การพัฒนาระบบการจัดพิมพ์บัตรเลือกตั้งแบบกระจายศูนย์พร้อมการเข้ารหัสลับเพื่อป้องกันการปลอมแปลงและทุจริต

นายวรากร ศรีเชวงทรัพย์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมไฟฟ้า ภาควิชาวิศวกรรมไฟฟ้า
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2545

ISBN 974-17-1995-7

DEVELOPMENT OF ENCRYPTED BALLOT PAPERS DISTRIBUTED PRINTING SYSTEM FOR FORGED AND DISHONEST PREVENTION

Mr. Warakorn Srichavengsup

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Engineering in Electrical Engineering

Department of Electrical Engineering
Faculty of Engineering
Chulalongkorn University

Academic Year 2002

ISBN 974-17-1995-7

หัวข้อวิทยานิพนธ์	การพัฒนาระบบการจัดพิมพ์บัตรเลือกตั้งแบบกระจายศูนย์พร้อมการเข้ารหัสลับเพื่อป้องกันการปลอมแปลงและทุจริต
โดย	นายวรากร ศรีเชวงทรัพย์
สาขาวิชา	วิศวกรรมไฟฟ้า
อาจารย์ที่ปรึกษา	อาจารย์สุวิทย์ นาคพีระยุทธ

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(ศาสตราจารย์ ดร.สมศักดิ์ ปัญญาแก้ว)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(รองศาสตราจารย์ ดร.วาทิต เบญจพลกุล)

..... อาจารย์ที่ปรึกษา
(อาจารย์สุวิทย์ นาคพีระยุทธ)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.ลัญฉกร วุฒิสิทธิกุลกิจ)

วรากร ศรีเชวงทรัพย์ : การพัฒนาระบบการจัดพิมพ์บัตรเลือกตั้งแบบกระจายศูนย์พร้อมการเข้ารหัสลับเพื่อป้องกันการปลอมแปลงและทุจริต. (DEVELOPMENT OF ENCRYPTED BALLOT PAPERS DISTRIBUTED PRINTING SYSTEM FOR FORGED AND DISHONEST PREVENTION) อ. ที่ปรึกษา : อาจารย์สุวิทย์ นาคพีระยุทธ 142 หน้า. ISBN 974-17-1995-7.

เนื่องจากบัตรเลือกตั้งที่ใช้ในปัจจุบันสามารถปลอมแปลงได้ง่ายจึงมีแนวคิดนำการเข้ารหัสลับแบบกุญแจสาธารณะมาใช้ เพื่อให้การปลอมแปลงทำได้ยากและสามารถตรวจสอบได้ง่าย แต่มีปัญหาในการนำมาใช้งานจริง เนื่องจากต้องเสียเวลามากในการจัดพิมพ์เช่น การสแกนเก็บภาพบัตรเลือกตั้ง การเข้ารหัสลับแบบกุญแจสาธารณะและการพิมพ์รหัสแท่ง 2 มิติลงบนบัตรเลือกตั้ง นอกจากนี้ยังต้องพิมพ์บัตรเลือกตั้งจำนวนมากให้เสร็จภายในระยะเวลาที่จำกัด

วิทยานิพนธ์ฉบับนี้จึงได้ออกแบบและพัฒนาระบบการจัดพิมพ์บัตรเลือกตั้งแบบกระจายศูนย์เพื่อให้แต่ละเขตเลือกตั้งสามารถจัดพิมพ์บัตรได้เอง แต่สามารถป้องกันการทุจริตโดยเจ้าหน้าที่และบุคคลอื่นๆ ได้ นอกจากนี้ยังได้ออกแบบบัตรเลือกตั้งให้เหมาะสมกับระบบการจัดพิมพ์และกระบวนการตรวจสอบ รวมทั้งพัฒนาโปรแกรมต่างๆ ที่เกี่ยวข้องบนเครื่องไมโครคอมพิวเตอร์ เพื่อใช้สำหรับการสร้างกุญแจ การเข้ารหัสลับ การพิมพ์รหัสแท่ง 2 มิติ และการตรวจสอบบัตรเลือกตั้ง ณ สถานที่นับคะแนนและที่ว่าการอำเภอ

ภาควิชา วิศวกรรมไฟฟ้า ลายมือชื่อนิสิต .....

สาขาวิชา วิศวกรรมไฟฟ้า ลายมือชื่ออาจารย์ที่ปรึกษา .....

ปีการศึกษา 2545

4270523721 : MAJOR ELECTRICAL ENGINEERING

KEY WORD: BALLOT PAPER / PUBLIC-KEY ENCRYPTION / 2-DIMENSION BARCODE / PRINTING SYSTEM

WARAKRON SRICHAVENGSUP : DEVELOPMENT OF ENCRYPTED BALLOT PAPERS DISTRIBUTED PRINTING SYSTEM FOR FORGED AND DISHONEST PREVENTION. THESIS ADVISOR : SUVIT NAKPEERAYUTH, 142 pp. ISBN 974-17-1995-7.

Because the current ballot papers can be easily forged, the idea of using public-key encryption on ballot papers has been proposed so that the forgery is harder and the verification is also simple. However, there are some problems in real practical situation because of too much time consuming on many ballot printing steps such as scanning the papers, public-key encryption and printing 2-dimension barcode on ballot papers. Moreover, it is difficult to print a large number of the ballot papers in limited time.

This thesis proposes the design and develops the distributed ballot printing system, in order that each constituency can print their ballot papers locally while preventing dishonesty from the authorities and other person. Moreover, the thesis includes the ballot paper design for the new printing system and verification process, and the program development on microcomputer for key generation, public-key encryption, barcode printing and ballot paper verification at the vote-counting center or district office.

Department Electrical Engineering Student's signature .....

Field of study Electrical Engineering Advisor's signature .....

Academic year 2002 .....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลงได้ ด้วยความช่วยเหลือของ อาจารย์สุวิทย์ นาคพีระยุทธ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งผู้วิจัยได้รับคำปรึกษา คำแนะนำและความคิดเห็น ในด้านต่างๆ ระหว่างการทำวิจัยมาโดยตลอด ผู้วิจัยจึงขอกราบขอบพระคุณมา ณ ที่นี้

ขอขอบคุณเพื่อนพี่น้องนิสิตที่อยู่ภายในห้องปฏิบัติการไฟฟ้าสื่อสาร รวมทั้งนายศิริพงษ์ ประยูรหงษ์ ที่ได้ให้ความช่วยเหลือแก่ผู้วิจัย

ท้ายที่สุดนี้ ผู้วิจัยขอกราบขอบพระคุณบิดามารดา ที่ให้กำลังใจและการสนับสนุนแก่ผู้วิจัยเสมอมาจนสำเร็จการศึกษา

สารบัญ

หน้า

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญ (ต่อ)

บทที่ หน้า

สารบัญ (ต่อ)

สารบัญตาราง

หน้า

สารบัญภาพ

หน้า

สารบัญภาพ (ต่อ)

หน้า

สารบัญภาพ (ต่อ)

หน้า

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

การเลือกตั้งในปัจจุบันมีการทุจริตเกิดขึ้นหลายรูปแบบ วิธีการหนึ่งที่นำมาใช้ในการทุจริตการเลือกตั้งก็คือการปลอมแปลงบัตรเลือกตั้ง ซึ่งบัตรเลือกตั้งที่ใช้ในปัจจุบันปลอมแปลงได้ไม่ยากนัก เพียงแค่นำบัตรเลือกตั้งฉบับจริงไปสั่งพิมพ์ตามโรงพิมพ์ทั่วๆ ไป ก็จะได้บัตรเลือกตั้งปลอมที่ไม่สามารถแยกออกจากบัตรเลือกตั้งจริงได้ จึงมีแนวคิดต่างๆ ที่จะป้องกันการทุจริต อย่างเช่น วิธีติดสติกเกอร์บนบัตรเลือกตั้ง ถ้าบัตรเลือกตั้งใบไหนไม่มีสติกเกอร์ติดก็จะเป็นบัตรเลือกตั้งปลอม และบัตรเลือกตั้งใบไหนมีสติกเกอร์ติดก็เป็นบัตรเลือกตั้งจริง ซึ่งวิธีนี้ก็ยังมีข้อเสียอยู่หลายๆ ประการ อย่างเช่น สติกเกอร์ที่ใช้ในการเลือกตั้งสามารถปลอมแปลงได้ไม่ยากนักและสติกเกอร์ที่ติดก็อาจจะหลุดจากบัตรเลือกตั้งเมื่อไรก็ได้ เลยอาจจะทำให้บัตรเลือกตั้งจริงเป็นบัตรเลือกตั้งปลอมได้ อีกแนวคิดหนึ่งที่เป็นไปได้ก็คือการพิมพ์บัตรเลือกตั้งแบบเดียวกับการพิมพ์ธนบัตร ซึ่งวิธีนี้เป็นการป้องกันการปลอมแปลงบัตรเลือกตั้งได้ดี เนื่องจากทำให้บัตรเลือกตั้งปลอมแปลงได้ยาก แต่ต้องเสียค่าใช้จ่ายสูงและบัตรเลือกตั้งแต่ละใบจะใช้เพียงครั้งเดียวไม่สามารถนำมาใช้ซ้ำได้เหมือนธนบัตร วิธีการนี้จึงไม่คุ้มค่าอย่างยิ่ง

วิทยานิพนธ์ของ ศิริพงษ์ ประยูรหงษ์ [1] ได้เสนอวิธีการที่จะทำให้การปลอมแปลงบัตรเลือกตั้งทำได้ยาก เสียค่าใช้จ่ายไม่สูงและสามารถตรวจสอบได้ว่าบัตรเลือกตั้งนั้นเป็นบัตรเลือกตั้งจริงหรือไม่ ด้วยการนำวิธีเข้ารหัสลับกุญแจสาธารณะมาใช้ โดยบัตรเลือกตั้งแต่ละใบจะฝังเส้นใยหรือเศษผงลงไปในเนื้อกระดาษบัตรเลือกตั้งระหว่างขั้นตอนการผลิต แล้วจึงสแกนเนื้อกระดาษบัตรเลือกตั้งเพื่อที่จะดึงคุณลักษณะเฉพาะตัวของกระดาษบัตรเลือกตั้งมาเข้ารหัสลับและพิมพ์เป็นรหัสแท่งเพื่อให้การตรวจสอบทำได้สะดวก ซึ่งวิธีการดังกล่าวมีข้อดีคือทำให้การปลอมแปลงบัตรเลือกตั้งทำได้ยาก มีราคาถูก และสามารถตรวจสอบได้ง่าย แต่มีปัญหาในการนำวิธีการนี้มาใช้อยู่หลายประการ ดังนี้

- ใช้เวลาอย่างมากในหลายๆ ขั้นตอนของการจัดพิมพ์ อย่างเช่น ขั้นตอนการสแกนบัตรเลือกตั้งแต่ละใบ ขั้นตอนการเข้ารหัสข้อมูลประจำบัตรเลือกตั้งและขั้นตอนการพิมพ์รหัสแท่งลงบนบัตรเลือกตั้ง
- การสั่งพิมพ์รหัสแท่งลงบนบัตรเลือกตั้งจะใช้เครื่องพิมพ์ที่ใช้กับไมโครคอมพิวเตอร์ ซึ่งจะพิมพ์ได้ช้ากว่าเครื่องพิมพ์ในโรงพิมพ์

- มีระยะเวลาในการจัดพิมพ์ที่จำกัด เนื่องจากรัฐธรรมนูญฉบับปัจจุบันได้กำหนดไว้ว่าหากมีการยุบสภาเกิดขึ้นต้องจัดให้มีการเลือกตั้งใหม่ภายใน 60 วัน
- จำนวนบัตรเลือกตั้งที่ต้องจัดพิมพ์มีปริมาณมาก เนื่องจากการเลือกตั้งระดับชาติในปัจจุบันได้กำหนดให้ผู้มาใช้สิทธิ์เลือกตั้งจะต้องกาบัตรเลือกตั้งคนละ 2 ใบ เพื่อเลือกสมาชิกสภาผู้แทนราษฎรแบบแบ่งเขตกับสมาชิกสภาผู้แทนราษฎรระบบบัญชีรายชื่อ โดยผู้มีสิทธิ์เลือกตั้งทั่วประเทศในปัจจุบันมีจำนวนประมาณ 40 ล้านคน และในการจัดพิมพ์บัตรเลือกตั้งจะต้องพิมพ์บัตรสำรองไว้ 1 ชุด ทำให้จำนวนบัตรเลือกตั้งที่ต้องจัดพิมพ์ทั้งหมดมีจำนวนประมาณ 160 ล้านใบ

เนื่องจากงานวิจัยของศิริพงษ์ ประยูรหงษ์ เป็นต้นแบบของการนำการเข้ารหัสลับแบบกุญแจสาธารณะมาใช้กับบัตรเลือกตั้ง จึงไม่ได้คำนึงถึงปัญหาในเรื่องการจัดพิมพ์บัตรเลือกตั้งอย่างที่ได้กล่าวมาข้างต้น วิทยานิพนธ์ฉบับนี้จึงมีแนวคิดที่จะหาวิธีการจัดพิมพ์บัตรเลือกตั้งที่ได้นำการเข้ารหัสลับแบบกุญแจสาธารณะมาใช้ ให้จัดพิมพ์เสร็จอย่างรวดเร็วทันเวลา รวมทั้งหาทางป้องกันการทุจริตจากบุคคลที่มีส่วนเกี่ยวข้องกับบัตรเลือกตั้ง

1.2 วัตถุประสงค์ของการวิจัย

1. เพื่อหาวิธีการจัดพิมพ์บัตรเลือกตั้งที่ได้นำการเข้ารหัสลับมาใช้ ให้จัดพิมพ์เสร็จอย่างรวดเร็วทันเวลา
2. เพื่อออกแบบบัตรเลือกตั้งให้เหมาะสมกับระบบการจัดพิมพ์และตรวจสอบ
3. เพื่อพัฒนาและปรับปรุงระบบการเลือกตั้งให้สอดคล้องกับบัตรเลือกตั้งที่นำระบบการเข้ารหัสลับมาใช้
4. เพื่อพัฒนาและปรับปรุงโปรแกรมบนเครื่องไมโครคอมพิวเตอร์ที่ได้นำการเข้ารหัสลับมาใช้กับบัตรเลือกตั้ง

1.3 ขอบเขตของการวิจัย

1. พัฒนาและปรับปรุงต้นแบบที่เป็นส่วนประกอบของระบบเลือกตั้ง ประกอบด้วย
   1.1. ออกแบบบัตรเลือกตั้งให้เหมาะสมกับระบบการจัดพิมพ์และตรวจสอบ
   1.2. พัฒนาและปรับปรุงโปรแกรมบนไมโครคอมพิวเตอร์สำหรับการดึงข้อมูลคุณลักษณะเฉพาะตัวของกระดาษ การสร้างกุญแจ การเข้ารหัสลับ การพิมพ์รหัสแท่ง และการตรวจสอบความถูกต้องของบัตรเลือกตั้งที่เขตเลือกตั้งและที่ว่าการอำเภอ
2. ปรับกระบวนการเลือกตั้งที่ได้ออกแบบ ให้สอดคล้องกับระบบการเลือกตั้งแบบเดิมจนสามารถนำไปใช้ได้โดยมีช่องโหว่น้อยที่สุด

1.4 วิธีดำเนินการวิจัย

1. ศึกษาวิทยาการเข้ารหัสลับ รหัสแท่ง 1 มิติ, รหัสแท่ง 2 มิติ, แฮชฟังก์ชัน (Hash function) และรหัสแก้ไขข้อมูลผิดพลาดรีดโซโลมอน (Reed Solomon error correction code)
2. ศึกษาข้อมูลเกี่ยวกับอุปกรณ์ที่ใช้ในการจัดพิมพ์บัตรเลือกตั้ง
3. ออกแบบระบบการจัดพิมพ์บัตรเลือกตั้งในทุกๆ ขั้นตอน ให้สามารถจัดพิมพ์บัตรเลือกตั้งจำนวนมากเสร็จอย่างรวดเร็วภายในเวลาที่จำกัด รวมทั้งหาทางป้องกันการทุจริตจากบุคคลที่มีส่วนเกี่ยวข้องกับบัตรเลือกตั้ง
4. ออกแบบบัตรเลือกตั้งให้เหมาะสมกับระบบการจัดพิมพ์และตรวจสอบ
5. พัฒนาและปรับปรุงโปรแกรมที่ใช้บนเครื่องไมโครคอมพิวเตอร์ เพื่อใช้ในการสร้างและบันทึกกุญแจ การพิมพ์รหัสแท่ง 2 มิติลงบนบัตรเลือกตั้ง และการตรวจสอบบัตรเลือกตั้ง
6. ทดสอบและปรับปรุงระบบการจัดพิมพ์บัตรเลือกตั้ง
7. สรุปผลการทดสอบและเขียนวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

สามารถนำไปพัฒนาต่อเพื่อใช้แทนระบบเลือกตั้งในปัจจุบัน เพื่อป้องกันการปลอมแปลงบัตรเลือกตั้งได้

บทที่ 2

ทฤษฎีที่เกี่ยวข้อง

ในบทนี้ จะกล่าวถึงทฤษฎีต่าง ๆ ที่ใช้ในวิทยานิพนธ์ฉบับนี้ ได้แก่ ระบบการเข้ารหัสลับแบบกุญแจสาธารณะด้วยวิธี RSA, การทำโครงร่างภาพ ซึ่งใช้ในการดึงข้อมูลเฉพาะตัวจากกระดาษที่ใช้พิมพ์บัตรเลือกตั้ง, รหัสแท่ง 1 มิติ Code 128, รหัสแท่ง 2 มิติ PDF417, แฮชฟังก์ชัน และรหัสแก้ไขความผิดพลาดรีดโซโลมอน

2.1 ระบบการเข้ารหัสลับแบบกุญแจสาธารณะ (Public-key Cryptosystem)

ระบบการเข้ารหัสลับแบบเดิมนั้น เรียกว่า ระบบการเข้ารหัสลับแบบกุญแจลับ (Secret-key Cryptosystem) เป็นระบบที่ใช้กุญแจลับ (Secret key) เพียงตัวเดียว เมื่อผู้ส่งต้องการส่งข้อความไปยังผู้รับก็จะใช้กุญแจลับเพื่อเข้ารหัสลับข้อความที่ต้องการส่ง และผู้รับจะใช้กุญแจลับตัวเดียวกันในการถอดรหัสลับข้อความ ซึ่งปัญหาหลักของระบบนี้คือ การตกลงเรื่องกุญแจลับระหว่างผู้ส่งกับผู้รับโดยไม่มีผู้อื่นรู้เห็น ถ้าทั้งคู่มิได้อยู่ในที่แห่งเดียวกัน ก็จะต้องมีช่องทางการสื่อสารที่ปลอดภัยที่ผู้อื่นไม่อาจรู้ได้ ซึ่งถ้ามีช่องทางดังกล่าวจริง ทำไมไม่ใช้ช่องทางนั้นส่งข้อความที่ต้องการสื่อสารกันเลย ไม่จำเป็นต้องใช้ระบบการเข้ารหัสลับ จะเห็นว่า ระบบการเข้ารหัสลับแบบกุญแจลับจะมีความยุ่งยากในการจัดการกุญแจ โดยเฉพาะในระบบที่มีผู้ใช้จำนวนมาก ก็จะต้องใช้กุญแจเป็นจำนวนมากด้วย ดังนั้น ระบบการเข้ารหัสลับแบบกุญแจสาธารณะจึงเกิดขึ้นในปี ค.ศ. 1976 โดย Whitfield Diffie และ Martin Hellman [2] เพื่อแก้ปัญหาในเรื่องการจัดการกุญแจ

ในระบบการเข้ารหัสลับแบบกุญแจสาธารณะ ผู้ใช้แต่ละคนจะมีกุญแจอยู่ 1 คู่ คือ กุญแจสาธารณะ (Public key) และกุญแจส่วนตัว (Private key) โดยกุญแจสาธารณะจะสามารถประกาศให้ผู้อื่นรู้ได้ ส่วนกุญแจส่วนตัวจะเก็บไว้เป็นความลับ ผู้ใช้ 2 คนจะสามารถติดต่อสื่อสารกันได้เพียงแค่รู้กุญแจสาธารณะของอีกฝ่ายหนึ่งเท่านั้น ดังนั้นจึงไม่มีความจำเป็นที่จะต้องแลกเปลี่ยนข้อมูลที่เป็นความลับกันระหว่างผู้ส่งกับผู้รับเหมือนกับในระบบการเข้ารหัสลับแบบกุญแจลับ นอกจากนั้น การรู้กุญแจตัวหนึ่งจะไม่สามารถคำนวณหากุญแจอีกตัวหนึ่งที่ใช้คู่กันได้โดยง่าย นอกจากลองเดาไปเรื่อย ๆ ซึ่งใช้เวลานานมาก

ในระบบการเข้ารหัสลับแบบกุญแจสาธารณะนั้น ความต้องการในเรื่อง *ความเป็นส่วนตัว (Privacy)* และ *การยืนยันข้อมูล (Authentication)* จะแยกจากกัน ดังนี้

- **ความเป็นส่วนตัว**

เมื่อผู้ใช้ A ต้องการส่งข่าวสาร M ไปให้กับผู้ใช้ B และ A ทราบกุญแจสาธารณะของ B ผู้ใช้ A ก็จะสามารถส่งข่าวสาร M ไปให้กับ B อย่างเป็นความลับได้ โดยการส่งข่าวสารที่เข้ารหัสลับด้วยกุญแจสาธารณะของ B นั่นคือ $C = E_B(M)$ เมื่อ B ได้รับก็จะถอดรหัสลับ C ด้วยกุญแจส่วนตัวของตนเอง นั่นคือ $D_B(C) = D_B(E_B(M)) = M$ ดังรูปที่ 2.1 ซึ่งผู้อื่นที่ไม่ใช่ B ถึงแม้จะดักฟังข่าวสารมาได้ แต่ก็ไม่สามารถถอดรหัสลับที่ได้มานั้นได้ เพราะไม่มีกุญแจส่วนตัวของ B จะเห็นว่าการส่งข่าวสารวิธีนี้จะไม่รับประกันในเรื่องการยืนยันข้อมูล เนื่องจากผู้ที่รู้กุญแจสาธารณะของ B สามารถปลอมข่าวสารเพื่อส่งให้ B ได้

รูปที่ 2.1 ความเป็นส่วนตัวในระบบกุญแจสาธารณะ

- **การยืนยันข้อมูล**

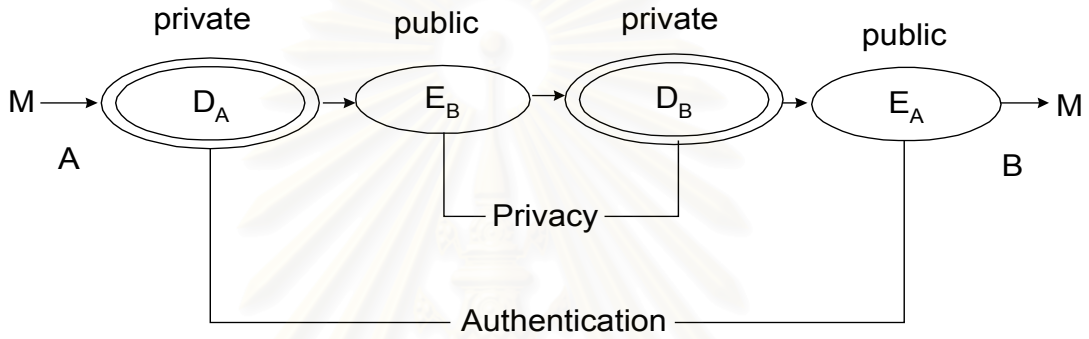
ความต้องการในเรื่องการยืนยันข้อมูล สามารถทำได้โดย A จะเข้ารหัสลับข้อมูลที่จะส่งโดยใช้กุญแจส่วนตัวของตนเอง คือจะส่ง $C = D_A(M)$ ไปให้ B เมื่อ B ได้รับก็จะถอดรหัสโดยใช้กุญแจสาธารณะของ A นั่นคือ $E_A(C) = E_A(D_A(M)) = M$ ดังรูปที่ 2.2 เนื่องจากบทบาทของ E_A และ D_A สามารถสลับกันได้ จะเห็นว่าข่าวสารที่ได้รับมาจาก A อย่างแน่นอนเพราะมี A เพียงคนเดียวที่รู้กุญแจส่วนตัวของ A แต่วิธีนี้จะไม่รับประกันว่าข่าวสารนี้จะเป็นความลับ เนื่องจากผู้ใดก็ตามที่รู้กุญแจสาธารณะของ A จะสามารถถอดรหัสลับได้

รูปที่ 2.2 การยืนยันข้อมูลในระบบกุญแจสาธารณะ

การจะทำให้ระบบการเข้ารหัสลับแบบกุญแจสาธารณะสามารถรับประกันได้ทั้งในเรื่องของความเป็นส่วนตัวและการยืนยันข้อมูล ทำได้โดยเมื่อ A ต้องการติดต่อกับ B ผู้ใช้ A จะเข้ารหัสลับโดยใช้กุญแจส่วนตัวของตนเอง จากนั้นจะเข้ารหัสลับอีกชั้นหนึ่งโดยใช้กุญแจสาธารณะของ B แล้วจึงส่งข้อความที่เข้ารหัสลับแล้ว $C = E_B(D_A(M))$ ไปให้ B เมื่อ B ได้รับก็จะถอดรหัสลับโดย

ใช้กุญแจส่วนตัวของตนเอง แล้วจึงใช้กุญแจสาธารณะของ A มาถอดรหัสลับอีกชั้นหนึ่ง ดังรูปที่ 2.3

ข้อดีของระบบการเข้ารหัสลับแบบกุญแจสาธารณะที่เหนือกว่าระบบการเข้ารหัสลับแบบกุญแจลับ (Secret-key cryptosystem) ก็คือเราสามารถให้กุญแจสาธารณะของเรากับทุก ๆ คนที่เรารู้จักหรือไม่รู้จักก็ได้ เพื่อที่จะสามารถส่งข่าวสารมาถึงเราได้ โดยจะไม่มีผู้ใดที่จะสามารถทราบข่าวสารนั้นได้นอกจากตัวเรา เพราะเราจะเป็นเพียงบุคคลเดียวที่มีกุญแจส่วนตัว แต่ในกรณีของระบบการเข้ารหัสลับแบบกุญแจลับ เราจะให้กุญแจลับ (Secret key) กับบุคคลที่เราไว้ใจเท่านั้น และกุญแจลับที่ให้กับแต่ละคนก็แตกต่างกันด้วย



รูปที่ 2.3 ความเป็นส่วนตัวและการยืนยันข้อมูลในระบบกุญแจสาธารณะ

2.2 ระบบการเข้ารหัสลับด้วยวิธี RSA

RSA เป็นระบบการเข้ารหัสลับแบบกุญแจสาธารณะซึ่งสามารถใช้รองรับความต้องการได้ทั้งความเป็นส่วนตัว (Privacy) โดยใช้ *การเข้ารหัสลับ* และการยืนยันข้อมูล (Authentication) โดยใช้ *ลายเซ็นดิจิตอล* Ron Rivest, Adi Shamir และ Leonard Adleman ได้พัฒนา RSA ขึ้นในปี ค.ศ.1977 [2] คำว่า RSA มาจากอักษรตัวแรกของชื่อท้ายของผู้คิดค้นแต่ละท่าน

2.2.1 การสร้างกุญแจ

การสร้างกุญแจของ RSA มีขั้นตอนดังนี้

- หาจำนวนเฉพาะที่มีค่ามาก 2 ค่า ให้เป็น p และ q
- คำนวณผลคูณ $n = pq$ โดยเรียก n ว่า modulus
- คำนวณหา Euler's totient function [3] ได้ดังนี้

$$\phi(n) = (p-1)(q-1) \tag{2-1}$$

- เลือกค่า e ให้มีค่าน้อยกว่า n และเป็นจำนวนเฉพาะสัมพัทธ์กับ $\phi(n)$ คือ e กับ $\phi(n)$ มี ห.ร.ม. เป็น 1 สาเหตุที่ e ต้องเป็นจำนวนเฉพาะสัมพัทธ์กับ $\phi(n)$

ก็เพื่อ e จะได้มีค่าผกผัน (inverse) โดยปกติแล้วเราจะเลือกค่า e ให้มีค่าน้อย เช่น $e = 2^{16} + 1$

- หาค่า d ที่ทำให้ $(ed - 1)$ หารด้วย $\phi(n)$ ลงตัว หรือ

$$1 = ed \bmod \phi(n) \tag{2-2}$$

(นั่นคือ d เป็นค่าผกผันของ e) ด้วยวิธี extended Euclidean algorithm [3]

- เรียกค่า e และ d ว่า ตัวยกกำลังสาธารณะ (Public exponent) และตัวยกกำลังส่วนตัว (Private exponent) ตามลำดับ
- กุญแจสาธารณะคือ (n, e) และกุญแจส่วนตัวคือ (n, d) ส่วนตัวประกอบ p และ q อาจเก็บไว้กับกุญแจส่วนตัวหรือทิ้งไปก็ได้

ในปัจจุบันนี้ ยังเป็นการยากที่จะหาค่ากุญแจส่วนตัว d จากกุญแจสาธารณะ (n, e) แต่อย่างไรก็ตาม หากสามารถแยกตัวประกอบ n เป็น p กับ q ได้ ก็จะรู้ค่ากุญแจส่วนตัว d ดังนั้น ความปลอดภัยของ RSA จึงตั้งอยู่บนสมมติฐานที่ว่า การแยกตัวประกอบเป็นเรื่องยาก การค้นพบวิธีใหม่ ๆ ที่ทำให้การแยกตัวประกอบง่ายขึ้น ก็จะทำให้ไม่สามารถใช้ RSA ได้ด้วย

2.2.2 การใช้งาน

การใช้งาน RSA อาจแบ่งได้เป็น 2 ประเภท คือ การเข้ารหัสลับกับการใช้ลายเซ็นดิจิตอล (การใช้งานจริงจะใช้โพรโตคอลที่ซับซ้อนกว่าที่กล่าวไว้ในที่นี้)

- **การเข้ารหัสลับ**

สมมติว่า อลิสต้องการส่งข้อความ m ให้กับบ็อบ อลิสจะสร้างรหัสลับ c โดยการยกกำลังตามสมการ

$$c = m^e \bmod n \tag{2-3}$$

โดย e และ n คือกุญแจสาธารณะของบ็อบ เมื่อสร้างเสร็จก็ส่ง c ไปให้บ็อบ

เมื่อบ็อบได้รับรหัสลับ c ก็จะนำมาถอดรหัสลับโดยการยกกำลังเช่นกัน ตามสมการ

$$m = c^d \bmod n \tag{2-4}$$

จากทฤษฎีบทของ Euler [3] ที่ว่า

$$a^{\phi(n)} = 1 \pmod n \tag{2-5}$$

เมื่อให้ n และ a เป็นค่าบวก และเป็นจำนวนเฉพาะสัมพัทธ์กัน และจากความสัมพันธ์ของ e กับ d ตามสมการ (2-2) สามารถเขียนได้เป็น $ed = 1 + k\phi(n)$ เมื่อ k เป็นจำนวนเต็มบางค่า จะได้

$$\begin{aligned} c^d &= (m^e)^d \pmod n \\ &= m^{ed} \pmod n \\ &= m^{1+k\phi(n)} \pmod n \\ &= m \cdot (m^{\phi(n)})^k \pmod n \\ &= m \cdot (1 \pmod n)^k \pmod n \\ &= m \cdot 1 \pmod n \\ &= m \end{aligned}$$

จึงทำให้บ็อบสามารถรู้ข้อความ m ได้อย่างถูกต้อง และเนื่องจากมีบ็อบเพียงคนเดียวที่รู้ค่า d บ็อบจึงเป็นคนเดียวที่สามารถถอดรหัสลับข้อความได้

- **ลายเซ็นดิจิตอล**

ลายเซ็นดิจิตอลจะมีลักษณะแตกต่างจากลายเซ็นที่เซ็นบนกระดาษ คือ เป็นฟังก์ชันของเอกสารดิจิตอล ขณะที่ลายเซ็นบนกระดาษจะเหมือนกันทุกเอกสาร

สมมติว่า อลิสต้องการส่งข้อความ m ให้บ็อบในลักษณะที่รับประกันได้ว่าบ็อบจะได้ข้อความต้นฉบับที่แท้จริงไม่มีการแก้ไข และส่งมาจากอลิสจริง อลิสจะสร้างลายเซ็นดิจิตอล s โดยการยกกำลังตามสมการ $s = m^d \bmod n$ โดย d และ n คือกุญแจส่วนตัวของอลิส เมื่อสร้างเสร็จก็ส่ง m กับ s ไปให้บ็อบ

เมื่อบ็อบได้รับข้อความ m กับลายเซ็นดิจิตอล s ก็จะนำมาตรวจสอบลายเซ็นโดยการยกกำลังเช่นกัน ตามสมการ $m = s^e \bmod n$ โดย e และ n คือกุญแจสาธารณะของอลิส แล้วตรวจสอบค่า m ว่าตรงกันหรือไม่

จะเห็นว่าทั้งความเป็นส่วนตัวและการยืนยันข้อมูลสามารถเกิดขึ้นได้โดยปราศจากการเปิดเผยข้อมูลกุญแจส่วนตัว แต่ละคนจะใช้เพียงกุญแจสาธารณะของคนอื่นและกุญแจส่วนตัวของคนผู้นั้นเอง ทุกคนสามารถส่งข้อความที่เข้ารหัสลับแล้ว และสามารถตรวจสอบข้อความที่มีลายเซ็นกำกับไว้ แต่มีเพียงคนเดียวที่เป็นเจ้าของกุญแจส่วนตัวที่ถูกต้องที่สามารถถอดรหัสลับหรือเซ็นข้อความได้

2.2.3 ตัวอย่างการคำนวณ

สมมติให้ $p = 5$ และ $q = 7$ เราสามารถสร้างกุญแจได้โดย

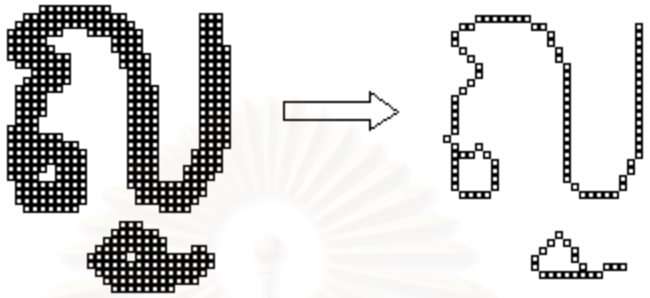
- หาผลคูณ $n = pq = 5x7 = 35$
- คำนวณค่า $(p-1)(q-1) = 4x6 = 24$
- เลือก e ที่มีค่าน้อยกว่า 24 และเป็นจำนวนเฉพาะสัมพัทธ์กับ 24 ในที่นี้เลือก 11
- หาค่า d ที่ทำให้ $1 = 11 \cdot d \bmod 24$ จะได้ $d = 11$

เมื่อต้องการเข้ารหัสลับข้อความ $m = 2$ จะได้ $c = m^e \bmod n = 2^{11} \bmod 35 = 18$

จากนั้น ทำการถอดรหัสลับข้อความ จะได้ $m = c^d \bmod n = 18^{11} \bmod 35 = 2$

2.3 กระบวนการทำโครงร่างภาพ

กระบวนการทำโครงร่างภาพ เป็นการทำให้ความหนาของภาพต้นแบบเปลี่ยนแปลงไป แต่ยังคงเค้าโครงเดิมอยู่ โดยความหนาของภาพจะเหลือเพียงหนึ่งจุดภาพ ดังแสดงในรูปที่ 2.4



(ก) (ข)

รูปที่ 2.4 กระบวนการทำโครงร่างภาพ (ก) ภาพต้นแบบ (ข) ภาพที่ผ่านการทำโครงร่างภาพ

ภาพที่ผ่านกระบวนการทำโครงร่างภาพจะได้คุณลักษณะของจุดต่อในภาพโครงร่าง เช่น จุดปลาย จุดต่อเนื่อง จุดแยกสาม จุดแยกสี่ เป็นต้น

การทำโครงร่างภาพ จะใช้ในการเขียนโปรแกรมเพื่อหาจุดปลายของกลุ่มจุดดำในภาพ ซึ่งเป็นขั้นตอนหนึ่งในการดึงคุณลักษณะเฉพาะตัวของกระดาษ

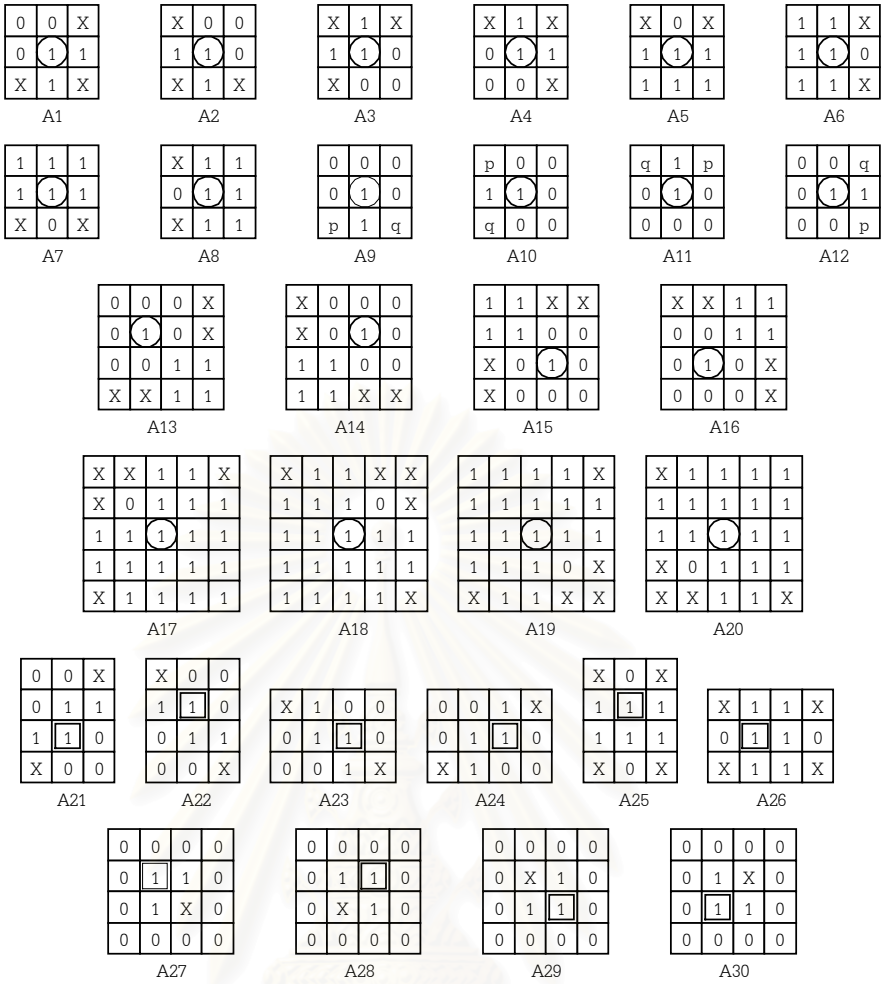
เนื่องจากการทำโครงร่างภาพมีอยู่ด้วยกันหลายวิธี วิธีที่ได้เลือกใช้คือวิธี One-Pass Parallel Thinning [4] ของ Ben K. Jang และ Roland T. Chin เพราะให้รายละเอียดคุณลักษณะของจุดต่อภาพได้ดีเพียงพอ โดยมีแม่แบบ (Template) ที่ใช้ในการทำโครงร่างภาพทั้งหมด 30 แบบ ซึ่งแม่แบบ A1 ถึง A20 เป็นแม่แบบการทำโครงร่างภาพ ในขณะที่ A21 ถึง A30 เป็นแม่แบบการเรียกกลับคืน (Restoring) p และ q เป็นตัวดำเนินการทางตรรกศาสตร์ : p or $q = 1$ และ X เป็นค่าที่ไม่สนใจ ดังแสดงในรูปที่ 2.5

ระเบียบวิธีการทำโครงร่างภาพ

1. จุดภาพจะถูกทำการตรวจสอบตามแม่แบบการทำโครงร่างภาพทั้งหมด

2. หากจุดภาพที่ถูกตรวจอยู่ในแม่แบบ A1 ถึง A20 จะถูกลบจุดภาพ ในขณะที่จุดภาพอยู่ในแม่แบบ A21 ถึง A30 จะถูกกู้กลับคืนมา

3. เมื่อภาพผ่านกระบวนการทำโครงร่างภาพจะเหลือความกว้างของภาพเพียง 1 จุดภาพ



รูปที่ 2.5 แม่แบบการทำโครงร่างภาพ

2.4 **รหัสแท่ง** Code 128

Code 128 [5 6 7 และ 8] เป็นรหัสแท่งสำหรับตัวอักษรและตัวเลขที่มีความหนาแน่นสูงมาก มีความยาวไม่จำกัด แล้วแต่ความยาวของข้อมูล สามารถเข้ารหัสตัวอักขระแอสกีได้ทั้ง 128 ตัว

2.4.1 **ลักษณะของรหัสแท่ง** Code 128

โครงสร้างของรหัสแท่ง Code 128 มีลักษณะดังรูปที่ 2.6 ประกอบด้วย

- เขตว่างเปล่า (Quiet zone) บริเวณด้านซ้ายของรหัสแท่ง
- ตัวอักขระเริ่มต้น (Start character)
- ข้อมูลที่เข้ารหัสไว้
- ตัวอักขระตรวจสอบ (Check character)
- ตัวอักขระหยุด (Stop character)

- เขตว่างเปล่า (Quiet zone) บริเวณด้านขวาของรหัสแท่ง

เขตว่างเปล่า (Quiet zone) ควรมีความกว้างอย่างน้อย 10 เท่าของความกว้างมอดูล

รูปที่ 2.6 ลักษณะของรหัสแท่ง Code 128

รหัสของตัวอักขระแต่ละตัวจะประกอบด้วยมอดูล (Module) สีขาวหรือดำรวม 11 มอดูล ยกเว้นตัวอักขระหยุด (Stop character) จะมี 13 มอดูล แถบดำ 3 แถบและช่องว่าง 3 ช่อง ซึ่งวางตัวสลับกันจะถูกสร้างขึ้นจากมอดูล 11 มอดูลนี้ โดยแถบดำแต่ละแถบและช่องว่างแต่ละช่องจะมีความกว้างได้ตั้งแต่ 1 ถึง 4 มอดูล ส่วนตัวอักขระหยุดจะมีแถบดำ 4 แถบและช่องว่าง 3 ช่อง เนื่องจากเป็นตัวสุดท้ายจึงมีแถบดำปิดท้ายอีก 1 แถบ

Code 128 มีชุดของตัวอักขระแตกต่างกัน 3 ชุด คือ ชุด A, ชุด B และ ชุด C แถบดำ 3 แถบและช่องว่าง 3 ช่อง จะถูกสร้างขึ้นให้มีลักษณะต่างกัน 106 แบบ แต่ละแบบจะถูกกำหนดให้กับตัวอักขระที่แตกต่างกันขึ้นกับชุดที่เลือกว่าเป็นชุด A, B หรือ C แต่ละชุดประกอบด้วยตัวอักขระที่แตกต่างกันดังนี้

- <u>ชุด A</u> ประกอบด้วยตัวอักษรตัวพิมพ์ใหญ่ เครื่องหมายวรรคตอน ตัวเลข (รหัสแอสกี 32 ถึง 95) และตัวอักขระควบคุม (Control character) เช่น return, tab (รหัสแอสกี 0 ถึง 31)
- <u>ชุด B</u> ประกอบด้วยตัวอักษรทั้งตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก เครื่องหมายวรรคตอน ตัวเลข (รหัสแอสกี 32 ถึง 127)
- <u>ชุด C</u> ประกอบด้วยตัวเลขเพียงอย่างเดียว โดยมีคู่ของตัวเลขตั้งแต่ 00 ถึง 99 รหัส 1 ตัว สามารถแทนตัวเลขได้ 1 คู่ จึงทำให้รหัสชุดนี้มีความหนาแน่นสูงขึ้นเป็น 2 เท่า

การเลือกชุดแต่ละชุดสามารถทำได้โดยใช้ตัวอักขระเริ่มต้นของชุดนั้น และภายในสัญลักษณ์ยังมีรหัส CODE และ SHIFT ซึ่งสามารถใช้เปลี่ยนชุดไปมาได้ โดยถ้าใช้รหัส CODE จะหมายถึงว่า รหัสที่ตามมาทั้งหมดนั้นจะเปลี่ยนชุดเป็นรหัสของชุดดังกล่าว ส่วนรหัส SHIFT นั้น จะ

เปลี่ยนรหัสของตัวอักขระถัดไปเพียง 1 ตัว ซึ่งจะเป็นการเปลี่ยนจากชุด A เป็นชุด B หรือชุด B เป็นชุด A เท่านั้น

นอกจากนี้ ยังมีรหัสฟังก์ชัน (Function code) FNC1 ถึง FNC4

- FNC1 ใช้สำหรับรหัสแท่ง EAN/UCC 128 โดยใช้ตัวอักขระเริ่มต้น Start C แล้วตามด้วย FNC1 แล้วต่อด้วยรหัสข้อมูลซึ่งใช้การเข้ารหัสเช่นเดียวกับ Code 128
- FNC2 ใช้เพื่อสั่งให้เครื่องอ่านรหัสแท่งรออ่านรหัสแท่งอันต่อไปแล้วนำข้อมูลมาต่อกับข้อมูลที่อ่านได้จากรหัสแท่งนี้
- FNC3 ใช้เพื่อสั่งให้เครื่องอ่านรหัสแท่ง reset
- FNC4 ยังไม่กำหนดให้ใช้กับสิ่งใดโดยเฉพาะ

2.4.2 การหาค่าตัวอักขระตรวจสอบ

รหัสของตัวอักขระแต่ละตัวจะมีค่ากำหนดไว้ตั้งแต่ 0 ถึง 105 ค่าเหล่านี้จะนำมาใช้ในการหาตัวอักขระตรวจสอบดังนี้

- นำค่าของรหัสของข้อมูลทุกตัวมาคูณกับตำแหน่งที่อยู่ในรหัสแท่ง โดยตำแหน่งของข้อมูลที่อยู่ซ้ายสุดมีค่าเป็น 1
- นำผลคูณที่ได้มาบวกกัน แล้วบวกกับค่าของตัวอักขระเริ่มต้น
- นำผลบวกที่ได้มาหาค่าเศษจากการหารด้วย 103 แล้วใช้เศษเป็นตัวอักขระตรวจสอบ

ตัวอย่างเช่น ข้อมูลคือ *Code 128* สามารถหาตัวอักขระตรวจสอบได้ดังนี้

รหัส	ตำแหน่ง	ค่า	ผลคูณ
C	1	35	35
o	2	79	158
d	3	68	204
e	4	69	276
	5	0	0
1	6	17	102
2	7	18	126
8	8	24	192
Start B			104
ผลรวม			1197
หารด้วย 103 เหลือเศษ			64

2.4.3 ขนาดของรหัสแท่ง

ความยาวของรหัสแท่งสามารถหาได้จากสมการ

$$L = (11 \cdot C + 35) \cdot X \quad (2\text{-}6)$$

โดย L คือ ความยาวของรหัสแท่ง (ไม่รวมเขตว่างเปล่า)

C คือ จำนวนรหัสของตัวอักขระ ซึ่งรวมถึงรหัส SHIFT, CODE และ FNC

X คือ ความกว้างของมอดูล

ความสูงของรหัสแท่งต้องมีค่าอย่างน้อย 15 % ของความยาวของรหัสแท่ง และต้องไม่น้อยกว่า 0.25 นิ้ว

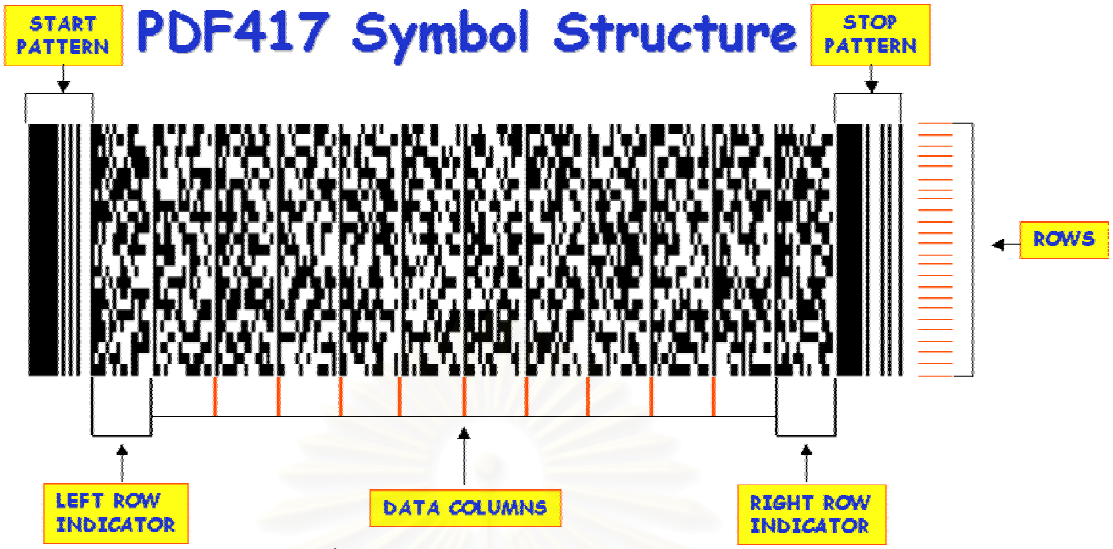
2.5 รหัสแท่ง 2 มิติ PDF417

PDF417 [9 และ10] เป็นรหัสแท่ง 2 มิติ สามารถใช้เก็บข้อมูลได้มากกว่า 1 กิโลไบต์ การสร้างรหัสแท่ง 2 มิติเริ่มจากการแปลงข้อมูลเป็นคำรหัส (Codeword) ที่มีค่าตั้งแต่ 0 – 928 หลังจากนั้นจะนำคำรหัสไปเปลี่ยนให้อยู่ในรูปแบบของแถบดำและช่องว่าง (Bar space pattern) ได้รหัสแท่ง 2 มิติออกมา ข้อดีหนึ่งของรหัสแท่ง PDF417 ก็คือ ความสามารถในการแก้ไขความผิดพลาดที่เกิดจากคำรหัสถูกทำลายหรือถอดรหัสข้อมูลผิดพลาดได้โดยใช้รหัสแก้ไขความผิดพลาดรีดโซโลมอน (Reed Solomon error correction code) รหัสแท่งชนิดนี้จะถูกเลือกมาใช้ในขั้นตอนการพิมพ์รหัสลับลงบนบัตรเลือกตั้ง เนื่องจากกระดาษที่ใช้จัดพิมพ์มีเศษผงและเส้นใยฝังอยู่จึงอาจจะทำให้รหัสแท่งที่พิมพ์ลงบนบัตรเลือกตั้งเสียหายไปบางส่วนได้

2.5.1 ลักษณะของรหัสแท่ง PDF417

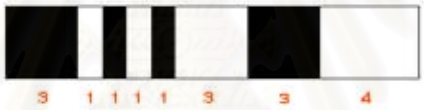
โครงสร้างของรหัสแท่ง PDF417 มีลักษณะดังรูปที่ 2.7 ซึ่งประกอบด้วย

- เขตว่างเปล่า (Quiet zone) บริเวณด้านซ้าย, ขวา, บน ,ล่าง ของรหัสแท่ง
- รูปแบบเริ่มต้น (Start pattern)
- ตัวชี้แถวทางด้านซ้าย (Left row indicator)
- ข้อมูล (Data)
- ตัวชี้แถวทางด้านขวา (Right row indicator)
- รูปแบบหยุด (Stop pattern)



รูปที่ 2.7 ลักษณะของรหัสแท่ง 2 มิติ PDF417

โครงสร้างของคำรหัสมีลักษณะดังรูปที่ 2.8



รูปที่ 2.8 ตัวอย่างของคำรหัสในรหัสแท่ง 2 มิติ PDF417

แต่ละคำรหัสในรหัสแท่ง PDF417 จะประกอบด้วยมอดูล (Module) สีขาวและดำรวมกัน 17 มอดูล ยกเว้นรูปแบบหยุด จะมี 18 มอดูล คำรหัสโดยทั่วไปที่ไม่ใช่รูปแบบหยุดจะมีแถบดำ 4 แถบและแถบช่องว่าง 4 แถบ ซึ่งวางตัวสลับกัน โดยแถบดำแต่ละแถบและแถบช่องว่างแต่ละแถบของคำรหัสจะมีความกว้างได้ตั้งแต่ 1 ถึง 6 มอดูล ส่วนรูปแบบหยุดจะมีแถบดำ 5 แถบและแถบช่องว่าง 4 แถบ เนื่องจากเป็นอยู่ตำแหน่งสุดท้ายจึงมีแถบดำปิดท้ายอีก 1 แถบ รูปแบบหยุดมีรูปแบบแถบดำและช่องว่างดังนี้ 711311121 รูปแบบเริ่มต้นมีรูปแบบแถบดำและช่องว่างดังนี้ 81111113

เนื่องจากรหัสแท่ง 2 มิติ PDF417 มีแถวของคำรหัสหลายๆ แถวซ้อนกันอยู่จึงอาจทำให้การถอดรหัส PDF417 ผิดพลาดได้ อย่างกรณีที่รหัสแท่ง PDF417 เอียง อาจจะทำให้อ่านข้อมูลข้ามแถวได้ เพื่อแก้ปัญหานี้จึงได้แบ่งกลุ่มของคำรหัสออกเป็น 3 กลุ่ม (Cluster) คือ กลุ่ม 0 กลุ่ม 1 และ กลุ่ม 2 แต่ละกลุ่มจะมีคำรหัสตั้งแต่ 0-928 โดยคำรหัสเดียวกันแต่อยู่ต่างกลุ่มจะมีรูปแบบแถบดำและช่องว่างแตกต่างกัน อย่างเช่น คำรหัส 5 ในกลุ่ม 0 จะมีรูปแบบแถบดำและช่องว่างต่างจากคำรหัส 5 ในกลุ่ม 1 และกลุ่ม 2 ดังนี้

คำรหัส 5 ในกลุ่ม 0 จะมีรูปแบบแถบดำและช่องว่าง 51111251

คำรหัส 5 ในกลุ่ม 1 จะมีรูปแบบแถบดำและช่องว่าง 41111311

คำรหัส 5 ในกลุ่ม 2 จะมีรูปแบบแถบดำและช่องว่าง 11111345

โดยการแบ่งกลุ่มของคำรหัสจะขึ้นอยู่กับหมายเลขแถวที่คำรหัสนั้นอยู่ ถ้าอยู่แถวแรกก็จะใช้รูปแบบแถบดำและช่องว่างกลุ่ม 0 ถ้าอยู่แถวที่ 2 ก็จะใช้รูปแบบแถบดำและช่องว่างกลุ่ม 1 ถ้าอยู่แถวที่ 3 ก็จะใช้รูปแบบแถบดำและช่องว่างกลุ่ม 2 และถ้าอยู่แถวที่ 4 ก็จะใช้รูปแบบแถบดำและช่องว่างกลุ่ม 0 วนไปเรื่อยๆ โดยแถวที่ติดๆ กันจะใช้รูปแบบแถบดำและช่องว่างในกลุ่มที่ต่างกัน ดังนั้นถ้าเกิดการอ่านข้อมูลข้ามแถวไปเจอรูปแบบแถบดำและช่องว่างที่อยู่ในกลุ่มอื่นที่ไม่ใช่กลุ่มในแถวนั้น ก็จะรู้ว่าอ่านข้อมูลรหัสแท่งข้ามแถว จะต้องบิดเอียงภาพให้ตรงเพื่อที่จะอ่านข้อมูลรหัสแท่งได้ถูกต้อง

สำหรับตัวชี้แถวทางด้านซ้ายและตัวชี้แถวทางด้านขวาสามารถคำนวณได้จากข้อมูลหมายเลขหลัก, หมายเลขแถว, จำนวนหลัก, จำนวนแถว และระดับความปลอดภัย ซึ่งแสดงการคำนวณได้ดังตารางที่ 2.1 นี้

ตารางที่ 2.1 การคำนวณตัวชี้แถวทางซ้ายและตัวชี้แถวทางขวา

แถว	ตัวชี้แถวทางซ้าย	ตัวชี้แถวทางขวา
0	30*(หมายเลขของแถว div 3)+((จำนวนของแถว - 1) div 3)	30*(หมายเลขของแถว div 3)+(จำนวนของหลัก - 1)
1	30*(หมายเลขของแถว div 3)+ระดับความปลอดภัย*3+(จำนวนของแถว - 1) mod 3	30*(หมายเลขของแถว div 3)+((จำนวนของแถว - 1) div 3)
2	30*(หมายเลขของแถว div 3)+(จำนวนของหลัก - 1)	30*(หมายเลขของแถว div 3)+ระดับความปลอดภัย*3+(จำนวนของแถว - 1) mod 3

จำนวนแถวของข้อมูลในรหัสแท่ง PDF417 จะมีได้ตั้งแต่ 3 แถว จนถึง 90 แถว ส่วนจำนวนหลักของข้อมูลจะมีได้ตั้งแต่ 1 หลัก จนถึง 30 หลัก

2.5.2 รหัสแก้ไขความผิดพลาด

รหัสแท่ง 2 มิติ PDF417 สามารถแก้ไขความผิดพลาดของข้อมูลได้ โดยใช้รหัสแก้ไขความผิดพลาดรีดโซโลมอน (Reed Solomon) ซึ่งสามารถเลือกระดับของการแก้ไขความผิดพลาดได้ตั้งแต่ระดับ 0 จนถึง 8 โดยระดับ 0 จะทำได้เพียงตรวจจับความผิดพลาดว่ามีความผิดพลาดเกิดขึ้นหรือไม่ แต่ไม่สามารถแก้ไขความผิดพลาดได้ สำหรับระดับ 1 จนถึง 8 จะทำได้ทั้งตรวจจับความผิดพลาดและแก้ไขคำรหัสให้ถูกต้องได้ ระดับการแก้ไขข้อมูลที่ถูกแนะนำให้ใช้กับรหัสแท่งที่มีความยาวของคำรหัสต่างๆ กัน แสดงได้ดังตารางที่ 2.2 ดังนี้

ตารางที่ 2.2 ระดับการแก้ไขข้อมูลที่ถูกแนะนำให้ใช้กับคำรหัสที่มีความยาวต่างๆ กัน

จำนวนของคำรหัส	ระดับการแก้ไขข้อมูล	จำนวนคำรหัสถูกทำลายที่สามารถแก้ไขได้
1-40	2	3
41-160	3	7
161-320	4	15
321-863	5	31

จากตารางที่ 2.2 แสดงระดับการแก้ไขข้อมูลที่ถูกแนะนำให้ใช้กับคำรหัสที่มีความยาวต่างๆ กัน แต่ถ้ารหัสแท่ง 2 มิติ ถูกใช้ในสภาวะแวดล้อมที่อาจจะทำให้คำรหัสของรหัสแท่งถูกทำลายไปอย่างมาก ก็อาจจะเพิ่มระดับการแก้ไขข้อมูลได้ดังตารางที่ 2.3 นี้

ตารางที่ 2.3 ระดับการแก้ไขข้อมูลทั้งหมด

ระดับการแก้ไขข้อมูล	จำนวนคำรหัสถูกทำลายที่สามารถแก้ไขได้
1	1
2	3
3	7
4	15
5	31
6	63
7	127
8	255

2.5.3 การเข้ารหัสข้อมูล

ข้อมูลที่จะนำมาเข้ารหัสรหัสแท่ง PDF417 จะต้องถูกเปลี่ยนเป็นคำรหัสก่อน โดยแบบแผนที่จะใช้ในการเข้ารหัสจะแตกต่างกันตามชนิดของข้อมูลที่จะเข้ารหัสซึ่งโมด (mode) ในการเข้ารหัส มีดังนี้

- โมดกระชับตัวอักขระ (Text compaction mode)
- โมดกระชับไบต์ (Byte compaction mode)
- โมดกระชับตัวเลข (Numeric compaction mode)

การเปลี่ยนจากโมดเข้ารหัสแบบหนึ่งไปยังโมดเข้ารหัสอีกแบบหนึ่งสามารถทำได้โดยใช้โมดแลทช์ชิฟท์ (Latchesshifts) สำหรับข้อมูลในแต่ละโมดจะใช้คำรหัสต่างๆ กันอยู่ 900 คำรหัส ตั้งแต่คำรหัส 0 - 899 และที่เหลืออีก 29 คำรหัส ตั้งแต่ 900 จนถึง 928 จะถูกกำหนดให้เป็นฟังก์ชันพิเศษที่กำหนดเฉพาะในแต่ละโมด

2.5.3.1 โมดกระชับตัวอักขระ

ประกอบด้วยตัวอักขระแอสกีทั้งหมด โดยโมดกระชับตัวอักขระจะประกอบด้วย 4 โมดย่อย (Sub-mode) ดังนี้

- โมดย่อยอัลฟา (Alpha) ประกอบด้วยตัวอักษรภาษาอังกฤษตัวใหญ่
- โมดย่อยต่ำ (Lower) ประกอบด้วยตัวอักษรภาษาอังกฤษตัวเล็ก
- โมดย่อยผสม (Mixed) ประกอบด้วยตัวเลขและเครื่องหมายวรรคตอนบางตัว
- โมดย่อยเครื่องหมายวรรคตอน (Punctuation) ประกอบด้วยเครื่องหมายวรรคตอนที่เหลือจากโมดผสม

แต่ละโมดย่อยข้างต้น จะประกอบด้วย ตัวอักขระ 30 ตัว รวมทั้งโมดย่อยแลทช์ (Sub-mode latch) และตัวอักขระชิฟท์ (Shift characters)

ในการเข้ารหัสรหัสแท่ง PDF417 โมดเริ่มต้น (Default mode) ที่ถูกกำหนดไว้ได้แก่โมดกระชับตัวอักขระซึ่งใช้โมดย่อยอัลฟา ถ้าจะเปลี่ยนจาก โมดนี้ไปเป็นโมดอื่นๆ จะต้องใช้ คำรหัสแลทช์ (Latch)

2.5.3.2 โมดกระชับไบต์

โมดกระชับไบต์จะถูกนำมาใช้ในงานวิจัยนี้ เนื่องจากข้อมูลที่จะนำมาเข้ารหัสรหัสแท่ง 2 มิติ จะเป็นตัวอักขระแอสกีในรูปแบบเลขฐาน 16 ซึ่งโมดนี้ประกอบด้วยตัวอักขระ 256 ตัว โดยจะรวมอักขระแอสกีที่มีค่าตั้งแต่ 0 – 127 โมดนี้จะสามารถเข้ารหัสข้อมูลได้ 6 ไบต์ต่อ 5 คำรหัส คิดเป็นสัดส่วนได้ 1.2 ไบต์ ต่อ 1 คำรหัส

สำหรับการเปลี่ยนจากโมดอื่นมายังโมดกระชับไบต์ ทำได้โดยใช้โมดแลทช์ดังนี้

- โมดแลทช์ 924 จะใช้เมื่อจำนวนตัวอักขระทั้งหมดในโมดกระชับไบต์หารด้วย 6 ลงตัว
- โมดแลทช์ 901 จะใช้เมื่อจำนวนตัวอักขระทั้งหมดในโมดกระชับไบต์หารด้วย 6 ไม่ลงตัว
- โมดแลทช์ 913 สามารถใช้แทนโมดแลทช์ 901 ได้ เมื่อต้องการเข้ารหัสตัวอักขระตัวเดียวในโมดกระชับไบต์

สำหรับขั้นตอนที่ใช้ในการเข้ารหัสตัวอักขระในโมดกระชับไบต์ แสดงตัวอย่างได้ดังนี้

ต้องการนำข้อมูล $(18BB439443147B28)_{16}$ ไปเข้ารหัสรหัสแท่ง 2 มิติ PDF417

ขั้นที่ 1 นับขนาดข้อมูลทั้งหมดได้ 8 ไบต์ ซึ่งหารด้วยเลข 6 ไม่ลงตัว จึงต้องใช้โมดแลทช์ 901 ในการเปลี่ยนจากโมดเริ่มต้นมาเป็นโมดกระชับไบต์

ขั้นที่ 2 เปลี่ยนจากเลขฐาน 16 ไปเป็นเลขฐาน 256 จะได้

$(18BB439443147B28)_{16} = (24,187,67,148,67,20,123,40)_{256}$

ขั้นที่ 3 แบ่งข้อมูลออกเป็นกลุ่มๆ โดยแต่ละกลุ่มจะมีข้อมูลขนาด 6 ไบต์ จะได้

กลุ่มที่มีข้อมูลครบ 6 ไบต์ได้แก่

$(18BB43944314)_{16} = (24,187,67,148,67,20)_{256}$

กลุ่มที่มีข้อมูลไม่ครบ 6 ไบต์ ได้แก่

$(7B28)_{16} = (123,40)_{256}$

ขั้นที่ 4 หาผลรวมของข้อมูลในกลุ่มที่มีข้อมูลครบ 6 ไบต์ จะได้

ผลรวมของข้อมูล $= 24*256^5 + 187*256^4 + 67*256^3 + 148*256^2 + 67*256^1 + 20*256^0$

$= 27,192,571,740,948$

ขั้นที่ 5 นำผลรวมของข้อมูลซึ่งเป็นเลขฐาน 10 มาเปลี่ยนเป็นข้อมูลในรูปแบบเลขฐาน 900 จะได้

ผลรวมของข้อมูล$=27,192,571,740,948= 41*900^4+401*900^3+176*900^2+201*900^1+48*900^0$

$= (41,401,176,201,48)_{900}$

ขั้นที่ 6 นำข้อมูลในกลุ่มที่มีตัวอักขระไม่ครบ 6 ตัวมาเปลี่ยนเป็นคำรหัส 1 คำรหัสต่อ 1 ไบต์

จะได้คำรหัส 123,40

นำคำรหัสทั้งหมดมารวมกันจะได้คำรหัส 901,41,401,176,201,48,123,40

ขั้นที่ 7 นำคำรหัสที่ได้ไปคำนวณหาคำรหัสที่ใช้ในการแก้ไขข้อมูลผิดพลาด โดยความสามารถในการแก้ไขข้อมูลผิดพลาดจะขึ้นอยู่กับระดับการแก้ไขข้อมูลที่เลือกไว้

ขั้นที่ 8 นำคำรหัสทั้งหมดที่ได้ไปเปลี่ยนให้อยู่ในรูปแบบแถบดำและช่องว่างตามกลุ่มที่คำรหัสนั้นอยู่ จะได้รหัสแท่ง 2 มิติ PDF417 ออกมา

2.5.3.3 โมดกระชับตัวเลข

โมดกระชับตัวเลขใช้ในการเก็บข้อมูลเลขฐาน 10 โดยโมดกระชับตัวเลขจะสามารถเข้ารหัสเลขโดดได้ 2.93 ตัวต่อ 1 คำรหัส ถ้าจะเปลี่ยนจากโมดอื่นๆ มาเป็นโมดกระชับตัวเลขจะต้องใช้โมดแลทช์ 902

2.6 **แฮชฟังก์ชัน**

แฮชฟังก์ชัน [11 และ 12] เป็นการแปลงข้อมูลขาเข้า (m) โดยคืนค่าอักขระขาออกที่มีความยาวคงที่ออกมา ซึ่งจะเรียกอักขระเหล่านั้นว่าค่าแฮช (Hash value) ถ้าให้ h คือค่าแฮช และ $H(x)$ คือแฮชฟังก์ชัน จะได้ความสัมพันธ์ดังนี้

$$h = H(m) \tag{2-7}$$

คุณสมบัติพื้นฐานเกี่ยวกับแฮชฟังก์ชันมีดังนี้

- ข้อมูลขาเข้ามีความยาวเท่าใดก็ได้
- ข้อมูลขาออกมีความยาวคงที่
- $H(x)$ สามารถคำนวณได้ง่ายสำหรับข้อความ x ใดๆ
- $H(x)$ มีลักษณะไปทางเดียว (One way)
- $H(x)$ มีการอิสระในการชน (Collision free)

แฮชฟังก์ชัน ($H(x) = h$) มีลักษณะไปทางเดียว หมายความว่า ถ้าให้ค่าแฮช h มา จะหาข้อมูลขาเข้า x ได้ยาก และถ้าให้ข้อความ x มา เป็นไปได้ยากที่จะคำนวณหาข้อความ y ซึ่งไม่เท่ากับ x แล้วได้ $H(x) = H(y)$ ซึ่งถ้าเกิดกรณีนี้ขึ้น แฮชฟังก์ชันนั้นจะถูกเรียกว่าแฮชฟังก์ชันที่มีการอิสระในการชนอย่างอ่อน (Weakly collision-free hash function) และจะถูกเรียกว่าแฮชฟังก์ชันที่มีอิสระในการอย่างแข็ง (Strongly collision-free hash function) เมื่อไม่สามารถหาข้อความ x และ y ที่มีค่า $H(x) = H(y)$

แฮชฟังก์ชันถูกนิยามในรูปของ ฟังก์ชันบีบอัด (Compression function) ฟังก์ชันบีบอัดจะรับข้อมูลขาเข้าที่มีความยาวคงที่เข้าไปและคืนค่าที่มีความยาวคงที่แต่สั้นกว่าออกมา จากรูปที่ 2.9 ข้อความที่มีความยาวใดๆ ถูกแบ่งออกเป็นกลุ่ม ซึ่งความยาวของแต่ละกลุ่มขึ้นอยู่กับฟังก์ชันบีบอัดและข้อความเติมให้เต็ม (Padded) ดังนั้นขนาดของข้อความทั้งหมดก็จะเป็นจำนวนเท่าของขนาดกลุ่ม และแต่ละกลุ่มก็จะเปรียบเสมือนเป็นข้อมูลขาเข้าของฟังก์ชันบีบอัดและข้อมูลขาออกสุดท้ายก็จะได้ค่าแฮชออกมา

2.7 **รหัสรีดโซโลมอน** (Reed-Solomon Codes)

รหัสรีดโซโลมอน [13 และ 14] เป็นรหัส BCH (Bose-Chaudhuri-Hocquenghem Codes) ชนิดที่ไม่ใช่สองระดับ (Non-binary) กล่าวคือรหัส BCH จะมีค่าสัมประสิทธิ์ของพหุนามเป็นส่วนประกอบของ กาลัวส์ฟิลด์ 2 (Galois Field 2 (GF2)) ซึ่งได้แก่ 0 กับ 1 แต่ในส่วนของรหัสรีดโซโลมอน ค่าสัมประสิทธิ์ของพหุนามจะเป็นส่วนประกอบของ GF(p) หรือ GF(2^m) โดยที่ p คือจำนวนเฉพาะใดๆ และ m คือจำนวนนับใดๆ ที่มีค่าตั้งแต่ 0,1,2,...

สำหรับ GF(p) จะมี 0,1,2,..., $p-1$ เป็นส่วนประกอบ และ GF(2^m) จะมี $\alpha^0, \alpha^1, \alpha^2, ..., \alpha^{2^m-1}$ เป็นส่วนประกอบ โดยที่ α^i คือสัญลักษณ์ที่สามารถแทนได้ด้วยเลขฐานสองจำนวน m บิต และ i มีค่า 0,1,2,..., 2^m-1

รหัสรีดโซโลมอนถูกนำมาประยุกต์ใช้งานในด้านการสื่อสารผ่านดาวเทียมสำหรับข้อมูลเสียง และสัญญาณโทรทัศน์ตามมาตรฐานการสื่อสารโทรคมนาคมยุโรป (European Telecommunication Standard) โดยใช้รหัสรีดโซโลมอนบน GF(2^4) หรือ GF(16) ที่มี $\alpha^0, \alpha^1, \alpha^2, ..., \alpha^{15}$ เป็นส่วนประกอบ โดย α^i คือสัญลักษณ์ที่สามารถแทนได้ด้วยเลขฐานสองจำนวน 4 บิต ตามตารางที่ 2.4

ตารางที่ 2.4 แสดงเลขฐานสองจำนวน 4 บิตของ GF(2^4) เมื่อ $\alpha^4 = \alpha + 1$

ค่า	เลขฐานสองจำนวน 4 บิต
α^0	(1 0 0 0)
α^1	(0 1 0 0)
α^2	(0 0 1 0)
α^3	(0 0 0 1)
α^4	(1 1 0 0)
α^5	(0 1 1 0)
α^6	(0 0 1 1)
α^7	(1 0 0 1)
α^8	(1 0 1 0)
α^9	(0 1 0 1)
α^{10}	(1 0 0 0)
α^{11}	(1 1 1 0)
α^{12}	(0 1 1 1)
α^{13}	(1 1 1 1)
α^{14}	(1 0 1 1)
α^{15}	(1 0 0 0)

2.7.1 การเข้ารหัสรีดโซโลมอน

ในการเข้ารหัสรีดโซโลมอน จะมองข้อมูลในรูปแบบของสัญลักษณ์ จึงเขียนข่าวสาร $a(x)$ ในรูปแบบพหุนามได้ดังนี้

$$a(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + ... + a_2x^2 + a_1x + a_0 \qquad (2\text{-}8)$$

โดย $(a_{k-1}, a_{k-2}, ..., a_2, a_1, a_0)$ เป็นส่วนประกอบของ GF(2^m) หรือ GF(p)

เมื่อต้องการให้รหัสรีดโซโลมอนสามารถแก้ไขข่าวสารผิดพลาดได้ t สัญลักษณ์ (t symbol-error-correction) ต้องใช้พหุนามตัวกำเนิดที่มีรากของสมการเป็น $\alpha^1, \alpha^2, \alpha^3 ..., \alpha^{2t}$ ดังสมการที่ (2-9)

$$G(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)....(x-\alpha^{2t}) \quad (2\text{-}9)$$

ในการส่งข้อมูลคำรหัส $(c(x))$ สามารถทำได้ โดยใช้พหุนามที่ยกกำลังเท่ากับความยาวของคำรหัสลบด้วยความยาวของข่าวสารที่ต้องการจะส่ง $(n-k)$ และนำไปคูณกับข่าวสารที่ต้องการจะส่ง $(a(x))$ จากนั้นจึงนำไปหารด้วยพหุนามตัวกำเนิด $(x^{n-k}a(x)/G(x))$ แล้วจึงนำเศษของการหาร ($b(x)$) ไปรวมกับ $x^{n-k}a(x)$ ได้คำรหัสที่จะส่งดังนี้

$$c(x) = x^{n-k}a(x) + b(x) \quad (2\text{-}10)$$

ตัวอย่างการเข้ารหัสรีดโซโลมอน

ถ้าต้องการส่งข่าวสาร $(\alpha^{10}, \alpha^2, 0, 0, 0, 0, 0, \alpha^9)$ และต้องการให้รหัสรีดโซโลมอนสามารถแก้ไขสัญลักษณ์ผิดพลาดได้ 3 สัญลักษณ์ สามารถทำได้ดังขั้นตอนต่อไปนี้

ขั้นที่ 1 เขียนข่าวสารในรูปของพหุนาม

$$a(x) = \alpha^{10}x^8 + \alpha^2x^7 + \alpha^9 \quad (2\text{-}11)$$

ขั้นที่ 2 คำนวณ $G(x)$ สำหรับแก้ไขสัญลักษณ์ผิดพลาด 3 สัญลักษณ์ ตามสมการที่ (2-9) ได้

$$G(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)(x-\alpha^5)(x-\alpha^6) \quad (2\text{-}12)$$

ขั้นที่ 3 นำพหุนาม x^{n-k} (ซึ่ง $n-k=2t=6$) คูณกับข่าวสารในสมการที่ (2-11) ได้

$$x^6a(x) = \alpha^{10}x^{14} + \alpha^2x^{13} + \alpha^9x^6 \quad (2\text{-}13)$$

ขั้นที่ 4 หารสมการ (2-13) ด้วย $G(x)$ ได้เศษเหลือ ($b(x)$) ดังนี้

$$b(x) = \alpha^{14}x^5 + \alpha^3x^4 + \alpha^2x^3 + \alpha^7x^2 + \alpha^3x + \alpha^{13} \quad (2\text{-}14)$$

ขั้นที่ 5 หาคำรหัสที่จะส่งได้ ตามสมการที่ (2-10)

$$c(x) = x^6a(x) + b(x) \quad (2\text{-}15)$$

$$c(x) = \alpha^{10}x^{14} + \alpha^2x^{13} + \alpha^9x^6 + \alpha^{14}x^5 + \alpha^3x^4 + \alpha^2x^3 + \alpha^7x^2 + \alpha^3x + \alpha^{13} \quad (2\text{-}16)$$

2.7.2 การถอดรหัสรีดโซโลมอน

ให้คำรหัสที่ได้รับคือ

$$r(x) = r_0 + r_1x + ... + r_{n-1}x^{n-1} \quad (2\text{-}17)$$

และคำรหัสที่ถูกต้องคือ

$$c(x) = c_0 + c_1x + ... + c_{n-1}x^{n-1} \quad (2\text{-}18)$$

จะมีความผิดพลาด

$$e(x) = r(x) - c(x) = e_0 + e_1 x + ... + e_{n-1} x^{n-1} \quad (2\text{-}19)$$

สมมติให้ความผิดพลาดเกิดขึ้นทั้งหมด v ตำแหน่ง ที่ตำแหน่ง $i_1, i_2, ..., i_v$ จะได้

$$e(x) = e_{i_1} x^{i_1} + e_{i_2} x^{i_2} + ... + e_{i_v} x^{i_v} \quad (2\text{-}20)$$

ขั้นตอนแรกในการถอดรหัส จะต้องคำนวณหาซินโดรม (Syndrome) ออกมาจากคำรหัสที่รับได้ $r(x)$ โดยการแทนราก α^i ลงใน $r(x)$ จะได้จำนวนซินโดรมทั้งหมดเท่ากับ $2t$ ดังสมการ (2-21)

$$\begin{aligned} S_0 &= r(\alpha) = e(\alpha) = e_{i_1}\alpha^{i_1} + e_{i_2}\alpha^{i_2} + ... + e_{i_v}\alpha^{i_v} \quad (2\text{-}21) \\ S_1 &= r(\alpha^2) = e(\alpha^2) = e_{i_1}\alpha^{2i_1} + e_{i_2}\alpha^{2i_2} + ... + e_{i_v}\alpha^{2i_v} \\ S_2 &= r(\alpha^3) = e(\alpha^3) = e_{i_1}\alpha^{3i_1} + e_{i_2}\alpha^{3i_2} + ... + e_{i_v}\alpha^{3i_v} \\ &\bullet \\ &\bullet \\ &\bullet \\ S_{2t-1} &= r(\alpha^{2t}) = e(\alpha^{2t}) = e_{i_1}\alpha^{2ti_1} + e_{i_2}\alpha^{2ti_2} + ... + e_{i_v}\alpha^{2ti_v} \end{aligned}$$

ในกรณีคำรหัสที่ได้รับไม่มีความผิดพลาดเลย ค่าซินโดรมที่คำนวณได้จะเป็นศูนย์

สำหรับกรณีทั่วไปจะสามารถเขียนซินโดรมได้ในรูปทั่วไปได้ดังนี้

$$S_m = \sum_{l=1}^{v} e_{i_l} (\alpha^{i_l})^{m+1} = \sum_{u=1}^{t} Y_u V_u^{m+1} \quad (2\text{-}22)$$

โดยที่ m มีค่าได้ตั้งแต่ $0,1,2,3,....,2t-1$

u มีค่าได้ตั้งแต่ $1,2,3,..,t$

l มีค่าได้ตั้งแต่ $1,2,3,..,v$

นิยาม Y_u คือ ค่าผิดพลาดที่ u (Error value)

V_u คือ ตำแหน่งผิดพลาดที่ u (Error locator)

สามารถนิยามพหุนามตำแหน่งผิดพลาด (Error-locator polynomial) ได้ดังนี้

$$\Lambda(x) = (x + V_1)(x + V_2)...(x + V_t) = \prod_{u=1}^{t} (x + V_u)$$

$$\Lambda(x) = x^t + \sigma_1 x^{t-1} + \sigma_2 x^{t-2} + ... + \sigma_{t-1} x + \sigma_t \quad (2\text{-}23)$$

เนื่องจาก V_u คือรากของ $\Lambda(x)$ ดังนั้นจากสมการ (2-23) จะได้

$$V_u{}^t + \sigma_1 V_u{}^{t-1} + \sigma_2 V_u{}^{t-2} + ... + \sigma_{t-1} V_u + \sigma_t = 0 \quad (2\text{-}24)$$

คูณสมการ (2-24) ด้วย $Y_u V_u^{1+i}$

$$Y_u V_u^{t+1+i} + \sigma_1 Y_u V_u^{t+i} + \sigma_2 Y_u V_u^{t+1+i} + .. + \sigma_t Y_u V_u^{1+i} = 0 \quad (2\text{-}25)$$

จากสมการ (2-25) จะได้

$$\sum_{u=1}^{t}(Y_u V_u^{t+1+i} + \sigma_1 Y_u V_u^{t+i} + \sigma_2 Y_u V_u^{t+1+i} + .. + \sigma_t Y_u V_u^{1+i}) = S_{i+t} + \sigma_1 S_{i+(t-1)} + .. + \sigma_t S_i = 0 \quad (2\text{-}26)$$

จากสมการ (2-26) ที่ค่า $i = 0,1,2,...,t-1$ สามารถเขียนสมการในรูปของเมตริกซ์ได้ดังนี้

$$\begin{bmatrix} S_{t-1} & S_{t-2} & \bullet & \bullet & S_0 \\ S_t & S_{t-1} & \bullet & \bullet & S_1 \\ \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet & \bullet \\ S_{2(t-1)} & S_{2t-1} & \bullet & \bullet & S_{t-1} \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \bullet \\ \bullet \\ \sigma_t \end{bmatrix} = \begin{bmatrix} S_t \\ S_{t+1} \\ \bullet \\ \bullet \\ S_{2t-1} \end{bmatrix} \quad (2\text{-}27)$$

จากสมการที่ (2-27) สามารถแก้สมการหา $\sigma_1, \sigma_2, ..., \sigma_t$ ได้ โดยใช้กฎของคราเมอร์ (Cramer's Rule) จากนั้นนำค่า $\sigma_1, \sigma_2, ..., \sigma_t$ ที่ได้ไปหา V_u ต่อ โดยแทนลงในสมการ (2-24) โดยค่าที่สอดคล้องกับสมการก็คือตำแหน่งผิดพลาดที่รหัสรีดโซโลมอนสามารถตรวจพบได้

ขั้นตอนต่อไปก็คือการหาค่าผิดพลาด (Y_u) จากสมการ (2-22) จะได้

$$\begin{bmatrix} V_1 & V_2 & \bullet & \bullet & V_t \\ V_t^2 & V_2^2 & \bullet & \bullet & V_t^2 \\ \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet & \bullet \\ V_1^t & V_2^t & \bullet & \bullet & V_t^t \end{bmatrix} \begin{bmatrix} Y_1 \\ Y_2 \\ \bullet \\ \bullet \\ Y_t \end{bmatrix} = \begin{bmatrix} S_0 \\ S_1 \\ \bullet \\ \bullet \\ S_{t-1} \end{bmatrix} \quad (2\text{-}28)$$

สามารถหาค่า Y_u ได้โดยใช้กฎของคราเมอร์ เช่นเดียวกันกับการแก้สมการหา $\sigma_1, \sigma_2, ..., \sigma_t$

เมื่อทราบตำแหน่งผิดพลาดและค่าผิดพลาดแล้วก็สามารถแก้ไขคำรหัสที่ได้รับให้ถูกต้องได้

บทที่ 3

การออกแบบระบบการจัดพิมพ์บัตรเลือกตั้ง

เนื้อหาในบทนี้จะกล่าวถึง คุณสมบัติของระบบการจัดพิมพ์บัตรเลือกตั้งที่ต้องการ, การเลือกศูนย์กลางการจัดพิมพ์บัตรเลือกตั้ง, สถานที่ที่ใช้ในการดึงคุณลักษณะเฉพาะตัวของกระดาษบัตรเลือกตั้ง, อุปกรณ์ที่ใช้ในการเก็บภาพบัตรเลือกตั้ง, การออกแบบลักษณะของบัตรเลือกตั้ง, กุญแจที่ใช้สำหรับการเข้าและถอดรหัสลับข้อมูลประจำบัตรเลือกตั้ง, การพิมพ์รหัสลับลงบนบัตรเลือกตั้ง, การตรวจสอบบัตรเลือกตั้งทั้งที่หน่วยเลือกตั้ง สถานที่นับคะแนนและที่ว่าการอำเภอ, การหาวิธีการป้องกันการทุจริตเลือกตั้งด้วยวิธีการต่างๆ, การเปรียบเทียบค่าใช้จ่ายในการจัดพิมพ์บัตรเลือกตั้งระหว่างระบบการจัดพิมพ์ที่ได้นำเสนอในงานวิจัยนี้กับระบบการจัดพิมพ์ในปัจจุบัน และผลการออกแบบลักษณะบัตรเลือกตั้ง โดยมีรายละเอียดดังนี้

3.1 นิยามสัญลักษณ์

เนื่องจากระบบการจัดพิมพ์บัตรเลือกตั้งที่จะออกแบบประกอบด้วยข้อมูลต่างๆ อยู่หลายชนิดและข้อมูลบางส่วนมีความสัมพันธ์กันอยู่ ดังนั้นเพื่อความง่ายในการทำให้เห็นความสัมพันธ์ระหว่างข้อมูลเหล่านั้น จึงได้นิยามสัญลักษณ์ต่างๆ ขึ้นเพื่อประกอบคำอธิบาย

กฎเกณฑ์ในการตั้งชื่อสัญลักษณ์ก็คือ ตั้งชื่อสัญลักษณ์แทนข้อมูลต่างๆ ในระบบการเลือกตั้งและแสดงให้เห็นความสัมพันธ์ระหว่างข้อมูลเหล่านั้น โดยนิยามสัญลักษณ์เบื้องต้นดังนี้

K^* แทนกุญแจส่วนตัว

K แทนกุญแจสาธารณะ

$K^*[\cdot]$ แทนการเข้ารหัสข้อมูลที่อยู่ภายในสัญลักษณ์ [ ] ด้วยกุญแจส่วนตัว K^*

$K[\cdot]$ แทนการเข้ารหัสข้อมูลที่อยู่ภายในสัญลักษณ์ [ ] ด้วยกุญแจสาธารณะ K

$K[K^*[\cdot]]$ แทนการใช้กุญแจสาธารณะ K ในการถอดรหัสข้อมูลที่ถูกเข้ารหัสด้วยกุญแจส่วนตัว K^* ได้ข้อมูลที่อยู่ภายในสัญลักษณ์ [ ] ออกมา

$K^*[K[\cdot]]$ แทนการใช้กุญแจส่วนตัว K^* ในการถอดรหัสข้อมูลที่ถูกเข้ารหัสด้วยกุญแจสาธารณะ K ได้ข้อมูลที่อยู่ภายในสัญลักษณ์ [ ] ออกมา

$H[\cdot]$ แทนการนำข้อมูลที่อยู่ภายในสัญลักษณ์ [ ] มาผ่านแฮชฟังก์ชันได้ค่าแฮชออกมา

$H_4[\cdot]$ แทนการนำข้อมูลที่อยู่ภายในสัญลักษณ์ [ ] มาผ่านแฮชฟังก์ชันแล้วจึงลดขนาดค่าแฮชลงเหลือ 4 ไบต์

; แทนการนำข้อมูลมาวางต่อเรียงกัน โดยจะใช้สัญลักษณ์ ; คั่นระหว่างข้อมูล

นอกจากนี้ยังใช้ตัวห้อย (Subscript) กำกับข้อมูลเพื่อแสดงให้ทราบว่าข้อมูลนั้นมาจากไหน โดยตัวห้อยที่ใช้มีดังนี้

C มาจากคำว่า Central เพื่อแสดงให้ทราบว่าเป็นข้อมูลของกรรมการเลือกตั้ง

L มาจากคำว่า Local เพื่อแสดงให้ทราบว่าเป็นข้อมูลของกรรมการเขต

P มาจากคำว่า Program เพื่อแสดงให้ทราบว่าเป็นข้อมูลของโปรแกรม

S มาจากคำว่า Stub เพื่อแสดงให้ทราบว่าเป็นข้อมูลในส่วนของต้นขั้ว

V มาจากคำว่า Voting Part เพื่อแสดงให้ทราบว่าเป็นข้อมูลในส่วนของบัตรลงคะแนน

จากกฎเกณฑ์และนิยามเบื้องต้นสามารถนำไปนิยามสัญลักษณ์ต่างๆ ได้ดังนี้

กุญแจส่วนตัวของกรรมการเลือกตั้ง K_C^*

กุญแจสาธารณะของกรรมการเลือกตั้ง K_C

กุญแจส่วนตัวของกรรมการเขต K_L^*

กุญแจสาธารณะของกรรมการเขต K_L

กุญแจส่วนตัวของโปรแกรม K_P^*

กุญแจสาธารณะของโปรแกรม K_P

เลขประจำบัตร (วันเลือกตั้ง+หมายเลขเขต+หมายเลขเล่ม+เลขที่บัตร) N

เลขประจำต้นขั้ว (วันเลือกตั้ง+หมายเลขเขต+หมายเลขเล่ม+เลขที่ต้นขั้ว) N_S

เลขประจำบัตรลงคะแนน (วันเลือกตั้ง+หมายเลขเขต+หมายเลขเล่ม+เลขที่บัตรลงคะแนน) N_V

รหัสเฉพาะ U

รหัสเฉพาะของต้นขั้ว U_S

รหัสเฉพาะของบัตรลงคะแนน U_V

รหัสเฉพาะ 1 ชั้น (รหัสเฉพาะที่ถูกเข้ารหัสด้วยกุญแจส่วนตัวกรรมการเลือกตั้ง) $U_1 = K_C^*[U]$

รหัสเฉพาะ 1 ชั้น ของต้นขั้ว $U_{1S} = K_C^*[U_S]$

รหัสเฉพาะ 1 ชั้น ของบัตรลงคะแนน $U_{1V} = K_C^*[U_V]$

รหัสเฉพาะ 2 ชั้น (รหัสเฉพาะ 1 ชั้นที่ถูกเข้ารหัสด้วยกุญแจส่วนตัวโปรแกรม) $U_2 = K_P^*[K_C^*[U]]$

รหัสเฉพาะ 2 ชั้น ของต้นขั้ว $U_{2S} = K_P^*[K_C^*[U_S]]$

รหัสเฉพาะ 2 ชั้น ของบัตรลงคะแนน $U_{2V} = K_P^*[K_C^*[U_V]]$

คุณลักษณะเฉพาะตัวของกระดาษบัตรเลือกตั้ง F

คุณลักษณะเฉพาะตัวของกระดาษต้นขั้ว F_S

คุณลักษณะเฉพาะตัวของกระดาษบัตรลงคะแนน F_V

ค่าแฮช $H = H[N; U_1; F]$

ค่าแฮชของต้นขั้ว $H_S = H[N_S;U_{1S};F_S]$

ค่าแฮชของบัตรลงคะแนน $H_V = H[N_V;U_{1V};F_V]$

ค่าแฮช 4 ไบต์ (ค่าแฮชที่ถูกลดขนาดลงเหลือ 4 ไบต์) $H_4 = H_4[N;U_1;F]$

ค่าแฮชของต้นขั้ว 4 ไบต์ $H_{4S} = H_4[N_S;U_{1S};F_S]$

ค่าแฮชของบัตรลงคะแนน 4 ไบต์ $H_{4V} = H_4[N_V;U_{1V};F_V]$

ข้อมูลประจำบัตร $D = N;U_1;F;H_4$

ข้อมูลประจำต้นขั้ว $D_S = N;U_{1S};F_S;H_{4S}$

ข้อมูลประจำบัตรลงคะแนน $D_V = N;U_{1V};F_V;H_{4V}$

ข้อมูลรหัสลับของบัตร $K_L^*[D]$

ข้อมูลรหัสลับของต้นขั้ว $K_L^*[D_S]$

ข้อมูลรหัสลับของบัตรลงคะแนน $K_L^*[D_V]$

3.2 **คุณสมบัติที่ต้องการของระบบการจัดพิมพ์บัตรเลือกตั้ง**

ระบบการจัดพิมพ์บัตรเลือกตั้ง มีคุณสมบัติที่ต้องการดังนี้

- *จัดพิมพ์บัตรเลือกตั้งจำนวนมากเสร็จภายในระยะเวลาที่จำกัด* การเลือกตั้งที่นำวิธีการเข้ารหัสลับมาใช้ จะมีปัญหาในเรื่องเวลาที่ใช้ในการจัดพิมพ์ เนื่องจากบัตรเลือกตั้งแต่ละใบจะต้องเสียเวลาในขั้นตอนการสแกนบัตรเลือกตั้ง การเข้ารหัสข้อมูลประจำบัตรเลือกตั้งและการพิมพ์รหัสแท่งลงบนบัตรเลือกตั้ง รวมทั้งจำนวนบัตรเลือกตั้งที่ต้องจัดพิมพ์มีจำนวนมากถึง 160 ล้านใบ และต้องจัดพิมพ์ให้เสร็จภายในระยะเวลาที่จำกัด จึงต้องออกแบบระบบการจัดพิมพ์บัตรเลือกตั้งให้สามารถจัดพิมพ์บัตรเลือกตั้งจำนวนมากเสร็จภายในระยะเวลาที่จำกัด
- *ใช้ต้นทุนในการจัดพิมพ์ต่ำ* เนื่องจากบัตรเลือกตั้งที่ต้องการจัดพิมพ์มีปริมาณมาก ถ้าต้นทุนการพิมพ์บัตรเลือกตั้งต่อใบมีราคาสูงก็จะทำให้เสียค่าใช้จ่ายในการจัดพิมพ์สูงตามไปด้วย ดังนั้นจึงต้องออกแบบระบบการจัดพิมพ์บัตรเลือกตั้งที่ใช้ต้นทุนในการจัดพิมพ์ไม่สูงมากนัก
- *ป้องกันการทุจริตจากบุคคลที่เกี่ยวข้องกับบัตรเลือกตั้ง* นอกจากจะต้องจัดพิมพ์บัตรเลือกตั้งได้อย่างรวดเร็วแล้วยังต้องคำนึงถึงความปลอดภัยของระบบการเลือกตั้ง โดยออกแบบขั้นตอนต่างๆ ให้รัดกุม และป้องกันไม่ให้ผู้ที่มีส่วนเกี่ยวข้องกับบัตรเลือกตั้งทุจริตได้

3.3 การเลือกศูนย์กลางการจัดพิมพ์บัตรเลือกตั้ง

ขั้นตอนแรกในการออกแบบระบบการพิมพ์บัตรเลือกตั้งก็คือ การเลือกศูนย์กลางการจัดพิมพ์บัตรเลือกตั้ง ว่าจะจัดพิมพ์ที่ใดจึงจะสะดวกและรวดเร็ว ในงานวิจัยนี้ได้กำหนดให้ระยะเวลาที่ใช้ในการจัดพิมพ์อย่างมากคือ 1 เดือน เนื่องจากต้องเผื่อเวลาไว้ใช้ในการขนส่งบัตรเลือกตั้ง ซึ่งศูนย์กลางการจัดพิมพ์บัตรเลือกตั้งแบ่งได้ดังนี้

- *รวมศูนย์การจัดพิมพ์บัตรเลือกตั้งไว้ที่ส่วนกลาง*

ให้ส่วนกลางรับผิดชอบในการจัดพิมพ์แล้วจึงค่อยกระจายบัตรเลือกตั้งไปยังเขตเลือกตั้ง กรณีนี้จะมีความปลอดภัยต่อการทุจริตสูง เนื่องจากผู้ที่ถือกุญแจที่ใช้ในการจัดพิมพ์ก็คือกรรมการเลือกตั้ง บุคคลอื่นที่ไม่รู้กุญแจของกรรมการเลือกตั้งจะไม่สามารถจัดพิมพ์เองได้ แต่มีข้อเสียตรงที่ส่วนกลางจะรับภาระหนักในการจัดพิมพ์ ซึ่งมีตัวอย่างการคำนวณดังนี้

ใช้เครื่องพิมพ์รุ่น Infoprint 70 [15] ของ IBM ซึ่งสามารถพิมพ์ได้ความเร็วสูงสุด 70 แผ่นต่อนาที แต่สามารถพิมพ์ได้สูงสุด 400,000 ใบต่อเดือน บัตรเลือกตั้งที่ต้องพิมพ์ทั้งหมดมีจำนวน 160 ล้านใบ ถ้าใช้เครื่องพิมพ์รุ่นนี้จะต้องใช้ถึง 400 เครื่อง จึงจะสามารถจัดพิมพ์เสร็จภายใน 1 เดือน ซึ่งราคาแต่ละเครื่องในปัจจุบันประมาณ 1,500,000 บาท ต้องใช้จำนวนเงินถึง 600 ล้านบาทในการจัดหาเครื่องพิมพ์และยังต้องจัดหาคนมาช่วยในการจัดพิมพ์จำนวนมาก จึงเป็นภาระหนักของส่วนกลาง

- *กระจายศูนย์การจัดพิมพ์บัตรเลือกตั้งไปยังเขตเลือกตั้ง*

ให้แต่ละเขตจัดพิมพ์บัตรเลือกตั้ง ซึ่งมีข้อดีตรงที่ช่วยส่วนกลางในการแบ่งเบาภาระการจัดพิมพ์ได้ ซึ่งมีตัวอย่างการคำนวณดังนี้

ใช้เครื่องพิมพ์รุ่น LaserJet 2200DN [16] ของ Hewlett Packard ซึ่งสามารถพิมพ์ได้ 19 แผ่นต่อนาที แต่สามารถพิมพ์ได้สูงสุด 40,000 แผ่นต่อเดือน บัตรเลือกตั้งที่ต้องพิมพ์ทั้งหมดมีจำนวน 160 ล้านใบ เขตเลือกตั้งทั่วประเทศมีอยู่ 400 เขต หนึ่งเขตจะต้องพิมพ์บัตรเลือกตั้ง 400,000 ใบ ถ้าใช้เครื่องพิมพ์รุ่นนี้ 10 เครื่อง จะสามารถจัดพิมพ์เสร็จภายใน 1 เดือน ซึ่งราคาแต่ละเครื่องในปัจจุบันประมาณ 40,000 บาท เขตหนึ่งเขตต้องใช้เงินจำนวน 400,000 บาท ในการจัดหาเครื่องพิมพ์ รวมทั้งหมดทุกเขตทั่วประเทศจะต้องใช้เงิน 160 ล้านบาท ในการจัดซื้อเครื่องพิมพ์ แต่การกระจายศูนย์การจัดพิมพ์มีข้อดีตรงที่สามารถนำเครื่องพิมพ์และไมโครคอมพิวเตอร์มาใช้งานได้ ในช่วงเวลาที่ไม่มีการเลือกตั้งและการกระจายบัตรเลือกตั้งไปยังหน่วยเลือกตั้งจะทำได้สะดวก

วิธีการกระจายศูนย์การจัดพิมพ์ มีปัญหาเรื่องการควบคุมไม่ให้กรรมการเขตทุจริต เนื่องจากกรรมการเขตถือกุญแจในการจัดพิมพ์และอุปกรณ์ที่ใช้ในการจัดพิมพ์อยู่ที่กรรมการเขตเอง การป้องกันการทุจริตโดยบังคับให้กรรมการเขตพิมพ์บัตรเลือกตั้งชุดเดียวย่อมเป็นไปไม่ได้ ดัง

นั้นการป้องกันการทุจริตก็คือหาวิธีที่ทำให้กรรมการเขตไม่สามารถนำบัตรเลือกตั้งที่พิมพ์ซ้ำกันหลายๆ ชุดนั้นมาทุจริตด้วยวิธีการสับเปลี่ยนบัตรเลือกตั้งในภายหลังได้

ในงานวิจัยนี้ได้เลือกใช้วิธีกระจายการพิมพ์บัตรเลือกตั้ง โดยให้เขตเลือกตั้งแต่ละเขตดูแลระบบการจัดพิมพ์ในเขตของตน เนื่องจากต้องการแบ่งเบาภาระการจัดพิมพ์ที่ส่วนกลางทั้งเรื่องการจัดหาเครื่องพิมพ์และการจัดหาคนมาช่วยในการพิมพ์บัตรเลือกตั้ง นอกจากนี้ยังสามารถนำอุปกรณ์ที่ใช้ในงานจัดพิมพ์ อย่างเช่น เครื่องพิมพ์และไมโครคอมพิวเตอร์มาใช้งานได้ในช่วงเวลาที่ไม่มีการเลือกตั้ง

3.4 สถานที่ที่ใช้ในการดึงคุณลักษณะเฉพาะตัวของกระดาษบัตรเลือกตั้ง

ขั้นตอนที่ต้องเสียเวลาอย่างมากในการจัดพิมพ์บัตรเลือกตั้งก็คือ ขั้นตอนการดึงคุณลักษณะเฉพาะตัวของกระดาษบัตรเลือกตั้งแต่ละใบ ซึ่งขั้นตอนนี้สามารถกระทำได้ที่ส่วนกลางหรือเขตเลือกตั้งก็ได้ โดยมีรายละเอียดดังนี้

- *การดึงคุณลักษณะเฉพาะตัวของกระดาษบัตรเลือกตั้งที่ส่วนกลาง* กรณีนี้จะดึงคุณลักษณะเฉพาะตัวของกระดาษบัตรเลือกตั้งที่ส่วนกลาง แล้วจึงนำข้อมูลคุณลักษณะเฉพาะตัวของกระดาษบัตรเลือกตั้ง (F) ไปพิมพ์ลงบนบัตรเลือกตั้งในรูปแบบรหัสแท่ง 1 มิติ เมื่อใกล้กำหนดวันเลือกตั้ง ทางเขตเลือกตั้งจะนำบัตรเลือกตั้งไปพิมพ์โดยใช้เครื่องอ่านรหัสแท่งอ่านรหัสแท่ง 1 มิติ ได้ข้อมูลคุณลักษณะเฉพาะตัวของกระดาษ (F) ซึ่งจะนำไปใช้เป็นข้อมูลส่วนหนึ่งของบัตรเลือกตั้งได้ทันที ทำให้ทางเขตเลือกตั้งลดเวลาที่ใช้ในขั้นตอนการสแกนบัตรเลือกตั้ง แต่วิธีการนี้จะใช้ได้ก็ต่อเมื่อมีเวลาก่อนการเลือกตั้งนานเพียงพอเพราะต้องใช้เวลาในการดึงคุณลักษณะเฉพาะตัวของบัตรเลือกตั้งของบัตรเลือกตั้งทุกใบและส่วนกลางจะต้องมีระบบการดูแลและจัดเก็บบัตรเลือกตั้งที่ดี
- *การดึงคุณลักษณะเฉพาะตัวของกระดาษบัตรเลือกตั้งที่เขตเลือกตั้ง* กรณีนี้ทางเขตเลือกตั้งจะต้องมีอุปกรณ์เก็บภาพต่อกับไมโครคอมพิวเตอร์และเครื่องพิมพ์ เมื่อนำกระดาษบัตรเลือกตั้งไปวางอุปกรณ์เก็บภาพจะเก็บภาพบัตรเลือกตั้งและจะดึงข้อมูลคุณลักษณะเฉพาะตัวจากกระดาษแล้วนำข้อมูลคุณลักษณะเฉพาะตัวของกระดาษ (F) ไปรวมกับข้อมูลอื่นของบัตรเลือกตั้ง ($N;U_1;H_4$) ได้ข้อมูลประจำบัตรเลือกตั้ง ($D = N;U_1;F;H_4$) หลังจากนั้นจะเข้ารหัสลับข้อมูลประจำบัตรเลือกตั้ง ($K_L^*[D]$) และพิมพ์รหัสลับลงบนบัตรเลือกตั้งในรูปแบบรหัสแท่ง 2 มิติ ทันที

ในงานวิจัยนี้ได้ออกแบบระบบการจัดพิมพ์บัตรเลือกตั้ง โดยจะดึงคุณลักษณะเฉพาะตัวของบัตรเลือกตั้งที่เขตเลือกตั้ง เนื่องจากการดึงคุณลักษณะเฉพาะตัวของบัตรเลือกตั้งที่ส่วนกลางจะทำได้ยากในกรณีที่มีการเลือกตั้งบ่อยๆ

3.5 อุปกรณ์ที่ใช้ในการเก็บภาพบัตรเลือกตั้ง

บัตรเลือกตั้งทุกใบจะต้องถูกถ่ายภาพเพื่อนำภาพกระดาษบัตรเลือกตั้งไปดึงคุณลักษณะเฉพาะตัวของกระดาษ ซึ่งอุปกรณ์ที่ใช้ในการเก็บภาพก็มีอยู่หลายชนิด ดังนี้

- สแกนเนอร์ระดับเทา (Gray Scale Scanner) ตัวอย่างของสแกนเนอร์ระดับเทาที่ใช้ได้ ได้แก่ สแกนเนอร์ รุ่น DR-2080C [17] ของ Canon สามารถสแกนภาพระดับเทาได้ด้วยอัตราความเร็ว 20 แผ่นต่อนาที มีราคาประมาณ 20,400 บาท
- กล้องดิจิตอล (Digital Camera) ตัวอย่างของกล้องดิจิตอลที่ใช้ได้ ได้แก่ กล้องดิจิตอล รุ่น PowerShot A200 [18] ของ Canon สามารถเก็บภาพได้ละเอียดสูงสุด 1600x1200 พิกเซล มีราคาประมาณ 8,000 บาท
- กล้องประจำเครื่องคอมพิวเตอร์ส่วนบุคคล (PC Camera) ตัวอย่างของกล้องประจำเครื่องคอมพิวเตอร์ส่วนบุคคลที่ใช้ได้ ได้แก่ กล้องประจำเครื่องคอมพิวเตอร์ส่วนบุคคล รุ่น Intel® Pocket Digital PC Camera [19] ของ Intel มีราคาประมาณ 6,000 บาท
- เซนเซอร์สัมผัสภาพ (Contact Image Sensor) ตัวอย่างของเซนเซอร์สัมผัสภาพที่ใช้ได้ ได้แก่ เซนเซอร์สัมผัสภาพรุ่น PI250MC-A6 [20] ของ P-Imaging มีระยะสแกนภาพ 10.4 เซนติเมตร มีราคาประมาณ 800 บาท

งานวิจัยนี้ได้เลือกใช้ กล้องประจำเครื่องคอมพิวเตอร์ส่วนบุคคล ในการเก็บภาพกระดาษบัตรเลือกตั้งที่เขตเลือกตั้งและที่ว่าการอำเภอ เนื่องจากมีราคาถูกกว่าสแกนเนอร์กับกล้องดิจิตอล มีความไวในการเก็บภาพและมีความละเอียดเพียงพอที่จะนำไปใช้งานได้ สำหรับที่หน่วยเลือกตั้งจะใช้อุปกรณ์เก็บภาพกระดาษบัตรเลือกตั้งเพื่อนำไปสุ่มตรวจบัตรเลือกตั้ง ซึ่งการสุ่มตรวจบัตรเลือกตั้งไม่จำเป็นต้องใช้อุปกรณ์ที่มีความเร็วสูงในการเก็บภาพจึงเลือกใช้ เซนเซอร์สัมผัสภาพ เนื่องจากมีความละเอียดเพียงพอและมีราคาถูกกว่าสแกนเนอร์ระดับเทา กล้องดิจิตอลและกล้องประจำเครื่องคอมพิวเตอร์ส่วนบุคคล

3.6 ลักษณะของบัตรเลือกตั้งที่ใช้ในการเลือกตั้ง

การกระจายศูนย์การจัดพิมพ์บัตรเลือกตั้งไปยังเขตเลือกตั้งจะมีปัญหาในเรื่องกรรมการเขตอาจจะทุจริตได้โดยพิมพ์บัตรเลือกตั้งหลายๆ ชุดและนำบัตรเลือกตั้งไปสับเปลี่ยนในภายหลัง

จึงต้องออกแบบลักษณะของบัตรเลือกตั้งให้สามารถตรวจสอบการทุจริตจากกรรมการเขตและบุคคลอื่นๆ ที่เกี่ยวข้องกับบัตรเลือกตั้งได้ ซึ่งมีรายละเอียดดังนี้

3.6.1 กระดาษที่ใช้พิมพ์บัตรเลือกตั้ง

ระหว่างขั้นตอนการผลิตกระดาษบัตรเลือกตั้ง จะแทรกวัตถุชิ้นเล็ก ๆ เช่น เม็ดทราย หรือเส้นใยสีลงไปในเนื้อกระดาษด้วย ซึ่งบัตรเลือกตั้งแต่ละใบจะมีลักษณะการวางตัวของวัตถุชิ้นเล็กๆ แตกต่างกันทำให้เกิดความแตกต่างระหว่างบัตรใบหนึ่งกับอีกใบหนึ่ง ซึ่งจะใช้ลักษณะที่แตกต่างกันนี้แยกแยะว่าบัตรใบหนึ่งต่างจากบัตรใบหนึ่งอย่างไรซึ่งเป็นคุณสมบัติอย่างหนึ่งที่ทำให้การปลอมแปลงทำได้ยาก

3.6.2 ต้นขั้ว

การที่มีต้นขั้วบนบัตรเลือกตั้งก็เพื่อใช้ในการตรวจสอบจำนวนบัตรลงคะแนนที่ถูกฉีกออกไป โดยจำนวนบัตรลงคะแนนที่อยู่ในหีบเลือกตั้งจะต้องตรงกับจำนวนต้นขั้วของบัตรเลือกตั้งที่ถูกฉีกบัตรลงคะแนนออกไปแล้วและผู้มาใช้สิทธิ์เลือกตั้งจะต้องพิมพ์ลายนิ้วมือลงบนต้นขั้วบัตรเลือกตั้ง โดยจะมีช่องสำหรับให้ผู้มาใช้สิทธิ์เลือกตั้งพิมพ์ลายนิ้วมือของตน ซึ่งลายนิ้วมือเป็นข้อมูลเฉพาะตัวสำหรับแต่ละคน สามารถปลอมให้มีจำนวนมากโดยไม่ซ้ำกันได้ยาก ตำแหน่งสำหรับพิมพ์ลายนิ้วมือต้องอยู่บนต้นขั้วบัตรเลือกตั้งเท่านั้น เนื่องจากผลการลงคะแนนของผู้มาใช้สิทธิ์เลือกตั้งแต่ละคนจะต้องเป็นความลับ

3.6.3 ส่วนประกอบของบัตรเลือกตั้ง

บัตรเลือกตั้งที่ออกแบบจะส่วนประกอบ 2 ส่วนใหญ่ๆ ดังนี้

- *ต้นขั้ว* ประกอบด้วยส่วนสำคัญ ๆ ดังนี้
  - พื้นที่สำหรับดึงข้อมูลคุณลักษณะเฉพาะตัวของกระดาษ (F_S)
  - รหัสแท่ง 2 มิติ ของข้อมูลประจำต้นขั้วที่ผ่านการเข้ารหัสลับแล้ว ($K_L^*[D_S]$) เพื่อให้เจ้าหน้าที่ประจำหน่วยเลือกตั้ง, เจ้าหน้าที่ประจำที่ว่าการอำเภอและกรรมการเลือกตั้งสามารถตรวจสอบได้
  - ช่องสำหรับพิมพ์ลายนิ้วมือของผู้มาใช้สิทธิ์เลือกตั้ง
- *บัตรลงคะแนน* ประกอบด้วยส่วนสำคัญ ๆ ดังนี้
  - พื้นที่สำหรับดึงข้อมูลคุณลักษณะเฉพาะตัวของกระดาษ (F_V)
  - รหัสแท่ง 2 มิติ ของข้อมูลประจำบัตรลงคะแนนที่ผ่านการเข้ารหัสลับแล้ว ($K_L^*[D_V]$) เพื่อให้เจ้าหน้าที่ประจำหน่วยเลือกตั้ง, เจ้าหน้าที่ประจำสถานที่

นับคะแนน, เจ้าหน้าที่ประจำที่ว่าการอำเภอและกรรมการเลือกตั้งสามารถตรวจสอบได้

- ช่องสำหรับลงคะแนน

3.6.4 **ข้อมูลประจำบัตรเลือกตั้ง**

ต้นขั้วและบัตรลงคะแนนของบัตรเลือกตั้งแต่ละใบจะมีข้อมูลประจำบัตรที่ไม่ซ้ำกันประกอบด้วย

- *เลขประจำบัตร* (N) เป็นข้อมูลที่ประกอบด้วย วันเลือกตั้ง หมายเลขเขต หมายเลขเล่มและเลขที่บัตร เพื่อให้สามารถระบุได้ว่าบัตรใบนั้นมาจากที่ใด และเป็นการป้องกันการใช้บัตรข้ามพื้นที่ด้วย
- *รหัสเฉพาะ (Unique Code)* เป็นข้อมูลที่กรรมการเลือกตั้งสร้างขึ้นมา เพื่อป้องกันกรรมการเขตทุจริต โดยกรรมเลือกตั้งจะสร้างรหัสเฉพาะและส่งแฟ้ม ข้อมูลที่มีรหัสเฉพาะ 2 ชั้น ($U_2 = K_P^*[K_C^*[U]]$) อยู่ภายในไปให้กรรมการเขตเพื่อนำไปใช้เป็นส่วนหนึ่งของข้อมูลประจำบัตรเลือกตั้ง ซึ่งรหัสเฉพาะ (U) จะมีอยู่จำนวนจำกัด จึงทำให้กรรมการเขตไม่สามารถพิมพ์บัตรเลือกตั้งเกินจำนวนรหัสเฉพาะได้
- *คุณลักษณะเฉพาะตัวของกระดาษแผ่นที่ใช้พิมพ์บัตรเลือกตั้งใบนั้น ๆ* (F)เนื่องจากคุณลักษณะเฉพาะตัวของกระดาษแต่ละใบ (F) จะแตกต่างกัน จึงนำข้อมูลคุณลักษณะเฉพาะตัวของกระดาษนำมาใช้เพื่อป้องกันการคัดลอกชุดข้อมูลที่ผ่านการเข้ารหัสลับ ($K_L^*[D]$) จากบัตรเลือกตั้งจริงไปยังบัตรเลือกตั้งปลอมได้
- *ค่าแฮช* (H) ได้จากการนำข้อมูลทั้งสามส่วนข้างต้นไปผ่านแฮชฟังก์ชันได้ค่าแฮชออกมา ($H[N;U;F]$) จากนั้นจึงลดขนาดให้เหลือเพียง 4 ไบต์ ($H_4 = H_4[N;U;F]$) แล้วจึงนำค่าแฮชที่ได้ไปใช้เป็นข้อมูลส่วนหนึ่งของบัตรเลือกตั้ง ($D = N;U_1;F;H_4$) ค่าแฮชถูกนำมาใช้เพื่ออ้างอิงถึงบัตรเลือกตั้งแต่ละใบแบบย่อและป้องกันการทุจริตจากกรรมการเขตอีกทีหนึ่ง นอกเหนือจากรหัสเฉพาะ (U)

3.7 **หลักการทำงาน (ตรวจสอบ) ของข้อมูลต่าง ๆ บนบัตร**

หน้าที่ของข้อมูลที่ถูกใช้ในการตรวจสอบบัตรเลือกตั้งมีดังนี้

- *รหัสเฉพาะ* (U) ทั้งต้นขั้วและบัตรลงคะแนนจะมีรหัสเฉพาะอยู่ ซึ่งรหัสเฉพาะของต้นขั้วและบัตรลงคะแนน (U_S ,U_V) จะแตกต่างกันไปเพื่อป้องกันการโยงหากันของ

ต้นขั้วและบัตรลงคะแนน รหัสเฉพาะมีไว้เพื่อป้องกันกรรมการเขตทุจริต ด้วยการพิมพ์บัตรเลือกตั้งหลายชุดแล้วสับเปลี่ยนบัตรเลือกตั้งในภายหลัง โดยรหัสเฉพาะ (U) ที่กรรมการเลือกตั้งส่งไปให้กรรมการเขตจะมีจำนวนจำกัดและถูกเข้ารหัสด้วยกุญแจส่วนตัวของกรรมการเลือกตั้งและกุญแจส่วนตัวของโปรแกรม ($K_P^*[K_C^*[U]]$) สำหรับสาเหตุที่ต้องเข้ารหัสด้วยกุญแจส่วนตัวของกรรมการเลือกตั้ง ($K_C^*[U]$) ก็เพื่อป้องกันไม่ให้ผู้อื่นที่ไม่รู้กุญแจส่วนตัวของกรรมการเลือกตั้งสามารถปลอมแปลงได้และรหัสเฉพาะจะถูกเข้ารหัสอีกครั้งด้วยกุญแจส่วนตัวของโปรแกรมในแต่ละเขต ($K_P^*[K_C^*[U]]$) เพื่อควบคุมให้บัตรเลือกตั้งต้องผ่านการพิมพ์จากโปรแกรมพิมพ์บัตรเลือกตั้งที่กรรมการเลือกตั้งส่งไปเท่านั้น เนื่องจากโปรแกรมพิมพ์บัตรเลือกตั้งถูกฝังกุญแจสาธารณะของโปรแกรมไว้จึงสามารถถอดรหัสจากกรหัสเฉพาะ 2 ชั้นไปเป็นรหัสเฉพาะ 1 ชั้นได้ ($K_P[K_P^*[K_C^*[U]]] = K_C^*[U] = U_1$) นอกจากนี้ยังเป็นการป้องกันการนำรหัสเฉพาะไปใช้ข้ามเขต โดยโปรแกรมพิมพ์บัตรเลือกตั้งของแต่ละเขตจะถูกฝังกุญแจสาธารณะของโปรแกรมแตกต่างกัน ดังนั้นโปรแกรมพิมพ์บัตรเลือกตั้งในแต่ละเขตจะสามารถนำรหัสเฉพาะของเขตตนเองไปใช้ได้เท่านั้นไม่สามารถนำรหัสเฉพาะของเขตอื่นไปไปใช้ได้

เนื่องจากรหัสเฉพาะที่จะกล่าวถึงต่อไปนี้ มีทั้งรหัสเฉพาะที่ไม่ได้ถูกเข้ารหัสเลย (U) รหัสเฉพาะที่ถูกเข้ารหัส 1 ชั้น (U_1) และรหัสเฉพาะที่ถูกเข้ารหัส 2 ชั้น (U_2) ดังนั้นเพื่อความสะดวกในการเรียกชื่อรหัสเฉพาะ ในงานวิจัยนี้จะขอเรียกรหัสเฉพาะที่ไม่ได้ถูกเข้ารหัส (U) ว่ารหัสเฉพาะและเรียกรหัสเฉพาะที่ถูกเข้ารหัสด้วยกุญแจส่วนตัวของกรรมการเลือกตั้งเพียงอย่างเดียวว่า รหัสเฉพาะ 1 ชั้น ($U_1 = K_C^*[U]$) และเรียกรหัสเฉพาะที่ถูกเข้ารหัสด้วยกุญแจส่วนตัวของกรรมการเลือกตั้งและกุญแจส่วนตัวของโปรแกรมว่ารหัสเฉพาะ 2 ชั้น ($U_2 = K_P^*[U_1] = K_P^*[K_C^*[U]]$) กรรมการเลือกตั้งจะส่งรหัสเฉพาะ 2 ชั้น ($U_2 = K_P^*[K_C^*[U]]$) ของบัตรเลือกตั้งทุกใบไปให้กรรมการเขตในรูปแบบแฟ้มข้อมูล เมื่อกรรมการเขตรับแฟ้มข้อมูลรหัสเฉพาะมาแล้วก็จะนำรหัสเฉพาะ 2 ชั้น ($U_2 = K_P^*[K_C^*[U]]$) ไปป้อนเข้าโปรแกรมพิมพ์บัตรเลือกตั้ง เพื่อให้โปรแกรมพิมพ์บัตรเลือกตั้งถอดรหัสได้รหัสเฉพาะ 1 ชั้น ($K_P[K_P^*[K_C^*[U]] = K_C^*[U] = U_1$) ก่อนแล้วจึงนำไปใช้เป็นข้อมูลส่วนหนึ่งของบัตรแต่ละใบ การนำรหัสเฉพาะมาใช้ก็เพื่อป้องกันกรรมการเขตทุจริต เนื่องจากกรรมการเขตสามารถพิมพ์บัตรเลือกตั้งได้หลายชุดแต่สามารถนำรหัสเฉพาะไปใช้ได้เพียงครั้งเดียว ถ้าตรวจสอบบัตรเลือกตั้งแล้วพบรหัสเฉพาะซ้ำกันแสดงว่ามีการทุจริตโดยกรรมการเขตพิมพ์บัตรเลือกตั้งหลายชุด

- *ค่าแฮช* (H) ใช้สำหรับอ้างอิงถึงบัตรเลือกตั้งแต่ละใบอย่างย่อ ซึ่งภายหลังการตรวจสอบบัตรเลือกตั้งแต่ละใบ เจ้าหน้าที่ตรวจสอบจะต้องบันทึกค่าแฮชของบัตรเลือกตั้งใบนั้นและเซ็นชื่อกำกับไว้ นอกจากนี้ยังใช้ค่าแฮชสำหรับป้องกันกรรมการเขตทุจริตอีกชั้นหนึ่ง นอกเหนือจากรหัสเฉพาะ เนื่องจากถ้าใช้วิธีการตรวจสอบรหัสเฉพาะ (U) เพียงอย่างเดียวว่าใช้รหัสเฉพาะซ้ำหรือไม่ ทำให้กรรมการเขตอาจจะทุจริตได้โดยหาวิธีที่ทำให้การตรวจสอบบัตรเลือกตั้งไม่พบการใช้รหัสเฉพาะซ้ำ อย่างเช่นพิมพ์บัตรเลือกตั้งที่ใช้รหัสเฉพาะเดียวกัน 2 ชุด ชุดแรกนำไปให้ผู้มาใช้สิทธิ์ลงคะแนนและขณะที่กำลังขนย้ายหีบบัตรก็นำบัตรเลือกตั้งที่ใช้รหัสเฉพาะเดียวกันชุดที่ 2 มาเปลี่ยนทั้งหีบ ทำให้ตรวจแล้วไม่พบการใช้รหัสเฉพาะซ้ำจึงต้องมีการป้องกันการทุจริตโดยวิธีอื่นอีกที ด้วยการนำค่าแฮชมาใช้ (H) โดยขณะพิมพ์บัตรเลือกตั้ง โปรแกรมพิมพ์บัตรเลือกตั้งจะสร้างแฟ้มข้อมูลที่มีค่าแฮชและรหัสเฉพาะซึ่งถูกเข้ารหัสด้วยกุญแจสาธารณะของโปรแกรมอยู่ภายใน ($K_P[H_{4S};U_{1S}], K_P[H_{4V};U_{1V}]$) สำหรับสาเหตุที่เข้ารหัสลับค่าแฮชและรหัสเฉพาะด้วยกุญแจสาธารณะของโปรแกรม (K_P) ก็เพื่อไม่ให้กรรมการเขตหรือบุคคลอื่นๆ สามารถเปลี่ยนแปลงหรือแก้ไขข้อมูลค่าแฮชและรหัสเฉพาะได้ ซึ่งค่าแฮชและรหัสเฉพาะที่ถูกเข้ารหัส ($K_P[H_{4S};U_{1S}], K_P[H_{4V};U_{1V}]$) จะถูกบันทึกลงแฟ้มข้อมูล โดยเรียงจากน้อยไปหามากเพื่อป้องกันการจับคู่ค่าแฮชและรหัสเฉพาะของต้นขั้วและบัตรลงคะแนน ซึ่งถ้าสามารถจับคู่ต้นขั้วและบัตรลงคะแนนได้ก็จะทำให้การลงคะแนนไม่เป็นความลับ หลังจากนั้นกรรมการเขตจะต้องส่งแฟ้มข้อมูลไปให้กรรมการเลือกตั้งเพื่อรายงานให้กรรมการเลือกตั้งทราบว่าได้พิมพ์บัตรเลือกตั้งที่มีค่าแฮชและรหัสเฉพาะของต้นขั้วและบัตรลงคะแนนอย่างที่ส่งไปในแฟ้มข้อมูล ในที่นี้ขอเรียกแฟ้มข้อมูลที่กรรมการเขตส่งไปยังกรรมการเลือกตั้งว่าแฟ้มข้อมูลรายงานการจัดพิมพ์และเมื่อกรรมการเลือกตั้งได้รับแฟ้มข้อมูลรายงานการจัดพิมพ์ที่กรรมการเขตส่งมาก็จะรวบรวมและบันทึกค่าแฮชที่ถูกเข้ารหัสด้วยกุญแจสาธารณะของโปรแกรม ($K_P[H_{4S}], K_P[H_{4V}]$) ลงแฟ้มข้อมูลตรวจสอบค่าแฮช หลังจากนั้นจะส่งแฟ้มข้อมูลกลับไปยังเขตเลือกตั้งเพื่อใช้เป็นฐานข้อมูลในการตรวจสอบค่าแฮชของบัตรเลือกตั้ง โดยค่าแฮชจะถูกใช้ในการตรวจสอบว่ากรรมการเขตทุจริตหรือไม่ เนื่องจากบัตรเลือกตั้งที่กรรมการเขตจะนำไปใช้ได้ก็คือบัตรเลือกตั้งที่กรรมการเขตส่งค่าแฮชกลับไปให้กรรมการเลือกตั้งเท่านั้น ถ้าตรวจสอบค่าแฮชของบัตรเลือกตั้งแล้วไม่พบค่าแฮชในฐานข้อมูลแสดงว่ากรรมการเขตทุจริตโดยพิมพ์บัตรเลือกตั้งหลายชุด และนำบัตรเลือกตั้งที่ไม่ได้ส่งรายงานค่าแฮชไปใช้

- *ต้นขั้ว* ทั้งต้นขั้วและบัตรลงคะแนนจะมีรหัสลับของข้อมูลประจำบัตรพิมพ์ไว้ ($K_L^*[D_S]$, $K_L^*[D_V]$) และเพื่อรับประกันว่าการลงคะแนนเลือกตั้งเป็นความลับจริง รหัสลับบนต้นขั้วจะต้องไม่มีข้อมูลที่สามารถโยงจับคู่กันได้ระหว่างบัตรลงคะแนนกับต้นขั้ว สาเหตุที่ต้นขั้วต้องมีการพิมพ์ข้อมูลคุณลักษณะเฉพาะตัวของกระดาษที่ได้เข้ารหัสลับไว้ด้วย ก็เพื่อป้องกันการทำต้นขั้วปลอม เนื่องจากว่า หากต้นขั้วสามารถปลอมได้ คือไม่มีข้อมูลคุณลักษณะเฉพาะตัวของกระดาษ (F) เมื่อเจ้าหน้าที่นำบัตรเลือกตั้งปลอม ซึ่งหมายถึง ทั้งต้นขั้วและบัตรลงคะแนนที่ยังติดกันอยู่เป็นบัตรปลอมมาให้ผู้มาใช้สิทธิ์เลือกตั้งลงคะแนนที่หน่วยเลือกตั้ง เมื่อเสร็จสิ้นการลงคะแนน จึงนำบัตรลงคะแนนปลอมที่ผู้มาใช้สิทธิ์ได้ลงคะแนนไว้ไปสับเปลี่ยนกับบัตรลงคะแนนจริงที่ได้ลงคะแนนให้กับผู้สมัครคนหนึ่งคนใดไว้ และระหว่างการนับคะแนนที่เขตเลือกตั้ง เจ้าหน้าที่ประจำเขตเลือกตั้งก็จะตรวจสอบบัตรลงคะแนน พบว่าเป็นบัตรจริง และในภายหลังเจ้าหน้าที่ตรวจสอบต้นขั้วพบว่าเป็นต้นขั้วที่มีลายพิมพ์นิ้วมือไม่ซ้ำ จึงสรุปว่า ไม่มีการทุจริตเกิดขึ้น ทั้งที่จริงแล้ว ได้มีการสับเปลี่ยนบัตรลงคะแนนเกิดขึ้น จึงต้องออกแบบต้นขั้วให้ปลอมไม่ได้ คือมีข้อมูลคุณลักษณะเฉพาะตัว (F) ของกระดาษอยู่ด้วย ภายหลังการเลือกตั้งเจ้าหน้าที่จะตรวจสอบต้นขั้วก็จะทราบว่าเป็นต้นขั้วปลอม หรือหากมีการสับเปลี่ยนต้นขั้ว นำต้นขั้วจริงมาให้เจ้าหน้าที่ตรวจสอบ ก็ต้องว่าจ้างคนมาพิมพ์ลายนิ้วมือลงบนต้นขั้วจริง ซึ่งหากเป็นดังที่กล่าวมานี้ ก็จะเป็นหลักฐานที่จะโยงไปสู่ผู้กระทำผิดได้

3.8 กุญแจสำหรับการเข้าและถอดรหัสลับ

ข้อมูลประจำบัตรเลือกตั้งแต่ละใบจะถูกเข้ารหัสลับ โดยใช้การเข้ารหัสลับแบบกุญแจสาธารณะด้วยวิธี RSA ซึ่งเป็นวิธีการเข้ารหัสลับที่ได้รับความนิยมอย่างแพร่หลาย

3.8.1 การสร้างกุญแจ

จะต้องสร้างกุญแจขึ้นก่อนที่จะเข้ารหัสลับหรือถอดรหัสลับได้ ความยาวของกุญแจขึ้นอยู่กับระดับความปลอดภัยที่ต้องการของข้อมูลที่ถูกเข้ารหัส โดยกุญแจที่สร้างขึ้นจะมีหลายรูปแบบอย่างเช่น แฟ้มข้อมูลกุญแจ แฟ้มข้อมูลภาพรหัสแท่ง 1 มิติ และแฟ้มข้อมูลภาพรหัสแท่ง 2 มิติ แล้วแต่ความสะดวกของผู้ที่ถือกุญแจ

3.8.2 ส่วนประกอบของกุญแจ

กุญแจที่ใช้สำหรับการเข้าและถอดรหัสลับจะถูกสร้างทีละคู่คือ กุญแจส่วนตัวกับกุญแจสาธารณะ

3.8.2.1 กุญแจส่วนตัว

กุญแจส่วนตัวมีลักษณะพิเศษคือสามารถแบ่งออกเป็นส่วน ๆ ตามจำนวนคณะกรรมการที่มีอยู่ แล้วให้กรรมการแต่ละท่านเก็บรักษากุญแจของตนเองไว้เป็นความลับ

กุญแจส่วนตัวจะถูกเข้ารหัสลับไว้โดยใช้การเข้ารหัสลับแบบกุญแจลับ จึงต้องมีรหัสผ่านเมื่อต้องการนำกุญแจมาใช้ เพื่อป้องกันไม่ให้ผู้อื่นนำเอากุญแจส่วนตัวไปใช้ได้

3.8.2.2 กุญแจสาธารณะ

กุญแจสาธารณะ สามารถประกาศให้ผู้อื่นรับรู้ได้ เพื่อให้ผู้อื่นใช้กุญแจสาธารณะในการตรวจสอบความถูกต้องของข้อมูลบนบัตรเลือกตั้งได้

3.9 การพิมพ์รหัสลับลงบนบัตรเลือกตั้ง

ในการพิมพ์รหัสลับลงบนบัตรเลือกตั้ง จะมีขั้นตอนต่าง ๆ ดังนี้

- *อ่านข้อมูลกุญแจส่วนตัวของกรรมการเขต*

เพื่อใช้กุญแจส่วนตัวของกรรมการเขต (K_L^*) ในการเข้ารหัสลับข้อมูลประจำบัตร ($K_L^*[D]$)

- *การดึงคุณลักษณะเฉพาะตัวจากกระดาษที่ใช้พิมพ์บัตรเลือกตั้ง*

ใช้กล้องประจำเครื่องคอมพิวเตอร์ส่วนบุคคลเก็บภาพบริเวณพื้นที่ใช้สำหรับดึงข้อมูลคุณลักษณะของวัตถุชิ้นเล็ก ๆ ที่ฝังตัวอยู่ในกระดาษที่ใช้พิมพ์บัตรเลือกตั้งใบนั้น ทั้งในส่วนของต้นขั้วและบัตรลงคะแนน แล้วใช้โปรแกรมบนเครื่องไมโครคอมพิวเตอร์ดึงคุณลักษณะเฉพาะตัวของกระดาษ

- *รับรหัสเฉพาะ 2 ชั้นเข้ามา*

นำรหัสเฉพาะ 2 ชั้นไปถอดรหัส โดยใช้กุญแจสาธารณะของโปรแกรมในการถอดรหัส ($K_P[U_2] = K_P[K_P^*[K_C^*[U]]]$) ได้รหัสเฉพาะ 1 ชั้น ($U_1 = K_C^*[U]$) แล้วจึงนำรหัสเฉพาะ 1 ชั้น ($U_1 = K_C^*[U]$) ไปใช้เป็นข้อมูลส่วนหนึ่งของบัตรเลือกตั้ง

- *นำข้อมูลมาผ่านแฮชฟังก์ชันและลดขนาดค่าแฮช*

เลขประจำบัตร (N) คุณลักษณะเฉพาะตัวของเนื้อกระดาษ (F) และรหัสเฉพาะ 1 ชั้น ($U_1 = K_C^*[U]$) จะถูกนำมาผ่านแฮชฟังก์ชันได้ค่าแฮชขนาด 160 ไบต์ ($H[N;U_1;F]$) หลังจากนั้นจึงลดขนาดค่าแฮชให้เหลือ 4 ไบต์ ($H_4[N;U_1;F]$) โดยค่าแฮช ขนาด 4 ไบต์ จะสามารถแทนหมายเลขได้ทั้งหมด 2^{32} หรือ 4,294,967,296 หมายเลขและบัตรเลือกตั้งภายในเขตเลือกตั้งมีจำนวนต้นขั้วและบัตรลงคะแนนทั้งหมด 800,000 ใบ จึงทำให้มีโอกาสที่ค่าแฮชของบัตรแต่ละใบซ้ำกันได้น้อย ดังนั้นค่าแฮชขนาด 4 ไบต์ ($H_4 = H_4[N;U_1;F]$) จึงมีขนาดเพียงพอที่จะนำไปใช้อ้างอิงถึงบัตรเลือกตั้งแต่ละใบแบบย่อได้

- *การเข้ารหัสลับข้อมูลประจำบัตร*

นำข้อมูลค่าแฮชที่ได้ ($H_4 = H_4[N;U_1;F]$) ไปรวมกับเลขประจำบัตร (N) รหัสเฉพาะ 1 ชั้น (U_1) และคุณลักษณะเฉพาะตัวของกระดาษ (F) กลายเป็นข้อมูลประจำบัตรเลือกตั้ง ($D = N;U_1;F;H_4$) ใบนั้นๆ จากนั้น กรรมการเขตจะนำข้อมูลประจำบัตรมาเข้ารหัสลับด้วยวิธี RSA โดยใช้กุญแจส่วนตัวของกรรมการเขตได้ข้อมูลรหัสลับออกมา ($K_L^*[D]$)

- *การบันทึกรหัสลับลงบนบัตรเลือกตั้ง*

นำรหัสลับที่ได้จากขั้นตอนที่แล้วทั้งในส่วนของต้นขั้วและบัตรลงคะแนน ($K_L^*[D_S], K_L^*[D_V]$) มาเปลี่ยนเป็นรหัสแท่ง 2 มิติ แล้วจึงพิมพ์รหัสแท่ง 2 มิตินั้นลงบนบัตรเลือกตั้งแต่ละใบ เพื่อให้การตรวจสอบความถูกต้องของบัตรทำได้สะดวก ซึ่งอ่านได้แม่นยำและรวดเร็วกว่าการพิมพ์ชุดตัวเลขลงบนอุปกรณ์ตรวจสอบความถูกต้องเอง

3.10 การเปรียบเทียบค่าใช้จ่ายในการจัดพิมพ์บัตรเลือกตั้งระหว่างระบบการจัดพิมพ์ที่ได้นำเสนอในงานวิจัยนี้กับระบบการจัดพิมพ์ในปัจจุบัน

ค่าใช้จ่ายในการจัดพิมพ์บัตรเลือกตั้งของระบบการจัดพิมพ์ที่ได้นำเสนอ สามารถคำนวณได้อย่างคร่าวๆ ดังนี้

1. ค่าอุปกรณ์ที่ใช้ในการจัดพิมพ์บัตรเลือกตั้ง (เครื่องพิมพ์, กล้องประจำเครื่องคอมพิวเตอร์ส่วนบุคคล และไมโครคอมพิวเตอร์) ชุดละประมาณ 66,000 บาท ทั่วประเทศต้องใช้ถึง 4,000 ชุด จึงต้องเสียค่าใช้จ่ายประมาณ 264 ล้านบาท

2. ค่าหมึกพิมพ์และค่ากระดาษบัตรเลือกตั้ง ประมาณแผ่นละ 2 บาท บัตรเลือกตั้งที่จะต้องจัดพิมพ์ทั่วประเทศมีจำนวนทั้งหมด 160 ล้านใบ ดังนั้นจึงต้องเสียค่าใช้จ่ายประมาณ 320 ล้านบาท

3. ค่าจ้างเจ้าหน้าที่ดูแลการจัดพิมพ์ของเครื่องพิมพ์แต่ละเครื่อง ซึ่งจะต้องจ้างเจ้าหน้าที่ทั้งหมดประมาณ 4,000 คน ทั่วประเทศ และการจัดพิมพ์บัตรเลือกตั้งในแต่ละเขตจะต้องใช้เวลาประมาณ 10 วัน ถ้าเสียค่าจ้างเจ้าหน้าที่วันละ 200 บาทต่อคน จะเสียค่าใช้จ่ายทั้งหมดประมาณ 8 ล้านบาท

รวมค่าใช้จ่ายในการจัดพิมพ์บัตรเลือกตั้งอย่างคร่าวๆ ประมาณ 592 ล้านบาท (3.7 บาทต่อใบ) ซึ่งค่าใช้จ่ายดังกล่าวเป็นค่าใช้จ่ายในการจัดพิมพ์บัตรเลือกตั้งครั้งแรก หากมีการจัดพิมพ์บัตรเลือกตั้งในครั้งต่อๆ ไป จะเสียค่าใช้จ่ายในการจัดพิมพ์ที่ถูกลง เนื่องจากไม่ต้องเสียค่าอุปกรณ์ที่ใช้ในการจัดพิมพ์ ซึ่งค่าใช้จ่ายจะเหลือเพียง 328 ล้านบาท (2.05 บาทต่อใบ)

เมื่อเปรียบเทียบกับต้นทุนที่ใช้ในการจัดพิมพ์บัตรเลือกตั้งในปัจจุบัน ซึ่งจะมีราคาประมาณ 140 ล้านบาท (0.88 บาท ต่อใบ) จะเห็นว่าระบบการจัดพิมพ์ที่ได้นำเสนอในงานวิจัยนี้ใช้ต้นทุนในการจัดพิมพ์บัตรเลือกตั้งสูงกว่าระบบการจัดพิมพ์ในปัจจุบัน แต่บัตรเลือกตั้งที่นำการ

นำการเข้ารหัสลับแบบกุญแจสาธารณะมาใช้จะมีข้อดีตรงที่ทำให้การปลอมแปลงบัตรเลือกตั้งทำได้ยาก และสามารถตรวจสอบบัตรเลือกตั้งได้ง่ายว่าบัตรเลือกตั้งดังกล่าวเป็นบัตรเลือกตั้งจริงหรือไม่ ในขณะที่การตรวจสอบบัตรเลือกตั้งที่ใช้กันอยู่ในปัจจุบันจะใช้การมองว่าบัตรเลือกตั้งใบดังกล่าวมีสติกเกอร์ติดอยู่หรือไม่ ถ้าหากว่าบัตรเลือกตั้งใบไหนมีสติกเกอร์ติดก็จะเป็นบัตรเลือกตั้งจริง ในขณะที่บัตรเลือกตั้งใบไหนไม่มีสติกเกอร์ติดก็จะเป็นบัตรเลือกตั้งปลอม ซึ่งข้อเสียของการนำวิธีการติดสติกเกอร์มาใช้ก็คือ สติกเกอร์ที่ติดอยู่บนบัตรเลือกตั้งอาจจะหลุดออกจากบัตรเลือกตั้งเมื่อไหร่ก็ได้ จึงอาจจะทำให้บัตรเลือกตั้งจริงเป็นบัตรเลือกตั้งปลอมได้ และสติกเกอร์ที่ใช้ก็สามารถปลอมแปลงได้ไม่ยากนัก ดังนั้นวิธีการนำสติกเกอร์มาติดบนบัตรเลือกตั้งจึงมีความปลอดภัยต่อการปลอมแปลงและทุจริตค่อนข้างต่ำ

3.11 การตรวจสอบบัตรเลือกตั้งที่หน่วยเลือกตั้ง, สถานที่นับคะแนนและที่ว่าการอำเภอ

เนื่องจากบัตรเลือกตั้งมีจำนวนมาก การตรวจสอบบัตรเลือกตั้งทุกใบจะทำได้ยากเนื่องจากต้องใช้เวลาอย่างมากจึงใช้วิธีการสุ่มตรวจแทน โดยเลือกอัตราสุ่มตรวจที่เหมาะสม ถ้าอัตราสุ่มตรวจน้อยเกินไปก็อาจจะทำให้ผู้ที่อยากทุจริตเห็นว่าโอกาสที่จะถูกจับมีน้อยจึงอาจทุจริตได้ และถ้าอัตราสุ่มตรวจมากเกินไปก็จะทำให้เสียเวลาระหว่างขนย้ายบัตรเลือกตั้งได้ ในงานวิจัยนี้เสนออัตราการสุ่มตรวจบัตรเลือกตั้ง 1 ใบ ต่อบัตรเลือกตั้งทั้งหมด 100 ใบ สำหรับอุปกรณ์ที่ใช้ในการตรวจสอบบัตรเลือกตั้งที่หน่วยเลือกตั้งจะต่างจากการตรวจสอบที่สถานที่นับคะแนนและที่ว่าการอำเภอ เนื่องจากหน่วยเลือกตั้งในปัจจุบันมีทั้งหมด 80,000 หน่วย ถ้าใช้ไมโครคอมพิวเตอร์ทุกหน่วยจะทำให้เสียค่าใช้จ่ายสูง จึงใช้ไมโครคอนโทรลเลอร์แทนเนื่องจากเสียค่าใช้จ่ายต่ำกว่า แต่สำหรับสถานที่นับคะแนน ซึ่งปัจจุบันใช้สถานที่เดียวกับเขตเลือกตั้งและที่ว่าการอำเภอจะมีไมโครคอมพิวเตอร์ไว้ใช้ในการตรวจสอบ

3.11.1 การตรวจสอบบัตรเลือกตั้งที่หน่วยเลือกตั้ง

เมื่อบัตรเลือกตั้งถูกขนย้ายจากเขตเลือกตั้งมายังหน่วยเลือกตั้ง เจ้าหน้าที่ประจำหน่วยเลือกตั้งจะต้องสุ่มตรวจบัตรเลือกตั้ง ซึ่งอุปกรณ์ในการตรวจบัตรเลือกตั้งที่หน่วยเลือกตั้งประกอบด้วย ไมโครคอนโทรลเลอร์ เซนเซอร์สัมผัสภาพ และ LCD (Liquid Crystal Display) ซึ่งการตรวจสอบบัตรเลือกตั้งทำได้โดยใช้เซนเซอร์สัมผัสภาพและโปรแกรมบนไมโครคอนโทรลเลอร์อ่านรหัสแท่ง 2 มิติ ได้ข้อมูลรหัสลับออกมา ($K_L^*[D]$) แล้วจึงถอดรหัสลับได้ข้อมูลประจำบัตร ($D = K_L[K_L^*[D]]$) แสดงบนหน้าจอ LCD หลังจากนั้นเจ้าหน้าที่ประจำหน่วยจะตรวจสอบว่าข้อมูลประจำบัตร ($D = N;U_1;F;H_4$) ถูกต้องหรือไม่

3.11.2 การตรวจสอบบัตรเลือกตั้ง ณ สถานที่นับคะแนน

เมื่อบัตรลงคะแนนถูกส่งจากหน่วยเลือกตั้งมาถึงสถานที่นับคะแนน เจ้าหน้าที่ประจำสถานที่นับคะแนนจะสุ่มตรวจบัตรเลือกตั้งระหว่างการนับคะแนนโดยใช้โปรแกรมบนไมโครคอมพิวเตอร์ตรวจสอบข้อมูลประจำบัตรเลือกตั้ง ($D = N;U_1;F;H_4$)

3.11.3 การตรวจสอบบัตรเลือกตั้ง ณ ที่ว่าการอำเภอ

ภายหลังการลงคะแนนเลือกตั้ง เจ้าหน้าที่ประจำหน่วยเลือกตั้งจะส่งต้นขั้วของบัตรเลือกตั้งที่ใช้แล้วกับบัตรเลือกตั้งเปล่าที่ยังไม่ได้ใช้ไปยังที่ว่าการอำเภอเพื่อป้องกันผู้ทุจริตที่อาจจะนำบัตรลงคะแนนของบัตรเลือกตั้งเปล่าที่ยังไม่ได้ใช้ไปสับเปลี่ยนกับบัตรลงคะแนนที่ส่งไปยังสถานที่นับคะแนน ซึ่งที่ว่าการอำเภอจะมีไมโครคอมพิวเตอร์ไว้ตรวจสอบบัตรเลือกตั้ง เจ้าหน้าที่ประจำที่ว่าการอำเภอจะตรวจสอบบัตรเลือกตั้ง โดยใช้โปรแกรมบนไมโครคอมพิวเตอร์ตรวจสอบข้อมูลประจำบัตรเลือกตั้ง ($D = N;U_1;F;H_4$)

3.12 การป้องกันการปลอมแปลงและทุจริตในกระบวนการเลือกตั้ง

การกระจายการพิมพ์บัตรเลือกตั้งไปยังเขตเลือกตั้งต่างๆ จะมีข้อดีตรงที่ ส่วนกลางไม่ต้องรับภาระหนักในการจัดพิมพ์ โดยแต่ละเขตรับผิดชอบการพิมพ์บัตรเลือกตั้งเอง แต่มีข้อเสียตรงที่กรรมการเขตอาจจะทุจริตโดยพิมพ์บัตรเลือกตั้งหลายชุดและนำไปสับเปลี่ยนในภายหลัง จึงต้องหากระบวนการป้องกันการทุจริตจากบุคคลที่มีส่วนเกี่ยวข้องกับบัตรเลือกตั้ง โดยการทุจริตด้วยวิธีการต่างๆ มีดังนี้

3.12.1 พิมพ์บัตรเลือกตั้งหลายชุดเพื่อเตรียมสับเปลี่ยนในภายหลัง

เนื่องจากกรรมการเขตเป็นผู้ถือกุญแจในการจัดพิมพ์จึงอาจจะทุจริตได้โดยพิมพ์บัตรเลือกตั้งหลายชุดและนำไปสับเปลี่ยนในภายหลัง ดังนั้นกรรมการเลือกตั้งต้องหาวิธีป้องกันการทุจริตจากวิธีนี้ โดยการนำรหัสเฉพาะ (U) มาใช้เป็นส่วนหนึ่งของข้อมูลประจำบัตรเลือกตั้ง ($D = N;U_1;F;H_4$) แต่ละใบ ทั้งในส่วนต้นขั้วและบัตรลงคะแนนซึ่งรหัสเฉพาะของบัตรแต่ละใบจะมีข้อมูลไม่เหมือนกันและจะถูกเข้ารหัสโดยกรรมเลือกตั้ง ($U_1 = K_C^*[U]$) ซึ่งทำให้คนอื่นๆ ไม่สามารถปลอมแปลงได้ รหัสเฉพาะจะมีจำนวนจำกัดตามจำนวนบัตรเลือกตั้งที่กรรมการเขตต้องพิมพ์สำหรับการเลือกตั้งในครั้งนั้น ถ้ากรรมการเขตทุจริตโดยพิมพ์บัตรเลือกตั้งหลายๆ ชุด ก็ต้องใช้รหัสเฉพาะซ้ำกัน ขณะตรวจสอบบัตรเลือกตั้งหากพบรหัสเฉพาะซ้ำกันแสดงว่ามีการทุจริตเกิดขึ้นก็จะต้องมีการสอบสวนกรรมการเขต

3.12.2 พิมพ์บัตรเลือกตั้งหลายชุดและหาวิธีที่ทำให้ตรวจสอบไม่พบการใช้รหัสเฉพาะซ้ำ

การทุจริตโดยวิธีนี้กระทำได้โดยจัดพิมพ์บัตรเลือกตั้งหลายชุด ภายในชุดๆ หนึ่งจะไม่ใช้รหัสเฉพาะ (U) ซ้ำกันเลย แต่ระหว่างชุดจะใช้รหัสเฉพาะซ้ำกัน หลังจากที่ผู้มาใช้สิทธิ์ลงคะแนนหมดแล้วก็เทบัตรเลือกตั้งที่ลงคะแนนแล้วทิ้งทั้งหมดแล้วจึงเปลี่ยนบัตรลงคะแนนที่เตรียมมาทั้งชุด การทุจริตโดยวิธีนี้จะตรวจสอบได้ยากเนื่องจากบัตรลงคะแนนที่ส่งมายังสถานที่นับคะแนนใช้รหัสเฉพาะไม่ซ้ำกันเลย จึงต้องหาทางป้องกันการทุจริตด้วยวิธีนี้ โดยให้กรรมการเขตส่งแฟ้มข้อมูลรายงานการจัดพิมพ์ที่มีค่าแฮชและรหัสเฉพาะ 1 ชั้น ที่ถูกเข้ารหัสด้วยกุญแจสาธารณะของโปรแกรม ($K_P[H_{4S};U_{1S}], K_P[H_{4V};U_{1V}]$) มาให้กรรมการเลือกตั้ง หลังจากนั้นกรรมการเลือกตั้งก็จะรวบรวมและบันทึกค่าแฮชที่ถูกเข้ารหัสทั้งหมด ($K_P[H_{4S}], K_P[H_{4V}]$) ลงแฟ้มข้อมูลตรวจสอบค่าแฮชแล้วจึงส่งกลับไปให้กรรมการเขตเพื่อนำไปใช้เป็นฐานข้อมูลในการตรวจสอบค่าแฮชของบัตรเลือกตั้ง จึงทำให้กรรมการเขตใช้ได้เฉพาะบัตรเลือกตั้งที่ส่งค่าแฮชมาเท่านั้น หากพบบัตรเลือกตั้งที่มีค่าแฮชไม่ตรงกับค่าแฮชในฐานข้อมูลแสดงว่ามีการทุจริตเกิดขึ้น

3.12.3 นำบัตรเลือกตั้งปลอมไปให้ผู้มาใช้สิทธิ์ลงคะแนน

การทุจริตโดยวิธีนี้สามารถตรวจพบได้โดยการนำระบบต้นขั้วมาใช้ ซึ่งถ้านำต้นขั้วมาตรวจสอบภายหลังแล้วพบต้นขั้วปลอมที่มีลายพิมพ์นิ้วมือของผู้มาใช้สิทธิ์ แสดงว่าเกิดการทุจริตโดยนำบัตรเลือกตั้งปลอมไปให้ผู้มาใช้สิทธิ์ลงคะแนน

3.12.4 สับเปลี่ยนบัตรลงคะแนนก่อนถึงสถานที่นับคะแนน

การทุจริตโดยวิธีนี้สามารถตรวจพบได้ หากสุ่มตรวจพบบัตรเลือกตั้งปลอม ณ สถานที่นับคะแนน แต่เมื่อนำต้นขั้วมาตรวจแล้วพบว่าเป็นต้นขั้วจริงและมีลายพิมพ์นิ้วมือของผู้มาใช้สิทธิ์ด้วย แสดงว่ามีการทุจริตเกิดขึ้นระหว่างการขนส่งหีบบัตรเลือกตั้ง

3.12.5 นำบัตรเลือกตั้งปลอมมาเทเพิ่มหรือนำบัตรเลือกตั้งที่ลงคะแนนแล้วออกไป

การทุจริตโดยวิธีนี้สามารถตรวจพบได้ โดยขณะที่บัตรเลือกตั้งมาถึงเขตเลือกตั้งเจ้าหน้าที่ประจำเขตจะนับจำนวนบัตรเลือกตั้งทั้งหมดและบันทึกไว้ เพื่อที่จะนำไปตรวจสอบกับจำนวนต้นขั้วในภายหลัง หากพบว่ามีจำนวนไม่เท่ากันแสดงว่ามีการนำบัตรมาเทเพิ่มหรือนำออกไปจากหีบ

3.12.6 นำบัตรเลือกตั้งจริงจากเขตอื่นมาใช้

การทุจริตโดยวิธีนี้สามารถที่จะตรวจพบได้ ขณะที่ถอดรหัสลับข้อมูลก็จะรู้ข้อมูลประจำบัตรว่าบัตรนั้นมาจากเขตเลือกตั้งไหน หากมาจากเขตอื่นแสดงว่ามีการทุจริตเกิดขึ้น

3.12.7 นำบัตรเลือกตั้งจริงจากหน่วยอื่นมาใช้

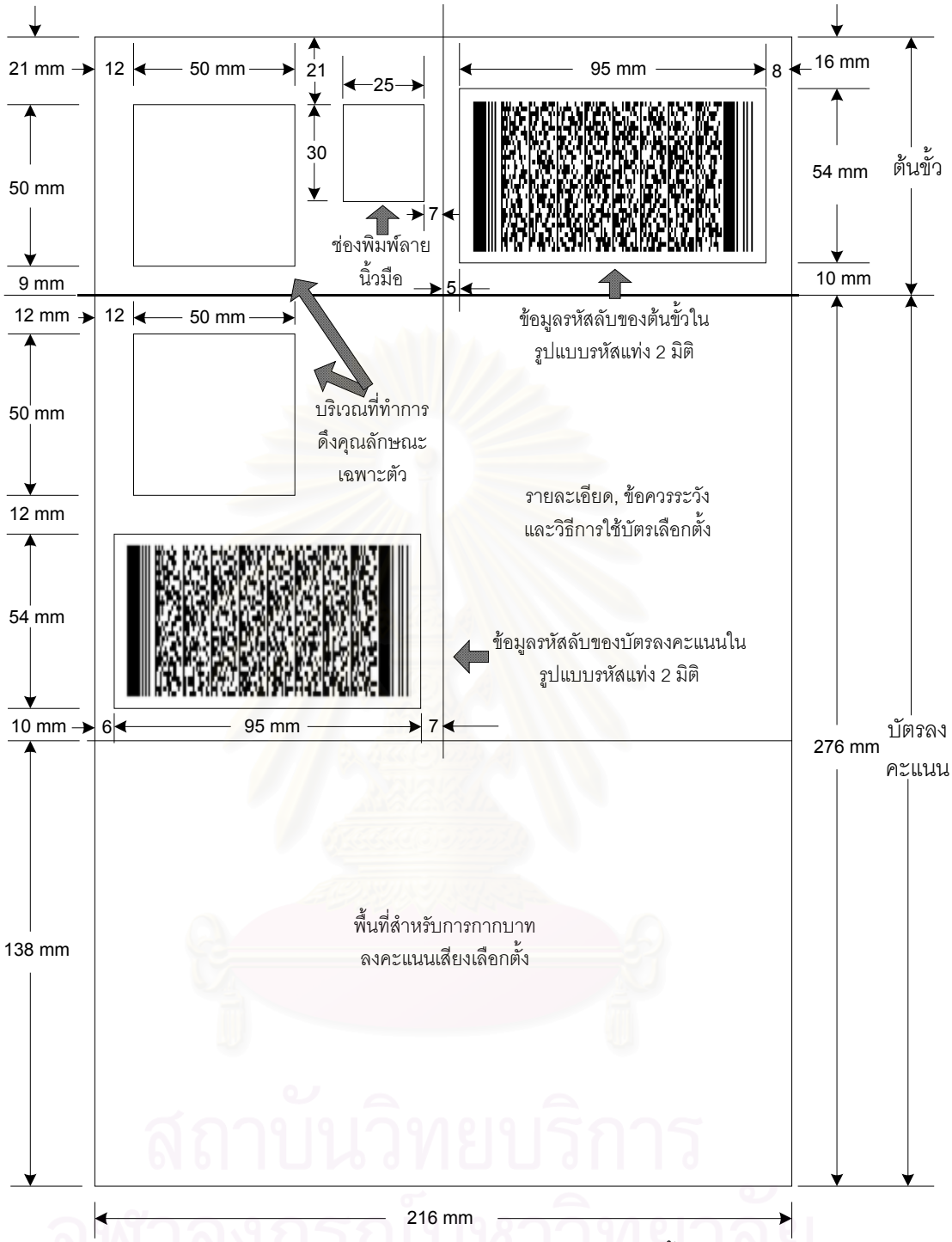
การทุจริตโดยวิธีนี้จะตรวจพบได้โดยตรวจสอบบัตรเลือกตั้งที่ยังไม่ได้ใช้ของทุกหน่วยเลือกตั้ง หากบัตรเลือกตั้งที่ยังไม่ได้ใช้ของหน่วยเลือกตั้งไหนหายไปหรือพบบัตรเลือกตั้งปลอมต้องสอบสวน

จากที่ได้กล่าวมาข้างต้น ไม่ว่าจะทุจริตด้วยวิธีใดๆ ก็ตาม ขณะตรวจสอบบัตรเลือกตั้ง หากพบบัตรเลือกตั้งปลอมจะต้องตรวจสอบบัตรเลือกตั้งทุกใบในเขตเลือกตั้งนั้น หากพบบัตรเลือกตั้งปลอมจำนวนไม่กี่ใบ ซึ่งมีไม่มากพอที่จะเปลี่ยนผลการเลือกตั้งได้ ก็ไม่ต้องเลือกตั้งใหม่ หากว่าพบบัตรเลือกตั้งปลอมจำนวนมากที่เพียงพอจะเปลี่ยนผลการเลือกตั้งได้ ก็ต้องเลือกตั้งใหม่ทั้งเขตเลือกตั้ง

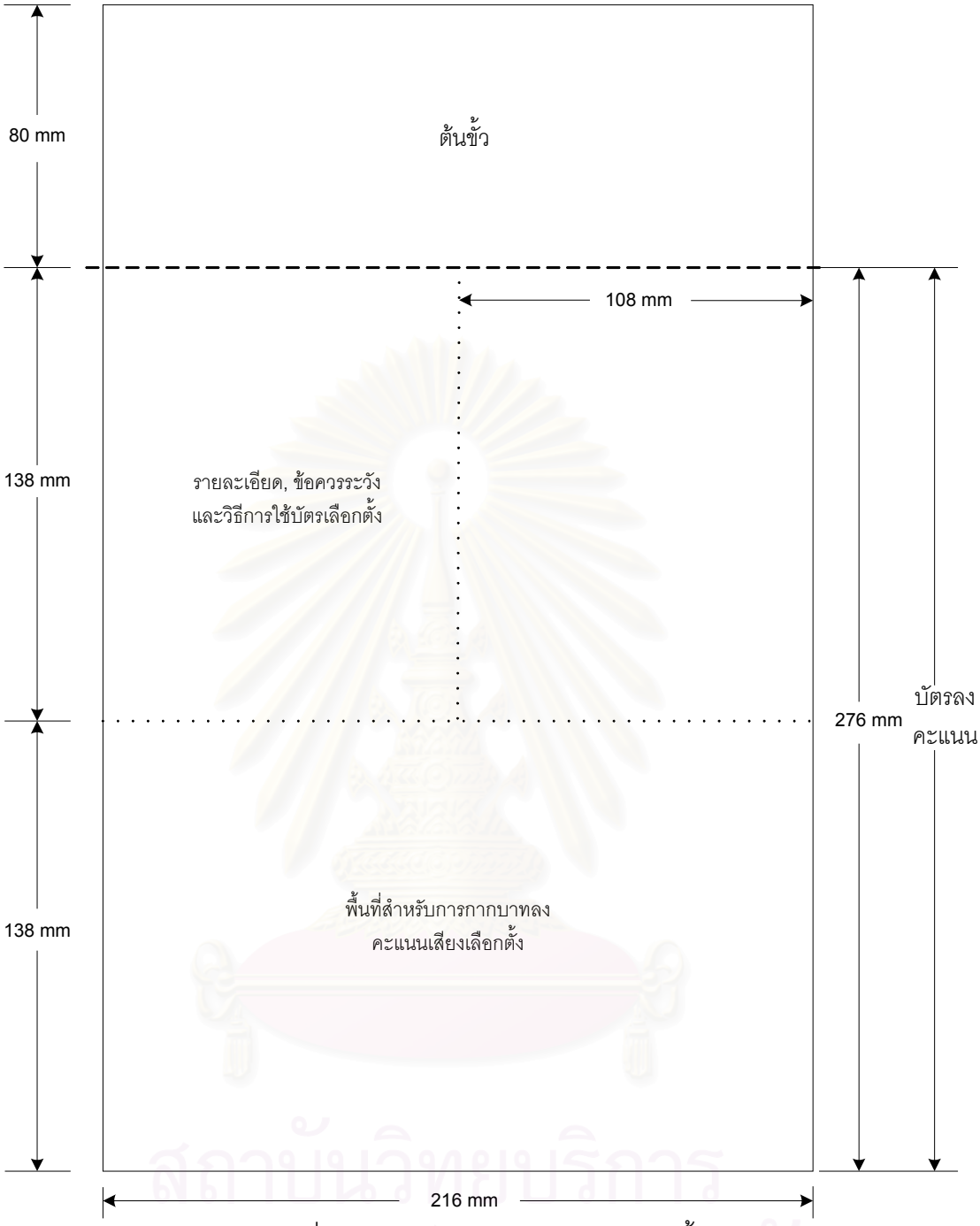
3.13 ผลการออกแบบ

3.13.1 ลักษณะของบัตรเลือกตั้ง

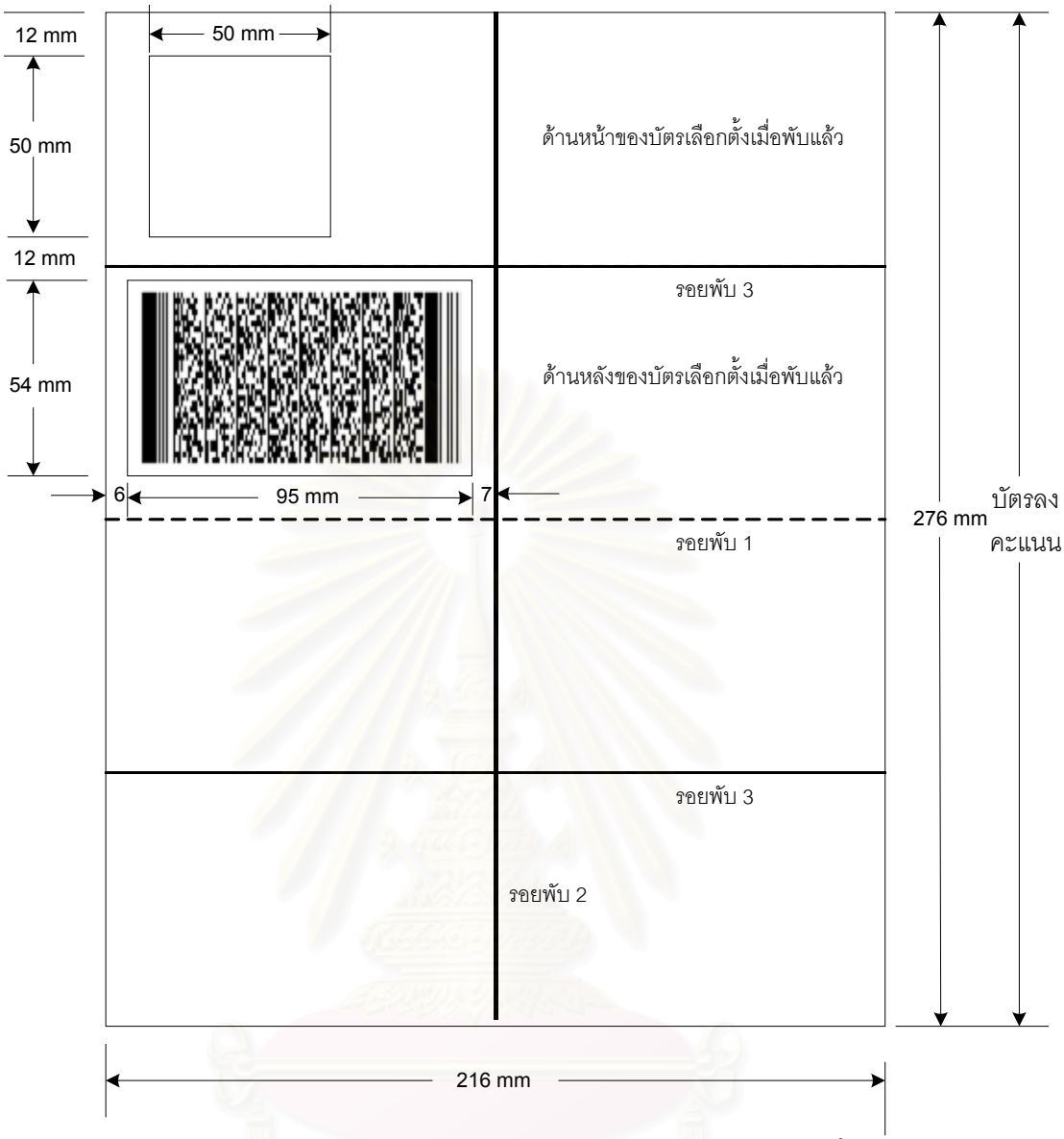
บัตรเลือกตั้งที่นำการเข้ารหัสลับมาใช้จะมีลักษณะคล้ายกับบัตรเลือกตั้งที่ใช้ในปัจจุบัน แต่จะมีส่วนที่เพิ่มขึ้นมาคือ รหัสแท่ง 2 มิติ และส่วนที่ใช้เป็นพื้นที่สำหรับการดึงข้อมูลคุณลักษณะเฉพาะของเนื้อกระดาษบัตรเลือกตั้ง โดยจะตีกรอบสี่เหลี่ยมไว้ทั้งที่ต้นขั้วและบัตรลงคะแนน บัตรเลือกตั้งที่พิมพ์ออกมาจะมีลักษณะเป็นเล่ม ในแต่ละเล่มมีบัตรเลือกตั้งจำนวน 100 ใบ บัตรเลือกตั้งแต่ละใบจะมีลักษณะดังรูปที่ 3.1, 3.2 และ 3.3



รูปที่ 3.1 ลักษณะด้านหน้าของบัตรเลือกตั้ง



รูปที่ 3.2 ลักษณะด้านหลังของบัตรเลือกตั้ง



รูปที่ 3.3 รอยพับของบัตรลงคะแนนก่อนหย่อนลงหีบเลือกตั้ง

3.13.2 **ข้อมูลประจำบัตรเลือกตั้ง**

บัตรเลือกตั้งจะประกอบด้วยข้อมูล 2 ส่วน คือ ข้อมูลประจำต้นขั้วและข้อมูลประจำบัตรลงคะแนน ($D_S; D_V$) โดยข้อมูลประจำบัตรแต่ละส่วนของทั้งต้นขั้วและบัตรลงคะแนนจะมีความยาวไม่เกิน 128 ไบต์ ประกอบด้วย

- *เลขประจำบัตร* (N) เป็นเลข BCD ขนาด 10 ไบต์ ประกอบด้วย
  - *วันเลือกตั้ง* ขนาด 4 ไบต์ ประกอบด้วย วันที่ ขนาด 1 ไบต์ เดือน ขนาด 1 ไบต์ และ ปี ขนาด 2 ไบต์ เช่น 31032003 หมายถึง วันที่ 31 มีนาคม ค.ศ.2003
  - *รหัสเขตเลือกตั้ง* ขนาด 2 ไบต์ จาก 1-400
  - *หมายเลขสมุดเลือกตั้ง* ขนาด 2 ไบต์ จาก 1-4,000

- *เลขที่บัตร* ขนาด 2 ไบต์ จาก 1-100 แบ่งได้ 2 ประเภทดังนี้
  - เลขที่ของต้นขั้ว จะมีเลขที่เรียงกันจาก 1-100
  - เลขที่ของบัตรลงคะแนน จะมีเลขที่ไม่เรียงกันแต่อยู่ระหว่าง 1-100
- *ข้อมูลรหัสเฉพาะ 1 ชั้น* ($U_1 = K_C^*[U]$) เป็นเลขฐาน 16 มีขนาด 64 ไบต์ เป็นข้อมูลรหัสเฉพาะที่ถูกเข้ารหัสโดยกุญแจส่วนตัวของกรรมการเลือกตั้ง ($U_1 = K_C^*[U]$) ข้อมูลรหัสเฉพาะก่อนเข้ารหัส (U) จะประกอบด้วยเลข BCD ดังนี้
  - *รหัสชนิด* ขนาด 1 ไบต์ แบ่งออกเป็น 2 ประเภท มีดังนี้
    - 01 คือ รหัสเฉพาะของต้นขั้ว
    - 02 คือ รหัสเฉพาะของบัตรลงคะแนน
  - *รหัสเขตเลือกตั้ง* ขนาด 2 ไบต์ จาก 1-400
  - *หมายเลขรหัสเฉพาะ* ขนาด 3 ไบต์ จากเลข 1-400,000 แบ่งได้ 2 ประเภท ดังนี้
    - หมายเลขรหัสเฉพาะของต้นขั้ว จะมีหมายเลขรหัสเฉพาะเรียงกัน มีค่าตั้งแต่ 1-400,000
    - หมายเลขรหัสเฉพาะของบัตรลงคะแนน จะมีหลายเลขรหัสเฉพาะไม่เรียงกัน แต่มีค่าอยู่ในช่วงระหว่าง 1-400,000
- *ข้อมูลคุณลักษณะเฉพาะตัวของกระดาษที่ใช้พิมพ์บัตรเลือกตั้ง* (F) เป็นเลขฐาน 16 มีขนาดไม่เกิน 50 ไบต์
- *ค่าแฮช* เป็นเลขฐาน 16 มีขนาด 4 ไบต์ได้จากการนำข้อมูลทั้งสามส่วนข้างต้นมาผ่านแฮชฟังก์ชัน ($H[N;U_1;F]$) ได้ค่าแฮชออกมา 160 ไบต์แล้วจึงตัดบางส่วนของค่าแฮชออกไป นำมาใช้เพียง 4 ไบต์ ($H_4 = H_4[N;U_1;F]$)

ข้อมูลเหล่านี้จะถูกนำมาเข้ารหัสลับ ($K_L^*[D] = K_L^*[N;U_1;F;H_4]$) แล้วเปลี่ยนเป็นรหัสแท่ง 2 มิติ ก่อนพิมพ์ลงบนบัตรเลือกตั้ง

บทที่ 4

ต้นแบบระบบการจัดพิมพ์และตรวจสอบบัตรเลือกตั้ง

ในบทนี้ จะกล่าวถึงรายละเอียดของระบบการจัดพิมพ์และตรวจสอบบัตรเลือกตั้งที่ได้พัฒนาขึ้น รวมทั้งปรับกระบวนการเลือกตั้งให้สอดคล้องกับวิธีการที่จะนำมาใช้ตามที่ได้ออกแบบไว้ในบทที่ 3

4.1 กระบวนการในการจัดพิมพ์, ควบคุมและตรวจสอบบัตรเลือกตั้ง

สำหรับระบบการจัดพิมพ์บัตรเลือกตั้งในปัจจุบันจะประกอบด้วยหน่วยงาน 4 หน่วยงานหลักๆ ได้แก่

1.*ส่วนกลาง* กรรมการเลือกตั้งจะประจำอยู่ที่ส่วนกลางคอยทำหน้าที่ต่างๆ ดังนี้

- *จัดพิมพ์บัตรเลือกตั้ง* กรรมการเลือกตั้งจะคอยดูแลเรื่องการจัดพิมพ์บัตรเลือกตั้งให้เสร็จทันกำหนดเวลา
- *จัดส่งบัตรเลือกตั้ง* เมื่อกรรมการเลือกตั้งจัดพิมพ์บัตรเลือกตั้งเสร็จแล้วก็จะส่งบัตรเลือกตั้งและสติกเกอร์ไปให้กรรมการเขต

2. *เขตเลือกตั้ง* กรรมการเขตและเจ้าหน้าที่ประจำเขตจะประจำอยู่ที่เขตเลือกตั้งคอยทำหน้าที่ต่างๆ ดังนี้

- *จัดส่งบัตรเลือกตั้ง* เมื่อกรรมการเขตได้รับบัตรเลือกตั้งและสติกเกอร์จากกรรมการเลือกตั้งแล้วก็จะนำไปแจกจ่ายตามหน่วยเลือกตั้งต่างๆ

3. *หน่วยเลือกตั้ง* กรรมการหน่วยจะประจำอยู่ที่หน่วยเลือกตั้ง มีหน้าที่ดังนี้

- *นำบัตรไปให้ผู้มาใช้สิทธิ์ลงคะแนน* โดยเมื่อกรรมการหน่วยได้รับสติกเกอร์และบัตรเลือกตั้งจากกรรมการเขตแล้วก็จะนำสติกเกอร์ไปติดบนบัตรเลือกตั้งแล้วจึงนำบัตรเลือกตั้งไปให้ผู้มาใช้สิทธิ์ลงคะแนน
- *จัดส่งบัตรเลือกตั้ง* หลังจากหมดเวลาในการเลือกตั้ง เจ้าหน้าที่ประจำหน่วยจะต้องส่งบัตรลงคะแนนไปยังสถานที่นับคะแนน และส่งสติกเกอร์, ต้นขั้วของบัตรเลือกตั้งที่ใช้แล้วกับบัตรเลือกตั้งเปล่าที่ยังไม่ได้ใช้ไปเก็บไว้ยังสถานีตำรวจเพื่อป้องกันการนำบัตรลงคะแนนของบัตรเลือกตั้งเปล่าที่ยังไม่ได้ใช้ไปสับเปลี่ยนกับบัตรลงคะแนนที่ส่งไปยังสถานที่นับคะแนน

4. *สถานีตำรวจ* เจ้าหน้าที่ตำรวจจะประจำอยู่ที่สถานีตำรวจ โดยทำหน้าที่ดังนี้

- *เก็บรักษาบัตรเลือกตั้ง* เจ้าหน้าที่ตำรวจจะต้องเก็บรักษาต้นขั้วของบัตรเลือกตั้งที่ใช้แล้วกับบัตรเลือกตั้งเปล่าที่ยังไม่ได้ใช้เพื่อป้องกันไม่ให้ผู้อื่นนำไปทุจริตได้

สำหรับระบบการจัดพิมพ์บัตรเลือกตั้งแบบกระจายศูนย์การจัดพิมพ์ที่ได้ออกแบบในงานวิจัยนี้จะจัดพิมพ์ที่เขตเลือกตั้งโดยจะมีหน่วยงานที่เกี่ยวข้องกับระบบเลือกตั้งอยู่ 4 แห่ง ดังนี้

1. *ส่วนกลาง* กรรมการเลือกตั้งจะอยู่ที่ส่วนกลาง ทำหน้าที่หลักๆ ดังนี้
   - *ควบคุมไม่ให้กรรมการเขตทุจริต* เนื่องจากกรรมการเขตอาจจะทุจริตโดยพิมพ์บัตรเลือกตั้งหลายชุดและสับเปลี่ยนบัตรเลือกตั้งในภายหลังได้ ดังนั้นกรรมการเลือกตั้งจึงต้องหาวิธีป้องกันกรรมการเขตทุจริต โดยสิ่งที่กรรมการเลือกตั้งใช้ควบคุมไม่ให้กรรมการเขตทุจริตมีดังนี้
     - *แฟ้มข้อมูลรหัสเฉพาะ* ($U_2 = K_P^*[K_C^*[U]]$) ที่กรรมการเลือกตั้งจะต้องส่งไปให้กรรมการเขตเพื่อให้กรรมการเขตพิมพ์บัตรเลือกตั้งได้เพียงชุดเดียว
     - *แฟ้มข้อมูลรายงานการจัดพิมพ์* ($K_P[H_{4S};U_{1S}], K_P[H_{4V};U_{1V}]$) ที่ทางกรรมการเขตจะต้องส่งไปให้กรรมการเลือกตั้ง เพื่อรายงานว่าบัตรเลือกตั้งที่กรรมการเขตพิมพ์ไปแล้วนั้นมีค่าแฮชและรหัสเฉพาะอย่างที่ส่งไปในรายงาน สำหรับรายละเอียดในการใช้รหัสเฉพาะและค่าแฮชเพื่อป้องกันการทุจริตของกรรมการเขตได้กล่าวไว้แล้วในหัวข้อที่ 3.7
   - *จัดส่งสิ่งต้องใช้ในการจัดพิมพ์และตรวจสอบบัตรเลือกตั้ง* กรรมการเลือกตั้งจะต้องจัดส่งสิ่งที่กรรมการเขตต้องใช้ในการจัดพิมพ์และตรวจสอบบัตรเลือกตั้งไปให้กรรมการเขต ซึ่งสิ่งที่กรรมการเลือกตั้งจะต้องส่งมีดังนี้
     - *กระดาษบัตรเลือกตั้ง* เพื่อให้กรรมการเขตนำไปดึงคุณลักษณะเฉพาะตัวของกระดาษ (F) และพิมพ์รหัสลับ ($K_L^*[D]$) ในรูปแบบรหัสแท่ง 2 มิติ ลงบนบัตรเลือกตั้ง
     - *โปรแกรมสร้างกุญแจ* เพื่อให้กรรมการเขตสร้างกุญแจของตนเองและใช้กุญแจในการเข้ารหัสข้อมูลประจำบัตรเลือกตั้ง ($K_L^*[D]$)
     - *แฟ้มข้อมูลรหัสเฉพาะ* ($U_2 = K_P^*[K_C^*[U]]$) เพื่อให้กรรมการเขตนำรหัสเฉพาะ 1 ชั้น ($U_1 = K_C^*[U]$) ไปใช้เป็นส่วนหนึ่งของข้อมูลประจำบัตรเลือกตั้ง ($D = N;U_1;F;H_4$)

- *โปรแกรมพิมพ์บัตรเลือกตั้ง* เพื่อให้กรรมการเขตนำไปใช้ในการพิมพ์บัตรเลือกตั้ง ซึ่งโปรแกรมพิมพ์บัตรเลือกตั้งจะถูกฝังกุญแจสาธารณะของโปรแกรม (K_P) ไว้เพื่อใช้ในการเข้ารหัสค่าแฮชและรหัสเฉพาะที่จะบันทึกลงแฟ้มข้อมูลรายงานการจัดพิมพ์ ($K_P[H_{4S};U_{1S}], K_P[H_{4V};U_{1V}]$) นอกจากนี้ยังใช้กุญแจสาธารณะของโปรแกรมถอดรหัส รหัสเฉพาะ 2 ชั้น เพื่อนำรหัสเฉพาะ 1 ชั้น ($K_P[U_2] = K_P[K_P^*[K_C^*[U]]] = K_C^*[U] = U_1$) ไปใช้เป็นส่วนหนึ่งของข้อมูลประจำบัตรเลือกตั้ง ($D = N;U_1;F;H_4$)
- *แฟ้มข้อมูลตรวจสอบค่าแฮช* ($K_P[H_{4S}], K_P[H_{4V}]$) เมื่อกรรมการเลือกตั้งได้รับแฟ้มข้อมูลรายงานการจัดพิมพ์ ($K_P[H_{4S};U_{1S}], K_P[H_{4V};U_{1V}]$) จากกรรมการเขตแล้วก็จะรวบรวมและบันทึกค่าแฮชที่ถูกเข้ารหัสลงแฟ้มข้อมูลตรวจสอบค่าแฮช ($K_P[H_{4S}], K_P[H_{4V}]$) และส่งแฟ้มข้อมูลไปให้กรรมการเขตเพื่อใช้เป็นฐานข้อมูลในการตรวจสอบค่าแฮชของบัตรเลือกตั้ง
- *โปรแกรมตรวจสอบบัตรเลือกตั้ง* เพื่อให้กรรมการเขตสามารถตรวจสอบบัตรเลือกตั้งที่ลงคะแนนแล้วจากหน่วยเลือกตั้งได้

2. *เขตเลือกตั้ง* กรรมการเขตและเจ้าหน้าที่ประจำเขตจะอยู่ที่เขตเลือกตั้ง ซึ่งมีหน้าที่ดังนี้
   - *จัดพิมพ์บัตรเลือกตั้ง* กรรมการเขตจะคอยดูแลระบบการจัดพิมพ์อย่างใกล้ชิด เพื่อป้องกันไม่ให้บัตรเลือกตั้งที่พิมพ์เสร็จแล้ว ถูกลักลอบนำออกไปเพื่อทุจริตได้และยังต้องคอยดูแลเวลาระบบการจัดพิมพ์ให้พิมพ์บัตรเลือกตั้งเสร็จทันตามกำหนด
   - *จัดส่งบัตรเลือกตั้งเปล่าและกุญแจ* เมื่อทางเขตเลือกตั้งจัดพิมพ์บัตรเลือกตั้งเสร็จ จะต้องส่งสิ่งต่อไปนี้ไปยังหน่วยเลือกตั้ง
     - *บัตรเลือกตั้งเปล่า* เพื่อให้กรรมการหน่วยนำไปให้ผู้มาใช้สิทธิ์ลงคะแนน
     - *กุญแจสาธารณะของกรรมการเขต* (K_L) เพื่อให้กรรมการหน่วยนำไปถอดรหัสข้อมูลรหัสลับของบัตรเลือกตั้ง ($K_L[K_L^*[D]] = D$) ได้ข้อมูลประจำบัตรเลือกตั้ง ($D = N;U_1;F;H_4$) ออกมาตรวจสอบ
   - *ส่งรายงานการจัดพิมพ์ไปให้กรรมการเลือกตั้ง* กรรมการเขตจะส่งแฟ้มข้อมูลรายงานการจัดพิมพ์ ($K_P[H_{4S};U_{1S}], K_P[H_{4V};U_{1V}]$) ไปยังส่วนกลางเพื่อรายงานว่าได้จัดพิมพ์บัตรเลือกตั้งที่มีข้อมูลค่าแฮชและรหัสเฉพาะอย่างที่ได้รายงานไป
   - *นับคะแนนและตรวจสอบบัตรเลือกตั้ง* เจ้าหน้าที่ประจำเขตจะต้องนับคะแนนและตรวจสอบบัตรเลือกตั้งที่ได้รับมาจากหน่วยเลือกตั้ง

3. *หน่วยเลือกตั้ง* ที่หน่วยเลือกตั้งจะมีเจ้าหน้าที่ประจำหน่วยอยู่ โดยมีหน้าที่ดังนี้
   - *ตรวจสอบบัตรเลือกตั้ง* เมื่อเจ้าหน้าที่ประจำหน่วยได้รับบัตรเลือกตั้งจากกรรมการเขตก็จะสุ่มตรวจสอบว่าบัตรเลือกตั้งใบนั้นเป็นบัตรเลือกตั้งที่กรรมการเขตส่งมาจริงหรือไม่ โดยใช้กุญแจสาธารณะของกรรมการเขตในการถอดรหัสข้อมูลรหัสลับ ($K_L[K_L^*[D]] = D$) หลังจากนั้นจะตรวจสอบข้อมูลประจำบัตรเลือกตั้ง (D) ว่าถูกต้องหรือไม่
   - *นำบัตรเลือกตั้งไปให้ผู้มาใช้สิทธิ์ลงคะแนน* กรรมการหน่วยจะนำบัตรเลือกตั้งไปให้ผู้มาใช้สิทธิ์ลงคะแนน
   - *จัดส่งบัตรเลือกตั้ง* หลังจากหมดเวลาในการลงคะแนนการเลือกตั้ง กรรมการหน่วยจะต้องส่งบัตรเลือกตั้งที่ลงคะแนนแล้วกลับไปยังเขตเลือกตั้ง เพื่อให้เจ้าหน้าที่ประจำเขตเลือกตั้งนับคะแนนและตรวจสอบ นอกจากนี้ยังต้องส่งต้นขั้วของบัตรเลือกตั้งที่ใช้แล้วกับบัตรเลือกตั้งเปล่าที่ยังไม่ได้ใช้ไปยังที่ว่าการอำเภอ
4. *ที่ว่าการอำเภอ* เจ้าหน้าที่ประจำที่ว่าการอำเภอจะมีหน้าที่ดังนี้
   - *เก็บรักษาบัตรเลือกตั้ง* เจ้าหน้าที่ประจำที่ว่าการอำเภอจะต้องเก็บรักษาต้นขั้วของบัตรเลือกตั้งที่ใช้แล้วกับบัตรเลือกตั้งเปล่าที่ยังไม่ได้ใช้
   - *ตรวจสอบบัตรเลือกตั้ง* ภายหลังการเลือกตั้ง เจ้าหน้าที่ประจำที่ว่าการอำเภอจะต้องจะต้องสุ่มตรวจสอบต้นขั้วของบัตรเลือกตั้งที่ใช้แล้วกับบัตรเลือกตั้งเปล่าที่ยังไม่ได้ใช้ เพื่อป้องกันเจ้าหน้าที่ประจำหน่วยนำบัตรเลือกตั้งปลอมไปให้ผู้มาใช้สิทธิ์ลงคะแนน และป้องกันการทุจริตด้วยการนำบัตรลงคะแนนของบัตรเลือกตั้งที่ยังไม่ได้ใช้ไปสับเปลี่ยนกับบัตรลงคะแนนที่ส่งไปยังสถานที่นับคะแนน

เมื่อลองเปรียบเทียบข้อดี-ข้อเสียของระบบการจัดพิมพ์และตรวจสอบบัตรเลือกตั้งในปัจจุบันกับระบบการจัดพิมพ์และตรวจสอบบัตรเลือกตั้งที่ได้นำเสนอในงานวิจัยนี้ จะสามารถเปรียบเทียบได้ดังนี้

- *ระบบการจัดพิมพ์บัตรเลือกตั้งในปัจจุบัน*

<u>ข้อดี</u>

- สามารถจัดพิมพ์บัตรเลือกตั้งให้เสร็จภายในระยะสั้นๆ ได้ และมีความยุ่งยากในการจัดพิมพ์ไม่มากนักเพียงแค่นำบัตรเลือกตั้งและสติกเกอร์ไปสั่งพิมพ์ตามโรงพิมพ์ทั่วไป
- การตรวจสอบบัตรเลือกตั้งแต่ละใบสามารถทำได้อย่างสะดวกรวดเร็ว เพียงแค่ตรวจสอบว่าบัตรลงคะแนนแต่ใบมีสติกเกอร์ติดอยู่หรือไม่

ข้อเสีย

- การทุจริตสามารถทำได้ไม่ยากเพียงแค่นำสติกเกอร์และบัตรเลือกตั้งไปสั่งพิมพ์เพิ่มตามโรงพิมพ์ทั่วๆ ไป แล้วจึงค่อยนำมาสับเปลี่ยนกับบัตรเลือกตั้งจริงในภายหลังได้
- สติกเกอร์ที่ติดบนบัตรเลือกตั้งอาจจะหลุดออกจากบัตรเลือกตั้งเมื่อไหร่ก็ได้จึงอาจจะทำให้บัตรเลือกตั้งปลอมเป็นบัตรเลือกตั้งจริงได้

- *ระบบการจัดพิมพ์และตรวจสอบบัตรเลือกตั้งที่ได้นำเสนอในงานวิจัยนี้*

ข้อดี

- สามารถป้องกันการปลอมแปลงบัตรเลือกตั้งและป้องกันการทุจริตจากเจ้าหน้าที่ที่เกี่ยวข้องได้

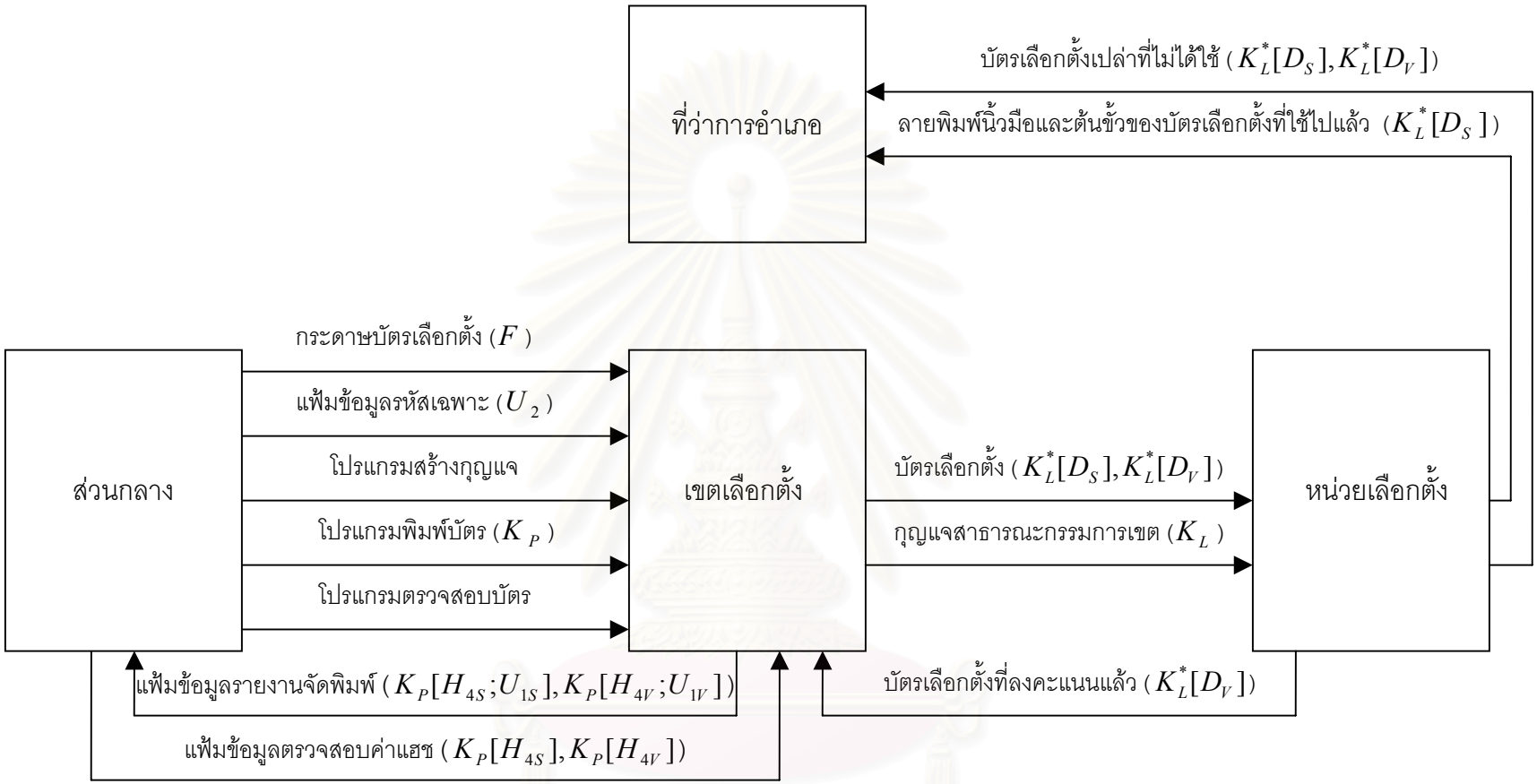
ข้อเสีย

- เสียค่าใช้จ่ายในการจัดพิมพ์ที่สูงกว่าระบบการจัดพิมพ์ในปัจจุบัน

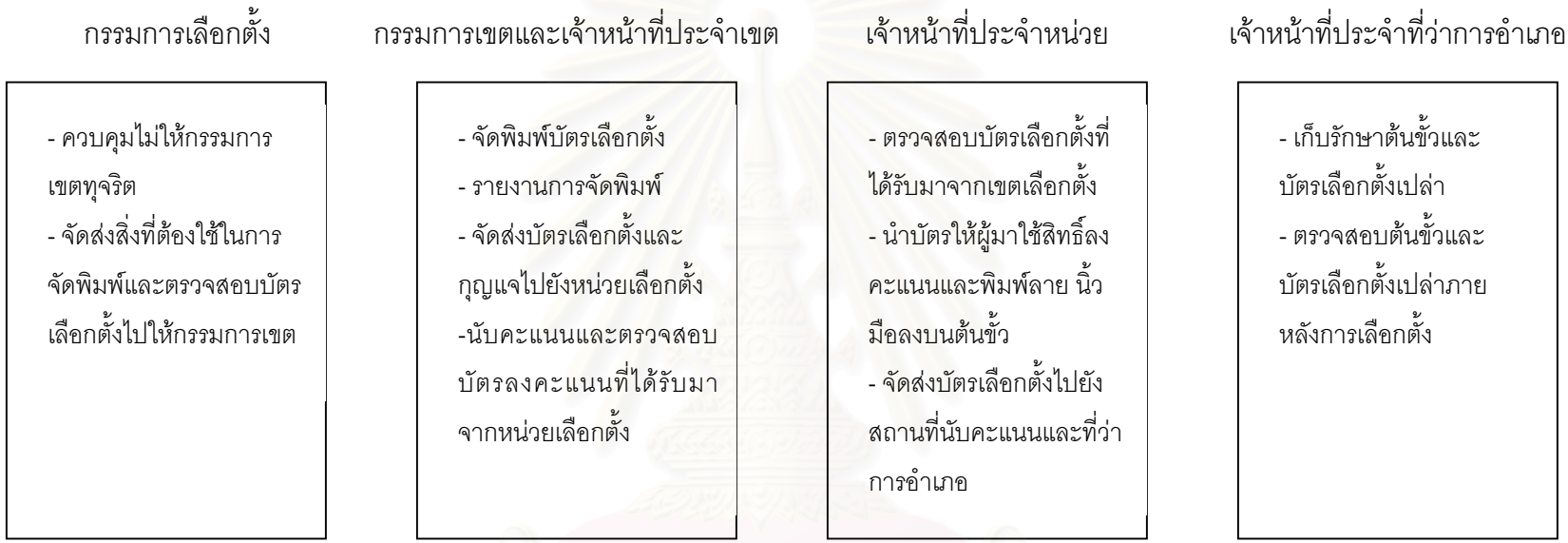
จากข้อดี-ข้อเสีย ที่ได้กล่าวไว้ข้างต้น ถึงแม้ว่าระบบการจัดพิมพ์บัตรเลือกตั้งแบบกระจายศูนย์จะเสียค่าใช้จ่ายใช้ในการจัดพิมพ์สูงกว่าระบบการจัดพิมพ์ในปัจจุบันแต่สามารถป้องกันการทุจริตและการปลอมแปลงบัตรเลือกตั้งได้ ในงานวิจัยนี้จึงได้นำระบบการจัดพิมพ์แบบกระจายศูนย์มาใช้

จากกระบวนการที่ได้กล่าวไว้ของระบบการจัดพิมพ์บัตรเลือกตั้งแบบกระจายศูนย์ สามารถแสดงเป็นแผนผังต่างๆ ได้ดังนี้

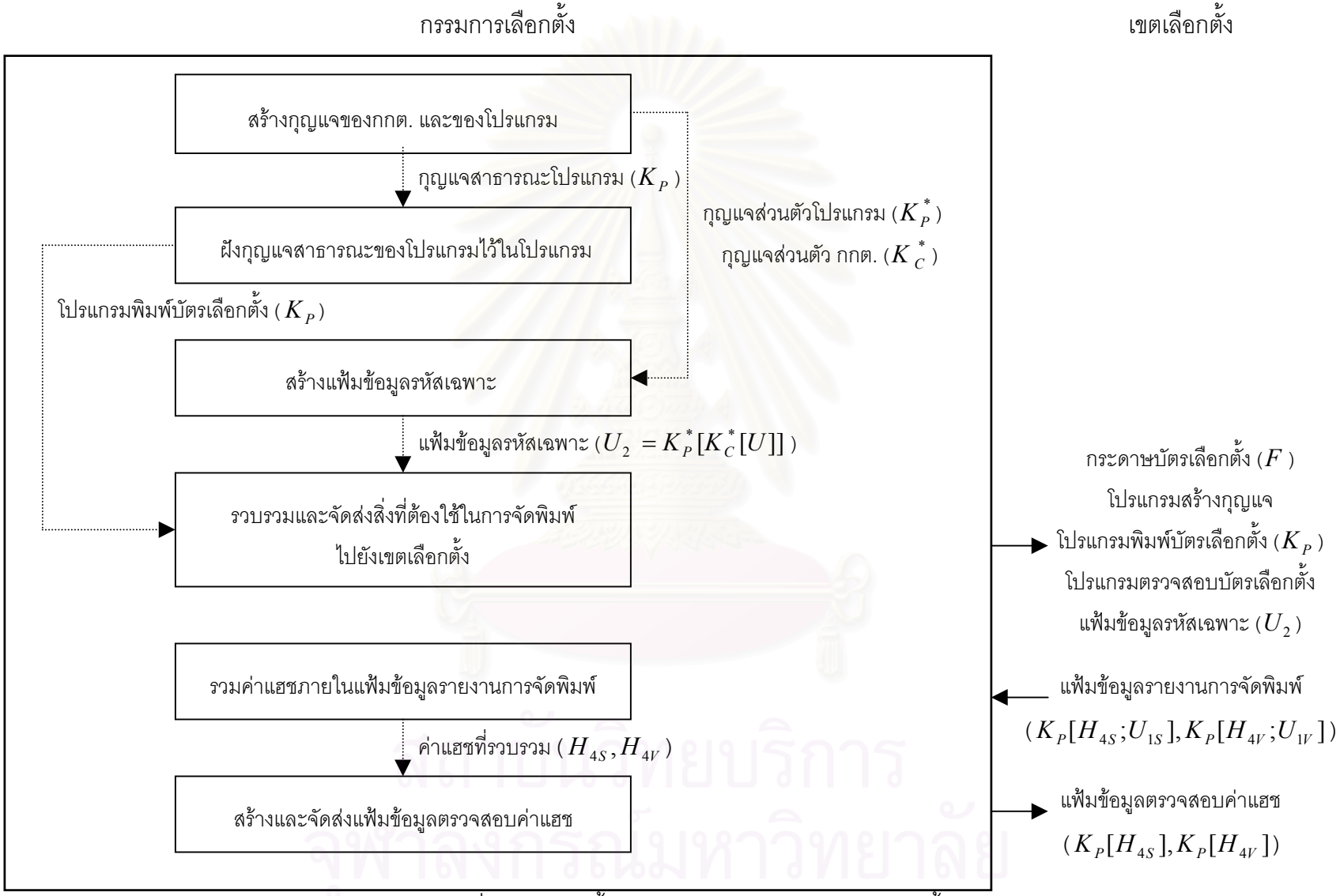
- แผนผังการรับส่งบัตรเลือกตั้ง แฟ้มข้อมูล กุญแจและโปรแกรม ระหว่างหน่วยงานต่างๆ แสดงได้ดังรูปที่ 4.1
- แผนผังหน้าที่หลักของเจ้าหน้าที่ประจำหน่วยงานต่างๆ แสดงได้ดังรูปที่ 4.2
- แผนผังขั้นตอนการทำงานของกรรมการเลือกตั้ง แสดงได้ดังรูปที่ 4.3
- แผนผังขั้นตอนการทำงานของกรรมการเขตและเจ้าหน้าที่ประจำเขต แสดงได้ดังรูปที่ 4.4
- แผนผังขั้นตอนการทำงานของเจ้าหน้าที่ประจำหน่วย แสดงได้ดังรูปที่ 4.5
- แผนผังขั้นตอนการทำงานของเจ้าหน้าที่ประจำที่ว่าการอำเภอ แสดงได้ดังรูปที่ 4.6



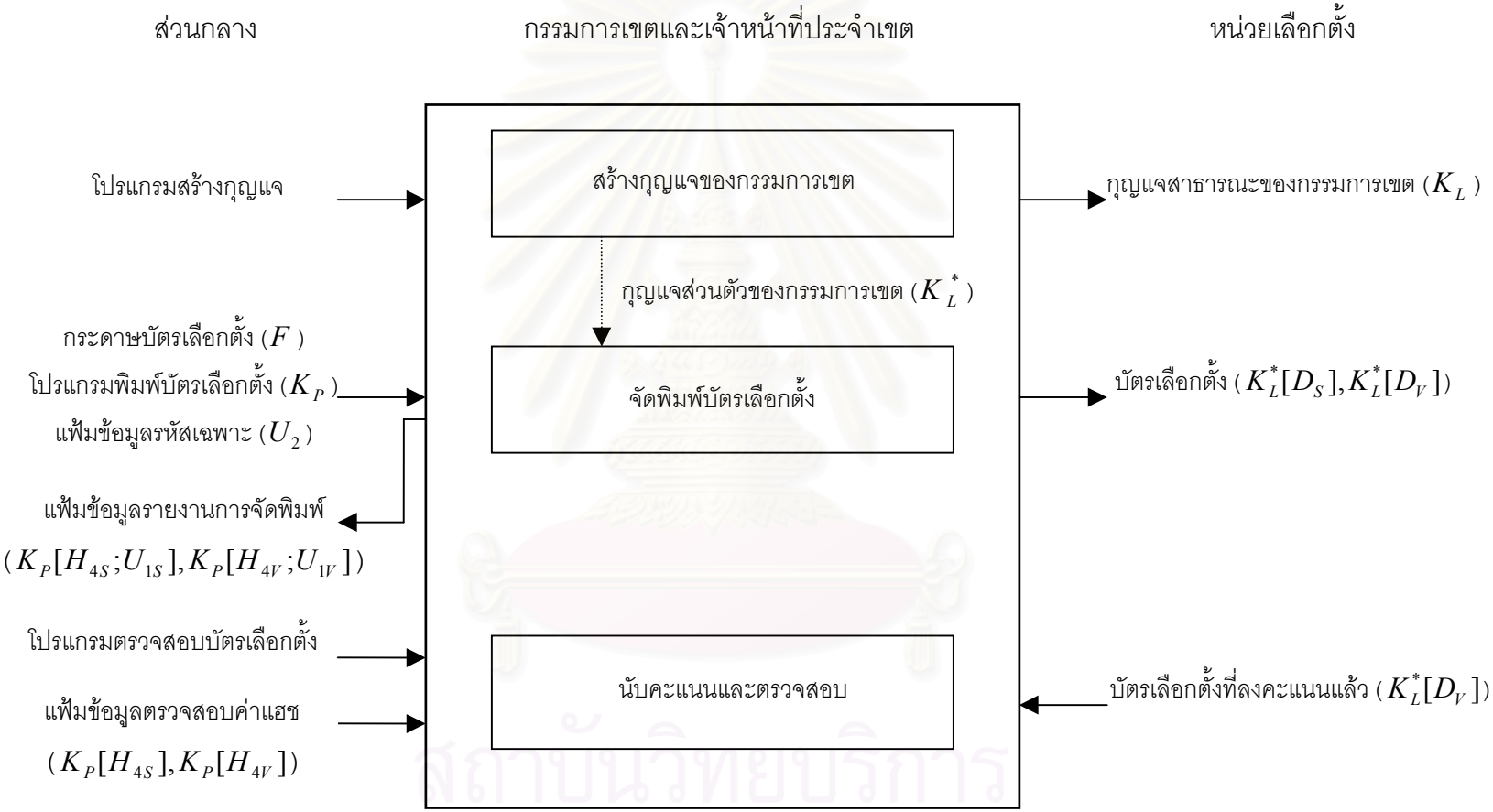
รูปที่ 4.1 แผนผังการรับส่งบัตรเลือกตั้ง แฟ้มข้อมูล กุญแจและโปรแกรมระหว่างหน่วยงานต่างๆ



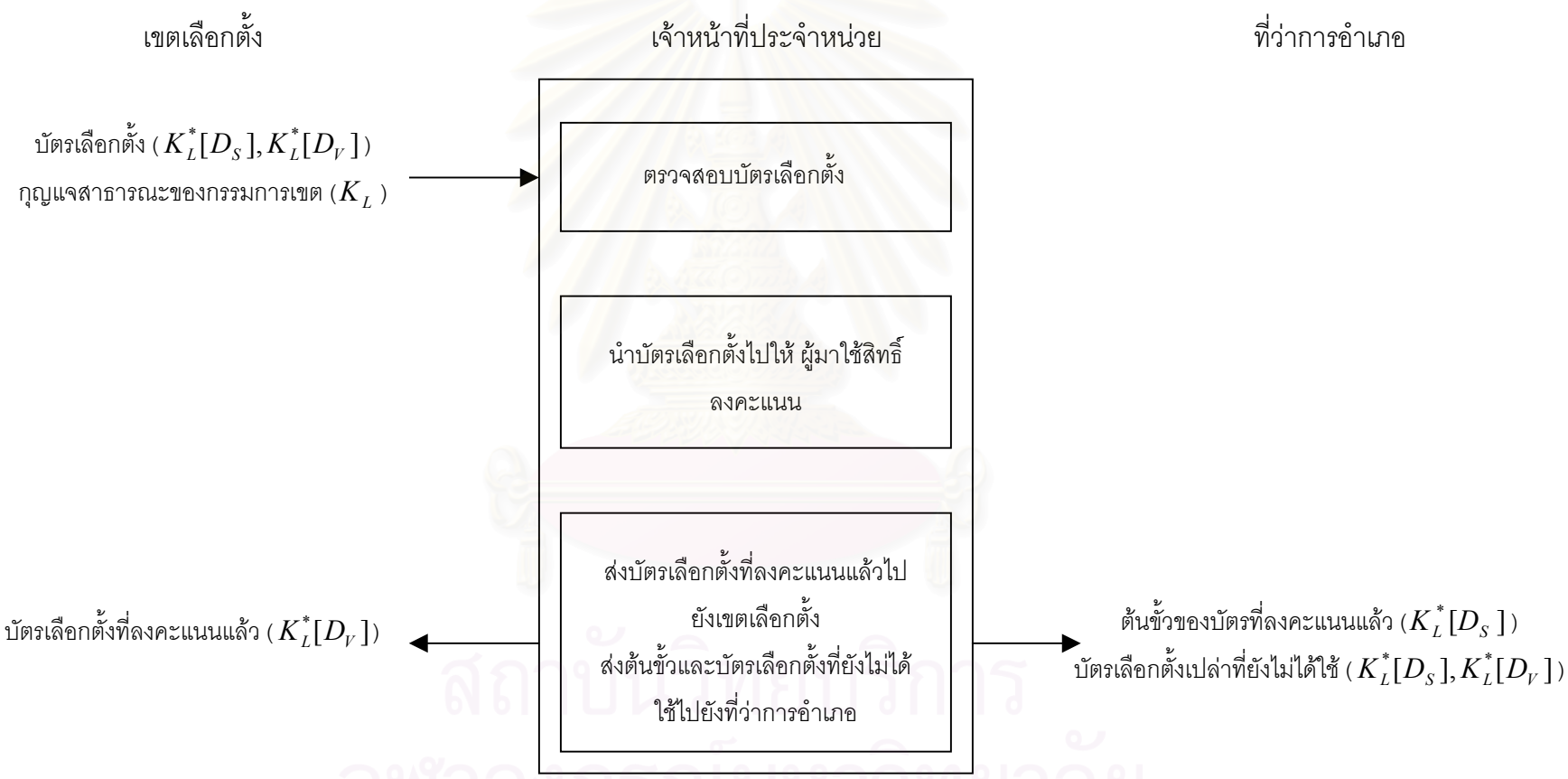
รูปที่ 4.2 แผนผังหน้าที่หลักของเจ้าหน้าที่ประจำหน่วยงานต่างๆ



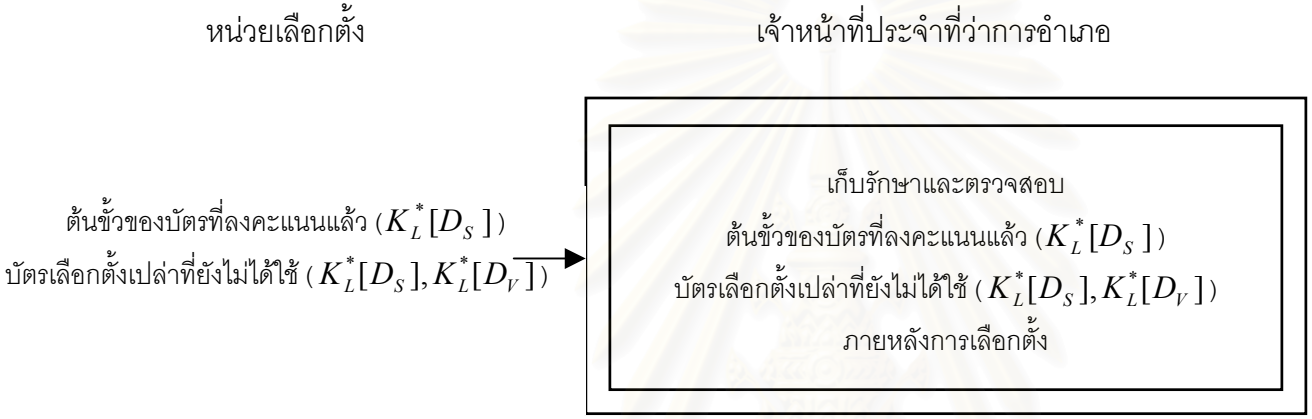
รูปที่ 4.3 แผนผังขั้นตอนการทำงานของกรรมการเลือกตั้ง



รูปที่ 4.4 แผนผังขั้นตอนการทำงานของกรรมการเขตและเจ้าหน้าที่ประจำเขต



รูปที่ 4.5 แผนผังขั้นตอนการทำงานของเจ้าหน้าที่ประจำหน่วย



รูปที่ 4.6 แผนผังขั้นตอนการทำงานของเจ้าหน้าที่ประจำที่ว่าการอำเภอ

4.2 รายละเอียดการพัฒนาโปรแกรมต่าง ๆ

ในหัวข้อนี้ จะกล่าวถึงรายละเอียดของโปรแกรมที่ได้พัฒนาขึ้นบนเครื่องไมโครคอมพิวเตอร์ เพื่อนำมาใช้ร่วมกับระบบการจัดพิมพ์และตรวจสอบบัตรเลือกตั้งที่ได้ออกแบบไว้

โปรแกรมหลักๆ ที่ได้พัฒนาขึ้นมีทั้งหมด 4 โปรแกรม ดังนี้

- *โปรแกรมสร้างกุญแจ*
- *โปรแกรมสร้างรหัสเฉพาะ*
- *โปรแกรมพิมพ์บัตรเลือกตั้ง*
- *โปรแกรมตรวจสอบบัตรเลือกตั้ง*

โปรแกรมต่างๆ ข้างต้นถูกพัฒนาขึ้นโดยใช้ Microsoft Visual C++ 6.0 ในการเขียนและแปลโปรแกรม โดยมีรายละเอียดของแต่ละโปรแกรมดังนี้

4.2.1 โปรแกรมสร้างกุญแจ

ใช้ในการสร้างกุญแจเพื่อเข้ารหัสลับและถอดรหัสลับ โดยโปรแกรมสร้างกุญแจถูกพัฒนาและปรับปรุงมาจากโปรแกรมสร้างกุญแจของ ศิริพงษ์ ประยูรหงษ์ [1] ซึ่งกุญแจส่วนตัวและกุญแจสาธารณะจะสามารถถูกบันทึกได้หลายรูปแบบ เช่น แฟ้มข้อมูลกุญแจ แฟ้มข้อมูลภาพรหัสแท่ง 2 มิติ และแฟ้มข้อมูลภาพรหัสแท่ง 1 มิติ ทำให้ผู้ถือกุญแจสามารถเลือกรูปแบบของกุญแจที่ถือได้หลายอย่างแล้วแต่ความสะดวก

4.2.2 โปรแกรมสร้างรหัสเฉพาะ

ใช้สร้างแฟ้มข้อมูลรหัสเฉพาะ เพื่อนำรหัสเฉพาะไปใช้ป้องกันกรรมการเขตทุจริต ก่อนที่จะสามารถสร้างแฟ้มข้อมูลรหัสเฉพาะได้ จะต้องสร้างกุญแจส่วนตัวของกรรมการเลือกตั้งและกุญแจส่วนตัวของโปรแกรม (K_C^*, K_P^*) ขึ้นมาก่อน เพื่อใช้ในการเข้ารหัสรหัสเฉพาะ ได้รหัสเฉพาะ 2 ชั้นออกมา $(U_2 = K_P^*[K_C^*[U]])$

4.2.3 โปรแกรมพิมพ์บัตรเลือกตั้ง

ใช้ในการพิมพ์รหัสลับลงบนบัตรเลือกตั้ง โดยจะดึงคุณลักษณะเฉพาะตัวของกระดาษบัตรเลือกตั้งแต่ละใบ (F) แล้วจึงนำข้อมูลคุณลักษณะเฉพาะตัวไปใช้เป็นส่วนหนึ่งของข้อมูลประจำบัตรเลือกตั้ง $(D = N; U_1; F; H_4)$ หลังจากนั้นจึงพิมพ์รหัสลับของข้อมูลประจำต้นขั้วและข้อมูล

ประจำบัตรลงคะแนนลงบนบัตรเลือกตั้ง ($K_L^*[D_S], K_L^*[D_V]$) ในรูปแบบรหัสแท่ง 2 มิติ เพื่อความสะดวกในการตรวจสอบ

สำหรับการพัฒนาโปรแกรมพิมพ์บัตรเลือกตั้งในงานวิจัยนี้ ได้ใช้สมมติฐานว่ามีอุปกรณ์รอบข้างครบถ้วนแล้วซึ่งได้แก่ กล้องประจำเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องพิมพ์ ซึ่งเชื่อมต่อกับไมโครคอมพิวเตอร์ รวมทั้งไดรเวอร์สำหรับอุปกรณ์รอบข้างเหล่านี้ เพื่อให้รับส่งข้อมูลกับโปรแกรมพิมพ์บัตรเลือกตั้งแบบเวลาจริง (Real time) แต่ในงานวิจัยนี้ใช้การรับส่งข้อมูลผ่านแฟ้มข้อมูลแทน โดยไม่มีอุปกรณ์รอบข้างจริง ดังนั้นการนำโปรแกรมพิมพ์บัตรเลือกตั้งไปใช้งานจริงนอกจากจะต้องมีความพร้อมของอุปกรณ์รอบข้างดังกล่าวแล้ว ยังต้องพัฒนาโปรแกรมพิมพ์บัตรเลือกตั้งเพิ่มเติม โดยเปลี่ยนรูปแบบการรับข้อมูลคุณลักษณะเฉพาะตัวของกระดาษจากแฟ้มข้อมูลไปเป็นการรับข้อมูลคุณลักษณะเฉพาะตัวของกระดาษในเวลาจริงจากกล้องประจำเครื่องคอมพิวเตอร์ส่วนบุคคลแทน

4.2.4 โปรแกรมตรวจสอบบัตรเลือกตั้ง

ใช้ในการตรวจสอบบัตรเลือกตั้ง ณ สถานที่นับคะแนนและที่ว่าการอำเภอ เนื่องจากบัตรเลือกตั้งแต่ละใบต้องผ่านการขนส่งไปยังหลายๆ แห่ง ทำให้บัตรเลือกตั้งอาจจะมีรอยสกปรกตรงบริเวณที่ใช้ดึงคุณลักษณะเฉพาะตัวของกระดาษได้จึงทำให้การตรวจคุณลักษณะเฉพาะตัวของกระดาษบัตรเลือกตั้งผิดพลาดได้ ในงานวิจัยนี้จึงได้แก้ปัญหาดังกล่าวโดยพัฒนาโปรแกรมตรวจสอบบัตรเลือกตั้งให้สามารถแสดงพิกัดคุณลักษณะเฉพาะตัวของกระดาษที่ได้จากการถอดรหัสลับออกทางหน้าจอไมโครคอมพิวเตอร์ ทำให้สามารถตรวจสอบบัตรเลือกตั้งที่มีบริเวณที่ใช้ดึงคุณลักษณะเฉพาะตัวของกระดาษสกปรกได้โดยใช้การมองเปรียบเทียบพิกัดคุณลักษณะเฉพาะตัวของกระดาษบนหน้าจอไมโครคอมพิวเตอร์กับพิกัดคุณลักษณะเฉพาะตัวของกระดาษบัตรเลือกตั้งจริง

4.3 กระบวนการจัดพิมพ์และตรวจสอบบัตรเลือกตั้งร่วมกับโปรแกรมที่พัฒนาขึ้น

ในหัวข้อนี้ จะกล่าวถึงขั้นตอนการทำงานร่วมกับโปรแกรมที่ได้พัฒนาขึ้นของกรรมการเลือกตั้ง กรรมการเขต เจ้าหน้าที่ประจำเขต เจ้าหน้าที่ประจำหน่วย และเจ้าหน้าที่ประจำที่ว่าการอำเภอ ดังที่ได้แสดงแผนผังไว้ในรูปที่ 4.3, 4.4, 4.5 และ 4.6 ซึ่งมีรายละเอียดขั้นตอนดังนี้

4.3.1 การสร้างกุญแจของกรรมการเลือกตั้งและกุญแจของโปรแกรม

กรรมการเลือกตั้งจะสร้างกุญแจของตนเองและกุญแจของโปรแกรม โดยใช้โปรแกรมสร้างกุญแจซึ่งมีลักษณะดังรูปที่ 4.7 ในงานวิจัยนี้ได้กำหนดให้ความยาวกุญแจของกรรมการเลือกตั้งมีขนาด 64 ไบต์ และความยาวกุญแจของโปรแกรม มีขนาด 64 ไบต์

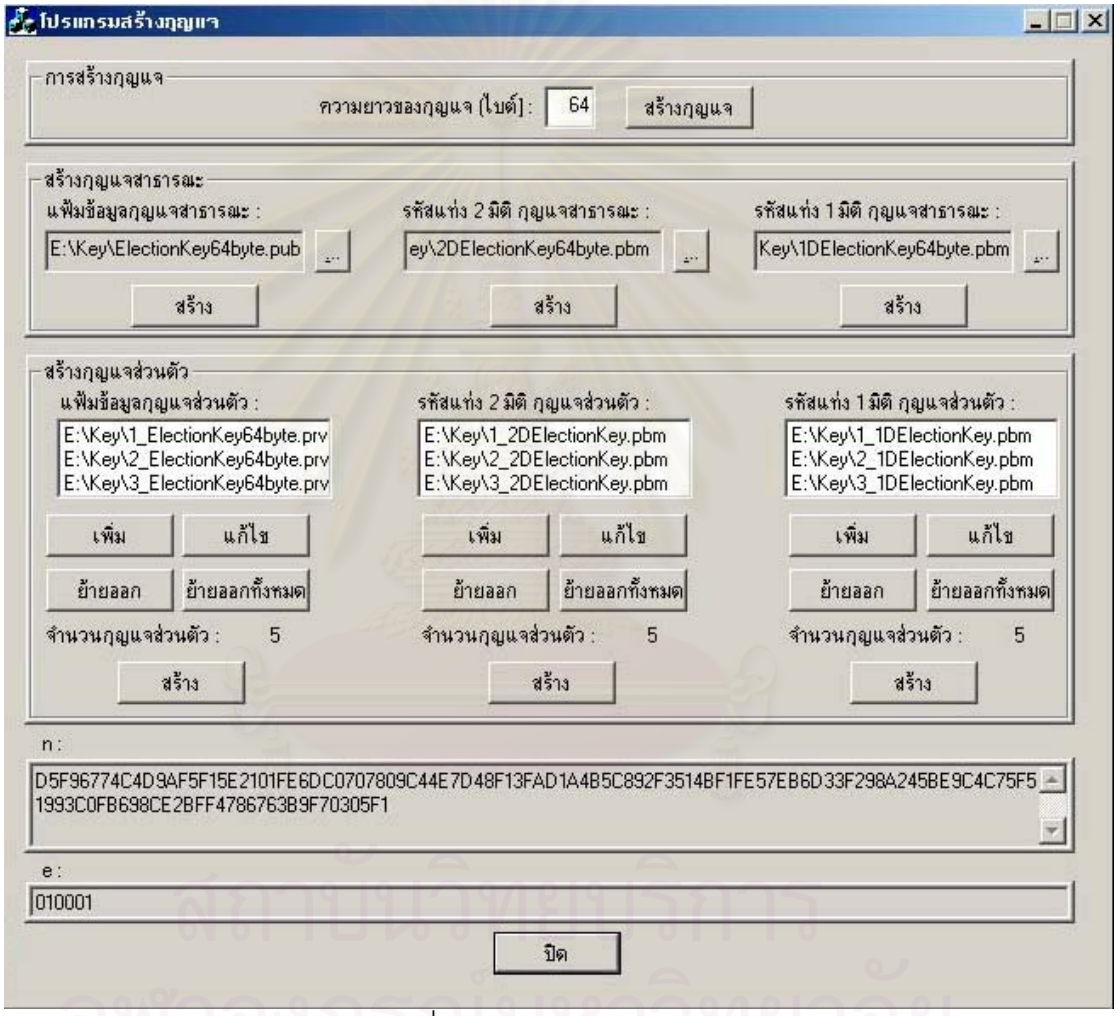
การสร้างกุญแจต้องใช้ทรัพยากร ดังต่อไปนี้

ฮาร์ดแวร์ : ไมโครคอมพิวเตอร์

ซอฟต์แวร์ : โปรแกรมสร้างกุญแจ

ผู้ปฏิบัติการ : กรรมการเลือกตั้งทั้ง 5 คน

ผลลัพธ์ที่ได้ : กุญแจของกรรมการเลือกตั้งและกุญแจของโปรแกรม (K_C^*, K_C, K_P^*, K_P)



รูปที่ 4.7 โปรแกรมสร้างกุญแจ

ขั้นตอนการสร้างกุญแจและบันทึกกุญแจ มีรายละเอียดดังนี้

4.3.1.1 **การสร้างกุญแจ**

การสร้างกุญแจจะใช้โปรแกรมบนเครื่องไมโครคอมพิวเตอร์โดยมีขั้นตอนดังนี้

- เรียกใช้ซอฟต์แวร์สำหรับการเข้ารหัสลับของ Peter Gutmann [21] เพื่อสร้างกุญแจ จะได้กุญแจมา 2 ตัว คือ กุญแจส่วนตัวและกุญแจสาธารณะ
- สุ่มค่าขึ้นมาค่าหนึ่งเพื่อใช้เป็นหมายเลขของกุญแจที่ได้สร้างขึ้น

กุญแจที่สร้างขึ้นจะประกอบไปด้วยส่วนต่าง ๆ ดังนี้

- *องค์ประกอบสาธารณะ*

- ค่า n (Modulus) - ความยาวของ n (หน่วยเป็นบิต)
- ค่า e - ความยาวของ e (หน่วยเป็นบิต)

- *องค์ประกอบส่วนตัว*

- ค่า d - ความยาวของ d (หน่วยเป็นบิต)
- ค่า p - ความยาวของ p (หน่วยเป็นบิต)
- ค่า q - ความยาวของ q (หน่วยเป็นบิต)
- ค่า u - ความยาวของ u (หน่วยเป็นบิต)
- ค่า e1 - ความยาวของ e1 (หน่วยเป็นบิต)
- ค่า e2 - ความยาวของ e2 (หน่วยเป็นบิต)

4.3.1.2 **การบันทึกแฟ้มข้อมูลกุญแจสาธารณะ**

กุญแจที่สร้างขึ้นสามารถบันทึกเป็นแฟ้มข้อมูลลงบนเครื่องไมโครคอมพิวเตอร์ได้ ถ้าบันทึกกุญแจสาธารณะในรูปแบบแฟ้มข้อมูลกุญแจสาธารณะจะมีนามสกุลเป็น pub แต่ถ้าบันทึกกุญแจสาธารณะในรูปแบบแฟ้มข้อมูลภาพรหัสแท่งจะมีนามสกุลเป็น pbm (Portable bit map) ซึ่งกุญแจสาธารณะมีรูปแบบของแฟ้มข้อมูลตามตารางที่ 4.1

ตารางที่ 4.1 รูปแบบแฟ้มข้อมูลกุญแจสาธารณะ

ส่วนประกอบ	ความยาว (ไบต์)
- หมายเลขกุญแจ	2
- ความยาวของ n (หน่วยเป็นบิต)	4
- ค่า n	ตามค่าที่เก็บไว้
- ความยาวของ e (หน่วยเป็นบิต)	4
- ค่า e	ตามค่าที่เก็บไว้

4.3.1.3 การบันทึกแฟ้มข้อมูลกุญแจส่วนตัว

กุญแจส่วนตัวสามารถบันทึกได้ในรูปแบบแฟ้มข้อมูลกุญแจส่วนตัวซึ่งจะมีนามสกุลเป็น prv แต่ถ้าบันทึกกุญแจส่วนตัวในรูปแบบแฟ้มข้อมูลภาพรหัสแท่งจะมีนามสกุลเป็น pbm ซึ่งกุญแจส่วนตัวจะมีลักษณะพิเศษคือ สามารถถูกแบ่งออกเป็นส่วนๆ ได้ตามความต้องการ โดยปกติแล้วจะแบ่งให้เท่ากับจำนวนคณะกรรมการที่มีอยู่ นอกจากนี้ กุญแจส่วนตัวยังต้องมีรหัสผ่าน เพื่อป้องกันไม่ให้ผู้อื่นนำเอากุญแจส่วนตัวไปใช้ได้ ก่อนการบันทึกข้อมูล จะต้องแบ่งกุญแจส่วนตัวเป็นส่วนๆ ตามขั้นตอนดังนี้

- นำองค์ประกอบส่วนตัวของกุญแจที่สร้างขึ้นมาเรียงต่อกัน แล้วแบ่งออกเป็นส่วน ๆ ตามจำนวนคณะกรรมการ
- เก็บค่าความยาวขององค์ประกอบส่วนตัวแต่ละส่วนที่ถูกแบ่งออกมา
- แทรก “CAST” ที่ส่วนหัวขององค์ประกอบส่วนตัวแต่ละส่วน เพื่อใช้เป็น header ในการตรวจสอบการถอดรหัสลับแบบกุญแจลับ
- เติมศูนย์ต่อท้ายองค์ประกอบส่วนตัวแต่ละส่วนเพื่อให้จำนวนไบต์ขององค์ประกอบส่วนตัวแต่ละส่วนหาร 8 ได้ลงตัว
- เข้ารหัสลับองค์ประกอบส่วนตัวแต่ละส่วนด้วยวิธี CAST ในโหมด CBC (Cipher block chaining) ซึ่งเป็นวิธีการเข้ารหัสลับแบบกุญแจลับ โดยกุญแจที่ใช้คำนวณมาจากรหัสผ่านของกรรมการแต่ละท่าน
- อ่านค่าเวกเตอร์เริ่มต้น (Initialization vector) ที่ใช้ในการเข้ารหัสลับ

หลังจากนั้นจึงบันทึกข้อมูลลงแฟ้ม โดยรูปแบบแฟ้มข้อมูลของกุญแจส่วนตัวแต่ละส่วนเป็นไปตามตารางที่ 4.2

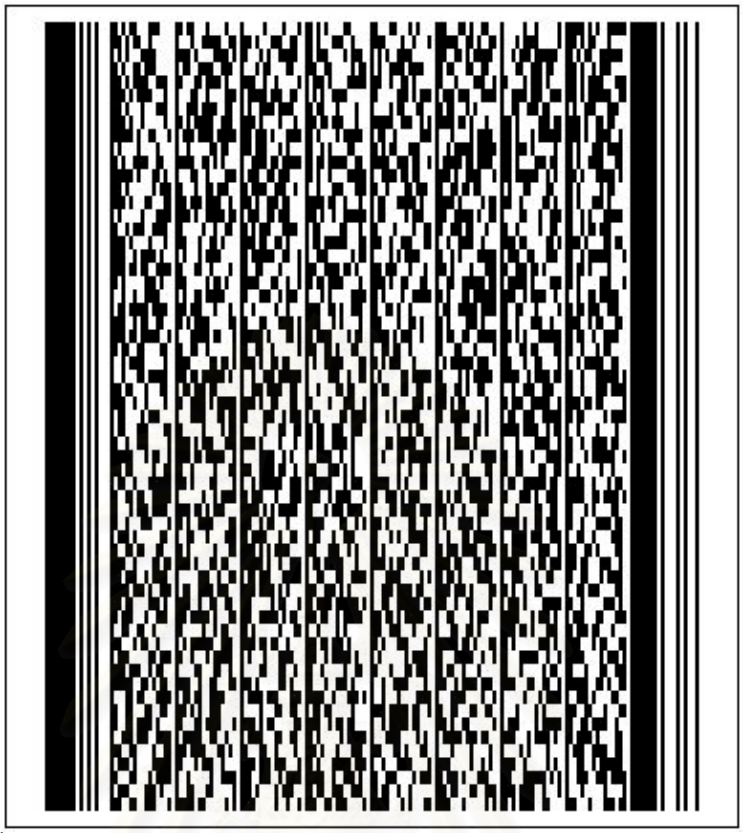
ตารางที่ 4.2 รูปแบบแฟ้มข้อมูลกุญแจส่วนตัวแต่ละส่วน

ส่วนประกอบ	ความยาว (ไบต์)
- หมายเลขกุญแจ	2
- ความยาวของ n (หน่วยเป็นบิต)	4
- ค่า n	ตามค่าที่เก็บไว้
- ความยาวของ e (หน่วยเป็นบิต)	4
- ค่า e	ตามค่าที่เก็บไว้
- หมายเลขส่วน (ส่วนที่เท่าไร)	1
- จำนวนส่วนทั้งหมด	1
- เวกเตอร์เริ่มต้น (Initialization vector)	8
- ความยาวขององค์ประกอบส่วนตัวก่อนเข้ารหัสลับ (หน่วยเป็นไบต์)	2
- องค์ประกอบส่วนตัวที่เข้ารหัสลับแล้ว	ตามค่าที่เก็บไว้

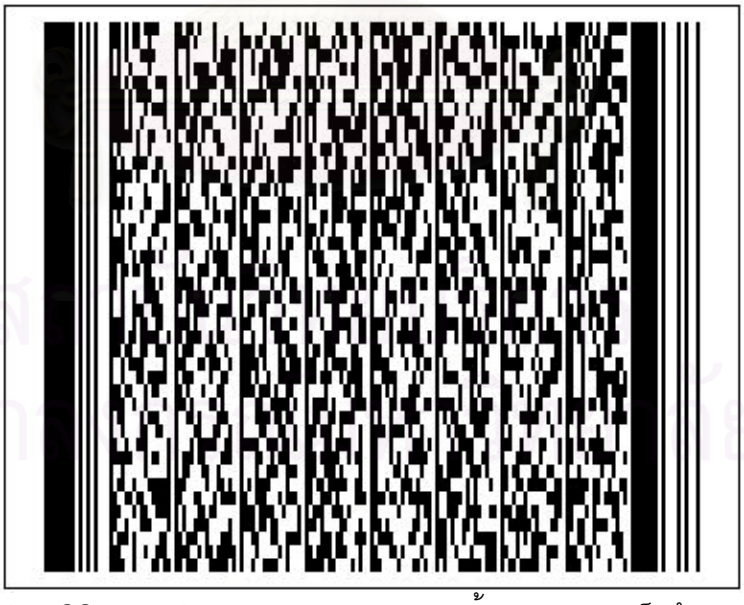
จะเห็นว่ากุญแจส่วนตัวจะมีองค์ประกอบสาธารณะรวมอยู่ด้วย จึงสามารถนำกุญแจส่วนตัวมาใช้ในการถอดรหัสลับได้

เมื่อสร้างกุญแจของกรรมการเลือกตั้งและกุญแจของโปรแกรมเสร็จก็จะนำกุญแจที่ได้ไปใช้ในการเข้ารหัสและถอดรหัสต่อไป

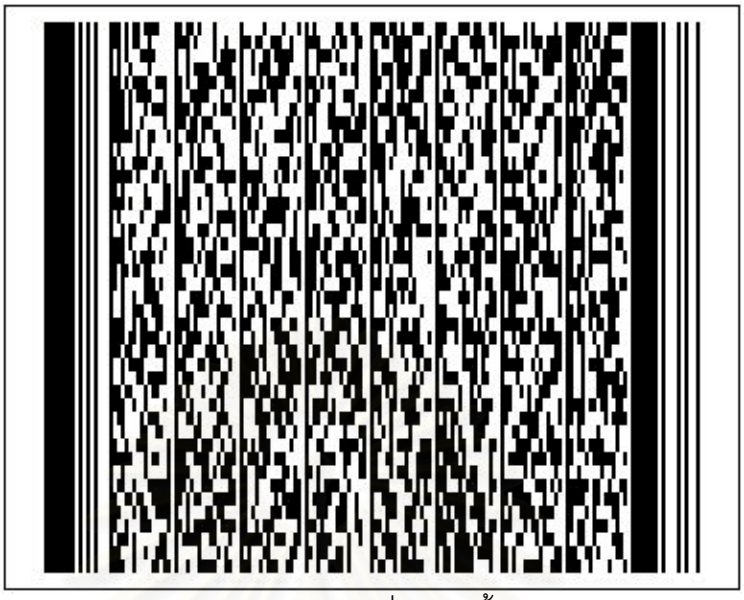
ตัวอย่างของกุญแจขนาด 64 ไบต์ ที่บันทึกในรูปแบบแฟ้มข้อมูลภาพกุญแจส่วนตัวและแฟ้มข้อมูลภาพกุญแจสาธารณะ แสดงได้ดังรูปที่ 4.8, 4.9, 4.10 และ 4.11



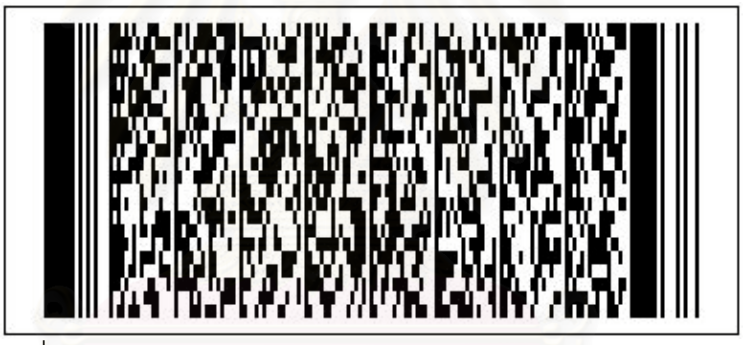
รูปที่ 4.8 รหัสแท่ง 2 มิติกุญแจส่วนตัวของบุคคลเดียว เก็บข้อมูล 340 ไบต์



รูปที่ 4.9 รหัสแท่ง 2 มิติกุญแจส่วนตัวของบุคคลแรกจากทั้งหมด 5 คน เก็บข้อมูลขนาด 139 ไบต์



รูปที่ 4.10 รหัสแท่ง 2 มิติกุญแจส่วนตัวของบุคคลที่ 2 จากทั้งหมด 5 คน เก็บข้อมูลขนาด 139 ไบต์



รูปที่ 4.11 รหัสแท่ง 2 มิติกุญแจสาธารณะเก็บข้อมูลขนาด 74 ไบต์

4.3.2 การฝังกุญแจสาธารณะของโปรแกรมไว้ในโปรแกรม

กรรมการเลือกตั้งจะเก็บกุญแจสาธารณะของโปรแกรม (K_P) ไว้เป็นความลับและจะฝังกุญแจสาธารณะของโปรแกรม (K_P) ไว้ในโปรแกรมพิมพ์บัตรเลือกตั้งและโปรแกรมตรวจสอบบัตรเลือกตั้ง สำหรับสาเหตุที่ต้องฝังกุญแจสาธารณะของโปรแกรม (K_P) ไว้ในโปรแกรมพิมพ์บัตรเลือกตั้งก็เพื่อที่จะใช้ในการเข้ารหัสค่าแฮชและรหัสเฉพาะ ($K_P[H_{4S};U_{1S}], K_P[H_{4V};U_{1V}]$) ที่จะบันทึกลงแฟ้มข้อมูลรายงานการจัดพิมพ์ นอกจากนี้ยังใช้กุญแจสาธารณะของโปรแกรม (K_P) ในการถอดรหัสข้อมูลที่อยู่ภายในแฟ้มข้อมูลรหัสเฉพาะ ($K_P[U_2] = K_P[K_P^*[K_C^*[U]]] = U_1$) เพื่อนำรหัสเฉพาะ 1 ชั้น (U_1) ไปใช้เป็นส่วนหนึ่งของข้อมูลประจำบัตรเลือกตั้ง ($D = N;U_1;F;H_4$)

การฝังกุญแจสาธารณะไว้ในโปรแกรมจะต้องใช้แฟ้มข้อมูลและทรัพยากร ดังต่อไปนี้

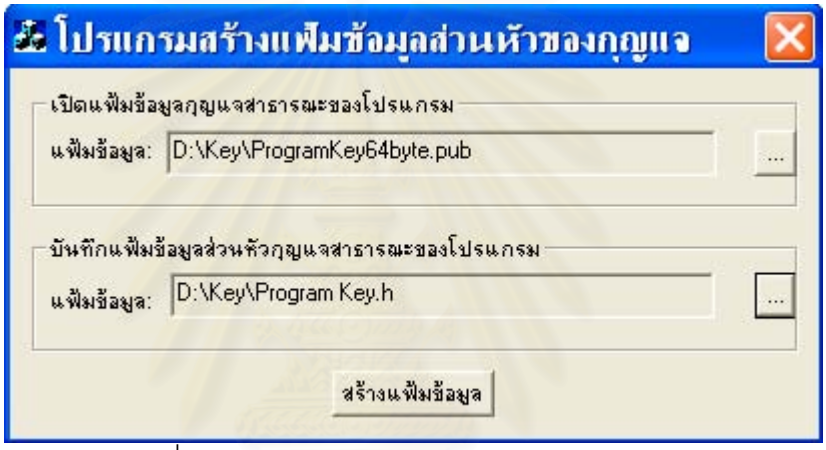
แฟ้มข้อมูล :กุญแจสาธารณะของโปรแกรม (K_P) และซอร์สโคด (Source Code) ของโปรแกรมพิมพ์บัตรเลือกตั้งและโปรแกรมตรวจสอบบัตรเลือกตั้ง

ฮาร์ดแวร์ :ไมโครคอมพิวเตอร์

ซอฟต์แวร์ :ตัวแปลโปรแกรม (Compiler) และโปรแกรมสร้างแฟ้มข้อมูลส่วนหัวกุญแจ (มีลักษณะดังรูปที่ 4.12)

ผู้ปฏิบัติการ :กรรมการเลือกตั้ง

ผลลัพธ์ที่ได้ :โปรแกรมพิมพ์บัตรเลือกตั้งและโปรแกรมตรวจสอบบัตรเลือกตั้งที่ถูกฝังกุญแจสาธารณะของโปรแกรม (K_P)



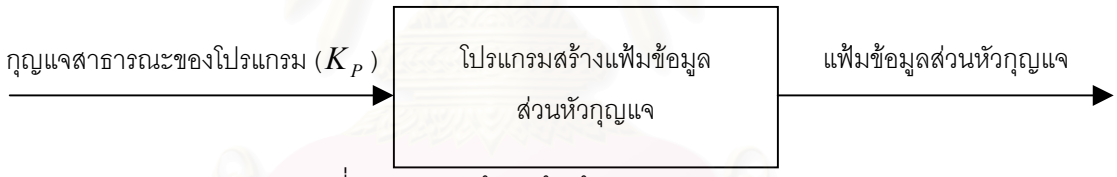
รูปที่ 4.12 โปรแกรมสร้างแฟ้มข้อมูลส่วนหัวกุญแจ

กรรมการเลือกตั้งจะฝังกุญแจสาธารณะของโปรแกรม (K_P) ไว้ในโปรแกรมพิมพ์บัตรเลือกตั้งและโปรแกรมตรวจสอบบัตรเลือกตั้ง โดยมีขั้นตอนดังนี้

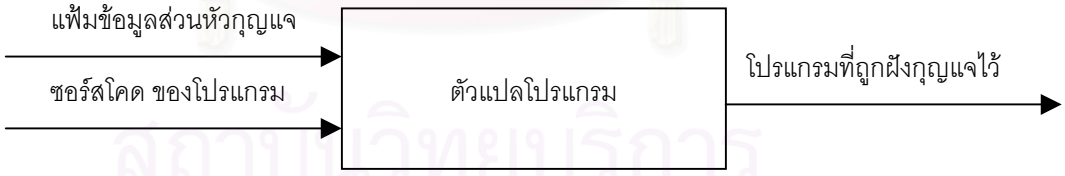
- ป้อนแฟ้มข้อมูลกุญแจสาธารณะของโปรแกรม (K_P) เข้าโปรแกรมสร้างแฟ้มข้อมูลส่วนหัวกุญแจและเลือกสารบบ (Directory) ที่จะบันทึกแฟ้มข้อมูล
- สั่งให้โปรแกรมสร้างแฟ้มข้อมูลส่วนหัวกุญแจออกมา
- โปรแกรมจะสร้างแฟ้มข้อมูลส่วนหัวกุญแจออกมา โดยแฟ้มข้อมูลที่สร้างออกมาจะมีนามสกุล h และภายในแฟ้มข้อมูลส่วนหัวกุญแจจะประกอบด้วยข้อมูลกุญแจสาธารณะดังตารางที่ 4.1 ซึ่งประกอบด้วย
  - หมายเลขกุญแจ
  - ค่า n
  - ความยาวของ n (บิต)

- ค่า e
- ความยาวของ e (บิต)

- นำแฟ้มข้อมูลส่วนหัวกุญแจที่ได้มาไว้ที่สารบบเดียวกับซอร์สโคดของโปรแกรมที่ต้องการฝังกุญแจ
- รวมแฟ้มข้อมูลส่วนหัวกุญแจไว้ในซอร์สโคดของโปรแกรม โดยจะประกาศการรวมแฟ้มข้อมูลไว้ที่เฮดเดอร์ (Header) ของซอร์สโคด ถ้าให้แฟ้มข้อมูลส่วนหัวกุญแจมีชื่อว่า Program Public Key.h ก็จะรวม โดยใช้คำสั่ง #include "Program Public Key.h"
- กรรมการเลือกตั้งจะสั่งตัวแปลโปรแกรมซึ่งในงานวิจัยนี้ใช้ Microsoft Visual C++ 6.0 ให้แปลโปรแกรมและสร้างโปรแกรมที่ถูกฝังกุญแจสาธารณะของโปรแกรมออกมา
- จัดเก็บโปรแกรมพิมพ์บัตรเลือกตั้งและโปรแกรมตรวจสอบบัตรเลือกตั้งที่ถูกฝังกุญแจสาธารณะของโปรแกรม (K_P) ไว้ในคอมแพคดิสก์ (Compact Disk) เพื่อเตรียมที่จะส่งโปรแกรมไปยังเขตเลือกตั้ง



รูปที่ 4.13 การสร้างแฟ้มข้อมูลส่วนหัวกุญแจ



รูปที่ 4.14 การฝังกุญแจสาธารณะของโปรแกรม

4.3.3 การสร้างแฟ้มข้อมูลรหัสเฉพาะ

กรรมการเลือกตั้งจะสร้างแฟ้มข้อมูลรหัสเฉพาะ (U_2) ขึ้นมาเพื่อป้องกันการทุจริตจากกรรมการเขตดังที่ได้กล่าวรายละเอียดไว้แล้วในหัวข้อที่ 3.7

การสร้างแฟ้มข้อมูลรหัสเฉพาะ (U_2) จะต้องใช้แฟ้มข้อมูลและทรัพยากร ดังต่อไปนี้

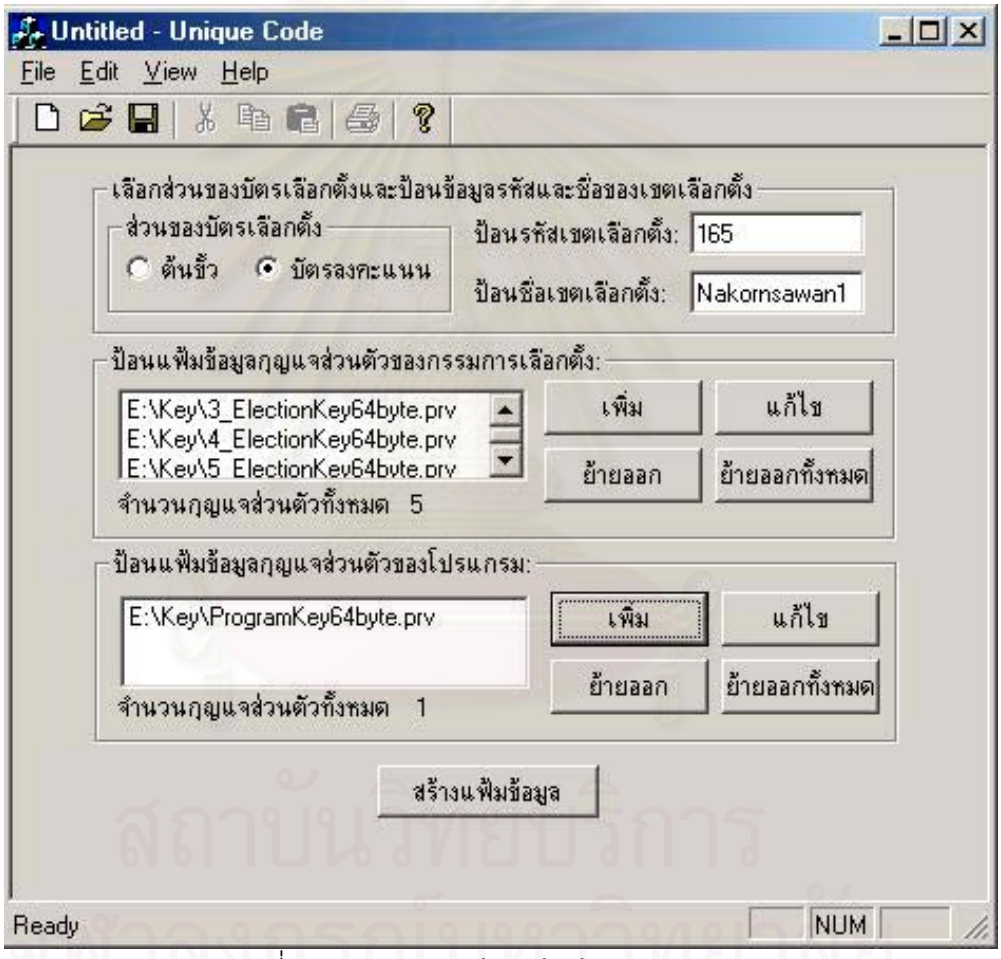
แฟ้มข้อมูล :กุญแจส่วนตัวของกรรมการเลือกตั้งและกุญแจส่วนตัวของโปรแกรม (K_C^*, K_P^*)

ฮาร์ดแวร์ :ไมโครคอมพิวเตอร์

ซอฟต์แวร์ :โปรแกรมสร้างแฟ้มข้อมูลรหัสเฉพาะ (ดูได้ดังรูปที่ 4.15)

ผู้ปฏิบัติการ :กรรมการเลือกตั้ง ทั้ง 5 คนพร้อมกัน

ผลลัพธ์ที่ได้ :แฟ้มข้อมูลรหัสเฉพาะ (U_2)



รูปที่ 4.15 โปรแกรมสร้างแฟ้มข้อมูลรหัสเฉพาะ

กรรมการเลือกตั้งจะป้อนข้อมูลและสั่งให้โปรแกรมทำงาน โดยมีขั้นตอนดังนี้

- ป้อนข้อมูลรหัสเขตเลือกตั้งและชื่อเขตเลือกตั้ง
- เลือกชนิดแฟ้มข้อมูลรหัสเฉพาะที่จะสร้าง ซึ่งมีอยู่ 2 ชนิด คือ
  - แฟ้มข้อมูลรหัสเฉพาะของต้นขั้ว
  - แฟ้มข้อมูลรหัสเฉพาะของบัตรลงคะแนน

- ป้อนกุญแจส่วนตัวของกรรมการเลือกตั้งและกุญแจส่วนตัวของโปรแกรม (K_C^*, K_P^*) เพื่อใช้กุญแจในการเข้ารหัส รหัสเฉพาะ $(K_P^*[K_C^*[U]])$
- สั่งโปรแกรมให้สร้างแฟ้มข้อมูลรหัสเฉพาะ
- เลือกสารบบที่จะเก็บแฟ้มข้อมูลรหัสเฉพาะ

โปรแกรมจะสร้างแฟ้มข้อมูลรหัสเฉพาะ โดยมีขั้นตอนดังนี้

- กำหนดรหัสชนิดให้รหัสเฉพาะ โดย
  - รหัสเฉพาะของต้นขั้วจะมีรหัสชนิด 01
  - รหัสเฉพาะของบัตรลงคะแนนจะมีรหัสชนิด 02
- สร้างหมายเลขประจำรหัสเฉพาะขึ้นมา 400,000 หมายเลข เพื่อต้องการให้รหัสเฉพาะ แต่ละรหัสมีหมายเลขประจำอยู่และหมายเลขเลขประจำรหัสเฉพาะของบัตรแต่ละใบจะไม่ซ้ำกัน โดย
  - รหัสเฉพาะของต้นขั้วจะมีหมายเลขประจำเรียงกันตั้งแต่ 1-400,000
  - รหัสเฉพาะของบัตรลงคะแนนจะมีหมายเลขประจำไม่เรียงกัน แต่มีค่าอยู่ระหว่าง 1-400,000

  สำหรับสาเหตุที่หมายเลขประจำรหัสเฉพาะของบัตรลงคะแนนไม่เรียงกันเนื่องจากบัตรลงคะแนนมีผลการลงคะแนนอยู่และผลการลงคะแนนของผู้มาใช้สิทธิ์เลือกตั้งจะต้องเป็นความลับ
- รวมรหัสชนิด รหัสเขตเลือกตั้งและหมายเลขประจำรหัสเฉพาะเป็นข้อมูลรหัสเฉพาะ
- เข้ารหัส รหัสเฉพาะ 2 ครั้ง ด้วยกุญแจส่วนตัวของกรรมการเลือกตั้งและกุญแจส่วนตัวของโปรแกรม $(U_2 = K_P^*[K_C^*[U]])$
- บันทึกรหัสเฉพาะที่ถูกเข้ารหัสลงในแฟ้มข้อมูลรหัสเฉพาะ

หลังจากที่ได้แฟ้มข้อมูลรหัสเฉพาะแล้วก็จะเก็บบันทึกไว้ในคอมแพคดิสก์ เพื่อเตรียมที่จะส่งไปให้ทางเขตเลือกตั้ง โดยเจ้าหน้าที่ประจำเขตจะนำรหัสเฉพาะที่ถูกเข้ารหัสโดยกุญแจส่วนตัวของกรรมการเลือกตั้ง $(U_1 = K_C^*[U])$ ไปใช้เป็นข้อมูลส่วนหนึ่งของบัตรเลือกตั้ง

รูปที่ 4.16 การสร้างแฟ้มข้อมูลรหัสเฉพาะ

สำหรับข้อมูลภายในแฟ้มข้อมูลรหัสเฉพาะ แสดงได้ดังรูปที่ 4.17

รูปที่ 4.17 ข้อมูลรหัสเฉพาะที่ถูกเข้ารหัสภายในแฟ้มข้อมูลรหัสเฉพาะ

4.3.4 กรรมการเลือกตั้งจัดส่งแฟ้มข้อมูลและโปรแกรมไปให้กรรมการเขต

กรรมการเขตจะได้รับโปรแกรมสร้างกุญแจ โปรแกรมพิมพ์บัตรเลือกตั้ง โปรแกรมตรวจสอบบัตรเลือกตั้งและแฟ้มข้อมูลรหัสเฉพาะ โดยกรรมการเขตจะนำแฟ้มข้อมูลและโปรแกรมไปใช้ในการจัดพิมพ์และตรวจสอบบัตรเลือกตั้ง

4.3.5 การสร้างกุญแจของกรรมการเขต

ก่อนที่กรรมการเขตจะสามารถจัดพิมพ์บัตรเลือกตั้งได้จะต้องสร้างกุญแจของตนเองขึ้นมา เพื่อใช้กุญแจในการเข้ารหัสข้อมูลประจำบัตรเลือกตั้ง ($K_L^*[D]$) โดยจะสร้างกุญแจด้วยโปรแกรมสร้างกุญแจที่กรรมการเลือกตั้งส่งมาให้ ซึ่งขั้นตอนนี้จะต้องใช้ทรัพยากรดังนี้

ฮาร์ดแวร์ : ไมโครคอมพิวเตอร์

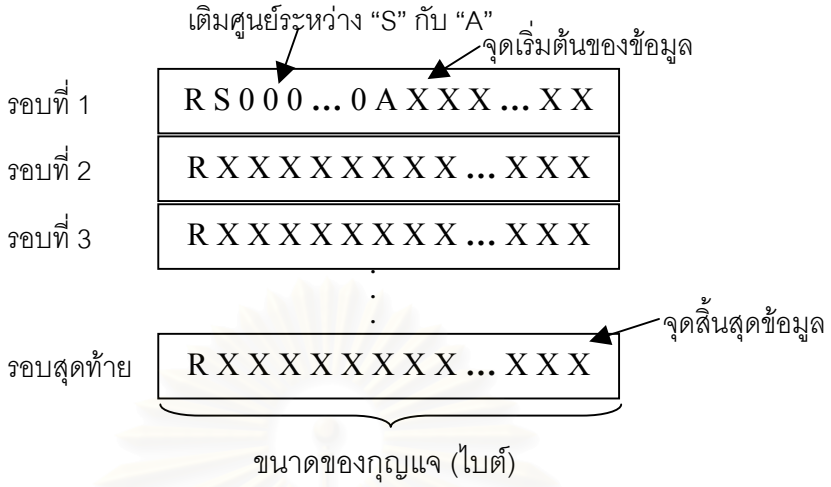
ซอฟต์แวร์ : โปรแกรมสร้างกุญแจ (ดังรูปที่ 4.7)

ผู้ปฏิบัติการ : กรรมการเขต

ผลลัพธ์ที่ได้ : กุญแจส่วนตัวและกุญแจสาธารณะของกรรมการเขต (K_L^*, K_L)

กรรมการเขตจะป้อนข้อมูลและสั่งให้โปรแกรมทำงาน โดยมีขั้นตอนดังนี้

- เลือกความยาวของกุญแจ ในงานวิจัยนี้กำหนดให้กุญแจของกรรมการเขตมีความยาว 68 ไบต์ เนื่องมาจากรูปแบบการจัดข้อมูลก่อนเข้ารหัส (ดังรูปที่ 4.18) ซึ่งมีรายละเอียดการจัดรูปแบบข้อมูลดังนี้
  - นำข้อมูลที่จะเข้ารหัสแทรก “R” ทางด้านหน้าของข้อมูลในแต่ละรอบ เพื่อให้แน่ใจว่าข้อมูลที่จะเข้ารหัสมีค่าไม่เกิน n (modulus) ทำให้ข้อมูลประจำบัตรเลือกตั้งที่จะเข้ารหัสในแต่ละรอบมีความยาวเท่ากับขนาดความยาวของกุญแจลบด้วย 1 (ไบต์) ยกเว้นรอบแรก
  - ในรอบแรก แทรก “S” ต่อจาก “R” เพื่อใช้เป็น header ในการตรวจสอบการถอดรหัสลับ
  - แทรก “A” หน้าจุดเริ่มต้นของข้อมูล เพื่อใช้เป็นตัวบอกจุดเริ่มต้นของข้อมูล
  - เติมศูนย์ระหว่าง “S” กับ “A” ให้ได้ความยาวของข้อมูลทั้งหมดเป็นจำนวนเท่าของ ขนาดความยาวของกุญแจ (ไบต์)



รูปที่ 4.18 การจัดรูปแบบข้อมูลก่อนการเข้ารหัสลับ

จากที่ได้กล่าวไว้ในหัวข้อ 3.12.2 ข้อมูลประจำบัตรเลือกตั้ง (D) จะมีความยาวไม่เกิน 128 ไบต์ และมีรูปแบบการจัดข้อมูลก่อนการเข้ารหัสเป็นดังรูป 4.18 ถ้าใช้กุญแจที่มีความยาว 64 ไบต์ ในการเข้ารหัสจะต้องเข้ารหัสถึง 3 รอบ และได้ข้อมูลที่ถูกเข้ารหัสแล้ว ($K_L^*[D]$) มีขนาด 192 ไบต์ แต่ถ้าใช้กุญแจที่มีความยาว 68 ไบต์ในการเข้ารหัสจะต้องเข้ารหัสเพียงแค่ 2 รอบ และได้ข้อมูลที่ถูกเข้ารหัสแล้ว ($K_L^*[D]$) มีขนาด 136 ไบต์ ซึ่งจะทำให้รหัสแท่ง 2 มิติ ที่จะพิมพ์มีขนาดไม่ใหญ่มากนัก ถ้ารหัสแท่ง 2 มิติ มีขนาดใหญ่ก็จะทำให้ต้นขั้วมีขนาดใหญ่ตามไปด้วย ซึ่งจะทำให้เสียพื้นที่ของช่องลงคะแนนเลือกตั้งไป

- หลังจากเลือกความยาวของกุญแจเสร็จก็จะเลือกชนิดแฟ้มข้อมูลของกุญแจที่ต้องการจะบันทึก และเลือกสารบบที่จะบันทึกแฟ้มข้อมูล
- สั่งโปรแกรมให้สร้างแฟ้มข้อมูลมูลกุญแจ

โปรแกรมจะสร้างกุญแจและบันทึกกุญแจ โดยมีขั้นตอนดังนี้

- สร้างกุญแจส่วนตัวและกุญแจสาธารณะของกรรมการเขต (K_L^*, K_L)
- บันทึกข้อมูลกุญแจส่วนตัวและกุญแจสาธารณะในรูปแบบที่กรรมการเขตเลือก

หลังจากสร้างกุญแจของกรรมการเขตเสร็จ กุญแจส่วนตัวของกรรมการเขต (K_L^*) จะถูกนำไปใช้ในการเข้ารหัสลับข้อมูลประจำบัตรลงคะแนน ($K_L^*[D_V]$) และข้อมูลประจำต้นขั้ว ($K_L^*[D_S]]$) ในขั้นตอนการจัดพิมพ์บัตรเลือกตั้งต่อไป

4.3.6 การจัดพิมพ์บัตรเลือกตั้ง

เมื่อกรรมการเขตสร้างกุญแจของตนเองเสร็จ ก็จะจัดพิมพ์บัตรเลือกตั้ง โดยใช้โปรแกรมพิมพ์บัตรเลือกตั้ง ซึ่งมีลักษณะดังรูปที่ 4.19 สำหรับขั้นตอนการพิมพ์รหัสลับลงบนบัตรเลือกตั้งจะต้องใช้แฟ้มข้อมูลและทรัพยากรดังนี้

วัตถุ :กระดาษบัตรเลือกตั้ง (F_S, F_V)

แฟ้มข้อมูล :แฟ้มข้อมูลรหัสเฉพาะของต้นขั้ว (U_{2S}) แฟ้มข้อมูลรหัสเฉพาะของบัตรลงคะแนน (U_{2V}) และกุญแจส่วนตัวของกรรมการเขต (K_L^*)

ฮาร์ดแวร์ :ไมโครคอมพิวเตอร์ กล้องประจำเครื่องคอมพิวเตอร์ส่วนบุคคล และเครื่องพิมพ์

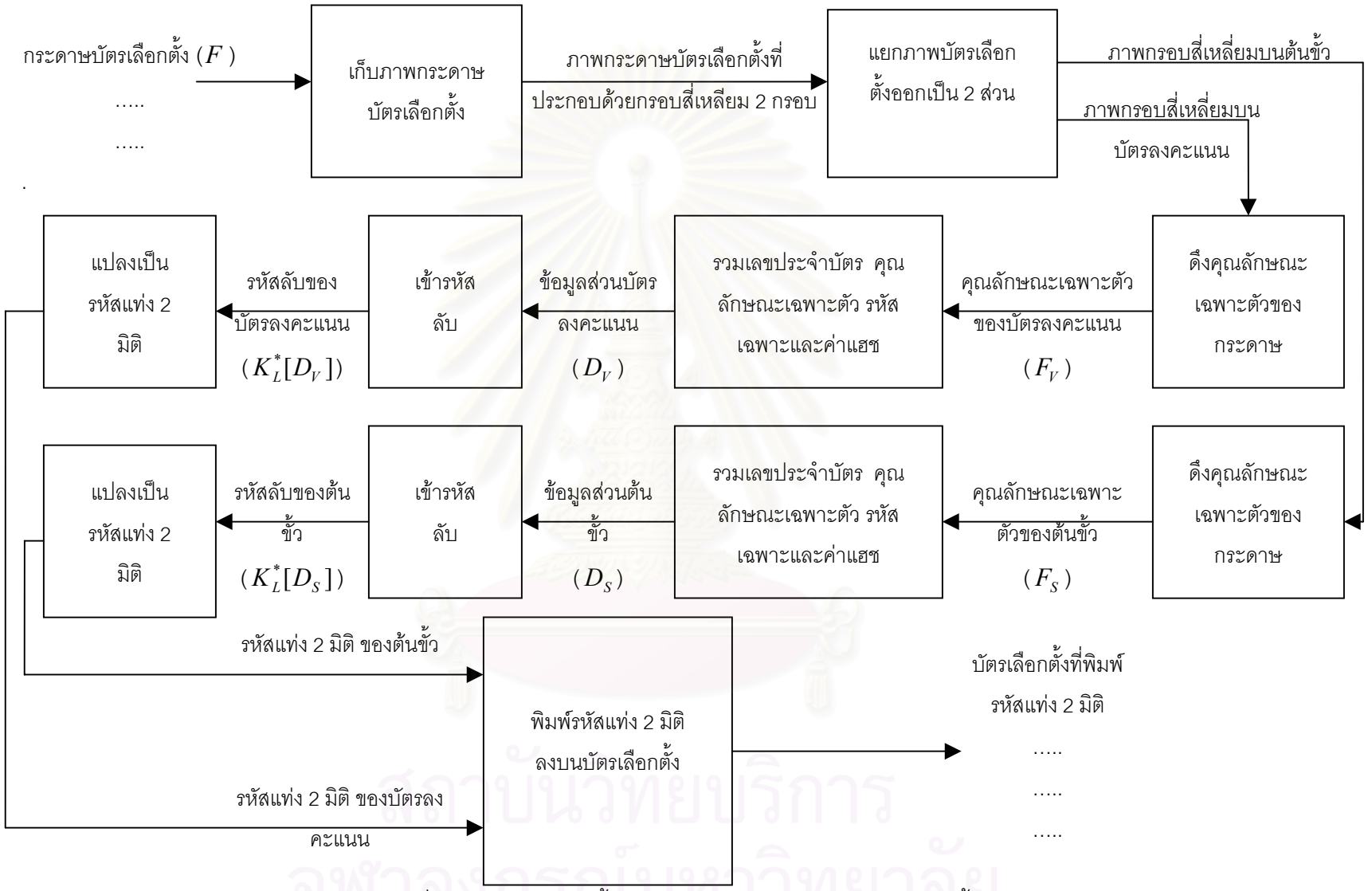
ซอฟต์แวร์ :โปรแกรมพิมพ์บัตรเลือกตั้ง (ดูได้ดังรูปที่ 4.19)

ผู้ปฏิบัติการ :กรรมการเขตและเจ้าหน้าที่ประจำเขต

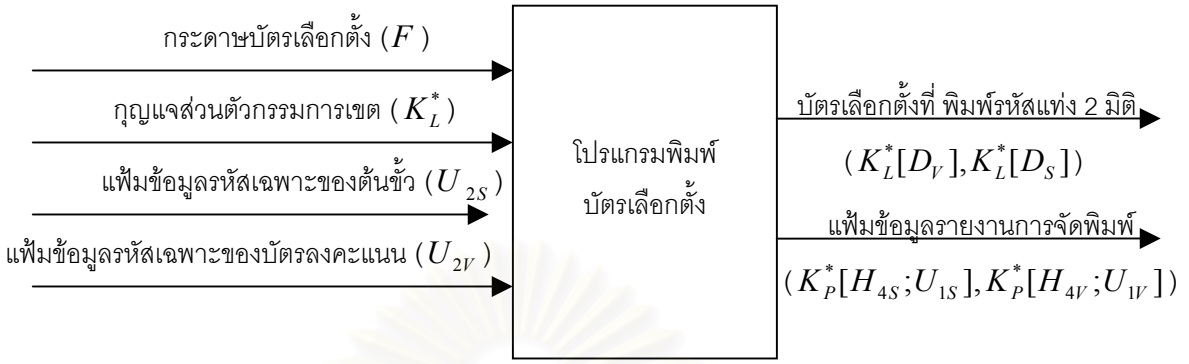
ผลลัพธ์ที่ได้ :บัตรเลือกตั้งที่ถูกพิมพ์รหัสลับ ($K_L^*[D_S], K_L^*[D_V]$) ในรูปแบบรหัสแท่ง 2 มิติ ลงบนต้นขั้ว และบัตรลงคะแนน

รูปที่ 4.19 โปรแกรมพิมพ์บัตรเลือกตั้ง

รายละเอียดขั้นตอนการพิมพ์บัตรเลือกตั้งและผลที่ได้จากโปรแกรมพิมพ์บัตรเลือกตั้งแสดงได้ดังรูปที่ 4.20 และ 4.21



รูปที่ 4.20 รายละเอียดขั้นตอนการพิมพ์รหัสลับลงบนบัตรเลือกตั้ง

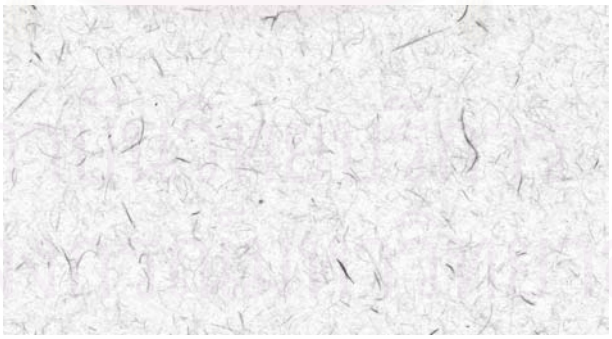


รูปที่ 4.21 ผลลัพธ์ที่ได้จากโปรแกรมพิมพ์บัตรเลือกตั้ง

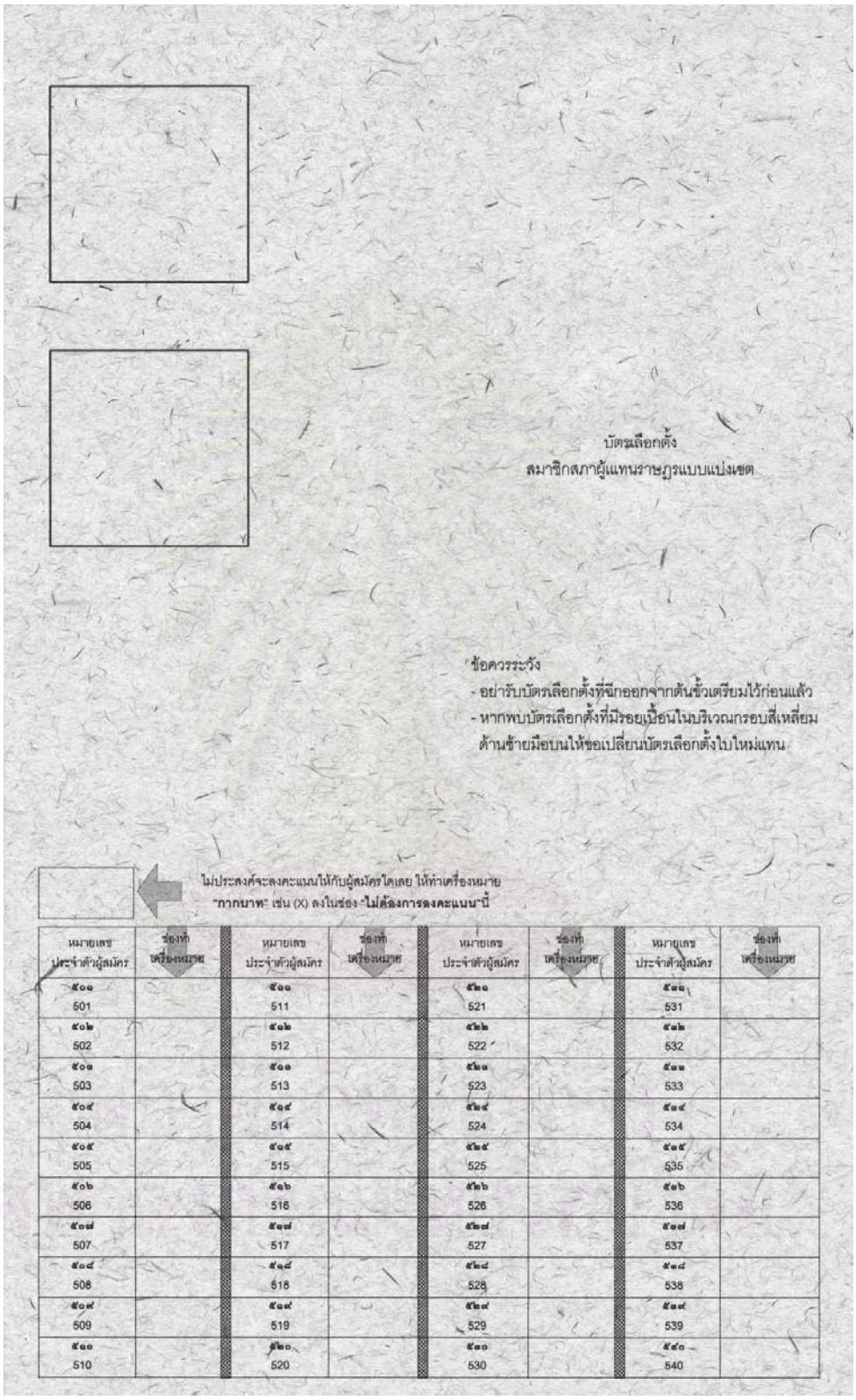
สำหรับรายละเอียดขั้นตอนการพิมพ์บัตรเลือกตั้งตามรูปที่ 4.20 มีรายละเอียดดังนี้

4.3.6.1 การเก็บภาพบัตรเลือกตั้ง

ใช้กล้องประจำเครื่องคอมพิวเตอร์ส่วนบุคคลเก็บภาพกระดาษบัตรเลือกตั้ง เพื่อนำภาพกระดาษบัตรเลือกตั้งไปดึงคุณลักษณะเฉพาะตัวของกระดาษและนำข้อมูลคุณลักษณะเฉพาะตัวของกระดาษ (F) ไปใช้เป็นส่วนหนึ่งของข้อมูลประจำบัตรเลือกตั้ง (D) สำหรับกระดาษที่ใช้พิมพ์บัตรเลือกตั้งจะมีวัตถุลักษณะเป็นเส้นฝังอยู่ดังรูปที่ 4.22 ซึ่งกระดาษบัตรเลือกตั้งจะมีกรอบสี่เหลี่ยมอยู่ทั้งในส่วนของต้นขั้วและบัตรลงคะแนนดังรูปที่ 4.23 เพื่อใช้เป็นพื้นที่สำหรับดึงข้อมูลคุณลักษณะเฉพาะตัวจากกระดาษ (F_S, F_V) ซึ่งบริเวณที่จะเก็บภาพของบัตรเลือกตั้งก็คือบริเวณกรอบสี่เหลี่ยมที่อยู่บนต้นขั้วและบัตรลงคะแนนดังรูปที่ 4.24



รูปที่ 4.22 ตัวอย่างกระดาษที่ใช้พิมพ์บัตรเลือกตั้ง



บัตรเลือกตั้ง
สมาชิกสภาผู้แทนราษฎรแบบแบ่งเขต

ข้อควรระวัง
- อย่ารับบัตรเลือกตั้งที่ฉีกออกจากต้นขั้วเตรียมไว้ก่อนแล้ว
- หากพบบัตรเลือกตั้งที่มีรอยเปื้อนในบริเวณกรอบสีเหลี่ยมด้านซ้ายมือบนให้ขอเปลี่ยนบัตรเลือกตั้งใบใหม่แทน

ไม่ประสงค์จะลงคะแนนให้กับผู้สมัครใดเลย ให้ทำเครื่องหมาย "กากบาท" เช่น (X) ลงในช่อง "ไม่ต้องการลงคะแนน" นี้

หมายเลขประจำตัวผู้สมัคร	ช่องทำเครื่องหมาย	หมายเลขประจำตัวผู้สมัคร	ช่องทำเครื่องหมาย	หมายเลขประจำตัวผู้สมัคร	ช่องทำเครื่องหมาย	หมายเลขประจำตัวผู้สมัคร	ช่องทำเครื่องหมาย
๕๐๑ 501		๕๑๑ 511		๕๒๑ 521		๕๓๑ 531	
๕๐๒ 502		๕๑๒ 512		๕๒๒ 522		๕๓๒ 532	
๕๐๓ 503		๕๑๓ 513		๕๒๓ 523		๕๓๓ 533	
๕๐๔ 504		๕๑๔ 514		๕๒๔ 524		๕๓๔ 534	
๕๐๕ 505		๕๑๕ 515		๕๒๕ 525		๕๓๕ 535	
๕๐๖ 506		๕๑๖ 516		๕๒๖ 526		๕๓๖ 536	
๕๐๗ 507		๕๑๗ 517		๕๒๗ 527		๕๓๗ 537	
๕๐๘ 508		๕๑๘ 518		๕๒๘ 528		๕๓๘ 538	
๕๐๙ 509		๕๑๙ 519		๕๒๙ 529		๕๓๙ 539	
๕๑๐ 510		๕๒๐ 520		๕๓๐ 530		๕๔๐ 540	

รูปที่ 4.23 ลักษณะของบัตรเลือกตั้งก่อนพิมพ์ข้อมูลรหัสลับ

รูปที่ 4.24 ภาพที่เก็บเข้าเครื่องคอมพิวเตอร์เพื่อใช้ในการดึงคุณลักษณะเฉพาะตัว

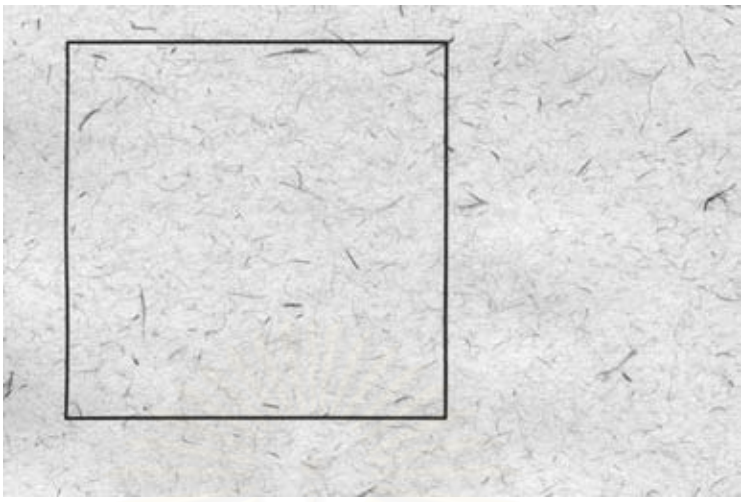
4.3.6.2 การแยกส่วนภาพออกเป็น 2 ส่วน

โปรแกรมพิมพ์บัตรเลือกตั้งจะนำภาพที่ถ่ายได้ไปแยกออกเป็น 2 ส่วน ส่วนบนก็คือกรอบสี่เหลี่ยมที่ใช้ดึงคุณลักษณะเฉพาะตัวของกระดาษต้นขั้ว ในขณะที่ส่วนล่างก็คือกรอบสี่เหลี่ยมที่ใช้ดึงคุณลักษณะเฉพาะตัวของกระดาษบัตรลงคะแนน โดยขั้นตอนการแยกส่วนภาพจะมีรายละเอียดดังนี้

- กำหนดให้จุดมุมบนด้านซ้ายเป็นจุดกำเนิด (มีพิกัด (0,0)) แกน +X ชี้ไปทางขวา ส่วนแกน +Y ชี้ลงด้านล่าง
- คัดลอกภาพเพื่อใช้ในการแยกภาพออกเป็น 2 ส่วน
- แปลงภาพที่ได้คัดลอกมาให้เป็นภาพสองระดับ ดังรูปที่ 4.25

- หากลุ่มจุดดำที่มีพื้นที่มากที่สุด 2 กลุ่ม ซึ่งน่าจะเป็นกรอบส่วนบนและส่วนล่างของภาพ
- ลบกลุ่มจุดดำอื่น ๆ ที่ไม่เกี่ยวข้องออกให้หมด
- หาพิกัดต่ำสุดของกรอบบนและพิกัดสูงสุดของกรอบล่าง
- นำค่า y ของพิกัดต่ำสุดของกรอบบนและค่า y ของพิกัดสูงสุดของกรอบล่างมาเฉลี่ยหาค่า y ที่อยู่กึ่งกลาง
- นำค่า y กึ่งกลางที่ได้ ไปแบ่งภาพต้นฉบับออกเป็นสองส่วน จะได้ภาพบัตรเลือกตั้งที่ถูกแยกออกเป็นสองส่วน ดังรูปที่ 4.26

รูปที่ 4.25 ภาพบัตรเลือกตั้งที่ถูกแปลงเป็นภาพ 2 ระดับ



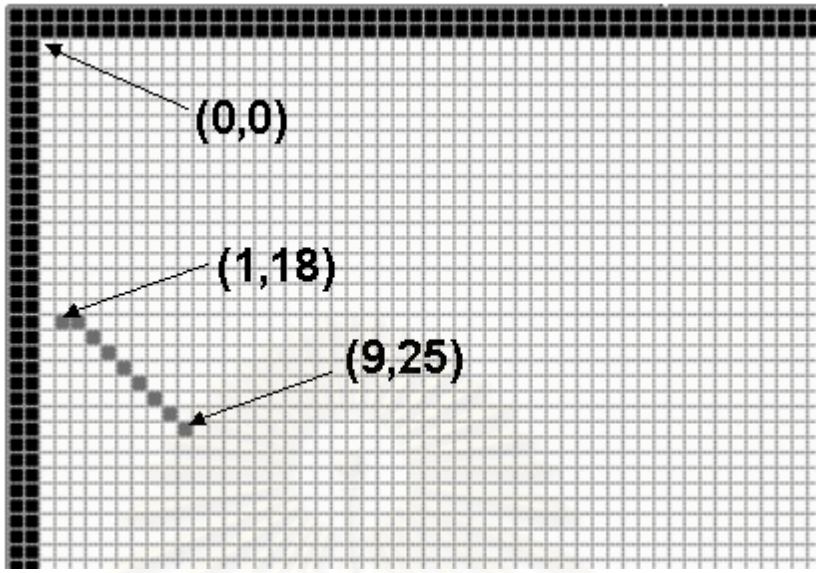
(ก)

(ข)

รูปที่ 4.26 ภาพบัตรเลือกตั้งที่ถูกแยกออกเป็นสองส่วน (ก) ส่วนบน (ข) ส่วนล่าง

4.3.6.3 **การดึงคุณลักษณะเฉพาะตัวจากกระดาษ**

หลังจากแยกภาพออกเป็น 2 ส่วนแล้ว ภาพแต่ละส่วนจะถูกดึงคุณลักษณะเฉพาะตัวของกระดาษ โดยคุณลักษณะเฉพาะตัวที่ใช้ก็คือ ค่าพิกัดของจุดปลายของวัตถุที่ฝังอยู่ในเนื้อกระดาษ ดังรูปที่ 4.27



รูปที่ 4.27 พิกัดของจุดปลายของวัตถุที่ฝังอยู่ในกระดาษที่ใช้พิมพ์บัตรเลือกตั้ง

สำหรับขั้นตอนการดึงคุณลักษณะเฉพาะตัวของกระดาษมีดังนี้

1. การหากรอบภาพ

การหากรอบของภาพที่จะใช้ดึงคุณลักษณะเฉพาะตัว มีขั้นตอนดังนี้

- กำหนดให้จุดมุมบนด้านซ้ายเป็นจุดกำเนิด (มีพิกัด (0,0)) แกน +X ชี้ไปทางขวา ส่วนแกน +Y ชี้ลงด้านล่าง
- คัดลอกภาพเพื่อใช้ในการหากรอบภาพ
- แปลงภาพที่ได้คัดลอกมาให้เป็นภาพสองระดับ
- หากลุ่มจุดดำที่มีพื้นที่มากที่สุด ซึ่งน่าจะเป็นกรอบของภาพ
- ลบกลุ่มจุดดำอื่น ๆ ที่ไม่เกี่ยวข้องออกให้หมด
- สุ่มหาจุดซึ่งอยู่บนขอบด้านในของกรอบแต่ละด้านของภาพ ทั้ง 4 ด้าน
- หาสมการเส้นตรงของขอบด้านในของกรอบแต่ละด้านจากจุดที่หาได้ โดยใช้การถดถอยเชิงเส้น (Linear regression)
- หาจุดตัดของสมการเส้นตรงที่หาได้ ซึ่งจะเป็นมุมทั้ง 4 ของขอบด้านในของกรอบ
- เมื่อสามารถหากรอบได้แล้ว จึงนำภาพต้นฉบับมาลบกรอบและข้อมูลที่ไม่เกี่ยวข้องซึ่งอยู่ภายนอกกรอบออก

- เนื่องจากภาพที่สแกนได้อาจเอียงและขอบด้านในของกรอบด้านมุมบนซ้ายไม่อยู่ตรงจุดกำเนิด จึงต้องหาค่ามุมเอียงและค่าพิกัดที่เลื่อนไปจากจุดกำเนิดเพื่อใช้ในขั้นตอนการเลื่อนและหมุนภาพต่อไป

2. การหากลุ่มจุดดำบนภาพ

นำภาพที่ผ่านการหากรอบภาพมาแปลงจากภาพชนิดสเกลสีเทา ให้เป็นภาพสองระดับเมื่อได้ภาพสองระดับ จึงนำภาพมาหากลุ่มจุดดำที่จะใช้ในการหาคุณลักษณะตัวของกระดาษในกระบวนการอื่นภายหลัง โดยมีขั้นตอนดังนี้

- หาพื้นที่ของกลุ่มจุดดำบนภาพ ถ้ามีพื้นที่น้อยกว่า 3 จุด ให้ลบทิ้ง ถ้ามีพื้นที่ตั้งแต่ 3 จุดขึ้นไป ให้เก็บไว้
- เรียงลำดับกลุ่มจุดดำที่เก็บได้ จากกลุ่มที่มีพื้นที่มากไปพื้นที่น้อย ซึ่งทำให้การเก็บคุณลักษณะจะได้คุณลักษณะของกลุ่มจุดดำที่มีพื้นที่มากก่อน
- ลบกลุ่มจุดดำส่วนที่เกินจากความต้องการซึ่งมีพื้นที่น้อยออกไป

3. การทำโครงร่างภาพ

นำกลุ่มจุดดำที่ได้มาทำโครงร่างภาพ เพื่อเตรียมภาพสำหรับการหาจุดปลายของกลุ่มจุดดำในกระบวนการถัดไป โดยการทำโครงร่างภาพที่ใช้เป็นการทำโครงร่างภาพโดยวิธี One-Pass Parallel Thinning [4] ของ Ben K. Jang และ Roland T. Chin เนื่องจากให้รายละเอียดคุณลักษณะของจุดต่อภาพได้ดีเพียงพอ โดยได้นำฟังก์ชันการทำโครงร่างภาพของนายประเสริฐ ฉอเรืองวิวัฒน์ ในวิทยานิพนธ์เรื่อง “การรู้จำตัวอักษรเขียนภาษาไทยโดยใช้การวิเคราะห์ลักษณะบ่งความต่าง” [22] มาดัดแปลงใช้ กลุ่มจุดดำที่ผ่านการทำโครงร่างภาพจะเหลือความกว้างเพียง 1 จุดภาพ

4. การหาจุดปลายของกลุ่มจุดดำ

หลังจากผ่านการทำโครงร่างภาพ ก็จะจัดแบ่งประเภทของจุดดำบนภาพ โดยนับจำนวนครั้งของการเปลี่ยนค่าของจุดที่อยู่ล้อมรอบจุดดำนั้น โดยอาจนับในทิศทางทวนเข็มนาฬิกาหรือตามเข็มนาฬิกาก็ได้ จะได้ประเภทของจุดดำบนภาพ ซึ่งประกอบด้วย

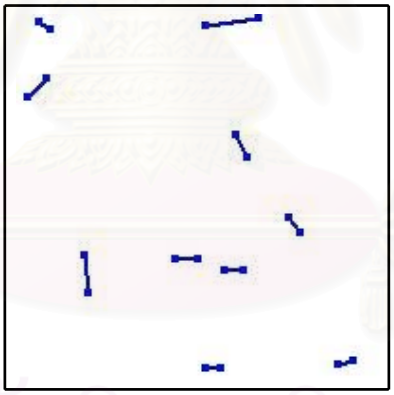
- จุดเดี่ยว คือ จุดดำที่ไม่มีการเปลี่ยนค่าของจุดที่อยู่ล้อมรอบจุดดำนั้น
- จุดปลาย คือ จุดดำที่มีจำนวนครั้งของการเปลี่ยนค่าของจุดที่อยู่ล้อมรอบจุดดำนั้น เท่ากับ “สอง”

- จุดต่อเนื่อง คือ จุดดำที่มีจำนวนครั้งของการเปลี่ยนค่าของจุดที่อยู่ล้อมรอบจุดดำนั้น เท่ากับ “สี่”
- จุดแยก คือ จุดดำที่มีจำนวนครั้งของการเปลี่ยนค่าของจุดที่อยู่ล้อมรอบจุดดำนั้น ตั้งแต่ “หก” ขึ้นไป

เมื่อได้ประเภทของจุดดำแล้ว จะเก็บค่าพิกัดของจุดดำที่เป็น “จุดปลาย” หรือ “จุดเดี่ยว” ของกลุ่มจุดดำนั้น ซึ่งเป็นคุณลักษณะที่ต้องการ โดยจะเรียกรวมกันว่า จุดปลาย

5. การเลื่อนหมุนภาพและการลดรายละเอียดของภาพ

นำค่าพิกัดที่เก็บได้ในกระบวนการที่แล้วมาเลื่อนและหมุน โดยใช้ค่ามุมเอียงและค่าพิกัดที่เลื่อนไปจากจุดกำเนิดที่คำนวณได้ในกระบวนการหากรอบภาพ หลังจากนั้นจะลดรายเอียดของพิกัดเนื่องจากพิกัดที่ได้มีความละเอียดมากเกินไป โดยจะหารค่าพิกัดด้วยค่าคงที่ค่าหนึ่ง ทำให้พิกัดมีความละเอียดลดลง เมื่อผ่านขั้นตอนนี้จะได้พิกัดของจุดปลายซึ่งนำมาใช้เป็นคุณลักษณะเฉพาะตัวของกระดาษ ตัวอย่างภาพพิกัดจุดปลายของวัตถุที่ผ่านกระบวนการดึงคุณลักษณะเฉพาะตัวของกระดาษ แสดงได้ดังรูปที่ 4.28



รูปที่ 4.28 พิกัดของจุดปลายที่ได้จากกระบวนการดึงคุณลักษณะเฉพาะตัว

6. การจัดรูปแบบข้อมูลคุณลักษณะที่ได้

ข้อมูลคุณลักษณะเฉพาะตัวของต้นขั้วและบัตรลงคะแนน (F_S, F_V) ที่ได้จะเป็นเลขฐาน 16 มีขนาดไม่เกิน 50 ไบต์ แบ่งออกเป็นกลุ่มตามชนิดของจุด เรียงต่อกันไปเรื่อย ๆ โดยในแต่ละกลุ่มจะมีรูปแบบข้อมูลดังนี้

ส่วนประกอบ	ความยาว (ไบต์)
- ชนิดซึ่งแบ่งตามจำนวนจุด เช่น 01 หมายถึง มีจุด 1 จุด ในกลุ่มจุดดำนั้น 02 หมายถึง พิกัดจุดปลาย 2 จุด ของกลุ่มจุดดำนั้น	1
- ความยาวของจุดทั้งหมดที่อยู่ในกลุ่มจุดดำชนิดเดียวกัน (หน่วยเป็นไบต์)	1
- พิกัดของจุดที่อยู่ในกลุ่มจุดดำชนิดเดียวกัน	ตามค่าที่เก็บไว้

ยกตัวอย่างเช่น ให้ข้อมูลคุณลักษณะเฉพาะตัวของกระดาษ (F) ที่ได้มีรูปแบบดังนี้

02080C410F451C55243F010424574731

02 ก็คือชนิดของกลุ่มจุดดำนั้นเป็นชนิด 2 จุด (จุดปลาย)

08 ก็คือความยาวของจุดทั้งหมดที่อยู่ในกลุ่มจุดดำชนิด 2 จุดนั้นมีความยาว 8 ไบต์

จุดที่อยู่ในกลุ่มจุดดำชนิด 2 จุด มีขนาด 8 ไบต์ ได้แก่ 0C410F451C55243F

0C410F45 ก็คือพิกัดจุดปลาย 2 จุด อยู่ที่คู่พิกัด {(12,65),(15,69)}

1C55243F ก็คือพิกัดจุดปลาย 2 จุด อยู่ที่คู่พิกัด {(28,85),(36,63)}

01 ก็คือชนิดของกลุ่มจุดดำนั้นเป็นชนิด 1 จุด (จุดเดี่ยว)

04 ก็คือความยาวของจุดทั้งหมดที่อยู่ในกลุ่มจุดดำชนิด 1 จุดนั้นมีความยาว 4 ไบต์

จุดที่อยู่ในกลุ่มจุดดำชนิด 1 จุด มีขนาด 4 ไบต์ ได้แก่ 24574731

2457 ก็คือพิกัด (36,87)

4731 ก็คือพิกัด (71,49)

4.3.6.4 การสร้างข้อมูลประจำบัตรเลือกตั้งและแฟ้มข้อมูลรายงานการจัดพิมพ์

หลังจากที่ได้คุณลักษณะเฉพาะตัวของกระดาษทั้งในส่วนต้นขั้วและบัตรลงคะแนน (F_S, F_V) แล้วจะนำคุณลักษณะเฉพาะตัวไปใช้ในการสร้างข้อมูลประจำต้นขั้วและข้อมูลประจำบัตรลงคะแนน ($D_S = N_S; U_{1S}; F_S; H_{4S}, D_V = N_V; U_{1V}; F_V; H_{4V}$) ซึ่งการสร้างข้อมูลประจำต้นขั้ว (D_S) และข้อมูลประจำบัตรลงคะแนน (D_V) จะมีหลักการเดียวกัน โดยมีขั้นตอนดังนี้

- *อ่านแฟ้มข้อมูลรหัสเฉพาะ* โปรแกรมจะอ่านแฟ้มข้อมูลรหัสเฉพาะของต้นขั้วและบัตรลงคะแนน ได้รหัสเฉพาะ 2 ชั้นออกมา ($U_2 = K_p^*[K_C^*[U]]$)

- *ถอดรหัส รหัสเฉพาะ* โปรแกรมจะถอดรหัส รหัสเฉพาะ 2 ชั้น ด้วยกุญแจสาธารณะของโปรแกรมซึ่งฝังอยู่ในโปรแกรมพิมพ์บัตรเลือกตั้งได้รหัสเฉพาะ 1 ชั้นออกมา ($K_P[U_2] = K_P[K_P^*[K_C^*[U]]] = K_C^*[U] = U_1$)
- *รวบรวมข้อมูล* นำข้อมูลรหัสเฉพาะ 1 ชั้น (U_1) ไปรวมกับเลขประจำบัตร (N) และคุณลักษณะเฉพาะตัวของกระดาษ (F) เพื่อเตรียมที่จะนำไปผ่านแฮชฟังก์ชัน
- *สร้างค่าแฮช* นำข้อมูลที่รวบรวมไปผ่านแฮชฟังก์ชัน โดยนำซอฟต์แวร์การสร้างค่าแฮชด้วยวิธี RIPE-MD 160 ของ Antoon Bosselaers [23] มาดัดแปลงใช้จะได้ค่าแฮช ($H = H[N;U_1;F]$) ออกมาขนาด 160 ไบต์
- *ลดขนาดค่าแฮช* ค่าแฮชจะถูกลดขนาดจาก160 ไบต์ เหลือเพียง 4 ไบต์ ($H_4 = H_4[N;U_1;F]$) ซึ่งมีขนาดเพียงพอที่จะนำไปใช้ได้ หลังจากนั้นจึงนำค่าแฮชขนาด 4 ไบต์ ไปใช้เป็นส่วนหนึ่งของข้อมูลประจำบัตรเลือกตั้ง (D)
- *สร้างแฟ้มข้อมูลรายงานการจัดพิมพ์* โปรแกรมพิมพ์บัตรเลือกตั้งจะเข้ารหัสค่าแฮชและรหัสเฉพาะ 1 ชั้น ด้วยกุญแจสาธารณะของโปรแกรม ($K_P[H_4;U_1]$) แล้วจึงบันทึกลงแฟ้มข้อมูลรายงานการจัดพิมพ์เพื่อรายงานให้กรรมการเลือกตั้งทราบว่าได้พิมพ์บัตรเลือกตั้งที่มีค่าแฮชและรหัสเฉพาะอย่างที่อยู่ในแฟ้มข้อมูล
- *สร้างข้อมูลประจำบัตรเลือกตั้ง* นำค่าแฮช 4 ไบต์ (H_4) ที่ได้ไปรวมกับเลขประจำบัตร (N) รหัสเฉพาะ 1 ชั้น (U_1) และคุณลักษณะเฉพาะตัวของกระดาษ (F) กลายเป็นข้อมูลประจำบัตรเลือกตั้ง ($D = N;U_1;F;H_4$) ใบนั้น ๆ ตามตารางที่ 4.3

ตารางที่ 4.3 รูปแบบข้อมูลประจำต้นขั้วและบัตรลงคะแนน

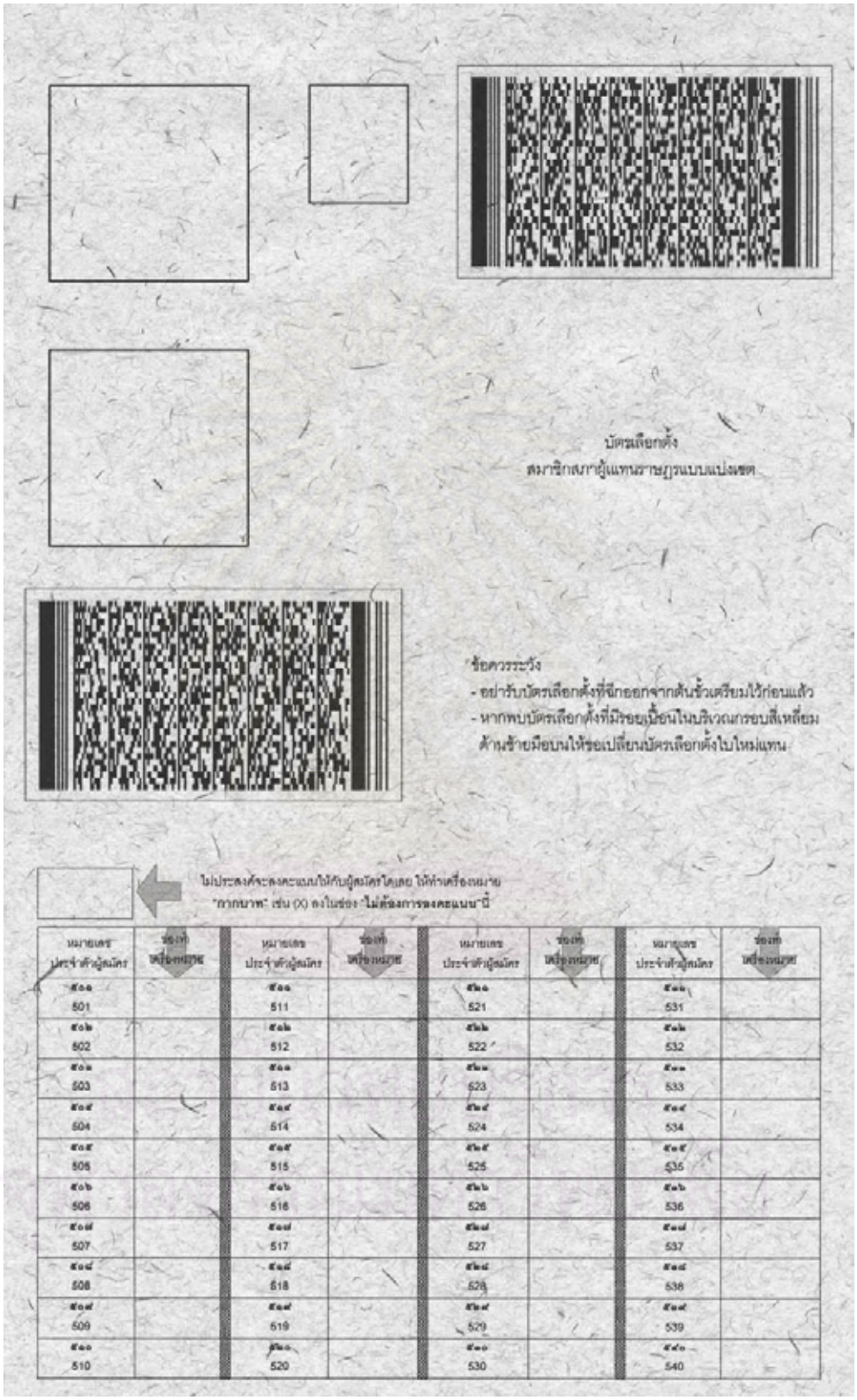
ส่วนประกอบ	ความยาว (ไบต์)
- วันเลือกตั้ง	4
- รหัสเขตเลือกตั้ง	2
- หมายเลขสมุดเลือกตั้ง	2
- หมายเลขประจำบัตร	2
- รหัสเฉพาะ 1 ชั้น	64
- คุณลักษณะเฉพาะตัวของกระดาษ	ไม่เกิน 50
- ค่าแฮช	4

4.3.6.5 การเข้ารหัสลับข้อมูลประจำต้นขั้วและบัตรลงคะแนน

หลังจากที่ได้ข้อมูลประจำต้นขั้ว (D_S) และข้อมูลประจำบัตรลงคะแนน (D_V) แล้วจะนำไปเข้ารหัสลับโดยใช้กุญแจส่วนตัวของกรรมการเขต (K_L^*) ได้ข้อมูลรหัสลับของต้นขั้ว ($K_L^*[D_S]$) และบัตรลงคะแนน ($K_L^*[D_V]$) ในรูปเลขฐาน 16 มีความยาว 136 ไบต์

4.3.6.6 การพิมพ์รหัสลับลงบนบัตรเลือกตั้ง

นำรหัสลับที่ได้ของต้นขั้ว ($K_L^*[D_S]$) และบัตรลงคะแนน ($K_L^*[D_V]$) ซึ่งอยู่ในรูปเลขฐาน 16 มาเปลี่ยนเป็นรหัสแท่ง 2 มิติ โดยนำซอฟต์แวร์การสร้างรหัสแท่ง 2 มิติ PDF417 ของ John Lien [24] มาดัดแปลงใช้ ซึ่งจะทำการสร้างรหัสแท่ง 2 มิติ ตามขั้นตอนที่ได้กล่าวไว้แล้วในหัวข้อที่ 2.5 หลังจากนั้นจึงพิมพ์รหัสแท่ง 2 มิติลงบนกระดาษบัตรเลือกตั้งจะได้ลักษณะบัตรเลือกตั้งดังรูปที่ 4.29



รูปที่ 4.29 ลักษณะของบัตรเลือกตั้งหลังจากพิมพ์ข้อมูลรหัสลับ

4.3.7 การส่งแฟ้มข้อมูลรายงานการจัดพิมพ์ไปยังส่วนกลาง

กรรมการเขตจะต้องส่งแฟ้มข้อมูลรายงานการจัดพิมพ์ ($K_P[H_4,U_1]$) ไปให้กรรมการเลือกตั้งเพื่อรายงานให้ทราบว่าได้จัดพิมพ์บัตรเลือกตั้งที่มีค่าแฮชและรหัสเฉพาะอย่างที่อยู่ภายในแฟ้มข้อมูล สำหรับสาเหตุที่เข้ารหัสลับค่าแฮชและรหัสเฉพาะ 1 ชั้น ด้วยกุญแจสาธารณะของโปรแกรม (K_P) ก็เพื่อป้องกันไม่ให้กรรมการเขตสามารถเปลี่ยนแปลงหรือแก้ไขข้อมูลได้

4.3.8 การสร้างและจัดส่งแฟ้มข้อมูลตรวจสอบค่าแฮช

หลังจากที่กรรมการเลือกตั้งได้รับแฟ้มข้อมูลรายงานการจัดพิมพ์จากกรรมการเขตแล้ว ก็จะรวบรวมค่าแฮช แล้วจึงเข้ารหัสค่าแฮชด้วยกุญแจส่วนตัวของโปรแกรม ($K_P[H_{4S}], K_P[H_{4V}]$) หลังจากนั้นจะบันทึกค่าแฮชที่ถูกเข้ารหัสลงแฟ้มข้อมูลตรวจสอบค่าแฮช และส่งแฟ้มข้อมูลไปให้กรรมการเขตเพื่อนำไปใช้เป็นฐานข้อมูลในการตรวจสอบค่าแฮชของบัตรเลือกตั้ง

4.3.9 การตรวจรับบัตรเลือกตั้งเปล่า ณ หน่วยเลือกตั้ง

เมื่อกรรมการเขตพิมพ์บัตรเลือกตั้งเสร็จ จะต้องส่งบัตรเลือกตั้งเปล่าไปให้เจ้าหน้าที่ประจำหน่วยเพื่อนำไปให้ผู้มาใช้สิทธิ์ลงคะแนน ซึ่งระหว่างการขนย้ายบัตรเลือกตั้งเปล่าจากเขตเลือกตั้งไปยังหน่วยเลือกตั้ง อาจจะเกิดการสับเปลี่ยนบัตรเลือกตั้งระหว่างทางได้ ดังนั้นเจ้าหน้าที่ประจำหน่วยจึงต้องสุ่มตรวจบัตรเลือกตั้ง ซึ่งการตรวจสอบบัตรเลือกตั้งที่หน่วยเลือกตั้งจะใช้แฟ้มข้อมูลและทรัพยากร ดังนี้

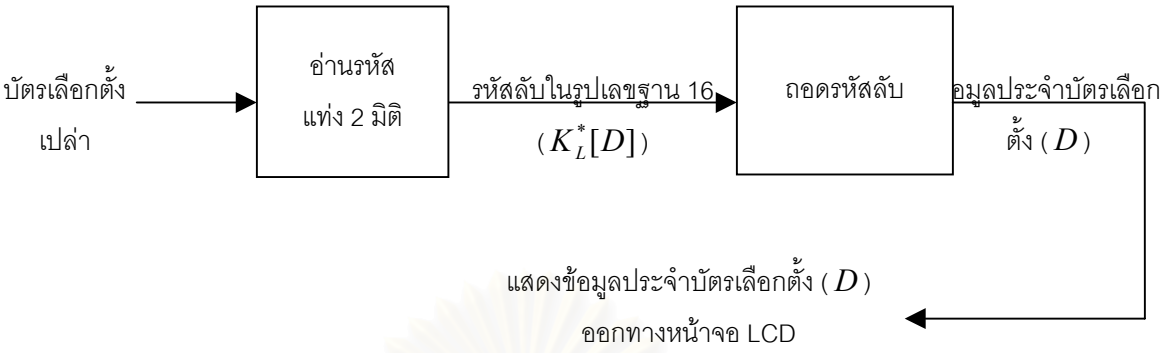
วัตถุ : บัตรเลือกตั้ง

ข้อมูล : กุญแจสาธารณะของกรรมการเขต (K_L)

ฮาร์ดแวร์ : ไมโครคอนโทรลเลอร์ เซนเซอร์สัมผัสภาพและ LCD (Liquid Crystal Display)

ซอฟต์แวร์ : โปรแกรมภาษาแอสเซมบลี ใช้ในการอ่านรหัสแท่ง 2 มิติ และถอดรหัสข้อมูลรหัสลับ

ผู้ปฏิบัติการ : เจ้าหน้าที่ประจำหน่วยเลือกตั้ง



รูปที่ 4.30 แผงผังขั้นตอนการทำงานของโปรแกรมตรวจสอบบัตรเลือกตั้งที่หน่วยเลือกตั้ง

สำหรับรายละเอียดขั้นตอนการตรวจสอบบัตรเลือกตั้ง ณ หน่วยเลือกตั้งมีขั้นตอนดังนี้

4.3.9.1 **อ่านรหัสแท่ง 2 มิติ**

เจ้าหน้าที่ประจำหน่วยจะใช้เซนเซอร์สัมผัสภาพและโปรแกรมบนเครื่องไมโครคอนโทรลเลอร์ในการอ่านรหัสแท่ง 2 มิติ ได้รหัสลับ ($K_L^*[D]]$) ในรูปเลขฐาน 16 ออกมา

4.3.9.2 **ถอดรหัสลับ**

โปรแกรมบนเครื่องไมโครคอนโทรลเลอร์จะรับข้อมูลกุญแจสาธารณะของกรรมการเขต (K_L) เข้ามา แล้วจึงนำกุญแจสาธารณะของกรรมการเขตไปถอดรหัสข้อมูลลับได้ข้อมูลประจำบัตรเลือกตั้ง ($K_L[K_L^*[D]] = D$) และแสดงข้อมูลประจำบัตรเลือกตั้งออกทางหน้าจอ LCD

4.3.9.3 **ตรวจสอบความถูกต้องของข้อมูล**

เจ้าหน้าที่ประจำเขตจะตรวจสอบความถูกต้องของข้อมูลประจำบัตร (D) ที่แสดงบนจอ LCD หลังจากตรวจสอบเสร็จ เจ้าหน้าที่ประจำเขตจะบันทึกค่าแฮชของบัตรเลือกตั้งใบนั้น (H_4) และเซ็นชื่อกำกับไว้

4.3.10 **การจัดส่งบัตรลงคะแนน, ต้นขั้วและบัตรเลือกตั้งเปล่าที่เหลือไปยังสถานที่ต่าง ๆ**

หลังจากหมดเวลาในการลงคะแนนเลือกตั้งแล้ว เจ้าหน้าที่ประจำหน่วยจะต้องส่งบัตรลงคะแนนไปยังสถานที่นับคะแนนเพื่อทำการนับคะแนนการเลือกตั้ง นอกจากนี้เจ้าหน้าที่ประจำหน่วยยังต้องส่งบัตรเลือกตั้งเปล่าที่ยังไม่ได้ใช้และต้นขั้วของบัตรเลือกตั้งที่ใช้แล้วไปยังที่ว่าการอำเภอเพื่อให้เจ้าหน้าที่ประจำที่ว่าการอำเภอเก็บรักษาไม่ให้ผู้ที่ต้องการทุจริตนำบัตรลงคะแนนของบัตรเลือกตั้งเปล่าที่ยังไม่ได้ใช้ไปสับเปลี่ยนกับบัตรลงคะแนนที่ขนส่งไปยังสถานที่นับคะแนน

4.3.11 การตรวจสอบบัตรลงคะแนน ณ สถานที่นับคะแนน

หลังจากที่บัตรลงคะแนนถูกส่งมายังสถานที่นับคะแนน ก่อนที่จะนำบัตรลงคะแนนไปเทรวมเจ้าหน้าที่ประจำเขตจะตรวจสอบจำนวนบัตรลงคะแนนก่อนว่าครบตามจำนวนที่เจ้าหน้าที่ประจำหน่วยได้รายงานมาหรือไม่ หลังจากนั้นจะนำไปเทรวมและเริ่มนับคะแนนพร้อมทั้งสุ่มตรวจบัตรลงคะแนนไปด้วยโดยใช้โปรแกรมตรวจสอบบัตรเลือกตั้ง การตรวจสอบความถูกต้องของบัตรลงคะแนนจะต้องใช้แฟ้มข้อมูลและทรัพยากรดังนี้

วัตถุ : บัตรลงคะแนน

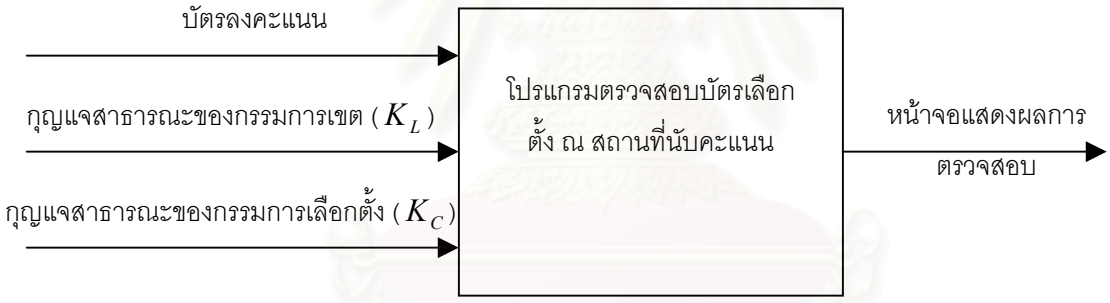
แฟ้มข้อมูล : กุญแจสาธารณะของกรรมการเขต (K_L), กุญแจสาธารณะของเลือกตั้ง (K_C)

ฮาร์ดแวร์ : ไมโครคอมพิวเตอร์และกล้องประจำเครื่องคอมพิวเตอร์ส่วนบุคคล

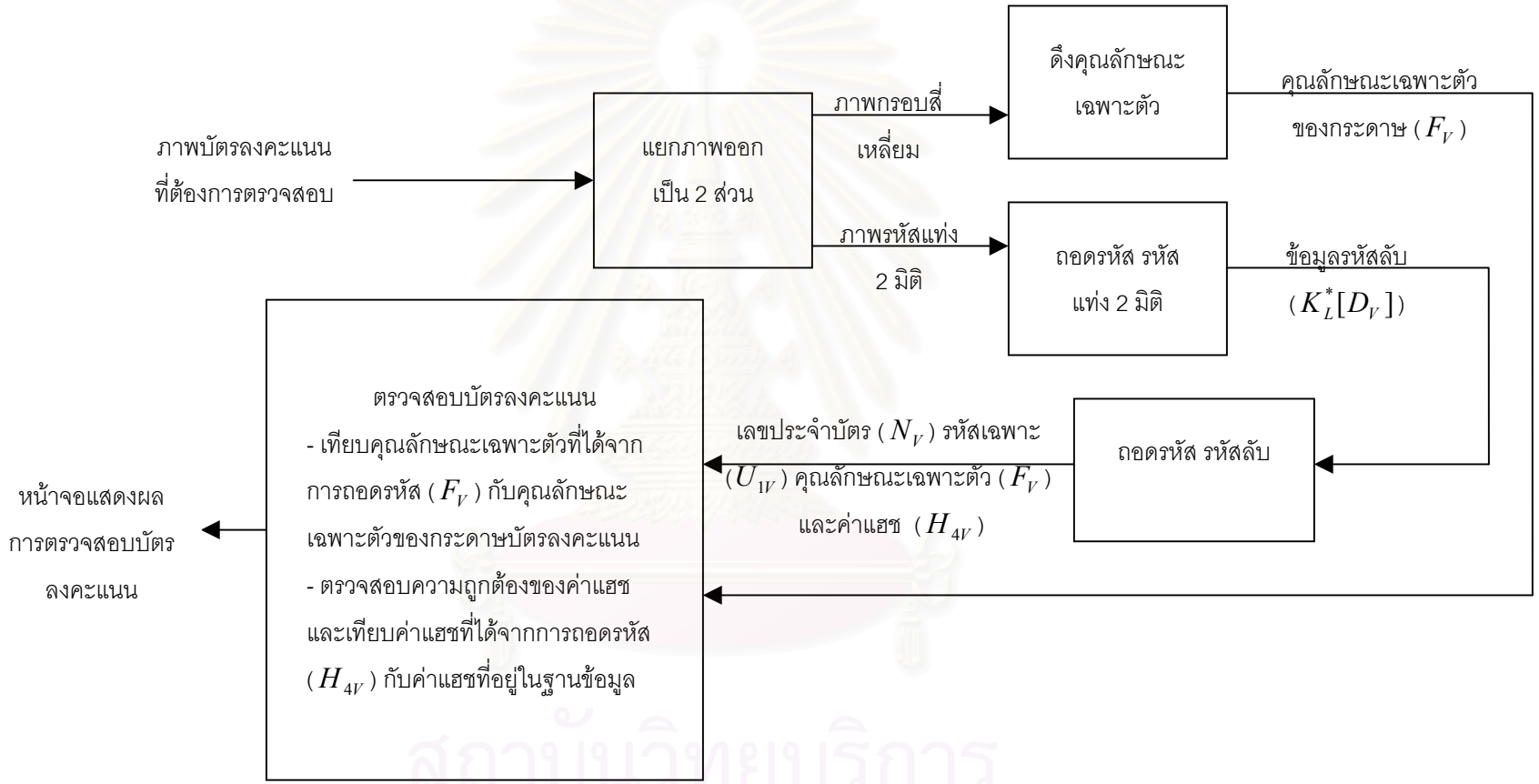
ซอฟต์แวร์ : โปรแกรมตรวจสอบบัตรเลือกตั้ง (ดูได้ดังรูปที่ 4.33)

ผู้ปฏิบัติการ : เจ้าหน้าที่ประจำเขตเลือกตั้ง

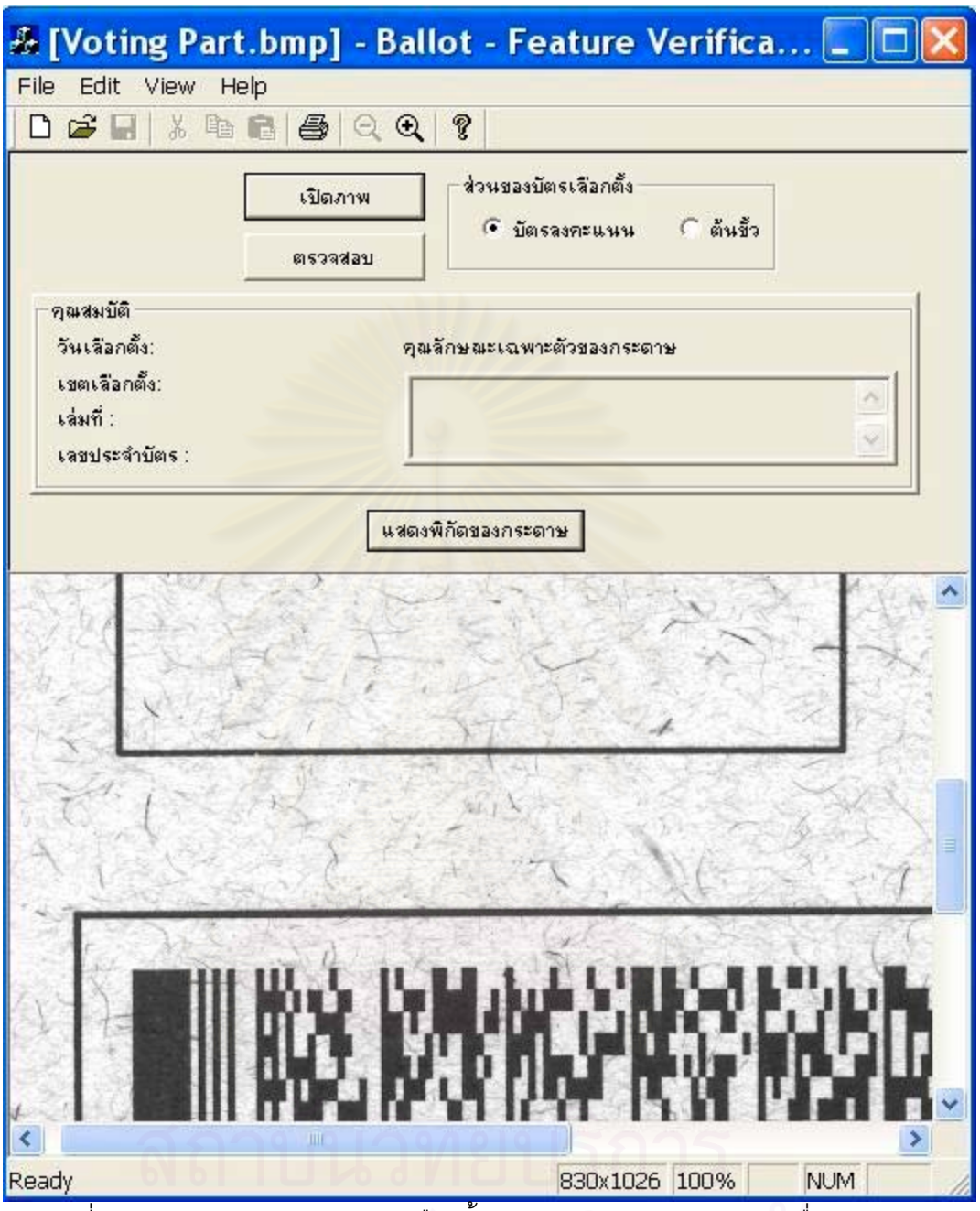
ผลลัพธ์ที่ได้ : หน้าจอแสดงผลการตรวจสอบความถูกต้องของบัตรลงคะแนน



รูปที่ 4.31 ผลลัพธ์ที่ได้จากโปรแกรมตรวจสอบบัตรเลือกตั้ง



รูปที่ 4.32 แผนผังการทำงานของโปรแกรมตรวจสอบบัตรลงคะแนน ณ สถานที่นับคะแนน

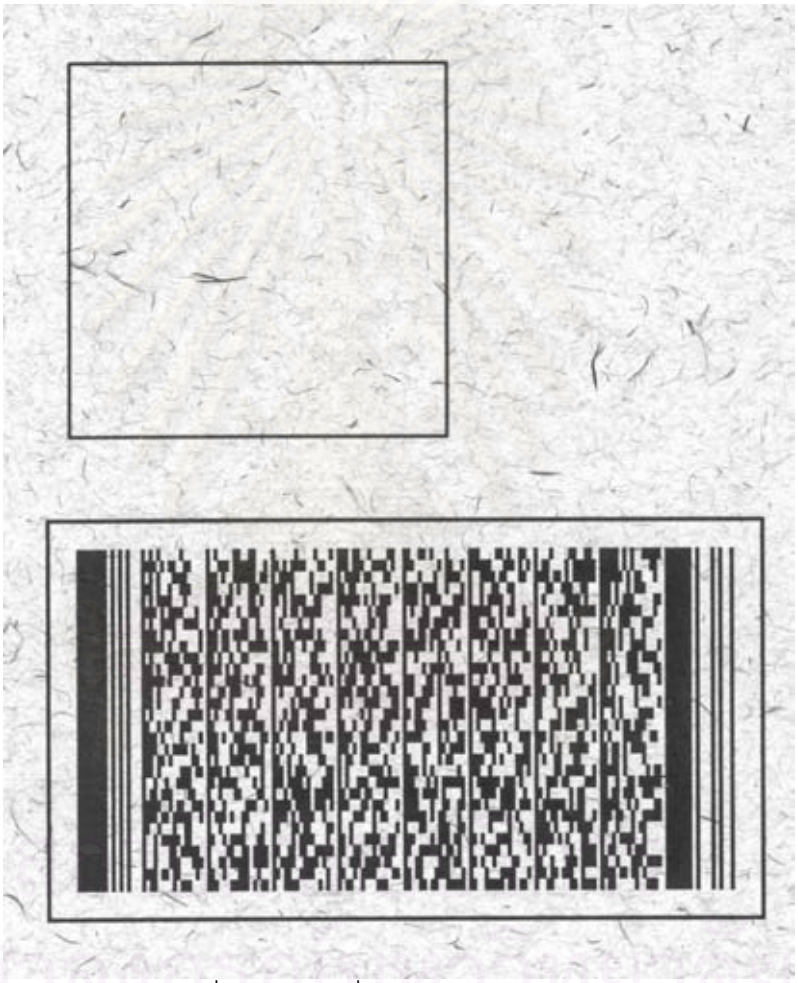


รูปที่ 4.33 โปรแกรมตรวจสอบบัตรเลือกตั้งขณะเปิดภาพบัตรลงคะแนนเพื่อตรวจสอบ

สำหรับขั้นตอนการตรวจสอบบัตรลงคะแนน ณ สถานที่นับคะแนนดังรูปที่ 4.32 มีรายละเอียดดังนี้

4.3.11.1 การเก็บภาพบัตรลงคะแนน

ใช้กล้องประจำเครื่องคอมพิวเตอร์ส่วนบุคคลถ่ายภาพ โดยให้บริเวณกรอบสำหรับดึงข้อมูลคุณลักษณะเฉพาะตัวของกระดาษและรหัสแท่ง 2 มิติ อยู่ในภาพด้วย ดังรูปที่ 4.34 จากนั้นจึงบันทึกภาพเป็นแฟ้มข้อมูลในรูปแบบ bitmap (bmp) แบบสเกลสีเทา



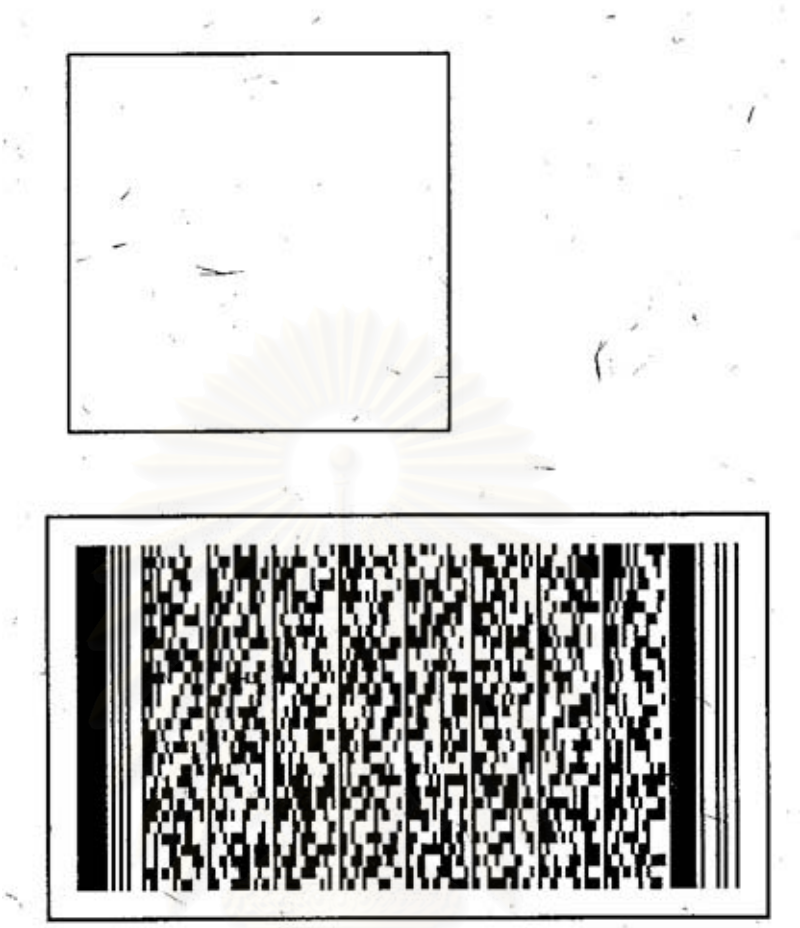
รูปที่ 4.34 ภาพที่ได้จากอุปกรณ์เก็บภาพ

4.3.11.2 การแยกภาพออกเป็น 2 ส่วน

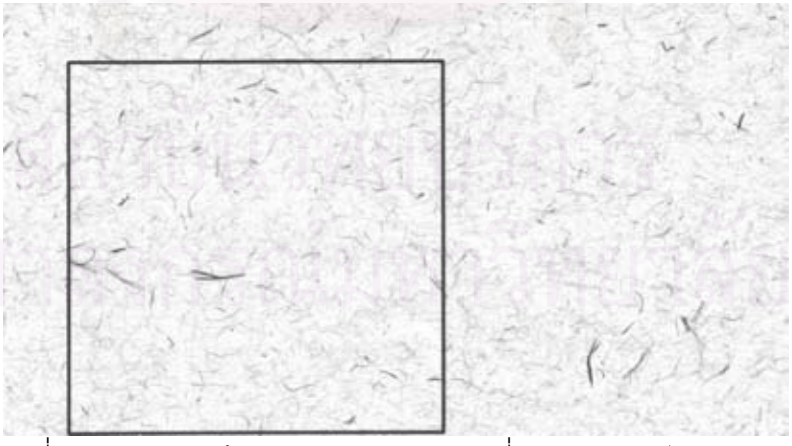
หลังจากเก็บภาพบัตรลงคะแนนแล้ว เจ้าหน้าที่ประจำเขตจะใช้โปรแกรมตรวจสอบบัตรเลือกตั้งเปิดภาพและสั่งให้โปรแกรมตรวจสอบบัตรลงคะแนน หลังจากนั้นโปรแกรมจะแยกภาพ

ออกเป็น 2 ส่วน โดยส่วนแรกคือ กรอบสี่เหลี่ยมใช้ดึงคุณลักษณะเฉพาะตัวของกระดาษบัตรลงคะแนน และส่วนที่ 2 คือ รหัสแท่ง 2 มิติ ซึ่งมีข้อมูลประจำบัตรลงคะแนนอยู่ ขั้นตอนการแยกส่วนภาพมีดังนี้

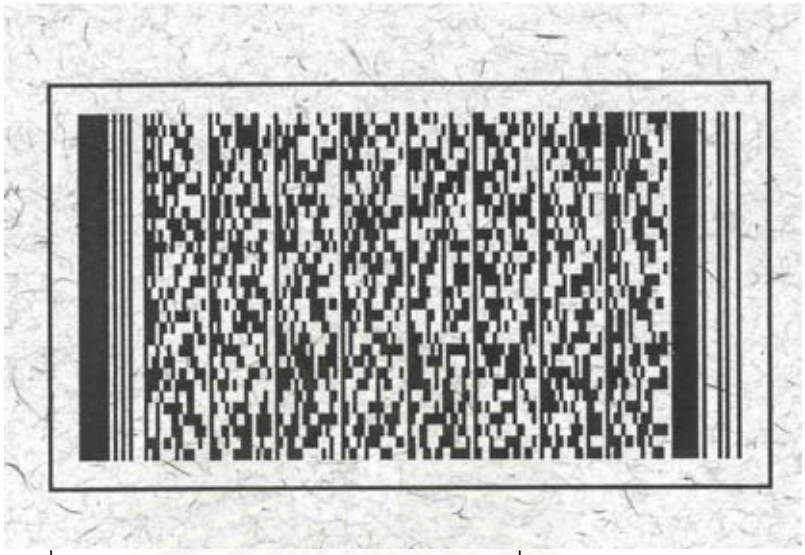
- กำหนดให้จุดมุมบนด้านซ้ายเป็นจุดกำเนิด (มีพิกัด (0,0)) แกน +X ชี้ไปทางขวา ส่วนแกน +Y ชี้ลงด้านล่าง
- คัดลอกภาพเพื่อใช้ในการแยกส่วนภาพ
- แปลงภาพที่ได้คัดลอกมาให้เป็นภาพสองระดับ จะได้ภาพสองระดับดังรูปที่ 4.35
- เนื่องจากรูปภาพที่ได้คัดลอกมามีกลุ่มจุดดำขนาดใหญ่อยู่หลายกลุ่ม เช่น กรอบสี่เหลี่ยมที่ใช้ดึงคุณลักษณะเฉพาะตัวของกระดาษ กรอบสี่เหลี่ยมของรหัสแท่ง 2 มิติ และกลุ่มจุดดำภายในรหัสแท่ง 2 มิติ ดังนั้นการหากรอบสี่เหลี่ยมที่ใช้ดึงคุณลักษณะเฉพาะตัวของกระดาษทำได้โดยตั้งค่าพื้นที่ระดับกั้น (Area Threshold) ของกลุ่มจุดดำไว้ ซึ่งค่าพื้นที่ระดับกั้นจะมากกว่าค่าพื้นที่กลุ่มจุดดำของวัตถุที่ฝังในกระดาษ แต่จะน้อยกว่าค่าพื้นที่กลุ่มจุดดำของกรอบสี่เหลี่ยมที่ใช้ดึงคุณลักษณะเฉพาะตัวของกระดาษ
- หาพื้นที่กลุ่มจุดดำในภาพโดยเริ่มต้นหาจากจุดกำเนิดไปทางขวาและหาจากบนลงล่าง ถ้าพบพื้นที่กลุ่มจุดดำกลุ่มแรกที่มีค่ามากกว่าพื้นที่ระดับกั้น กลุ่มจุดดำนั้นก็คือกรอบสี่เหลี่ยมที่ใช้ดึงคุณลักษณะเฉพาะตัวของกระดาษ
- หาค่า y ที่มากที่สุดของกรอบสี่เหลี่ยมที่ใช้ดึงคุณลักษณะเฉพาะตัวของกระดาษ โดยเรียกค่า y นั้นว่า ค่า y จุดแบ่งและใช้ค่า y จุดแบ่งในการแยกภาพต้นฉบับออกเป็นสองส่วน คือส่วนของภาพที่มีค่า y น้อยกว่าหรือเท่ากับค่า y จุดแบ่ง อีกส่วนของภาพจะมีค่า y มากกว่าค่า y จุดแบ่ง เมื่อแบ่งภาพแล้วจะได้ภาพดังรูปที่ 4.36



รูปที่ 4.35 ภาพสองระดับที่ได้จากการแปลงภาพต้นฉบับ



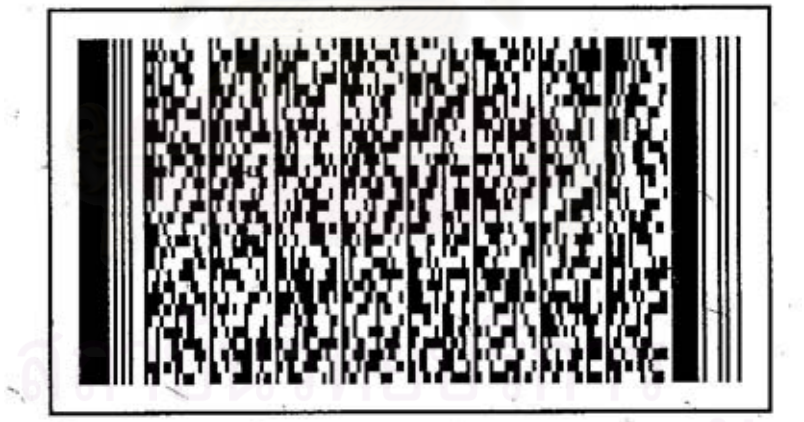
รูปที่ 4.36 (ก) ภาพต้นฉบับส่วนบนหลังจากที่ถูกแยกออกเป็นสองส่วน



รูปที่ 4.36 (ข) ภาพต้นฉบับส่วนล่างหลังจากที่ถูกแยกออกเป็นสองส่วน

4.3.11.3 การแปลงภาพรหัสแท่ง 2 มิติ ให้เป็นภาพสองระดับ

ภาพรหัสแท่ง 2 มิติพร้อมกรอบสี่เหลี่ยม จากรูปที่ 4.36 (ข) จะถูกเปลี่ยนให้เป็นภาพสองระดับ ดังรูปที่ 4.37



รูปที่ 4.37 ภาพสองระดับของรหัสแท่ง 2 มิติ ภายในกรอบสี่เหลี่ยม

4.3.11.4 การหากรอบสี่เหลี่ยมที่อยู่รอบ ๆ รหัสแท่ง 2 มิติ

ขั้นตอนการหากรอบสี่เหลี่ยมที่อยู่รอบๆ รหัสแท่ง 2 มิติ มีดังนี้

- กำหนดให้จุดมุมบนด้านซ้ายเป็นจุดกำเนิด (มีพิกัด (0,0)) แกน +X ชี้ไปทางขวา ส่วนแกน +Y ชี้ลงด้านล่าง

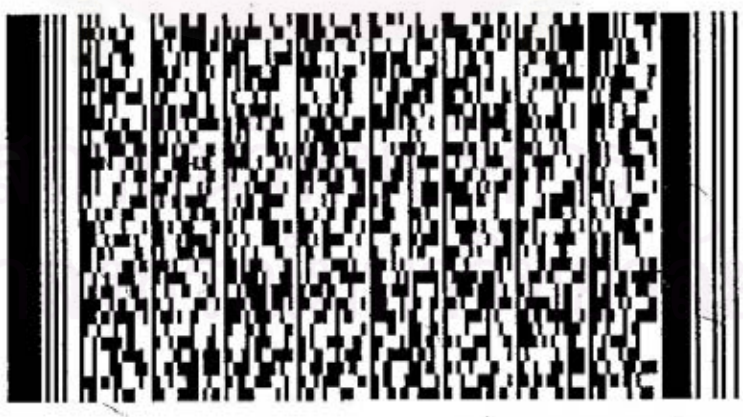
- หากลุ่มจุดดำกลุ่มแรกที่มีค่าพื้นที่มากกว่าค่าพื้นที่ระดับกั้น ซึ่งกลุ่มจุดดำนั้นน่าจะเป็นกรอบที่อยู่รอบๆ รหัสแท่ง 2 มิติ
- ลบกลุ่มจุดดำอื่น ๆ ที่อยู่นอกกรอบออกให้หมด
- สุ่มหาจุดซึ่งอยู่บนขอบด้านในของกรอบแต่ละด้านของภาพ ทั้ง 4 ด้าน
- หาสมการเส้นตรงของขอบด้านในของกรอบแต่ละด้านจากจุดที่หาได้ โดยใช้การถดถอยเชิงเส้น (Linear regression)
- หาจุดตัดของสมการเส้นตรงที่หาได้ ซึ่งจะเป็นมุมทั้ง 4 ของขอบด้านในของกรอบ
- เนื่องจากภาพที่สแกนได้อาจเอียงและขอบด้านในของกรอบด้านมุมบนซ้ายไม่อยู่ตรงจุดกำเนิด จึงต้องหาค่ามุมเอียงและค่าพิกัดที่เลื่อนไปจากจุดกำเนิดเพื่อใช้ในขั้นตอนการเลื่อนและหมุนภาพต่อไป

4.3.11.5 **การเลื่อนและหมุนภาพ** (Translation and rotation)

นำค่าพิกัดจุดดำทุกจุดของภาพมาเลื่อนและหมุน โดยใช้ค่ามุมเอียงและค่าพิกัดที่เลื่อนไปจากจุดกำเนิดที่คำนวณได้ในกระบวนการหากรอบภาพ

4.3.11.6 **การลบกรอบสี่เหลี่ยมที่อยู่รอบ ๆ รหัสแท่ง 2 มิติ**

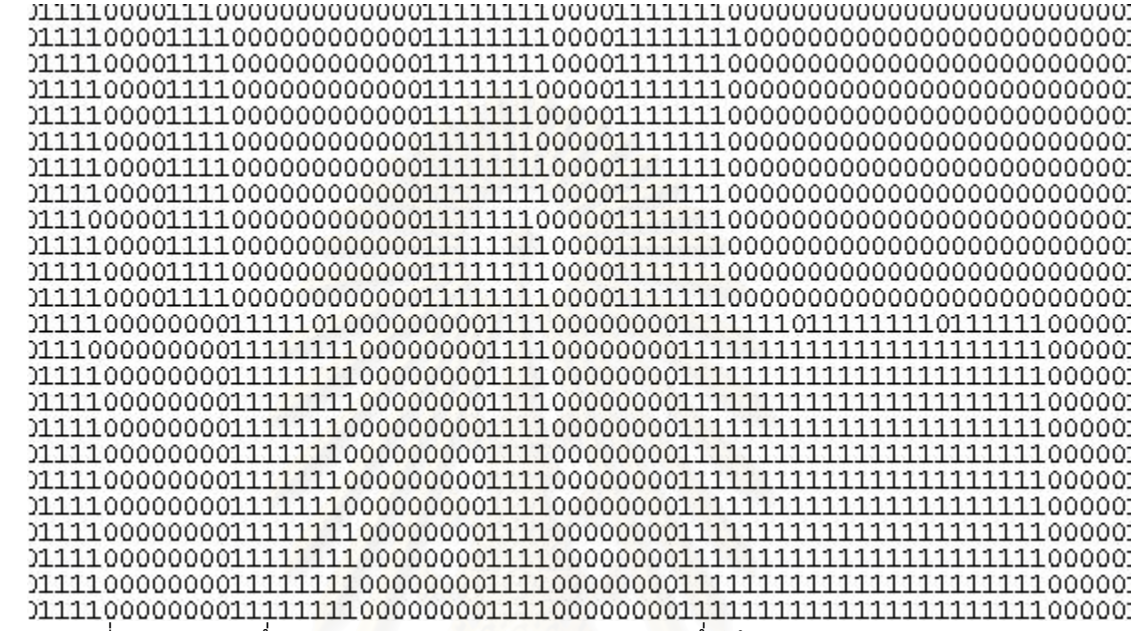
ทำการลบกรอบสี่เหลี่ยมที่อยู่รอบๆ รหัสแท่ง 2 มิติ ออกจะได้ภาพรหัสแท่ง 2 มิติ ดังรูปที่ 4.38



รูปที่ 4.38 ภาพรหัสแท่ง 2 มิติ ที่ผ่านการลบกรอบแล้ว

4.3.11.7 **การสร้างแฟ้มข้อมูลชนิด** pbm

หลังจากลบกรอบสี่เหลี่ยมออกไปแล้ว ก่อนที่จะถอดรหัส รหัสแท่ง 2 มิติ จะนำภาพรหัสแท่ง 2 มิติ ไปสร้างแฟ้มข้อมูลในรูปแบบ pbm [25] ซึ่งเป็นชนิดของภาพอย่างหนึ่ง ที่มีรูปแบบง่ายๆ คือ “0” แทนพิกัดจุดขาว 1 พิกเซลและ “1” แทนพิกัดจุดดำ 1 พิกเซล ดังรูปที่ 4.39



รูปที่ 4.39 ส่วนหนึ่งของรหัสแท่ง 2 มิติ ในรูปแบบ pbm ซึ่งใช้ในการถอดรหัส รหัสแท่ง 2 มิติ

4.3.11.8 **การถอดรหัส รหัสแท่ง 2 มิติ**

หลังจากสร้างแฟ้มข้อมูลชนิด pbm แล้ว จะนำข้อมูลภายในแฟ้มข้อมูล ไปถอดรหัสรหัสแท่ง 2 มิติ ซึ่งมีขั้นตอนดังนี้

- นับจำนวนเลข 1 ที่อยู่ที่ติดกันภายในแถบและนับจำนวนเลข 0 ที่อยู่ติดกันภายในแถบ โดยจะนับทีละ 8 แถบ

  ยกตัวอย่าง จากรูปที่ 4.39 นับจำนวนของเลข 1 ในแถบแรกได้ 8 ตัว นับจำนวนของเลข 0 ในแถบถัดมาได้ 4 ตัว และนับจำนวนเลข 1 และเลข 0 ถัดไปเรื่อยๆ จนครบ 8 แถบ จะได้ความกว้างของทั้ง 8 แถบเป็นดังนี้

  4 4 4 12 8 4 7 25

- นำความกว้างของทุกแถบมารวมกัน

  $4 + 4 + 4 + 12 + 8 + 4 + 7 + 25 = 68$

- นำเลข 17 (จำนวนของมอดูลใน 1 คำรหัส) ไปหารผลรวมของความกว้างทุกแถบ เพื่อหาความกว้างของ 1 มอดูล

ความกว้างของ 1 มอดูล = $\frac{68}{17} = 4$

- นำเลขความกว้างของ 1 มอดูลไปหารความกว้างของทุกแถบจะได้ สัดส่วนดังนี้

1 1 1 3 2 1 2 6

พิจารณาว่ารูปแบบแท่งดำและช่องว่างที่ได้ตรงกับคำรหัสใด ในที่นี้รูปแบบแท่งดำและช่องว่าง 1 1 1 3 2 1 2 6 ตรงกับคำรหัส 84 ในกลุ่ม 0

- หาคำรหัสทั้งหมดและเมื่อได้ครบทุกคำรหัสแล้วจึงค่อยแปลงคำรหัสจากเลขฐาน 900 ไปเป็นเลขฐาน 256 ทีละ 5 คำรหัส

ยกตัวอย่างเช่น

ให้คำรหัสที่ได้คือ 84,620,89,74,846 ซึ่งเป็นคำรหัสในรูปเลขฐาน 900 แปลงเป็นเลขฐาน 256 ดังวิธีการต่อไปนี้นี้

หาผลรวมของ $(84,620,89,74,846)_{900}$

$(84,620,89,74,846)_{900} = 84*900^4+620*900^3+89*900^2+74*900^1+846*900^0$

$= 55,564,452,157,446$

เขียนผลรวมของข้อมูลในรูปของเลขฐาน 256 จะได้

$55,564,452,157,446 = (50,137,27,110,216,60)_{256}$

- เมื่อได้เลขฐาน 256 ครบแล้วจะนำเลขแต่ละตัวมาแปลงเป็นเลขฐาน 16 ยกตัวอย่างเช่น

$(33,211,210,108,188,6,48,37,110,\ldots)_{256} = (21D3D26CBC0630256E\ldots)_{16}$

- เลขฐาน 16 ที่ได้ก็คือข้อมูลประจำบัตรลงคะแนนที่ถูกเข้ารหัสลับไว้ ซึ่งจะถูกนำไปถอดรหัสลับต่อไป

กรณีที่ไม่สามารถถอดรหัส รหัสแท่ง 2 มิติได้ ซึ่งอาจจะเกิดจากคำรหัสในรหัสแท่งสกปรกหรือถูกทำลายไปบางส่วน โปรแกรมจะเรียกใช้รหัสรีดโซโลมอนในการแก้ไขเพื่อนำคำรหัสที่ถูกต้องกลับคืนมา โดยรหัสแท่ง 2 มิติ PDF417 จะมีคำรหัสที่ใช้ในการแก้ไขคำรหัสผิดพลาดอยู่ ถ้าจำนวนคำรหัสที่ถูกทำลายไปน้อยกว่าจำนวนคำรหัสที่รหัสรีดโซโลมอนสามารถแก้ไขได้ คำรหัสที่ถูกทำลายจะถูกแก้ไขให้เป็นคำรหัสถูกต้องได้ แต่ถ้าจำนวนคำรหัสที่ถูกทำลายไปมากกว่าจำนวนคำรหัส

ที่รหัสรีดโซโลมอนสามารถแก้ไขได้ จะไม่สามารถนำคำรหัสที่ถูกต้องกลับคืนมาได้ ซึ่งรหัสรีดโซโลมอนที่ถูกเรียกใช้ดัดแปลงมาจากซอฟต์แวร์การแก้ไขข้อมูลผิดพลาดของ Phil Karn [26]

ตัวอย่างของรูปรหัสแท่ง 2 มิติ ที่สกปรกและรหัสรีดโซโลมอนสามารถแก้ไขคำรหัสที่ถูกทำลายให้ถูกต้องได้ แสดงดังรูปที่ 4.40 ซึ่งรหัสแท่ง 2 มิติ จากรูปตัวอย่างมีคำรหัสที่ใช้แก้ไขความผิดพลาดอยู่และสามารถแก้ไขคำรหัสที่ถูกทำลายไปได้ 64 คำรหัส

รูปที่ 4.40 รหัสแท่ง 2 มิติ ที่สามารถใช้รหัสรีดโซโลมอนในการแก้ไขคำรหัสที่ถูกทำลายได้

4.3.11.9 การถอดรหัสลับข้อมูลประจำบัตรลงคะแนน

โปรแกรมจะใช้กุญแจสาธารณะของกรรมการเขต (K_L) ในการถอดรหัสรหัสลับได้ข้อมูลประจำบัตรออกมา ($D_V = N_V; U_{1V}; F_V; H_{4V}$) ซึ่งประกอบด้วย

- เลขประจำบัตร (N_V)
- รหัสเฉพาะ 1 ชั้น (U_{1V})
- คุณลักษณะเฉพาะตัวของกระดาษ (F_V)
- ค่าแฮช (H_{4V})

4.3.11.10 การตรวจสอบข้อมูลประจำบัตรลงคะแนน

โปรแกรมตรวจสอบบัตรลงคะแนน จะตรวจสอบข้อมูลต่อไปนี้

- *ค่าแฮช* (H_{4V}) โปรแกรมจะตรวจสอบความถูกต้องของค่าแฮชด้วยการนำข้อมูลที่ได้จากการถอดรหัสซึ่งได้แก่เลขประจำบัตร (N_V) รหัสเฉพาะ 1 ชั้น (U_{1V}) และคุณลักษณะเฉพาะตัวของกระดาษ (F_V) มาเรียงต่อกัน จากนั้นจะนำไปผ่านแฮชฟังก์ชันแล้วจึงลดขนาดลงเหลือ 4 ไบต์ ($H_{4V} = H_4[N_V; U_{1V}; F_V]$) และนำค่าแฮ

ช 4 ไบต์ ที่ได้ไปเทียบกับค่าแฮชของบัตรที่ได้จากการถอดรหัสว่าตรงกันหรือไม่ นอกจากนี้โปรแกรมยังต้องตรวจสอบว่าค่าแฮชของบัตรลงคะแนนใบนั้นอยู่ในฐานข้อมูลของเขตเลือกตั้งหรือไม่ ขณะตรวจสอบบัตรลงคะแนนหากพบค่าแฮชที่ไม่ได้อยู่ในฐานข้อมูลแสดงว่ากรรมการเขตทุจริตโดยพิมพ์บัตรเลือกตั้งหลายชุดและนำบัตรเลือกตั้งที่ไม่ได้รายงานค่าแฮชไปใช้

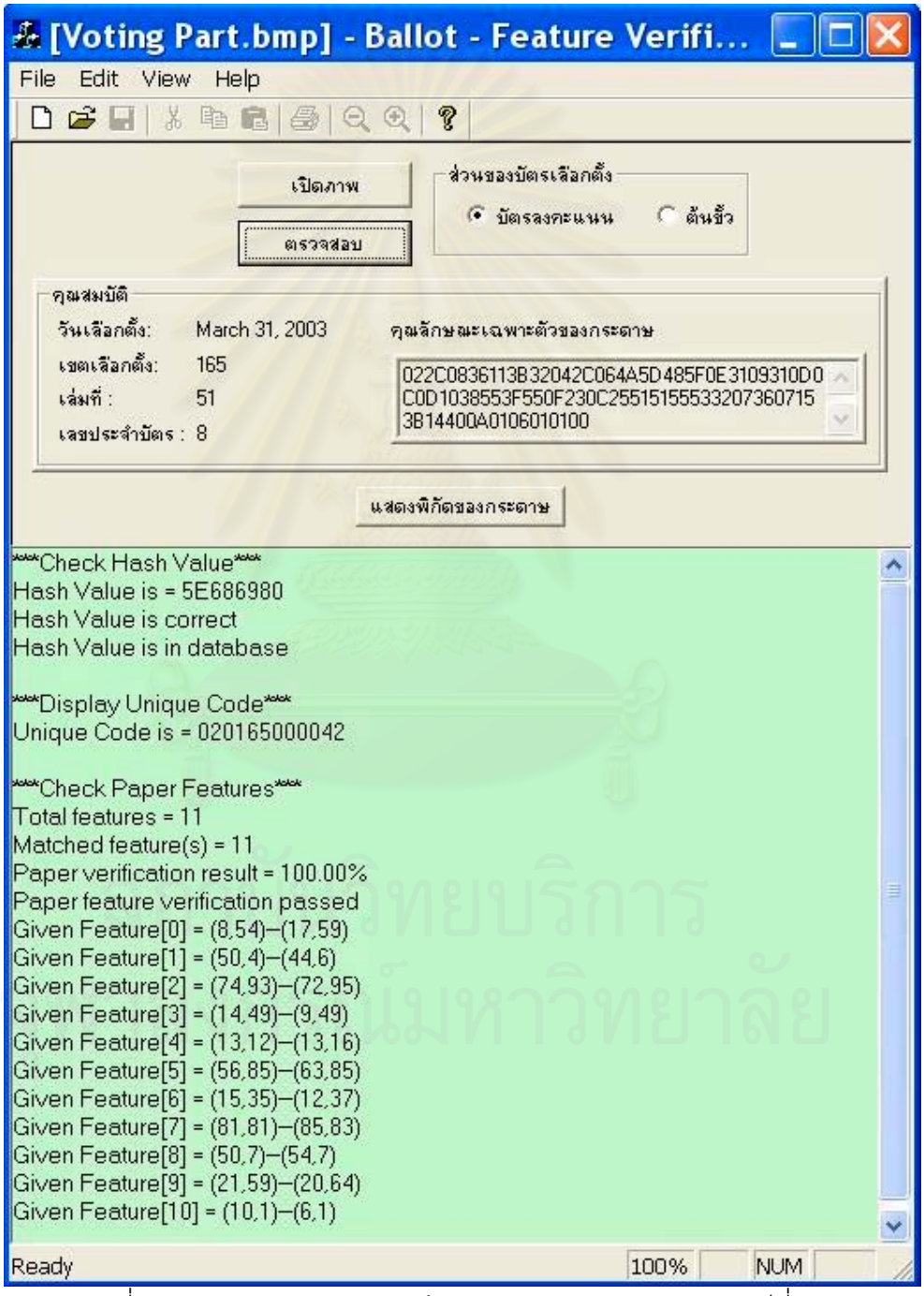
- *คุณลักษณะเฉพาะตัวของกระดาษ* (F_V) โปรแกรมจะนำพิกัดจุดปลายที่ได้จากการถอดรหัสข้อมูลไปเปรียบเทียบกับพิกัดจุดปลายคุณลักษณะเฉพาะตัวของกระดาษบัตรลงคะแนนและตัดสินว่าคุณลักษณะเฉพาะตัวของกระดาษใบนี้ถูกต้องหรือไม่ โดยดูจากจำนวนพิกัดของจุดปลายที่ตรงกันเทียบกับจำนวนพิกัดของจุดปลายทั้งหมด

4.3.11.11 การแสดงผลการตรวจสอบข้อมูลประจำบัตรลงคะแนน

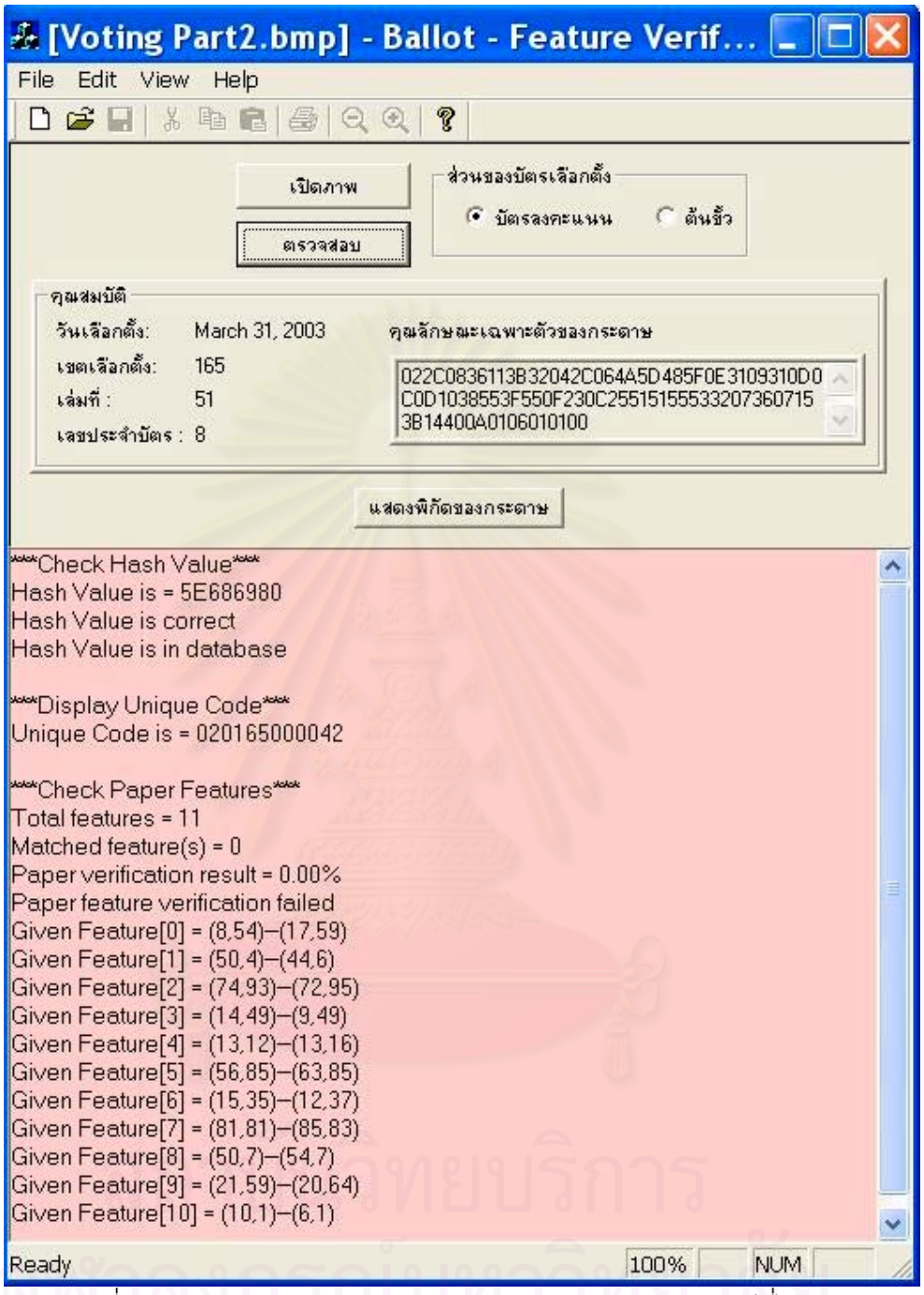
โปรแกรมจะแสดงข้อมูลประจำบัตรลงคะแนน (D_V) และผลการตรวจสอบที่ได้ออกทางหน้าจอของเครื่องไมโครคอมพิวเตอร์ ซึ่งมีลักษณะดังรูปที่ 4.41 เจ้าหน้าที่ประจำเขตจะต้องพิจารณา วันเลือกตั้ง เขตเลือกตั้ง ผลการตรวจสอบค่าแฮช (H_{4V}) และคุณลักษณะเฉพาะตัวของกระดาษ (F_V) ว่าถูกต้องหรือไม่ หากผลการตรวจสอบข้อมูลประจำบัตรลงคะแนนผ่าน เจ้าหน้าที่ประจำเขตจะต้องจดบันทึกค่าแฮชและรหัสเฉพาะที่อ่านได้จากหน้าจอไมโครคอมพิวเตอร์ (H_{4V}, U_V) ลงในบันทึกผลการสุ่มตรวจและเซ็นชื่อกำกับไว้ แต่ถ้าผลการตรวจสอบไม่ผ่านเจ้าหน้าที่ประจำเขตจะต้องพิจารณาว่าข้อมูลใดที่ทำให้ผลการตรวจสอบไม่ผ่าน ถ้าข้อมูลค่าแฮชทำให้ผลการตรวจสอบไม่ผ่าน โดยพบว่าค่าแฮชของบัตรลงคะแนนที่ได้จากการถอดรหัส (H_{4V}) ไม่ตรงกับค่าแฮชที่ได้จากการนำข้อมูลส่วนอื่นๆ ของบัตรมาผ่านแฮชฟังก์ชัน ($H_{4V} = H_4[N_V; U_{1V}; F_V]$) แสดงว่ามีการทุจริตเกิดขึ้น ด้วยการพิมพ์บัตรเลือกตั้งปลอมและนำค่าแฮชที่อยู่ในฐานข้อมูลมาใส่แทนค่าแฮชจริงๆ ของบัตรใบนั้น และถ้าพบว่าค่าแฮชของบัตรลงคะแนนไม่อยู่ในฐานข้อมูลของเขตเลือกตั้ง แสดงว่ากรรมการเขตเลือกตั้งทุจริตโดยพิมพ์บัตรเลือกตั้งหลายชุดและนำบัตรลงคะแนนที่ไม่ได้รายงานค่าแฮชไปใช้ แต่ถ้าข้อมูลคุณลักษณะเฉพาะตัวของกระดาษ (F_V) ทำให้ผลการตรวจสอบไม่ผ่าน ซึ่งอาจจะเกิดขึ้นได้หากบริเวณที่ใช้ดึงคุณลักษณะเฉพาะตัวของกระดาษมีรอยสกปรกอยู่ กรณีนี้เจ้าหน้าที่ประจำเขตสามารถสั่งให้โปรแกรมแสดงพิกัดคุณลักษณะเฉพาะตัวที่ได้จากข้อมูลประจำบัตรลงคะแนนออกทางหน้าจอได้ดังรูปที่ 4.42 หลังจากนั้นเจ้าหน้าที่ประจำเขตจะใช้การมองในการเปรียบเทียบพิกัดคุณ

ลักษณะเฉพาะตัวของกระดาษบนหน้าจอ (F_V) กับพิกัดคุณลักษณะเฉพาะตัวของกระดาษจริงว่าตรงหรือไม่

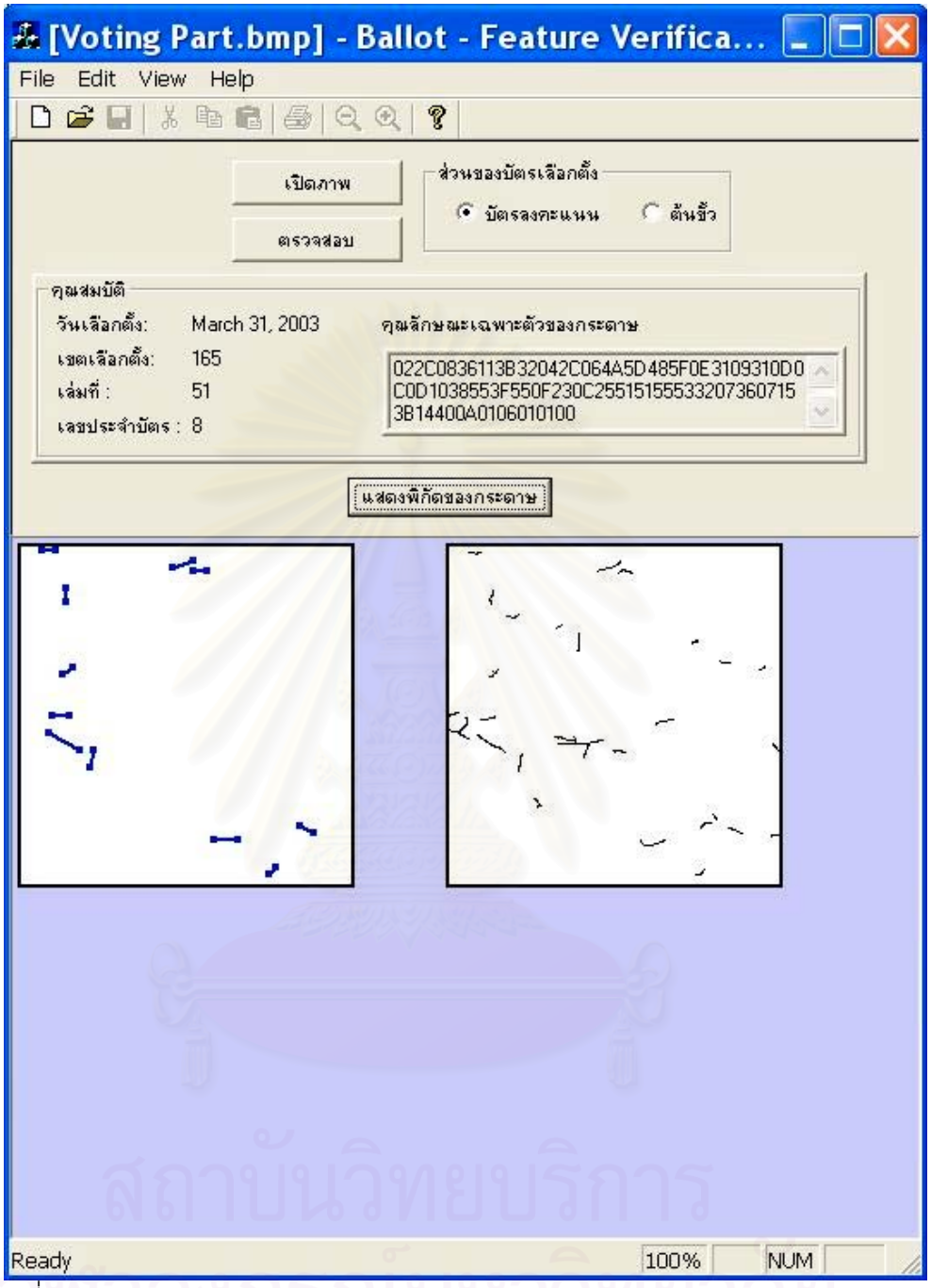
ขณะตรวจสอบบัตรลงคะแนนหากพบบัตรลงคะแนนปลอมจะต้องตรวจสอบบัตรลงคะแนนทุกใบในเขตเลือกตั้งนั้น หากพบจำนวนบัตรลงคะแนนปลอมมากเพียงพอที่จะเปลี่ยนผลการเลือกตั้งได้ จะต้องยกเลิกผลการเลือกตั้งในเขตเลือกตั้งนั้นและจัดให้มีการเลือกตั้งใหม่



รูปที่ 4.41 (ก) ผลการตรวจสอบข้อมูลประจำบัตรลงคะแนน กรณีที่ผ่าน



รูปที่ 4.41 (ข) ผลการตรวจสอบข้อมูลประจำบัตรลงคะแนน กรณีที่ไม่ผ่าน



รูปที่ 4.42 หน้าจอแสดงข้อมูลบัตรลงคะแนนและพิกัดคุณลักษณะเฉพาะตัวของกระดาษ

4.3.12 การตรวจสอบบัตรเลือกตั้งเปล่าที่ยังไม่ได้ใช้และต้นขั้วของบัตรเลือกตั้งที่ใช้แล้ว

เจ้าหน้าที่ประจำหน่วยเลือกตั้งจะต้องส่งต้นขั้วของบัตรเลือกตั้งที่ใช้แล้วกับบัตรเลือกตั้งเปล่าที่ยังไม่ได้ใช้ไปเก็บไว้ที่ที่ว่าการอำเภอเพื่อป้องกันการนำบัตรลงคะแนนของบัตรเลือกตั้งเปล่าที่ยังไม่ได้ใช้ไปสับเปลี่ยนกับบัตรลงคะแนนที่ใช้แล้ว ซึ่งบัตรเลือกตั้งเปล่าที่ยังไม่ได้ใช้และต้นขั้วของบัตรเลือกตั้งที่ใช้แล้วจะถูกตรวจสอบในภายหลังการนับคะแนนเลือกตั้ง

4.3.12.1 การตรวจสอบต้นขั้วของบัตรเลือกตั้งที่ใช้แล้ว

ต้นขั้วของบัตรเลือกตั้งที่ใช้แล้วจะต้องถูกตรวจสอบว่าเป็นต้นขั้วจริงหรือไม่ โดยเจ้าหน้าที่ตรวจสอบจะต้องตรวจสอบ

- *จำนวนต้นขั้วของบัตรเลือกตั้งที่ใช้แล้ว* ซึ่งจะต้องมีจำนวนเท่ากับจำนวนบัตรลงคะแนนของผู้มาใช้สิทธิ์เลือกตั้งในเขตเลือกตั้งนั้น
- *ลายพิมพ์นิ้วมือ* เจ้าหน้าที่ตรวจสอบจะต้องดูลักษณะของลายพิมพ์นิ้วมือบนต้นขั้วว่ามีลักษณะซ้ำกันบ้างหรือไม่ เนื่องจากลายพิมพ์นิ้วมือของแต่ละบุคคลจะลักษณะแตกต่างกัน ดังนั้นถ้าเจ้าหน้าที่ตรวจสอบพบต้นขั้วที่มีลายพิมพ์นิ้วมือซ้ำกันหลายๆ ใบ แสดงว่าเกิดการทุจริตขึ้น และลายพิมพ์นิ้วมือนั้นจะสามารถโยงไปหาผู้ที่กระทำผิดได้
- *คุณลักษณะเฉพาะตัวของกระดาษ* ถ้าเจ้าหน้าที่ประจำหน่วยเลือกตั้งนำบัตรเลือกตั้งปลอมไปให้ผู้มาใช้สิทธิ์เลือกตั้งลงคะแนน แล้วจึงค่อยนำบัตรลงคะแนนจริงซึ่งได้ลงคะแนนให้ผู้สมัครเลือกตั้งคนใดคนหนึ่งไว้ไปสับเปลี่ยนขณะกำลังขนส่งบัตรลงคะแนนไปยังสถานที่นับคะแนน เมื่อบัตรลงคะแนนไปถึงสถานที่นับคะแนน ขณะเจ้าหน้าที่ประจำสถานที่นับคะแนนตรวจสอบบัตรลงคะแนนก็จะพบว่าเป็นบัตรลงคะแนนจริง ทั้งที่ได้มีการสับเปลี่ยนบัตรลงคะแนนระหว่างการขนย้าย ดั้งนั้นจึงต้องมีการตรวจสอบคุณลักษณะเฉพาะตัวของต้นขั้วด้วย ถ้าต้นขั้วที่ตรวจสอบมีคุณลักษณะเฉพาะตัวของกระดาษที่ได้จากการถอดรหัสไม่ตรงกับคุณลักษณะเฉพาะตัวของกระดาษต้นขั้วจริง แต่ลายพิมพ์นิ้วมือเป็นของผู้มาใช้สิทธิ์เลือกตั้งจริงๆ แสดงว่าเจ้าหน้าที่ประจำหน่วยทุจริตนำบัตรเลือกตั้งปลอมไปให้ผู้มาใช้สิทธิ์เลือกตั้งลงคะแนน

สำหรับการตรวจสอบคุณลักษณะเฉพาะตัวของต้นขั้วจะต้องใช้แฟ้มข้อมูลและทรัพยากรดังนี้

วัตถุ :ต้นขั้วของบัตรเลือกตั้งที่ใช้แล้ว

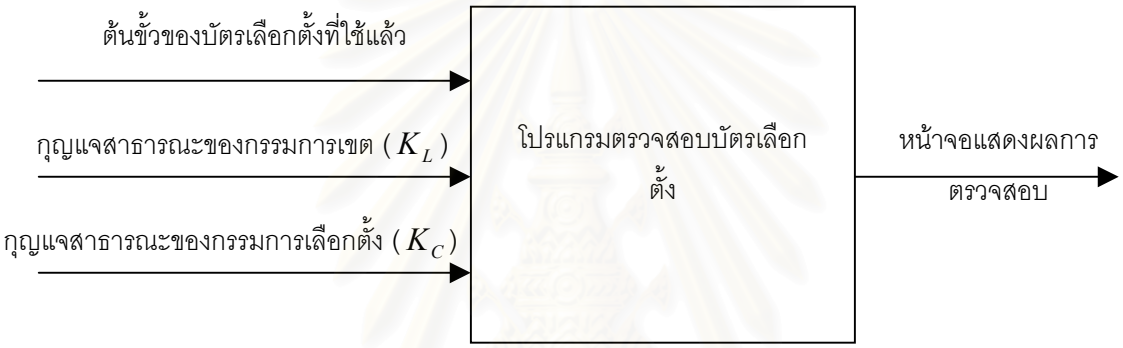
แฟ้มข้อมูล :กุญแจสาธารณะของกรรมการเขตและกรรมการเลือกตั้ง (K_L, K_C)

ฮาร์ดแวร์ :ไมโครคอมพิวเตอร์และกล้องประจำเครื่องคอมพิวเตอร์ส่วนบุคคล

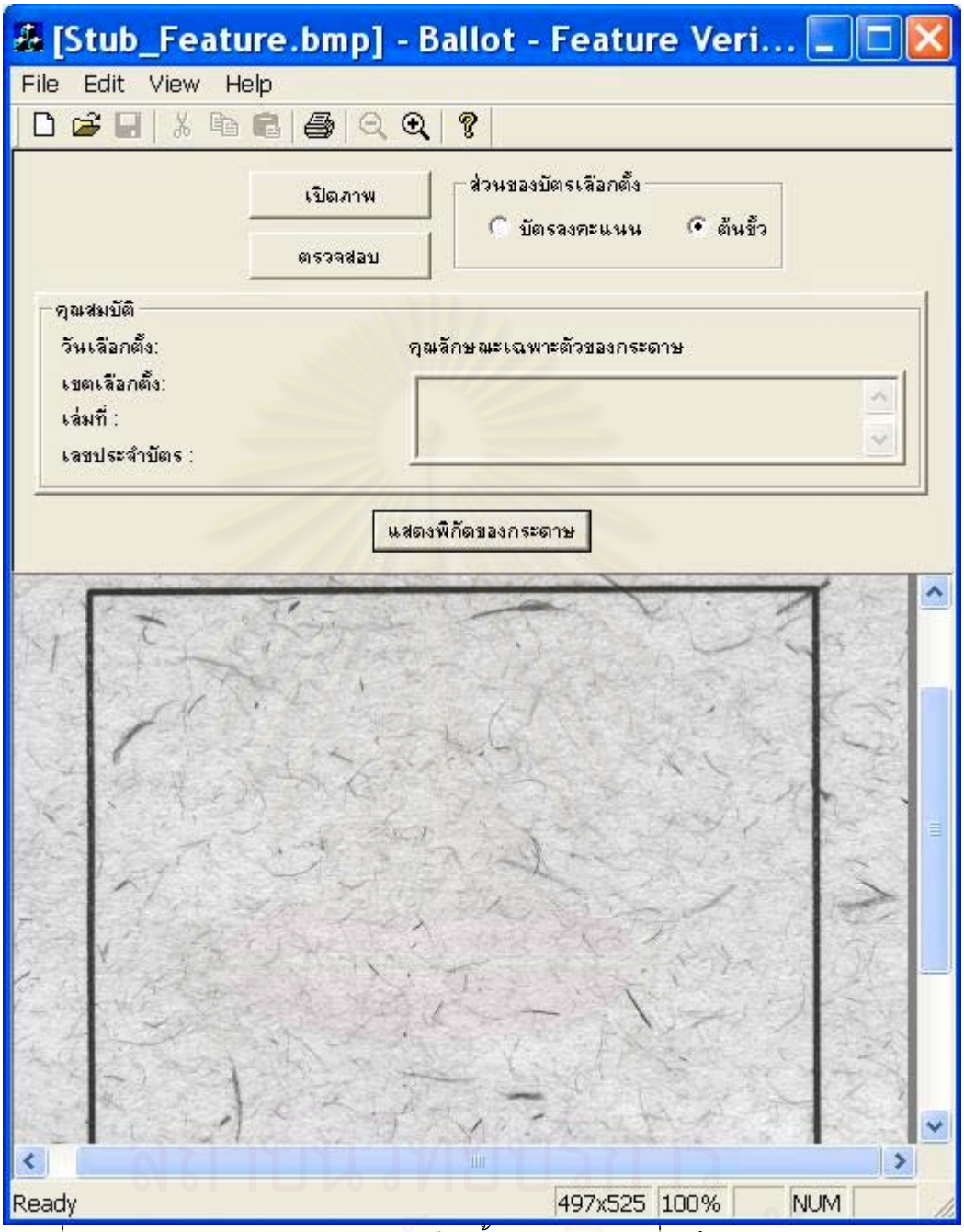
ซอฟต์แวร์ :โปรแกรมตรวจสอบบัตรเลือกตั้ง (ดูได้ดังรูปที่ 4.44)

ผู้ปฏิบัติการ :เจ้าหน้าที่ตรวจสอบ

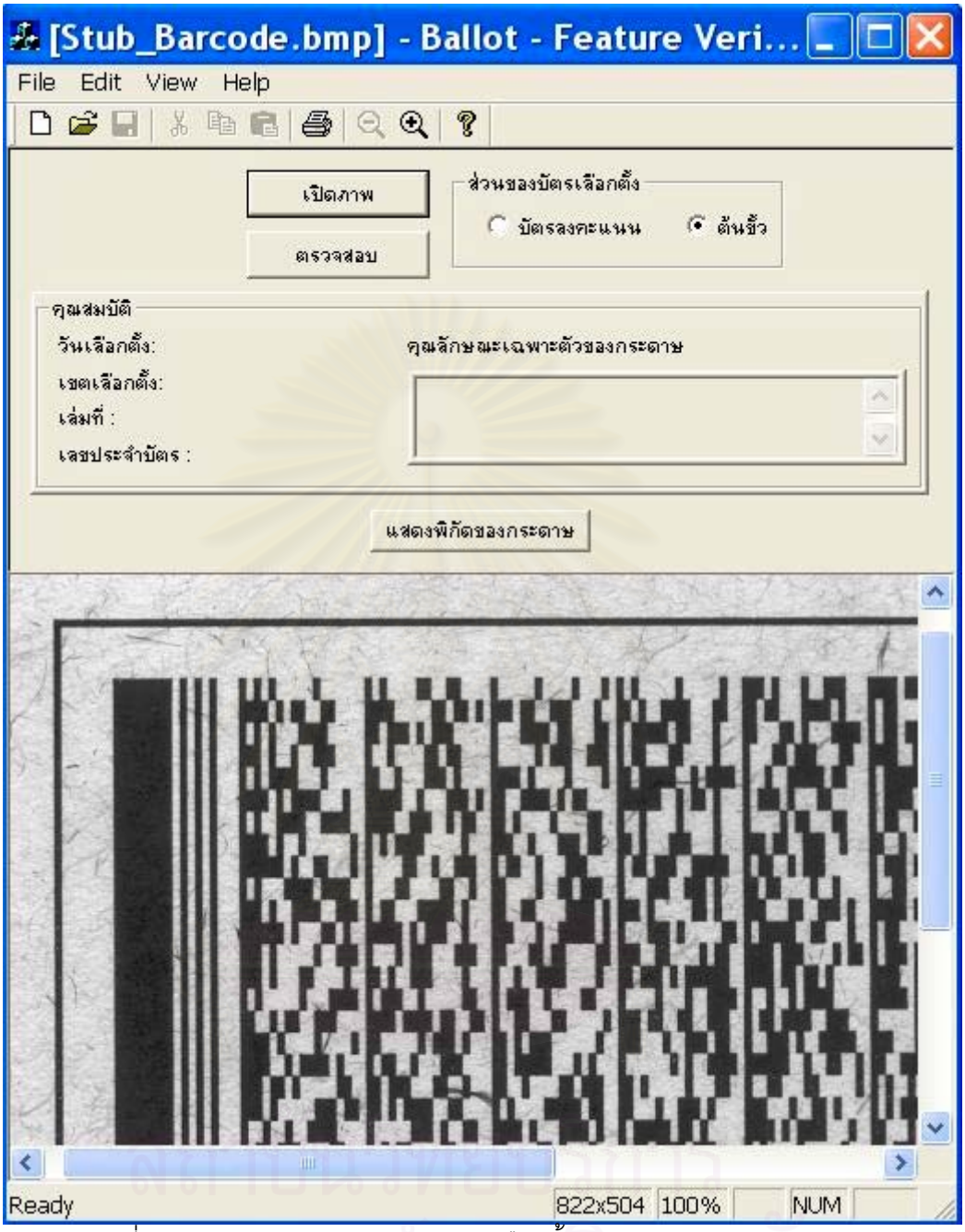
ผลลัพธ์ที่ได้ :หน้าจอแสดงผลการตรวจสอบความถูกต้องของต้นขั้ว



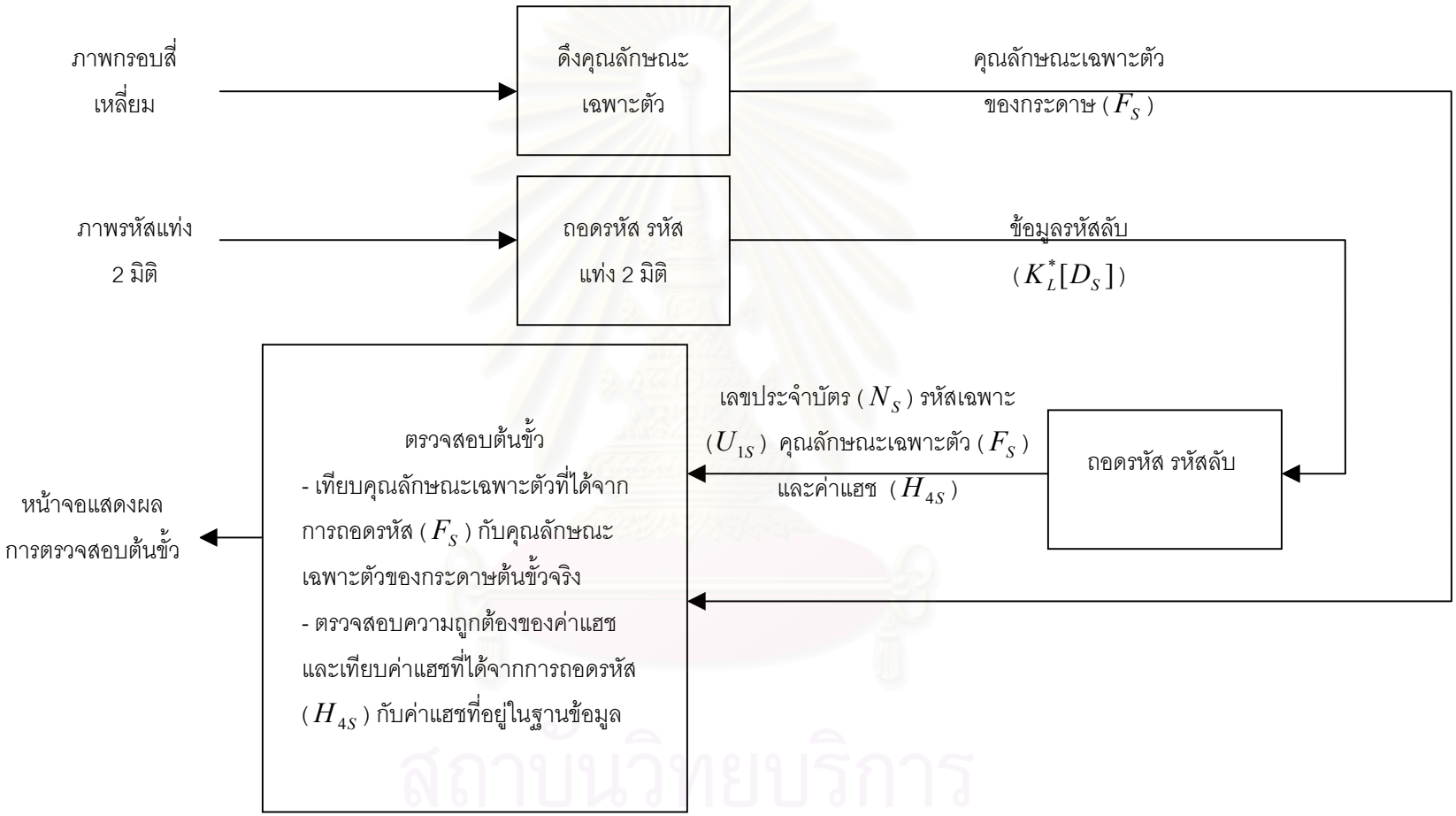
รูปที่ 4.43 การตรวจสอบต้นขั้วของบัตรเลือกตั้งที่ใช้แล้ว



รูปที่ 4.44 (ก) โปรแกรมตรวจสอบบัตรเลือกตั้งขณะเปิดภาพที่ใช้ดึงคุณลักษณะเฉพาะตัว



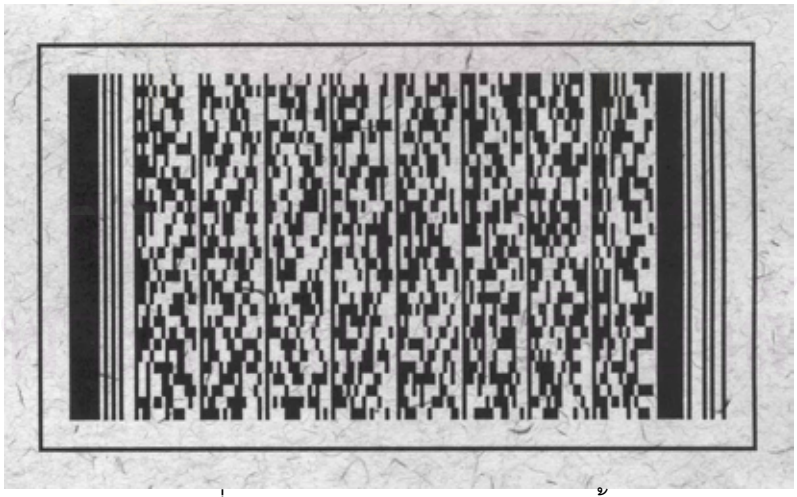
รูปที่ 4.44 (ข) โปรแกรมตรวจสอบบัตรเลือกตั้งขณะเปิดภาพรหัสแท่ง 2 มิติ



รูปที่ 4.45 แผนผังการทำงานของโปรแกรมตรวจสอบต้นขั้วของบัตรเลือกตั้งที่ใช้แล้ว

สำหรับรายละเอียดขั้นตอนการตรวจสอบต้นขั้วของบัตรเลือกตั้งที่ใช้ไปแล้ว สามารถแสดงได้ดังรูปที่ 4.45 ซึ่งขั้นตอนดังกล่าวจะมีบางขั้นตอนที่ซ้ำกับการตรวจสอบบัตรลงคะแนน ณ สถานที่นับคะแนนอยู่ ในที่นี้จึงขอกล่าวเฉพาะขั้นตอนที่แตกต่างจากการตรวจสอบบัตรลงคะแนน ซึ่งก็คือ ขั้นตอนการเก็บภาพต้นขั้ว โดยจะใช้กล้องประจำเครื่องคอมพิวเตอร์ส่วนบุคคลถ่ายภาพต้นขั้ว 2 ครั้ง โดยครั้งแรกถ่ายภาพบริเวณกรอบสี่เหลี่ยมที่ใช้ดึงคุณลักษณะเฉพาะตัวของต้นขั้วและครั้งที่ 2 ถ่ายภาพบริเวณรหัสแท่ง 2 มิติ บนต้นขั้ว ดังรูปที่ 4.46 จากนั้นจึงบันทึกภาพเป็นแฟ้มข้อมูลในรูปแบบ bitmap (bmp) แบบสเกลสีเทา

รูปที่ 4.46 (ก) บริเวณที่ใช้ดึงคุณลักษณะเฉพาะตัวของต้นขั้ว



รูปที่ 4.46 (ข) รหัสแท่ง 2 มิติ ของต้นขั้ว

หลังจากที่ได้ภาพของต้นขั้วบัตรเลือกตั้งทั้ง 2 ส่วนแล้วเจ้าหน้าที่ตรวจสอบจะเปิดภาพทั้ง 2 โดยครั้งแรกเปิดภาพบริเวณที่ใช้ดึงคุณลักษณะเฉพาะตัวก่อนซึ่งแสดงได้ดังรูปที่ 4.44 (ก) และครั้งที่ 2 จะเปิดภาพรหัสแท่ง 2 มิติ ซึ่งแสดงได้ดังรูปที่ 4.44 (ข) หลังจากนั้นเจ้าหน้าที่ตรวจสอบจะสั่งให้โปรแกรมตรวจสอบ ซึ่งจะใช้วิธีการเดียวกันกับการตรวจสอบบัตรลงคะแนน โดยเริ่มจากขั้นตอนในหัวข้อที่ 4.3.11.3 จนถึงหัวข้อที่ 4.3.11.11 และผลการตรวจสอบต้นขั้วของบัตรลงคะแนนก็จะมีลักษณะดังรูปที่ 4.41 และ 4.42

4.3.12.2 การตรวจสอบบัตรเลือกตั้งเปล่าที่ยังไม่ได้ใช้

บัตรเลือกตั้งเปล่าที่ยังไม่ได้ใช้จะต้องถูกตรวจสอบด้วย โดยเจ้าหน้าที่ตรวจสอบสามารถเลือกตรวจสอบเพียงต้นขั้วหรือบัตรลงคะแนนของบัตรเลือกตั้งใบนั้นก็ได้ เนื่องจากทั้ง 2 ส่วนติดกันอยู่ ถ้าส่วนหนึ่งเป็นของจริงอีกส่วนก็ต้องเป็นของจริงด้วย

สำหรับวิธีการตรวจสอบนั้นสามารถใช้โปรแกรมตรวจสอบบัตรเลือกตั้งในการตรวจสอบได้ ซึ่งใช้วิธีการตรวจสอบเช่นเดียวกันกับการตรวจสอบบัตรลงคะแนนในหัวข้อ 4.3.11 และการตรวจสอบต้นขั้วในหัวข้อ 4.3.12.1

ขณะตรวจสอบต้นขั้วของบัตรเลือกตั้งที่ใช้แล้วหรือบัตรเลือกตั้งที่ยังไม่ได้ใช้ ถ้าพบต้นขั้วของบัตรเลือกตั้งที่ใช้แล้วปลอมหรือบัตรเลือกตั้งเปล่าที่ยังไม่ได้ใช้ปลอม จะต้องตรวจสอบต้นขั้วหรือบัตรเลือกตั้งเปล่าที่ยังไม่ได้ใช้ทั้งเขตเลือกตั้งซึ่งถ้าตรวจสอบแล้วพบจำนวนต้นขั้วหรือบัตรเลือกตั้งเปล่าที่ยังไม่ได้ใช้ปลอมจำนวนมาก กรรมการเลือกตั้งสามารถยกเลิกผลการเลือกตั้งในเขตเลือกตั้งนั้นๆ ได้

4.4 การทดสอบการป้องกันการปลอมแปลงและทุจริต

ในงานวิจัยนี้ได้ทดสอบนำบัตรเลือกตั้งปลอมที่ได้จากการคัดลอกข้อมูลชุดรหัสลับ ($K_L^*[D]$) จากบัตรเลือกตั้งจริงไปยังบัตรเลือกตั้งปลอม, บัตรเลือกตั้งที่ใช้รหัสเฉพาะ (U) ซ้ำกัน และบัตรเลือกตั้งที่ไม่ได้ส่งค่าแฮช (H_4) ไปในแฟ้มข้อมูลรายการจัดพิมพ์ ($K_P[H_4;U_1]$) มาตรวจสอบโดยใช้โปรแกรมตรวจสอบบัตรเลือกตั้ง พบว่าการทุจริตด้วยวิธีการดังกล่าวข้างต้นสามารถตรวจพบได้

4.5 การประเมินระบบการจัดพิมพ์บัตรเลือกตั้งที่ได้ออกแบบในงานวิจัยนี้

ในหัวข้อนี้ จะกล่าวถึงวิธีการประเมินระบบการจัดพิมพ์บัตรเลือกตั้งแบบกระจายศูนย์ว่าสามารถจัดพิมพ์บัตรเลือกตั้งจำนวนมากเสร็จทันกำหนดเวลาหรือไม่ และมีความปลอดภัยต่อการปลอมแปลงและทุจริตมากน้อยแค่ไหน ซึ่งมีรายละเอียดดังนี้

4.5.1 การประเมินในเรื่องการจัดพิมพ์บัตรเลือกตั้งจำนวนมากเสร็จภายในระยะเวลาที่กำหนด

สำหรับวิธีการประเมินว่าระบบการจัดพิมพ์บัตรเลือกตั้งแบบกระจายศูนย์ที่ใช้ในงานวิจัยนี้สามารถจัดพิมพ์บัตรเลือกตั้งจำนวนมากถึง 160 ล้านใบ เสร็จภายในระยะเวลาที่จำกัดเพียง 1 เดือนหรือไม่ สามารถทำได้โดยการทดสอบจับเวลาที่ใช้ในการจัดพิมพ์บัตรเลือกตั้งจำนวน 100 ใบ สำหรับเครื่องพิมพ์ที่ใช้ในการทดสอบได้แก่เครื่องพิมพ์รุ่น HP-2200DN ของ Hewlett packard และใช้ไมโครคอมพิวเตอร์รุ่น Pentium-4 ของ Intel ซึ่งมีความเร็วในการประมวลผล 2 กิกะเฮิรตซ์ เมื่อลองจับเวลาที่ใช้ในการจัดพิมพ์บัตรเลือกตั้งทั้ง 100 ใบ ได้ผลการทดสอบดังนี้

ตารางที่ 4.4 เวลาที่ใช้ในการจัดพิมพ์บัตรเลือกตั้ง

การจัดพิมพ์บัตรเลือกตั้ง	เวลาที่ใช้ในการจัดพิมพ์
ทดสอบจัดพิมพ์บัตรเลือกตั้ง 100 ใบ	12-13 นาที
คำนวณเวลาที่ใช้จัดพิมพ์บัตรเลือกตั้ง 40,000 ใบ	ประมาณ 5,200 นาที ประมาณ 87 ชั่วโมง ประมาณ 9 วัน (พิมพ์วันละ10 ชั่วโมง)

จากผลการทดสอบจับเวลาที่ใช้ในการพิมพ์บัตรเลือกตั้ง 100 ใบ สามารถนำไปคำนวณเวลาที่ใช้ในการจัดพิมพ์บัตรเลือกตั้ง 40,000 ใบได้ (จำนวนบัตรเลือกตั้งที่เครื่องพิมพ์แต่ละเครื่องในเขตเลือกตั้งจะต้องจัดพิมพ์ ถ้าในเขตเลือกตั้งนั้นใช้เครื่องพิมพ์ทั้งหมด 10 เครื่อง) ซึ่งจะต้องใช้เวลาในการจัดพิมพ์ประมาณ 9 วัน จึงสามารถประเมินได้ว่าวิธีการจัดพิมพ์บัตรเลือกตั้งแบบกระจายศูนย์สามารถจัดพิมพ์บัตรเลือกตั้งเสร็จทันเวลาที่กำหนดไว้

4.5.2 การประเมินในเรื่องความปลอดภัยต่อการปลอมแปลงและทุจริตของระบบการจัดพิมพ์บัตรเลือกตั้งที่ได้ออกแบบ

สำหรับการประเมินในเรื่องความปลอดภัยต่อการปลอมแปลงและทุจริตของระบบการจัดพิมพ์บัตรเลือกตั้งแบบกระจายศูนย์ที่ได้นำเสนอในงานวิจัยนี้ สามารถพิจารณาได้จากองค์ประกอบต่างๆ ที่นำมาใช้ป้องกันการปลอมแปลงและทุจริต ซึ่งได้แก่ การเข้ารหัสลับแบบกุญแจสาธารณะด้วยวิธี RSA, ระบบต้นขั้ว, การนำข้อมูลคุณลักษณะเฉพาะตัวของกระดาษบัตรเลือกตั้ง (F) มาใช้เป็นข้อมูลส่วนหนึ่งประจำบัตรเลือกตั้ง และการนำรหัสเฉพาะ (U) กับค่าแฮช (H_4) มาใช้ป้องกันกรรมการ

เขตทุจริต ซึ่งสามารถวิเคราะห์ระดับความปลอดภัยขององค์ประกอบต่างๆ ที่นำมาใช้แต่ละอย่างได้ดังนี้

1. *การนำวิธีการเข้าลับแบบกุญแจสาธารณะด้วยวิธี RSA มาใช้* สำหรับความปลอดภัยของการเข้ารหัสลับแบบกุญแจสาธารณะขึ้นอยู่กับความยาวของกุญแจที่นำมาใช้ และระยะเวลาที่ผู้ทุจริตต้องใช้ในการคำนวณหากุญแจส่วนตัวจากกุญแจสาธารณะ ในปัจจุบันความยาวของกุญแจที่ได้รับการยอมรับว่ามีความปลอดภัยสูงได้แก่ความยาวของกุญแจขนาด 128 ไบต์ [27] ในระบบการจัดพิมพ์บัตรเลือกตั้งที่ได้ออกแบบในงานวิจัยนี้กุญแจที่มีความสำคัญมากที่สุดสำหรับการทุจริตได้แก่ กุญแจส่วนตัวของกรรมการเขต (K_L^*) ที่ใช้ในขั้นตอนการเข้ารหัสลับข้อมูลประจำบัตรเลือกตั้ง ($K_L^*[D]$) ซึ่งในงานวิจัยนี้ได้กำหนดให้กุญแจของกรรมการเขตมีขนาด 68 ไบต์ ที่ความยาวของกุญแจดังกล่าวในปัจจุบันจะต้องใช้เวลาในการคำนวณหากุญแจส่วนตัวจากกุญแจสาธารณะไม่ต่ำกว่า 1 เดือน ซึ่งกรรมการเขตอาจจะประกาศกุญแจสาธารณะ (K_L) ของตนให้เจ้าหน้าที่ประจำหน่วยทราบเพื่อใช้ในขั้นตอนการสุ่มตรวจบัตรเลือกตั้งก่อนวันเลือกตั้งเพียงไม่กี่วันก็ได้ เพื่อลดจำนวนเวลาที่ผู้ที่ต้องการทุจริตสามารถใช้ในการคำนวณหากุญแจส่วนตัวของกรรมการเขต (K_L^*) และถึงแม้ว่าผู้ที่ต้องการทุจริตจะสามารถคำนวณหากุญแจส่วนตัวของกรรมการเขตได้ (K_L^*) ก็ยังไม่สามารถนำกุญแจส่วนตัวของกรรมการเขต (K_L^*) ที่คำนวณได้ไปใช้ทันที เนื่องจากผู้ที่ต้องการทุจริตจะต้องมีโปรแกรมพิมพ์บัตรเลือกตั้ง และแฟ้มข้อมูลรหัสเฉพาะ (U_2) ที่กรรมการเลือกตั้งได้ส่งไปให้กรรมการเขตด้วยเพื่อใช้ในขั้นตอนการพิมพ์บัตรเลือกตั้ง

จากความยาวกุญแจของกรรมการเขตและระยะเวลาที่ผู้ต้องการทุจริตต้องใช้ในการคำนวณหากุญแจส่วนตัวของกรรมการเขต (K_L^*) จากกุญแจสาธารณะของกรรมการเขต (K_L) มีน้อยมาก จึงทำให้ผู้ต้องการทุจริตมีโอกาสที่จะกระทำการทุจริตได้ยาก

สำหรับความยาวกุญแจของกรรมการเลือกตั้ง, กรรมการเขต และโปรแกรม ที่ใช้ในงานวิจัยนี้สามารถเปลี่ยนแปลงได้ ขึ้นอยู่กับว่าในขณะที่มีการเลือกตั้งครั้งนั้น ความยาวของกุญแจขนาดเท่าไหร่ที่ได้รับการยอมรับว่ามีความปลอดภัยสูง

2. *ระบบต้นขั้ว* การนำระบบต้นขั้วมาใช้กับบัตรเลือกตั้งจะช่วยป้องกันการทุจริตด้วยการลงคะแนนแทนผู้อื่นได้ เนื่องจากผู้มาใช้สิทธิ์เลือกตั้งจะต้องพิมพ์ลายนิ้วมือของตนเองลงบนต้นขั้วของบัตรเลือกตั้ง ซึ่งลายพิมพ์นิ้วมือของแต่ละบุคคลจะแตกต่างกันไป ทำให้บุคคลหนึ่งไม่สามารถลงคะแนนแทนอีกบุคคลได้ ดังนั้นระดับความปลอดภัยของการนำระบบต้นขั้วมาใช้ขึ้นอยู่กับโอกาสที่ผู้มาใช้สิทธิ์จะมีลายพิมพ์นิ้วมือตรงกับผู้ที่ต้องการทุจริต ซึ่งลายพิมพ์นิ้วมือของแต่ละบุคคลจะแตกต่างกัน จึงมีโอกาสที่ผู้ที่ต้องการทุจริตจะสามารถทุจริตได้น้อยมาก

3. *การนำข้อมูลคุณลักษณะเฉพาะตัวของกระดาษบัตรเลือกตั้งมาใช้เป็นข้อมูลส่วนหนึ่งของบัตรเลือกตั้ง* ถ้าผู้ที่ต้องการทุจริตสามารถหากระดาษบัตรเลือกตั้งซึ่งมีคุณลักษณะเฉพาะตัวของกระดาษตรงกับข้อมูลคุณลักษณะเฉพาะตัวของกระดาษบัตรลงคะแนน (F) ได้ก็จะสามารถทุจริตได้โดยการคัดลอกข้อมูลรหัสลับ ($K_L^*[D]$) จากบัตรเลือกตั้งจริงไปยังบัตรเลือกตั้งปลอมที่ข้อมูล คุณลักษณะเฉพาะตัวของกระดาษ (F) ตรงกัน และการทุจริตด้วยวิธีดังกล่าวจะไม่สามารถจับการทุจริตได้ ดังนั้นระดับความปลอดภัยของการนำข้อมูลคุณลักษณะเฉพาะตัวของกระดาษ (F) มาใช้จึงขึ้นอยู่กับจำนวนของคู่พิกัดคุณลักษณะเฉพาะตัวของกระดาษที่ใช้ ถ้าใช้จำนวนคู่พิกัดคุณลักษณะเฉพาะตัวของกระดาษจำนวนมาก ก็จะเป็นไปได้ยากที่จะหากระดาษ 2 ใบ ที่มีข้อมูลคุณลักษณะเฉพาะตัวของกระดาษตรงกัน ซึ่งมีตัวอย่างการคำนวณดังนี้

ในงานวิจัยนี้ได้ใช้จำนวนคู่พิกัดคุณลักษณะเฉพาะตัวของกระดาษประมาณ 11 คู่พิกัด ซึ่งคู่พิกัดทั้ง 11 คู่ อยู่บนบริเวณที่ใช้ดึงคุณลักษณะเฉพาะตัวของกระดาษซึ่งมีความกว้าง 100 หน่วย และ ความยาว 100 หน่วย ซึ่ง 1 คู่พิกัด จะมีรูปแบบที่เป็นไปได้ทั้งหมด

$$C_2^{10,000} = \frac{10,000!}{9,998!*2!} = 49,995,000 \text{ รูปแบบ}$$

ดังนั้นรูปแบบของคู่พิกัดทั้ง 11 คู่ที่เป็นไปได้ทั้งหมดจะมีมากถึง $\frac{49,995,000^{11}}{11!}$ รูปแบบ จึงทำให้โอกาสที่คุณลักษณะเฉพาะตัวของกระดาษบัตรเลือกตั้ง 1 ใบ ซึ่งมีอยู่ 1 รูปแบบจะไปซ้ำกับคุณลักษณะเฉพาะตัวของกระดาษบัตรเลือกตั้งใบอื่นๆ จึงน้อยมาก

4. *การนำรหัสเฉพาะกับค่าแฮชมาใช้เป็นข้อมูลส่วนหนึ่งของบัตรเลือกตั้ง* ถ้าผู้ที่ต้องการทุจริตสามารถหาบัตรลงคะแนนที่มีข้อมูลรหัสเฉพาะ (U) กับค่าแฮช (H_4) ตรงกันกับบัตรลงคะแนนที่ส่งไปยังสถานที่นับคะแนนได้ก็จะสามารถทุจริตโดยการสับเปลี่ยนบัตรลงคะแนนได้ ซึ่งโอกาสที่รหัสเฉพาะ (U) กับค่าแฮช (H_4) ของบัตรลงคะแนนใบหนึ่งจะไปซ้ำกับรหัสเฉพาะ (U) กับค่าแฮช (H_4) ของบัตรลงคะแนนอีกใบหนึ่งมีน้อยมาก เนื่องจากค่าแฮชของบัตรลงคะแนน (H_4) ได้จากการนำรหัสเฉพาะ 1 ชั้น, เลขประจำบัตร และข้อมูลคุณลักษณะเฉพาะตัวของกระดาษไปผ่านแฮชฟังก์ชันแล้วจึงลดขนาดลงเหลือ 4 ไบต์ ($H_4 = H_4[N;U_1;F]$) ซึ่งถึงแม้ว่ารหัสเฉพาะ 1 ชั้น (U_1) ของบัตรจะซ้ำกัน แต่เมื่อนำไปรวมกับข้อมูลอื่นๆ ก็จะทำให้ค่าแฮชที่ได้ (H_4) แตกต่างกัน จึงมีโอกาสที่ผู้ทุจริตจะสามารถทุจริตด้วยวิธีดังกล่าวน้อยมาก

จากองค์ประกอบต่างๆ ที่นำมาใช้ป้องกันการปลอมแปลงและทุจริตข้างต้น จะเห็นว่าโอกาสที่ผู้ที่ต้องการทุจริตจะสามารถกระทำการทุจริตโดยใช้องค์ประกอบต่างๆ ข้างต้นได้ มีน้อยมาก

จึงสามารถประเมินได้ว่าระบบการจัดพิมพ์และตรวจสอบบัตรเลือกตั้งที่ได้ออกแบบไว้ในงานวิจัยนี้มีความปลอดภัยต่อการปลอมแปลงและทุจริตสูง

บทที่ 5

บทสรุปและข้อเสนอแนะ

5.1 สรุปผลการวิจัย

วิทยานิพนธ์ฉบับนี้ได้นำเสนอวิธีการจัดพิมพ์บัตรเลือกตั้งที่ได้นำวิธีการเข้ารหัสลับแบบกุญแจสาธารณะมาใช้เพื่อป้องกันการปลอมแปลง โดยได้ออกแบบระบบการจัดพิมพ์บัตรเลือกตั้งแบบกระจายศูนย์ซึ่งแต่ละเขตเลือกตั้งจะดูแลระบบการจัดพิมพ์ภายในเขตของตนให้จัดพิมพ์เสร็จทันกำหนดเวลาและกรรมการเลือกตั้งได้นำรหัสเฉพาะ (U) และค่าแฮช (H_4) มาใช้เป็นข้อมูลส่วนหนึ่งของข้อมูลประจำบัตรเลือกตั้ง $(D = N; U_1; F; H_4)$ เพื่อป้องกันกรรมการเขตทุจริตด้วยการพิมพ์บัตรเลือกตั้งหลายชุดแล้วบัตรเลือกตั้งที่พิมพ์เกินมาสับเปลี่ยนในภายหลังได้ นอกจากนี้ในงานวิจัยนี้ยังได้ออกแบบบัตรเลือกตั้งให้เหมาะสมกับระบบการจัดพิมพ์และตรวจสอบ รวมทั้งพัฒนาและปรับปรุงโปรแกรมบนเครื่องไมโครคอมพิวเตอร์เพื่อใช้ในระบบการจัดพิมพ์และตรวจสอบเลือกตั้ง ซึ่งโปรแกรมบนเครื่องไมโครคอมพิวเตอร์ที่งานวิจัยนี้ได้พัฒนาและปรับปรุงได้แก่ โปรแกรมสร้างกุญแจ, โปรแกรมสร้างรหัสเฉพาะ, โปรแกรมพิมพ์บัตรเลือกตั้ง และโปรแกรมตรวจสอบบัตรเลือกตั้ง

5.2 สิ่งที่งานวิจัยนี้ได้พัฒนาและปรับปรุงจากงานวิจัยก่อนหน้านี้

วิทยานิพนธ์ของ ศิริพงษ์ ประยูรหงษ์ เรื่อง “การเข้ารหัสลับบนบัตรเลือกตั้งเพื่อป้องกันการปลอมแปลงและทุจริต” [1] ได้เสนอวิธีการนำการเข้ารหัสลับแบบกุญแจสาธารณะมาใช้กับบัตรเลือกตั้งเพื่อป้องกันการปลอมแปลงและทุจริต ซึ่งวิธีการดังกล่าวสามารถนำมาใช้ป้องกันการปลอมแปลงบัตรเลือกตั้งได้และมีข้อดีคือ ใช้ต้นทุนในการจัดพิมพ์ไม่สูงมากนักและการตรวจสอบสามารถทำได้ง่าย แต่เมื่อจะนำวิธีการดังกล่าวมาใช้ในทางปฏิบัติจะมีปัญหาในเรื่องการจัดพิมพ์ เนื่องจากระหว่างขั้นตอนการจัดพิมพ์บัตรเลือกตั้งจะต้องเสียเวลาในขั้นตอนการสแกนกระดาษบัตรเลือกตั้ง, การเข้ารหัสข้อมูลประจำบัตรเลือกตั้ง $(K_L^*[D])$ และการพิมพ์รหัสลับลงบนบัตรเลือกตั้งในรูปแบบรหัสแท่ง 2 มิติ ซึ่งบัตรเลือกตั้งที่ต้องจัดพิมพ์มีจำนวนมากถึง 160 ล้านใบ และต้องจัดพิมพ์ให้เสร็จภายในระยะเวลาที่จำกัด ซึ่งงานวิจัยของ ศิริพงษ์ ประยูรหงษ์ เป็นต้นแบบของการนำการเข้ารหัสลับแบบกุญแจสาธารณะมาใช้กับบัตรเลือกตั้ง จึงไม่ได้คำนึงถึงปัญหาในเรื่องการจัดพิมพ์บัตรเลือกตั้งอย่างที่ได้กล่าวมาข้างต้น วิทยานิพนธ์ฉบับนี้จึงได้นำเสนอวิธีการจัดพิมพ์บัตรเลือกตั้งที่ได้นำการเข้ารหัสลับแบบกุญแจสาธารณะมาใช้ ให้จัดพิมพ์เสร็จอย่างรวดเร็วทันเวลา รวมทั้งหาทางป้องกันการทุจริตจากบุคคลที่มีส่วนเกี่ยวข้องกับบัตร ซึ่งสิ่งที่งานวิจัยนี้ได้พัฒนาและปรับปรุงจากงานวิจัยของ ศิริพงษ์ ประยูรหงษ์ มีดังนี้

1. *การออกแบบระบบการจัดพิมพ์แบบกระจายศูนย์และการตรวจสอบบัตรเลือกตั้ง* ในงานวิจัยนี้ได้ออกแบบระบบการจัดพิมพ์แบบกระจายศูนย์เพื่อให้สามารถจัดพิมพ์บัตรเลือกตั้งเสร็จทันเวลาที่กำหนด และหาวิธีป้องกันกรรมการเขตทุจริตด้วยการพิมพ์บัตรเลือกตั้งหลายชุดแล้วนำบัตรเลือกตั้งที่พิมพ์เกินมาสับเปลี่ยนในภายหลัง โดยในงานวิจัยนี้ได้นำรหัสเฉพาะ (U) และค่าแฮช (H_4) มาใช้ เพื่อป้องกันกรรมการเขตทุจริต

2. *การออกแบบลักษณะของบัตรเลือกตั้งให้เหมาะสมกับระบบการจัดพิมพ์และตรวจสอบ* ในงานวิจัยของ ศิริพงษ์ ประยูรหงษ์ ได้นำรหัสแท่ง 1 มิติมาใช้ในขั้นตอนการพิมพ์รหัสลับลงบนบัตรเลือกตั้ง เพื่อช่วยให้การตรวจสอบทำได้สะดวก แต่เนื่องจากกระดาษที่ใช้พิมพ์บัตรเลือกตั้งมีเส้นใยหรือเศษผงฝังอยู่จึงอาจจะทำให้เครื่องอ่านรหัสแท่ง 1 มิติ ไม่สามารถอ่านรหัสแท่ง 1 มิติได้ ในงานวิจัยนี้จึงได้นำรหัสแท่ง 2 มิติมาใช้ โดยจะพิมพ์ข้อมูลรหัสลับ ($K_L^*[D]$) ในรูปของรหัสแท่ง 2 มิติ หากคำรหัสในรหัสแท่ง 2 มิติถูกทำลายไปบางส่วน จะสามารถใช้รหัสรีดโซโลมอนในการแก้ไขข้อมูลที่ผิดพลาดหรือถูกทำลายได้ ในขณะที่รหัสแท่ง 1 มิติ สามารถทำได้เพียงตรวจสอบว่ามีความผิดพลาดเกิดขึ้นหรือไม่ แต่ไม่สามารถแก้ไขข้อมูลที่ผิดพลาดหรือถูกทำลายให้ถูกต้องได้ และรหัสแท่ง 2 มิติยังมีขนาดที่กระชับซึ่งจะช่วยให้ต้นขั้วมีขนาดไม่ใหญ่มากนัก ซึ่งถ้าต้นขั้วมีขนาดใหญ่จะทำให้เสียพื้นที่ของช่องกาคะแนนของบัตรลงคะแนนไป นอกจากนี้ในงานวิจัยนี้ยังได้ออกแบบตำแหน่งของบริเวณที่ใช้ดึงคุณลักษณะเฉพาะตัวของกระดาษกับบริเวณรหัสแท่ง 2 มิติ ให้สะดวกต่อการจัดพิมพ์และตรวจสอบ

3 *การพัฒนาและปรับปรุงโปรแกรมบนเครื่องไมโครคอมพิวเตอร์* โปรแกรมบนเครื่องไมโครคอมพิวเตอร์ที่ถูกพัฒนาและปรับปรุงเพื่อใช้กับระบบการเลือกตั้ง ประกอบด้วย

- *โปรแกรมสร้างกุญแจ* โปรแกรมสร้างกุญแจต้นแบบของ ศิริพงษ์ สามารถบันทึกกุญแจได้เพียงรูปแบบแฟ้มข้อมูลกุญแจส่วนตัวและแฟ้มข้อมูลกุญแจสาธารณะ ซึ่งอาจจะทำให้ผู้ถือกุญแจไม่สะดวกมากนัก เนื่องจากต้องพกอุปกรณ์ที่ใช้ในการเก็บแฟ้มข้อมูลกุญแจอยู่ตลอดเวลา ในงานวิจัยนี้จึงได้พัฒนาโปรแกรมสร้างกุญแจให้สามารถบันทึกกุญแจในรูปแบบต่างๆ ได้หลายรูปแบบเช่น แฟ้มข้อมูลกุญแจ แฟ้มข้อมูลภาพรหัสแท่ง 1 มิติ และแฟ้มข้อมูลภาพรหัสแท่ง 2 มิติ แล้วแต่ความสะดวกของผู้ถือกุญแจ
- *โปรแกรมสร้างรหัสเฉพาะ* เป็นโปรแกรมที่พัฒนาขึ้นมาใหม่ในงานวิจัยนี้เพื่อใช้สำหรับสร้างแฟ้มข้อมูลรหัสเฉพาะเพื่อนำรหัสเฉพาะ (U) ไปใช้ป้องกันกรรมการเขตทุจริตด้วยการพิมพ์บัตรเลือกตั้งหลายชุดและนำไปสับเปลี่ยนในภายหลัง

- *โปรแกรมพิมพ์บัตรเลือกตั้ง* ส่วนของโปรแกรมพิมพ์บัตรเลือกตั้งที่ได้พัฒนาเพิ่มจากโปรแกรมพิมพ์บัตรเลือกตั้งต้นแบบ ได้แก่การพิมพ์รหัสลับ ($K_L^*[D]$) ลงบนบัตรเลือกตั้งในรูปแบบรหัสแท่ง 2 มิติ จากเดิมที่ใช้รหัสแท่ง 1 มิติ เพื่อให้สามารถใช้งานในทางปฏิบัติได้ นอกจากนี้ผู้วิจัยยังได้พัฒนาโปรแกรมพิมพ์บัตรเลือกตั้งให้สามารถพิมพ์บัตรเลือกตั้งอย่างต่อเนื่องได้ ในขณะที่โปรแกรมพิมพ์บัตรเลือกตั้งต้นแบบทำได้เพียงการสั่งพิมพ์บัตรเลือกตั้งทีละใบ
- *โปรแกรมตรวจสอบบัตรเลือกตั้ง* โปรแกรมตรวจสอบบัตรเลือกตั้งต้นแบบจะรับข้อมูลประจำบัตรเลือกตั้งที่ถูกเข้ารหัสลับ ($K_L^*[D]$) ด้วยการพิมพ์เลขฐาน 16 ลงบนช่องบนหน้าจอของโปรแกรม และโปรแกรมตรวจสอบบัตรเลือกตั้งต้นแบบจะตรวจสอบเพียงข้อมูลคุณลักษณะเฉพาะตัวของกระดาษบัตรเลือกตั้งที่ได้จากการถอดรหัส (F) ว่าตรงกับคุณลักษณะเฉพาะตัวของกระดาษบัตรเลือกตั้งจริงหรือไม่ สำหรับในกรณีที่บริเวณที่ใช้ดึงคุณลักษณะเฉพาะตัวของบัตรเลือกตั้งสกปรก โปรแกรมตรวจสอบบัตรเลือกตั้งต้นแบบจะให้ผลการตรวจสอบข้อมูลคุณลักษณะเฉพาะตัวของกระดาษ (F) ผิดพลาด สำหรับโปรแกรมตรวจสอบบัตรเลือกตั้งที่ได้พัฒนาในงานวิจัยนี้จะอ่านข้อมูลประจำบัตรเลือกตั้งที่ถูกเข้ารหัสลับ ($K_L^*[D]$) จากภาพรหัสแท่ง 2 มิติ ซึ่งถูกถ่ายพร้อมกับภาพบริเวณที่ใช้ดึงคุณลักษณะเฉพาะตัวของกระดาษ และโปรแกรมตรวจสอบบัตรเลือกตั้งจะตรวจสอบข้อมูลต่างๆ ของบัตรเลือกตั้งได้แก่ ค่าแฮช (H_4), รหัสเฉพาะ (U) และคุณลักษณะเฉพาะตัวของกระดาษ (F) ในกรณีบริเวณที่ใช้ดึงคุณลักษณะเฉพาะตัวของกระดาษมีรอยสกปรกอยู่ กรณีนี้ผู้ตรวจสอบสามารถสั่งให้โปรแกรมแสดงพิกัดคุณลักษณะเฉพาะตัวของกระดาษที่ได้จากการถอดรหัส (F) ออกทางหน้าจอได้ หลังจากนั้นผู้ตรวจสอบจะใช้การมองในการเปรียบเทียบพิกัดคุณลักษณะเฉพาะตัวของกระดาษบนหน้าจอ (F) กับพิกัดคุณลักษณะเฉพาะตัวของกระดาษจริงว่าตรงหรือไม่

5.3 การประยุกต์ใช้ในด้านอื่น

สามารถนำการเข้ารหัสลับไปประยุกต์ใช้กับเอกสารที่ต้องการความปลอดภัยต่อการปลอมแปลงสูง แต่สามารถตรวจสอบได้ง่าย ซึ่งความยาวของกุญแจที่ใช้ และจำนวนพิกัดคุณลักษณะเฉพาะตัวที่ถูกดึงออกจากกระดาษ จะแปรตามมูลค่าของเอกสาร ยกตัวอย่างเช่น

1. *โฉนดที่ดิน* สำหรับการตรวจสอบโฉนดที่ดินในปัจจุบันว่าใช่ฉบับจริงหรือไม่ สามารถทำได้โดยนำโฉนดที่ดินไปตรวจสอบกับต้นขั้ว ณ สำนักงานที่ดินจังหวัด หากนำวิธีการเข้ารหัสลับแบบกุญแจสาธารณะมาใช้กับโฉนด จะช่วยให้การตรวจสอบ ทำได้สะดวกขึ้น เนื่องจากผู้ตรวจสอบไม่ต้องเดินทางไปตรวจสอบ ณ สำนักงานที่ดินจังหวัด
2. *พันธบัตรรัฐบาล* การตรวจสอบพันธบัตรรัฐบาลสามารถทำได้โดยการเดินทางไปตรวจสอบ ณ ธนาคารแห่งประเทศไทยว่าพันธบัตรดังกล่าวเป็นจริงหรือไม่ หากนำวิธีการเข้ารหัสลับแบบกุญแจสาธารณะมาใช้กับพันธบัตรรัฐบาลจะช่วยให้การตรวจสอบ ทำได้สะดวกขึ้น เนื่องจากไม่ต้องเดินทางไปตรวจสอบ ณ ธนาคารแห่งประเทศไทย
3. *สลากกินแบ่งรัฐบาล* สลากกินแบ่งที่จำหน่ายในปัจจุบันมีการพิมพ์รหัสแท่งลงบนกระดาษด้วยโดยสลากดังกล่าวถูกเรียกว่าสลากบาร์โค้ด ซึ่งถูกนำมาใช้เพื่อป้องกันการแก้ไขเลขบนสลากกินแบ่ง การตรวจสอบสลากกินแบ่งทำได้โดยนำสลากไปตรวจสอบ ณ กองสลากกินแบ่งรัฐบาลหรือตรวจสอบโดยใช้คอมพิวเตอร์ที่ต่อกับระบบตรวจสอบซึ่งจะสามารถตรวจสอบได้ว่าสลากกินแบ่งนั้นใช่ของจริงหรือไม่และถูกรางวัลที่เท่าไหร่ด้วย แต่ข้อเสียของวิธีการนี้ก็คือ สามารถป้องกันได้เพียงการแก้ไขเลขบนสลากกินแบ่งแต่ไม่สามารถป้องกันผู้ที่ปลอมสลากกินแบ่งโดยการพิมพ์สลากกินแบ่งปลอมเหมือนสลากกินแบ่งต้นฉบับทั้งในส่วนเลขประจำสลากกินแบ่งและส่วนรหัสแท่ง ดังนั้นการนำวิธีการเข้ารหัสลับแบบกุญแจสาธารณะมาใช้กับสลากกินแบ่งรัฐบาลจะช่วยให้การตรวจสอบทำได้สะดวกขึ้น เนื่องจากไม่ต้องเดินทางไปตรวจสอบ ณ กองสลากกินแบ่งรัฐบาลและยังช่วยป้องกันการปลอมแปลงสลากกินแบ่งได้ด้วย

5.4 ข้อเสนอแนะ

ข้อควรระวังสำหรับบัตรเลือกตั้งที่นำวิธีการเข้ารหัสลับแบบกุญแจสาธารณะมาใช้นี้ก็คือ อย่าให้บัตรเลือกตั้งอยู่ในสภาวะแวดล้อมที่อาจจะทำให้บัตรเลือกตั้งเปื้อนหรือสกปรกได้ เนื่องจากรอยเปื้อนหรือรอยสกปรกอาจจะทำให้การดึงข้อมูลคุณลักษณะเฉพาะตัวของกระดาษผิดพลาดได้ หรือทำให้อ่านรหัสแท่ง 2 มิติไม่ได้ โดยปกติรหัสแท่ง 2 มิติ จะมีรหัสแก้ไขความผิดพลาดของข้อมูลอยู่แล้ว แต่ถ้าข้อมูลเสียหายหรือผิดพลาดไปมากกว่าความสามารถในการแก้ไขความผิดพลาดได้ของรหัสแท่ง 2 มิติจะทำให้ไม่สามารถอ่านรหัสแท่ง 2 มิตินั้นได้ ดังนั้นที่หน่วยเลือกตั้ง เจ้าหน้าที่ประจำหน่วยและผู้มาใช้สิทธิ์เลือกตั้งควรตรวจดูบัตรเลือกตั้งก่อนดึงบัตรลงคะแนนออกจากต้นขั้ว หากพบว่าบัตรเลือกตั้งมีรอยเปื้อนอยู่บนรหัสแท่ง 2 มิติ หรือบริเวณพื้นที่ภายในกรอบสี่เหลี่ยมที่ใช้

สำหรับการดึงคุณลักษณะเฉพาะตัวของกระดาษก็อาจจะขอยกเลิกการใช้บัตรเลือกตั้งใบนั้น โดยให้บัตรลงคะแนนนั้นยังคงอยู่ที่ต้นขั้วบัตรเลือกตั้งและนำบัตรเลือกตั้งใบอื่นๆ มาใช้แทน

สำหรับการพัฒนาโปรแกรมพิมพ์บัตรเลือกตั้งในงานวิจัยนี้ ได้ใช้สมมติฐานว่ามีอุปกรณ์รอบข้างครบถ้วนแล้วซึ่งได้แก่ กล้องประจำเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องพิมพ์ ซึ่งเชื่อมต่อกับไมโครคอมพิวเตอร์ รวมทั้งไดรเวอร์สำหรับอุปกรณ์รอบข้างเหล่านี้ เพื่อให้รับส่งข้อมูลกับโปรแกรมพิมพ์บัตรเลือกตั้งแบบเวลาจริง (Real time) แต่ในงานวิจัยนี้ใช้การรับส่งข้อมูลผ่านแฟ้มข้อมูลแทน โดยไม่มีอุปกรณ์รอบข้างจริง ดังนั้นการนำโปรแกรมพิมพ์บัตรเลือกตั้งไปใช้งานจริงนอกจากจะต้องมีความพร้อมของอุปกรณ์รอบข้างดังกล่าวแล้ว ยังต้องพัฒนาโปรแกรมพิมพ์บัตรเลือกตั้งเพิ่มเติม โดยเปลี่ยนรูปแบบการรับข้อมูลคุณลักษณะเฉพาะตัวของกระดาษจากแฟ้มข้อมูลไปเป็นการรับข้อมูลคุณลักษณะเฉพาะตัวของกระดาษในเวลาจริงจากกล้องประจำเครื่องคอมพิวเตอร์ส่วนบุคคลแทน

รายการอ้างอิง

1. ศิริพงษ์ ประยูรหงษ์. การเข้ารหัสลับบนบัตรเลือกตั้งเพื่อป้องกันการปลอมแปลงและทุจริต. วิทยานิพนธ์ปริญญามหาบัณฑิต ภาควิชาวิศวกรรมไฟฟ้า บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2544.
2. RSA Laboratories. Frequently Asked Questions About Today's Cryptography version 4.1 [Online]. RSA Data Security, 1995. Available from: http:// www.rsasecurity.com/rsalabs/faq/index.html. [2003,Feb 15]
3. Denning, D. E. Cryptography and data security. United States of America : Addison-Wesley Publishing, 1982.
4. Jang, B. K., and Chin, R. T. One-Pass Parallel Thinning: Analysis, Properties, and Quantitative Evaluation. IEEE Transactions on Pattern Analysis and Machine Intelligence Vol. 14 No. 11 (November 1992) : 1129-1140.
5. Thym Infoware. Code 128 Barcode Details [Online]. Thym Infoware, (n.d.). Available from: http://www.in-barcode.com/sym_c128.html. [2003,Feb 15]
6. IDAutomation.com. Code 128 / USS Code-128 Barcode FAQ [Online]. IDAutomation.com, (n.d.). Available from: http://www.idautomation.com/ code128faq.html. [2003,Feb 15]
7. Altek Instruments. Code 128 Barcode Specification [Online]. Altek Instruments, 2001. Available from: http://www.barcodeman.com/info/c128.php3. [2003,Feb 15]
8. Adams, R. Bar Code 1 Code 128 Specification Page [Online]. Adams Communications, 2001. Available from: http://www.barcode-1.net/pub/ russadam/128code.html. [2003,Feb 15]
9. Symbol Technologies. About PDF417 [Online]. Symbol Technologies, (n.d.). Available from: http://www.pdf417.com/about_pdf417.htm. [2003,Feb 15]
10. IDAutomation.com. PDF417 Barcode FAQ [Online]. IDAutomation.com, (n.d.). Available from: http://www.idautomation.com/pdf417faq.html. [2003,Feb 15]
11. X5 Networks. What is hash function ? [Online]. X5 Networks, (n.d.). Available from: http://www.x5.net/faqs/crypto/q94.html. [2003,Feb 15]

12. RSA Laboratories. What is a hash function ? [Online]. RSA Data Security, 1995. Available from: http://www.rsasecurity.com/rsalabs/faq/2-1-6.html. [2003,Feb 15]

13. Wade, G. Coding Techniques: an introduction to compression and error control. United Kingdom : PALGRAVE Publishing, 2000.

14. Matache, A. Encoding/Decoding Reed Solomon Codes [Online]. Adina Matache, 1996. Avalilable from: http://drake.ee.washington.edu/~adina/rsc/slide/slide.html. [2003,Feb 15]

15. IBM. IBM Infoprint 70 Plus Cut Sheet Printer [Online]. IBM, (n.d.). Available from: http://www.printers.ibm.com/R5PSC.NSF/Web/ip70home. [2003,Feb 15]

16. Hewlett-packard company. Hp Laserjet 2200dn printer (C7063A) specifications [Online]. Hewlett-packard company, 2002. Available from: http://h10010.www1.hp.com/wwpc/us/en/un/WF06/18972-236251-236263-14638-28861-28868-28869.html . [2003,Feb 15]

17. Canon Electronic Inc. DR-2080C/Specifications [Online]. Canon Electronic Inc, 2002. Available from: http://www.canon-elec.co.jp/english/products/dr2080c/spec.html. [2003,Feb 15]

18. Canon U.S.A., Inc. PowerShot A100/A200 - Specifications [Online]. Canon U.S.A., Inc, 2003. Available from: http://www.powershot.com/powershot2/a200-a100/specs.html. [2003,Feb 15]

19. Intel Corporation. Intel® Pocket Digital PC Camera Technical Specifications [Online]. Intel Corporation , 2001. Available from: http://www.mwave.com/mwave/doc2/071288.html. [2003,Feb 15]

20. Peripheral Imaging Corporation. Contact Image Sensor Module [Online]. Peripheral Imaging Corporation, 2002. Available from: http://www.p-imaging.com/modules.htm. [2003,Feb 15]

21. Gutmann, P. Cryptlib Security Toolkit Version 2.1 final beta [Computer Software]. Peter Gutmann, 1999. Available from: http://www.cs.auckland.ac.nz/~pgut001/cryptlib/. [2003,Feb 15]

22. ประเสริฐ ฉอเรืองวิวัฒน์. การรู้จำตัวอักษรเขียนภาษาไทยโดยการวิเคราะห์ลักษณะบ่งความต่าง. วิทยานิพนธ์ปริญญามหาบัณฑิต ภาควิชาวิศวกรรมไฟฟ้า บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย, 2541.

23. Bosselaers, A. The RIPE-MD160 page [Online]. Antoon Bosselaers, (1999). Available from: http://www.esat.kuleuven.ac.be/~bosselae/ripemd160.html. [2003,Feb 15]

24. Lien, J. PDF417 Encode Version 2.6 [Computer program]. John Lien, 2001. Available from: http:// sourceforge.net/projects/pdf417encode/. [2003,Feb 15]

25. Poskanzer, J. Manpage of pbm [Online]. Jef Poskanzer, (n.d.). Available from: http://netpbm.sourceforge.net/doc/pbm.html. [2003,Feb 15]

26. Karn, P. Forward Error Correcting codes [Computer program]. Phil Karn, 1996. Available from: http://www.ka9q.net/code/fec/. [2003,Feb 15]

27. Netcraft 2002. Netcraft Web Server Survey [Online]. Netcraft , 2002. Available from: http://www.netcraft.com/Survey/index-200203.html. [2003,April 5]

บรรณานุกรม

ภาษาไทย

นิรุธ อำนวยศิลป์. คู่มือการเขียนโปรแกรม Microsoft Visual C++ Version 6.0. กรุงเทพมหานคร : ซัคเซส มีเดีย, 2542.

เจนวิทย์ เหลืองอร่าม. การใช้ Turbo C++ เขียนโปรแกรมภาษา C. กรุงเทพมหานคร : สุขภาพใจ, 2537.

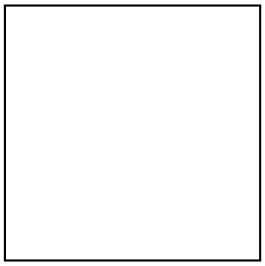
ภาษาอังกฤษ

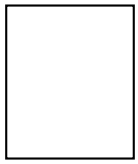
Bates, J. and Tompkins, T. Using Visual C++ 6. United States of America : Que, 1998.

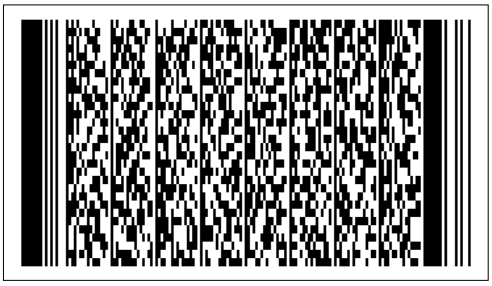
ภาคผนวก

ภาคผนวก ก

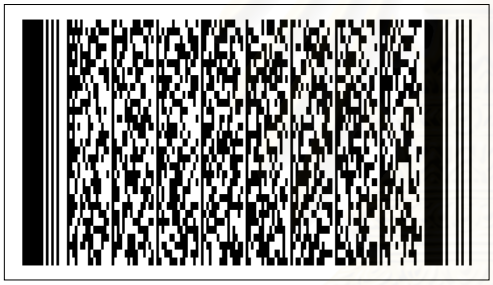
ตัวอย่างบัตรเลือกตั้งขนาด 216 X 356 ม.ม. ซึ่งถูกพิมพ์ลงบนกระดาษธรรมดา และตัวอย่างบัตรเลือกตั้งซึ่งย่อขนาดจากกระดาษ 216 X 356 ม.ม. พิมพ์ลงบนกระดาษที่สามารถใช้ในการพิมพ์บัตรเลือกตั้งได้



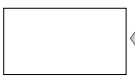




บัตรเลือกตั้ง
สมาชิกสภาผู้แทนราษฎรแบบแบ่งเขต



ข้อควรระวัง
- อย่ารับบัตรเลือกตั้งที่ฉีกออกจากต้นขั้วเตรียมไว้ก่อนแล้ว
- หากพบบัตรเลือกตั้งที่มีรอยเปื้อนในบริเวณกรอบสี่เหลี่ยมด้านซ้ายมือบนให้ขอเปลี่ยนบัตรเลือกตั้งใบใหม่แทน



ไม่ประสงค์จะลงคะแนนให้กับผู้สมัครใดเลย ให้ทำเครื่องหมาย "**กากบาท**" เช่น (X) ลงในช่อง "**ไม่ต้องการลงคะแนน**"นี้

หมายเลขประจำตัวผู้สมัคร	ช่องทำเครื่องหมาย	หมายเลขประจำตัวผู้สมัคร	ช่องทำเครื่องหมาย	หมายเลขประจำตัวผู้สมัคร	ช่องทำเครื่องหมาย	หมายเลขประจำตัวผู้สมัคร	ช่องทำเครื่องหมาย
๕๐๑ 501		๕๑๑ 511		๕๒๑ 521		๕๓๑ 531	
๕๐๒ 502		๕๑๒ 512		๕๒๒ 522		๕๓๒ 532	
๕๐๓ 503		๕๑๓ 513		๕๒๓ 523		๕๓๓ 533	
๕๐๔ 504		๕๑๔ 514		๕๒๔ 524		๕๓๔ 534	
๕๐๕ 505		๕๑๕ 515		๕๒๕ 525		๕๓๕ 535	
๕๐๖ 506		๕๑๖ 516		๕๒๖ 526		๕๓๖ 536	
๕๐๗ 507		๕๑๗ 517		๕๒๗ 527		๕๓๗ 537	
๕๐๘ 508		๕๑๘ 518		๕๒๘ 528		๕๓๘ 538	
๕๐๙ 509		๕๑๙ 519		๕๒๙ 529		๕๓๙ 539	
๕๑๐ 510		๕๒๐ 520		๕๓๐ 530		๕๔๐ 540	

ตัวอย่างบัตรเลือกตั้งด้านหน้า

หมายเลขประจำตัวผู้สมัคร	ช่องทำเครื่องหมาย	หมายเลขประจำตัวผู้สมัคร	ช่องทำเครื่องหมาย	หมายเลขประจำตัวผู้สมัคร	ช่องทำเครื่องหมาย	หมายเลขประจำตัวผู้สมัคร	ช่องทำเครื่องหมาย
๕๔๑ 541		๕๕๑ 551		๕๖๑ 561		๕๗๑ 571	
๕๔๒ 542		๕๕๒ 552		๕๖๒ 562		๕๗๒ 572	
๕๔๓ 543		๕๕๓ 553		๕๖๓ 563		๕๗๓ 573	
๕๔๔ 544		๕๕๔ 554		๕๖๔ 564		๕๗๔ 574	
๕๔๕ 545		๕๕๕ 555		๕๖๕ 565		๕๗๕ 575	
๕๔๖ 546		๕๕๖ 556		๕๖๖ 566		๕๗๖ 576	
๕๔๗ 547		๕๕๗ 557		๕๖๗ 567		๕๗๗ 577	
๕๔๘ 548		๕๕๘ 558		๕๖๘ 568		๕๗๘ 578	
๕๔๙ 549		๕๕๙ 559		๕๖๙ 569		๕๗๙ 579	
๕๕๐ 550		๕๖๐ 560		๕๗๐ 570		๕๘๐ 580	

ตัวอย่างบัตรเลือกตั้งด้านหลัง

ภาคผนวก ข

รายละเอียดของเซ็นเซอร์สัมผัสภาพ (Contact Image Sensor) ที่สามารถนำมาใช้ในการตรวจสอบบัตรเลือกตั้งที่หน่วยเลือกตั้งได้

รายละเอียดของเซ็นเซอร์สัมผัสภาพ (Contact Image Sensor) รุ่น PI250MC-A6 ของ P-Imaging จาก http://www.p-imaging.com/PDF_files/PI250MC-A6.PDF

Peripheral Imaging Corporation

68 Bonaventura Drive
San Jose California, 95134
Phone: 408-428-0123
Fax: 408-428-0168

PI250MC-A6 CIS Module
200DPI CIS Sensor
Engineering Data Sheet

Key Features

- Low power-Single Power Supply at 5.0Volts
- Light source, lens, and sensor are integrated into a single module
- 8 dpm resolution, 104 mm scanning length
- High Speed Page Scan - up to 167 µsec/line @ 5MHz pixel rate with internal optical modification (optional feature).
- Wide dynamic range
- Analog output
- Yellow-green LED light source
- Compact size ≅ 14 mm x 19 mm x 120 mm
- Light weight

General Description

The PI250MC-A6 is a contact imaging sensor, CIS, module. It is a successor module to its predecessor, PI223MC-A6, hence it possesses all superb qualities of its predecessor, except, it has one outstanding feature, it can operate from a single 5 volts supply. Like its predecessor it composed of 13 PI3020 sensor chips. The PI3020 is a 200 DPI solid-state line imaging array, also a product of Peripheral Imaging Corporation. This imaging device is fabricated using MOS imaging sensor technology for its high-speed performance and high sensitivity. Like its predecessor, the PI250MC-A6 is suitable for scanning A6 size (104 mm) documents with 8 dots per millimeter resolution. Applications include ticket, check and card scanners, variety of mark readers, and other automation equipment.

Functional Description

The PI250MC-A6 consists of 13 imaging array sensors that are cascaded to provide 832 photo-detectors. Each sensor has their associated multiplex switches, and a digital shift register that controls its sequential readout. Each also contains a chip select switch so that each following chip is accessed sequentially as its predecessor chip completes its scan. Theses chips are mounted on a PCB board along with clock buffers and video signal amplifier. The only change from predecessor module was in this amplifier. It was slightly altered from its predecessor module to gain the single supply feature. See Figure 1. PI250-A6 module block diagram.

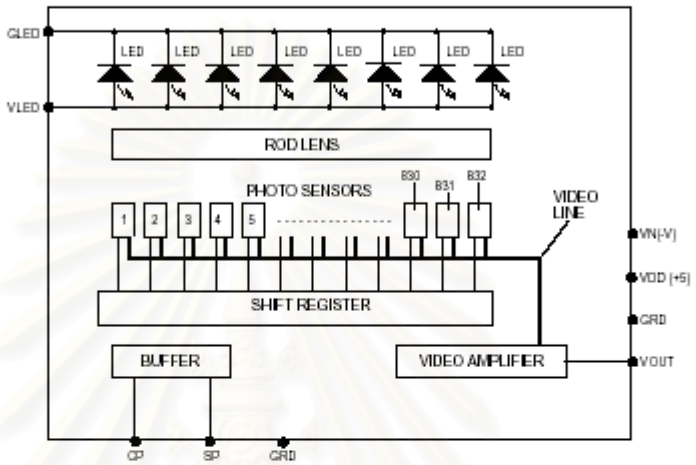
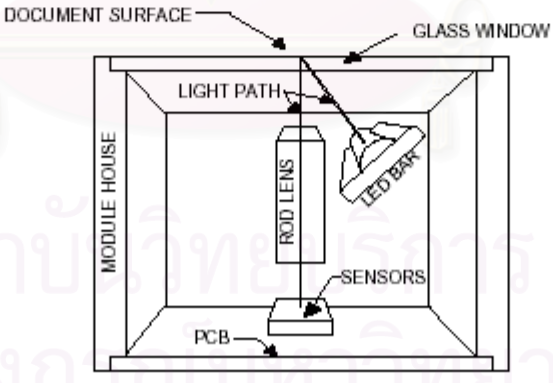


Figure 1. PI250MC-A6 module block diagram

The PCB containing the imaging array is enclosed in a module housing, along with a one-to-one graded indexed micro lens array that focuses the scanned documents' image onto the sensing line of the sensor chips. The document is illuminated with a LED light source which is also mounted in the housing. See Figure 2. PI250MC-A4 Cross Sectional View.



INSIDE PICTORIAL OF MODULE

Figure 2. PI250MC-A4 Cross Sectional View

This pictorial cross section shows the LED Bar light source and its Illumination path. The light on the document reflects images on the document. The reflected images focus through the micro lens onto the chips' image sensing line where images are converted to proportional electrical charges. An on board amplifier processes these signal charges into proportional video signal voltages, which is sent out to the output video port.

All components are housed in a small plastic housing and covered with a glass window. This cover glass not only serves to protect all of the critical components within the housing from dust, but, along with micro lens, it determines the depth-of-focus because it lies in the optical path.

Pin Out Description

There is one connector located at the end of the module. The outline of the module in Figure 4 of the mechanical section illustrates the connector location. With the module window facing down on flat surface, with the viewer looking down on backside of the module, and with the connector's pins facing viewer, the connector is located on the right hand end of the module. The connector is a 1.25 mm single 10-pin row. Its I/O designation is provided in Table 1. I/O Designation. Pin number 1 location is indicated on the module outline.

Pin Number	Symbol	Names and Functions
1	Vout	Analog Video Output
2	Gnd	Ground; 0V
3	Vdd (+5V)	Positive power supply
4	NA	Not used
5	Gnd	Ground; 0V
6	SP	Shift register start pulse
7	Gnd	Ground; 0V
8	CP	Sampling clock pulse
9	GLED	Ground for the light source; 0V
10	VLED	Supply for the light source

Table 1. I/O Designation

Absolute Maximum Rating:

The following is a table of absolute maximum parameters. These parameters should not be used in prolonged operation.

Parameter	Symbols	Maximum Rating	Units
Power Supply	Vdd	7.0	V
	Idd	50	mA
	VLED	5.7	V
	ILED	600	mA
Input Clock Pulse (high)	Vih	Vdd	V
Input Clock Pulse (low)	Vil	-0.5	V

Table 2. Absolute Maximum Rating

Operating Environment

Operating temperature	Top	0 to 50	^{0}C
Operating humidity	Hop	10 to 85	%
Storage temperature	Tstg	-25 to 85	^{0}C
Storage humidity	Hstg	5 to 95	%

Table 3. Operating Environment

Electro-Optical Characteristics (25° C)

Parameter	Symbol	Parameter	Units	Note
Number of photo detectors		832	elements	
Pixel to pixel spacing		125	µm	
Line scanning rate	Tint(1)	420	µsec	@ 2 MHz clock frequency
Clock frequency(2)	Fclk	2	MHz	See note 2 for 5.0 MHz operation.
Bright output voltage(3)	Video Output	1.0	V	Specified for 420µsec.
Bright output nonuniformity(4)	Up	<+/-30	%	
Adjacent pixel nonuniformity(5)	Uadj	<25	%	

Dark nonuniformity[6]	Ud	<50	mV	
Dark output voltage	Vd	200<Vd<300	mV	
Modulation transfer function[7]	MTF	>50	%	See note 7 for MTF & DOF.

Table 4. Electro-optical characteristics at 25° C.

Definition:

(1) Tint: Line scanning rate or integration time. Tint is determined by the interval of two SP, start pulses. See note 2 for the high scanning speed operation.
(2) Fclk: main clock frequency. The call out is at 2.0 MHz, but electrically module reliably operates to 5.0 MHz. However, it must be optically modified to obtain the minimum integration time of 167 μsec. This modification is offered as a user's option.
(3) Vpavg = $\sum$ Vp(n)/832
(4) Up = [(Vpmax - Vp) / Vp] x 100% or [(Vp - Vpmin) / Vp] x 100%
(5) Upadj = MAX[| (Vp(n) - Vp(n+l) | / Vp(n)] x 100%
Upadj is the nonuniformity percentage pixel to pixel
(6) Ud = Vdmax - Vdmin
Vdmin is the minimum output on a black document
Vdmax: maximum output voltage of black document
(7) MTF = [(Vmax - Vmin) / (Vmax + Vmin)] x 100 [%]. Depth of focus, DOF, range is defined with the MTF. MTF is measure at glass surface and at 0.4mm from the glass > 50% and peaks at approximately mid-point of 0.2mm.
Vmax: maximum output voltage at 50 lp/inch (At 1/2 of the optical Nyquest Frequency)
Vmin: minimum output voltage at 50 lp/inch
(8) lp / inch: line pair per inch

Table 5. Recommended Operating Conditions (25 °C)

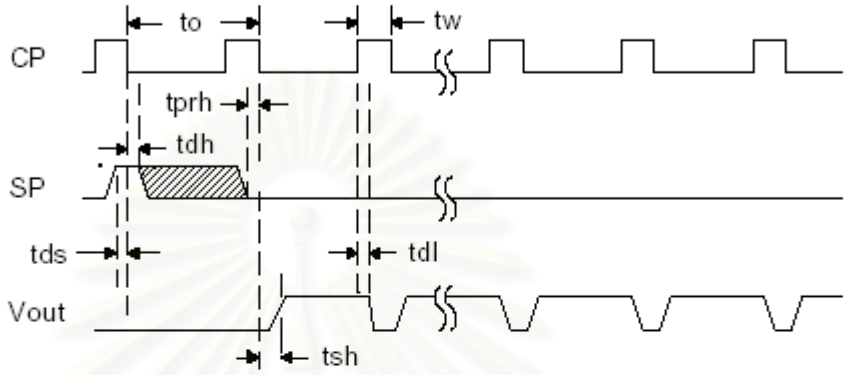
Item	Symbol	Min	Mean	Max	Units
Power Supply	Vdd	4.5	5.0	5.5	V
	VLED	4.5	5.0	5.5	V
	Idd	22	25	30	ma
	ILED	200	380	450	ma
Input voltage at digital high	Vih	Vdd-1.0	Vdd-.5	Vdd	V
Input voltage at digital low	Vil	0		0.6	V
Clock frequency	Fclk		2.0	5.0	MHz
Clock pulse high duty cycle[1]		25			%
Clock pulse high duration[1]		50			ns
Integration time[2]	Tint	0.167		5.0	ms
Operating temperature	Top		25	50	^{0}C

Table 5. Recommended Operating Conditions (25 °C)

(1) These duty cycle and high duration are for 5.0 MHz clock rate.

(2) Tint (Min) is the lowest line integration time available at 5.0 MHz clock rate with internal optical modifications. See note 2 under Table 4.

Switching Characteristics (25°C)



MODULE TIMING DIAGRAM

Figure 3. Clock and Start pluse Timing Diagram

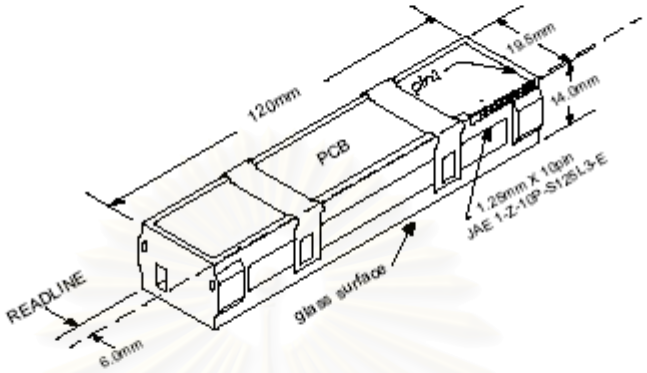
The switching characteristics for the I/O clocks are shown in Figure 3. Its corresponding timing symbol definitions are given in Table 6, below.

Item	Symbol	Min.	Typical	Max.	Units
Clock cycle time	to	0.2		4.0	µs
Clock pulse width	tw	50			ns
Clock duty cycle		25		75	%
Prohibit crossing time of Start Pulse	tprh	15			ns
Data setup time	tds	20			ns
Data hold time	tdh	20			ns
Signal delay time	tdl	50			ns
Signal settling time	tsh	120			ns

Table 6. Symbol Definition for the Above Timing Diagram

Module and Its Mechanical Dimensions

The sketch of this module is to provide a pictorial of the module size and structure. A detailed drawing is available upon request.



Pictorial of the Plastic
Standard A6 Housing Size

Figure 4. PI250MC-A6 Module Mechanical Outline

ภาคผนวก ค

บทความทางวิชาการของผู้วิจัยที่ได้รับการตีพิมพ์แล้ว

1 Public-Key Encryption on Ballot Paper for Forged and Dishonest Prevent.

- Proceedings of International Conference on Information and Communication Technologies.

Public-Key Encryption on Ballot Paper for Forged and Dishonest Prevention

Warakorn Srichavengsup, Suvit Nakpeerayuth and Siriphong Prayoonhong
Telecommunication Research Laboratory, Department of Electrical Engineering,
Chulalongkorn University, Bangkok 10330, Thailand
E-mail: warakorn@chula.com

Abstract

This paper presents an idea of how to apply the public-key encryption to the ballot paper for forged and dishonest prevention. Because the current ballot papers can be easily forged, the use of public-key encryption can prevent ballot paper forgery. Some small line-shaped objects are mixed in the paper which is used for printing the ballot paper. Coordinates of these objects are used as paper features. This feature data is included in the ballot paper data and encrypted by using the Election Commission's private key. The encrypted data is printed on the ballot paper as 2-dimension barcode. Anyone can verify whether the ballot paper is genuine by using the Election Commission's public key to decrypt the encrypted data. If the decryption is successful, that guarantee the ballot paper data is generated by the Election commission. Then the paper feature data is matched with the ballot paper feature. If they match, that ballot paper is genuine. If they don't, that ballot paper is forged by copying the 2-dimension barcode from the genuine one to the forged one which has the different paper feature. The distributed ballot printing system and the ballot verification procedure are also designed in this paper for the purpose of applying the public-key encryption to the ballot paper in the practical situation.

Keywords: *Ballot Paper, Paper Feature, Feature Extraction, Public-Key Encryption, Election System*

1. Introduction

Nowadays, forging the ballot papers is an easy way to cheat general election in Thailand. To prevent this, using the banknote printing system is possible solution. It could work with good efficiency but its cost is also very high. The public-key encryption [1], [2] can be used in the ballot papers to reduce cost, make the forgery more difficult and to simplify the authenticity check. Some small objects like fiber or dust are deliberately mixed in the paper tissue during manufacturing process. Then each ballot paper can be scanned to extract its features of its fiber or dust coordinates. These features are included in the ballot paper data and encrypted by using the Election Commission's private key for preventing the forgery. The public-key encryption lets any people able to verify the ballot. But it is difficult to forge a new one because this requires the knowledge of the key or ability to produce a paper with specific feature.

When anyone wants to verify the ballot, he must use the public key of the Election Commission to decrypt the encrypted data. If the decryption is successful, that means this ballot paper data is encrypted by the Election Commission. Then verify the paper features data with the ballot paper features. If they match, that ballot is genuine. If they don't match, that ballot is forged by copying the data from the genuine one to the forged one which has different paper features.

This paper proposes an idea of how to apply the public-key encryption to the election system for forged and dishonest prevention [3], [4]. The distributed ballot printing system and the ballot verification procedure are also proposed in this paper for the purpose of applying the public-key encryption to the ballot paper in the practical situation.

Section 2 describes the concept of paper features, public-key encryption, hash function [5], [6], fingerprint and 2-dimension barcode [7], [8]. Section 3 describes the design of the ballot paper. Section 4 describes the election organization in Thailand [9] and the ballot printing scheme. Section 5 describes how to design the distributed ballot printing system [4]. Section 6 describes the ballot paper verification process. Finally, the conclusions of this paper is given in section 7.

2. Basic Concept and Tools

2.1 Paper features

During the paper manufacturing process, grains of sand or colored fiber are randomly mixed in the paper tissue, consequently each ballot paper has its own random pattern as depicted in Figure 1. This brings about the uniqueness of each ballot paper. If anyone wants to duplicate the ballot paper, he must control the position of

grains of sand or colored fiber during the manufacturing process but it is very difficult to do that.

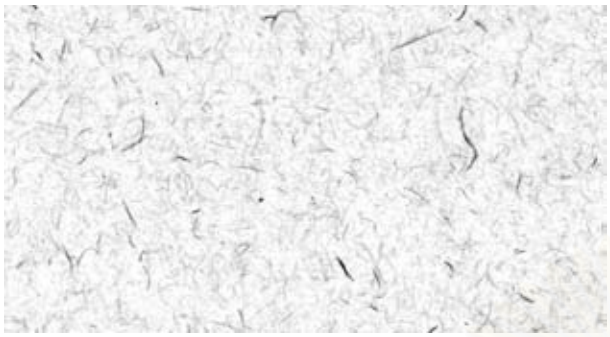


Figure 1. An example of ballot paper texture.

The paper feature data is the coordinate of the end points of embedded particles, sand grains or colored fiber. These features are unique for each ballot, so it is unable to copy the data from the genuine ballot to the forged ballot. The coordinates of the ends of particles in the paper can be shown in Figure 2.

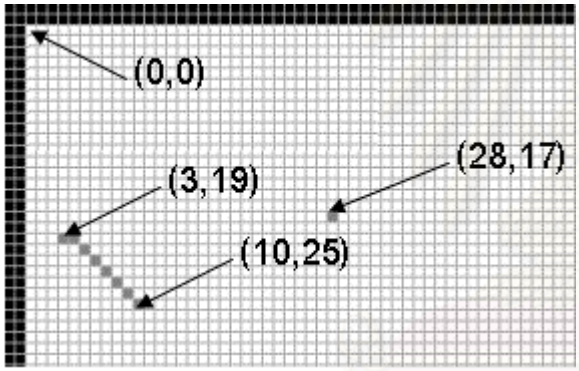


Figure 2. Coordinates of the end of particle embedded to ballot paper.

2.2 Public-key encryption

The paper features data together with other data is encrypted by using the public-key encryption to prevent forgery**.**

In the public-key encryption, two keys are needed, a public key and a private key, both of them are simultaneously generated by the Election Commission. The Election Commission 's public key is published and known to anyone. The Election Commission 's private key, on the other hand, is kept secret. A message encrypted by the private key, can only be decrypted by the associated public key. Then anyone can prove whether the ballot paper data is encrypted by the Election Commission or not by using the Election Commission 's public key.

2.3 One-way hash function

A one-way hash function, also known as a message digest, is a mathematical function that takes a message string of any length and returns a fixed-length string (hash value). These functions are designed in such a way that it is hard to reverse the process, that is, to find a string that hashes to a given value. A good hash function also makes it hard to find two strings that would produce the same hash value.

In this paper, we use the hash function to transform the ballot paper data to the hash value. This value is used for referring to ballot paper in short.

2.4 Fingerprint

The voters will print their fingerprints on the stubs. This fingerprint is unique, so the fingerprint on the stub can show the identification of the voter. If anyone votes more than once, he must leave his fingerprints on the stubs more than once as well. Consequently, these fingerprints can link to the offenders. The fingerprint is used only on the stub because the voting part should not contain any identification of the voter. After tearing the voting part from the stub, the voter's decision will be secret.

2.5 2-Dimension barcode

The long length encrypted ballot paper data can be printed on the ballot paper in any following forms:

1. Hexadecimal ASCII text.
2. 1-D barcode (1-dimension barcode).
3. 2-D barcode (2-dimension barcode).

Key in the very long hexadecimal data during the decryption process is not convenient and error prone.

In this paper, we select 2-D barcode which is compact and robust appropriate for the ballot paper with particles or colored fiber. Because 2-D barcode has the error correction capability, it is selected instead of the common 1-D barcode which only has the error detection. An example of 2-D barcode can be shown in Figure 3.

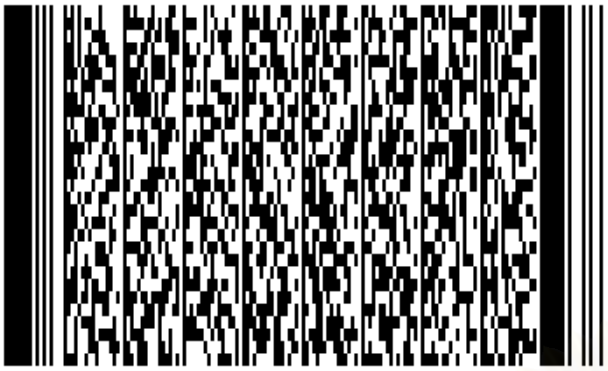


Figure 3. An example of 2-D barcode.

3. Ballot Paper Design

Design of the ballot paper is proposed in this section as depicted in Figure 4. This must consider all factor such as size, folding, features extraction, stub, etc. But only the encryption related design will be presented as following.

3.1 Symbols definition

Because the ballot paper consists of many data and there is a relationship between these data. To describe the relationship between these data, the following symbols will be used.

K^* denotes a private key.

K denotes a public key corresponding to K^*.

$K^*[\cdot]$ denotes an encrypted/decrypted data inside the bracket [ ] using a key K^*.

$K[K^*[\cdot]]$ denotes decryption using a public key K to the encrypted data using private key K^*. The result is the data inside the bracket [ ].

; denotes gathering the data which are separated by this semicolon.

F denotes the paper feature data.

I denotes an information data which includes election date, constituency code, volume number and ballot number.

$H = H[\cdot]$ denotes a hash value of the data inside the bracket [ ].

$D = I;F;H$ denotes the ballot paper data.

Moreover, these following subscripts are used to show the different sources of the data.

C denotes Central for showing that data is belong to the Election Commission.

L denotes Local for showing that data is belong to the local constituency election commission.

S denotes Stub for showing that data is part of the stub data.

V denotes Voting part for showing that data is part of the voting part data.

3.2 Ballot paper components

Each ballot paper consists of stub and voting part.

1. Stub consists of 3 areas including an area for extracting the paper feature, 2-dimension barcode of the encrypted stub data and voter's fingerprint block.

2. Voting part consists of 3 areas including an area for extracting the paper feature, 2-dimension barcode of the encrypted voting part data and marking block.

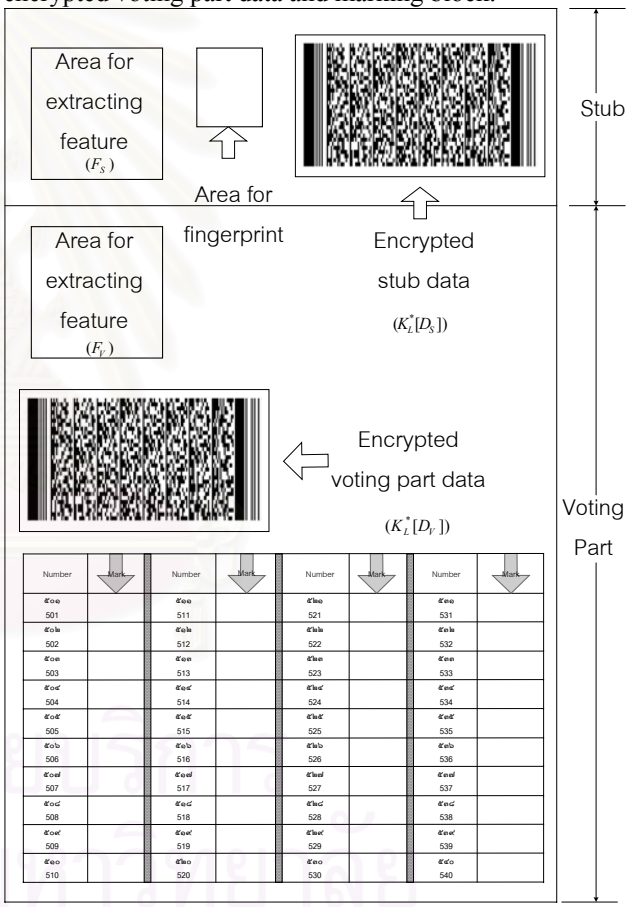


Figure 4. Designed ballot paper.

3.3 Ballot paper data

Each stub data (D_S) and voting part data (D_V) consists of

1. Information data (I) consists of election date, constituency code, volume number and stub or voting part number. This information data shows the place where the ballot came from. So it can prevent using the ballot paper across the constituency.

2. Paper feature data (F) includes the coordinate of the embedded particle or colored fiber. This feature is a unique data so it is unable to copy the data from the genuine ballot paper to other forged ballot paper.

3. Hash value (H) is calculated from the 2 previous data ($H[I;F]$). This value is used for referring to ballot paper in short.

All above data are concatenated ($D = I;F;H$) and encrypted by the Election Commission's private key ($K_C^*[D]$) and printed as 2-dimension barcode on the stub and voting part of the ballot paper. Both of them ($K_C^*[D_S], K_C^*[D_V]$) are independent from each other for the secretion of the voter's decision.

3.4 Ballot paper verification

Anyone can verify the ballot paper by using the Election Commission 's public key (K_C) to decrypt the encrypted ballot paper data ($K_C[K_C^*[D]] = D$). If the decryption successful, this means that data is encrypted by the Election Commission. Then the decrypted paper feature data (F) can be matched with the ballot paper features. If they don't match, that ballot paper is forged by copying the 2-D barcode from the genuine one to the forged one which has the different paper feature.

If the number of the forged ballot papers is more than an acceptable number, the Election Commission can decide to cancel the election.

4. Election Organization and Ballot Printing Scheme

4.1 Election organization in Thailand

In Thailand, there is an independent organization with a responsibility of political election according to the 1997's constitution. The election system consists of the following committees.

1. Election Commission, situated in central Bangkok, is responsible for controlling the overall election and managing the election process.

2. Local Constituency Election Commission manages the election process within a constituency and transports the printed ballot papers to all polling stations within the constituency.

3 Polling station authority, situated in a polling station, distributes the ballot papers to the voters then collects and sends back the marked ballot papers to the counting station.

4.2 Ballot printing scheme

The ballot printing scheme can be arranged in two levels.

1. Centralized ballot printing - Election Commission is responsible for the printing burden.

2. Distributed ballot printing - Each local constituency election commission takes the printing burden instead of Election Commission. This can reduce the transportation and increase the utilization of microcomputers and printers.

This paper chooses distributed ballot printing approach in order to distribute the printing burden to the local constituency election commission including printer arrangement and man power. Each constituency oversees its own printing system.

4.3 Problem of distributed ballot printing

The main problem of distributed ballot printing is the forgery by the local constituency election commission. It can be done by printing some extra ballot papers and shuffling them afterward.

The next section will describe the design of the distributed ballot paper printing system for preventing local constituency election commission's dishonest.

5. Distributed Ballot Printing System Design

The purpose of the distributed ballot paper printing system design is to prevent the dishonesty by the local constituency election commission who can generate some extra ballot papers and shuffle them afterward.

5.1 Controlling data

The Election Commission use these controlling data to prevent the dishonesty by the local constituency election commission.

1. Unique Code – Unique code is generated by the Election Commission. There are the limited number of the unique codes, equal to the total number of the stubs and the voting papers in that constituency. One unique code is included in one stub data or one voting part data. Then the local constituency election commission can not print the

ballot papers more than the number of the unique codes received.

2. Hash Value – Hash value is used for referring to ballot paper in short and identifying the forgery. At the counting station, there is a database of all existing hash value in that constituency, a hash value which is not in the database shows an occurring of extra ballot paper.

5.2 Additional symbols definition

These following symbols, in addition to section 3.1, are used in the distributed ballot paper printing system.

U denotes a unique code generated by the Election Commission.

$U_1 = K_C^*[U]$ denotes an encrypted unique code which is encrypted by the Election Commission's private key and sent out to each constituency.

$H = H[I;U_1;F]$ denotes the hash value of ballot paper data.

$D = I;U_1;F;H$ denotes the data of the ballot paper.

5.3 Ballot paper data

The ballot data components can be shown in Figure. 5. Each stub data (D_S) and voting part data (D_V) in distributed ballot paper printing system consists of

1. Information data (I) consists of election date, constituency code, volume number and stub or voting part number. This information data shows the place where the ballot came from. This can prevent using the ballot paper across the constituency.

2. Encrypted unique code (U_1) is randomly generated by the Election Commission to control the number of printed ballot. To prevent the forged unique code, the unique code is encrypted by the Election Commission's private key ($K_C^*[U] = U_1$) and sent out to the local constituency election commission. Then the local constituency election commission can prove whether that unique code is sent from the Election Commission or not by using the Election Commission's public key (K_C) to decrypt the encrypted unique code ($K_C[K_C^*[U]] = U$). If it is sent from the Election Commission's then the local constituency election commission includes the encrypted unique code (U_1) to the ballot paper data (D).

3. Paper feature data (F) includes the coordinate of the embedded particle or colored fiber.

4. Hash value (H) is calculated from the 3 previous data ($H = H[I;U_1;F]$). This value is used for referring to ballot paper in short and identifying the forgery. At the counting station, there is a database of all existing hash value in that constituency, a hash value which is not in the database shows an occurring of extra ballot paper.

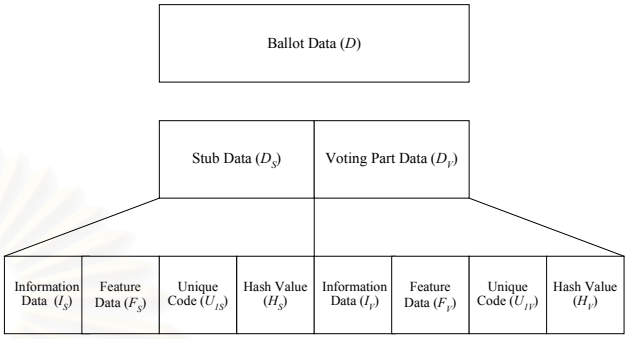


Figure 5. Ballot data components.

The stub data and the voting part data are encrypted by the local constituency election commission's private key ($K_L^*[D_S], K_L^*[D_V]$) and printed in 2-D barcodes on the stub and voting part of ballot paper. Both of them are independent from each other for the secretion of the voter's decision.

6. Ballot paper verification procedure

If the ballot papers is transported from the one place to the another place, there must be the ballot paper random sampling verification done by the ballot paper receiver.

6.1 Verification place

The ballot paper verification is done at these following places.

1. The polling station - After the local constituency election commission prints the whole ballot papers in that constituency, then transport the ballot paper from the constituency to the polling station. The polling station's authority will sample and verify the ballot paper.

2. The counting station – The marked voting parts are sent back from the polling station to the counting station. The counting station's authority will sample and verify the marked voting part.

6.2 Verification procedure

The sampling ballot paper is verified, follow the steps below:

1. Reading 2-D barcode as the encrypted ballot paper data ($K_L^*[D_S], K_L^*[D_V]$).

2. Decrypting the encrypted ballot paper data and get the ballot paper data (D_S , D_V).

3. Verifying the following data.

3.1 Ballot paper feature data (F) - Verifying the feature data whether the feature position of the ballot paper matches the decrypted feature data.

3.2 Unique code (U) - Verifying the unique code whether there is any repetitions. The number of unique codes assigned for each constituency is limited. Therefore the repeating of a unique code indicates the dishonesty of the local constituency election commission.

3.3 Hash value (H) - Verifying the hash value whether it is in the counting station's database. Hash value is checked with the same purpose as that of unique code. The ballot paper which its hash value is not in the constituency's database can not be used.

These verification can be done only partially or fully depend on the situation. Normally only step 2 is enough for quick check. But step 3.1 or up to 3.3 for all ballots check may be necessary later in court.

If the number of the ballot that is abnormal according to the given criteria is more than an acceptable number, the Election Commission can decide to cancel the election in that constituency.

7. Conclusions

This paper proposed an election mechanism utilizing a public-key encryption for forged and dishonesty prevention. The distributed ballot printing system and the ballot verification system were also proposed in this paper for the purpose of applying the public-key encryption to the ballot paper in the practical situation.

8. Acknowledgements

The author wishes to thank Supattarachai Chompun and Datchakorn Tancharoen for their assistance and guidance in this paper.

9. References

[1] D. E. Denning, "Cryptography and data security", Addison-Wesley Publishing, 1982.

[2] W. Diffie and M.E. Hellman, "Privacy and authentication : An Introduction to Cryptography", Proc. IEEE 67 (1979), 397-427.

[3] S. Prayoonhong,, "Encryption on ballot paper for forgery and dishonesty prevention", Master's Thesis, Department of Electrical Engineering, Chulalongkorn University, 2001. (In Thai)

[4] W. Srichavengsup, "Development of fast encrypted ballot papers printing system for forged and dishonest prevention", Master's Thesis, Department of Electrical Engineering, Chulalongkorn University, 2002. (In Thai)

[5] RSA Laboratories. "What is a hash function ?" [Online]. RSA Data Security, 1995. Available from: http://www.rsasecurity.com/rsalabs/faq/2-1-6.html. (Accessed 2 January 2003).

[6] National Institute of Standards and Technology, "Secure Hash Standard (SHA-1)", Federal Information Processing Standards Publication #180-1, 1993.

[7] IDAutomation.com. "PDF417 Barcode FAQ" [Online]. IDAutomation.com, 2000. Available from: http://www.idautomation.com/pdf417faq.html (Accessed 2 January 2003).

[8] Symbol Technologies. "About PDF417" [Online]. Symbol Technologies, 2001. Available from: http://www.pdf417.com/about_pdf417.htm (Accessed 2 January 2003).

[9] Office of the Election Commission of Thailand. "Election Commission of Thailand" [Online]. Office of the Election Commission of Thailand, 2002. Available from: http://www.ect.go.th/english/ (Accessed 2 January 2003).

ประวัติผู้เขียนวิทยานิพนธ์

นายวรากร ศรีเชวงทรัพย์ เกิดเมื่อวันที่ 10 ธันวาคม พ.ศ.2519 ที่จังหวัดกรุงเทพมหานคร เข้าศึกษาในหลักสูตรวิศวกรรมศาสตรบัณฑิต คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2537 สำเร็จการศึกษาปริญญาวิศวกรรมศาสตรบัณฑิต ภาควิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2540 จากนั้นได้เข้าศึกษาต่อในหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต ที่ห้องปฏิบัติการไฟฟ้าสื่อสาร สาขาวิศวกรรมไฟฟ้า ภาควิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2542