การซ่อนข้อความ และการสกัดพร้อมการทวนสอบข้อความที่ได้ในภาพใบหน้าด้านหน้า

Concealing and Extracting with Verifying Text in Frontal Face Image

ไพจิตร กชกรจารุพงศ์[1] และศิริพล ปัญญาธิโป[2]

Paijit Kochakornjarupong[1] and Siriphon Panyathipo[2]

บทคัดย่อ

การส่งผ่านข้อมูลผ่านทางเครือข่ายคอมพิวเตอร์สาธารณะเป็นสิ่งที่จำเป็น แต่ข้อมูลอาจเกิดความเสียหายได้หากมีการเปลี่ยนหรือดัดแปลงข้อความโดยการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต ดังนั้นการซ่อนข้อความไว้ในภาพจะเป็นการป้องกันข้อมูลไว้ไม่ให้ข้อมูลเปิดเผยต่อบุคคลทั่วไปโดยตรง ในบทความนี้ได้อธิบายขั้นตอนวิธีการที่ใช้สำหรับซ่อนข้อความไว้ในรูปภาพใบหน้าด้านหน้าของรูปภาพที่ต้องการ โดยผลลัพธ์การซ่อนข้อความจะได้รูปภาพที่มีข้อมูลซ่อนอยู่ที่มีลักษณะเหมือนกับรูปภาพต้นฉบับ ซึ่งขั้นตอนวิธีจะเริ่มจากการอ่านภาพใบหน้าด้านหน้าและอ่านข้อความที่ต้องการซ่อนแล้วนำมาคำนวณหาค่าแฮชของข้อความ จากนั้นข้อความและค่าแฮชจะนำมาเข้าสู่กระบวนการซ่อนข้อมูลลงในภาพที่ต้องการ เมื่อต้องการอ่านค่าข้อมูลจะนำภาพที่ซ่อนข้อมูลไว้มาเข้ากระบวนการถอดข้อมูลโดยได้ผลลัพธ์เป็นค่าข้อความและค่าแฮชของข้อความ นอกจากนี้วิธีการนี้สามารถตรวจสอบความถูกต้องของข้อมูลที่ซ่อนไว้ได้ว่ามีการเปลี่ยนแปลงของข้อความที่ซ่อนไว้ต่างไปจากข้อความต้นฉบับหรือไม่จากการตรวจสอบความถูกต้องของข้อความที่ได้กับค่าแฮชที่อยู่ในภาพ จึงทำให้ข้อมูลที่ซ่อนอยู่มีความปลอดภัยและน่าเชื่อถือสำหรับการป้องกันการเสียหายจากข้อมูลถูกปลอมแปลง จากการทดลองโดยใช้ภาพใบหน้าที่แตกต่างกันจำนวน 10 คนและข้อความเดียวกันพบว่าได้ผลลัพธ์รูปภาพที่ซ่อนข้อมูลไม่ต่างจากรูปภาพต้นฉบับและเมื่อถอดข้อมูลก็ได้ข้อความที่ถูกต้องครบถ้วนทั้งหมด โดยวิธีการนี้สามารถนำไปใช้ประโยชน์ในงานด้านอื่นๆ ต่อไปได้ เช่น การรักษาความปลอดภัยของข้อมูลที่สำคัญ หรือการป้องกันทรัพย์สินทางปัญญา

คำสำคัญ: การซ่อนข้อความ การสกัดข้อความ การทวนสอบข้อความ ภาพใบหน้าด้านหน้า ค่าแฮช

Abstract

The transmission of data via public networks is often necessary, but such data may be easily compromised. One solution is to hide the true message in an innocent-looking image transmitted as the data. This paper describes an algorithm for concealing and extracting text in a frontal face image based around the hiding of the message. We can easily validate the hidden text by using the included hash. Our experiments use different facial images and the same hidden text to produce images that are exactly the same as the originals. This method can be easily applied to other areas, such as the protection of intellectual property.

Keywords: Concealing Text, Extracting Text, Verifying Text, Frontal Face Image, Hash Value

---

[1] อ.ดร., ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยสงขลานครินทร์ สงขลา 90112

[2] นักศึกษาปริญญาตรี ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยสงขลานครินทร์ สงขลา 90112

[1] Lecturer, Dr., Department of Computer Engineering, Faculty of Engineering, Prince of Songkla University, Songkla, 90112

[2] Student, Department of Computer Engineering, Faculty of Engineering, Prince of Songkla University, Songkla, 90112

[*] Corresponding author: Tel.: 074-287342. E-mail address: paijit@coe.psu.ac.th

บทนำ

ในปัจจุบันเทคโนโลยีการสื่อสารข้อมูลทางเครือข่ายคอมพิวเตอร์และอินเตอร์เน็ตมีความครอบคลุมหลากหลายช่วยอำนวยความสะดวกและรวดเร็วมากขึ้น จึงเป็นวิธีการสื่อสารข้อมูลที่สำคัญที่บุคคลต่างๆ ใช้เป็นช่องทางหลักในการส่งข้อมูลระหว่างกัน ซึ่งมีหลายวิธีด้วยกันที่ใช้ในการสื่อสารข้อมูลผ่านทางอินเทอร์เน็ต เช่น อีเมล์, การส่งข้อมูลทางเว็บไซต์, การสนทนาทางสื่อสังคมออนไลน์ เป็นต้น ซึ่งทำให้สามารถส่งข้อมูลได้ง่าย สะดวกและ รวดเร็ว แต่ปัญหาสำคัญอย่างหนึ่งที่เกิดขึ้นจากการส่งข้อมูลผ่านอินเทอร์เน็ต คือ การคุกคามความปลอดภัยของข้อมูลสำคัญ เช่น ข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นความลับอาจจะถูกขโมย หรือโดนเปลี่ยนแปลงทำให้ข้อมูลคลาดเคลื่อนเสียหายได้ ดังนั้นการรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญอย่างยิ่ง เพื่อเป็นการป้องกันข้อมูลและการรักษาความปลอดภัยของข้อมูลจึงได้มีการนำวิธีที่จะซ่อนข้อความในภาพ ซึ่งจะเป็นวิธีที่ทำให้ไม่ต้องใช้การส่งข้อมูลที่มีการเข้ารหัสข้อมูลเป็นพิเศษทำให้ข้อมูลเปลี่ยนไปจากเดิมจนอาจทำให้เกิดความสงสัยให้มีผู้ดักจับข้อมูลที่ส่งได้ โดยการใช้วิธีการอำพรางข้อมูล (Steganography) กับภาพใบหน้าด้านหน้าของบุคคลมาใช้ในการรักษาความปลอดภัยของข้อมูล

การใช้และส่งภาพใบหน้าของบุคคลได้ใช้กันอย่างแพร่หลายเพื่อเป็นการแนะนำบุคคลและเป็นข้อมูลที่สำคัญที่ใช้สำหรับระบุตัวตนของบุคคลในการใช้งานระดับนานาชาติอย่างแพร่หลาย [1] ภาพใบหน้าเป็นส่วนหนึ่งที่จะต้องมีการบันทึกไว้ในหนังสือเดินทาง หรือ บัตรประจำตัวของบุคคลทุกคน

วิธีการอำพรางข้อมูลสามารถที่จะซ่อนข้อความที่ต้องการให้เป็นความลับไว้ในรูปภาพได้โดยไม่ทำให้ภาพมองเห็นเปลี่ยนไปจากเดิม [2-4] ซึ่งจะทำให้ยากต่อการสังเกตเห็นได้ จึงทำให้ลดโอกาสสำหรับการถูกขโมย หรือเปลี่ยนแปลงข้อความ อันจะเป็นการเพิ่มความปลอดภัยให้กับข้อมูล

ในการตรวจสอบข้อมูลว่ามีความเหมือนกันระหว่างข้อมูลที่ได้รับกับต้นฉบับเป็นการยืนยันได้ว่าข้อมูลที่ได้รับมีความถูกต้อง วิธีที่จะตรวจสอบที่ใช้กันอย่างแพร่หลายและมีความปลอดภัยสูงเป็นการใช้ค่าแฮช (Hash Value) ที่ได้จากขั้นตอนวิธีแฮช (Hash Algorithm) [6-7] ที่สามารถยืนยันความเหมือนกันของข้อมูลได้

วิธีการที่นำเสนอนี้เป็นการศึกษาข้อมูลและทดลองพัฒนาจากงานวิจัยอื่น ๆ ที่มีมาก่อนหน้านี้ ซึ่งได้มีการซ่อนข้อความในภาพและมีการเพิ่มเติมให้สามารถตรวจสอบความถูกต้องของข้อความที่ซ่อนหลังจากได้รับว่ามีค่าถูกต้องตามขั้นตอนวิธีแฮช วิธีการซ่อนข้อความที่ทวนสอบได้ในภาพใบหน้าด้านหน้านี้เป็นเทคนิคที่มีประโยชน์ในการนำไปใช้ในหลายด้าน เช่น ใช้สำหรับการรักษาความปลอดภัยข้อมูลอื่น ๆ ต่อไป การใช้ประยุกต์สำหรับการป้องกันการละเมิดทรัพย์สินทางปัญญา เป็นต้น วิธีการที่นำเสนอนี้จึงเป็นหัวข้อที่น่าสนใจเพื่อที่จะนำไปใช้ในงานอื่น ๆ ที่ประยุกต์เกี่ยวข้องกับใช้การประมวลผลภาพเพื่อรักษาความปลอดภัยของข้อมูลต่อไป

งานที่เกี่ยวข้อง

มีผู้นำเสนอการซ่อนข้อมูลในภาพด้วยการซ่อนไว้ในจุดภาพ [2-5] ซึ่งผลที่ได้ทำให้สามารถซ่อนข้อความในภาพต้นฉบับได้โดยผู้ใช้ทั่วไปไม่ทราบว่ามีข้อมูลซ่อนอยู่ วิธีการ LSB (Least Significant Bit) เป็นการเลือกตำแหน่งที่จะใส่ข้อมูลลงในจุดภาพทำให้ภาพที่ซ่อนข้อมูลแล้วยังเหมือนกับภาพต้นฉบับ [2-5] ทั้งนี้เมื่อเทียบกับวิธีอื่นวิธีการ LSB มีจุดเด่นที่มีการประมวลผลที่ไม่ซับซ้อน รวมทั้งภาพผลลัพธ์มีขนาดเท่าเดิมและภาพที่ได้ไม่แตกต่างกับภาพต้นฉบับเมื่อมองด้วยตา [2, 5] อย่างไรก็ตามข้อความที่ซ่อนไว้ในภาพที่ได้รับอาจเกิดการผิดพลาดหรือเปลี่ยนแปลงจากข้อความเดิมเมื่อมีการส่งภาพไปยังบุคคลอื่นจากการสื่อสารหรือการถูกแก้ไข

สำหรับการใช้ภาพใบหน้าสำหรับการซ่อนข้อมูล มีผู้นำเสนอการใส่ค่าของกุญแจลับ (Secret Key) ที่ได้จากภาพใบหน้าใส่ลงในรหัส QR (Quick Response Code) ซึ่งจะต้องใช้ทั้งภาพใบหน้าและรหัส QR เพื่อส่งข้อมูล [7] ซึ่งไม่สามารถประมวลผลข้อมูลที่ต้องการภายในภาพเดียวได้

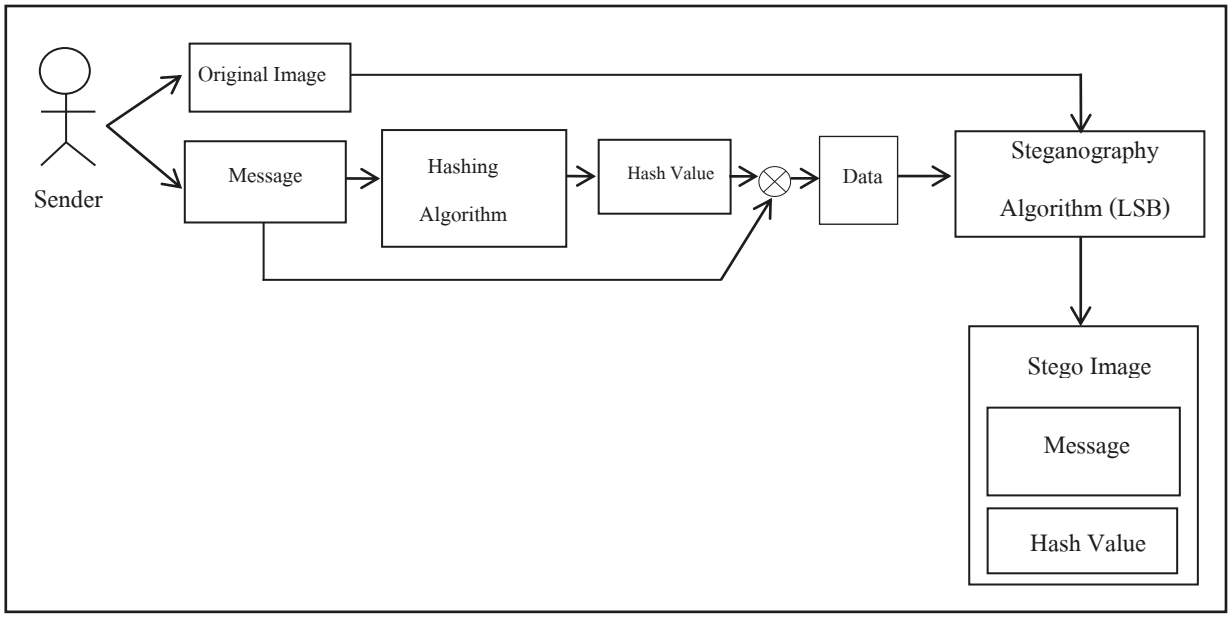
บทความนี้จะนำเสนอวิธีการซ่อนข้อความในภาพที่รูปภาพที่ซ่อนข้อมูลอยู่จะมีลักษณะเหมือนกับรูปภาพต้นฉบับ และสามารถยืนยันความถูกต้องของข้อความที่ซ่อนไว้ได้ว่ามีการเปลี่ยนแปลงของข้อความที่ซ่อนไว้หรือไม่โดยใช้เพียงการตรวจสอบจากภาพผลลัพธ์ที่ได้

วิธีการซ่อนและตรวจสอบข้อมูล

วิธีการซ่อนและตรวจสอบข้อมูลจะเป็นการซ่อนข้อความลงในรูปภาพใบหน้าด้านหน้าของบุคคลแบบอัตโนมัติ โดยการนำข้อความที่ต้องการซ่อนลงในรูปภาพใบหน้าด้านหน้าของบุคคล ซึ่งภาพผลลัพธ์ที่ได้จากวิธีการนี้จะเป็นรูปภาพที่มีข้อมูลซ่อนอยู่ (Stego Image) ที่มีลักษณะไม่เปลี่ยนแปลงไปจากรูปภาพต้นฉบับ ซึ่งวิธีการทำงานที่นำเสนอประกอบด้วย 2 ขั้นตอน คือ ขั้นตอนการซ่อนข้อมูล (Hiding Process) และขั้นตอนการถอดข้อมูล (Extraction Process)

1. ขั้นตอนการซ่อนข้อมูล

การซ่อนข้อมูลมีขั้นตอนขั้นตอนเฉพาะส่วนของการซ่อนข้อมูลลงในรูปภาพใบหน้าด้านหน้าของบุคคลแบบอัตโนมัติที่เสนอดังภาพที่ 1



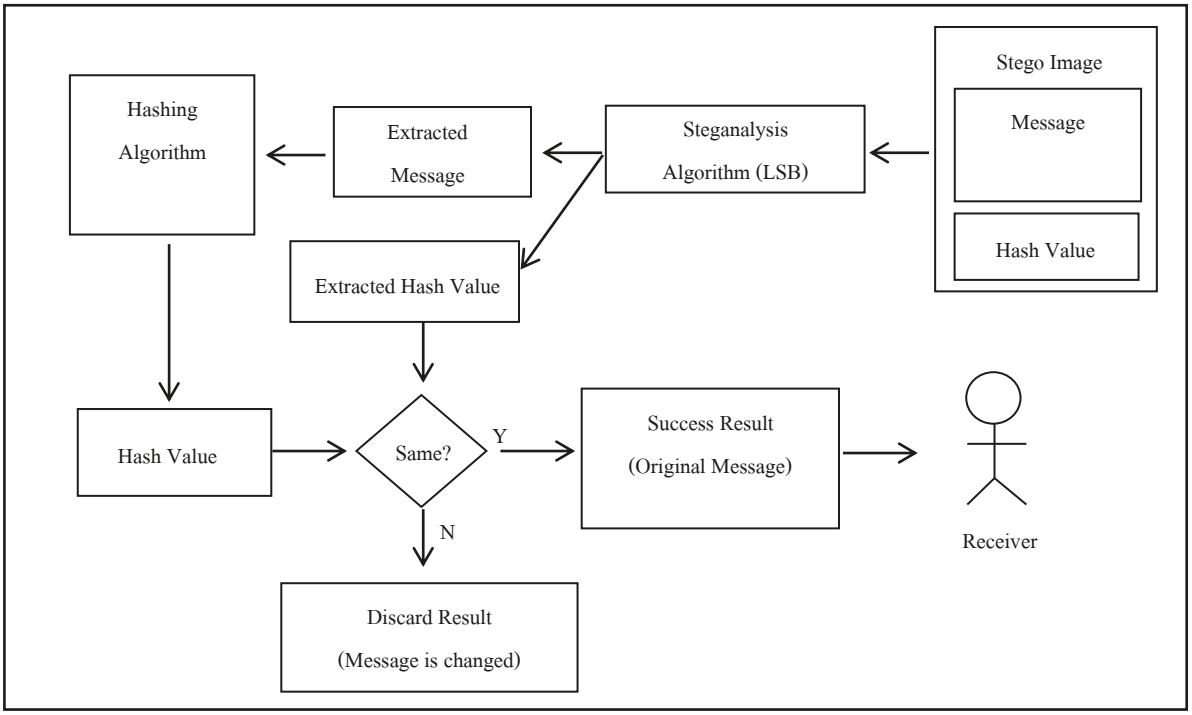
ภาพที่ 1 ขั้นตอนการซ่อนข้อมูล

สรุปขั้นตอนการซ่อนข้อมูล

- เริ่มจากผู้ใช้เลือกรูปภาพใบหน้าที่ต้องการซ่อนข้อมูลและข้อความที่ต้องการซ่อน
- คำนวณหาค่าแฮช (Hash Value) ด้วยวิธีแฮช โดยวิธีแฮชแบบ SHA (Secure Hash Algorithm) เนื่องจากเป็นอัลกอริทึมที่ได้รับความนิยม และได้มีการนำไปประยุกต์ใช้งานกันอย่างแพร่หลาย และเป็นวิธีที่มีความสามารถรับสายอักขระได้จำนวนมากที่มีขนาดต่างกันแต่ได้ผลลัพธ์ค่าแฮชที่มีความยาวเท่ากัน การใช้ SHA256 จะได้ค่าแฮชจำนวน 256 บิต และโอกาสที่เกิดปัญหาการซ้ำกันของค่าแฮชน้อยกว่าแบบ MD5 [8]
- รวมข้อความที่ต้องการซ่อนกับค่าแฮช
- ทำการซ่อนข้อความโดยการอำพรางข้อมูลด้วย วิธี LSB โดยการซ่อนข้อมูลไว้ที่บิตสุดท้ายของแต่ละจุดภาพในรูปภาพ โดยจะใส่ใน LSB (Least Significant Bit) ของค่า Pixel สีของรูปภาพ ซึ่งการเปลี่ยนแปลงค่าบิตสุดท้ายของจุดภาพจะไม่สามารถมองเห็นถึงความแตกต่างของภาพไปจากเดิม [2] จึงทำให้สามารถนำเอาข้อมูลมาใส่ไว้ในภาพโดยไม่เพิ่มขนาดของภาพซึ่งผลลัพธ์ที่ได้จะเป็นภาพที่มีการซ่อนข้อความและค่าแฮชไว้แล้ว

2. ขั้นตอนการถอดข้อมูล

การถอดข้อมูลจะนำภาพที่มีการซ่อนข้อมูลแล้วมาประมวลผลกับขั้นตอนเฉพาะส่วนของการถอดข้อมูลดังแสดงในภาพที่ 2



ภาพที่ 2 ขั้นตอนการถอดข้อมูล

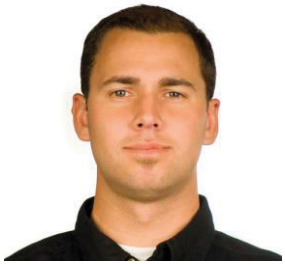
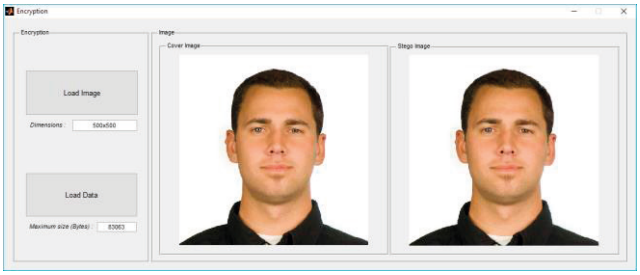
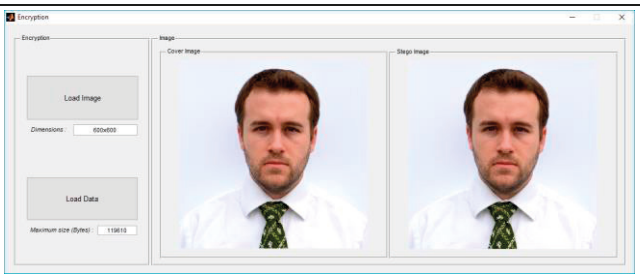
สรุปขั้นตอนการถอดข้อมูล

- เริ่มนำรูปภาพใบหน้าที่มีการซ่อนข้อมูลมาเข้าวิธีถอดข้อมูลที่อำพรางไว้ด้วยวิธี LSB ที่นำข้อมูลบิตสุดท้ายของแต่ละจุดภาพในรูปภาพมาเป็นข้อความและค่าแฮช
- คำนวณหาค่าแฮช (Hash Value) ของข้อความที่ถอดข้อมูลออกมาด้วยวิธีแฮช โดยวิธีแฮชแบบ SHA256
- เปรียบเทียบค่าแฮชที่ได้จากการถอดข้อมูลกับค่าแฮชที่คำนวณจากข้อความที่ถอดข้อมูลออกมา
  - หากมีค่าเหมือนกันแสดงว่าข้อความถูกต้องตามต้นฉบับให้แสดงเพื่อนำไปใช้ต่อได้
  - หากมีค่าต่างกันแสดงว่าเกิดข้อผิดพลาดของข้อความที่ถอดได้กับข้อความต้นฉบับมีค่าแฮชต่างกันให้ยกเลิกการใช้งานข้อความที่ถอดข้อมูล

ผลการทดสอบ

ในการทดสอบวิธีการ ซ่อนข้อมูลลงในรูปภาพใบหน้าด้านหน้าของบุคคลแบบอัตโนมัตินี้ ได้นำรูปภาพใบหน้าด้านหน้าของบุคคลจำนวน 10 คน มาใช้ในการทดสอบซ่อนข้อมูลลงในรูปภาพ ข้อมูลที่สอบเป็นรูปแบบ JPEG (Joint Photographic Experts Group) โดยข้อมูลเดียวกันที่ใช้ซ่อนจะประกอบไปด้วยตัวอักษรทั้งภาษาไทย ภาษาอังกฤษ และตัวเลข ผลลัพธ์จะได้รูปภาพที่ไม่บีบอัดข้อมูลในรูปแบบ PNG (Portable Network Graphics) ที่เป็นที่นิยมสำหรับใช้ในการประมวลผลภาพชั้นสูง [9] สำหรับการแสดงผลลัพธ์ 4 ตัวอย่างรูปภาพต้นฉบับและรูปภาพผลลัพธ์จากการซ่อนข้อมูลแสดงดังตารางที่ 1

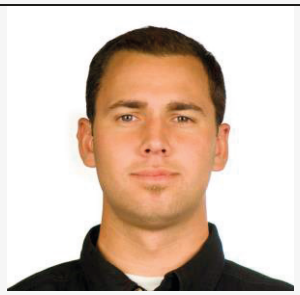
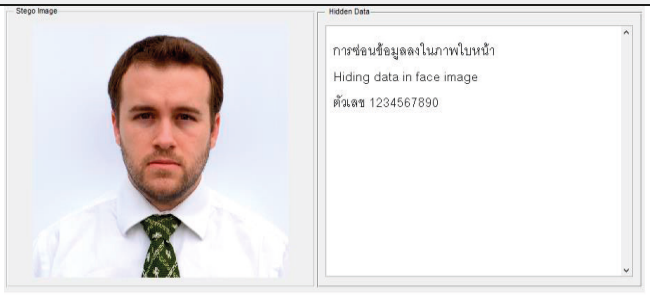
ตารางที่ 1 ผลการทดลองซ่อนข้อมูลลงในรูปภาพใบหน้าด้านหน้า

รูปที่	รูปภาพต้นฉบับ	ผลลัพธ์ของการทดลอง
1		
2		
3		
4		

จากตารางที่ 1 แสดงว่าผลการทดลองสามารถซ่อนข้อมูลลงในรูปภาพใบหน้าด้านหน้าของบุคคลได้ โดยได้ผลลัพธ์เป็นรูปภาพที่มีข้อมูลซ่อนอยู่ มีลักษณะไม่ต่างไปจากรูปภาพต้นฉบับ หรือเปลี่ยนแปลงน้อยในลักษณะที่ไม่สามารถมองเห็นด้วยตาเปล่า

สำหรับการทดลองถอดข้อมูลจากภาพที่มีการซ่อนข้อมูลของตัวอย่าง 4 ภาพแสดงได้ในตารางที่ 2

ตารางที่ 2 ผลการทดลองถอดข้อมูลจากรูปภาพใบหน้าด้านหน้าที่มีการซ่อนข้อมูล

รูปที่	รูปภาพที่มีข้อมูลซ่อนอยู่	ผลลัพธ์ของการทดลอง
1		
2		
3		
4		

ผลการทดลองได้ผลลัพธ์ค่าแฮชเดียวกันทั้งหมด คือ 79bd6c691e51332d13904671f91883d7 ซึ่งจากตารางที่ 2 แสดงข้อมูลที่ซ่อนอยู่เป็นค่าเดียวกันทั้งหมด แสดงว่าวิธีการถอดข้อมูลสามรถถอดข้อมูลออกจากรูปภาพที่มีข้อมูลซ่อนอยู่ ได้อย่างถูกต้อง ครบถ้วน สมบูรณ์ และได้ภาพผลลัพธ์ที่ถูกต้องในทุกภาพ

สรุปผลการวิจัย

บทความนี้ได้นำเสนอขั้นตอนการซ่อนข้อมูลที่ต้องการและข้อมูลสำหรับตรวจสอบความถูกต้องในภาพ โดยจะการอ่านภาพใบหน้าด้านหน้าที่ต้องการซ่อนข้อความและอ่านข้อความที่ต้องการซ่อนแล้วจะมีการคำนวณหาค่าแฮชของข้อความ จากนั้นข้อความและค่าแฮชจะนำมาเข้าสู่กระบวนการซ่อนข้อมูลลงในภาพที่ต้องการ ผลลัพธ์จะได้เป็นภาพที่ซ่อนข้อมูลที่มองเห็นไม่ต่างไปจากภาพต้นฉบับและสามารถนำไปใช้สำหรับใช้งานต่อไปได้ เมื่อต้องการจะอ่านข้อความก็จะนำภาพที่ซ่อนข้อมูลไว้มาเข้ากระบวนการถอดข้อมูลโดยได้ผลลัพธ์เป็นข้อความและค่าแฮชของข้อความ จากการทดลองกับ

ภาพใบหน้าที่แตกต่างกันจำนวน 10 คนและใช้ข้อความที่ซ่อนเหมือนกันพบว่าได้ผลลัพธ์รูปภาพที่ซ่อนข้อมูลไม่ต่างจากรูปภาพต้นฉบับและเมื่อถอดข้อมูลก็ได้ข้อความที่ถูกต้องครบถ้วนและได้ค่าแฮชตรงกันกับข้อความที่ซ่อนกับค่าแฮชที่ใช้ตรวจสอบทั้งหมด

ดังนั้นวิธีการนี้จึงสามารถซ่อนข้อมูลและตรวจสอบความถูกต้องของข้อมูลที่ซ่อนถึงการเปลี่ยนแปลงของข้อความที่ซ่อนไว้กับภาพหรือไม่ได้อย่างถูกต้อง จึงทำให้ข้อมูลที่ซ่อนอยู่มีความปลอดภัยและน่าเชื่อถือสำหรับการป้องกันการปลอมแปลงหรือคลาดเคลื่อนของข้อมูล โดยวิธีการนี้สามารถนำไปใช้ประโยชน์ในงานด้านอื่นๆ ต่อไปได้ เช่น การส่งข้อมูลที่สำคัญ หรือการตรวจสอบการละเมิดทรัพย์สินทางปัญญาเป็นต้น อย่างไรก็ตามวิธีที่นำเสนอนี้ไม่ได้รวมถึงการระบุความผิดปกติของข้อมูลว่ามีการผิดพลาดอย่างไร ดังนั้นการระบุความผิดปกติของข้อมูลจึงจำเป็นต้องมีการเพิ่มเติมวิธีการวิเคราะห์อื่น ๆ ต่อไป

เอกสารอ้างอิง

[1] Hirzer, M., Urschler, M., Bishof, H., and Birchbauer, J. A. (2009). “An automatic hybrid segmentation approach for aligned face portrait images”, In **Proceedings of the workshop of the Austrian association for pattern recognition**. 49-60.

[2] K.Thangadurai and G.Sudha Devi. (2014). “An analysis of LSB Based Image Steganography Techniques”, In **International Conference on Computer Communication and Informatics**. 1-4.

[3] Chi-Kwong Chan and L.M. Cheng. (2004). “Hiding data in images by simple LSB substitution”, **Pattern Recognition**. 37(3), 469-474.

[4] M. S. Sutaone and M. V. Khandare. (2008). "Image based steganography using LSB insertion technique", In **2008 IET International Conference on Wireless, Mobile and Multimedia Networks**. 146-151.

[5] G. Vanjare and S. Gharge. (2015). “Performance Evaluation of LSB Substitution and DWT Method for Steganography”, **International Journal of Advanced Research in Computer Science and Software Engineering**. 5(3), 699-705.

[6] P. Vadhera and B. Lall. (2014). “Review Paper on Secure Hashing Algorithm and Its Variants”, **International Journal of Science and Research**. 3(6), 629-632.

[7] S. Aygün and M. Akçay. (2015). “Securing biometric face images via steganography for QR code”, In **8th International Conference on Information Security and Cryptology**, 128-133.

[8] S. Aggarwal, N. Goyal, and K. Aggarwal. (2014). “A review of Comparative Study of MD5 and SHA Security Algorithm”, **International Journal of Computer Applications**. 104(14), 1-4.

[9] H. Mao, Z. Hu, L. Zhu and H. Qin. (2012). “PNG File Decoding Optimization Based Embedded System”, In **8th International Conference on Wireless Communications, Networking and Mobile Computing**. 1-4.