

การสร้างความมั่นคงปลอดภัยให้เอกสารกระดาษโดยใช้ลายมือชื่อดิจิทัลและรหัสคิวอาร์

Secure Paper-based Document using Digital Signature and QR Code

เมฆินทร์ วรรณศาสตร์ และ ปราโมทย์ ก้วเจริญ

สาขาวิทยาการคอมพิวเตอร์ คณะสถิติประยุกต์ สถาบันบัณฑิตพัฒนบริหารศาสตร์

118 ถนนเสรีไทย แขวงคลองจั่น เขตบางกะปิ กรุงเทพฯ 10240

maykin.w@grads.nida.ac.th, pramote@as.nida.ac.th

Abstract

There are still needs for paper-based documents in certain circumstances where electronic documents cannot efficiently replace them. For example, documents issued by the government such as birth certificates, driver licenses, and passports must be paper-based. With advanced scanning and printing technologies, document fraud can easily be conducted without significant high cost. In this paper, an implementation of secure paper-based documents is presented. The integrity of the text message and the author of the document can be verified with the use of a digital signature and QR code. The proposed method is semi-automatic in that it requires the user to compare the text message on the paper and the one obtained from the QR code; however, this method does provide convenience for the user in dealing with a large amount of documents.

Keywords: Paper-based Document, Digital Signature, QR Code, Authentication

บทคัดย่อ

เอกสารที่อยู่ในรูปของกระดาษ (Paper-based Document) ยังคงมีความจำเป็นในงานบางประเภทที่เทคโนโลยีเอกสารอิเล็กทรอนิกส์ (E-Document) ยังไม่สามารถทดแทนได้อย่างมีประสิทธิภาพ เช่น สูติบัตร ใบอนุญาตขับขี่ หรือหนังสือเดินทาง เป็นต้น กอปรกับเทคโนโลยีขั้นสูงทางการสแกนและการพิมพ์ที่ถูกนำไปใช้เพื่อการฉ้อโกงในปัจจุบันนั้นมีราคาที่ไม่สูงและการจัดหาทำได้ไม่ยาก จึงเป็นที่มาของงานวิจัยเพื่อการออกแบบวิธีการในการสร้างความมั่นคงให้กับเอกสารที่มีกลไกการพิสูจน์ตัวตนจริง (Authentication) ข้อความบนเอกสารว่าเป็นของผู้ที่ได้กล่าวอ้างว่าเป็นผู้ส่งจริง และไม่ได้ถูกแก้ไขโดยผู้ที่ไม่มีความสิทธิในระหว่างการขนส่ง โดยการใช้ประโยชน์

ของเทคโนโลยีลายมือชื่อดิจิทัล (Digital Signature) และรหัสคิวอาร์ (QR Code) ที่สามารถทำงานแบบกึ่งอัตโนมัติในการเปรียบเทียบข้อความบนเอกสารกับข้อความจากรหัสคิวอาร์โดยผู้ใช้งาน ซึ่งเป็นการอำนวยความสะดวกให้กับระบบงานที่ต้องเกี่ยวข้องกับเอกสารเป็นปริมาณมาก

คำสำคัญ: เอกสารกระดาษ, ลายมือชื่อดิจิทัล, รหัสคิวอาร์, การพิสูจน์ตัวตนจริง

1. คำนำ

แม้ว่ากระแสของสำนักงานไร้กระดาษ (Paperless Office) หรือรัฐบาลอิเล็กทรอนิกส์ (E-Government) จะเติบโตอย่างรวดเร็ว และถูกนำมาใช้งานจริงมากสักเพียงใดก็ตาม แต่สำหรับงานบางประเภทนั้น ก็ยังมีความจำเป็นต้องใช้การสื่อสารด้วยเอกสารที่อยู่ในรูปของกระดาษ เช่น เอกสารที่ออกโดยราชการ เช่น สูติบัตร ใบอนุญาตขับขี่ หนังสือเดินทาง เอกสารในงานประกันภัย หรือแม้กระทั่งหนังสือสัญญาซื้อขาย ฯลฯ [1]

ด้วยพัฒนาการของเทคโนโลยีการกราดภาพ (Scanning) หรือการสแกน และการพิมพ์ (Printing) ซึ่งมีราคาต่ำแต่กลับมีประสิทธิภาพการทำงานที่สูงมาก จึงทำให้อาชญากร หรือผู้ไม่ประสงค์ดีสามารถทำการปลอมแปลงเอกสารเพื่อการฉ้อโกงต่าง ๆ ได้ง่ายและมีคุณภาพสูงเทียบเท่าของจริง ด้วยการนำประโยชน์จากเทคโนโลยีสมัยใหม่ไม่ว่าจะเป็น เครื่องสแกน เครื่องพิมพ์สี แทนพิมพ์ เป็นต้น ซึ่งจัดว่าเป็นภัยคุกคามต่อสังคม และเศรษฐกิจของชาติ [2]

ในการพิสูจน์ตัวตนจริง (Authentication) ข้อความบนเอกสารนั้นมักจะขึ้นอยู่กับความสามารถของผู้เชี่ยวชาญเฉพาะด้าน จึงทำให้ในหลายประเทศมีการจัดตั้งองค์กรเพื่อทำงานในด้านนิติวิทยาศาสตร์ (Forensic) ขึ้นมา ซึ่งมีการใช้อุปกรณ์พิเศษช่วยสำหรับการตรวจสอบ เช่น หลอดไฟยูวี แวนขยายเครื่องตรวจรังสีอินฟราเรด เป็นต้น [3] ซึ่งในทางปฏิบัติถือว่าเป็นไปได้ลำบาก สำหรับหน่วยงานที่ต้องทำงานกับเอกสารเป็นจำนวนมาก รวมถึงต้องการความรวดเร็ว เช่น ธนาคาร ที่ต้องมีการรับเช็ค ตัวแลกเงิน ใบชำระเงิน ฯลฯ เนื่องจากงานด้านนิติวิทยาศาสตร์จำเป็นต้องมีขั้นตอนที่สอดคล้องกับกฎหมายหลายอย่าง เช่น ต้องส่งเอกสารที่จะพิสูจน์ไปให้กับเจ้าหน้าที่ตำรวจ รอการพิสูจน์จากผู้เชี่ยวชาญ ฯลฯ ซึ่งทำให้ต้องใช้เวลานานพอสมควร

บทความวิจัยนี้ เสนอกระบวนการเพื่อพิสูจน์ตัวตนข้อความบนเอกสารที่สามารถใช้งานได้ค่อนข้างสะดวก รวดเร็ว แบบกึ่งอัตโนมัติ โดยการประยุกต์ใช้ลายมือชื่อดิจิทัลร่วมกับรหัสคิวอาร์ (QR Code) ซึ่งสามารถใช้งานได้โดยไม่ต้องพึ่งพาหน่วยงานพิเศษ เช่น ศูนย์นิติวิทยาศาสตร์แต่อย่างใด

ในบทความนี้ประกอบด้วย 6 ส่วน ซึ่งส่วนถัดไป คือ ส่วนที่ 2 กล่าวถึงงานวิจัยที่เกี่ยวข้องกับแนวคิดที่นำเสนอในงานวิจัยนี้ ส่วนที่ 3 คือ รายละเอียดของแนวคิดที่นำเสนอ ส่วนที่ 4 เป็นการวิเคราะห์คุณสมบัติทางด้านความมั่นคงปลอดภัย ส่วนที่ 5 จะเป็นรายละเอียดของการพัฒนาระบบ และสุดท้ายส่วนที่ 6 เป็นการสรุปผลงานวิจัยนี้

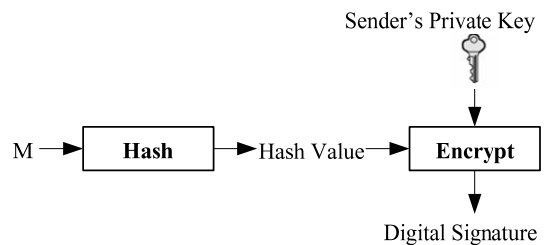
2. ทฤษฎีที่เกี่ยวข้อง

2.1 ฟังก์ชันแฮช (Hash Function)

เป็นวิธีการสำหรับการย่อข้อมูล โดยรับข้อมูลอินพุตขนาดไม่จำกัด และไม่มีการใช้คีย์ใด ๆ ซึ่งผลลัพธ์ที่ได้เรียกว่าค่าแฮช (Hash Value) เป็นข้อความที่มีความยาวคงที่ และไม่สามารถคำนวณย้อนกลับเพื่อค้นหาเนื้อหาและความยาวของข้อความตั้งต้นนั้นได้ (One-way Function) ฟังก์ชันแฮชมักถูกนำมาใช้สำหรับการสร้างสิ่งที่เรียกว่าลายพิมพ์นิ้วมือดิจิทัล (Digital Fingerprint) นิยมเรียกค่าแฮชว่า Message Digest ซึ่งใช้สำหรับตรวจสอบว่าข้อมูลมีการเปลี่ยนแปลงหรือไม่

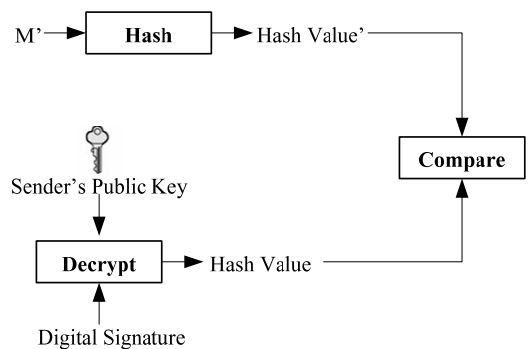
2.2 ลายมือชื่อดิจิทัล (Digital Signature)

ลายมือชื่อดิจิทัล [4] เป็นเทคนิคที่ใช้เพื่อให้ได้คุณสมบัติการพิสูจน์ตัวตนจริง (Authentication) ของผู้สร้างเอกสารหรือผู้ส่งข้อความ ซึ่งจำเป็นต้องอาศัยวิทยาการเข้ารหัสลับแบบอสมมาตร (Asymmetric Cryptography) ดังรูปที่ 1 เป็นการนำเอาข้อความ M ซึ่งเป็นข้อความที่จะส่งไปให้ยังผู้รับมาผ่านฟังก์ชันแฮช (Hash Function) ซึ่งได้ผลลัพธ์ออกมาเป็นค่าแฮช (Hash Value หรือ Message Digest) และนำไปเข้ารหัสลับด้วยไพรเวทคีย์ (Private Key) ของผู้ส่ง ซึ่งจะได้ออกมาเป็นลายมือชื่อดิจิทัลของข้อความ M



รูปที่ 1 กระบวนการสร้างลายมือชื่อดิจิทัล

ในการตรวจสอบความถูกต้องของลายมือชื่อดิจิทัลสามารถทำได้โดยนำข้อความ M มาผ่านฟังก์ชันแฮช แล้วนำค่าแฮชนั้นมาเปรียบเทียบกับค่าแฮชที่ได้จากการถอดรหัสลับจากลายมือชื่อดิจิทัลที่ส่งมาด้วยพับ บลิคคีย์ของผู้ส่ง ถ้าทั้ง 2 ค่าตรงกันแสดงว่าเป็นข้อความดังกล่าวส่งมาจากผู้ที่เป็นเจ้าของพับบลิคคีย์จริง ดังรูปที่ 2



รูปที่ 2 กระบวนการตรวจสอบลายมือชื่อดิจิทัล

ความมั่นคงปลอดภัยของลายมือชื่อดิจิทัลจะขึ้นอยู่กับฟังก์ชันแฮช และอัลกอริทึมในการเข้ารหัสลับ (Cryptographic

Algorithm) ถ้าหากจะทำการโจมตี ผู้โจมตีต้องสร้างลายมือชื่อดิจิทัลปลอมจากข้อความปลอมที่มีค่าของลายมือชื่อดิจิทัลเหมือนกับลายมือชื่อดิจิทัลที่มีอยู่ ซึ่งเป็นการโจมตีฟังก์ชันแฮช หรือสร้างลายเซ็นดิจิทัลปลอมจากข้อความจริง ซึ่งเป็นการโจมตีอัลกอริทึมการเข้ารหัสลับ ฟังก์ชันแฮชจึงจำเป็นต้องมีความทนทานต่อการสร้างผลลัพธ์ที่เหมือนกันจากข้อความต้นฉบับที่ต่างกัน (Collision) และอัลกอริทึมแบบพบบลิตคีย์ก็ต้องทนทานต่อการถูกโจมตีด้วย เทคนิคนี้จึงจะถือได้ว่ามีความมั่นคงปลอดภัย เนื่องจากการคำนวณเพื่อทำการปลอมแปลงลายมือชื่อดิจิทัลเป็นไปได้ยากมาก

ลายมือชื่อดิจิทัลให้คุณสมบัติด้านการพิสูจน์ตัวจริง รวมถึงความคงสภาพ (Integrity) และการไม่สามารถปฏิเสธความรับผิดชอบได้ (Non-Repudiation) หมายความว่า ถ้าหากลายมือชื่อดิจิทัลถูกตรวจสอบว่าถูกต้อง ผู้ที่ส่งข้อความนั้น ๆ มาจะปฏิเสธไม่ได้ว่าเป็นผู้สร้างข้อความนั้นแล้วส่งมา

2.3 การบีบอัดข้อมูล (Compression)

เป็นวิธีการที่ช่วยให้ใช้เนื้อที่ในการจัดเก็บข้อมูลลดน้อยลง ซึ่งถือว่ามีความจำเป็นมากในระบบการสื่อสารและจัดเก็บข้อมูล เนื่องจากจะเป็นการช่วยให้สามารถจัดเก็บหรือรับส่งข้อมูลได้มากขึ้น โดยใช้เนื้อที่ในการจัดเก็บ หรือเนื้อที่ในช่องสัญญาณเท่าเดิม

2.4 รหัสคิวอาร์ (QR code)

รหัสแท่ง 2 มิติ (2D Barcode) [5][6] ถูกออกแบบมาเพื่อให้สามารถเก็บข้อมูลได้ทั้งแนวดิ่งและแนวนอน จึงสามารถเก็บข้อมูลได้มากขึ้น ในพื้นที่ที่เท่ากันหรือเล็กกว่าเมื่อเทียบกับรหัสแท่ง 1 มิติ ทั้งยังสามารถทำการถอดรหัสกลับมาได้ แม้ว่าภาพบางส่วนของรหัสแท่งจะเสียหาย ซึ่งลักษณะโดยทั่วไปของรหัสแท่ง 2 มิตินั้นจะเป็นรูปที่ประกอบด้วยสี่เหลี่ยมเล็ก ๆ สีดำอยู่บนพื้นสีขาวซึ่งสามารถเห็นได้โดยทั่วไป

รหัสคิวอาร์ เป็นรหัสแท่ง 2 มิติรูปแบบหนึ่งที่กำลังเป็นที่นิยมในปัจจุบัน ซึ่งมีคุณสมบัติที่โดดเด่นมากทั้งในเรื่องของการอ่านที่รวดเร็ว และความสามารถในการจัดเก็บข้อมูลได้มากที่สุด เมื่อเปรียบเทียบกับ PDF417 [7][8], DataMatrix [9] หรือ MaxiCode [10] ดังในตารางที่ 1 คือ สามารถเก็บข้อมูลที่เป็นตัวเลขได้ถึง 7,089 อักขระ ข้อมูลที่เป็นตัวอักษรได้ 4,296 อักขระ หรือถ้าเป็นเลขฐาน 2 เก็บได้ 2,953 ไบต์ [11] ซึ่งรหัส

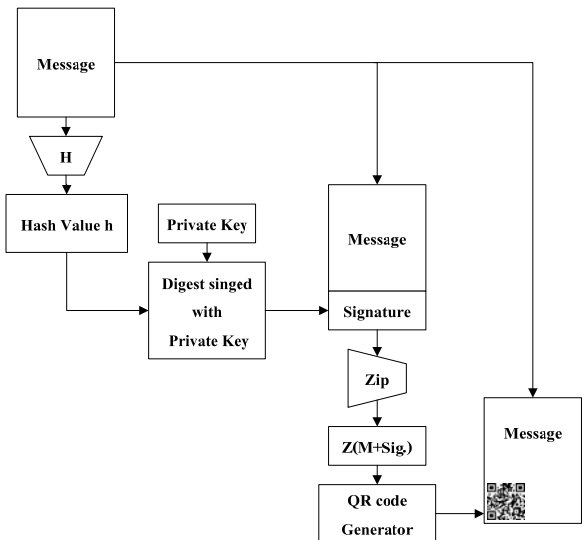
คิวอาร์ใช้วิธีการของ Reed-Solomon [12] ในการตรวจจับและแก้ไขข้อผิดพลาด

ตารางที่ 1 เปรียบเทียบคุณสมบัติของรหัสแท่ง 2 มิติ

	PDF417	Data Matrix	Maxi Code	QR Code
ตัวเลข	2,710	3,116	138	7,089
ตัวอักษร	1,850	2,355	93	4,296
เลขฐานสอง	1,018	1,556		2,953
จุดเด่น	ความสูง	มีขนาดเล็ก	อ่านได้เร็ว	ความสูง มีขนาดเล็ก อ่านได้เร็ว

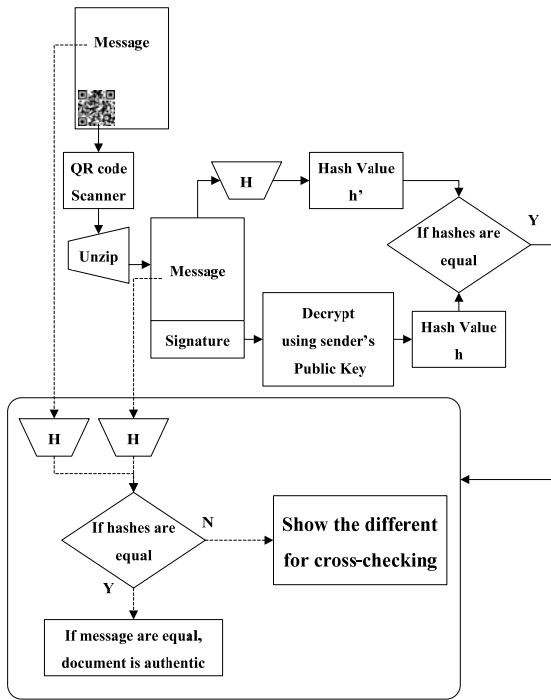
3. วิธีการที่นำเสนอ

3.1 ผู้ส่ง



รูปที่ 3 ข้อความที่จะส่งพร้อมลายมือชื่อดิจิทัล

เมื่อผู้ส่งเตรียมข้อความ M สำหรับการส่งให้ผู้รับเสร็จเรียบร้อยแล้ว ข้อความ M จะถูกนำมาผ่านฟังก์ชันแฮชซึ่งจะได้ออกมาเป็นค่าแฮช h ของข้อความ M จากนั้นนำค่าแฮช h มาเข้ารหัสลับด้วยไพรเวทคีย์ของผู้ส่งได้มาซึ่งลายมือชื่อดิจิทัล นำเอาทั้งข้อความ M และลายมือชื่อดิจิทัลของข้อความ M ต่อกันแล้วจึงนำไปผ่านฟังก์ชันบีบอัด (Compression) ให้มีขนาดที่เล็กลงเพื่อประโยชน์ในการนำไปสร้างเป็นรหัสคิวอาร์ ซึ่งหลังจากสร้างรหัสคิวอาร์เสร็จ จะทำการพิมพ์ข้อความ M ร่วมกับรหัสคิวอาร์ที่สร้างดังกล่าวนั้นลงบนกระดาษแล้วส่งไปให้ผู้รับ ดังรูปที่ 3



รูปที่ 4 การพิสูจน์ตัวจริงโดยฝั่งผู้รับ

3.2 ฝั่งผู้รับ

เมื่อผู้รับได้รับเอกสารจากผู้ส่งแล้ว ก็นำเอกสารดังกล่าวไปสแกนเป็นแฟ้มข้อมูลประเภทรูปภาพ เพื่อการพิสูจน์ตัวจริงข้อความด้วยระบบคอมพิวเตอร์ต่อไป สำหรับในส่วนของการหาคิวอาร์นั้นได้จัดเก็บข้อมูลที่ประกอบด้วยข้อความ M และลายมือชื่อดิจิทัลของข้อความ M ซึ่งได้ถูกบีบอัดเอาไว้ในขั้นตอนการส่ง ทำให้หลังจากถอดรหัสจากคิวอาร์มาแล้วจำเป็นต้องนำค่านั้นมาคลายการบีบอัดออก (Decompress) เสียก่อน ซึ่งผลจากการคลายการบีบอัดออกมาจะประกอบด้วยข้อความ M พร้อมด้วยลายมือชื่อดิจิทัลของข้อความ M และสำหรับการพิสูจน์นั้นทำได้โดยการนำข้อความ M ดังกล่าวนี้อ่านผ่านฟังก์ชันแฮชเพื่อให้ได้ค่าแฮช h' และนำไปเปรียบเทียบกับค่าแฮช h ที่ได้จากการถอดรหัสลับด้วยฟังก์ชันของผู้ส่ง ถ้าตรงกันถือว่าถูกต้องพร้อมสำหรับการนำไปพิสูจน์ตัวจริงของข้อความบนเอกสารกระดาษ โดยการนำแฟ้มรูปภาพในส่วนที่เป็นข้อความมาผ่านฟังก์ชันโอซีอาร์ และฟังก์ชันแฮชจนได้ h'' เพื่อนำมาเปรียบเทียบกับ h' ถ้าหากตรงกัน แสดงว่าข้อความบนเอกสารไม่ได้ถูกปลอมแปลงหรือแก้ไขระหว่าง

การส่ง แต่ถ้าไม่ตรงกันจำเป็นต้องแสดงให้เห็นถึงความแตกต่างของทั้ง 2 ข้อความเพื่อเปรียบเทียบกับสายตาต่อไป

4. การวิเคราะห์ทางด้านความมั่นคงปลอดภัย

เนื่องจากแนวคิดที่ได้นำเสนอนี้ ได้มีการนำเอาเทคโนโลยีลายมือชื่อดิจิทัลมาใช้งาน ซึ่งทำให้ได้คุณสมบัติทางด้านความมั่นคงปลอดภัย 3 ประการด้วยกันคือ

การพิสูจน์ตัวจริง (Authentication) จากในขั้นตอนการส่งมีการเข้ารหัสลับค่าแฮชด้วยไพรเวทคีย์ของผู้ส่งที่มีเพียงผู้ส่งเท่านั้นที่ทราบ และมีเพียงฟังก์ชันคีย์ของผู้ส่งเท่านั้นที่ถอดได้ ถ้าหากตรวจสอบลายมือชื่อดิจิทัลผ่าน หมายความว่าข้อความถูกส่งมาจากผู้ส่งคนนั้นจริง

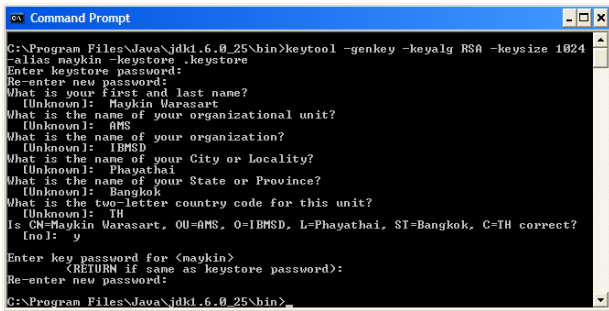
ความคงสภาพ (Integrity) ในระหว่างการสื่อสารที่ทั้งผู้ส่งและผู้รับ ต่างก็ต้องการความมั่นใจว่าข้อมูลที่สื่อสารกันนั้นไม่ได้ถูกแก้ไขระหว่างการส่ง ถึงแม้ว่าหากใช้การเข้ารหัสลับจะสามารถซ่อนเนื้อหาของข้อความที่ต้องการส่งได้ แต่ก็มีความเป็นไปได้ที่จะทำการเปลี่ยนแปลงข้อมูลที่เข้ารหัสลับเอาไว้ โดยที่ไม่ต้องทราบถึงเนื้อหาของข้อความจริง ๆ แต่ถ้าข้อความที่จะส่งมีการสร้างลายมือชื่อดิจิทัลเอาไว้ การเปลี่ยนแปลงข้อความที่ต้องการส่งจะทำให้การตรวจสอบลายมือชื่อดิจิทัลไม่ผ่าน กล่าวคือ ยังไม่มีวิธีการที่มีประสิทธิภาพเพียงพอที่จะทำการแก้ไขข้อความที่ต้องการส่งพร้อมกับสร้างลายมือชื่อดิจิทัลของข้อความใหม่ได้ถูกต้อง อันเนื่องมาจากข้อจำกัดในประเด็นของความสามารถในการคำนวณเพื่อหาค่าซ้ำกันของค่าแฮช (Collision Resistance)

สุดท้าย การไม่สามารถปฏิเสธความรับผิดชอบได้ (Non-repudiation) เพราะบุคคลที่เป็นผู้เข้ารหัสลับข้อมูล (Sign) ใดไปแล้ว จะไม่สามารถปฏิเสธในภายหลังได้ว่าไม่ได้เป็นผู้ที่เข้ารหัสลับ รวมถึงบุคคลอื่นจะมีได้เพียงแค่ฟังก์ชันคีย์ของบุคคลข้างต้นเท่านั้น ซึ่งก็ไม่สามารถที่จะใช้ฟังก์ชันคีย์ที่มีอยู่ดังกล่าวนี้ มาใช้เพื่อทำการปลอมแปลงลายมือชื่อดิจิทัลของบุคคลข้างต้นได้

5. การพัฒนาระบบต้นแบบ

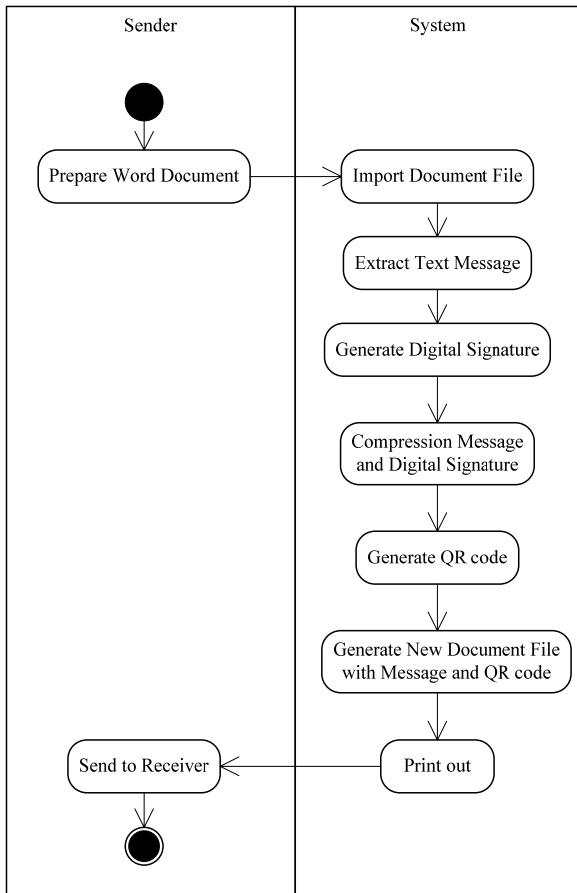
ในการพัฒนาระบบต้นแบบเพื่อพิสูจน์ว่าระบบที่นำเสนอสามารถนำไปใช้งานได้จริงนั้น ผู้วิจัยเลือกพัฒนาโปรแกรมด้วยภาษาจาวา ซึ่งมี JCA (Java Cryptographic Architecture) ที่ได้เตรียมฟังก์ชันสำหรับการพัฒนาโปรแกรมทางด้านความ

มั่นคงปลอดภัยไว้ให้แล้ว เช่น การใช้งานใบรับรองดิจิทัล หรือ การใช้งานลายมือชื่อดิจิทัล เป็นต้น



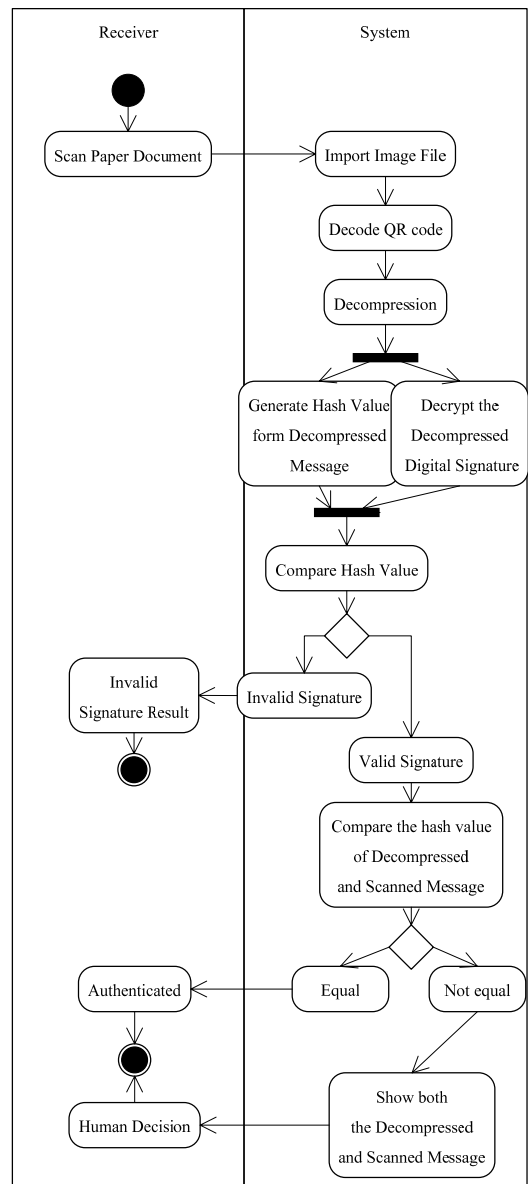
รูปที่ 5 การสร้างคีย์และที่เก็บคีย์ด้วย keytool

ในการจัดเก็บคีย์ (Key Storage) ของผู้ใช้งาน ผู้วิจัยเลือกใช้ Java keytool [13] ในการจัดเก็บคีย์ ซึ่งเป็นไปตามมาตรฐาน ใบรับรองรุ่น X.509 ดังรูปที่ 5 โดยที่สามารถส่งออก (Export) ในส่วนของพบบลิตคีย์ออกมาเป็นแฟ้มข้อมูล แล้วส่งต่อไปให้ผู้รับเก็บไว้เพื่อใช้งานต่อไปในอนาคตได้



รูปที่ 6 Activity Diagram ฝั่งผู้ส่ง

เนื่องจากส่วนใหญ่ การสร้างเอกสารภายในองค์กรมักจะ ใช้โปรแกรมประมวลผลคำ (Word Processor) เช่น Microsoft Word จึงจำเป็นต้องใช้ไลบรารี POI API [16] มาช่วยในการ สกัด (Extract) ข้อความจากแฟ้มข้อมูลดังกล่าวออกมาเพื่อใช้ สำหรับสร้างลายมือชื่อดิจิทัลของข้อความนั้น โดยใช้ SHA-256 [14] ซึ่งให้เอาพุดขนาด 256 บิต ร่วมกับ RSA [15] และใช้ แฟ้มเอกสารสำหรับการบีบอัดข้อมูลของภาษาจาวาเพื่อลดขนาด ก่อนนำไปสร้างเป็นรหัสคิวอาร์ ซึ่งรับอินพุตที่มีขนาดจำกัด ดังแสดงในตารางที่ 1 โดยที่ผู้วิจัยเลือกใช้ไลบรารี ZXing [17] ในการสร้างรหัสคิวอาร์ เมื่อมีข้อมูลที่พร้อมสำหรับการส่งไป ยังผู้รับแล้ว จะทำการจัดรูปแบบหน้าตาเอกสารสำหรับพิมพ์ ลงกระดาษจริงเพื่อส่งต่อให้ผู้รับด้วยไลบรารี iText® PDF [18]



รูปที่ 7 Activity Diagram ฝั่งผู้รับ

สำหรับโปรแกรมในฝั่งผู้รับนั้น จะรองรับรูปภาพซึ่งได้มาจากการสแกนเอกสารกระดาษที่ผู้ส่งส่งมา โดยในการทดลองใช้ความละเอียดของการสแกนที่ 200 dpi และใช้ ZXing ในการแปลงรูปภาพในส่วนของรหัสคิวอาร์ได้ออกมาเป็นข้อความต้นฉบับและลายมือชื่อดิจิทัลของข้อความนั้น ซึ่งถูกบีบอัดอยู่ จึงต้องทำการคลายการบีบอัดก่อน แล้วจึงนำมาถอดรหัสลับในส่วน of ลายมือชื่อดิจิทัลด้วยฟังก์ชันของผู้ส่งในแฟ้มพบบลิตที่ผู้ส่งทำการส่งให้ไว้ล่วงหน้าแล้ว ซึ่งจะได้ออกมาเป็นค่าแฮช นำค่าแฮชนี้ มาเปรียบเทียบกับค่าแฮชที่ได้จากการนำข้อความที่อยู่กับลายมือชื่อดิจิทัลมาผ่านฟังก์ชันแฮช ถ้าผลการเปรียบเทียบออกมาตรงกัน แสดงว่าข้อความที่ได้มาจากรหัสคิวอาร์นั้นถูกส่งจากผู้ส่งจริงตามที่ได้กล่าวอ้าง และไม่ได้ถูกแก้ไขระหว่างทาง แล้วจึงนำรูปภาพในส่วนที่เป็นข้อความบนเอกสารมาผ่านฟังก์ชันโอซีอาร์ แล้วนำไปเปรียบเทียบกับข้อความที่ได้จากรหัสคิวอาร์ด้วยค่าแฮชของทั้ง 2 ข้อความ ถ้าตรงกันถือว่าข้อความบนเอกสารเชื่อถือได้ แต่กรณีที่ไม่ตรงกัน ก็เป็นไปได้ว่ามีคนปลอมแปลงข้อความบนเอกสารจริง หรือไม่ก็เป็นประเด็นจากความแม่นยำของฟังก์ชันโอซีอาร์ จึงต้องมีการแสดงให้เห็นถึงความแตกต่างในส่วนที่มีนัยสำคัญของข้อความ เพื่อตัดสินใจในขั้นสุดท้าย

6. สรุปผล

บทความวิจัยนี้นำเสนอการสร้างความปลอดภัยให้กับเอกสารกระดาษโดยใช้ลายมือชื่อดิจิทัลและรหัสคิวอาร์ซึ่งสามารถทำงานได้รวดเร็วแบบกึ่งอัตโนมัติกับเอกสารเป็นจำนวนมาก โดยที่ข้อความที่จะทำการส่งจะถูกนำมาสร้างลายมือชื่อดิจิทัลของข้อความดังกล่าวก่อน แล้วจึงนำไปสร้างเป็นรหัสคิวอาร์ พิมพ์ข้อความและรหัสคิวอาร์ลงบนกระดาษแล้วจึงส่งไปให้ผู้รับ เมื่อผู้รับได้รับเอกสารแล้วจะนำเอกสารที่อยู่ในรูปของกระดาษที่ได้รับมาไปสแกนให้ได้ออกมาเป็นแฟ้มรูปภาพ ซึ่งในส่วนที่เป็นรหัสคิวอาร์จะนำไปเข้าสู่ฟังก์ชันในการอ่านออกมาเป็นข้อความและลายมือชื่อดิจิทัลแล้วทำการตรวจสอบลายมือชื่อดิจิทัลนั้น เพื่อเป็นการพิสูจน์ตัวจริงของข้อความบนเอกสารที่ส่งมาว่าเป็นของผู้ส่งที่กล่าวอ้างจริงหรือไม่ รวมถึงข้อความดังกล่าวนี้ไม่ได้ถูกแก้ไขโดยผู้ที่ไม่ได้รับอนุญาตในระหว่างการจัดส่ง

สำหรับแนวทางในการพัฒนาต่อ นั้น ผู้วิจัยจะทำการพัฒนารหัสแท่ง 2 มิติขึ้นมาใหม่ โดยที่มีคุณสมบัติในการเก็บข้อมูลให้ได้มากกว่าเดิม รวมถึงการกระจายพบบลิตที่สะดวกขึ้น

เอกสารอ้างอิง

- [1] van Renesse, Rudolf L., "Paper-based document security—A Review", European Conference on Security and Detection, London, UK, April 28-30, 1997.
- [2] U. Garain, B. Halder, "On Automatic Authenticity Verification of Printed Security Documents", Sixth Indian Conference on Computer Vision, Graphics & Image Processing, 2008, pp. 706-713.
- [3] Procedure Manuals prepared by Directorate of Forensic Science, Ministry of Home Affairs, Govt. of India, <http://www.dfs.gov.in>.
- [4] P. Kuacharoen, "Design and Analysis of Methods for Signing Electronic Documents Using Mobile Phones", International Conference on Computer Applications and Network Security (ICCANS 2011), pp. 154-158, May 2011.
- [5] Intermec's White paper, Sizing App for 2D Barcode, Available: http://epsfiles.intermec.com/eps_files/eps_wp/Sizeing2DApp_wp_web.pdf
- [6] J.Z. Gao, L. Prakash, R. Jagatesan, "Understanding 2D-BarCode Technology and Applications in M-Commerce – Design and Implementation of A 2D Barcode Processing Solution", 31st Annual Intl . Computer Software and Applications Conference (COMPSAC 2007), Beijing, July 24-27, 2007.
- [7] PDF417 Barcode, Available: <http://www.pdf417.com/>
- [8] Hee Il Hahn, Joung Koo Joung, "Implementation of algorithm to decode two-dimensional barcode PDF-417", 6th International Conference on Signal Processing, Aug 26-30, 2002.
- [9] Data Matrix, Available: http://en.wikipedia.org/wiki/Data_Matrix
- [10] MaxiCode, Available: <http://en.wikipedia.org/wiki/MaxiCode>
- [11] QR-Code, Available: <http://www.denso-wave.com/qr-code/>
- [12] K. Kamijo, N. Kamijo, G. Zhang, "Invisible barcode with optimized error correction", 15th IEEE Intl. Conference on Image Processing, Oct 12-15, 2008
- [13] keytool - Key and Certificate Management Tool, Available: <http://download.oracle.com/javase/6/docs/technotes/tools/windows/keytool.html>
- [14] SHA-2, <http://en.wikipedia.org/wiki/SHA-2>
- [15] RSA, Available: <http://en.wikipedia.org/wiki/RSA>
- [16] Apache POI - the Java API for Microsoft Documents, Available: <http://poi.apache.org/>
- [17] Zxing multi-format 1D/2D barcode image processing library, Available: <http://code.google.com/p/zxing/>
- [18] iText®, Available: <http://www.itextpdf.com/>