื่อยืนยันความเป็นตัวตนไม่ว่าจะเป็นการเซ็นบนเอกสารสำคัญ การเซ็นเพื่อถอนเงินจากบัญชีธนาคารก็ตาม สำหรับคำว่าอิเล็กทรอนิกส์นั้นหมายถึงการแปลงรูปแบบการเซ็นของลายเซ็นมือให้อยู่ในรูปแบบที่สามารถเก็บค่าเพื่อบันทึกในคอมพิวเตอร์ได้ ซึ่งในปัจจุบันนี้มีอุปกรณ์มากมายที่รองรับการแปลงค่าลายเซ็นนี้ เช่น Mouse pad หรืออุปกรณ์มือถือ PDA ที่สามารถเขียนและบันทึกลายเซ็นได้ สำหรับวิธีการตรวจสอบจะอาศัยฐานข้อมูลลายเซ็นมือที่เคยบันทึกไว้ที่ server เพื่อทำหน้าที่เปรียบเทียบลายเซ็นที่ต้องการตรวจสอบ ซึ่งมีเทคนิคมากมายในการตรวจสอบ สำหรับ

โครงการวิจัยนี้จะกล่าวถึงเพียงเทคนิคเปรียบเทียบในหัวข้อที่ 2.3 และเทคนิคการแปลงเชิงมุมในหัวข้อ 2.4 ซึ่งเป็นเทคนิคที่เสนอใหม่จากโครงการวิจัยนี้

2.2.10 ตารางเปรียบเทียบข้อดีข้อเสียของการตรวจสอบยืนยันตัวตนแต่ละชนิด

ารตรวจสอบยืนยันตัวตน	ข้อดี	ข้อเสีย
ไม่มีการตรวจสอบยืนยันตัวตนตน	ง่ายต่อการใช้งานและค่าใช้จ่ายต่ำ	ความปลอดภัยของข้อมูลจะขึ้นอยู่กับผู้ใช้ว่าจะนำข้อมูลเหล่านั้นไปใช้ในทางที่ควรหรือไม่
การตรวจสอบยืนยันตัวตนโดยใช้รหัสผ่าน	สามารถใช้ได้กับทุกระบบ	จะไม่ปลอดภัยเมื่อมีการส่งข้ามระบบเครือข่ายที่เป็นสาธารณะหรือไม่มีการเข้ารหัสข้อมูล
การตรวจสอบยืนยันตัวตนโดยใช้ PIN	- ง่ายต่อการจำและความปลอดภัยค่อนข้างดี (บัตร ATM) - สามารถสื่อสารข้ามเครือข่ายสาธารณะได้อย่างปลอดภัย	- ต้องใช้ฮาร์ดแวร์เฉพาะในการอ่าน PIN - ไม่สามารถใช้กับต่างระบบกันได้ - ราคาแพง
การตรวจสอบยืนยันตัวตนโดยใช้ password authenticators หรือ tokens แบบซิงโครนัส	- มีความปลอดภัยมากกว่าการใช้การจำรหัสผ่านแบบธรรมดา - ไม่ต้องใช้เครื่องอ่านการ์ด - ผู้ที่ละเมิดเข้ามาไม่สามารถจะเข้ามาจู่โจมได้	- การใช้งานยุ่งยากกว่าแบบจำรหัสผ่าน - authenticator เป็นวัตถุจึงง่ายต่อการสูญหายและการถูกขโมยได้
การตรวจสอบยืนยันตัวตนตนโดยใช้ password authenticators หรือ tokens แบบอะซิงโครนัส	- มีความปลอดภัยมากกว่าการใช้การจำรหัสผ่าน แบบธรรมดา - ไม่ต้องใช้เครื่องอ่านการ์ด - เป็นวิธีการป้องกันที่ดีที่สุดเมื่อเปรียบเทียบกับ วิธีการใช้การตรวจสอบยืนยันตัวตนโดยใช้ password authenticators หรือ tokens	- การใช้งานยุ่งยากกว่าแบบจำรหัสผ่าน - authenticator เป็นวัตถุจึงง่ายต่อการสูญหาย และการถูกขโมยได้ ไม่สามารถป้องกันผู้ที่ละเมิดเข้ามาในระบบได้ - การใช้งานค่อนข้างยุ่งยากกว่า

		วิธีการใช้ "รหัสผ่านซึ่งเปลี่ยนแปลงได้ (dynamic password)" วิธีอื่นๆ
การตรวจสอบยืนยันตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล	มีความปลอดภัยสูงเพราะเลียนแบบกันได้ยาก	- ระบบมีความซับซ้อนสูง - ยังไม่ได้รับความนิยมกันอย่างแพร่หลาย - ค่าใช้จ่ายสูง
การตรวจสอบยืนยันตัวตนโดยวิธี One-Time Password	ทำให้การเดาหรือขโมยรหัสผ่านเป็นไปได้ยาก	- ไม่สะดวกต่อการใช้งาน เพราะผู้ใช้ต้องจำรหัสผ่านหลายตัว - ถ้าผู้ใช้จำรหัสผ่านไม่ได้ หรือ ทำรหัสผ่านสูญหาย ก็ไม่สามารถเข้าใช้ระบบได้
การตรวจสอบยืนยันตัวตนโดยการเข้ารหัสแบบคู่รหัสกุญแจ	- การจัดการกุญแจทำได้ปลอดภัย เพราะ ใช้กุญแจในการเข้ารหัส และถอดรหัสต่างกัน - สามารถระบุผู้ใช้โดยการใช้ร่วมกับลายมือชื่อ อิเล็กทรอนิกส์	- ใช้เวลาในการเข้าและถอดรหัสค่อนข้างนาน เพราะต้องใช้การคำนวณอย่างมาก - ต้องใช้ระบบที่สนับสนุนการทำงาน
การตรวจสอบยืนยันตัวตนโดยการใช้ลายเซ็นดิจิตอล	- สามารถระบุตัวผู้ส่งได้ชัดเจน - ป้องกันข้อมูลถูกแก้ไขระหว่างการส่งได้ หรือสามารถตรวจสอบข้อมูลได้ว่าผ่านการแก้ไขมาหรือไม่	ใช้เวลาในการเข้าและถอดรหัสค่อนข้างนาน เพราะต้องใช้การคำนวณอย่างมาก
การตรวจสอบยืนยันตัวตนโดยวิธี zero-knowledge proofs	ความปลอดภัยค่อนข้างสูง เพราะคำถามและคำตอบจะมีเพียงผู้ใช้ และเซิร์ฟเวอร์เท่านั้นที่ทราบ	ความซับซ้อนของระบบเพิ่มขึ้นตามความฉลาดของระบบ
การตรวจสอบยืนยันตัวตนโดยการใช้ลายเซ็นมืออิเล็กทรอนิกส์	- สามารถระบุตัวผู้ส่งได้ชัดเจน - ป้องกันการปลอมแปลงจากการขโมยระหว่างการส่งข้อมูลได้	ต้องการความซับซ้อนในการประมวลผล

2.3 การตรวจสอบยืนยันลานเซ็นมือด้วยวิธีเปรียบเทียบ

จากวิธีการตรวจสอบยืนยันที่กล่าวถึงในหัวข้อ 2.2 นั้นโครงการวิจัยนี้สนใจการใช้ลายเซ็นมืออิเล็กทรอนิกส์เพื่อบ่งบอกถึงความเป็นตัวตนผ่านเครือข่ายอินเตอร์เน็ต เทคนิคหนึ่งที่ใช้ในการตรวจสอบลายเซ็นมือคือวิธีการเปรียบเทียบ โดยที่จะนำลายเซ็นมือที่ได้มาจากฐานข้อมูล ตรวจสอบลักษณะเพื่อหาค่าอ้างอิงสำหรับการยืนยันในครั้งถัดไป แนวคิดเรื่องการเปรียบเทียบมีให้เห็นมากมาย แต่สำหรับโครงการนี้มีหลักการเปรียบเทียบดังแสดงในรายละเอียดต่อไปนี้

2.3.1 หลักการเปรียบเทียบ

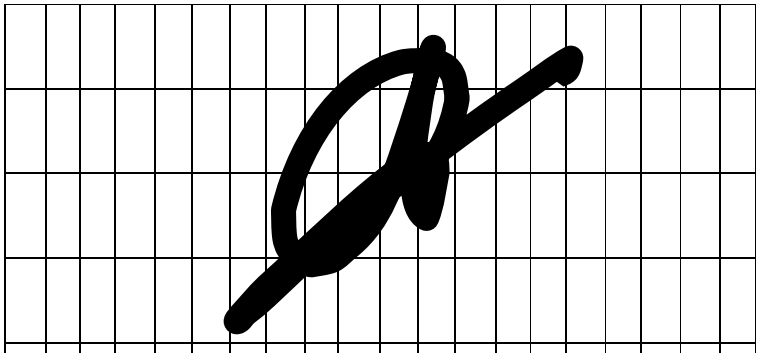
หลักการที่ใช้ในการเปรียบเทียบลายเซ็นมืออิเล็กทรอนิกส์ จะใช้หลักการเปรียบเทียบ 4 หลักการ

1 หลักการเปรียบเทียบโดยใช้วิธีการ Map

หลักการเปรียบเทียบโดยวิธีการ Map คือ เมื่อทำการเซ็นลงในพื้นที่สำหรับการเซ็นชื่อแล้วค่าที่เก็บจะเก็บค่าเป็น pixel โดยใช้ตัวแปร i กับ j เก็บค่าเป็นเหมือนค่าพิกัด แล้วทำการเปรียบเทียบว่า การเซ็นแต่ละครั้งมีรูปร่าง ลักษณะคลายกันหรือไม่

2 หลักการเปรียบเทียบโดยใช้วิธีการเก็บค่าจำนวน Dot

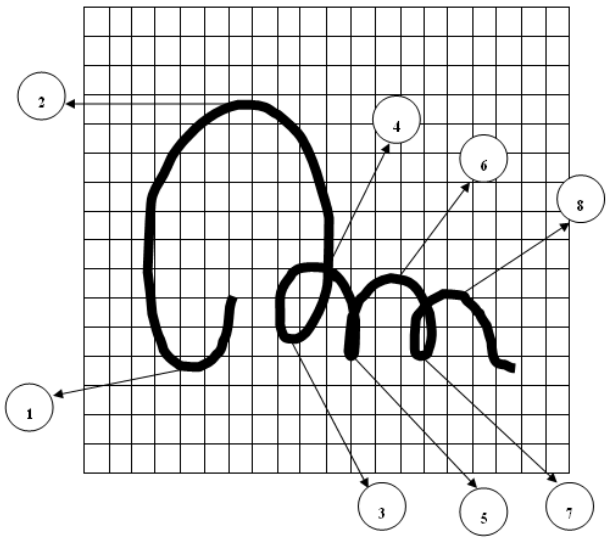
หลักการเปรียบเทียบโดยใช้วิธีการเก็บค่าจำนวน Dot มีวิธีการคือ ในขณะที่เซ็นลายเซ็นเส้นที่ลากไปนั้นจะถูกเก็บเป็นจำนวนจุด Dot ซึ่งเก็บไปเรื่อยๆ โดยไม่สนใจว่าจะไปทับกับเส้นที่ลากไว้ก่อนหรือไม่ ทำให้จำนวน Dot แสดงความยาวของลายเซ็นทั้งหมด แตกต่างจากวิธี Map ที่นับเฉพาะ pixel ที่มีการลากเส้นผ่าน ไม่ว่าจะผ่านกี่รอบก็นับแค่ pixel เดียว



รูปที่ 2-9 ตัวอย่างลายเซ็นมือและตารางเพื่อใช้เก็บค่า pixel

3 หลักการเปรียบเทียบโดยใช้วิธีการหาจุดเปลี่ยนของ Slope

มีหลักการคือจะนำลายเซ็นนั้นมาคำนวณหาความชันตามหลักการบนระนาบ x-y จากนั้นจะพบว่ามีลักษณะของการเปลี่ยนแปลงความชันจาก + ไป – หรือในทางตรงข้ามก็ตาม จะนับการเปลี่ยนแปลงนี้ว่าเป็นจุดเปลี่ยนของ Slope ซึ่งจำนวนจุดเปลี่ยนทั้งหมดจะใช้เป็นข้อมูลในการเปรียบเทียบ



รูปที่ 2-10 ตัวอย่างลายเซ็นและการเก็บค่าจุดเปลี่ยนของ Slope

4 หลักการเปรียบเทียบโดยใช้วิธีการดูค่าแรกของ Slope

มีหลักการคือ ในการเขียนลายเซ็น ค่าของ Slope แรกของลายเซ็นจะมีค่าเป็นลบหรือเป็นบวกเสมอ ซึ่งเป็นลักษณะเฉพาะที่นำมาใช้ในการพิจารณาค่าบวกหรือลบของแต่ละลายเซ็นเปรียบเทียบว่าเหมือนกันหรือไม่

โดยจากเงื่อนไขการเปรียบเทียบนี้จะได้ว่า เมื่อทำการเปรียบเทียบออกมาทั้ง 4 หลักการแล้วนั้น จะกำหนดเงื่อนไขว่าค่าที่ได้ออกมานั้นจะต้องมีค่าไม่ต่ำกว่า 90-100% ยกเว้นหลักการของการหาจุดเปลี่ยนของ Slope ค่าที่ได้ต้องอยู่ในช่วง 70-100% โดยถ้ามีค่าใดค่าหนึ่งของหลักการเมื่อเปรียบเทียบออกมาแล้วนั้นไม่ผ่านเงื่อนไขที่กำหนดก็จะไม่นำข้อมูลของบุคคลคนนั้นมาแสดงผล นอกจากนี้สุดท้ายแล้วจะนำค่าที่ได้จากการเปรียบเทียบทั้ง 4 หลักการมาหาค่าเฉลี่ยอีกครั้งก่อนนำมาแสดงผล การแสดงผลเราจะนำข้อมูลของบุคคลที่มีผลการเปรียบเทียบออกมามีค่าใกล้เคียงกับข้อมูลที่เซ็นมากที่สุด

2.4 การตรวจสอบยืนยันลานเซ็นมือด้วยวิธีการแปลงเชิงมุม

เทคนิคการแปลงเชิงมุมสำหรับตรวจสอบยืนยันลายเซ็นมือนี้เป็นเทคนิคใหม่ที่เสนอในโครงการวิจัยโดยมีรายละเอียดต่างๆ สามารถแบ่งเป็นสองกระบวนการใหญ่ๆ คือ

กระบวนการประมวลลายเซ็นด้วยการแปลงเชิงมุม

เป็นกระบวนการแปลงลายเซ็นเพื่อให้อยู่ในรูปแบบข้อมูลเชิงมุม ซึ่งมีสองขั้นตอนดังนี้ ขั้นตอนการแปลงเชิงมุมและขั้นตอนการหาค่าหน่วงเวลา

กระบวนการยืนยันลายเซ็น

เป็นกระบวนการยืนยันลายเซ็นจากกลุ่มของลายเซ็นที่บันทึกไว้ในฐานข้อมูล มีขั้นตอนหลักดังนี้ ขั้นตอนการเก็บตัวอย่าง ขั้นตอนการเลือกลายเซ็นอ้างอิง ขั้นตอนการเลือกระดับค่าหน่วงเวลา และขั้นตอนการตัดสินใจ

ซึ่งรายละเอียดของแต่ละขั้นตอนมีดังนี้

2.4.1 ขั้นตอนการแปลงเชิงมุม

โดยทั่วไปนั้นลายเซ็นมือจะถูกบันทึกและแสดงเป็นภาพ 2 มิติคือตามแกนแนวนอนและแกนแนวตั้ง สำหรับการแปลงเชิงมุมนั้นจะยุบเหลือแค่มิติเดียว คือโดเมนเชิงมุมเพียงอย่างเดียวซึ่งจะทดแทนทั้งสองแกนของการเก็บลายเซ็นแบบปกติ สำหรับวิธีการแปลงเชิงมุมนั้นก็คือการเก็บค่ามุมอย่างต่อเนื่องของลายเซ็นที่กำลังเซ็นอยู่ ตัวอย่างการแปลงเชิงมุมนั้นสามารถแสดงในรูปที่ 2-11 จากรูปจะเห็นได้ว่าเป็นการเก็บค่ามุมอย่างต่อเนื่องไปทีละตำแหน่งของลายเซ็น ซึ่งค่าเหล่านี้เมื่อนำไปแสดงเทียบกับการเก็บข้อมูลของลายเซ็นปกติจะแสดงได้ในรูปที่ 2-12 โดยในรูปที่ 2-12 คือลายเซ็นเดียวกัน แต่แยกเป็นแบบปกติสองแกนแนวนอนและแนวตั้งเทียบกับแกนเวลา และแบบเชิงมุมเทียบกับเวลา จะเห็นได้ว่าเทคนิคที่นำเสนอขึ้นมานี้จะส่งข้อมูลจากผู้ใช้ไปยังเซิฟเวอร์เพียงแค่ครึ่งหนึ่งของแบบปกติเท่านั้นเอง ซึ่งเป็นการประหยัดพื้นที่ที่ต้องส่งข้อมูลและลดโอกาสเสี่ยงในการจารกรรมมากขึ้น

จากรูปกราฟเชิงมุมที่เห็นในรูปที่ 2-12 พบว่ามีความไม่ต่อเนื่องอยู่หลายครั้งด้วยกัน ซึ่งผู้วิจัยได้ค้นพบว่าความไม่ต่อเนื่องเหล่านั้นเกิดจากสองความหมายด้วยกันคือ เป็นจุดหักมุมของลายเซ็น หรือ เป็นจุดที่ลายเซ็นลากเป็นวงกลมผ่านมุม $\pm$180 องศา สำหรับจุดหักมุมนั้นคือตำแหน่งที่เส้นของลายเซ็นจะเริ่มต้นโค้งใหม่ๆ อยู่เสมอ ทั้งสองความหมายนี้มีส่วนช่วยให้การวิเคราะห์เชิงมุมมีลักษณะที่พิเศษ คือสามารถแยก

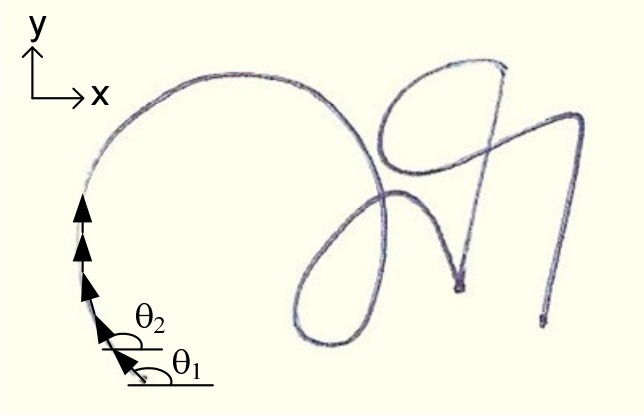
หรือแบ่งลายเซ็นออกเป็นองค์ประกอบย่อยๆ ได้ ซึ่งตัวอย่างการแบ่งลายเซ็นออกเป็นองค์ประกอบย่อย แสดงในรูปที่ 2-13 และสามารถเขียนสมการอธิบายได้ในสมการที่ (2-1)

$$S(t) = \sum_{i=1}^{M} S_i(t) \tag{2-1}$$

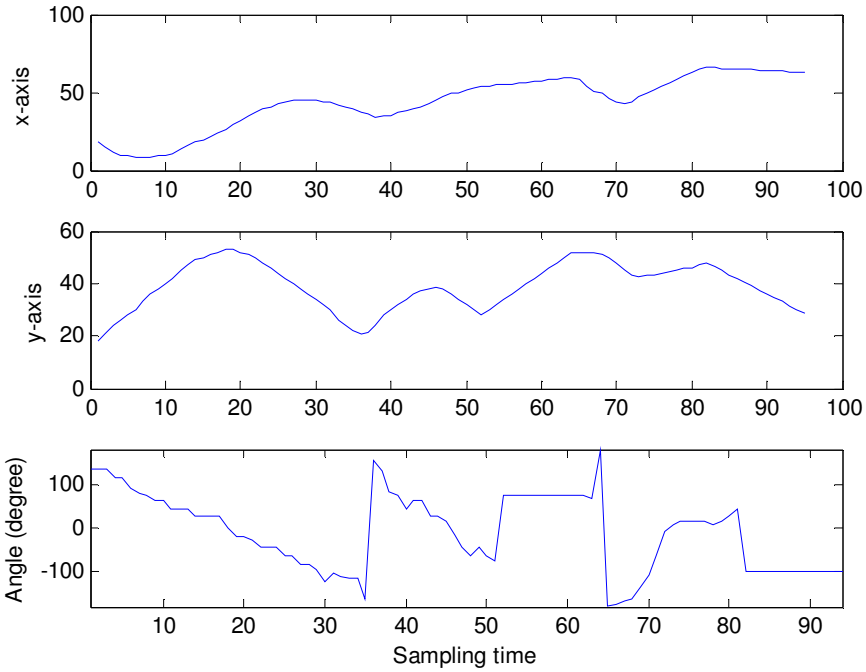
เมื่อ M คือจำนวนองค์ประกอบย่อยทั้งหมด $S(t)$ คือลายเซ็นมือที่เก็บตามเวลา และ $S_i(t)$ คือองค์ประกอบย่อยที่ i ของลายเซ็นมือ ซึ่งนิยามดังสมการที่ (2-2)

$$S_i(t) = \begin{cases} S(t) & ts_i \le t \le te_i \\ 0 & elsewhere \end{cases} \tag{2-2}$$

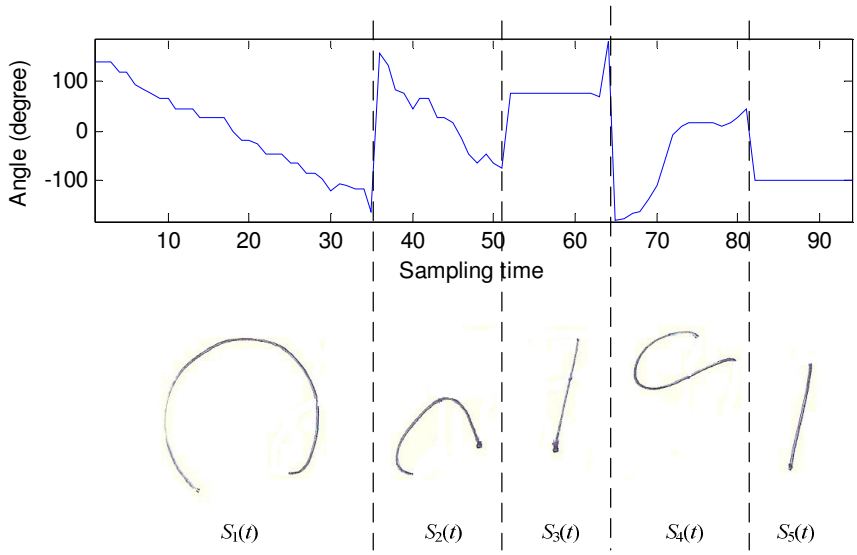
เมื่อ ts_i คือเวลาที่เริ่มต้นขององค์ประกอบที่ i ของลายเซ็นมือ และ te_i คือเวลาสิ้นสุดขององค์ประกอบที่ i ของลายเซ็นมือ



รูปที่ 2-11 ตัวอย่างการแปลงเชิงมุมของลายเซ็นมือ



รูปที่ 2-12 การแสดงข้อมูลของลายเซ็นมือในแนวแกนนอน แกนตั้ง และเชิงมุม



รูปที่ 2-13 ตัวอย่างการแบ่งลายเซ็นมือออกเป็นองค์ประกอบย่อย

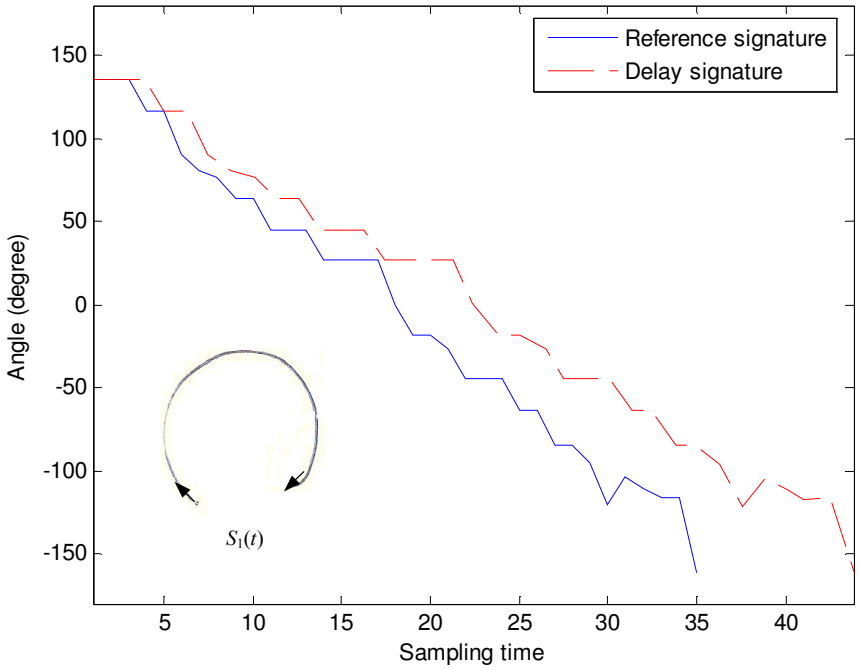
2.4.2 ขั้นตอนการหาค่าหน่วงเวลา

การแปลงเชิงมุมนั้นจะถูกทำที่ฝั่งผู้ใช้งานและถูกส่งกลับไปยังเซิฟเวอร์เพื่อใช้เปรียบเทียบกับฐานข้อมูลต่อไป โดยที่เซิฟเวอร์นั้นจะทำการแบ่งลายเซ็นมือออกเป็นองค์ประกอบย่อยตามที่อธิบายไว้ใน 2.4.1 กระบวนการต่อไปคือการประมาณค่าหน่วงเวลา และการคำนวณหาค่าความผิดพลาด สำหรับระบบออนไลน์นั้น เวลาที่ใช้ในการเซ็นย่อมมีผลกับการพิจารณายืนยันตัวตนของผู้ใช้งาน ซึ่งตรงนี้เองที่แตกต่างจากแบบไม่ออนไลน์ เพราะแบบไม่ออนไลน์จะใช้เวลานานแค่ไหนก็ได้ ทำให้การปลอมแปลงลายเซ็นมือสำหรับระบบออนไลน์ยากขึ้น และระบบออนไลน์มีความน่าเชื่อถือมากขึ้น ในงานวิจัยนี้ใช้การประมาณแบบเชิงเส้นสำหรับการประมาณค่าหน่วงเวลา

รูปที่ 2-14 แสดงองค์ประกอบย่อยลำดับแรกของลายเซ็นมือที่แสดงในรูปที่ 2-13 โดยเปรียบเทียบระหว่างลายเซ็นมือทดสอบและลายเซ็นมืออ้างอิง สำหรับลายเซ็นมืออ้างอิงนั้นถือว่าสำคัญมากเพราะจะใช้เป็นตัวแทนในการอ้างอิงสำหรับการยืนยันตัวตนของผู้ใช้งาน โดยวิธีการเลือกลายเซ็นอ้างอิงนั้นจะถูกอธิบายไว้ในหัวข้อถัดไป จากรูปพบว่าองค์ประกอบทั้งสองมีลักษณะที่ใกล้เคียงกัน แต่มีการกระจายของช่วงเวลาที่แตกต่างกัน ดังนั้นค่าหน่วงเวลาที่เลื่อนไปจากค่าอ้างอิง d_i ขององค์ประกอบย่อยที่ i สามารถกำหนดได้ดังนี้

$$S_i^d(t) = S_i^r(d_i t) \tag{2-3}$$

เมื่อ $S_i^r(d_i t)$ คือองค์ประกอบย่อยของลายเซ็นอ้างอิง และ $S_i^d(t)$ คือองค์ประกอบย่อยของสัญญาณทดสอบที่มีค่าหน่วงเวลา



รูปที่ 2-14 การเปรียบเทียบระหว่างองค์ประกอบย่อยลำดับแรกของลายเซ็นมือทดสอบและลายเซ็นอ้างอิง

เพื่อให้เห็นถึงความสัมพันธ์ของลายเซ็นอ้างอิงและลายเซ็นที่มีค่าหน่วงเวลา งานวิจัยนี้ได้นำลักษณะองค์ประกอบย่อยของลายเซ็นทั้งสองมาใหม่วาดบนสองแกนเวลา โดยแกนเวลาแรกใช้ค่าจากลายเซ็นอ้างอิง และแกนเวลาที่สองใช้ค่าตามลายเซ็นที่ต้องการประมาณค่าหน่วงเวลา ในรูปที่ 2-15 แสดงองค์ประกอบย่อยลำดับแรกที่แสดงในรูปที่ 2-14 จะเห็นได้ว่า ค่าความชันของรูปที่ 2-15 สามารถประมาณได้เป็นค่าความหน่วงเวลาที่เลื่อนไปจากลายเซ็นอ้างอิง d_i โดยการประมาณแบบเชิงเส้นตามสมการที่ 2-4

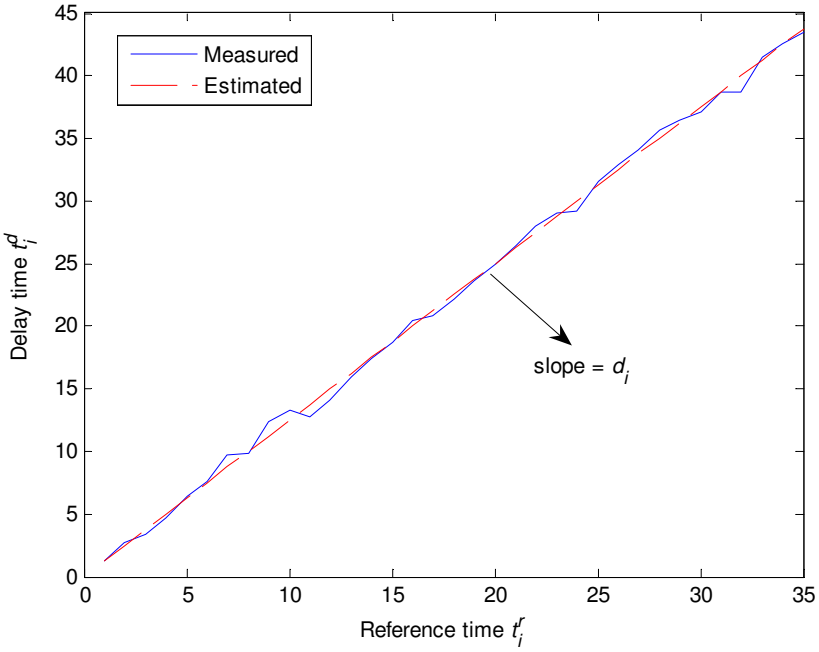
$$d_i = \min_{d_i}\left\{\sum_{t_i^r}\left|t_i^d - d_i t_i^r\right|^2\right\} \tag{2-4}$$

หลังจากการประมาณค่าหน่วงเวลาที่เลื่อนไปจากค่าอ้างอิงแล้ว ในตอนนี้ก็จะสามารถนำค่าหน่วงเวลานี้กลับไปชดเชยลายเซ็นทดสอบเพื่อประมาณให้เป็นค่าลายเซ็นที่ใช้เวลาเท่ากับลายเซ็นอ้างอิงได้ตามสมการที่ 2-5

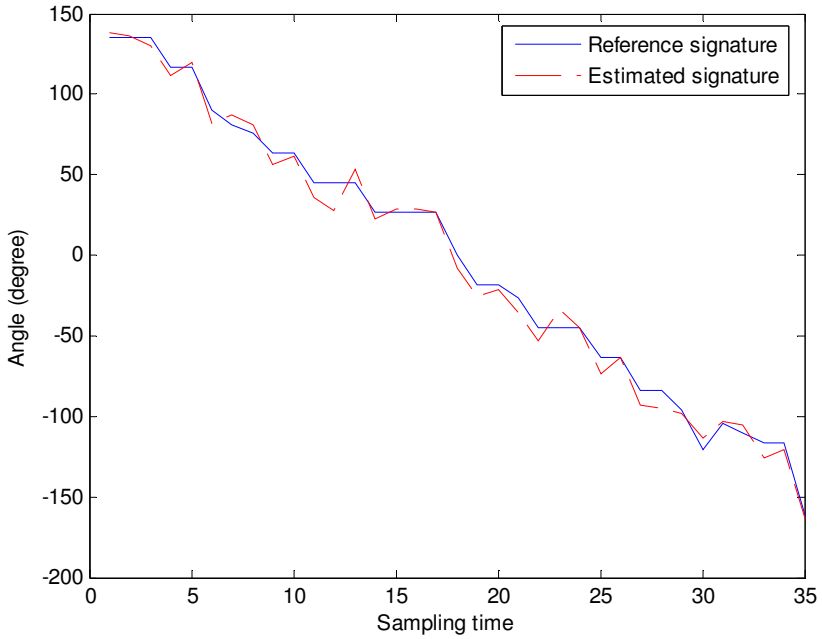
$$\tilde{S}_i^d(t) = S_i^d(t / d_i) \tag{2-5}$$

รูปที่ 2-16 แสดงการเปรียบเทียบองค์ประกอบย่อยลำดับแรกของลายเซ็นอ้างอิงกับลายเซ็นทดสอบที่ประมาณจากการชดเชยค่าหน่วงเวลาแล้ว สังเกตได้ว่าองค์ประกอบทั้งสองไม่เท่ากันทุกประการ ยังคงมีความผิดพลาดอยู่บ้างซึ่งผลรวมของกำลังสองของความผิดพลาดนี้สามารถหาได้จากสมการที่ 2-6

$$e_i = \sum_t \left| \tilde{S}_i^d(t) - S_i^r(t) \right|^2 \tag{2-6}$$



รูปที่ 2-15 องค์ประกอบย่อยลำดับแรกของลายเซ็นทดสอบที่วาดบนแกนเวลาทั้งของตัวเองและของลายเซ็นอ้างอิง



รูปที่ 2-16 การเปรียบเทียบองค์ประกอบลำดับแรกของลายเซ็นอ้างอิงกับลายเซ็นทดสอบที่ประมาณจากการชดเชยค่าหน่วงเวลาแล้ว

2.4.3 ขั้นตอนการเก็บตัวอย่าง

ขั้นตอนการเก็บตัวอย่างนี้เป็นขั้นตอนที่ต้องทำก่อนเริ่มการใช้งานเพื่อยืนยันตัวตน ทั้งนี้เพราะต้องเก็บลักษณะของลายเซ็นของผู้ใช้งานและเลือกเป็นลายเซ็นอ้างอิงก่อนถึงจะสามารถนำไปเปรียบเทียบกับลายเซ็นทดสอบได้ สำหรับการเก็บลายเซ็นมือนั้นจะใช้อุปกรณ์ที่มีขายในท้องตลาดทั่วไปที่มีชื่อว่า ปากกาและกระดานอิเล็กทรอนิกส์ (Electronic pencil and a tablet) เครื่องมือนี้จะถูกใช้ในการเก็บตัวอย่างลายเซ็นซึ่งสามารถบันทึกค่าตำแหน่งของลายเซ็นได้สองแกนในแนวนอนและแนวตั้ง ในงานวิจัยนี้ใช้อัตราการเก็บข้อมูลที่ 150 พิกัดต่อวินาที ค่าลักษณะของลายเซ็นจะถูกบันทึก และประมวลผลด้วยการแปลงเชิงมุมจากโปรแกรมที่พัฒนาขึ้นเองด้วยภาษา Java

สำหรับขั้นตอนนี้การเก็บบันทึกลักษณะของลายเซ็นจะใช้การแปลงเชิงมุมที่เหมือนกันทั้งฝั่งผู้ใช้งานและฝั่งเซิฟเวอร์ อย่างไรก็ตามที่เซิฟเวอร์เท่านั้นที่จะเก็บตัวอย่างที่บันทึกไว้จากผู้ใช้งานและขั้นตอนในการแยกองค์ประกอบรวมถึงการปรับเทียบค่าหน่วงเวลาก็จะดำเนินการที่ฝั่งเซิฟเวอร์เท่านั้นด้วย ดังนั้นโปรแกรม Java ที่ติดตั้งฝั่งผู้ใช้งานจึงมีขนาดเล็กและคอยทำหน้าที่แปลงเชิงมุมเท่านั้น ข้อสังเกตที่น่าสนใจคือการแยกองค์ประกอบออกเป็น M องค์ประกอบย่อยนั้นสามารถทำให้การปรับปรุงความเร็วใน

การประมวลผลลักษณะของลายเซ็นดีขึ้น นอกจากนี้ยังเพิ่มความน่าเชื่อถือในการตรวจสอบและยืนยันตัวตน เพราะเสมือนว่ามีการตรวจสอบถึง M เท่าจากลายเซ็นเดียว

2.4.4 ขั้นตอนการเลือกลายเซ็นอ้างอิง

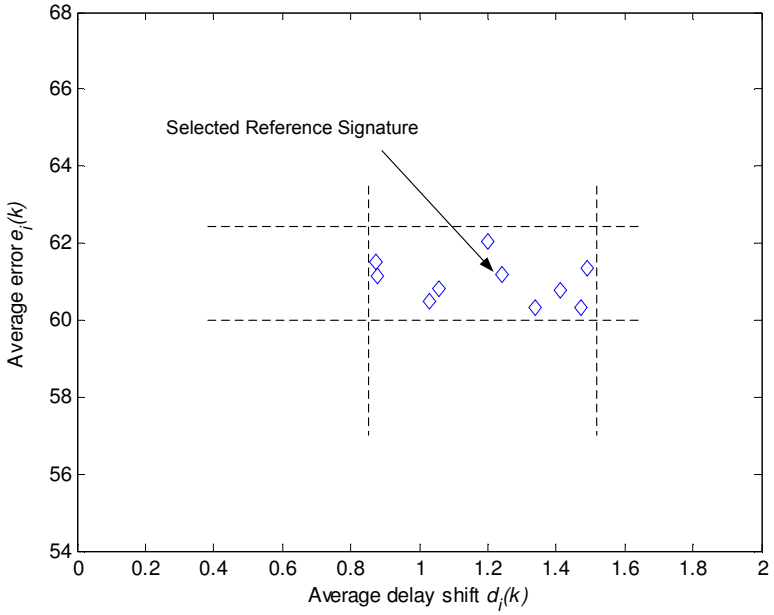
ผู้ใช้งานหนึ่งคนจะต้องทำการเก็บลายเซ็นมือไว้หลายๆ ลายเซ็นเพื่อลดความผิดพลาดจากการใช้ข้อมูลของลายเซ็นเดียว และเพิ่มความน่าเชื่อถือในการตรวจสอบ สมมุติให้ผู้ใช้งานหนึ่งคนเก็บตัวอย่าง N ลายเซ็นมือ จะต้องมีกรรมวิธีที่จะเลือกใช้ลายเซ็นอ้างอิงจากกลุ่ม N ลายเซ็นนั้น บางงานวิจัยใช้ค่าเฉลี่ยเป็นค่าอ้างอิง อย่างไรก็ตามการประมวลผลแบบออนไลน์นั้นต้องมีค่าหน่วงเวลาเป็นตัวแปรสำคัญในการตัดสินใจ ดังนั้นการประมาณจากการใช้ค่าเฉลี่ยจึงไม่เหมาะสมนักเพราะจะได้ค่าลักษณะของลายเซ็นอ้างอิงที่ไม่เปลี่ยนไปจากต้นฉบับมาก ในงานวิจัยนี้ใช้การเลือกลายเซ็นอ้างอิงจากลายเซ็นที่มีค่าเฉลี่ยของสองปัจจัยหลักอยู่ใกล้จุดศูนย์กลางของค่าทดสอบทั้งหมดมากที่สุด สองปัจจัยหลักได้แก่ ค่าหน่วงเวลา และค่าความผิดพลาดของการประมาณลายเซ็นทดสอบเทียบกับลายเซ็นอ้างอิง โดยที่ค่าเฉลี่ยของสองปัจจัยหลักนั้นสามารถหาได้จากสมการต่อไปนี้

$$d_i(k) = \frac{1}{N-1} \sum_{l}^{N-1} \arg\left\{ \min_{d_i(k,l)} \left\{ \sum_{t_i^k} \left| t_i^l - d_i(k,l) t_i^k \right|^2 \right\} \right\} \tag{2-7}$$

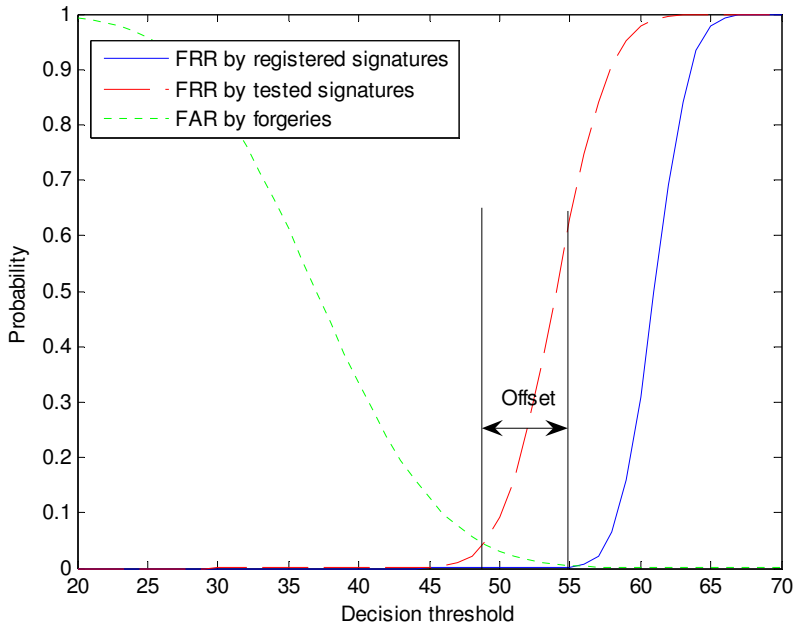
$$e_i(k) = \frac{1}{N-1} \sum_{l}^{N-1} \sum_{t} \left| \tilde{S}_i^l(t) - S_i^k(t) \right|^2 \tag{2-8}$$

เมื่อ $k, l = 1, \ldots, N$ และ $k \neq l$

รูปที่ 2-17 แสดงตัวอย่างของการหาลายเซ็นอ้างอิงโดยพิจาณาจากค่าหน่วงเวลาและค่าความผิดพลาดของ 10 ลายเซ็นที่บันทึกไว้ จากรูปลายเซ็นอ้างอิงถูกเลือกจากลายเซ็นที่มีค่าเฉลี่ยของทั้งค่าหน่วงเวลาและค่าความผิดพลาดใกล้จุดศูนย์กลางมากที่สุด



รูปที่ 2-17 ตัวอย่างของการหาลายเซ็นอ้างอิงโดยพิจาณาจากค่าหน่วงเวลาและค่าความผิดพลาดของ 10 ลายเซ็นที่บันทึกไว้



รูปที่ 2-18 ความน่าจะเป็นของ FRR และ FAR เทียบกับระดับการตัดสินใจ

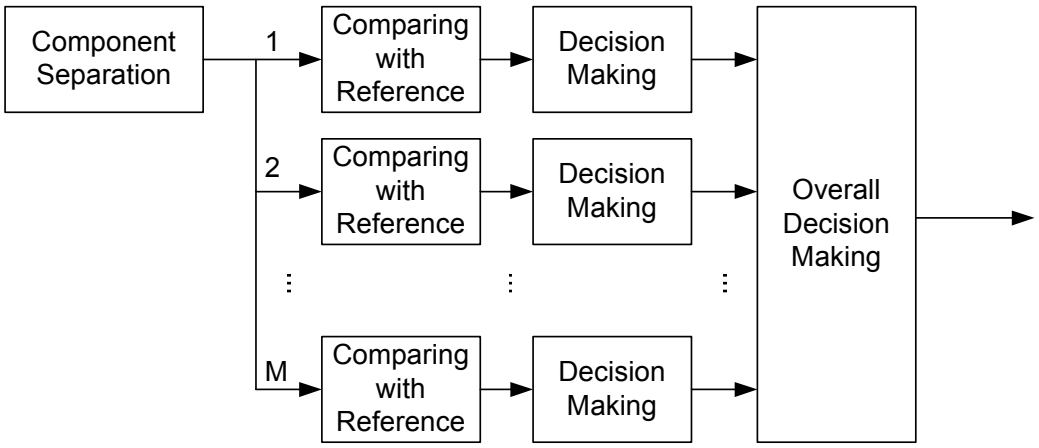
2.4.5 ขั้นตอนการเลือกระดับค่าหน่วงเวลา

ในการใช้งานจริงเป็นไปไม่ได้ที่เซ็นลายเซ็นทุกครั้งแล้วจะได้เวลาที่เท่ากันเสมอ สำหรับผู้ใช้งานหนึ่งคนการเก็บตัวอย่างที่ฝั่งเซิฟเวอร์มีค่าจำกัด ดังนั้นช่วงเวลาของการยืนยันตัวตนจะต้องมีการกำหนดระดับที่ยอมรับได้เมื่อค่าที่ได้มีความผิดพลาดไปจากค่าอ้างอิงเพื่อใช้ในการตัดสินใจว่าจะยอมรับลายเซ็นนั้นเป็นตัวตนของผู้ใช้งานหรือไม่ ระดับการตัดสินใจนี้สำคัญมากเพราะจะช่วยป้องกันลายเซ็นที่อาจจะเกิดจากการปลอมแปลงได้ งานวิจัยนี้พิจารณาคุณลักษณะของการตรวจสอบลายเซ็นมือเป็นสองประเภทดังนี้

ประเภทแรกเรียกว่า FRR (False Rejection Rate) เป็นกรณีที่ลายเซ็นที่ถูกต้องถูกปฏิเสธว่าไม่ใช่ตัวตนของผู้ใช้งาน ส่วนประเภทที่สองเรียกว่า FAR (False Acceptance Rate) เป็นกรณีที่ลายเซ็นปลอมถูกยอมรับว่าใช่ตัวตนของผู้ใช้งาน ค่าอัตราของทั้งสองประเภทนี้ขึ้นกับระดับการตัดสินใจที่กำหนดไว้ สำหรับงานวิจัยนี้เราเลือกค่าระดับการตัดสินใจที่ทำให้ระบบเป็น EER (Equal Error Rate) ซึ่งทำให้ FAR = FRR ในงานวิจัยนี้สร้างลายเซ็นปลอมจากการใช้ลายเซ็นมือของอาสาสมัคร 10 คน จากรูปที่ 2-18 แสดงความน่าจะเป็นของการใช้ระดับการตัดสินใจที่แตกต่างกัน ค่าส่วนต่าง (Offset) ที่ได้จากการใช้ฐานข้อมูลที่เก็บตัวอย่างมา กับลายเซ็นทดสอบของผู้ใช้งานนี้สามารถนำไปใช้ปรับเทียบให้ระบบมีความน่าเชื่อถือมากขึ้น ค่า Offset นี้มีความสัมพันธ์กับการแยกแยะข้อมูลระหว่างลายเซ็นที่ปลอม กับลายเซ็นจริง ตามกราฟในรูปที่ 2-18 ซึ่งถ้าเลือกค่า Offset ที่น้อยกว่าที่แสดงในรูป จะทำให้เกิด FAR สูงขึ้น แต่ถ้า Offset มากกว่าที่กำหนดจะทำให้เกิด FRR เพิ่มขึ้นกว่าที่ควรจะเป็น

2.4.6 ขั้นตอนการตัดสินใจ

จากการอธิบายในหัวข้อก่อนหน้านี้ เมื่อทำการแยกลายเซ็นมีออกเป็นองค์ประกอบย่อยๆ หลายองค์ประกอบ จึงทำให้ขั้นตอนการตัดสินใจสามารถดำเนินการแยกกันตามองค์ประกอบย่อยได้โดยอิสระ ทำให้งานวิจัยนี้มีการแยกการตัดสินใจตามองค์ประกอบย่อย จากนั้นมีการตัดสินใจสุดท้ายอีกครั้งหนึ่งเพื่อประเมินว่าเป็นลายเซ็นของผู้ใช้งานจริงหรือไม่ แม้ว่าการตัดสินใจสุดท้ายสามารถดำเนินการได้หลายรูปแบบ และแสดงเป็นระดับความเชื่อมั่นได้ แต่ในงานวิจัยนี้จะยอมรับว่าเป็นตัวตนจริงก็ต่อเมื่อทุกองค์ประกอบย่อยผ่านการยอมรับทั้งหมดกระบวนการดังกล่าวนี้สามารถแสดงในรูปที่ 2-19



รูปที่ 2-19 แผนภาพการดำเนินการเพื่อตัดสินใจยืนยันตัวตนของเจ้าของลายเซ็น

2.5 กล่าวท้ายบท

เนื้อหาในบทนี้กล่าวถึงรายละเอียดของเทคนิคการยืนยันตัวตนของเจ้าของลายเซ็น ซึ่งมีวิธีการใหม่ที่งานวิจัยนี้เสนอ กล่าวคือการแปลงเชิงมุมของลายเซ็นมือ ขั้นตอนและกระบวนการต่างๆ สามารถสรุปได้ดังนี้

กระบวนการประมวลลายเซ็นด้วยการแปลงเชิงมุม

เป็นกระบวนการแปลงลายเซ็นเพื่อให้อยู่ในรูปแบบข้อมูลเชิงมุม ซึ่งมีสองขั้นตอนดังนี้ ขั้นตอนการแปลงเชิงมุมและขั้นตอนการหาค่าหน่วงเวลา

กระบวนการยืนยันลายเซ็น

เป็นกระบวนการยืนยันลายเซ็นจากกลุ่มของลายเซ็นที่บันทึกไว้ในฐานข้อมูล มีขั้นตอนหลักดังนี้ ขั้นตอนการเก็บตัวอย่าง ขั้นตอนการเลือกลายเซ็นอ้างอิง ขั้นตอนการเลือกระดับค่าหน่วงเวลา และขั้นตอนการตัดสินใจ

บทที่ 3 โปรแกรมตรวจสอบลายเซ็นมืออิเล็กทรอนิกส์

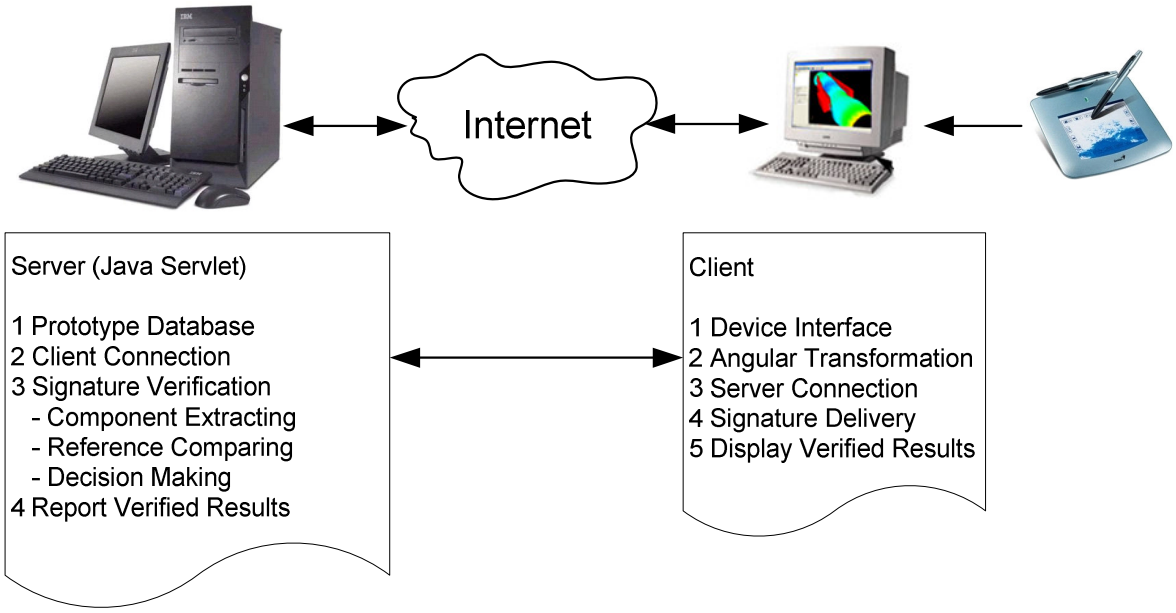
3.1 กล่าวนำ

เนื้อหาในบทที่ผ่านมาได้กล่าวถึงหลักการการตรวจสอบลายเซ็นมืออิเล็กทรอนิกส์ ซึ่งเป็นหลักการที่จะถูกนำไปใช้งานจริงต่อไป งานวิจัยนี้ได้นำหลักการเหล่านั้นมาเขียนด้วยโปรแกรมภาษา Java เพื่อใช้ทดสอบและวิเคราะห์แนวทางที่นำเสนอด้วยการแปลงเชิงมุม บทนี้จึงมีสาระสำคัญที่การพัฒนาโปรแกรมเพื่อรองรับหลักการในบทที่ผ่านมา โดยเริ่มที่การทำงานในภาพรวมของโปรแกรม การอธิบายวิธีการติดตั้งโปรแกรมเพื่อให้ผู้อ่านสามารถนำไปใช้งานได้โดยง่าย และสุดท้ายการอธิบายถึงการใช้งานของโปรแกรมที่เสนอในงานวิจัยนี้

3.2 ภาพรวมการทำงานของโปรแกรม

วัตถุประสงค์ของงานวิจัยนี้เพื่อให้สามารถนำหลักการที่เสนอเพื่อไปประยุกต์ใช้กับธุรกรรมทางอิเล็กทรอนิกส์หรือที่เรียกว่าบริการ e-Commerce ดังนั้นในโปรแกรมที่จะทำการตรวจสอบยืนยันตัวตนของผู้ใช้งานจึงถูกพัฒนาขึ้นใหม่ทั้งภาคผู้ใช้งานที่ปลายทางและภาคเซิฟเวอร์ งานวิจัยนี้เลือกใช้ Java Servlet เป็นโปรแกรมที่เชื่อมต่อการทำงานทั้งสองภาค รูปที่ 3-1 แสดงการเชื่อมต่อระหว่างภาคเซิฟเวอร์และภาคผู้ใช้งานซึ่งทำการยืนยันตัวตนในระบบออนไลน์ ฝั่งผู้ใช้งานนั้นจะต้องมีปากกาและกระดานอิเล็กทรอนิกส์เชื่อมต่อกับคอมพิวเตอร์เพื่อความสะดวกในการเขียนลายเซ็นมือ ซึ่งหลังจากที่มีการแปลงข้อมูลลายเซ็นมือเป็นข้อมูลในโดเมนเชิงมุมแล้ว โปรแกรมฝั่งผู้ใช้งานจะส่งข้อมูลนี้ไปถึงเซิฟเวอร์ ผ่านโปรโตคอลพื้นฐานอย่าง TCP/IP ซึ่งโปรแกรมใช้งานอินเทอร์เน็ตทั่วไปรองรับอยู่แล้ว

สำหรับฝั่งเซิฟเวอร์ จะมีลายเซ็นมือที่ถูกบันทึกและรวมไว้ที่ฐานข้อมูลเพื่อใช้เลือกลายเซ็นอ้างอิงสำหรับการเปรียบเทียบ ลายเซ็นที่ผ่านการตรวจสอบเท่านั้นจะถูกอนุญาตให้ดำเนินการทางธุรกรรมต่างๆ ในหน้าจอถัดไป มิฉะนั้นลายเซ็นที่ถูกปฏิเสธจะไม่สามารถเข้าใช้เวปไซต์อื่นๆ ได้ต่อไป

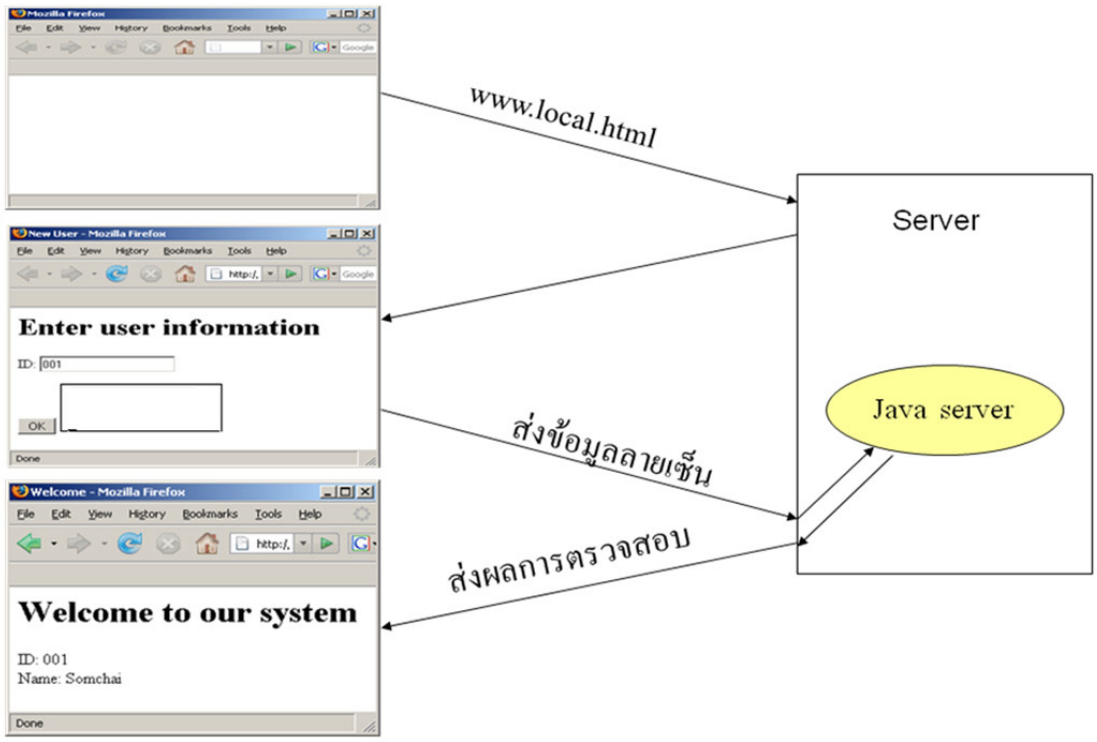


รูปที่ 3-1 แผนภาพการเชื่อมต่อระหว่างภาคผู้ใช้งาน (Client) และภาคเซิฟเวอร์

หลักการทำงานของโปรแกรมโดยสรุปมีทั้งหมด 4 ส่วน คือ

1. การแปลงข้อมูลของลายเซ็นมือ ซึ่งเป็นขั้นตอนในการรับลายเซ็นมือที่ฝั่ง ผู้ใช้งาน
2. การติดต่อผ่านเครือข่ายบน Internet ระหว่าง เซิฟเวอร์ และ ผู้ใช้งาน
3. ทำการประมวลผลที่ เซิฟเวอร์ เพื่อเปรียบเทียบลายเซ็นมือ
4. ส่งผลการตรวจสอบกลับมาที่ ผู้ใช้งาน และแสดงผลให้ทราบ

ทั้งนี้ที่ภาคผู้ใช้งานไม่จำเป็นต้องลงโปรแกรมใดๆ ไว้ก่อน เพราะเมื่อเรียกใช้งานผ่านอินเตอร์เน็ทมายังเซิฟเวอร์ โปรแกรมเล็กๆ ที่หน้าเวปของเซิฟเวอร์จะทำงานโดยทันที ดังนั้นจึงไม่มีการเก็บข้อมูลลายเซ็นมือที่เครื่องปลายทาง และไม่มีการส่งข้อมูลลายเซ็นใดๆ มาระหว่างการติดต่อ จึงทำให้ความปลอดภัยด้านเครือข่ายสูง สำหรับอุปกรณ์ปากกาและกระดานอิเล็กทรอนิกส์มีไว้เพื่อให้เขียนลายเซ็นได้สะดวกสะบายขึ้น ซึ่งหากใช้เมาส์ก็สามารถทำงานได้ แต่ลายเซ็นจะไม่สวยเหมือนของจริง ทำให้การยืนยันตัวตนล้มเหลวได้



รูปที่ 3-2 รูปแสดงตัวอย่างการเรียกใช้ เซิฟเวอร์

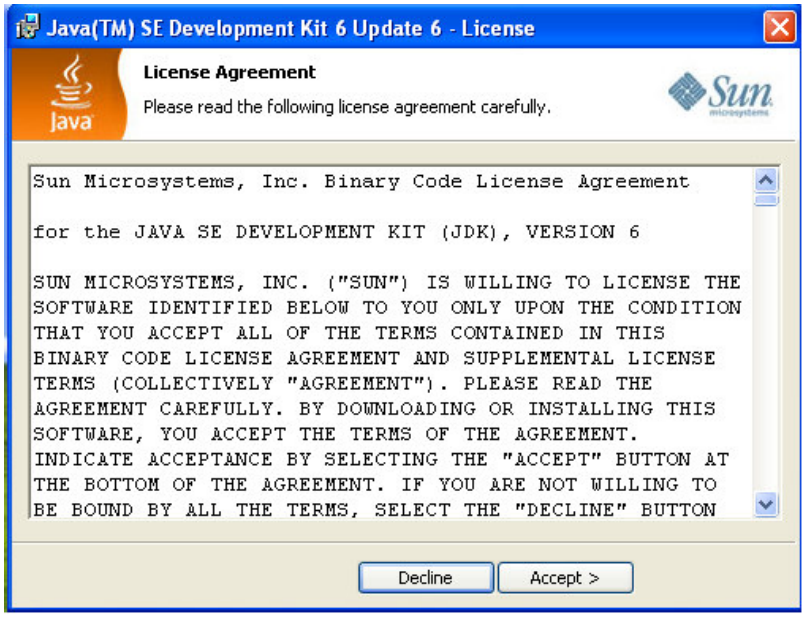
3.3 ขั้นตอนการติดตั้ง JAVA SERVLET เพื่อการพัฒนาโปรแกรม

เพื่อให้ผู้อ่านสามารถดำเนินการตามไปได้โดยง่าย ผู้เขียนขออธิบายขั้นตอนต่างๆ สรุปได้ดังนี้

ทำการดาวน์โหลด JDK 1.6.0 b96 หรือสูงกว่า (สามารถดาวน์โหลดได้ http: //java.sun.com/javase/downloads/index.jsp) เมื่อ download เสร็จแล้ว เราจะได้ไฟล์ตามรูปด้านล่าง

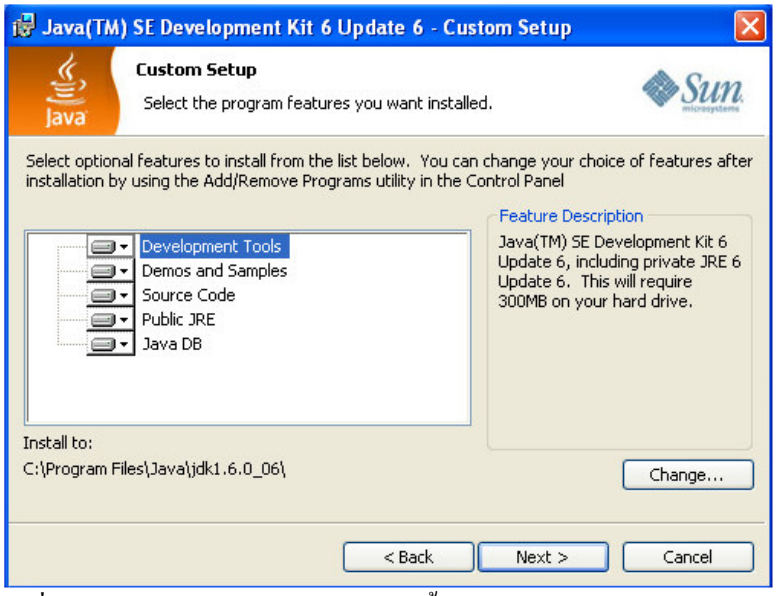
รูปที่ 3-3 ภาพไฟล์ JDK 1.6.0 b96

Double click ที่ไฟล์ในรูปที่ 3-3 เพื่อติดตั้งโปรแกรม JDK โปรแกรม Installer จะแสดงข้อความต้อนรับ ให้ click ที่ Accept เพื่อไปหน้าต่อไป



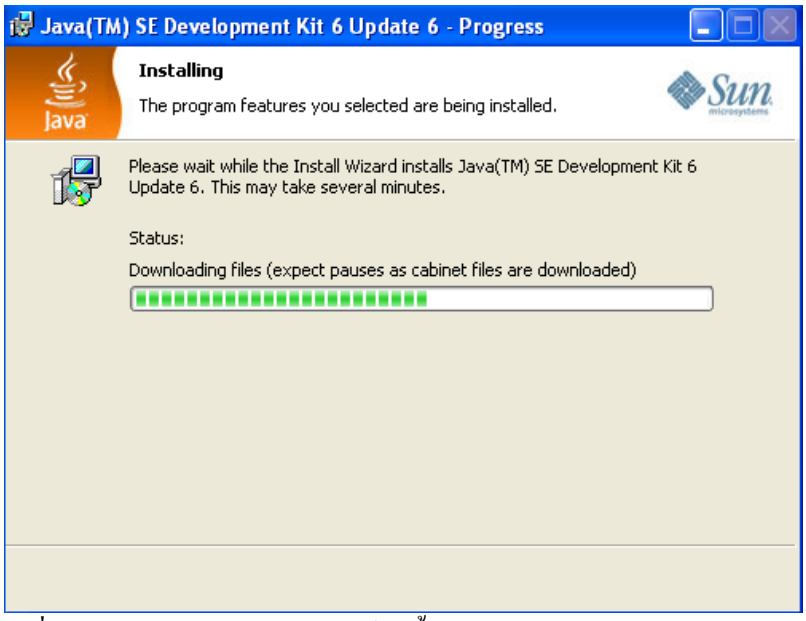
รูปที่ 3-4 หน้าต่างแสดง Installer ของโปรแกรม JDK

โปรแกรม Installer จะแสดง path ที่เราลงโปรแกรม JDK เอาไว้ แล้วแสดงให้เห็น โปรแกรมอื่นๆ ของโปรแกรม JDK ถ้าถูกต้องแล้ว คือตรงกับ path ที่เราได้ลงไว้จริง ก็ให้ click ที่ Next เพื่อไปยังหน้าต่อไป



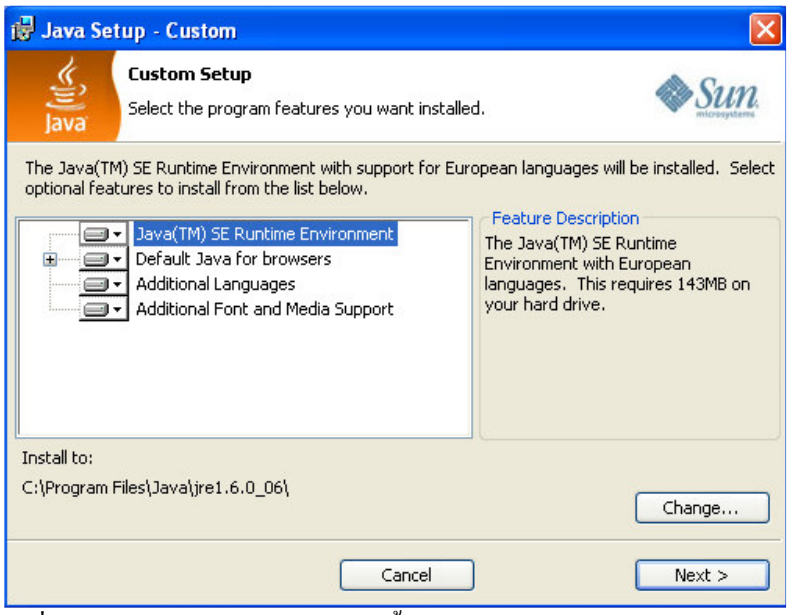
รูปที่ 3-5 หน้าต่างแสดงทางเลือกการติดตั้งของโปรแกรม JDK

โปรแกรม Installer จะทำการ copy ไฟล์ของ JDK ลงใน path ที่ระบุไว้



รูปที่ 3-6 หน้าต่างแสดงสถานการณ์ติดตั้ง JDK

โปรแกรม Installer จะแสดง path ที่เราลงโปรแกรม java เอาไว้ แล้วแสดงให้เห็น โปรแกรมอื่นๆ ของโปรแกรม java ถ้าถูกต้องแล้ว คือตรงกับ path ที่เราได้ลงไว้จริง ก็ให้ click ที่ Next เพื่อไปยังหน้าต่อไป



รูปที่ 3-7 หน้าต่างแสดงการเลือกติดตั้ง Java

โปรแกรม Installer จะทำการ copy ไฟล์ของ java ลงใน path ที่ระบุไว้

รูปที่ 3-8 หน้าต่างแสดงสถานะติดตั้ง Java

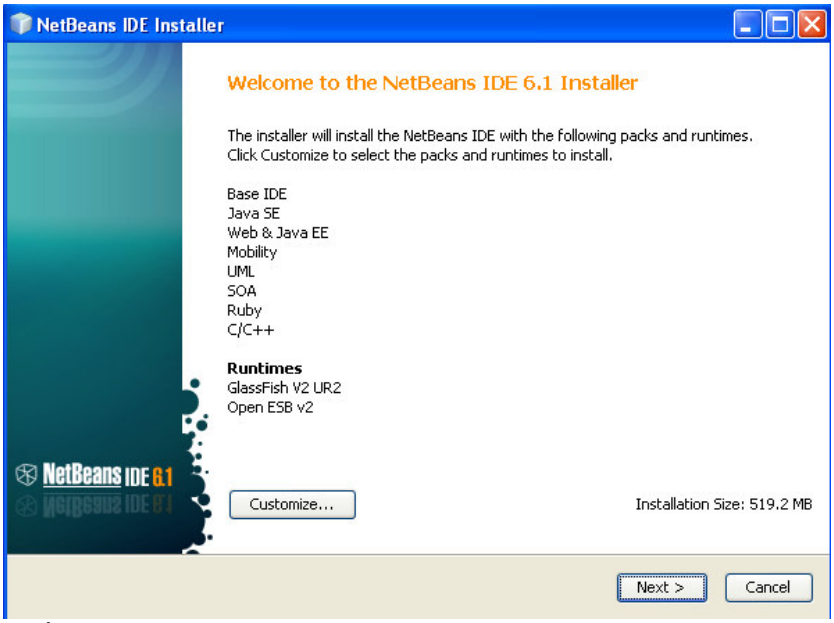
โปรแกรม Installer แสดงผลการติดตั้ง JDK ว่าสำเร็จเรียบร้อย โดยลงไว้ใน path ที่เราได้ระบุไว้ก่อนหน้านี้ ให้ click ที่ Finish เพื่อจบการติดตั้ง

รูปที่ 3-9 หน้าต่างแสดงการเสร็จสิ้นการติดตั้งโปรแกรม Java

ทำการดาวน์โหลด NetBeans 6 หรือสูงกว่า (สามารถดาวน์โหลดได้ http:// download. netbeans.org/netbeans/6.0/final/?cid=921887) เมื่อ download เสร็จแล้ว เราจะได้ไฟล์ตามรูปมา

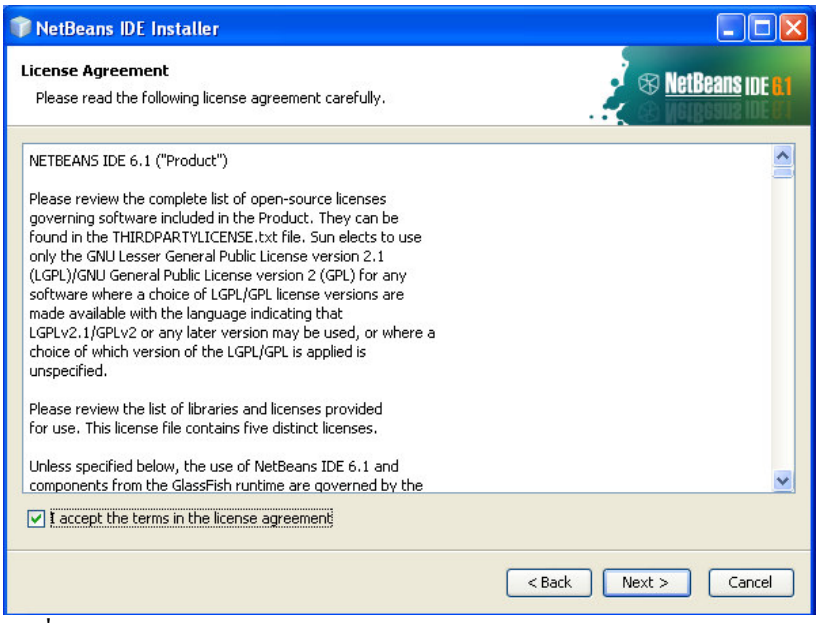
รูปที่ 3-10 ภาพไฟล์ NetBeans 6

Double click ที่ไฟล์ เพื่อติดตั้งโปรแกรม netbeans6-1_full โปรแกรม Installer จะแสดงให้เห็น โปรแกรมอื่นๆ ของโปรแกรม NetBeans IDE ถ้าถูกต้องแล้ว คือตรงกับความต้องการที่เราได้ลงไว้จริง ก็ให้ click ที่ Next เพื่อไปยังหน้าต่อไป



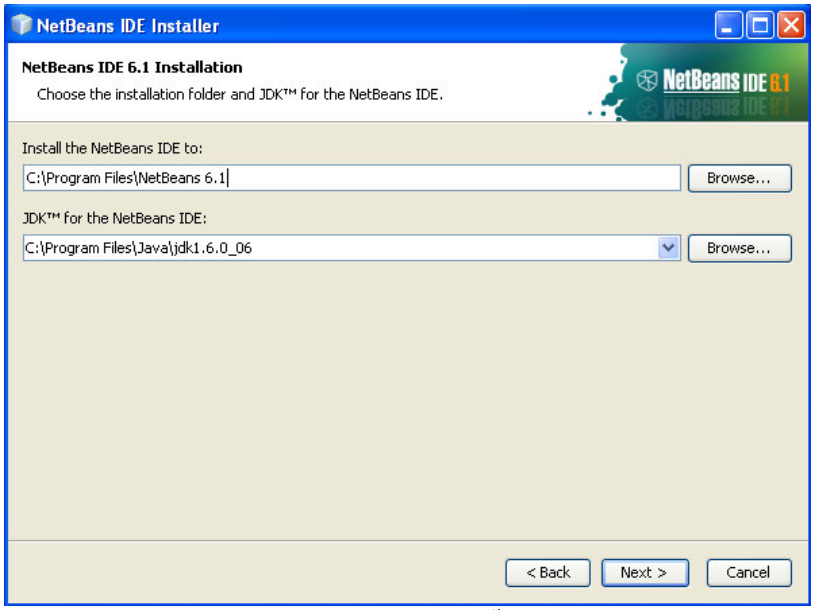
รูปที่ 3-11 หน้าต่างแสดง Installer ของโปรแกรม NetBeans 6

โปรแกรม Installer จะให้เรายืนยันว่าเราจะยอมรับข้อตกลงที่ระบุไว้ใน license agreement หรือไม่ ให้เลือกที่ I accept the terms in the license agreement แล้ว click ที่ Next เพื่อไปยังหน้าต่อไป



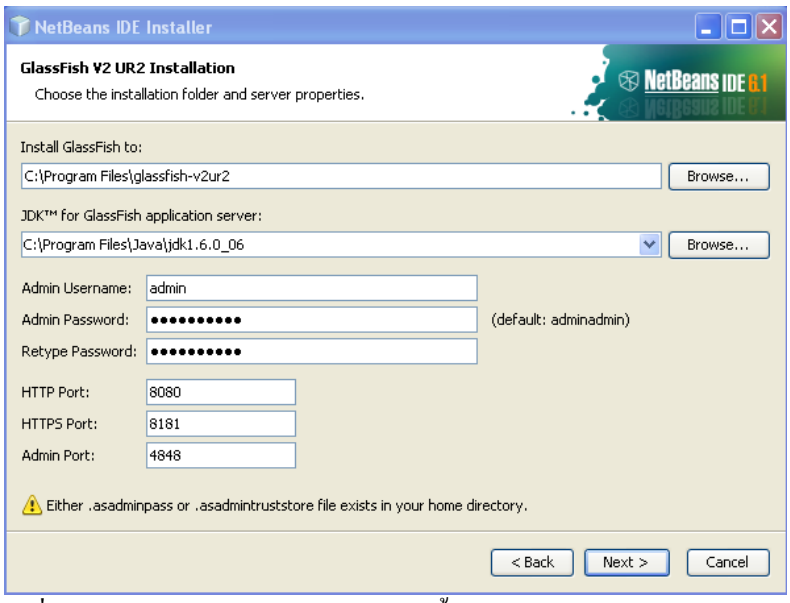
รูปที่ 3-12 หน้าต่างแสดง License agreement ของโปรแกรม NetBeans 6

โปรแกรม Installer จะค้นหา path ที่เราลงโปรแกรม NetBeans เอาไว้ แล้วแสดงให้เห็น เพื่อให้เรายืนยัน ถ้า path ของโปรแกรม NetBeans ถูกต้องแล้ว คือตรงกับ path ที่เราได้ลงไว้จริง ก็ให้ click ที่ Next เพื่อไปยังหน้าต่อไป



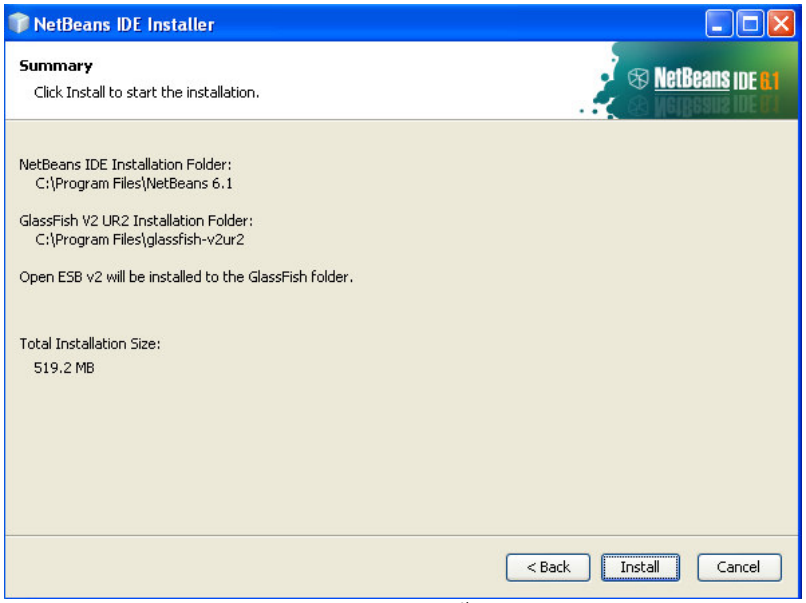
รูปที่ 3-13 หน้าต่างแสดงการเลือกตำแหน่งติดตั้งของโปรแกรม NetBeans 6

โปรแกรม Installer จะค้นหา path ที่เราลงโปรแกรม เซิฟเวอร์ เอาไว้ แล้วแสดงให้เห็น เพื่อให้เรายืนยัน ถ้า path ของโปรแกรม เซิฟเวอร์ ถูกต้องแล้ว คือตรงกับ path ที่เราได้ลงไว้จริง ก็ให้ click ที่ Next เพื่อไปยังหน้าต่อไป



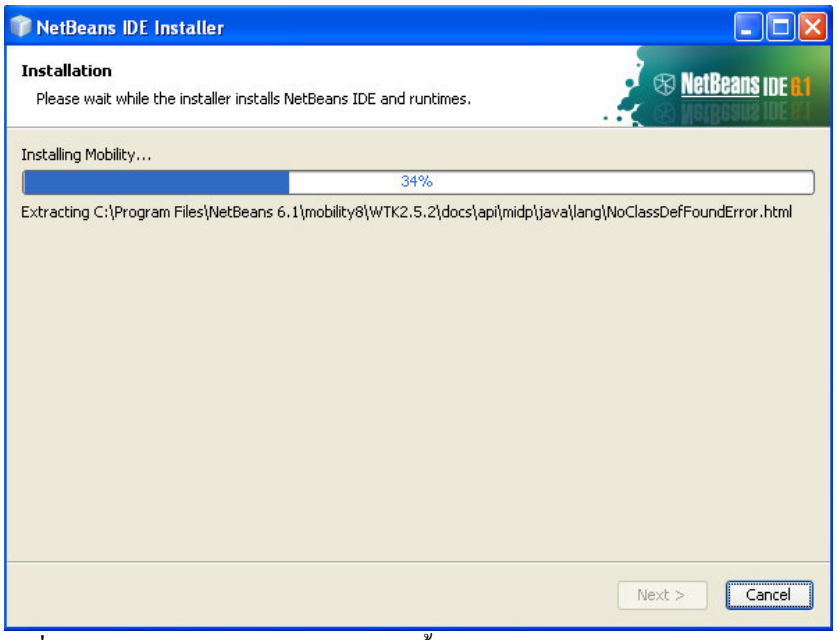
รูปที่ 3-14 หน้าต่างแสดงการใส่ข้อมูลติดตั้งของโปรแกรม NetBeans 6

โปรแกรม Installer แสดง path ที่จะทำการติดตั้งโปรแกรม NetBeans กับ เซิฟเวอร์ และขนาดของพื้นที่ที่จำเป็นต้องใช้ให้เราดู เพื่อให้เรายืนยันอีกครั้งหนึ่ง ให้ click ที่ Install เพื่อไปยังหน้าต่อไป



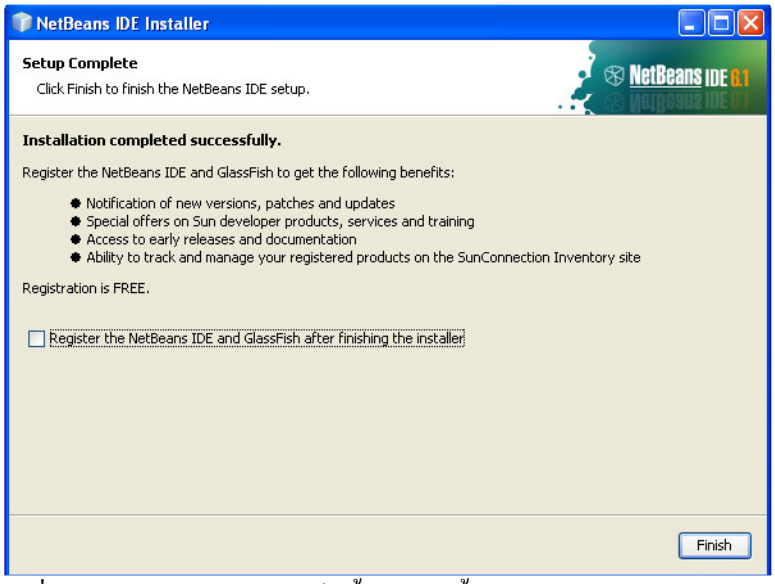
รูปที่ 3-15 หน้าต่างแสดงข้อมูลสรุปการติดตั้งของโปรแกรม NetBeans 6

โปรแกรม Installer จะทำการ copy ไฟล์ของ NetBeans ลงใน path ที่ระบุไว้



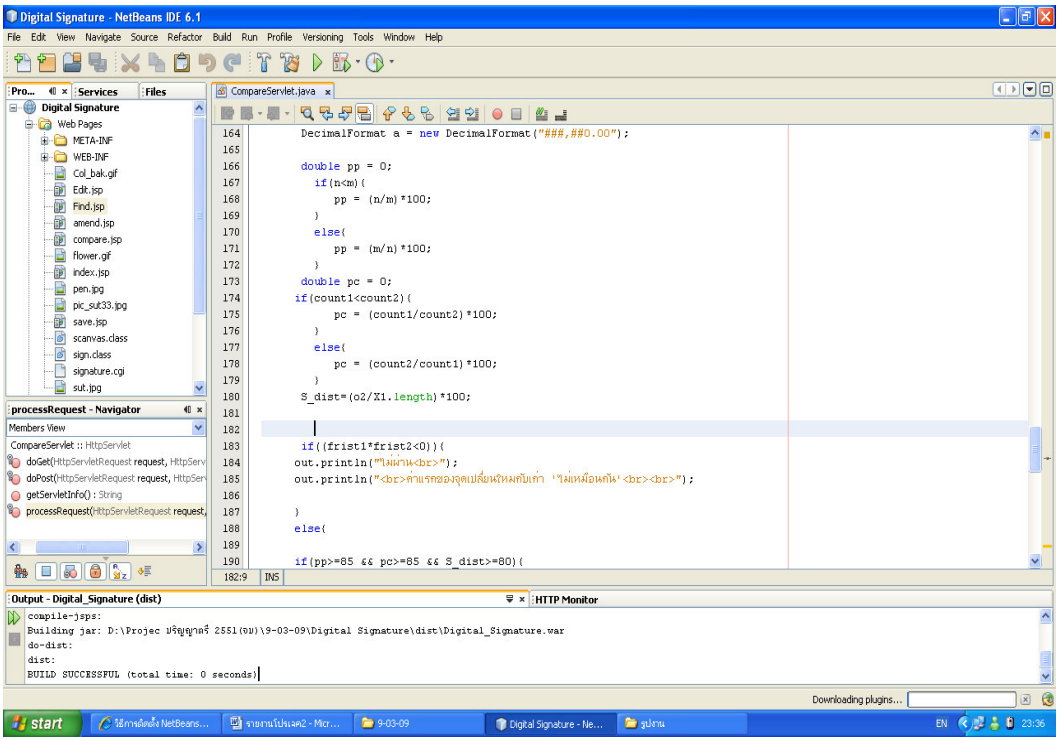
รูปที่ 3-16 หน้าต่างแสดงสถานะการติดตั้งโปรแกรม NetBeans 6

โปรแกรม Installer แสดงผลการติดตั้ง NetBeans ว่าสำเร็จเรียบร้อย โดยลงไว้ใน path ที่เราได้ระบุไว้ก่อนหน้านี้ ให้ click ที่ Finish เพื่อจบการติดตั้ง



รูปที่ 3-17 หน้าต่างแสดงว่าเสร็จสิ้นการติดตั้งโปรแกรม NetBeans 6

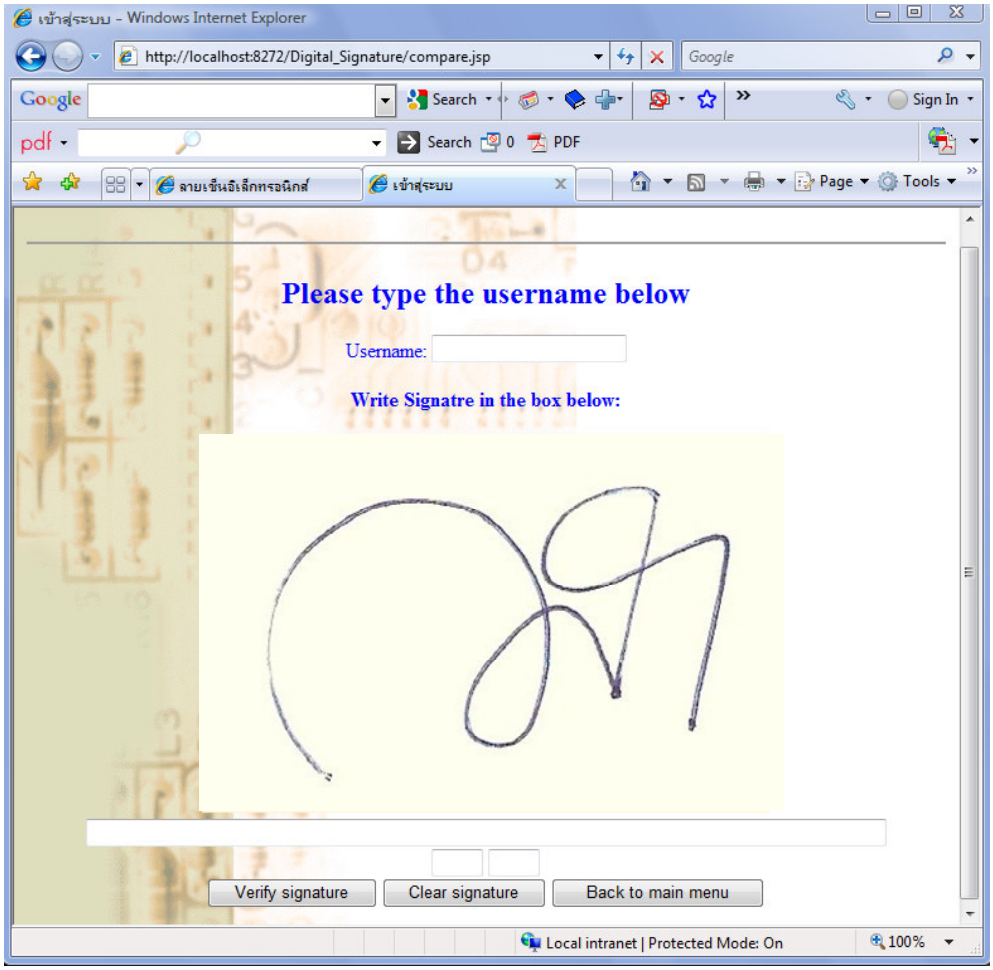
ในการพัฒนาโปรแกรมของงานวิจัยนี้ ผู้วิจัยใช้โปรแกรม NetBeans เป็นโปรแกรมในการช่วยพัฒนาซึ่งสามารถพัฒนาได้ทั้งโปรแกรมภาคผู้ใช้งาน และภาคเซิฟเวอร์ ตัวอย่างหน้าต่างของโปรแกรม Netbeans แสดงในรูปที่ 3-18



รูปที่ 3-18 หน้าต่างแสดงโปรแกรม NetBeans

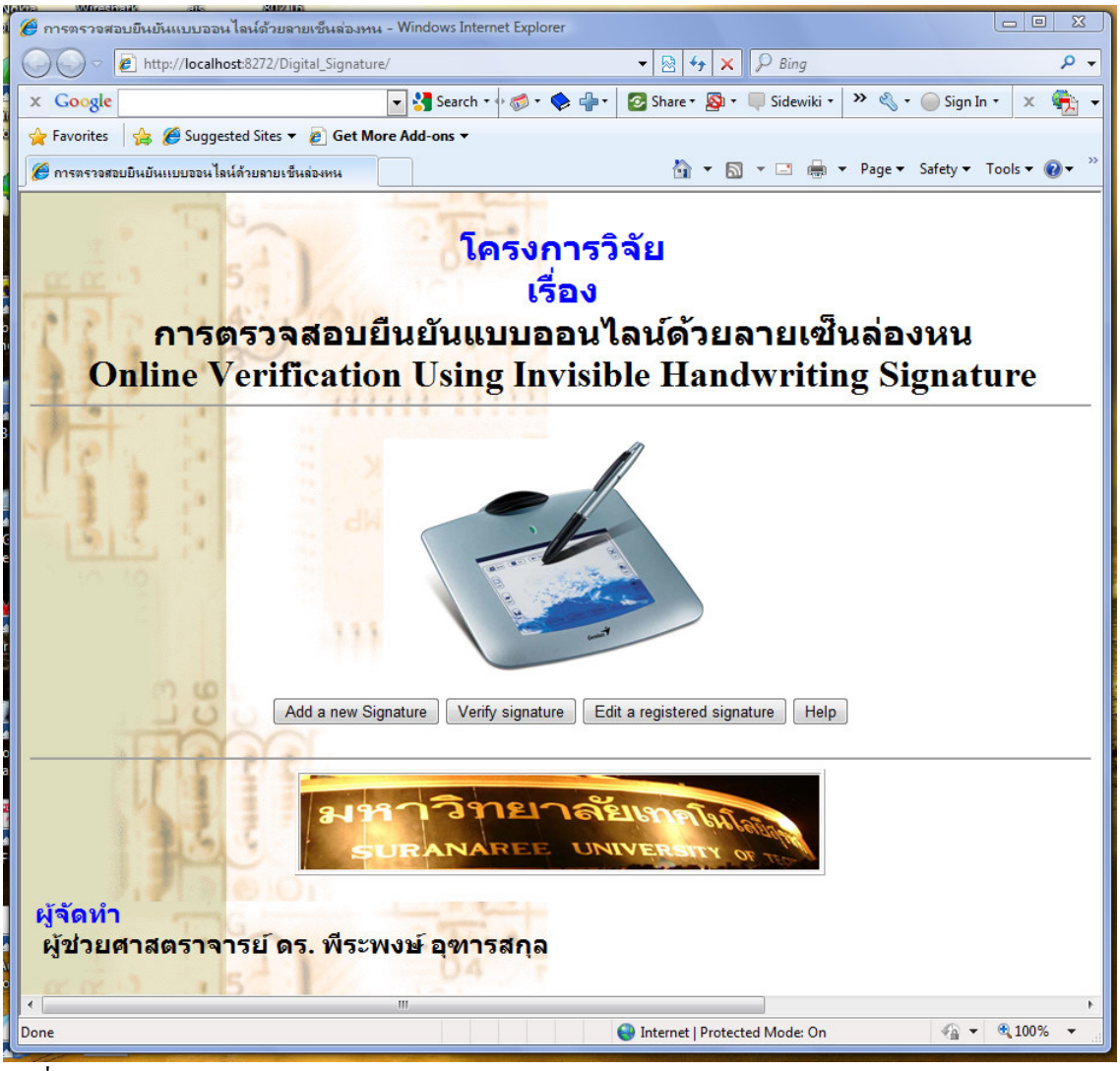
3.4 การทำงานของโปรแกรมที่พัฒนาขึ้น

เนื้อหาในส่วนที่แล้วได้กล่าวถึงการติดตั้งโปรแกรมที่ใช้สำหรับการพัฒนาในงานวิจัยนี้ ส่วนต่อไปจะอธิบายถึงลักษณะหน้าต่างของโปรแกรมที่ใช้สำหรับเก็บตัวอย่างลายเซ็นมือ และเป็นหน้าต่างสำหรับการตรวจสอบยืนยันลายเซ็นมือ ซึ่งผ่านระบบออนไลน์ โดยสามารถใช้งานผ่านเครือข่ายอินเตอร์เน็ตได้กับทุกโปรแกรม Browser ในตัวอย่างที่นำเสนอต่อไปนี้ใช้โปรแกรม Internet Explorer ของ Windows ดังแสดงตัวอย่างหน้าต่างในรูปที่ 3-19



รูปที่ 3-19 ตัวอย่างหน้าต่างหนึ่งของโปรแกรมเพื่อตรวจสอบยืนยันลายเซ็น

การทำงานของโปรแกรมสามารถแบ่งได้เป็น 3 รายการหลักคือการบันทึกลายเซ็นมือ การแก้ไขลายเซ็นมือที่บันทึก และการตรวจสอบยืนยัน โดยที่หน้าต่างแรกจะมีเมนูให้เลือกกดปุ่มเพื่อใช้งาน ดังแสดงในรูปที่ 3-20



รูปที่ 3-20 หน้าต่างแสดงเมนูหลักของโปรแกรม

หน้าต่างแรกนี้จะมีปุ่มให้เลือกกด 4 ปุ่ม ดังนี้

Add a new Signature เป็นปุ่มที่ใช้สำหรับผู้ใช้งานที่ยังไม่เลยลงทะเบียนในงานเป็นครั้งแรก

Verify Signature เป็นปุ่มที่ใช้สำหรับการตรวจสอบยืนยันลายเซ็นเพื่อเข้าใช้งานในเวปนี้ต่อไป

Edit a registered signature เป็นปุ่มที่ใช้แก้ไขข้อมูล หรือลายเซ็นมือของผู้ใช้งาน

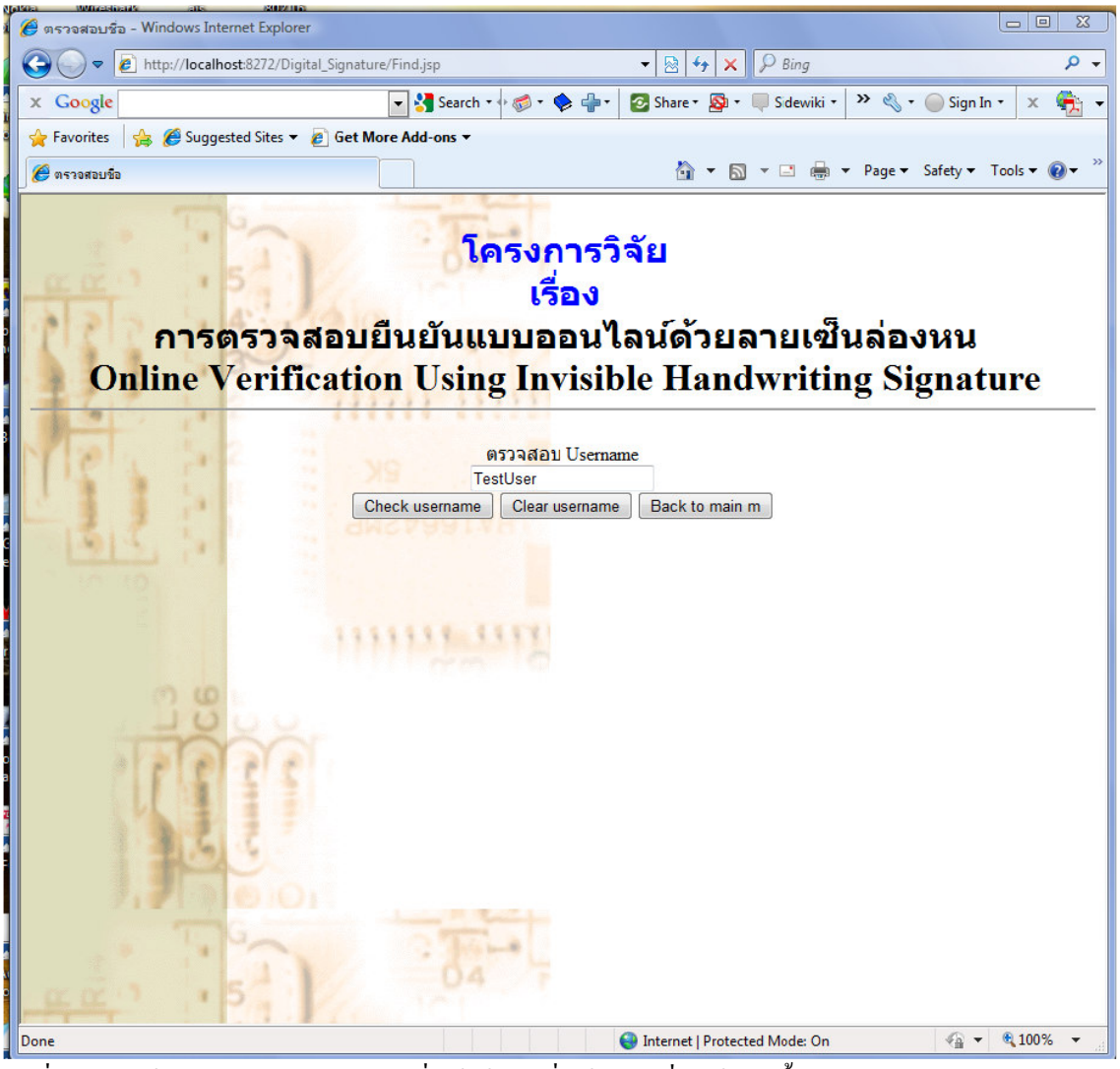
Help เป็นปุ่มที่อธิบายวิธีการใช้งานของโปรแกรม

เมื่อทำการกดปุ่ม Add a new Signature หน้าต่างจะพาไปสู่การกำหนดชื่อผู้ใช้งานดังแสดงในรูปที่ 3-21 ซึ่งจะมีปุ่มให้กดอีก 3 ปุ่ม ดังนี้

Check username เป็นปุ่มที่ใช้ตรวจสอบชื่อผู้ใช้งาน ว่ามีซ้ำกับฐานข้อมูลที่เก็บไว้หรือไม่

Clear username เป็นปุ่มที่ลบชื่อที่พิมพ์ไว้ด้านบน

Back to main menu เป็นปุ่มที่กลับไปยังหน้าเมนูหลัก



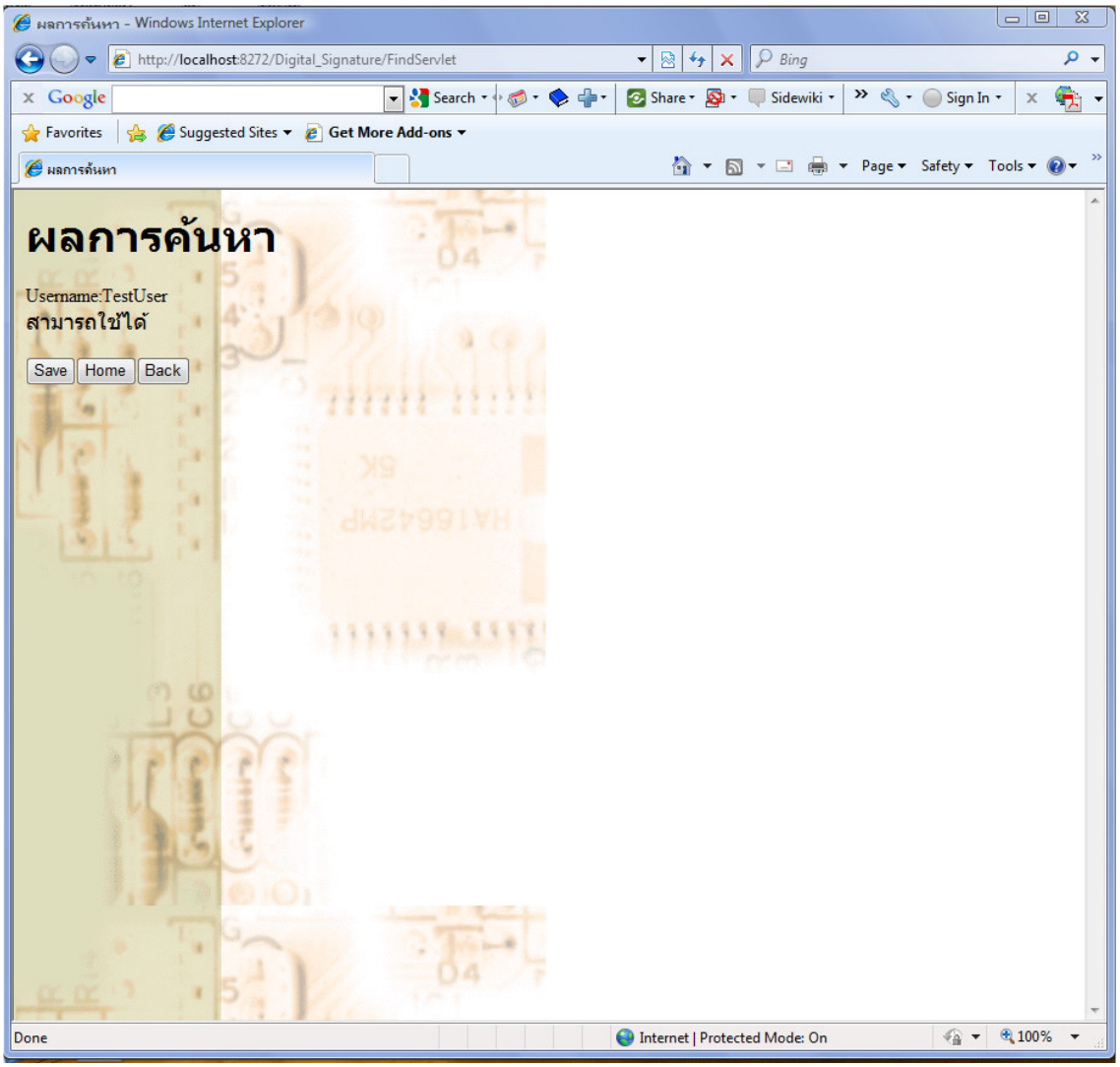
รูปที่ 3-21 หน้าต่างแสดงการตรวจสอบชื่อผู้ใช้งาน เมื่อต้องการเริ่มใช้งานครั้งแรก

ถ้าหากการค้นหาไม่พบชื่อซ้ำกันในฐานข้อมูลที่เก็บไว้ หน้าต่างก็จะแสดงข้อความยืนยันกลับมาดังแสดงในรูปที่ 3-22 ซึ่งถ้าสามารถใช้ชื่อที่พิมพ์ได้ ก็จะมีปุ่มให้เลือกกดอีก 3 ปุ่มดังนี้

Save เพื่อบันทึกชื่อผู้ใช้งานนี้ แล้วจะนำพาไปหน้าต่างที่ทำการบันทึกลายเซ็นมือ

Home เพื่อกลับไปยังหน้าเมนูหลัก

Back เพื่อกลับไปหน้าต่างที่ตรวจสอบชื่อผู้ใช้งานอีกครั้ง



รูปที่ 3-22 หน้าต่างแสดงผลการตรวจสอบชื่อผู้ใช้งาน

เมื่อกดปุ่ม Save ในรูปที่ 3-21 หน้าต่างใหม่จะแสดงขึ้นมาเพื่อรอบันทึกลายเซ็นมือ พื้นที่ในกรอบสี่เหลี่ยมเป็นพื้นที่สำหรับรับค่าลายเซ็นที่จะบันทึก

ในหน้าต่างนี้มีปุ่มให้เลือกกด 3 ปุ่มดังนี้

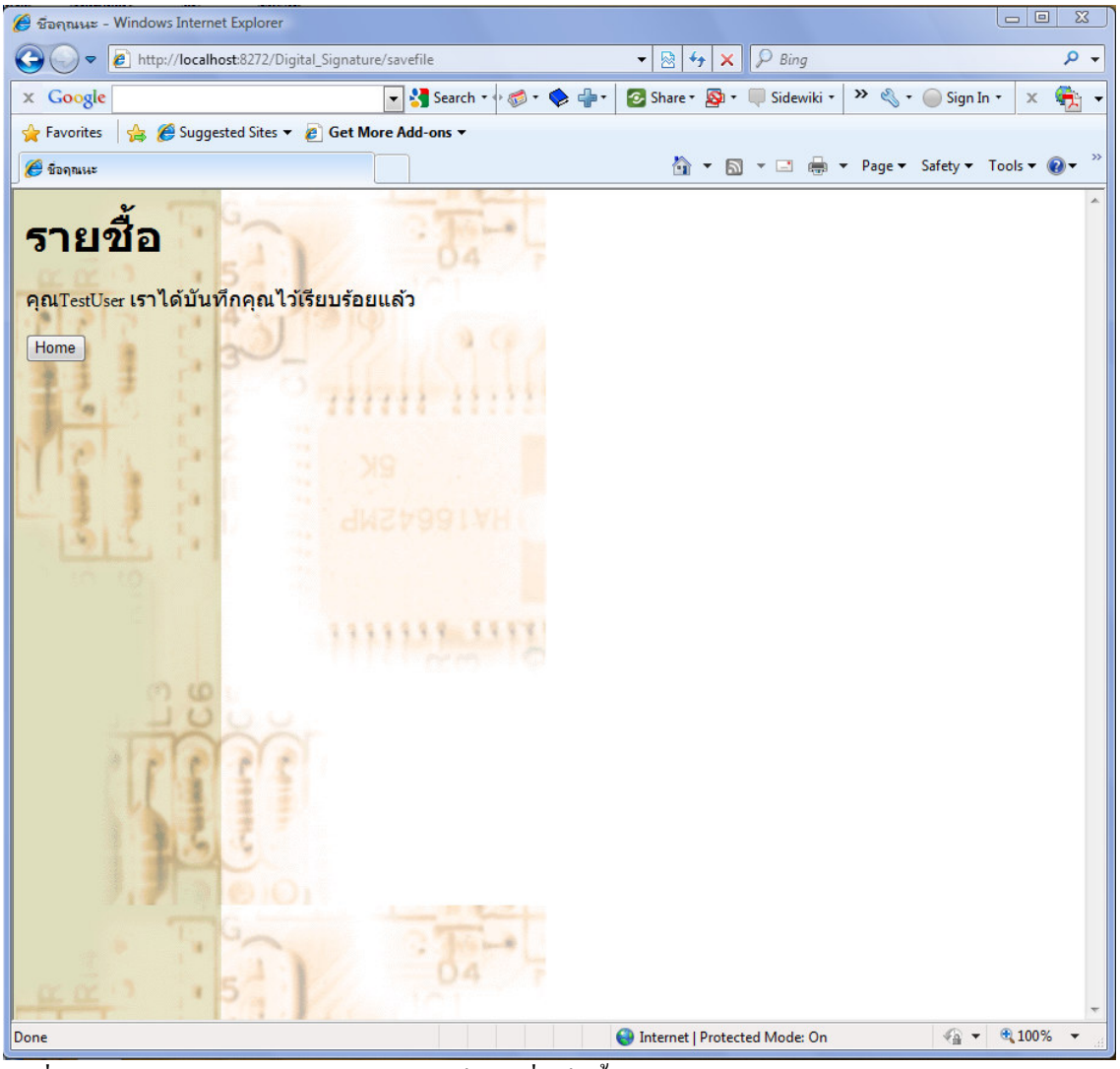
Save เพื่อบันทึกลายเซ็นมือในกรอบสี่เหลี่ยมที่เขียนไว้

Clear เพื่อลบลายเซ็นมือที่เขียนไว้ในกรอบสี่เหลี่ยม

Back to main menu เพื่อกลับไปยังหน้าเมนูหลัก

รูปที่ 3-23 หน้าต่างแสดงการเก็บบันทึกลายเซ็น

เมื่อกดปุ่ม Save ในรูปที่ 3-23 หน้าต่างใหม่จะแสดงขึ้นมาเพื่อยืนยันการบันทึกที่สมบูรณ์ของผู้ใช้งานรายนั้น สำหรับการทดลองในงานวิจัยนี้เก็บตัวอย่างลายเซ็นมือ อย่างต่อเนื่อง 10 ครั้งเพื่อใช้เป็นกลุ่มตัวอย่างที่ใช้เลือกลายเซ็นมืออ้างอิงสำหรับการตรวจสอบยืนยันต่อไป



รูปที่ 3-24 หน้าต่างแสดงผลการบันทึกลายเซ็นมือที่เสร็จสิ้นแล้ว

ต่อไปเป็นการทดสอบการตรวจสอบยืนยันผู้ใช้งาน จากรูปที่ 3-20 ในเมนูหลัก ให้ทำการกดปุ่ม Verify signature ก็จะแสดงหน้าต่างสำหรับการตรวจสอบดังแสดงในรูปที่ 3-25 ในหน้าต่างนี้จะต้องป้อนชื่อผู้ใช้งาน และเขียนลายเซ็นมือไว้ในกรอบสี่เหลี่ยม จากนั้นกดปุ่ม Verify signature เพื่อทำการตรวจสอบ ถ้าหากการเขียนลายเซ็นมือไม่สวย สามารถกดปุ่ม Clear signature เพื่อให้สามารถเขียนลายเซ็นมือใหม่

รูปที่ 3-25 หน้าต่างของการตรวจสอบยืนยันผู้ใช้งาน

หากผลการตรวจสอบเป็นที่ถูกต้อง ก็จะสามารถผ่านเข้าไปใช้งานให้เวปไซต์นี้ได้ แต่ถ้าไม่ถูกต้อง ระบบจะพากลับไปที่หน้าเมนูหลัก

3.5 กล่าวท้ายบท

เนื้อหาในบทนี้ได้ทำการอธิบายขั้นตอนการลงโปรแกรมที่ใช้พัฒนาโปรแกรมสำหรับงานวิจัยนี้ และรวมถึงการอธิบายหน้าต่างของโปรแกรมที่พัฒนาขึ้นสำหรับการเก็บค่าลายเซ็นมือ และการตรวจสอบลายเซ็นเพื่อยืนยันตัวตนของผู้ใช้งาน ผ่านระบบออนไลน์ของอินเตอร์เน็ตทั่วๆไป ซึ่งผลการทดสอบของลายเซ็นมือที่ใช้จากโปรแกรมนี้จะถูกนำเสนอ และวิเคราะห์ในบทถัดไป

บทที่ 4 ผลการทดสอบและบทวิเคราะห์

4.1 กล่าวนำ

บทนี้จะนำเสนอผลการทดสอบลายเซ็นมือที่ใช้โปรแกรมที่พัฒนาขึ้นตามที่อธิบายไว้ในบทที่ 3 ซึ่งหลักการยืนยันลายเซ็นนั้นได้ถูกอธิบายไว้ในบทที่ 2 โดยงานวิจัยนี้จะมุ่งวิเคราะห์เฉพาะวิธีการใช้เทคนิคการแปลงเชิงมุมเป็นสำคัญ สำหรับฐานข้อมูลที่ใช้ในการทดสอบนี้มาจากจำนวนทั้งหมด 300 ลายเซ็น ประกอบด้วย 100 ลายเซ็นที่ลงทะเบียนไว้จากผู้ใช้งาน 10 คน แต่ละคนเขียนลายเซ็นมือ 10 ครั้ง เพื่อใช้เลือกลายเซ็นอ้างอิง 100 ลายเซ็นของผู้ใช้งาน 10 คน แต่ละคนเขียนลายเซ็นมือ 10 ครั้ง เพื่อใช้ทดสอบยืนยันตัวตน และมีอีก 100 ลายเซ็นที่ทำหน้าที่เป็นลายเซ็นปลอมจากอาสาสมัคร 10 คน แต่ละคนเขียนลายเซ็นมือ 10 ครั้ง เพื่อทดสอบการแยกแยะความถูกต้องของลายเซ็นปลอม ในการทดสอบนี้ทั้งเซิฟเวอร์และผู้ใช้งานอยู่ในเครือข่าย LAN เดียวกัน

4.2 ผลการทดสอบจำนวนลายเซ็นต้นแบบ

โดยทั่วไปแล้วความน่าจะเป็นในการเลือกลายเซ็นมืออ้างอิงที่เหมาะสมที่สามารถใช้ตรวจสอบลายเซ็นได้อย่างน่าเชื่อถือ ขึ้นอยู่กับจำนวนของตัวอย่างในกลุ่มที่ใช้ในการเลือกนั่นเอง นอกจากนี้ระดับการตัดสินใจยังขึ้นอยู่กับการคำนวณหาค่าของ FAR และ FRR จากค่าของลายเซ็นที่ใช้ทดสอบของฐานข้อมูลที่เก็บลายเซ็นมือผู้ใช้งานไว้ ถ้าจำนวนตัวอย่างที่เก็บไว้เลือกลายเซ็นอ้างอิงน้อยการเลือกระดับตัดสินใจก็กว้างมากขึ้นทำให้การแยกแยะลายเซ็นปลอมทำไม่มีประสิทธิภาพ

ตารางที่ 4-1 แสดงถึงผลการตรวจสอบยืนยันเมื่อเปลี่ยนค่าจำนวนตัวอย่างที่เก็บมา ผลที่ได้แสดงให้เห็นว่าร้อยละของการแยกลายเซ็นที่ถูกต้อง และลายเซ็นปลอมจากฐานข้อมูลของผู้ใช้งาน ดีกว่า การใช้วิธีปลอมด้วยอาสาสมัคร หรือกล่าวได้ว่า การใช้อาสาสมัครปลอมลายเซ็นทำให้ระบบตรวจสอบความถูกต้องได้ยากขึ้น ทั้งนี้เป็นเพราะลายเซ็นปลอมจากอาสาสมัครมีความแตกต่างมากกว่าข้อมูลลายเซ็นที่เก็บไว้ในฐานจากผู้ใช้งานด้วยกันนั่นเอง

นอกจากนั้นผลในตารางที่ 4-1 ยังแสดงให้เห็นว่าจำนวนตัวอย่างที่เก็บไว้มีความสำคัญต่อความแม่นยำในการตรวจสอบ ถ้าจำนวนตัวอย่างลายเซ็นที่เก็บไว้มีมาก จะทำให้ร้อยละของความผิดพลาดน้อยลง ดังแสดงในตารางที่ 4-1

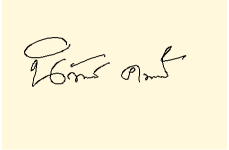
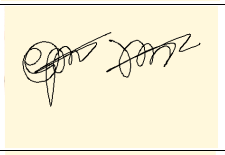
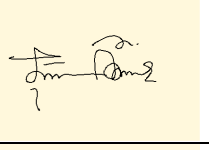
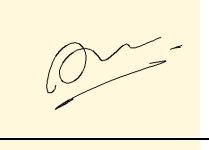
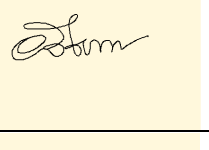
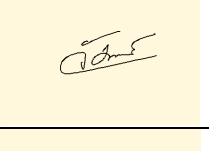
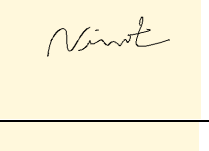
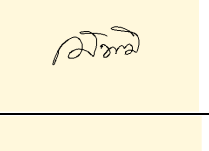
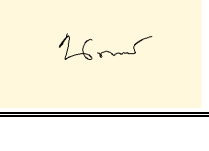
ตารางที่ 4-1 ผลการตรวจสอบยืนยันลายเซ็น เมื่อมีการเปลี่ยนแปลงจำนวนตัวอย่างลายเซ็น

Number of Training Signatures	All tested Signatures		All Forgeries	
	FRR (%)	FAR (%)	FRR (%)	FAR (%)
4	4.56	4.42	12.26	11.98
6	3.31	3.19	9.25	8.97
8	2.54	2.36	7.84	7.53
10	2.37	2.24	7.21	7.04

4.3 ผลการทดสอบการตรวจสอบยืนยันลายเซ็น

จากผลการทดสอบที่แล้ว งานวิจัยนี้เลือกใช้ค่าจำนวนตัวอย่างที่เก็บไว้เพื่อเลือกลายเซ็นอ้างอิงที่ 10 ลายเซ็น ต่อไปเป็นผลการทดสอบการยืนยันตัวตนของผู้ใช้งาน จำนวน 10 คน แต่ละคนเขียนลายเซ็น 10 ครั้ง ผลที่ได้จากทั้ง 10 คนแสดงในตารางที่ 4-2 จากผลการทดสอบพบว่าวิธีการที่เสนอใช้การแปลงเชิงมุมสามารถให้ค่าเฉลี่ยของความถูกต้องในการยืนยันถึง 95.39% นอกจากนี้ยังสังเกตได้ว่าลายเซ็นมือจากผู้ใช้งานที่มีความซับซ้อนนั้นจะให้ค่าความถูกต้องของการตรวจสอบที่ต่ำ และมีค่า FRR หรือ FAR สูง ในทางตรงกันข้าม ผู้ใช้งานที่เขียนลายเซ็นมือง่ายๆ ให้ความถูกต้องที่สูงมาก และมีค่าความผิดพลาดน้อย

ตารางที่ 4-2 ผลการตรวจสอบยืนยันลายเซ็นจากผู้ใช้งาน 10 คน

ผู้ใช้งาน	Correct (%)	FRR (%)	FAR (%)
	95.13	2.51	2.36
	97.17	1.46	1.37
	91.24	4.51	4.25
	95.28	2.44	2.28
	97.59	1.22	1.19
	91.36	4.41	4.23
	95.16	2.48	2.36
	95.72	2.21	2.07
	97.45	1.34	1.21
	97.8	1.12	1.08

4.4 ผลการทดสอบเปรียบเทียบกับวิธีอื่นๆ

เพื่อให้เห็นภาพที่ชัดขึ้นสำหรับสมรรถนะของวิธีการที่นำเสนอในงานวิจัยนี้ การเปรียบเทียบผลการทดสอบกับวิธีการตรวจสอบลายเซ็นมือแบบอื่นๆ จึงถูกนำมาพิจารณา ในงานวิจัยนี้เลือกใช้การเปรียบเทียบการแปลงเชิงมุมที่กล่าวไว้ในหัวข้อที่ 2.4 กับหลักการเปรียบเทียบที่อธิบายไว้ในหัวข้อที่ 2.3 (Basic Matching) สำหรับการแปลงเชิงมุมนั้น ผู้วิจัยได้ทำการแบ่งออกเป็นสองกรณีคือ กรณีที่ใช้การแปลงเชิงมุมเพียงอย่างเดียวโดยที่ไม่มีการแยกลายเซ็นมือนั้นออกเป็นองค์ประกอบย่อยๆ (Angular without extracting components) และกรณีที่แปลงเชิงมุมพร้อมทั้งแยกองค์ประกอบย่อยด้วย (Proposed) ซึ่งการแบ่งออกเป็นสองกรณีนี้ทำให้ทราบสมรรถนะที่แท้จริงของการแยกองค์ประกอบย่อยว่ามีส่วนช่วยในการตัดสินใจตรวจสอบที่ดีขึ้นหรือไม่ ส่วนวิธีการเปรียบเทียบนั้นจะใช้ลักษณะทั้ง 4 มาเปรียบเทียบร่วมกัน คือ ความยาวของลายเซ็นมือ ช่วงเวลาที่ใช้เขียน ขนาดของลายเซ็น และจำนวนจุดหักมุม ซึ่งทั้งหมดนี้ถูกอธิบายไว้ในหัวข้อที่ 2.3

ตารางที่ 4-3 แสดงผลการเปรียบเทียบวิธีการตรวจสอบยืนยันลายเซ็นมือด้วยวิธีต่างๆ จะเห็นได้ว่าวิธีการที่เสนอมาในงานวิจัยนี้สามารถให้ความถูกต้องในการตรวจสอบ 25.9% และ 29.5% เหนือกว่าวิธีเปรียบเทียบสำหรับกรณีที่เป็นลายเซ็นทดสอบจากผู้ใช้งาน และลายเซ็นลอมตาลำดับ นอกจากนี้วิธีการใช้การแปลงเชิงมุมโดยไม่แยกองค์ประกอบย่อยให้ความแม่นยำในการตรวจสอบน้อยกว่าการแยกองค์ประกอบย่อย นั่นแปลว่าการพิจารณาตัดสินลายเซ็นมือออกเป็นส่วนๆ ให้ผลที่ดีกว่าการพิจารณาโดยรวมเพียงครั้งเดียว

ตารางที่ 4-3 ผลการเปรียบเทียบวิธีการตรวจสอบยืนยันลายเซ็นมือด้วยวิธีต่างๆ

Methods	All tested Signatures		All Forgeries	
	FRR (%)	FAR (%)	FRR (%)	FAR (%)
Angular without extracting components	11.13	10.97	18.42	17.73
Basic matching	15.63	14.88	22.43	21.32
Proposed	2.37	2.24	7.21	7.04

4.5 กล่าวท้ายบท

การนำเสอนผลการทดสอบในบทนี้ได้แยกการพิจารณาเป็น 3 กรณีคือ กรณีที่พิจารณาจำนวนตัวอย่างของลายเซ็นมือที่ใช้เพื่อเลือกลายเซ็นอ้างอิง กรณีที่พิจารณาผลการตรวจสอบยืนยันจากผู้ใช้งาน 10 คน และกรณีที่เปรียบเทียบวิธีที่นำเสนอของงานวิจัยนี้เทียบกับวิธีอื่น ผลการวิเคราะห์พบว่างานวิจัยนี้ได้เสนอแนวทางที่น่าสนใจสำหรับการใช้ตรวจสอบยืนยันตัวตน ซึ่งมีค่าเฉลี่ยความถูกต้องอยู่ที่ 95.39%

บทที่ 5 สรุปและข้อเสนอแนะ

5.1 สรุป

งานวิจัยนี้นำเสนอการตรวจสอบยืนยันตัวตนจากลายเซ็นมือด้วยการใช้วิธีการแปลงเชิงมุมสำหรับนำไปประยุกต์ใช้กับบริการ e-Commerce เพื่อป้องกันการปลอมแปลงและเพิ่มความน่าเชื่อถือให้กับการทำธุรกรรมทางอินเตอร์เน็ต โดยหลักการที่เสนอประกอบด้วยการเปลี่ยนพิกัดของลายเซ็นมือเป็นค่าบนโดเมนเชิงมุม จากนั้นจะนำไปหาค่าหน่วงเวลาเพื่อใช้ตรวจสอบต่อไป ข้อสังเกตที่น่าสนใจของการแปลงเชิงมุมนี้คือการแยกองค์ประกอบย่อยของลายเซ็น โดยสังเกตจากมุมที่ไม่ต่อเนื่องทำให้การพิจารณาลายเซ็นมือมีความซับซ้อนมากขึ้น ซึ่งความซับซ้อนนี้นำไปสู่ความแม่นยำในการตรวจสอบที่ดีขึ้นด้วย

สำหรับหลักการตรวจสอบยืนยันที่เสนอในงานวิจัยนี้มีกระบวนการและขั้นตอนดังนี้

1. กระบวนการประมวลลายเซ็นด้วยการแปลงเชิงมุม

เป็นกระบวนการแปลงลายเซ็นเพื่อให้อยู่ในรูปแบบข้อมูลเชิงมุม ซึ่งมีสองขั้นตอนดังนี้ ขั้นตอนการแปลงเชิงมุมและขั้นตอนการหาค่าหน่วงเวลา

2. กระบวนการยืนยันลายเซ็น

เป็นกระบวนการยืนยันลายเซ็นจากกลุ่มของลายเซ็นที่บันทึกไว้ในฐานข้อมูล มีขั้นตอนหลักดังนี้ ขั้นตอนการเก็บตัวอย่าง ขั้นตอนการเลือกลายเซ็นอ้างอิง ขั้นตอนการเลือกระดับค่าหน่วงเวลา และขั้นตอนการตัดสินใจ

งานวิจัยนี้ได้พัฒนาโปรแกรมที่สามารถใช้งานจริงผ่านเครือข่ายอินเตอร์เน็ตและสามารถใช้กับโปรแกรมท่องอินเตอร์เน็ตใดๆ ก็ได้ ทำให้สะดวกในการนไปประยุกต์ติดตั้งกับเวปไซต์เดิมที่มีอยู่

สำหรับการทำงานของโปรแกรมที่พัฒนาขึ้นมีส่วนหลักๆ ดังนี้

1. การเพิ่มผู้ใช้งาน จะมีปุ่มที่ใช้สำหรับผู้ใช้งานที่ยังไม่เลยลงทะเบียนในงานเป็นครั้งแรก
2. การยืนยันตัวตนผู้ใช้งาน ใช้สำหรับการตรวจสอบยืนยันลายเซ็นเพื่อเข้าใช้งานในเวปนี้ต่อไป
3. การแก้ไขข้อมูลของผู้ใช้งาน ใช้แก้ไขข้อมูล หรือลายเซ็นมือของผู้ใช้งาน

5.2 ข้อแสนอแนะ

โครงการวิจัยนี้มีวิธีการที่สามารถตรวจสอบยืนยันลายเซ็นมือออนไลน์ที่สามารถใช้งานได้จริง แต่วิธีการที่นำเสนอนั้นให้ผลความถูกต้องที่ 95.39% เท่านั้น ผลความถูกต้องนี้อาจยอมรับได้สำหรับเวปไซต์ที่มีความสำคัญไม่มากนัก แต่ถ้าเป็นเวปไซต์ที่สำคัญมากๆ จำเป็นต้องเพิ่มระดับความแม่นยำนี้มากขึ้น ผู้วิจัยจึงขอเสนอแนะให้ใช้แนวทางการตรวจสอบด้วยการแปลงเชิงมุมนี้ แต่เพิ่มกระบวนการตัดสินใจด้วยการใช้อัลกอริทึมตัดสินใจแบบไม่เป็นเชิงเส้น เช่นการรู้จำแบบ การใช้เครือข่ายปรับตัว เพื่อเพิ่มประสิทธิภาพการตรวจสอบให้ดีขึ้น

บรรณานุกรม

[1] M. Fairhurst, K. Cowley, and E. Sweeney, “KAPPA Automatic Signature Verification: Signature Verification Public Trials and Public Survey on Biometrics,” British Technology Group, Tech. Rep., 1994.

[2] C.-C. Hsu, L.-F. Chen, P.-C. Chang, and B.-S. Jeng, “On-line chinese signature verification based on multi-expert strategy,” in Proc. 32nd Int. Carnahan Conf. Security Technology, 1998, pp. 169–173.

[3] R. Plamondon and G. Lorette, “Designing an automatic signature verifier: Problem definition and system description,” in Computer Processing of Handwriting, R. Plamondon and C. G. Leedham, Eds. Singapore: World Scientific, 1990, pp. 3–20.

[4] S. H. Kim, M. S. Park, and J. Kim, “Applying personalized weights to a feature set for on-line signature verification,” in Proc. 3rd Int. Conf. Document Analysis and Recognition,Montreal, QC, Canada, Aug. 1995, pp. 882–885.

[5] Y. Sato and K. Kogure, “On-line signature verification based on shape, motion, and writing pressure,” in Proc. IEEE Int. Conf. Pattern Recognition, vol. 2, 1982, pp. 823–826

[6] L. L. Lee, T. Berger, and E. Aviczer, “Reliable on-line human signature verification systems,” IEEE Trans. Pattern Anal. Machine Intell., vol. 18, no. 6, pp. 643–647, Jun. 1996.

[7] J. R. Yu, S. H. Kim, and J. Kim, “A class learning method for signature verification using dynamic programming,” J. Korea Inst. Telemat. Electron., vol. 32-B, no. 2, pp. 154–161, 1995.

[8] B. Wirtz, “Stroke-based time warping for signature verification,” in Proc. Int. Conf. Document Analysis and Recognition, vol. 1, 1995, pp. 179–182.

[9] J. G. A. Dolfing, “A comparison of ligature and contextual models for hidden Markov models based on on-line handwriting recognition,” in Proc. Int. Conf. Acoustics, Speech, and Signal Processing, vol. 2, 1998, pp. 1073–1076.

[10] M. Fuentes, S. Garcia-Salicetti, and B. Dorizzi, “On Line Signature Verification: Fusion of a Hidden Markov Model and a Neural Network via a Support Vector Machine,” Proc. Eighth Int’l Workshop Frontiers in Handwriting Recognition, 2002, pp. 253-258, Aug. 2002.

[11] J. G. A. Dolfing, “Handwriting recognition and verification: A hidden Markov approach,” Ph.D. dissertation, Technische Universiteit Eindhoven, Eindhoven, The Netherlands, 1998.

[12] N.-J. Cheng, K. Liu, K.-C. Cheng, C.-C. Tseng, and B.-S. Jeng, “On-line chinese signature verification using voting scheme,” in Proc. 31st Annu IEEE Int. Carnahan Conf. Security Technology, 1997, pp. 123–126.

[13] A. Kandel, Fuzzy Techniques in Pattern Recognition. New York: Wiley, 1982.

[14] M. Nadler and E. Smith, Pattern Recognition Engineering. New York: Wiley, 1993, pp. 299–302.

[15] http://www.securecomputing.com/index.cfm?sKey=665

[16] http://www.altisinc.com/Biometric/techniques.html

ภาคผนวก

ภาคผนวก ก

การเผยแพร่ผลงานวิจัย

บทความวิจัยที่ได้รับการตีพิมพ์เผยแพร่ในวารสารวิชาการนานาชาติ

P. Uthansakul and M. Uthansakul, "Online Signature Verification using Angular Transformation for e-Commerce Services," International Journal of Information and Communication Engineering, Volume 6, Number 1, Pages 33-38, 2010.

ส่วนหนึ่งของผลงานวิจัยที่ได้รับรางวัลในการประกวดสิ่งประดิษฐ์

รางวัลชนะเลิศอันดับที่ 2 ประเภทอุปกรณ์คอมพิวเตอร์ เรื่อง โปรแกรมรักษาความปลอดภัยด้วยลายเซ็นมืออิเล็กทรอนิกส์สำหรับธุรกรรมอิเล็กทรอนิกส์ ใน การประกวดสิ่งประดิษฐ์ ประจำปี 2552 วันที่ 18-19 สิงหาคม 2552 ณ อาคารสุรพัฒน์ 2

รางวัลชนะเลิศอันดับที่ 2 ประเภทอุปกรณ์คอมพิวเตอร์ เรื่อง โปรแกรมรักษาความปลอดภัยด้วยลายเซ็นมืออิเล็กทรอนิกส์ ใน การประกวดสิ่งประดิษฐ์ ประจำปี 2551 วันที่ 18-19 สิงหาคม 2551ณ อาคารสุรพัฒน์ 2

ภาคผนวก ข

บทความวิจัยที่ได้รับการตีพิมพ์

International Journal of Information and Communication Engineering 6:1 2010

Online Signature Verification Using Angular Transformation for e-Commerce Services

Peerapong Uthansakul and Monthippa Uthansakul

***Abstract*—**The rapid growth of e-Commerce services is significantly observed in the past decade. However, the method to verify the authenticated users still widely depends on numeric approaches. A new search on other verification methods suitable for online e-Commerce is an interesting issue. In this paper, a new online signature-verification method using angular transformation is presented. Delay shifts existing in online signatures are estimated by the estimation method relying on angle representation. In the proposed signature-verification algorithm, all components of input signature are extracted by considering the discontinuous break points on the stream of angular values. Then the estimated delay shift is captured by comparing with the selected reference signature and the error matching can be computed as a main feature used for verifying process. The threshold offsets are calculated by two types of error characteristics of the signature verification problem, False Rejection Rate (FRR) and False Acceptance Rate (FAR). The level of these two error rates depends on the decision threshold chosen whose value is such as to realize the Equal Error Rate (EER; FAR = FRR). The experimental results show that through the simple programming, employed on Internet for demonstrating e-Commerce services, the proposed method can provide 95.39% correct verifications and 7% better than DP matching based signature-verification method. In addition, the signature verification with extracting components provides more reliable results than using a whole decision making.

***Keywords*—**Online signature verification, e-Commerce services, Angular transformation.

I. Introduction

RECENTLY, the growth of purchasing merchandises via electronic online services so-called e-Commerce has been rapidly driven by huge user demand. However, the technology of user authorization is still based on numeric or alphabet methods such as credit cards, user name and password. These methods are simple to implement but along with ease of frauds. There is an increasing interest in reliable identity verification. Several biometric features have been studied and proved useful, including signature, fingerprint, face, speech, iris, and retina pattern [1]-[2]. These biometric features have advantages over conventional keys or personal identification numbers (PINs) and passwords in that they are free from carriage and memorization problems. However, because most biological characteristics are unchangeable, a more serious problem arises when they are duplicated. Hence, one will hesitate to use the disclosed biological features. The online signature is more robust to the copy problem than other biological features in that it has dynamic characteristics in addition to the morphological characteristics while the others generally provide only the morphological characteristics [3]-[5]. As one can expect, it is very difficult to construct a similarly shaped signature that also contains dynamic features simultaneously. Moreover, one can change his or her signature intentionally in case of security leakage. Because of the dynamic characteristics of online signatures, identical parts of signatures appear at different times. Then there exist delay shifts in signature. In the parametric approaches, they used global features that are not greatly affected by the nonlinear delay shifts [6]. Using only global features has the advantage of being very fast, but the error rates are generally high.

The functional approaches represent the signature signal as a function of time and compare the similarity by accumulating the difference between two functions in time. The delay relationship between two functions is established by the dynamic programming (DP) matching method [7] or hidden Markov Models (HMMs) [8]-[11]. In the DP matching methods, they tried to find the exact matching points between signatures by means of searching which resulted in too much computation. In the HMM methods, much effort was spent on selecting the type of Markov models, and much computation power was used in enrollment procedures for training the models. Recently, to get higher security, hybrid approaches that use more than one kind of feature have been researched [12]. While they acquire very low error rates, the processing time seems to increase.

In this paper, we propose a new method for extracting signature components by considering angle representation in time. This method splits a global delay shifts into many delay shifts for each component. Therefore, it reduces error rate acquisitions when combining verification results of all components. The other advantage of angular transformation is that it reduces the data size of transmission on Internet connection because only angle characteristics are sent from client to server instead of both vertical and horizontal characteristics. In the proposed method, the estimated delay is captured by comparing with the selected reference signature and the error matching can be computed as a main feature used for verifying process. The threshold offsets are calculated by two types of error characteristics of the signature verification

The authors are with the School of Telecommunication Engineering, Suranaree University of Technology, Nakhon Ratchasima, Thailand 30000 (corresponding author phone: 66-44-224351; fax: 66-44-224603; e-mail: uthansakul@sut.ac.th).

This work is financially supported by Suranaree University of Technoogy.

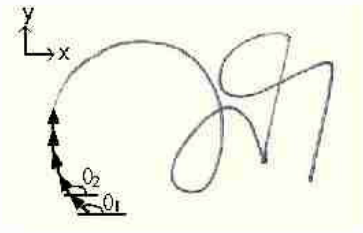


Fig. 1 Demonstration of angular transformation

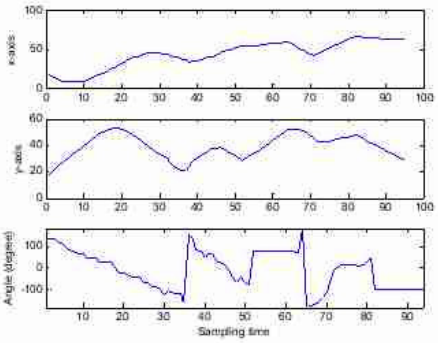


Fig. 2 Features of signature in (a) horizontal axis (b) vertical axis (c) angle representation

problem, False Rejection Rate (FRR) and False Acceptance Rate (FAR). The level of these two error rates depends on the decision threshold chosen whose value is such as to realize the Equal Error Rate (EER; FAR = FRR). All experiments are tested through existing Internet connection. Own developed programming based Java Servlet is employed.

In particular, the contributions of this paper are i) the concept of using angular transformation for online signature verification ii) the verification process using many decidion making from extracted components and iii) its performances through real-time Internet applications in comparing with other methods. The remainder of paper is organized as follows. In the following section, we describe the online signature processing including angular transformation and error-delay estimations. Section III provides the details of programming for e-Commerce services and then the verification procedure through such a program is described in Section IV. After showing the experimental results in Section V, we conclude in Section VI.

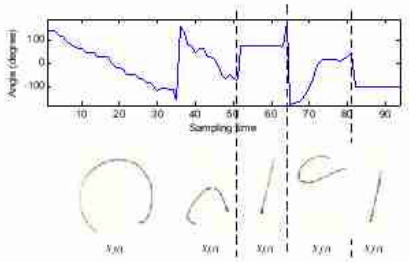


Fig. 3 Example of extracting components from angle representation

II. Online Signature Processing

A. Angular Transformation

In general, the handwriting signature are captured and represented in 2 dimensions, horizontal and vertical axes. For angular transformation, the domain considered instead of both axes is the angle domain which is calculated by slope from one captured point to another. The example of angular transformation is shown in Fig. 1. Fig. 2 presents the value of signature in term of horizontal, vertical and angular values in time. For proposed technique, only angular values of signature are transmitted from client to server. Hence, it saves some overheads due to reducing the size of signature feature.

As seen in Fig. 2(c), the plot of angular representation has many discontinuous points. These positions indicate two meanings, sharp tip and crossing pi. For sharp tip, it is the position when stroke of signature is started. The other discontinuous potion is a crossing pi because it is occurred when angular value is changing between opposite sign at 180 degree. Both meanings are helpful for angular transformation to extract signature into many components. The example of extraction is illustrated in Fig. 3 and expressed in (1).

$$S(t) = \sum_{i=1}^{M} S_i(t) \tag{1}$$

where M is the total components of signature, $S(t)$ is the angular representation of handwriting signature and $S_i(t)$ is the ith components of $S(t)$ which is defined by

$$S_i(t) = \begin{cases} S(t) & ts_i \le t \le te_i \\ 0 & elsewhere \end{cases} \tag{2}$$

where ts_i is the starting time of ith component and te_i is the ending time of ith comoponent.

B. Delay and Error Estimations

The angular transformation has been done in the client side and sent to server. After extracting all components by server,

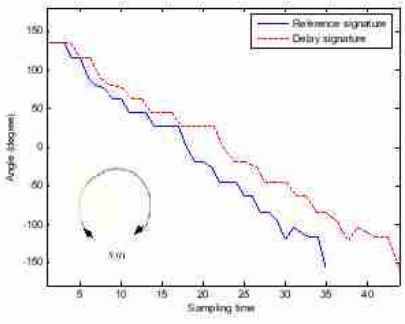


Fig. 4 Comparison between reference and delay signatures of first component shown in Fig. 3

the next process is to estimate delay shift and then calculate the errors. For online system, the time usage of writing signature becomes the most important information to be used for verifying process. This value is uniquely different from offline verification because the offline system cannot capture this delay time. In this paper, the linear approximation is applied to estimate the delay.

Fig. 4 shows the angular values of the first component presented in Fig. 3. The reference signature is the selected prototype used for comparing with testing signature. The method to choose reference signature will be described in the next section. As seen in Fig. 4, both signature have a similar trend but spreading by different times. Hence the delay shift d_i of ith component can be defined as

$$S_i^d(t) = S_i^r(d_i t) \tag{3}$$

where $S_i^r(t)$ is the ith component of reference signature and $S_i^d(t)$ is the ith component of delay signature.

To illustrate the relation between reference and delay signatures, the time intervals of both signatures are necessary to be investigated. Fig. 5 presents time intervals of first components given in Fig. 4. It is clearly seen that the slope of Fig. 5 is approximately defined by delay shift d_i. Using linear approximation shown in (4), then the delay shift can be easily estimated.

$$d_i = \min_{d_i}\left\{\sum_{t_i^r}\left|t_i^d - d_i t_i^r\right|^2\right\} \tag{4}$$

After estimating the delay shift, the estimated signature by compensating the delay shift can be expressed as

$$\tilde{S}_i^d(t) = S_i^d(t/d_i) \tag{5}$$

Fig. 6 shows the comparison between the first components of reference and estimated signatures derived by signatures presented in Fig. 4. It is noticed that there is some errors

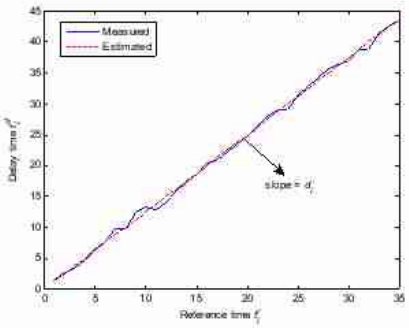


Fig. 5 Approximating the delay shift by slope of estimated line

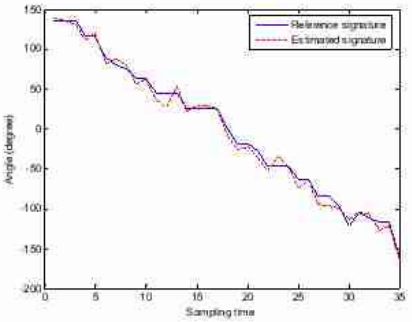


Fig. 6 Comparison between reference and estimated signatures

between them which summation of square errors can be expressed by

$$e_i = \sum_t\left|\tilde{S}_i^d(t) - S_i^r(t)\right|^2 \tag{6}$$

III. PROGRAMMING FOR E-COMMERCE SERVICES

This paper aims to implement the proposed technique for e-Commerce services. Therefore, the platform to support this idea are simulated by own developing program. In this paper, the Java Servlet is used to program both client and server interfaces. Fig. 7 demonstrates the connection between client and server for online verification. For client, the tablet pen mouse is attached to make a signature writing more comfortable. After digital handwriting signature is transformed into angular domains, the client program will transmit this data to server side through normal TCP/IP protocol in which any internet browser can be used.

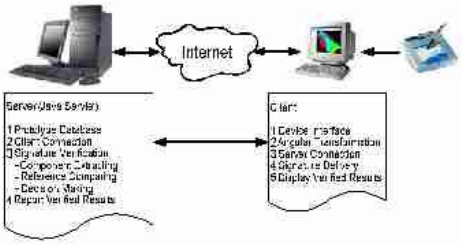


Fig.7 Connection between server and client

For server side, all training signatures are collected in the database for comparing with the data transmitted by client. Only matched signature will be authorized into the other section of web site otherwise the rejection will be transmitted back to client. Fig. 8 illustrated a program screen at client side opened by internet explorer.

IV. Verification Procedures

A. Signature Input Interface

Signatures are input by using a commercial electronic pencil and a tablet. The apparatus used in the experiments samples horizontal and vertical positions 150 times per second. The low-pass filtering and the size and direction normalization are applied on the input signature signals. The feature profile is extracted from the preprocessed input signal. All captured features are performed by Java programming.

B. Angular Transformation

An angular transformation is applied to the signature feature profile at client side. As described earlier, the delay shift estimation can be calculated by comparing with the reference signature. However, only server has these references, the process of estimating delay shift is carried out at server. Using only this angular feature, the component extraction is easily performed by considering the discontinuous point in time. By extracting process, the server can categorize signatures by number of components M. This can improve the speed of cross check between similar signature features. In addition, it can increase the quality of verification by M time examinations.

C. Selection of Reference Signature

One authorized user has been request to input multiple N signatures when registering. In this paper only one reference signature is chosen from those registered signatures. However, the criteria to choose reference signature depends on the delay shift and error estimations. The average value of delay shift and error estimations when use each registered signatures as a referenced signature among those N signatures can be expressed by

$$d_l(k) = \frac{1}{N-1}\sum_{l}^{N-1}\arg\left\{\min_{d_l(k,l)}\left\{\sum_{t}\left|t_l^l - d_l(k,l)t_t^k\right|^2\right\}\right\} \quad (7)$$

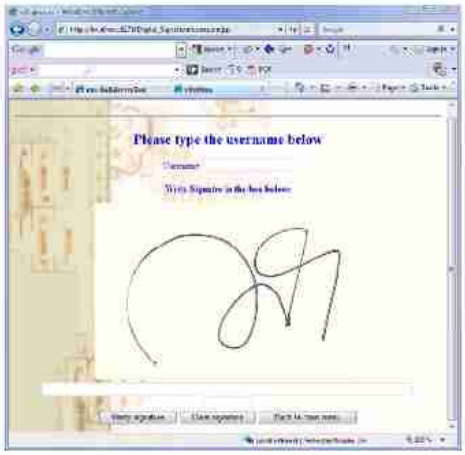


Fig. 8 Example of screen short at the client side to input the signature

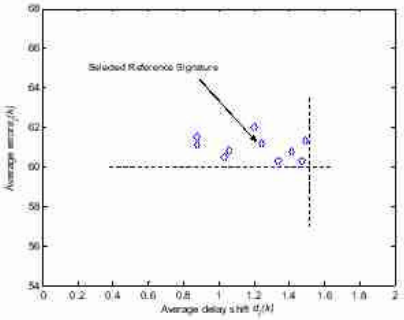


Fig. 9 Selecting reference signature

$$e_l(k) = \frac{1}{N-1}\sum_{l}^{N-1}\sum_{t}\left|\bar{S}_t^l(t) - S_t^k(t)\right|^2 \quad (8)$$

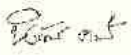
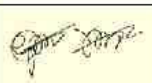
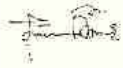
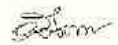
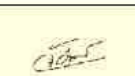
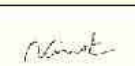
where $k, l = 1,\ldots,N$ and $k \neq l$

Fig. 9 presents the example of average delay shift and average errors from 10 registered signatures. The reference signature is selected from the one closest to the center.

D. Selection of Delay and Error Thresholds

For each authorized client, verification learning is done only on registered signatures. The server approximates, during the verification phase, the score of the signature. Signature verification for client I was performed using a decision

TABLE II
SIGNATURE VERIFICATION RESULTS FOR 10 CLIENTS

Client	Correct (%)	FRR (%)	FAR (%)
	95.13	2.51	2.36
	97.17	1.46	1.37
	91.24	4.51	4.25
	95.28	2.44	2.28
	97.59	1.22	1.19
	91.36	4.41	4.23
	95.16	2.48	2.36
	95.72	2.21	2.07
	97.45	1.34	1.21
	97.8	1.12	1.08

V. EXPERIMENTS AND RESULTS

The dataset used in the experiment is composed of 300 signatures produced by 10 clients writing 20 registered/tested signatures and 100 forgery signatures forged by 10 volunteers. The server and client are on the same local area network. The proposed signature-verification algorithm was implemented with Java Servlet compiler. We compared the performance of the proposed algorithm with a DP matching-based functional approach [7] which was developed by one of the authors. The DP matching-based method selects multiple prototypes by using ISODATA clustering algorithm.

TABLE III
COMPARISON WITH OTHER METHODS

Methods	All tested Signatures		All Forgeries	
	FRR (%)	FAR (%)	FRR (%)	FAR (%)
Angular without extracting components	11.13	10.97	18.42	17.73
DP matching	9.46	9.29	15.09	14.76
Basic matching	15.63	14.88	22.43	21.32
Proposed	2.37	2.24	7.21	7.04

TABLE I
SIGNATURE VERIFICATION RESULTS FOR NUMBER OF TRAINING SIGNATURES

Number of Training Signatures	All tested Signatures		All Forgeries	
	FRR (%)	FAR (%)	FRR (%)	FAR (%)
4	4.56	4.42	12.26	11.98
6	3.31	3.19	9.25	8.97
8	2.54	2.36	7.84	7.53
10	2.37	2.24	7.21	7.04

A. Number of Training Signatures

It is natural that the possibility of selecting an appropriate reference signature increases as the number of training samples increases. In addition, because the decision threshold is computed from FAR and FRR among the tested signatures, if the number of training samples is too small, selecting the decision boundary for deciding authentic or forged signatures will also be difficult.

Table I shows the verification results when increasing number of training signatures. The results from all registered signatures are better than forgeries. This is because the forgery signatures have more variety features than registered clients.

B. Verification Results

Table II presents the verification results of 10 clients for 10 training signatures. The proposed technique can offer average 95.39% correct verification. It is also noticed that the complex signatures provide low correct rate and high FRR/FAR.

C. Comparison with Other Methods

To illustrate the performance of our proposed method, we compared the results with other approaches which are the angular transformation without extracting components, DP

matching [7] and basic matching methods. For proposed method, the decision making is done under the conclusion of all components extracted from signature. However, it is interesting to see whether only one feature without extraction produces the different results or not. For basic matching method, we use four combinations of signature's length, time, size and number of turning curve.

Table III presents the comparison results between proposed method and others. The proposed method can provide 7% and 7.7% better than DP matching based signature-verification method for all tested signatures and forgeries respectively. In addition, the signature verification with extracting components offers more reliable verification results than using a whole decision making. This is because the use of component extraction can screen dissimilarities of other signatures before making a decision. As seen in Table III, it is obvious that the basic matching approach is the worst verification but it needs, however, the least complexity for implementation.

VI. Conclusion

In this paper, we propose an online signature verification using angular transformation for e-Commerce services. To more effectively avoid the copy problem, the angular features of signatures in the form of delay shifts are examined. In addition, it is easy for angular feature to extract a whole signature into many components so the decision making has to be relied on individual judgment of each component. This procedure increases the verification correction rate. By own developing server-client program, the verification results are able to collect through Internet connection. Experimental results show that the proposed method could compare more accurate than other approaches.

References

[1] M. Fairhurst, K. Cowley, and E. Sweeney, "KAPPA Automatic Signature Verification: Signature Verification Public Trials and Public Survey on Biometrics," British Technology Group, Tech. Rep., 1994.

[2] C.-C. Hsu, L.-F. Chen, P.-C. Chang, and B.-S. Jeng, "On-line chinese signature verification based on multi-expert strategy," in Proc. 32nd Int. Carnahan Conf. Security Technology, 1998, pp. 169–173.

[3] R. Plamondon and G. Lorette, "Designing an automatic signature verifier: Problem definition and system description," in Computer Processing of Handwriting, R. Plamondon and C. G. Leedham, Eds. Singapore: World Scientific, 1990, pp. 3–20.

[4] S. H. Kim, M. S. Park, and J. Kim, "Applying personalized weights to a feature set for on-line signature verification," in Proc. 3rd Int. Conf. Document Analysis and Recognition,Montreal, QC, Canada, Aug. 1995, pp. 882–885.

[5] Y. Sato and K. Kogure, "On-line signature verification based on shape, motion, and writing pressure," in Proc. IEEE Int. Conf. Pattern Recognition, vol. 2, 1982, pp. 823–826.

[6] L. L. Lee, T. Berger, and E. Aviczer, "Reliable on-line human signature verification systems," IEEE Trans. Pattern Anal. Machine Intell., vol. 18, no. 6, pp. 643–647, Jun. 1996.

[7] J. R. Yu, S. H. Kim, and J. Kim, "A class learning method for signature verification using dynamic programming," J. Korea Inst. Telemat. Electron., vol. 32-B, no. 2, pp. 154–161, 1995.

[8] B. Wirtz, "Stroke-based time warping for signature verification," in Proc. Int. Conf. Document Analysis and Recognition, vol. 1, 1995, pp. 179–182.

[9] J. G. A. Dolfing, "A comparison of ligature and contextual models for hidden Markov models based on on-line handwriting recognition," in Proc. Int. Conf. Acoustics, Speech, and Signal Processing, vol. 2, 1998, pp. 1073–1076.

[10] M. Fuentes, S. Garcia-Salicetti, and B. Dorizzi, "On Line Signature Verification: Fusion of a Hidden Markov Model and a Neural Network via a Support Vector Machine," Proc. Eighth Int'l Workshop Frontiers in Handwriting Recognition, 2002, pp. 253-258, Aug. 2002.

[11] J. G. A. Dolfing, "Handwriting recognition and verification: A hidden Markov approach," Ph.D. dissertation, Technische Universiteit Eindhoven, Eindhoven, The Netherlands, 1998.

[12] N.-J. Cheng, K. Liu, K.-C. Cheng, C.-C. Tseng, and B.-S. Jeng, "On-line chinese signature verification using voting scheme," in Proc. 31st Annu IEEE Int. Carnahan Conf. Security Technology, 1997, pp. 123–126.

[13] A. Kandel, Fuzzy Techniques in Pattern Recognition, New York: Wiley, 1982.

[14] M. Nadler and E. Smith, Pattern Recognition Engineering. New York: Wiley, 1993, pp. 299–302.

Peerapong Uthansakul (M'07) received B.Eng and M.Eng degrees from Chulalongkorn University, Thailand in 1996 and 1998, respectively. In 1998-2000, he worked as Telecommunication Engineer with Telephone Organization of Thailand (TOT) and then he has joined Suranaree University of Technology since 2000. During 2003-2007, he studied PhD at University of Queensland, Australia, in the area of wireless communications especially MIMO technology.

He currently works as Assistant Professor in school of Telecommunication Engineering, Faculty of Engineering, Suranaree Unviersity of Technology, Thailand. He wrote 1 book entitled Adaptive MIMO Systems: Explorations for Indoor Wireless Communications (also available on amazon.com) and he has published more than 60 referee journal and conference papers. His current research interests include MIMO, OFDM, WiMAX and Wireless Mesh Network.

Dr. Uthansakul received 2005 Best Student Presentation Prize winner at the 9th Australian Symposium on Antennas, Sydney, 16-17 February 2005, Australia and 2004 Young Scientist Travel Grant winner at the 2004 International Symposium on Antenna and Propagation, 17-21 August 2004, Japan.

Monthippa Uthansakul (M'07) received B.Eng degree from Suranaree University of Technology, Thailand, in 1997 and M.Eng degrees from Chulalongkorn University, Thailand in 1999. She has joined Suranaree University of Technology since 1999. During 2003-2007, she studied PhD at University of Queensland, Australia, in the area of smart antenna especially wideband beamforming.

She currently works as Assistant Professor in school of Telecommunication Engineering, Faculty of Engineering, Suranaree Unviersity of Technology, Thailand. She wrote 1 book chapter entitled Wideband smart antenna avoiding tapped-delay lines and filters in Handbook on Advancements in Smart Antenna Technologies for Wireless Networks, Idea Group Publishing, USA, 2008 and she has published more than 50 referee journal and conference papers. Her current research interests include antenna array processing, compact switched beam antenna and body communications.

Dr. Uthansakul received Young Scientist Contest 2nd Prize at 16th International Conference on Microwaves, Radar and Wireless Communications, Krakow, Poland, 22-24 May 2006.

ประวัติผู้วิจัย

ผู้ช่วยศาสตราจารย์ ดร. พีระพงษ์ อุฑารสกุล สำเร็จการศึกษาหลักสูตรวิศวกรรมศาสตรบัณฑิต และวิศวกรรมศาสตรมหาบัณฑิตจากจุฬาลงกรณ์มหาวิทยาลัย เมื่อ พ.ศ. 2539 และ 2541 จากนั้นเข้าทำงานในตำแหน่งวิศวกรระบบโทรคมนาคมที่องค์การโทรศัพท์แห่งประเทศไทย จนกระทั้ง พ.ศ. 2543 จึงได้ย้ายมาเป็นอาจารย์ประจำสาขาวิชาวิศวกรรมโทรคมนาคม สำนักวิชาวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีสุรนารี และได้ลาศึกษาต่อระดับปริญญาเอกตั้งแต่ปี พ.ศ. 2546 ณ University of Queensland, Australia เมื่อ พ.ศ. 2549 จึงได้กลับเข้ามาปฏิบัติหน้าที่อาจารย์ตามเดิม ผู้วิจัยมีเชี่ยวชาญในด้านระบบ MIMO, Information Theory, Signal Processing, Radio Wave Modelling, Mobile Communication, Advance Wireless Communication ปัจจุบันมีบทความวิจัยตีพิมพ์เผยแพร่ในวารสารวิชาการ 21 บทความ และในการประชุมวิชาการ 60 บทความ หนังสือวิชาการในประเทศ 1 เล่มและต่างประเทศ 1 เล่ม มีลิขสิทธิ์ 1 รายการและ สิทธิบัตร 1 รายการ

ผู้ช่วยศาสตราจารย์ ดร. พีระพงษ์ อุฑารสกุล ได้รับรางวัล Young Scientist Travel Grant Award จากงานประชุมวิชาการนานาชาติ International Symposium on Antenna Propagation ปี พ.ศ. 2547 ณ ประเทศญี่ปุ่น และได้รับรางวัล Best Student Presentation Award จากงานประชุมวิชาการนานาชาติ Australian Symposium on Antanna ปี พ.ศ. 2548 ณ ประเทศออสเตรเลีย ในปี พ.ศ. 2553 ผู้ช่วยศาสตราจารย์ ดร. พีระพงษ์ อุฑารสกุล ได้รับรางวัลพนักงานดีเด่น ด้านการวิจัย สำหรับนักวิจัยรุ่นใหม่ จากมหาวิทยาลัยเทคโนโลยีสุรนารี