การตรวจสอบความถูกต้องของวีดีโอด้วยลายเซ็นดิจิตอลแบบสมทบส่วนต่าง

AN INCREMENTAL DIGITAL SIGNATURE APPROACH FOR VIDEO CONTENT AUTHENTICATION

วิไลพร กุลตังวัฒนา
WILAIPORN KULTANGWATTANA

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาเทคโนโลยีสารสนเทศ
บัณฑิตวิทยาลัย
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ. 2547

ISBN 974-9708-93-8

การตรวจสอบความถูกต้องของวีดีโอด้วยลายเซ็นดิจิตอล แบบสมทบส่วนต่าง

AN INCREMENTAL DIGITAL SIGNATURE APPROACH FOR VIDEO CONTENT AUTHENTICATION

วิไลพร กุลตังวัฒนา

WILAIPORN KULTANGWATTANA

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาเทคโนโลยีสารสนเทศ

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ.2547

ISBN 974-9708-93-8

AN INCREMENTAL DIGITAL SIGNATURE APPROACH FOR VIDEO CONTENT AUTHENTICATION

WILAIPORN KULTANGWATTANA

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

SCHOOL OF GRADUATE STUDIES

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2004

ISBN 974-9708-93-8

หัวข้อวิทยานิพนธ์	การตรวจสอบความถูกต้องของวีดีโอด้วยลายเซ็นดิจิตอลแบบสมทบส่วนต่าง
นักศึกษา	นางสาววิไลพร กุลตังวัฒนา
รหัสประจำตัว	43067018
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
พ.ศ.	2547
อาจารย์ผู้ควบคุมวิทยานิพนธ์	ผศ.ดร.นพพร โชติกกำธร

บทคัดย่อ

วิทยานิพนธ์ฉบับนี้นำเสนอวิธีการสร้างลายเซ็นดิจิตอลสำหรับวีดีโอต้นฉบับและวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ โดยใช้หลักการของ Incremental-based digital signature เพื่อใช้ในการตรวจสอบความถูกต้องของวีดีโอ โดยลายเซ็นดิจิตอลจะสร้างขึ้นสำหรับแต่ละเฟรมของวีดีโอ ซึ่งได้จากการเข้ารหัส feature code ที่ได้จากการเปรียบเทียบความสัมพันธ์ของแต่ละรูปภาพย่อยในเฟรมใดๆ ของวีดีโอต้นฉบับ สำหรับวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ ลายเซ็นดิจิตอลจะสร้างจากผลต่างของ feature code ระหว่างวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับใดๆ และวีดีโอที่มีการแก้ไขโดยผู้ที่กรรมสิทธิ์ในการทำสำเนาลำดับก่อนหน้านั้น โดยจำนวนลายเซ็นดิจิตอลจะเพิ่มขึ้นตามจำนวนครั้งของการแก้ไข ซึ่งวิธีการที่นำเสนอนี้ทำให้ทราบว่าวีดีโอที่นำมาตรวจสอบมีการแก้ไขโดยผู้ที่ประสงค์ร้ายหรือไม่ และถ้ามีการแก้ไขโดยผู้ที่ประสงค์ร้ายก็สามารถระบุได้ว่าเกิดการแก้ไขที่ส่วนใดของวีดีโอเมื่อเปรียบเทียบกับวีดีโอต้นฉบับหรือวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ นอกจากนี้ยังสามารถตรวจสอบได้ว่าวีดีโอที่นำมาตรวจสอบเป็นวีดีโอต้นฉบับหรือวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ และสามารถระบุถึงความแตกต่างของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ ได้

Thesis Title	An Incremental Digital Signature Approach for Video Content Authentication
Student	Miss Wilaiporn Kultangwattana
Student ID.	43067018
Degree	Master of Science
Programme	Information Technology
Year	2004
Thesis Advisor	Asst. Prof. Dr. Nopporn Chotikakamthorn

ABSTRACT

This thesis describes a method for constructing a digital signature for both original video and its rightful modified versions. The method is based on the incremental-based digital signature principle, applied to video authentication. Digital signature corresponding to each video frame is constructed from a feature code, which in turn is obtained by comparing certain relationship between adjacent image blocks. For the rightful modified video, digital signature is generated from the feature code obtained as the difference between the rightful modified video and the original one. The proposed method can be used to detect video tampering, as well as to identify tampered areas. Besides, the method can check whether the test video is in its original version or has been rightfully modified. The method can also identify the difference between the original video and its rightful modified version.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้อย่างดี ส่วนหนึ่งก็เพราะได้รับความช่วยเหลือไม่ทางตรงก็ทางอ้อมจากบุคคลเหล่านี้ ซึ่งผู้วิจัยขอแสดงความขอบคุณ มา ณ โอกาสนี้

ขอขอบพระคุณบิดา-มารดาของผู้วิจัย ที่เป็นแรงผลักดัน ให้ทั้งกำลังใจและกำลังทรัพย์แก่ผู้วิจัยในการทำงานวิจัยนี้

ขอขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร. นพพร โชติกกำธร อาจารย์ที่ปรึกษา ผู้ซึ่งให้คำแนะนำและแนวคิดต่างๆในงานวิจัยให้แก่ผู้วิจัยอย่างอดทน อีกทั้งยังให้การสนับสนุนอุปกรณ์และเอกสารที่เกี่ยวข้องกับงานวิจัยได้อย่างดีเยี่ยม

ขอขอบคุณเจ้าหน้าที่คณะเทคโนโลยีสารสนเทศ ซึ่งให้ความอนุเคราะห์ในการอำนวยความสะดวกต่างๆ ในการทำงานตั้งแต่ต้น รวมถึงเพื่อนๆ นักศึกษาทุกคนที่ช่วยเหลือให้คำแนะนำต่างๆ พร้อมทั้งช่วยตรวจเทียบและแก้ไขทฤษฎีและอื่นๆ ที่ผิดพลาด จนสำเร็จสมบูรณ์ยิ่งขึ้นและยังให้กำลังใจต่อผู้วิจัยอย่างใกล้ชิดตลอดมา

อนึ่ง งานวิจัยที่นำเสนอในงานวิทยานิพนธ์ฉบับนี้นั้น ส่วนหนึ่งกระทำภายใต้ห้องปฏิบัติการ Multimedia and Virtual Research Laboratory ของสำนักวิจัยการสื่อสารและเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

สุดท้ายขอขอบคุณบัณฑิตวิทยาลัย ที่ได้ให้ทุนสนับสนุนการทำวิทยานิพนธ์ครั้งนี้

คุณค่าและประโยชน์อันพึงมีจากวิทยานิพนธ์ฉบับนี้ ผู้วิจัยขอมอบแด่ผู้มีพระคุณทุกท่าน

วิไลพร กุลตังวัฒนา

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

รูปที่ หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันเทคโนโลยีคอมพิวเตอร์และสื่อประสมมีการพัฒนาไปมากทำให้การแก้ไขตัดต่อวีดีโอสามารถทำได้ง่ายขึ้น เป็นเหตุให้ปัจจุบันนี้ได้มีความพยายามในการพัฒนาวิธีการตรวจสอบความถูกต้องของวีดีโอ ซึ่งสามารถแบ่งวิธีการต่างๆ ออกเป็น 2 ประเภทคือ เทคนิคของลายเซ็นดิจิตอล และเทคนิคของลายน้ำดิจิตอล

การแก้ไขวีดีโอโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ ก็เป็นปัญหาหนึ่งที่ต้องมีวิธีการตรวจสอบเพื่อที่จะทำให้ผู้ใช้วีดีโอทราบว่า วีดีโอที่ได้รับมาผ่านการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ หรือไม่ และถูกแก้ไขมากน้อยเพียงใด แต่วิธีการตรวจสอบความถูกต้องของวีดีโอที่มีอยู่ในปัจจุบันมักจะมองข้ามปัญหานี้

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

ความมุ่งหมายและวัตถุประสงค์ของการศึกษางานวิทยานิพนธ์นี้ เพื่อศึกษาและพัฒนาวิธีการตรวจสอบความถูกต้องของวีดีโอซึ่งจัดอยู่ในประเภทเทคนิคของลายเซ็นดิจิตอลให้สามารถแก้ปัญหาของวิธีการตรวจสอบความถูกต้องของวีดีโอที่มีอยู่ในปัจจุบันได้ ซึ่งปัญหาต่างๆ สามารถสรุปได้ดังต่อไปนี้

1. ไม่สามารถตรวจพบว่าวีดีโอมีการแก้ไขเมื่อเฟรมของวีดีโอมีการแก้ไขโดยการสลับค่าของพิกเซลในแถวใดๆ ของเฟรมแล้วให้ค่า feature code เท่าเดิม [5]
2. ไม่สามารถตรวจพบว่าวีดีโอมีการแก้ไขเมื่อวีดีโอมีการเปลี่ยนแปลงระดับความเข้มของแสงสว่างเฉพาะบางส่วนของเฟรม [6]
3. ไม่สามารถระบุได้ว่าส่วนใดของวีดีโอที่มีการแก้ไข [7]
4. ไม่สามารถตรวจสอบความถูกต้องของเฟรม P,B ได้ [9]
5. ไม่สามารถตรวจสอบได้ว่าวีดีโอที่นำมาตรวจสอบเป็นวีดีโอต้นฉบับหรือวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ [5, 6, 7, 8, 9]
6. ไม่สามารถระบุถึงความแตกต่างของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ ได้ [5, 6, 7, 8, 9]

1.3 ทฤษฎีหรือแนวคิดที่ใช้ในงานวิจัย

งานวิจัยนี้จะทำการตรวจสอบความถูกต้องของวีดีโอโดยใช้เทคนิคของลายเซ็นดิจิตอล ซึ่งลายเซ็นดิจิตอลจะได้จากการเข้ารหัส feature code ที่ได้จากการเปรียบเทียบความสัมพันธ์ของแต่ละรูปภาพย่อยในเฟรมใดๆ แทนการใช้ message digest ที่ได้จากกระบวนการ Hash function เพราะการใช้ feature code จะสามารถรองรับกระบวนการเปลี่ยนแปลงรูปภาพหรือวีดีโอ เช่น การตัดพื้นที่บางส่วนของรูปภาพ การปรับความสว่างของรูปภาพ การปรับความแตกต่างของความสว่างของรูปภาพ การบีบอัดรูปภาพ และการเพิ่มสัญญาณรบกวน เป็นต้น

1.4 สมมุติฐานของการศึกษา

งานวิจัยนี้จะทำการตรวจสอบความถูกต้องของวีดีโอโดยใช้เทคนิคของลายเซ็นดิจิตอล เนื่องจากไม่จำเป็นต้องใช้วีดีโอต้นฉบับในการเปรียบเทียบ โดยจะทำการแนบลายเซ็นดิจิตอลเข้าไปในเฮดเดอร์ของแต่ละเฟรมวีดีโอ

วีดีโอที่นำมาตรวจสอบอาจจะไม่ใช่วีดีโอต้นฉบับ แต่เป็นวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ ดังนั้นการตรวจสอบวีดีโอจะต้องสามารถบอกได้ว่า วีดีโอที่นำมาตรวจสอบถูกแก้ไขหรือไม่เมื่อเปรียบเทียบกับวีดีโอต้นฉบับหรือวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ

1.5 ขอบเขตของการศึกษา

1. วีดีโอที่ใช้ในงานวิจัยนี้เป็นวีดีโอที่มีการบีบอัดแบบ MPEG-1 ซึ่งจะทำการตรวจสอบความถูกต้องเฉพาะระดับความเข้มของแสงสว่างของแต่ละเฟรมเท่านั้น
2. เฟรมวีดีโอหรือรูปภาพที่ผ่านการแก้ไขเปลี่ยนแปลงและนำมาตรวจสอบถูกแก้ไขโดยกระบวนการแก้ไขรูปภาพดังต่อไปนี้
   - การปรับค่าความสว่าง
   - การปรับค่าความแตกต่างของความสว่าง
   - การบีบอัดรูปภาพแบบ JPEG
   - การเพิ่มสัญญาณรบกวน
   - การแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1
   - การแก้ไขโดยผู้ที่ประสงค์ร้าย
3. การตรวจสอบความถูกต้องของวีดีโอที่ทำการวิจัยนี้จะเป็นแบบ Non-real-time

1.6 ขั้นตอนของการศึกษา

1. กำหนดหัวข้อ เป้าหมาย จุดประสงค์ และขอบเขตของการทำวิทยานิพนธ์
2. ศึกษาทฤษฎีและหลักการพื้นฐานที่ใช้ในการวิจัย
3. ศึกษาเทคนิคต่างๆ ที่มีอยู่ถึงแนวคิด หลักการ ข้อดี และข้อบกพร่องของแต่ละเทคนิค
4. พัฒนาวิธีการสร้างลายเซ็นดิจิตอล
5. ทำการทดลอง ปรับปรุง และสรุปผล
6. จัดทำเอกสารประกอบวิทยานิพนธ์

1.7 โครงสร้างของวิทยานิพนธ์

ในบทที่ 1 จะกล่าวถึงลักษณะทั่วไปของวิทยานิพนธ์ตั้งแต่ความเป็นมา จุดเริ่มต้นและความสำคัญของปัญหา ซึ่งเป็นที่มาของการศึกษาโดยระบุถึงหลักการหรือทฤษฎีต่างๆ ที่นำมาใช้ภายใต้สมมุติฐานที่เรากำหนด โดยมีจุดมุ่งหมาย ขอบเขต และขั้นตอนในการศึกษาระบุไว้อย่างชัดเจน

สำหรับบทที่ 2 จะเป็นบทที่กล่าวถึงหลักการเบื้องต้นของการบีบอัดวีดีโอแบบ MPEG-1 และหลักการทั่วไปที่ใช้ในการตรวจสอบความถูกต้องของวีดีโอ

บทที่ 3 จะกล่าวถึงตัวอย่างของวิธีการที่ใช้ในการตรวจสอบความถูกต้องของวีดีโอรวมทั้งปัญหาต่างๆ ที่เกิดจากการใช้วิธีการเหล่านี้

ส่วนของการพัฒนาจะกล่าวไว้ในบทที่ 4 โดยในบทนี้ได้อธิบายวิธีการสร้างลายเซ็นดิจิตอลแบบสมทบส่วนต่างเพื่อใช้ในการตรวจสอบความถูกต้องของวีดีโอที่มีการบีบอัดแบบ MPEG-1

ในบทที่ 5 จะเป็นผลการทดลองการสร้างลายเซ็นดิจิตอลแบบสมทบส่วนต่างเพื่อใช้ในการตรวจสอบความถูกต้องของวีดีโอที่มีการบีบอัดแบบ MPEG-1

สำหรับในบทสุดท้าย คือบทที่ 6 เป็นบทสรุปถึงเนื้อหาทั้งหมดที่ได้กล่าวมา ผลลัพธ์ในการสร้างลายเซ็นดิจิตอลแบบสมทบส่วนต่างเพื่อใช้ในการตรวจสอบความถูกต้องของวีดีโอที่มีการบีบอัดแบบ MPEG-1

บทที่ 2
การจัดเก็บและบีบอัดข้อมูลวีดีโอ

2.1 การบีบอัดวีดีโอแบบ MPEG-1 [1]

MPEG : Moving Pictures Experts Group คือ เทคนิคที่ใช้ในการบีบอัดวีดีโอให้มีขนาดเล็กลงแต่ยังคงคุณภาพที่ดีเหมือนเดิม ซึ่งเทคนิคของการบีบอัดแบบนี้จะใช้ประโยชน์ของการซ้ำกันของเฟรมแต่ละเฟรมโดยจะทำการตัดรายละเอียดที่ซ้ำกันของเฟรมใกล้เคียงออกและเข้ารหัสเฉพาะส่วนที่แตกต่างกันเท่านั้น โดย MPEG-1 ได้กำหนดข้อจำกัดของพารามิเตอร์บิตสตรีม (Constrained parameters bit stream) ดังตารางที่ 2.1 ซึ่งตัวอย่างของวีดีโอที่ใช้เทคนิคนี้ในการบีบอัด เช่น วีดีโอซีดี เป็นต้น

ตารางที่ 2.1 ข้อจำกัดของพารามิเตอร์ MPEG-1

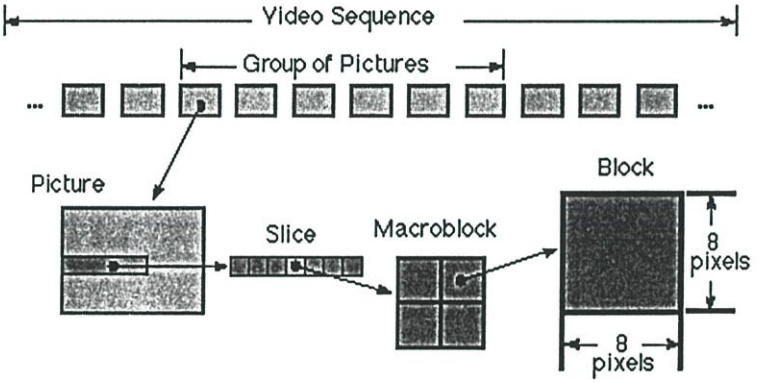
พารามิเตอร์	ค่าสูงสุด
ขนาดของเฟรมในแนวนอน	768 พิกเซล
ขนาดของเฟรมในแนวตั้ง	576 เส้น
จำนวนมาโครบล็อกต่อเฟรม	396
จำนวนมาโครบล็อกต่อวินาที	9900
อัตราเฟรมต่อวินาที	30
อัตราบิตต่อวินาที	1,856,000

MPEG-1 จะกำหนดการเข้ารหัสแบบลำดับชั้น ซึ่งแบ่งเป็น 6 ชั้น คือ

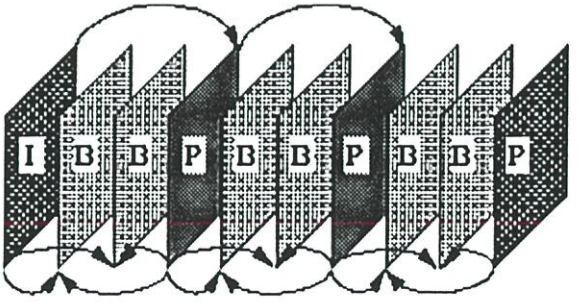
1. **ชั้นของลำดับภาพ (Video Sequence)** เป็นชั้นสูงสุดของการเข้ารหัส ซึ่งจะประกอบด้วยกลุ่มของรูปภาพหนึ่งกลุ่มหรือมากกว่านั้น
2. **ชั้นของกลุ่มของรูปภาพ (Group of Picture)** คือรูปภาพจำนวนหนึ่งที่แสดงผลต่อเนื่องกันเป็นลำดับซึ่งจะต้องมีรูปภาพ (I-frame) อย่างน้อย 1 ภาพ เป็นส่วนประกอบ แต่โดยทั่วไปจะประกอบด้วยรูปภาพประมาณ 10-30 ภาพ
3. **ชั้นของรูปภาพ (Picture)** แต่ละรูปภาพจะเรียกว่า เฟรม ซึ่งแบ่งออกเป็น 3 ชนิด คือ
   - **เฟรมที่เข้ารหัสภายใน (Intracoded Frame : I - frame)** เป็นเฟรมที่มีการเข้ารหัสในลักษณะเฟรมเดี่ยวๆ โดยไม่ได้ใช้ประโยชน์ของข้อมูลในเฟรมอื่นๆ ดังนั้นการบีบอัด

จึงทำได้น้อย ซึ่งเฟรม I นี้จะเป็นเฟรมที่มีข้อมูลอยู่มากที่สุด เนื่องจากต้องเก็บข้อมูลทั้งหมดของเฟรมไว้อย่างชัดเจนเพื่อเป็นเฟรมหลักที่เฟรมอื่นๆ จะนำข้อมูลไปใช้

- **เฟรมที่เข้ารหัสแบบทำนาย (Predicted Frame : P – frame)** เป็นเฟรมที่มีการเข้ารหัสโดยเปรียบเทียบกับข้อมูลของเฟรม I และเฟรม P ที่ถูกแสดงมาในลำดับก่อนหน้าของเฟรมที่จะทำการเข้ารหัส (เฟรม P) โดยจะเก็บข้อมูลเฉพาะส่วนที่เปลี่ยนไปเท่านั้น ดังนั้นการบีบอัดจึงทำได้มากขึ้นเพราะสามารถกำจัดส่วนที่ซ้ำซ้อนกันของเฟรมออกไปได้
- **เฟรมที่เข้ารหัสแบบทำนายสองทิศทาง (Bidirectional Frame : B – frame)** เป็นเฟรมที่มีการเข้ารหัสโดยเปรียบเทียบกับข้อมูลของเฟรม I และเฟรม P ที่ถูกแสดงมาในลำดับก่อนหน้าและล่วงหน้าของเฟรมที่จะทำการเข้ารหัส (เฟรม B) โดยจะเก็บข้อมูลเฉพาะส่วนที่เปลี่ยนไปเท่านั้น ดังนั้นการบีบอัดจึงทำได้มากที่สุด เพราะสามารถกำจัดส่วนที่ซ้ำซ้อนกันของเฟรมออกไปได้มากที่สุด



รูปที่ 2.1 ลำดับชั้นของ MPEG-1



รูปที่ 2.2 ลำดับของเฟรม

4. **ชั้นของสไลด์ (Slice)** คือ กลุ่มของมาโครบล็อก ที่อยู่ติดกันโดยเริ่มจากซ้ายไปขวาและบนลงล่าง โดยแต่ละสไลด์อาจจะมีเพียง 1 มาโครบล็อกหรือมากกว่าก็ได้
5. **ชั้นของมาโครบล็อก (Macroblock)** จะมีรูปแบบของสีเป็นแบบ YCbCr ซึ่งแยกออกเป็นระดับความเข้มของแสงสว่าง (Y) และระดับความเข้มของสี (Cb,Cr) โดยมาโครบล็อกจะประกอบด้วย 4 บล็อกสำหรับระดับความเข้มของแสงสว่าง และ 1 บล็อกสำหรับแต่ละระดับความเข้มของสี
6. **ชั้นของบล็อก (Block)** คือชั้นต่ำสุดของการเข้ารหัส ซึ่งมีขนาด 8×8 พิกเซล

2.2 การตรวจสอบความถูกต้องของวีดีโอ [3]

2.2.1 การตรวจสอบความถูกต้องอย่างสมบูรณ์ (Exact authentication) คือ การตรวจสอบความถูกต้องของวีดีโอที่พิจารณาความถูกต้องของทุกๆ บิตในวีดีโอ โดยวีดีโอจะมีความถูกต้องก็ต่อเมื่อทุกๆ บิตไม่มีการแก้ไขเปลี่ยนแปลงใดๆ ดังนั้นการตรวจสอบความถูกต้องของวีดีโอประเภทนี้จึงไม่สามารถรองรับการเปลี่ยนแปลงทั่วๆ ไปของวีดีโอ เช่น การตัดพื้นที่บางส่วนของรูปภาพ การปรับความสว่างของรูปภาพ การปรับความแตกต่างของความสว่างของรูปภาพ การบีบอัดรูปภาพ และการเพิ่มสัญญาณรบกวน เป็นต้น

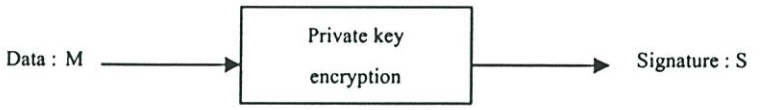
2.2.2 การตรวจสอบความถูกต้องเฉพาะส่วน (Selective authentication) คือ การตรวจสอบความถูกต้องของวีดีโอที่พิจารณาความถูกต้องของเนื้อหาในวีดีโอ โดยวีดีโอจะมีความถูกต้องก็ต่อเมื่อความหมายของเนื้อหาในวีดีโอไม่มีการแก้ไขเปลี่ยนแปลงใดๆ ถึงแม้ว่าบางบิตในวีดีโอจะถูกแก้ไขเปลี่ยนแปลง ดังนั้นการตรวจสอบความถูกต้องของวีดีโอประเภทนี้จึงสามารถรองรับการเปลี่ยนแปลงทั่วๆ ไปของวีดีโอ เช่น การตัดพื้นที่บางส่วนของรูปภาพ การปรับความสว่างของรูปภาพ การปรับความแตกต่างของความสว่างของรูปภาพ การบีบอัดรูปภาพ และการเพิ่มสัญญาณรบกวน เป็นต้น

2.3 เทคนิคของการตรวจสอบความถูกต้องของวีดีโอ

2.3.1 ลายเซ็นดิจิตอล (Digital Signature)

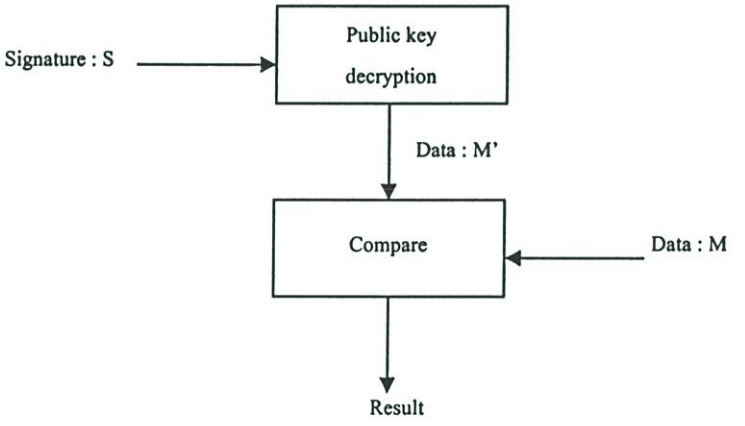
การใช้ลายเซ็นดิจิตอลบนสื่อดิจิตอลจะเหมือนกับลายเซ็นที่ใช้เซ็นในเอกสารทั่วไปที่สามารถพิสูจน์ได้ว่าเป็นลายเซ็นของใครและไม่สามารถปลอมแปลงได้

ลายเซ็นดิจิตอล คือ การนำเอกสารที่ต้องการส่งออกไปมาเข้ารหัสด้วย private key ของผู้ส่ง จะได้ลายเซ็นดิจิตอลส่งออกไปพร้อมกับเอกสารที่ต้องการส่ง ดังรูปที่ 2.3



รูปที่ 2.3 การสร้างลายเซ็นดิจิตอล

เมื่อผู้รับต้องการตรวจสอบความถูกต้องของเอกสารที่ได้รับก็จะนำลายเซ็นดิจิตอล (S) มาถอดรหัสด้วย public key ของผู้ส่ง จะได้ข้อมูลเอกสาร (M') และนำมาเปรียบเทียบกับเอกสารที่ได้รับ (M) ถ้าเหมือนกันแสดงว่าเอกสารที่ได้รับมาถูกต้อง ดังรูปที่ 2.4



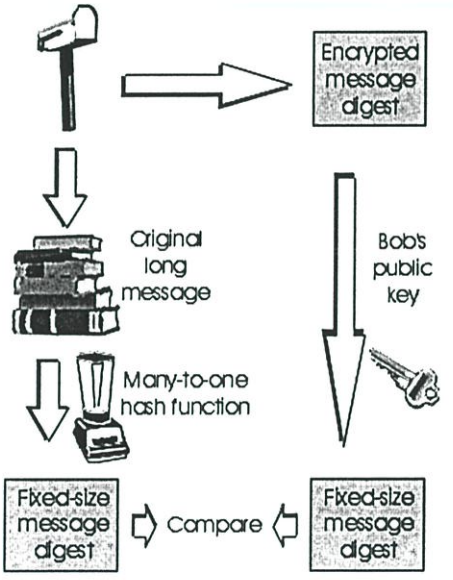
รูปที่ 2.4 การตรวจสอบความถูกต้องของเอกสาร

การเข้ารหัสข้อความที่ยาวนั้นจะใช้เวลานานเนื่องจากขั้นตอนการเข้ารหัสต้องใช้การคำนวณมากจึงมีการเปลี่ยนข้อความทั้งหมดด้วยกระบวนการที่เรียกว่า Hash function ให้เหลือเพียงข้อความสั้นๆ ที่เป็นเอกลักษณ์เฉพาะเพื่อเป็นตัวแทนของข้อความทั้งหมดโดยเรียกว่า message digest ดังรูปที่ 2.5

รูปที่ 2.5 Hash function ถูกใช้สร้าง message digest

เมื่อผู้ส่งต้องการส่งเอกสารถึงผู้รับ ก็จะนำเอกสารต้นฉบับผ่านกระบวนการ Hash function เพื่อสร้าง message digest แล้วทำการเข้ารหัส message digest ด้วย private key ของผู้ส่งก็จะได้ลายเซ็นดิจิตอลส่งไปพร้อมกับเอกสาร

ขั้นตอนการตรวจสอบความถูกต้องของเอกสารสามารถทำได้โดยถอดรหัสลายเซ็นดิจิตอลด้วย public key ของผู้ส่ง ก็จะได้ message digest และใช้ Hash function เปลี่ยนเอกสารที่ได้รับมาเป็น message digest อีกชุด จากนั้นนำมาเปรียบเทียบกัน หากเหมือนกันแสดงว่าเอกสารที่ได้รับมาถูกต้อง ดังรูปที่ 2.6



รูปที่ 2.6 การตรวจสอบความถูกต้องของเอกสาร

2.3.2 ลายน้ำดิจิตอล (Digital Watermark)

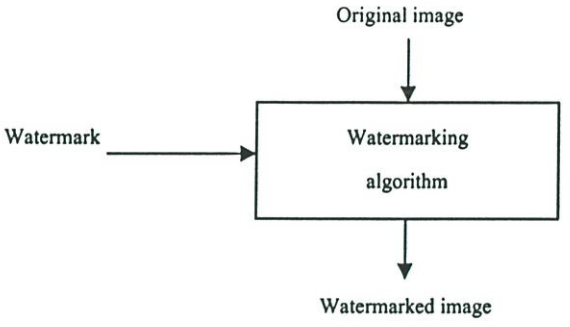
2.3.2.1 การสร้างลายน้ำดิจิตอล

หลักการเบื้องต้นในการสร้างลายน้ำดิจิตอลสามารถแสดงได้ดังรูปที่ 2.7 กล่าวคือจะทำการซ่อนลายน้ำดิจิตอลเข้าไปในรูปภาพด้วยวิธีการต่างๆ ตามวัตถุประสงค์ที่ต้องการ เช่น ถ้าต้องการพิสูจน์ความถูกต้องของรูปภาพก็จะต้องซ่อนลายน้ำดิจิตอลด้วยวิธีการต่างๆ ที่จัดอยู่ในประเภท fragile watermark เป็นต้น

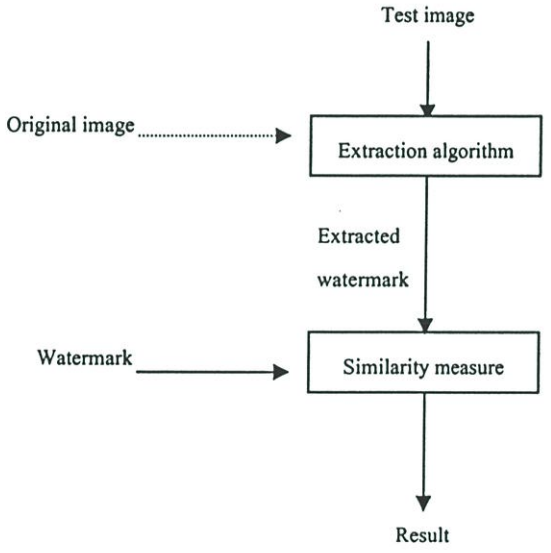
2.3.2.2 การดึงลายน้ำดิจิตอล

หลักการเบื้องต้นในการดึงลายน้ำดิจิตอลนั้นจะต้องทำการตรวจหาลายน้ำดิจิตอล ซึ่งอาจจะใช้รูปภาพต้นฉบับในการตรวจหาลายน้ำดิจิตอลหรือไม่นั้นขึ้นอยู่กับประเภทของเทคนิคลายน้ำดิจิตอล (Oblivious คือ ไม่ต้องใช้รูปภาพต้นฉบับในการตรวจหาลายน้ำดิจิตอล , Non-Oblivious คือ

ต้องใช้รูปภาพต้นฉบับในการตรวจหาลายน้ำดิจิตอล) และเมื่อได้ลายน้ำดิจิตอลออกมาแล้วจึงนำไปเปรียบเทียบกับลายน้ำดิจิตอลต้นฉบับ เพื่อพิสูจน์ความเป็นเจ้าของหรือพิสูจน์ความถูกต้องของรูปภาพ ดังรูปที่ 2.8



รูปที่ 2.7 การสร้างลายน้ำดิจิตอล



รูปที่ 2.8 การดึงลายน้ำดิจิตอล

2.3.2.3 ลายน้ำดิจิตอลที่ใช้ในการตรวจสอบความถูกต้อง

- **ลายน้ำเปราะบาง (Fragile Watermark)** คือลายน้ำดิจิตอลที่ถูกทำลายหรือผิดเพี้ยนได้ง่าย เมื่อค่าของพิกเซลต่างๆ เกิดการเปลี่ยนแปลงเนื่องจากกระบวนการประมวลผลภาพด้วยวิธีต่างๆ ทั้งที่เจตนาและไม่เจตนา ดังนั้นจึงนำมาใช้ในการพิสูจน์ความถูกต้องของรายละเอียดข้อมูลของสื่อ
- **ลายน้ำกึ่งเปราะบาง (Semi Fragile Watermark)** คือลายน้ำดิจิตอลที่ถูกทำลายหรือผิดเพี้ยนเมื่อค่าของพิกเซลต่างๆ เกิดการเปลี่ยนแปลงเนื่องจากกระบวนการประมวลผล

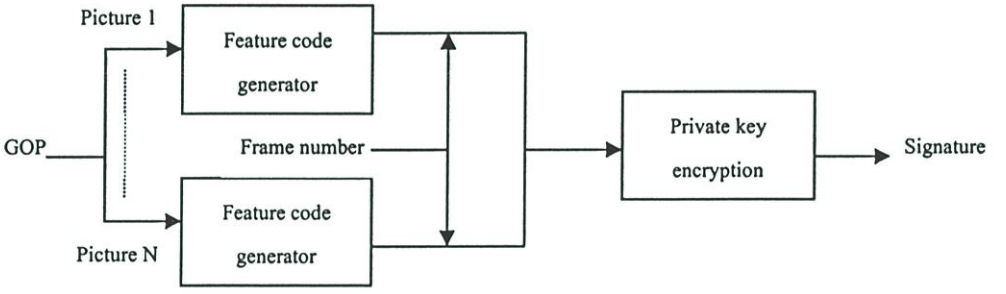
ภาพด้วยวิธีต่างๆ ของผู้ที่ประสงค์ร้าย แต่จะมีความคงทนต่อการเปลี่ยนแปลงทั่วๆ ไปของรูปภาพ เช่น การตัดพื้นที่บางส่วนของรูปภาพ การปรับความสว่างของรูปภาพ การปรับความแตกต่างของความสว่างของรูปภาพ การบีบอัดรูปภาพ และการเพิ่มสัญญาณรบกวน เป็นต้น

บทที่ 3
งานวิจัยที่เกี่ยวข้อง

3.1 ตัวอย่างการใช้เทคนิคของลายเซ็นดิจิตอล

3.1.1 วิธีการของ Ching-Yung Lin [5]

ลายเซ็นดิจิตอลจะสร้างขึ้นสำหรับแต่ละกลุ่มของเฟรมวีดีโอ (Group of picture: GOP) โดยมีขั้นตอนคือ นำ feature code ของแต่ละเฟรมที่ได้จากกระบวนการ Feature code generator มารวมกับลำดับที่ของเฟรม แล้วเข้ารหัสด้วย private key ดังรูปที่ 3.1



รูปที่ 3.1 การสร้างลายเซ็นดิจิตอล

Feature code generator

มีขั้นตอนคือ แบ่งรูปภาพออกเป็นรูปภาพย่อยขนาด 8×8 พิกเซล และแบ่งรูปภาพย่อยต่างๆ ออกเป็น 2 กลุ่ม และนำค่า DCT coefficient ของแต่ละรูปภาพย่อยในกลุ่มที่ 1 และกลุ่มที่ 2 ที่อยู่ในลำดับเดียวกันมาเปรียบเทียบกัน ดังสมการที่ 3.1

$$F_a = \begin{cases} 1 & \text{if} \quad D_a \geq D_b \\ 0 & \text{if} \quad D_a < D_b \end{cases} \tag{3.1}$$

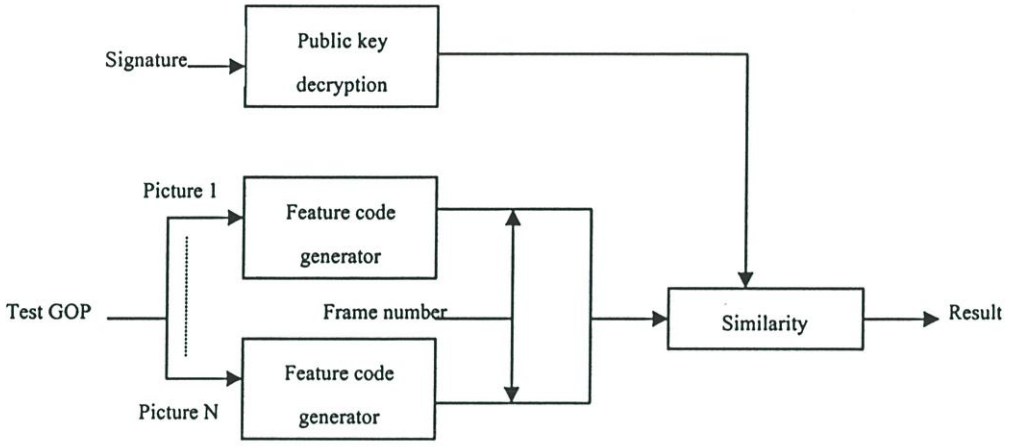
โดยที่

D_a คือ DCT coefficient ของรูปภาพย่อยตำแหน่งที่ a

D_b คือ DCT coefficient ของรูปภาพย่อยตำแหน่งที่ b

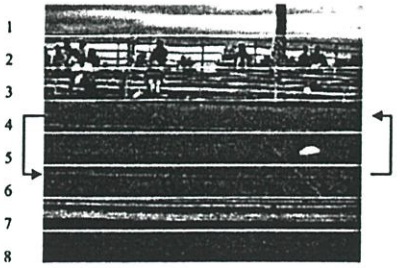
F_a คือ feature code ของรูปภาพย่อยตำแหน่งที่ a

ส่วนวิธีการตรวจสอบความถูกต้องของวีดีโอมีขั้นตอนคือ นำลายเซ็นดิจิตอลมาถอดรหัสด้วย public key ก็จะได้ feature code แล้วนำ feature code ที่ได้ไปเปรียบเทียบกับ feature code ของเฟรมวีดีโอที่นำมาตรวจสอบ ถ้าเหมือนกันก็แสดงว่ากลุ่มของเฟรมวีดีโอ (GOP) ที่นำมาตรวจสอบมีความถูกต้อง ดังรูปที่ 3.2



รูปที่ 3.2 การตรวจสอบความถูกต้องของวีดีโอ

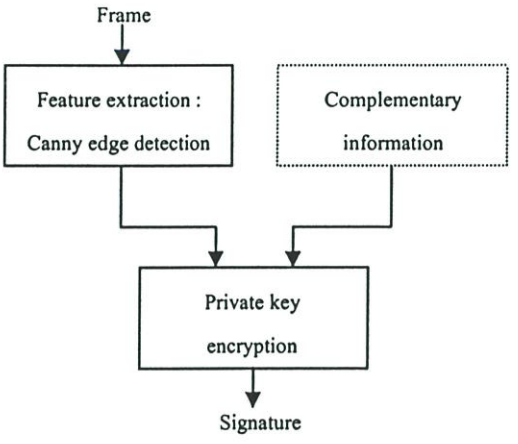
วิธีนี้จะสามารถตรวจสอบความถูกต้องของเฟรมวีดีโอได้ ถึงแม้ว่ากลุ่มของเฟรมวีดีโอ (GOP) จะถูกแก้ไข โดยสามารถระบุตำแหน่งของวีดีโอที่ถูกแก้ไขได้ แต่ถ้ามีการสลับลำดับที่ของรูปภาพย่อยในกลุ่มที่ 1 หรือ 2 แล้วให้ค่า feature code เหมือนเดิม ก็จะไม่สามารถตรวจพบว่าวีดีโอมีการแก้ไข เช่นจากรูปที่ 3.3 กำหนดให้รูปภาพย่อยในแถวที่ 1,3,5,7 อยู่ในกลุ่มที่ 1 และรูปภาพย่อยในแถวที่ 2,4,6,8 อยู่ในกลุ่มที่ 2 ถ้าสลับแถวระหว่างแถวที่ 4 และแถวที่ 6 แล้วให้ค่า feature code เหมือนเดิมก็จะไม่สามารตรวจพบว่าวีดีโอมีการแก้ไข



รูปที่ 3.3 ตัวอย่างวิธีการแก้ไขรูปภาพที่ไม่สามารถตรวจพบได้

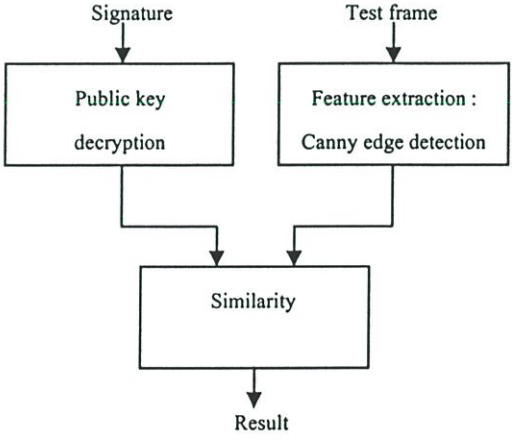
3.1.2 วิธีการของ Jana Dittmann [6]

ลายเซ็นดิจิตอลจะสร้างขึ้นสำหรับแต่ละเฟรมของวีดีโอ ซึ่งได้จากการนำขอบของรูปภาพ ที่สามารถหาได้โดยใช้วิธี Canny edge detection มารวมกับข้อมูลอื่นๆ (complementary information) เช่น ลำดับที่ของเฟรม อัตราการแสดงภาพ เป็นต้น แล้วเข้ารหัสด้วย private key ดังรูปที่ 3.4



รูปที่ 3.4 การสร้างลายเซ็นดิจิตอล

ส่วนวิธีการตรวจสอบความถูกต้องของวีดีโอมีขั้นตอนคือ นำลายเซ็นดิจิตอลมาถอดรหัสด้วย public key ก็จะได้ขอบของรูปภาพ แล้วนำขอบของรูปภาพที่ได้ไปเปรียบเทียบกับขอบของรูปภาพที่นำมาตรวจสอบ ถ้าเหมือนกันก็แสดงว่าเฟรมของวีดีโอมีความถูกต้อง ดังรูปที่ 3.5

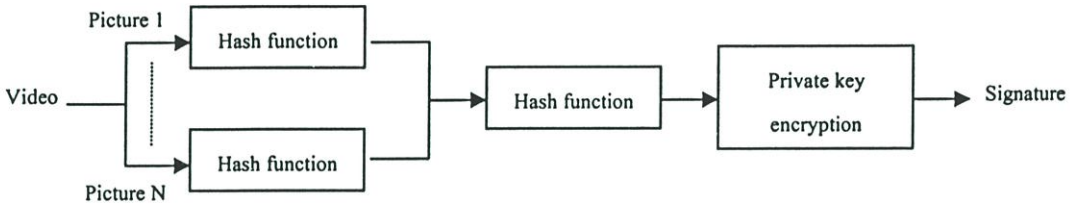


รูปที่ 3.5 การตรวจสอบความถูกต้องของวีดีโอ

วิธีนี้มีข้อเสียคือจะไม่สามารถตรวจพบว่าเฟรมมีการแก้ไขเมื่อเฟรมมีการเปลี่ยนแปลงระดับความเข้มของแสงสว่างเฉพาะบางส่วนของเฟรม

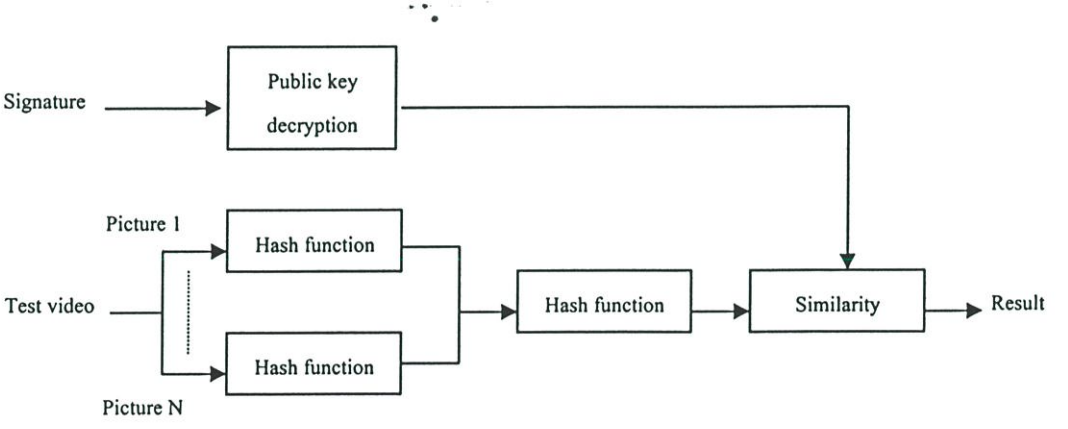
3.1.3 วิธีการของ Marc Schneider [7]

ลายเซ็นดิจิตอลจะได้จากการนำ message digest ของวีดีโอ มาเข้ารหัสด้วย private key ซึ่ง message digest สามารถหาได้โดยนำทุกเฟรมมาผ่านกระบวนการ Hash function ก็จะได้ message digest ของแต่ละเฟรม แล้วนำ message digest ทั้งหมดมาผ่านกระบวนการ Hash function อีกครั้งหนึ่งก็จะได้ message digest ของวีดีโอ ดังรูปที่ 3.6



รูปที่ 3.6 การสร้างลายเซ็นดิจิตอล

ส่วนวิธีการตรวจสอบความถูกต้องของวีดีโอมีขั้นตอนคือ ถอดรหัสลายเซ็นดิจิตอลด้วย public key ก็จะได้ message digest มาเปรียบเทียบกับ message digest ของวีดีโอที่นำมาตรวจสอบ ถ้าเหมือนกันก็แสดงว่าวีดีโอมีความถูกต้อง ดังรูปที่ 3.7



รูปที่ 3.7 การตรวจสอบความถูกต้องของวีดีโอ

วิธีนี้มีข้อเสียคือ ถ้ามีบางเฟรมถูกแก้ไขก็จะไม่สามารถระบุได้ว่าส่วนใดของวีดีโอที่มีการแก้ไข

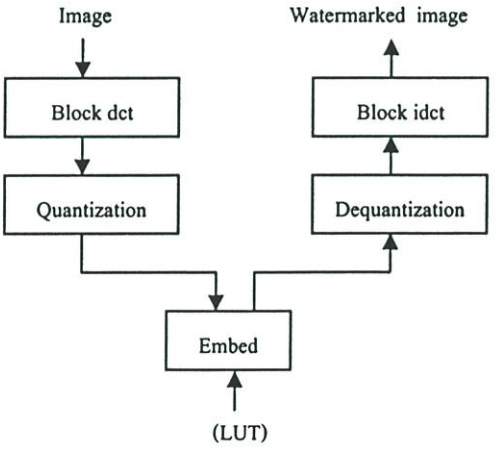
3.2 ตัวอย่างการใช้เทคนิคของลายน้ำดิจิตอล

3.2.1 วิธีการของ Bijan G. Mobasseri [8]

วิธีนี้จะทำการซ่อนลายน้ำดิจิตอลในทุกเฟรมของวีดีโอ โดยอาศัยหลักการของ Spread Spectrum Technique ซึ่งจะทำให้ลายน้ำดิจิตอลทนต่อกระบวนการเปลี่ยนแปลงต่างๆ (robust watermark) ทำให้สามารถตรวจสอบได้ว่าเฟรมใดถูกตัดหรือถูกแทรกเข้ามา

Spread Spectrum Technique คือเทคนิคการมอดูเลชั่นในระบบสื่อสารที่ใช้ขนาดความกว้างของช่องสัญญาณ (Bandwidth) มากกว่าที่ใช้ในเทคนิคการมอดูเลชั่นแบบอื่น ทำให้สามารถลดขนาดของสัญญาณที่จะทำการส่งในแต่ละช่วงความถี่ลงไปได้ ทำให้การส่งสัญญาณด้วยเทคนิคนี้มีความทนทานสูง และตรวจจับได้ยากเนื่องจากระดับสัญญาณในแต่ละย่านความถี่มีระดับต่ำมาก (อยู่ในระดับเดียวกับสัญญาณรบกวนที่มีอยู่ทั่วไปในช่องสัญญาณ) จากคุณสมบัตินี้สามารถนำมาประยุกต์ใช้กับการซ่อนลายน้ำดิจิตอลเข้าไปในรูปภาพได้เป็นอย่างดี โดยรูปภาพที่ต้องการซ่อนลายน้ำดิจิตอลนั้นเปรียบเสมือนกับช่องสัญญาณที่จะทำการส่งข้อมูล ในขณะที่แต่ละพิกเซลของรูปภาพเปรียบเสมือนสัญญาณรบกวนในระบบสื่อสาร และลายน้ำดิจิตอลเปรียบเสมือนข้อมูลที่ต้องการจะส่งเข้าไปในช่องสัญญาณ ซึ่งเทคนิคนี้จะทำการกระจายความถี่ของลายน้ำดิจิตอลทำให้ความสว่างของลายน้ำดิจิตอลอยู่ในระดับต่ำเพียงพอที่จะไม่ทำให้รูปภาพที่ซ่อนลายน้ำดิจิตอลเกิดการผิดเพี้ยนหรือเปลี่ยนแปลงจนสามารถสังเกตเห็นได้ และลายน้ำดิจิตอลจะมีความทนทานต่อการประมวลผลรูปภาพทั้งในกรณีที่กระทำโดยเจตนาที่จะทำลายลายน้ำที่ซ่อนอยู่ หรือในกรณีอื่นๆ เช่น เพื่อปรับปรุงรูปภาพ หรือเพื่อลดขนาดของรูปภาพ เป็นต้น

3.2.2 วิธีการของ Minwu [9]



รูปที่ 3.8 ขั้นตอนการซ่อนลายน้ำดิจิตอลโดยใช้ Lookup Table

วิธีนี้จะทำการซ่อนลายน้ำดิจิตอลเฉพาะเฟรม I ดังนั้นจึงไม่สามารถตรวจสอบความถูกต้องของเฟรม P,Bได้ ซึ่งการซ่อนลายน้ำดิจิตอลด้วยวิธีนี้จะมีวิธีคือ ทำการซ่อนลายน้ำดิจิตอล (binary

image) เข้าไปใน quantized DCT coefficient โดยใช้ Lookup Table ดังรูปที่ 3.8 ซึ่ง quantized DCT coefficient จะได้จากการแบ่งรูปภาพออกเป็นรูปภาพย่อยที่มีขนาด 8×8 พิกเซล แล้วนำรูปภาพย่อยมาผ่านกระบวนการ DCT ก็จะได้ DCT coefficient เพื่อนำไปหาค่า quantized DCT coefficient จากกระบวนการ Quantization ซึ่งมีสูตรในการคำนวณ ดังสมการที่ 3.2

$$Y_Q[x,y] = \text{Integer Round}\left(\frac{Y[x,y]}{q[x,y]}\right) \tag{3.2}$$

โดยที่

$Y_Q[x,y]$ คือ quantized DCT coefficient ตำแหน่งที่ x,y

$Y[x,y]$ คือ DCT coefficient ตำแหน่งที่ x,y

$q[x,y]$ คือ quantization table ตำแหน่งที่ x,y

$$q = \begin{matrix} 8 & 16 & 19 & 22 & 26 & 27 & 29 & 34 \\ 16 & 16 & 22 & 24 & 27 & 29 & 34 & 37 \\ 19 & 22 & 26 & 27 & 29 & 34 & 34 & 38 \\ 22 & 22 & 26 & 27 & 29 & 34 & 37 & 40 \\ 22 & 26 & 27 & 29 & 32 & 35 & 40 & 48 \\ 26 & 27 & 29 & 32 & 35 & 40 & 48 & 58 \\ 26 & 27 & 29 & 34 & 38 & 46 & 56 & 69 \\ 27 & 29 & 35 & 38 & 46 & 56 & 69 & 83 \end{matrix}$$

ส่วนกระบวนการ Dequantization มีสูตรในการคำนวณดังสมการที่ 3.3

$$Y[x,y] = Y_Q[x,y] \times q[x,y] \tag{3.3}$$

สำหรับวิธีการซ่อนลายน้ำดิจิตอลโดยใช้ Lookup Table (LUT : จะมี 2 แถวคือ แถวแรกจะเก็บค่า quantized DCT coefficient ต่างๆ ส่วนแถวที่ 2 จะเก็บค่าตัวเลขสุ่ม 1 และ 0) ที่ได้สร้างเอาไว้แล้ว สามารถทำได้ดังสมการที่ 3.4

$$V_i' = \begin{cases} V_i & \text{if} \quad LUT(V_i) = b_i \\ V_i + \delta & \text{if} \quad LUT(V_i) \neq b_i \text{and} \quad \delta = \min_{|d|}\{d \in Z : LUT(V_i + d) = b_i\} \end{cases} \tag{3.4}$$

โดยที่

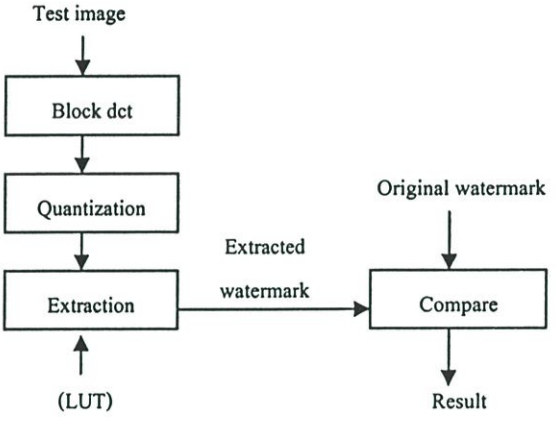
V_i คือ quantized DCT coefficient ของรูปภาพที่ต้องการซ่อนลายน้ำดิจิตอล

V_i' คือ quantized DCT coefficient ของรูปภาพที่มีลายน้ำดิจิตอลซ่อนอยู่

b_i คือ พิกเซลของลายน้ำดิจิตอล

b_i' คือ พิกเซลของลายน้ำดิจิตอลที่ได้จากการตรวจสอบ

การดึงลายน้ำดิจิตอล สามารถทำได้ดังรูปที่ 3.9 โดยจะนำรูปภาพที่ต้องการตรวจหาลายน้ำดิจิตอลมาแบ่งออกเป็นรูปภาพย่อยที่มีขนาด 8×8 พิกเซล แล้วนำรูปภาพย่อยมาหาค่า quantized DCT coefficient แล้วดึงลายน้ำดิจิตอลโดยใช้ Lookup Table ตามสมการที่ 3.5 และนำลายน้ำดิจิตอลที่ได้ไปเปรียบเทียบกับลายน้ำดิจิตอลต้นฉบับ ถ้าเหมือนกันก็แสดงว่ารูปภาพมีความถูกต้อง

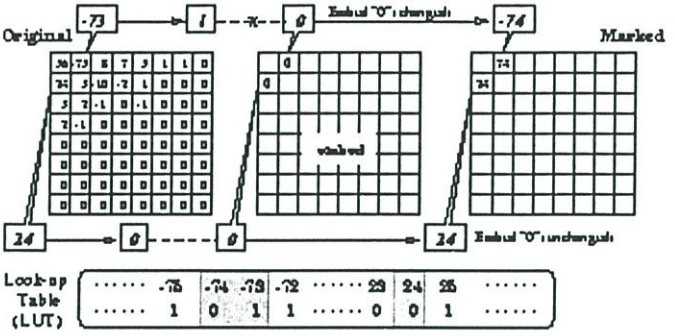


รูปที่ 3.9 ขั้นตอนการดึงลายน้ำดิจิตอลโดยใช้ Lookup Table

$$b_i' = \mathrm{LUT}(V_i') \tag{3.5}$$

ตัวอย่างการซ่อนลายน้ำดิจิตอลเข้าไปในรูปภาพ เช่น ต้องการซ่อนลายน้ำดิจิตอลที่มีค่าเท่ากับ 0 ลงในพิกเซลของรูปภาพที่มีค่า quantized DCT coefficient เท่ากับ 24 ซึ่งเมื่อดูใน LUT จะพบว่าค่าในแถวที่ 2 ของ LUT ที่มีค่า quantized DCT coefficient เท่ากับ 24 คือ 0 ดังนั้นค่า quantized DCT coefficient ของรูปภาพที่มีลายน้ำดิจิตอลซ่อนอยู่จะมีค่าเท่าเดิมคือ 24 แต่ถ้าต้องการซ่อนลายน้ำดิจิตอลที่มีค่าเท่ากับ 0 ลงในพิกเซลของรูปภาพที่มีค่า quantized DCT coefficient เท่ากับ –73 ซึ่งเมื่อดูใน LUT จะพบว่าค่าในแถวที่ 2 ของ LUT ที่มีค่า quantized DCT coefficient เท่ากับ –73 คือ 1 เพราะฉะนั้น จะต้องเลือกค่า quantized DCT coefficient ที่มีค่าใกล้เคียงกับ –73 มากที่สุดที่มีค่าในแถวที่ 2 เท่ากับ 0 ซึ่งก็คือ –74 ดังนั้น ค่า quantized DCT coefficient ของรูปภาพที่มีลายน้ำดิจิตอลซ่อนอยู่จะเท่ากับ -74 ดังรูปที่ 3.10 สำหรับค่าของลายน้ำดิจิตอลที่ได้จากรูปภาพที่นำมาตรวจสอบจะมีค่าเท่ากับค่าในแถวที่ 2 ของ LUT ที่มีค่า quantized DCT coefficient เท่ากับค่า quantized DCT

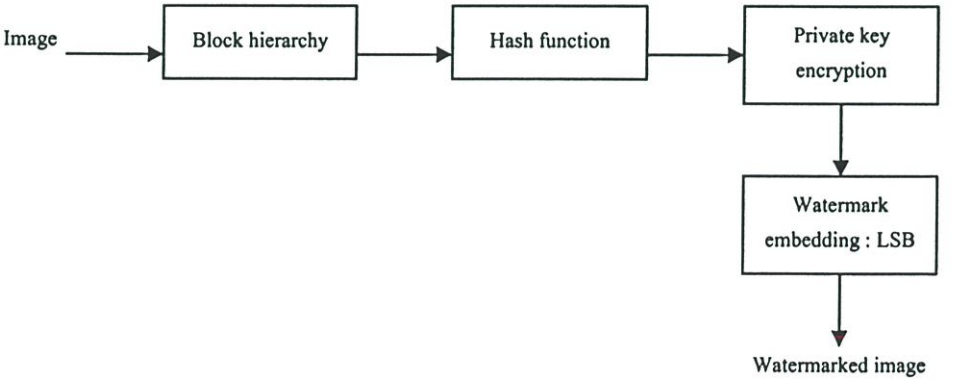
coefficient ของรูปภาพที่นำมาตรวจสอบ เช่น ค่า quantized DCT coefficient ของรูปภาพเท่ากับ –74 และ 24 แสดงว่าค่าของพิกเซลของลายน้ำดิจิตอลเท่ากับ 0



รูปที่ 3.10 ตัวอย่างวิธีการซ่อนลายน้ำดิจิตอลโดยใช้ Lookup Table

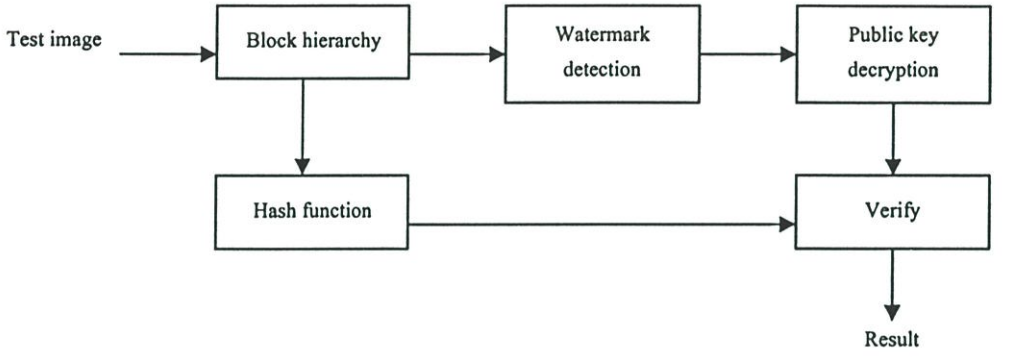
3.2.3 วิธีการของ Mehmet Utka Celik [10]

วิธีนี้จะทำการซ่อนลายน้ำดิจิตอลแบบลำดับชั้นเข้าไปในรูปภาพ โดยมีขั้นตอนคือ แบ่งรูปภาพออกเป็นรูปภาพย่อยแบบลำดับชั้น (โดยชั้นล่างสุดของรูปภาพย่อยจะมีขนาดเล็กที่สุดและชั้นถัดไปรูปภาพย่อยจะมีขนาดเป็น 2×2 เท่า ของชั้นที่อยู่ต่ำลงมาส่วนชั้นบนสุดรูปภาพย่อยจะมีขนาดเท่ากับขนาดของรูปภาพ) คำนวณหา message digest ของแต่ละรูปภาพย่อยจากกระบวนการ Hash function และนำ message digest ที่ได้มาเข้ารหัสด้วย private key ก็จะได้ลายเซ็นดิจิตอลของแต่ละรูปภาพย่อย แล้วซ่อนลายเซ็นดิจิตอลเข้าไปในแต่ละรูปภาพย่อยของชั้นล่างสุดด้วยวิธีการ Least Significant Bit Replacement : LSB ดังรูปที่ 3.11



รูปที่ 3.11 การซ่อนลายน้ำดิจิตอล

ส่วนวิธีการตรวจสอบความถูกต้องของรูปภาพมีขั้นตอนคือ แบ่งรูปภาพออกเป็นรูปภาพย่อยแบบลำดับชั้น และดึงลายเซ็นดิจิตอลออกจากรูปภาพแล้วถอดรหัสลายเซ็นดิจิตอลด้วย public key จะได้ message digest มาเปรียบเทียบกับ message digest ของแต่ละรูปภาพย่อยของรูปภาพที่นำมาตรวจสอบ ถ้าเหมือนกันแสดงว่ารูปภาพมีความถูกต้อง ดังรูปที่ 3.12



รูปที่ 3.12 การตรวจสอบความถูกต้องของรูปภาพ

วิธีนี้มีข้อเสียคือ ถ้าการตรวจสอบพบว่ารูปภาพย่อยชั้นบนสุดเท่านั้นที่มีการแก้ไข ก็จะไม่สามารถระบุได้ว่ามีการแก้ไขที่ส่วนใดของรูปภาพ

จากวิธีการข้างต้นพบว่า การใช้เทคนิคของลายเซ็นดิจิตอลในการตรวจสอบความถูกต้องของวีดีโอจะมีความปลอดภัยมากกว่าการใช้เทคนิคของลายน้ำดิจิตอล เนื่องจากลายเซ็นดิจิตอลไม่สามารถปลอมหรือแก้ไขได้ แต่ลายน้ำดิจิตอลสามารถปลอมหรือแก้ไขได้ถ้าลายน้ำดิจิตอลเป็นอิสระหรือไม่ได้สร้างจากวีดีโอที่ทำการซ่อนลายน้ำดิจิตอลนั้น เช่น ผู้ที่ประสงค์ร้ายสามารถดึงลายน้ำดิจิตอลของวีดีโอต้นฉบับออกมาก่อนแล้วจึงซ่อนกลับเข้าไปในวีดีโอที่มีการแก้ไข เมื่อผู้ใช้ทำการตรวจสอบความถูกต้องของวีดีโอก็จะไม่พบว่าวีดีโอมีการแก้ไขเนื่องจากลายน้ำดิจิตอลไม่ได้ถูกทำลายหรือผิดเพี้ยนไปจากลายน้ำดิจิตอลต้นฉบับ

การตรวจสอบความถูกต้องของวีดีโอด้วยเทคนิคของลายเซ็นดิจิตอลจะมีวิธีการส่งลายเซ็นดิจิตอลออกไปพร้อมกับวีดีโอ 2 วิธี คือ

1. แนบเข้าไปในเฮดเดอร์ของวีดีโอ ซึ่งวิธีนี้จะมีข้อดีคือ วีดีโอไม่ถูกแก้ไข และไม่มีข้อจำกัดเรื่องขนาดของลายเซ็นดิจิตอลที่จะแนบเข้าไป แต่จะมีข้อเสียคือ ลายเซ็นดิจิตอลอาจถูกทำลายหรือสูญหายเมื่อมีการเปลี่ยนแปลงฟอร์แมตของวีดีโอหรือมีการแก้ไขวีดีโอ
2. ซ่อนเข้าไปในวีดีโอด้วยวิธีการของการซ่อนลายน้ำดิจิตอล ซึ่งแบ่งออกเป็น 2 วิธี คือ
   - **การซ่อนลายน้ำแบบเปราะบาง (Fragile watermarking)** การซ่อนลายเซ็นดิจิตอลด้วยวิธีนี้ สามารถซ่อนลายเซ็นดิจิตอลที่มีขนาดใหญ่กว่าการซ่อนลายน้ำแบบทนทาน แต่

ลายเซ็นดิจิตอลที่ซ่อนเข้าไปจะถูกทำลายหรือผิดเพี้ยนได้ง่ายเมื่อมีการประมวลผลภาพด้วยวิธีการต่างๆ ทั้งที่เจตนาและไม่เจตนา

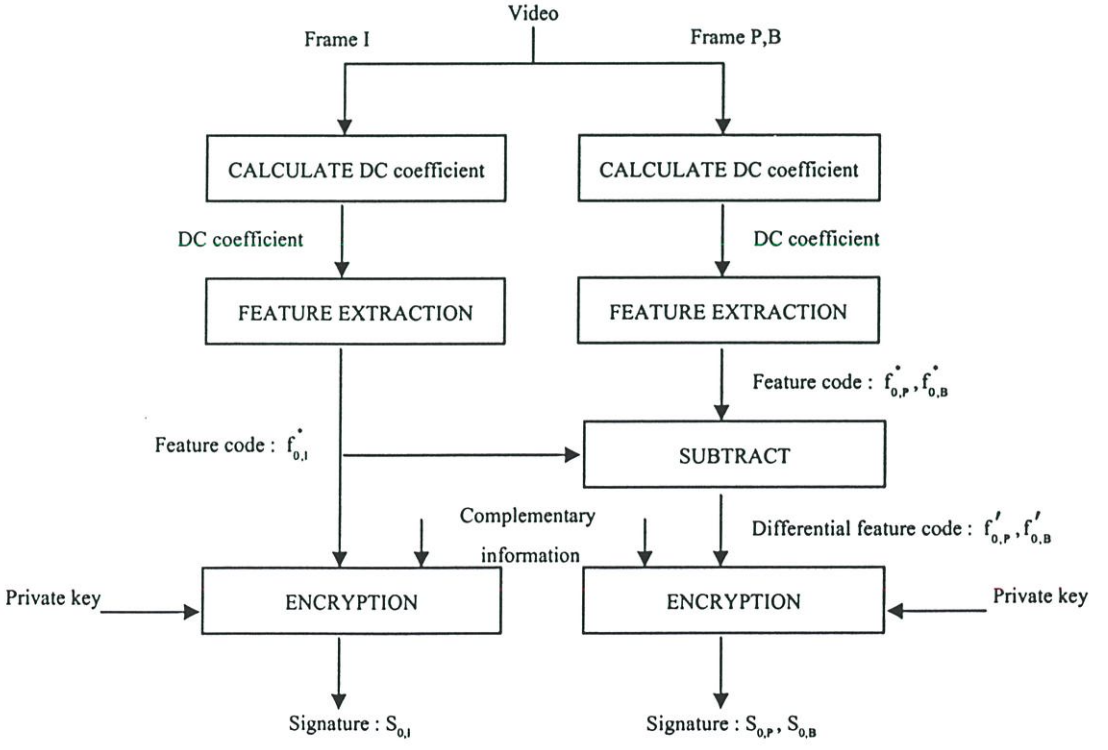
- **การซ่อนลายน้ำแบบทนทาน (Robust watermarking)** การซ่อนลายเซ็นดิจิตอลด้วยวิธีนี้จะทนต่อการประมวลผลภาพด้วยวิธีการต่างๆ ทั้งที่เจตนาและไม่เจตนา แต่จะมีข้อเสียคือ ขนาดของลายเซ็นดิจิตอลที่สามารถซ่อนเข้าไปจะมีขนาดเล็ก ซึ่งถ้าลายเซ็นดิจิตอลมีขนาดเล็กลงจะทำให้ความสามารถในการระบุพื้นที่ที่ถูกแก้ไขต่ำลง

ในงานวิจัยนี้จะเลือกใช้เทคนิคของลายเซ็นดิจิตอลในการตรวจสอบความถูกต้องของวีดีโอ และจะทำการแนบลายเซ็นดิจิตอลเข้าไปในเฮดเดอร์ของวีดีโอ เนื่องจากไม่มีข้อจำกัดในเรื่องความจุของการซ่อนข้อมูล โดยในการวิจัยจะทำการปรับปรุงเทคนิคของการใช้ลายเซ็นดิจิตอลในการตรวจสอบความถูกต้องของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ โดยใช้หลักการของ Incremental-based digital signature

บทที่ 4
ลายเซ็นดิจิตอลแบบสมทบส่วนต่าง

4.1 การสร้างลายเซ็นดิจิตอลแบบสมทบส่วนต่างสำหรับวีดีโอต้นฉบับ

การสร้างลายเซ็นดิจิตอลแบบสมทบส่วนต่างจะมีขั้นตอนคือ นำแต่ละเฟรมของวีดีโอมาแบ่งเป็นรูปภาพย่อยขนาด b×b ที่ไม่ซ้อนทับกัน (เช่น กำหนดให้ b มีค่าเท่ากับ 8, 16 หรือ 32...) แล้วนำแต่ละรูปภาพย่อยมาคำนวณหาค่า DC coefficient จากนั้นนำค่า DC coefficient ของแต่ละรูปภาพย่อยมาหาค่า feature code จากกระบวนการ FEATURE EXTRACTION ซึ่งถ้าเป็นเฟรม I ก็จะนำ feature code ที่ได้ไปรวมกับ complementary information (ในที่นี้ใช้ค่าของ วัน เดือน ปี ชม. นาที วินาที ลำดับที่ของเฟรม และอัตราการแสดงภาพ) แล้วเข้ารหัสด้วย private key จะได้ลายเซ็นดิจิตอลของเฟรม I แต่ถ้าเป็นเฟรม P,B จะต้องนำ feature code ที่ได้ไปหาค่า differential feature code จากกระบวนการ SUBTRACT แล้วจึงนำ differential feature code ที่ได้ไปรวมกับ complementary information แล้วเข้ารหัสด้วย private key จะได้ลายเซ็นดิจิตอลของเฟรม P,B ดังรูปที่ 4.1 จากนั้นนำลายเซ็นดิจิตอลที่ได้แนบเข้าไปในเฮดเดอร์ของแต่ละเฟรมของวีดีโอ ซึ่งรายละเอียดของกระบวนการต่างๆ อธิบายได้ดังต่อไปนี้



รูปที่ 4.1 กระบวนการสร้างลายเซ็นดิจิตอลแบบสมทบส่วนต่าง

4.1.1 กระบวนการ CALCULATE DC coefficient

คือ กระบวนการที่ใช้คำนวณหาค่า DC coefficient ของแต่ละรูปภาพย่อย โดยกำหนดให้

- รูปภาพหรือเฟรมของวีดีโอมีขนาด M×N พิกเซล
- n คือ ลำดับชั้นของสำเนาวีดีโอโดยที่ $n \in \{0,\ldots,w\}$ เมื่อ w คือ จำนวนเต็มบวกใดๆ
- c คือ ชนิดของเฟรมวีดีโอตามมาตรฐาน MPEG-1 โดยที่ $c \in \{I,P,B\}$

ขั้นตอนการคำนวณหาค่า DC coefficient อธิบายได้ดังต่อไปนี้

1. ปรับรูปแบบสีของรูปภาพหรือเฟรมของวีดีโอให้อยู่ในรูปแบบสีแบบ YCbCr ซึ่งในที่นี้จะใช้เฉพาะระดับความเข้มของแสงสว่าง (Y) แทนด้วย $g(x,y) \in 0,\ldots,255$ โดยที่ $x \in \{1,\ldots,M\}$, $y \in \{1,\ldots,N\}$
2. แบ่ง g(x,y) ออกเป็นรูปภาพย่อยขนาด b×b ที่ไม่ซ้อนทับกัน ให้แต่ละรูปภาพย่อยแทนด้วย $g_{ij}(x_1,y_1)$ เมื่อ $i \in \{1,\ldots,M_1\}$ (กำหนดให้ $M_1=\lfloor M/b \rfloor$) และ $j \in \{1,\ldots,N_1\}$ (กำหนดให้ $N_1=\lfloor N/b \rfloor$) $x_1 \in \{1,\ldots,b\}$, $y_1 \in \{1,\ldots,b\}$ โดยที่กำหนดให้ $g_{ij}(x_1, y_1) = g(((i-1)\cdot b)+ x_1,((j-1)\cdot b)+ y_1)$
3. คำนวณหาค่า DC coefficient ของแต่ละรูปภาพย่อย ($DC_{n,c,i,j}$) โดยจะแยกพิจารณาเป็น 2 กรณี คือ
   - ใน Pixel domain ให้ใช้ค่าเฉลี่ยของระดับความเข้มของแสงสว่างของแต่ละรูปภาพย่อย
   - ใน DCT domain ให้ใช้ค่า DC coefficient ของแต่ละรูปภาพย่อย

4.1.2 กระบวนการ FEATURE EXTRACTION

วิธีการคำนวณหาค่า feature code ที่ใช้ในงานวิจัยนี้จะใช้วิธีการของ Sangiamkun [11] เนื่องจากสามารถปรับเปลี่ยนความละเอียดในการตรวจสอบ และสามารถระบุพื้นที่ที่ถูกแก้ไขได้ (แต่อย่างไรก็ดีวิธีการที่เสนอสามารถประยุกต์ใช้กับวิธีการหา feature code แบบอื่นๆ ที่มีคุณสมบัติเทียบเคียงกับ [11] ได้)

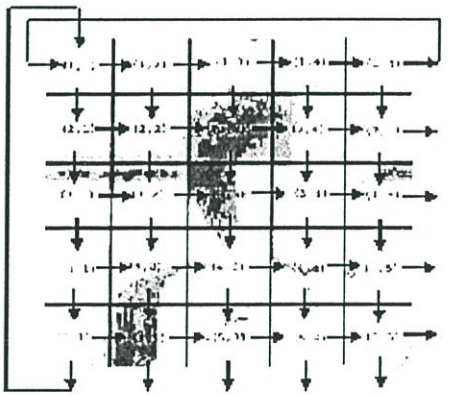
ขั้นตอนการทำ FEATURE EXTRACTION อธิบายได้ดังต่อไปนี้

1. คำนวณหาค่าลักษณะเฉพาะของแต่ละรูปภาพย่อย $g_{ij}(x_1,y_1)$ โดยใช้สมการที่ 4.1 และ 4.2

$$f^{(r)}_{n,c,i,j} = \frac{DC_{n,c,i,j} - DC_{n,c,i,j+1}}{DC_{n,c,i,j} + DC_{n,c,i,j+1}} \tag{4.1}$$

$$f^{(b)}_{n,c,i,j} = \frac{DC_{n,c,i,j} - DC_{n,c,i+1,j}}{DC_{n,c,i,j} + DC_{n,c,i+1,j}} \tag{4.2}$$

จากสมการที่ 4.1 และ 4.2 แต่ละรูปภาพย่อย $g_{i,j}(x_1,y_1)$ จะมีลักษณะเฉพาะ 2 ค่า ได้แก่ $f^{(r)}_{n,c,i,j}$ และ $f^{(b)}_{n,c,i,j}$ ที่ได้จากการเปรียบเทียบค่า DC coefficient ของรูปภาพย่อยตำแหน่งที่ i,j ใดๆ ($g_{i,j}(x_1,y_1)$) กับรูปภาพย่อยที่อยู่ติดกันทางด้านขวา ($g_{i,j+1}(x_1,y_1)$) และรูปภาพย่อยที่อยู่ติดกันทางด้านล่าง ($g_{i+1,j}(x_1,y_1)$) ตามลำดับ โดยความสัมพันธ์ระหว่างรูปภาพย่อยต่างๆ ที่ใช้ในการคำนวณหาค่าลักษณะเฉพาะสามารถแสดงได้ดังรูปที่ 4.2



รูปที่ 4.2 ความสัมพันธ์ระหว่างรูปภาพย่อยที่ใช้ในการคำนวณหาค่าลักษณะเฉพาะ

2. ผลลัพธ์ของลักษณะเฉพาะข้างต้นจะอยู่ในรูปของจำนวนจริง จากค่าที่ได้นำมาทำการ quantize โดยการแบ่งค่าลักษณะเฉพาะเป็น 4 ระดับ ตามสมการที่ 4.3 เพื่อให้สามารถแทนค่าที่ได้ ($f^{*(r)}_{n,c,i,j}, f^{*(b)}_{n,c,i,j}$) ด้วยเลขฐานสองขนาด 2 บิต ตามตารางที่ 4.1

$$f^{*(z)}_{n,c,i,j} = \begin{cases} 1 & f^{(z)}_{n,c,i,j} \geq \alpha_2 + \beta \\ 2 & \alpha_2 - \beta < f^{(z)}_{n,c,i,j} < \alpha_2 + \beta \\ 0 & \alpha_1 + \beta \leq f^{(z)}_{n,c,i,j} \leq \alpha_2 - \beta \\ 2 & \alpha_1 - \beta < f^{(z)}_{n,c,i,j} < \alpha_1 + \beta \\ -1 & f^{(z)}_{n,c,i,j} \leq \alpha_1 - \beta \end{cases} \quad (4.3)$$

โดยที่

$f^{(z)}_{n,c,i,j}$ คือ ลักษณะเฉพาะที่มีค่าเป็นจำนวนจริงของรูปภาพย่อยของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n ของ เฟรม c ในตำแหน่งที่ i,j ที่ได้จากการเปรียบเทียบกับรูปภาพย่อยที่อยู่ติดกันทางด้านขวาหรือด้านล่าง ($f^{(r)}_{n,c,i,j}$ หรือ $f^{(b)}_{n,c,i,j}$), $z \in \{r,b\}$

$f^{*(z)}_{n,c,i,j}$ คือ ลักษณะเฉพาะที่มีค่าเป็นจำนวนเต็มของรูปภาพย่อยของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n ของ เฟรม c ในตำแหน่งที่ i,j ที่ได้จากการเปรียบเทียบกับรูปภาพย่อยที่อยู่ติดกันทางด้านขวาหรือด้านล่าง ($f^{*(r)}_{n,c,i,j}$ หรือ $f^{*(b)}_{n,c,i,j}$) , $z \in \{ r,b\}$

α_1, α_2 คือ Threshold (ในการกำหนดค่า Threshold นั้น จะเลือกค่าที่ทำให้จำนวนของ feature code ที่มีค่าเท่ากับ 0,1 และ –1 มีค่าเท่าๆกัน)

β คือ ค่าที่ใช้ในการกำหนดพื้นที่ที่ไม่สามารถตรวจสอบได้ เพื่อให้การตรวจสอบความถูกต้องของรูปภาพสามารถรองรับสัญญาณรบกวนต่างๆ ของรูปภาพได้ (unknown band, $f^{*(z)}_{n,c,i,j} = 2$ ซึ่งถ้ากำหนดให้ β มีค่าสูงขึ้น ความน่าจะเป็นในการตรวจไม่พบว่ารูปภาพมีการแก้ไขทั้งที่รูปภาพมีการแก้ไข (missed detection) จะสูงขึ้น แต่ถ้ากำหนดค่า β ต่ำลงความน่าจะเป็นในการตรวจพบว่ารูปภาพมีการแก้ไขทั้งที่ภาพไม่มีการแก้ไข (false alarm) จะสูงขึ้น)

ตารางที่ 4.1 การแทนค่า feature code ด้วยเลขฐานสองขนาด 2 บิต

$f^{*(z)}_{n,c,i,j}$	Binary Code
0	00
1	01
2	10
-1	11

ผลลัพธ์ที่ได้จากกระบวนการนี้ คือ feature code ซึ่งแต่ละรูปภาพย่อยจะมี feature code ขนาด 2 บิต 2 ชุด ที่ได้จากความสัมพันธ์ทั้ง 2 ด้าน รวมมีขนาด 4 บิตต่อ 1 รูปภาพย่อย ดังนั้นแต่ละเฟรมของวีดีโอจะมี feature code ขนาด $4 \cdot M_1 \cdot N_1$ บิต ซึ่งแทนด้วย $f^{*}_{n,c}(k)$, $k \in 1,\ldots, 4 \cdot M_1 \cdot N_1$ โดยที่บิตที่ k, k+1, k+2, k+3 แทนค่าของ $t(i_1)$ เมื่อ $k = (i_1 - 1) \cdot 4 + 1$ และ $t(i_1) = f^{*(r)}_{n,c,i,j} \oplus f^{*(b)}_{n,c,i,j}$

$i_1 = ((i-1) \cdot N_1) + j$, โดยที่ $\oplus$ คือ concatenation operator เช่น $f^{*(r)}_{n,c,i,j} \oplus f^{*(b)}_{n,c,i,j}$ หมายถึงการนำค่า $f^{*(b)}_{n,c,i,j}$ ไปเรียงต่อกับ $f^{*(r)}_{n,c,i,j}$

4.1.3 กระบวนการ SUBTRACT

คือ กระบวนการที่ใช้คำนวณหาค่า differential feature code ซึ่งจะแทนด้วย $f'_{n,c}(k_1), k_1 \in 1,\ldots,s$ (กำหนดให้ s คือ ขนาดของ differential feature code ของเฟรมใดๆ) โดยจะแยกพิจารณาเป็น 2 กรณี คือ

1. n = 0 (วีดีโอต้นฉบับ)

การคำนวณหาค่า differential feature code ของรูปภาพย่อยตำแหน่งที่ i,j ใดๆ ($f'^{(z)}_{n,c,i,j}$) กระทำโดยการเปรียบเทียบค่า feature code ที่อยู่ในรูปของเลขฐานสอง ของรูปภาพย่อยตำแหน่งที่ i,j ใดๆ ของเฟรมที่ต้องการหาค่า differential feature code (เฟรม P หรือ เฟรม B) กับ feature code ของรูปภาพย่อยตำแหน่งที่ i,j ใดๆ ของเฟรม I (อยู่ในกลุ่มของรูปภาพกลุ่มเดียวกับเฟรมที่ต้องการหาค่า differential feature code) ตามตารางที่ 4.2

ตารางที่ 4.2 การคำนวณหาค่า differential feature code ของวีดีโอต้นฉบับสำหรับเฟรม P และ B

เงื่อนไข	$f'^{(z)}_{n,c,i,j}$
$f^{*(z)}_{n,c,i,j} = f^{*(z)}_{n,I,i,j}$	0
$f^{*(z)}_{n,c,i,j} \neq f^{*(z)}_{n,I,i,j}$	$1 \oplus f^{*(z)}_{n,c,i,j}$

หมายเหตุ : $c \in \{P,B\}$

2. $n \neq 0$ (สำเนาวีดีโอลำดับที่ n)

การคำนวณหาค่า differential feature code ของรูปภาพย่อยตำแหน่งที่ i,j ใดๆ ($f'^{(z)}_{n,c,i,j}$) กระทำโดยการเปรียบเทียบค่า feature code ที่อยู่ในรูปของเลขฐานสอง ของรูปภาพย่อยตำแหน่งที่ i,j ใดๆ ของเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n กับ feature code ของรูปภาพย่อยตำแหน่งที่ i,j ใดๆ ของเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n - 1 ตามตารางที่ 4.3

ตารางที่ 4.3 การคำนวณหาค่า differential feature code ของสำเนาวีดีโอลำดับที่ $n \neq 0$

เงื่อนไข	$f'^{(z)}_{n,c,i,j}$
$f^{*(z)}_{n,c,i,j} = f^{*(z)}_{n-1,c,i,j}$	0
$f^{*(z)}_{n,c,i,j} \neq f^{*(z)}_{n-1,c,i,j}$	$1 \oplus f^{*(z)}_{n,c,i,j}$

หมายเหตุ : $c \in \{I,P,B\}$

4.1.4 กระบวนการ ENCRYPTION

คือ กระบวนการที่นำข้อมูล feature code หรือ differential feature code ของแต่ละเฟรมของสำเนาวีดีโอลำดับที่ n ($d_{n,c}$) มาเข้ารหัสด้วย private key ของผู้ที่มีกรรมสิทธิ์ในการทำสำเนาวีดีโอลำดับที่ n ตามสมการที่ 4.4 จะได้ลายเซ็นดิจิตอล ซึ่งแทนด้วย $S_{n,c}$

$$S_{n,c} = E_{n^{th}\,\text{private key}}(d_{n,c}) \tag{4.4}$$

การหาค่า $d_{n,c}$ จะมี 2 กรณีคือ

1. $n = 0$ (วีดีโอต้นฉบับ)

ค่า $d_{n,c}$ สามารถหาได้ตามสมการที่ 4.5

$$\begin{aligned} d_{n,c} &= f^{*}_{n,c} \quad \text{if} \quad c \in \{I\} \\ d_{n,c} &= f'_{n,c} \quad \text{if} \quad c \in \{P,B\} \end{aligned} \tag{4.5}$$

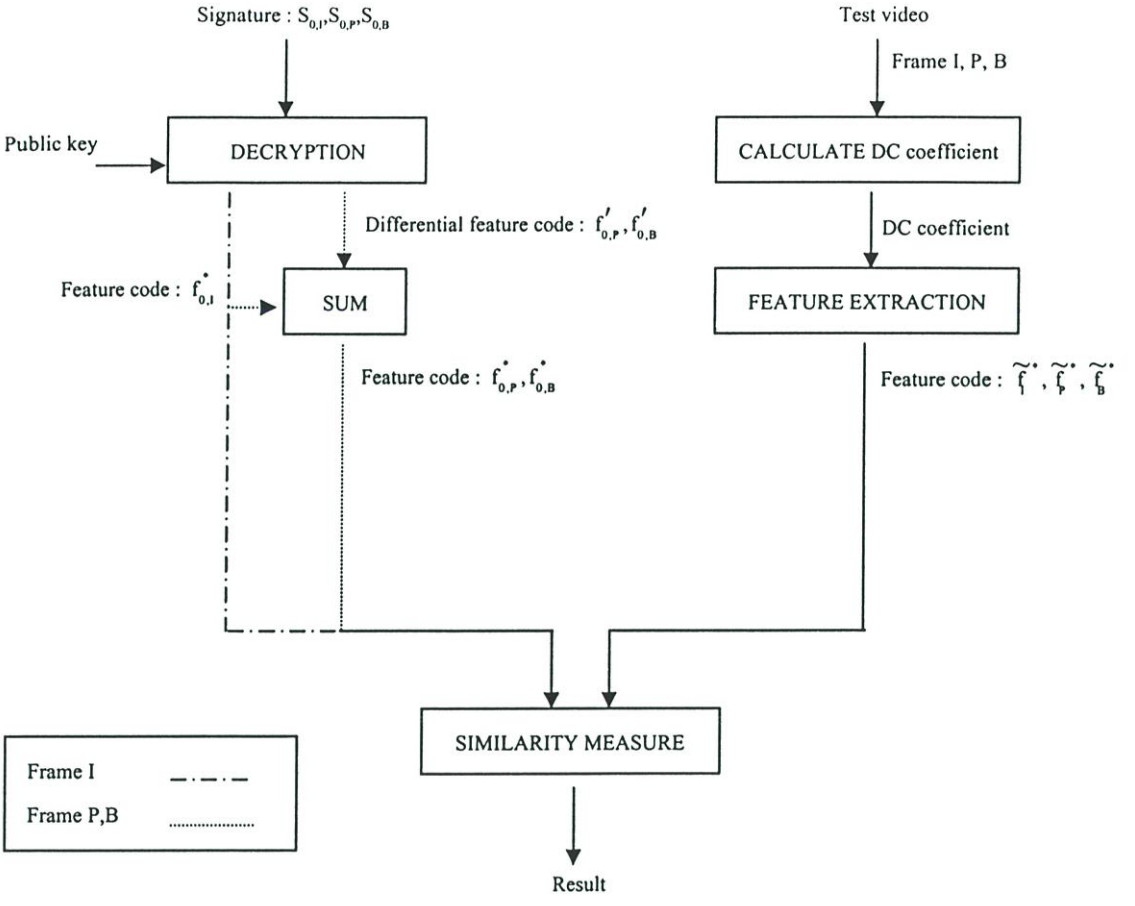
2. $n \neq 0$ (สำเนาวีดีโอลำดับที่ n)

ค่า $d_{n,c}$ สามารถหาได้จากการนำ differential feature code ของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n ($f'_{n,c}$) มาเรียงต่อกับลายเซ็นดิจิตอลของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1 ($S_{n-1,c}$) ตามสมการที่ 4.6

$$d_{n,c} = S_{n-1,c} \oplus f'_{n,c} \tag{4.6}$$

4.2 การตรวจสอบความถูกต้องของวีดีโอต้นฉบับ

วิธีการตรวจสอบความถูกต้องของวีดีโอมีขั้นตอนคือ นำลายเซ็นดิจิตอลที่ได้จากเฮดเดอร์ของแต่ละเฟรมของวีดีโอมาถอดรหัสด้วย public key จะได้ feature code สำหรับเฟรม I แต่ถ้าเป็นเฟรม P,B จะได้ differential feature code ซึ่งต้องนำไปหาค่า feature code จากกระบวนการ SUM แล้วจึงนำ feature code ที่ได้ไปเปรียบเทียบกับ feature code ของเฟรมวีดีโอที่นำมาตรวจสอบ (ขั้นตอนการคำนวณหาค่า feature code จะใช้วิธีเดียวกับการคำนวณหาค่า feature code เพื่อสร้างลายเซ็นดิจิตอลดังที่ได้กล่าวไว้ในหัวข้อที่ 4.1.2) กระบวนการทั้งหมดแสดงได้ดังรูปที่ 4.3 โดยมีรายละเอียดดังต่อไปนี้



รูปที่ 4.3 กระบวนการตรวจสอบความถูกต้องของวีดีโอ

4.2.1 กระบวนการ DECRYPTION

คือ กระบวนการที่ใช้ในการถอดรหัสลายเซ็นดิจิตอล ($S_{n,c}$) ของแต่ละเฟรมของวีดีโอด้วย public key ของผู้ที่มีกรรมสิทธิ์ในการทำสำเนาวีดีโอลำดับที่ n ดังสมการที่ 4.7

$$d_{n,c} = D_{n^{th}\text{public key}}(S_{n,c}) \tag{4.7}$$

4.2.2 กระบวนการ SUM

คือ กระบวนการที่กระทำกลับกันกับกระบวนการ SUBTRACT ในหัวข้อที่ 4.1.3 กล่าวคือ จะเป็นการแปลงค่า differential feature code (ของเฟรม P,B หรือ เฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n) ให้เป็น feature code โดยมีขั้นตอนดังอัลกอริทึมในรูปที่ 4.4

```
for i = 1 to M1
    for j = 1 to N1
        if  n = 0
            if f'n,c(k1) = 0 ( c ∈ {P,B})
                f*(r)n,c,i,j = f*(r)n,I,i,j
                k1= k1+1
            else
                f*(r)n,c,i,j = f'n,c(k1 +1)⊕f'n,c(k1 +2)
                k1= k1+3
            end
            if f'n,c(k1) = 0 ( c ∈ {P,B})
                f*(b)n,c,i,j = f*(b)n,I,i,j
                k1= k1+1
            else
                f*(b)n,c,i,j = f'n,c(k1 +1)⊕f'n,c(k1 +2)
                k1 = k1+3
            end
        else
            if  f'n,c(k1) = 0 ( c ∈ {I,P,B})
                f*(r)n,c,i,j = f*(r)n-1,c,i,j
                k1 = k1+1
            else
                f*(r)n,c,i,j = f'n,c(k1 +1)⊕f'n,c(k1 +2)
                k1 = k1+3
            end
            if f'n,c(k1) = 0 ( c ∈ {I,P,B})
                f*(b)n,c,i,j = f*(b)n-1,c,i,j
                k1 = k1+1
            else
                f*(b)n,c,i,j = f'n,c(k1 +1)⊕f'n,c(k1 +2)
                k1 = k1+3
            end
        end
    end
end
```

รูปที่ 4.4 Pseudo code แสดงอัลกอริทึมการแปลงค่า differential feature code ให้เป็น feature code

4.2.3 กระบวนการ SIMILARITY MEASURE

คือ กระบวนการที่ใช้ในการตรวจสอบความถูกต้องของแต่ละรูปภาพย่อย (i,j ใดๆ) ซึ่งจะมีขั้นตอนคือ เปรียบเทียบค่าของ feature code ระหว่าง feature code ที่ได้จากการถอดรหัสลายเซ็นดิจิตอล และ feature code ที่ได้จากเฟรมของวีดีโอที่นำมาตรวจสอบตามสมการที่ 4.8, 4.9

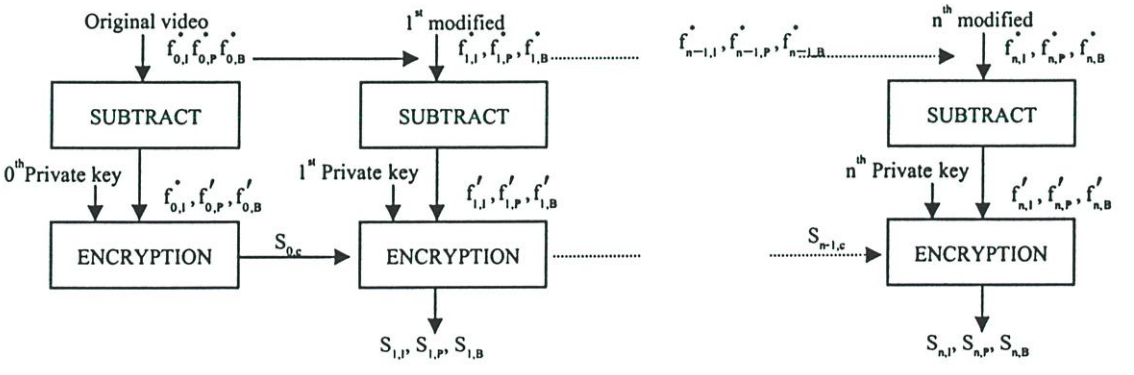
$$A_{i,j} = 1 \quad \text{if} \quad L^{(r)}_{i,j} + L^{(b)}_{i,j} + L^{(l)}_{i,j} + L^{(t)}_{i,j} \geq 3$$
$$A_{i,j} = 0 \quad \text{if} \quad L^{(r)}_{i,j} + L^{(b)}_{i,j} + L^{(l)}_{i,j} + L^{(t)}_{i,j} < 3 \tag{4.8}$$

$$L^{(r)}_{i,j} = 1 \quad \text{if} \quad f^{*(r)}_{n,c,i,j} \neq \tilde{f}^{*(r)}_{i,j} \neq 2$$
$$L^{(b)}_{i,j} = 1 \quad \text{if} \quad f^{*(b)}_{n,c,i,j} \neq \tilde{f}^{*(b)}_{i,j} \neq 2$$
$$L^{(l)}_{i,j} = 1 \quad \text{if} \quad f^{*(r)}_{n,c,i,j-1} \neq \tilde{f}^{*(r)}_{i,j-1} \neq 2 \tag{4.9}$$
$$L^{(t)}_{i,j} = 1 \quad \text{if} \quad f^{*(b)}_{n,c,i-1,j} \neq \tilde{f}^{*(b)}_{i-1,j} \neq 2$$

จากสมการข้างต้นแสดงให้เห็นว่า ถ้ารูปภาพย่อยใดมีความแตกต่างในแง่ของ feature code เมื่อเปรียบเทียบกับรูปภาพย่อยข้างเคียงตั้งแต่ 3 ด้านขึ้นไป ($A_{i,j} = 1$) ถือว่ารูปภาพย่อยนั้นมีการแก้ไขเกิดขึ้น โดยในที่นี้ใช้การแสดงผลด้วยการล้อมรอบด้วยเส้นตรงทั้ง 4 ด้าน

4.3 การสร้างลายเซ็นดิจิตอลแบบสมทบส่วนต่างสำหรับวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ $n \neq 0$

การสร้างลายเซ็นดิจิตอลแบบสมทบส่วนต่างสำหรับวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ $n \neq 0$ สามารถแสดงได้ดังรูปที่ 4.5 โดยจะมีขั้นตอน คือ



รูปที่ 4.5 การสร้างลายเซ็นดิจิตอลแบบสมทบส่วนต่างสำหรับวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ $n \neq 0$

1. คำนวณหาค่า feature code ของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n โดยกำหนดให้ขนาดของรูปภาพย่อยเท่ากับขนาดของรูปภาพย่อยที่ใช้กับวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1
2. นำลายเซ็นดิจิตอลที่ได้จากเฮดเดอร์ของแต่ละเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1 มาถอดรหัสด้วย public key ที่เป็นคู่กับ private key ที่ใช้เข้ารหัสตามอัลกอริทึมต่อไปนี้

```
for a = n-1 to 0
        d_{a,c} = D_{a'spublic key}(S_{a,c})
end
```

ผลลัพธ์ที่ได้จะมี 2 กรณีคือ

- c = 'I'

ผลลัพธ์ที่ได้คือ feature code ของวีดีโอต้นฉบับและ differential feature code ของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1,2,3,….,n-1 $(f^{*}_{0,c}, f'_{1,c}, ..., f'_{n-1,c})$

- c = 'P' หรือ c = 'B'

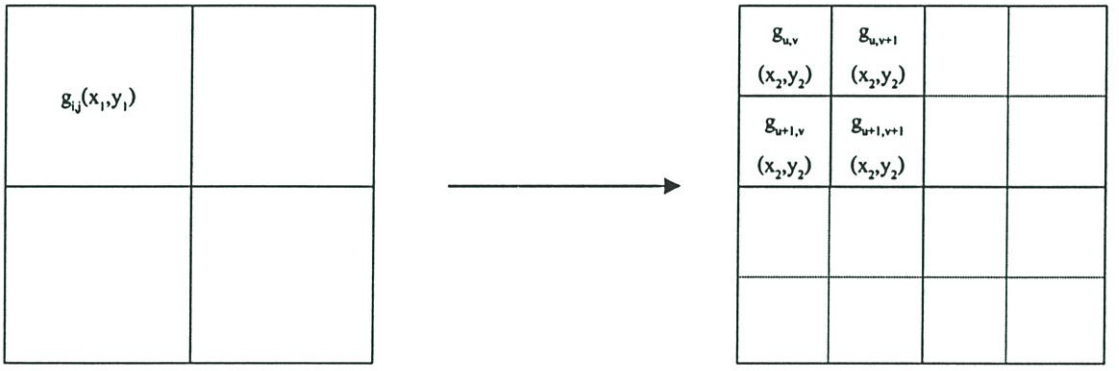
ผลลัพธ์ที่ได้คือ differential feature code ของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 0,1,2,….,n-1 $(f'_{0,c}, f'_{1,c}, ..., f'_{n-1,c})$

3. นำผลลัพธ์ที่ได้จากขั้นตอนที่ 2 มาคำนวณหาค่า feature code ของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1 ตามกระบวนการ SUM ในหัวข้อที่ 4.2.2
4. นำผลลัพธ์ที่ได้ $(f^{*}_{n,c}, f^{*}_{n-1,c})$ มาคำนวณหาค่า differential feature code ของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n ตามกระบวนการ SUBTRACT ในหัวข้อที่ 4.1.3
5. เข้ารหัสลายเซ็นดิจิตอลของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n -1 และ differential feature code ของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n ด้วย private key ของผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n ตามสมการที่ 4.4

4.3.1 การลดขนาดของรูปภาพย่อยที่ใช้กับวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ $n \neq 0$

การลดขนาดของรูปภาพย่อยจะเป็นการเพิ่มความละเอียดในการตรวจสอบ แต่ในขณะเดียวกัน feature code ที่ได้จะมีขนาดใหญ่ขึ้น จะใช้ในกรณีที่วีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาต้องการความละเอียดในการตรวจสอบสูงขึ้น ซึ่งจะมีขั้นตอนคือ

1. คำนวณหาค่า feature code ของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n โดยกำหนดขนาดของรูปภาพย่อยให้เล็กลงเป็น 1/h เท่าของรูปภาพย่อยที่ใช้ในการสร้างลายเซ็นดิจิตอลสำหรับวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1 โดยในที่นี้จะยกตัวอย่างกรณีที่ h = 4 ดังรูปที่ 4.6 ซึ่งจะแทนด้วย $\bar{f}^{*}_{n,c}(k_2), k_2 \in 1,...,4 \cdot M_2 \cdot N_2$ โดยกำหนดให้รูปภาพย่อยมีขนาด (b/2)×(b/2) ซึ่งแต่ละรูปภาพย่อยจะแทนด้วย $g_{u,v}(x_2,y_2)$ เมื่อ $u \in \{1,...,M_2\}$ (กำหนดให้ $M_2=\lfloor M/(b/2) \rfloor$) และ $v \in \{1,...,N_2\}$ (กำหนดให้ $N_2=\lfloor N/(b/2) \rfloor$)



รูปที่ 4.6 เปรียบเทียบขนาดของรูปภาพย่อยที่ใช้คำนวณค่า feature code สำหรับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1 กับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n เมื่อมีการลดขนาดของรูปภาพย่อย

2. นำลายเซ็นดิจิตอลที่ได้จากเฮดเดอร์ของแต่ละเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1 มาถอดรหัสด้วย public key ที่เป็นคู่กับ private key ที่ใช้เข้ารหัสตามอัลกอริทึมต่อไปนี้

```
for a = n-1 to 0
        d_{a,c} = D_{a'th public key}(S_{a,c})
end
```

ผลลัพธ์ที่ได้จะมี 2 กรณีคือ

- c = 'I'

ผลลัพธ์ที่ได้คือ feature code ของวีดีโอต้นฉบับและ differential feature code ของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1,2,3,….,n-1 $(f^{*}_{0,c}, f'_{1,c},..., f'_{n-1,c})$

- c = 'P' หรือ c = 'B'

ผลลัพธ์ที่ได้คือ differential feature code ของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 0,1,2,….,n-1 $(f'_{0,c}, f'_{1,c},..., f'_{n-1,c})$

3. นำผลลัพธ์ที่ได้จากขั้นตอนที่ 2 มาคำนวณหาค่า feature code ของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1 ตามกระบวนการ SUM ในหัวข้อที่ 4.2.2
4. นำ feature code ของเฟรมวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1 มาคำนวณหาค่า feature code ของเฟรมวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1 โดยกำหนดให้รูปภาพย่อยมีขนาดเท่ากับขนาดของรูปภาพย่อยที่ใช้กับเฟรมวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n ตามสมการที่ 4.10, 4.11 และ 4.12 ตามลำดับ แล้วแทนค่าที่ได้ ($\bar{f}^{*(z)}_{n-1,c,u,v}$) ด้วยเลขฐานสองขนาด 2 บิต ตามตารางที่ 4.1

$$f^{(z)}_{n-1,c,i,j} = \begin{cases} \alpha_2 + \beta & , f^{*(z)}_{n-1,c,i,j} = 1 \\ ((\alpha_1 + \beta) + (\alpha_2 - \beta))/2 & , f^{*(z)}_{n-1,c,i,j} = 0 \\ \alpha_1 - \beta & , f^{*(z)}_{n-1,c,i,j} = -1 \\ 0 & , f^{*(z)}_{n-1,c,i,j} = 2 \end{cases} \tag{4.10}$$

$$\bar{f}^{(z)}_{n-1,c,u,v} = f^{(z)}_{n-1,c,i,j} \quad , i = \lceil u/2 \rceil, j = \lceil v/2 \rceil \tag{4.11}$$

$$\bar{f}^{*(z)}_{n-1,c,u,v} = \begin{cases} 1 & \bar{f}^{(z)}_{n-1,c,u,v} \geq \alpha_2 + \beta \\ 2 & \alpha_2 - \beta < \bar{f}^{(z)}_{n-1,c,u,v} < \alpha_2 + \beta \\ 0 & \alpha_1 + \beta \leq \bar{f}^{(z)}_{n-1,c,u,v} \leq \alpha_2 - \beta \\ 2 & \alpha_1 - \beta < \bar{f}^{(z)}_{n-1,c,u,v} < \alpha_1 + \beta \\ -1 & \bar{f}^{(z)}_{n-1,c,u,v} \leq \alpha_1 - \beta \end{cases} \tag{4.12}$$

โดยที่

$\bar{f}^{(z)}_{n-1,c,u,v}$ คือ feature code ที่มีค่าเป็นจำนวนจริงของรูปภาพย่อยของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1 โดยกำหนดให้รูปภาพย่อยมีขนาดเล็กลงเท่ากับขนาดของรูปภาพย่อยที่ใช้กับวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n ของเฟรม c ในตำแหน่งที่ u,v ($\bar{f}^{(r)}_{n-1,c,u,v}$, $\bar{f}^{(b)}_{n-1,c,u,v}$) , $z \in \{ r,b \}$

$\vec{f}^{*(z)}_{n-1,c,u,v}$ คือ feature code ที่มีค่าเป็นจำนวนเต็มของรูปภาพย่อยของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1 โดยกำหนดให้รูปภาพย่อยมีขนาดเล็กลงเท่ากับขนาดของรูปภาพย่อยที่ใช้กับวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n ของเฟรม c ในตำแหน่งที่ u,v ($\vec{f}^{*(r)}_{n-1,c,u,v}$, $\vec{f}^{*(b)}_{n-1,c,u,v}$) , $z \in \{ r,b\}$

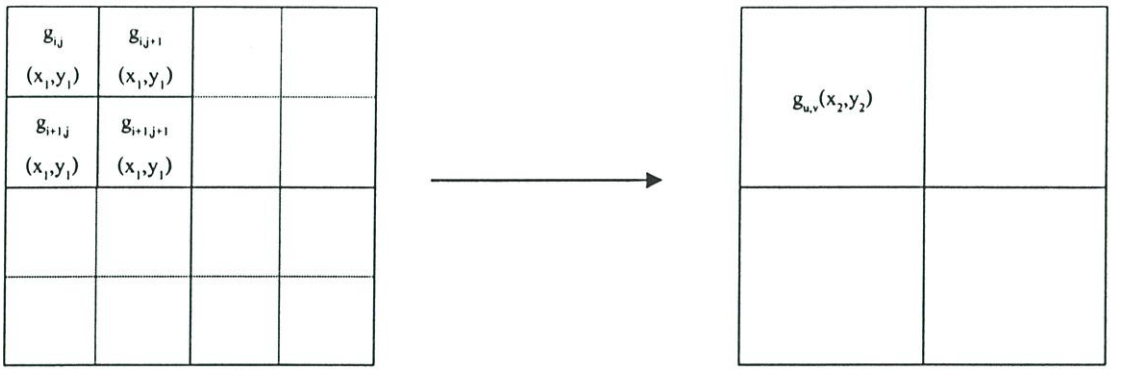
5. นำผลลัพธ์ที่ได้ ($\vec{f}^{*}_{n,c}$, $\vec{f}^{*}_{n-1,c}$) มาคำนวณหาค่า differential feature code ของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n ซึ่งจะแทนด้วย $\vec{f}'_{n,c}(k_3), k_3 \in 1,...,s_1$ (กำหนดให้ s_1 คือ ขนาดของ differential feature code ที่มีการลดขนาดของรูปภาพย่อย) ตามกระบวนการ SUBTRACT ในหัวข้อที่ 4.1.3
6. เข้ารหัสลายเซ็นดิจิตอลของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1 และ differential feature code ของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n ด้วย private key ของผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n ตามสมการที่ 4.13

$$S_{n,c} = E_{n^{th}\text{ private key}}(S_{n-1,c} \oplus \vec{f}'_{n,c}) \qquad (4.13)$$

4.3.2 การเพิ่มขนาดของรูปภาพย่อยที่ใช้กับวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ $n \neq 0$

การเพิ่มขนาดของรูปภาพย่อยจะเป็นการลดความละเอียดในการตรวจสอบ แต่ในขณะเดียวกัน feature code ที่ได้จะมีขนาดเล็กลง จะใช้ในกรณีที่วีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาต้องการความละเอียดในการตรวจสอบไม่มากนัก ซึ่งจะมีวิธีคือ

1. คำนวณหาค่า feature code ของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n โดยกำหนดขนาดของรูปภาพย่อยให้ใหญ่ขึ้นเป็น h เท่าของรูปภาพย่อยที่ใช้ในการสร้างลายเซ็นดิจิตอลสำหรับวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1 โดยในที่นี้จะยกตัวอย่างกรณีที่ h = 4 ดังรูปที่ 4.7 ซึ่งจะแทนด้วย $\vec{f}^{*}_{n,c}(k_2), k_2 \in 1,...,4 \cdot M_2 \cdot N_2$ โดยกำหนดให้รูปภาพย่อยมีขนาด $(b\cdot 2)\times(b\cdot 2)$ ซึ่งแต่ละรูปภาพย่อยจะแทนด้วย $g_{u,v}(x_2,y_2)$ เมื่อ $u \in \{1,...,M_2\}$ (กำหนดให้ $M_2=\lfloor M/(b\cdot 2)\rfloor$) และ $v \in \{1,...,N_2\}$ (กำหนดให้ $N_2=\lfloor N/(b\cdot 2)\rfloor$)



รูปที่ 4.7 เปรียบเทียบขนาดของรูปภาพย่อยที่ใช้คำนวณค่า feature code สำหรับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1 กับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n เมื่อมีการเพิ่มขนาดของรูปภาพย่อย

2. นำลายเซ็นดิจิตอลที่ได้จากเฮดเดอร์ของแต่ละเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1 มาถอดรหัสด้วย public key ที่เป็นคู่กับ private key ที่ใช้เข้ารหัสตามอัลกอริทึมต่อไปนี้

```
for a = n-1 to 0
        d_{a,c} = D_{a's public key}(S_{a,c})
end
```

ผลลัพธ์ที่ได้จะมี 2 กรณีคือ

- c = 'I'

ผลลัพธ์ที่ได้คือ feature code ของวีดีโอต้นฉบับและ differential feature code ของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1,2,3,….,n-1 ($f^{*}_{0,c}, f'_{1,c}, \ldots, f'_{n-1,c}$)

- c = 'P' หรือ c = 'B'

ผลลัพธ์ที่ได้คือ differential feature code ของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 0,1,2,….,n-1 ($f'_{0,c}, f'_{1,c}, \ldots, f'_{n-1,c}$)

3. นำผลลัพธ์ที่ได้จากขั้นตอนที่ 2 มาคำนวณหาค่า feature code ของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1 ตามกระบวนการ SUM ในหัวข้อที่ 4.2.2
4. นำ feature code ของเฟรมวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1 มาคำนวณหาค่า feature code ของเฟรมวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1 โดยกำหนดให้รูปภาพย่อยมีขนาดเท่ากับขนาดของรูปภาพย่อยที่ใช้กับเฟรมวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n ตามสมการที่

4.10, 4.14 และ 4.15 ตามลำดับ แล้วแทนค่าที่ได้ $\vec{f}^{*(z)}_{n-1,c,u,v}$ ด้วยเลขฐานสองขนาด 2 บิต ตามตารางที่ 4.1

$$\vec{f}^{(z)}_{n-1,c,u,v} = f^{(z)}_{n-1,c,i,j} + f^{(z)}_{n-1,c,i,j+1} + f^{(z)}_{n-1,c,i+1,j} + f^{(z)}_{n-1,c,i+1,j+1} \quad (4.14)$$
$$, i = ((u-1)\cdot 2)+1, j = ((v-1)\cdot 2)+1$$

$$\vec{f}^{*(z)}_{n-1,c,u,v} = \begin{cases} 1 & \vec{f}^{(z)}_{n-1,c,u,v} \geq \alpha_2 + \beta \\ 2 & \alpha_2 - \beta < \vec{f}^{(z)}_{n-1,c,u,v} < \alpha_2 + \beta \\ 0 & \alpha_1 + \beta \leq \vec{f}^{(z)}_{n-1,c,u,v} \leq \alpha_2 - \beta \\ 2 & \alpha_1 - \beta < \vec{f}^{(z)}_{n-1,c,u,v} \alpha_1 + \beta \\ -1 & \vec{f}^{(z)}_{n-1,c,u,v} \leq \alpha_1 - \beta \end{cases} \quad (4.15)$$

โดยที่

$\vec{f}^{(z)}_{n-1,c,u,v}$ คือ feature code ที่มีค่าเป็นจำนวนจริงของรูปภาพย่อยของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1 โดยกำหนดให้รูปภาพย่อยมีขนาดใหญ่ขึ้นเท่ากับขนาดของรูปภาพย่อยที่ใช้กับวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n ของเฟรม c ในตำแหน่งที่ u,v ($\vec{f}^{(r)}_{n-1,c,u,v}, \vec{f}^{(b)}_{n-1,c,u,v}$) , $z \in$ { r,b}

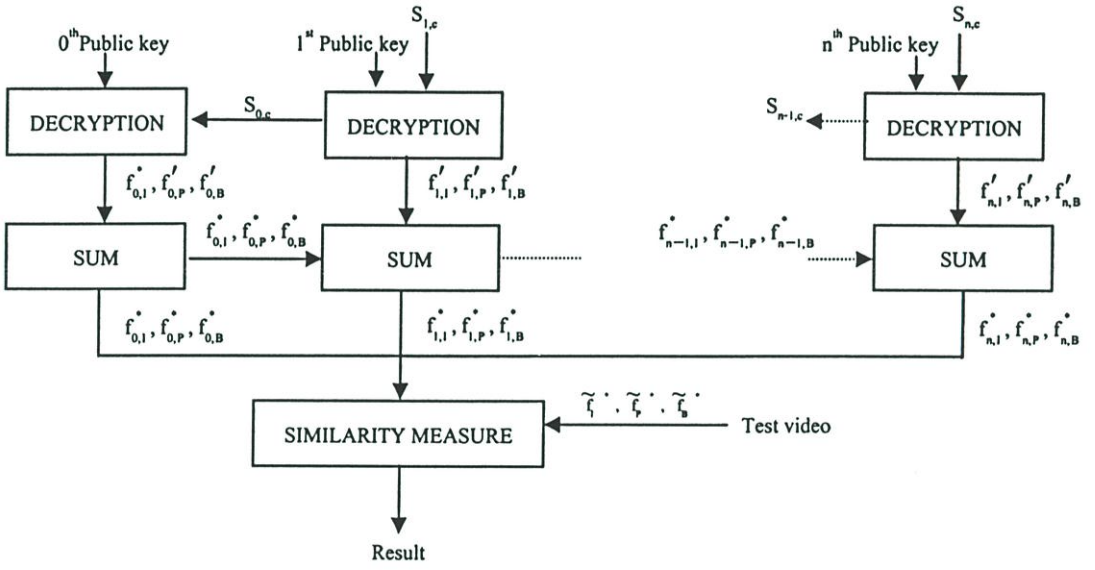
$\vec{f}^{*(z)}_{n-1,c,u,v}$ คือ feature code ที่มีค่าเป็นจำนวนเต็มของรูปภาพย่อยของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1 โดยกำหนดให้รูปภาพย่อยมีขนาดใหญ่ขึ้นเท่ากับขนาดของรูปภาพย่อยที่ใช้กับวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n ของเฟรม c ในตำแหน่งที่ u,v ($\vec{f}^{*(r)}_{n-1,c,u,v}, \vec{f}^{*(b)}_{n-1,c,u,v}$) , $z \in$ { r,b}

5. นำผลลัพธ์ที่ได้ ($\vec{f}^{*}_{n,c}, \vec{f}^{*}_{n-1,c}$) มาคำนวณหาค่า differential feature code ของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n ซึ่งจะแทนด้วย $\vec{f}'_{n,c}(k_3), k_3 \in 1,...,s_1$ (กำหนดให้ s_1 คือ ขนาดของ differential feature code เมื่อมีการเพิ่มขนาดของรูปภาพย่อย) ตามกระบวนการ SUBTRACT ในหัวข้อที่ 4.1.3
6. เข้ารหัสลายเซ็นดิจิตอลของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n-1 และ differential feature code ของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n ด้วย private key ของผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n ตามสมการที่ 4.16

$$S_{n,c} = E_{n^{th}\text{ private key}}(S_{n-1,c} \oplus \vec{f}'_{n,c}) \quad (4.16)$$

4.4 การตรวจสอบความถูกต้องของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n ≠ 0

การตรวจสอบความถูกต้องของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n ≠ 0 สามารถแสดงได้ดังรูปที่ 4.8 โดยจะมีขั้นตอน คือ



รูปที่ 4.8 การตรวจสอบความถูกต้องของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ n ≠ 0

1. ถอดรหัสลายเซ็นดิจิตอลที่ได้จากเฮดเดอร์ของแต่ละเฟรมของวีดีโอที่นำมาตรวจสอบด้วย public key ที่เป็นคู่กับ private key ที่ใช้เข้ารหัสตามอัลกอริทึมต่อไปนี้

```
for a = n to 0
        d_{a,c} = D_{a^th public key}(S_{a,c})
end
```

ผลลัพธ์ที่ได้จะมี 2 กรณีคือ

- c = 'I'

ผลลัพธ์ที่ได้คือ feature code ของวีดีโอต้นฉบับและ differential feature code ของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1,2,3,….,n ($f^*_{0,c}, f'_{1,c}, ..., f'_{n,c}$)

- c = 'P' หรือ c = 'B'

ผลลัพธ์ที่ได้คือ differential feature code ของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 0,1,2,….,n ($f'_{0,c}, f'_{1,c}, ..., f'_{n,c}$)

2. นำผลลัพธ์ที่ได้จากขั้นตอนที่ 1 มาคำนวณหาค่า feature code ของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 0,1,2,…,n ตามกระบวนการ SUM ในหัวข้อที่ 4.2.2
3. คำนวณหาค่า feature code ของเฟรมของวีดีโอที่นำมาตรวจสอบ โดยกำหนดให้ขนาดของรูปภาพย่อยเท่ากับขนาดของรูปภาพย่อยที่ใช้กับ feature code ที่ได้จากขั้นตอนที่ 2
4. นำ feature code ที่ได้ในขั้นตอนที่ 3 ไปเปรียบเทียบกับ feature code ของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ ตามกระบวนการ SIMILARITY MEASURE ในหัวข้อที่ 4.2.3

4.4.1 การตรวจสอบความถูกต้องของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ $n \neq 0$ เมื่อมีการลดขนาดของรูปภาพย่อย

สำหรับวิธีการตรวจสอบความถูกต้องของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ $n \neq 0$ เมื่อมีการเพิ่มความละเอียดในการตรวจสอบจะมีวิธีคือ

1. ถอดรหัสลายเซ็นดิจิตอลที่ได้จากเฮดเดอร์ของแต่ละเฟรมของวีดีโอที่นำมาตรวจสอบด้วย public key ที่เป็นคู่กับ private key ที่ใช้เข้ารหัสตามอัลกอริทึมต่อไปนี้

```
for a = n to 0
        d_{a,c} = D_{a^th public key}(S_{a,c})
end
```

ผลลัพธ์ที่ได้จะมี 2 กรณีคือ

- c = 'I'

ผลลัพธ์ที่ได้คือ feature code ของวีดีโอต้นฉบับและ differential feature code ของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1,2,3,….,n ($f^*_{0,c}, f'_{1,c}, ..., f'_{n-1,c}, \bar{f}'_{n,c}$)

- c = 'P' หรือ c = 'B'

ผลลัพธ์ที่ได้คือ differential feature code ของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 0,1,2,….,n ($f'_{0,c}, f'_{1,c}, ..., f'_{n-1,c}, \bar{f}'_{n,c}$)

2. นำผลลัพธ์ที่ได้จากขั้นตอนที่ 1 มาคำนวณหาค่า feature code ของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 0,1,2,…,n-1 ตามกระบวนการ SUM ในหัวข้อที่ 4.2.2
3. นำ $f^*_{n-1,c}$ มาคำนวณหาค่า $\bar{f}^*_{n-1,c}$ ตามสมการที่ 4.10, 4.11 และ 4.12 ตามลำดับ แล้วแทนค่าด้วยเลขฐานสองขนาด 2 บิต ตามตารางที่ 4.1
4. นำผลลัพธ์ที่ได้ $\bar{f}'_{n,c}$, $\bar{f}^*_{n-1,c}$ มาคำนวณหาค่า $\bar{f}^*_{n,c}$ ตามกระบวนการ SUM ในหัวข้อที่ 4.2.2

5. คำนวณหาค่า feature code ของเฟรมของวีดีโอที่นำมาตรวจสอบ โดยกำหนดให้ขนาดของรูปภาพย่อยเท่ากับขนาดของรูปภาพย่อยที่ใช้กับเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ
6. นำ feature code ที่ได้ในขั้นตอนที่ 5 ไปเปรียบเทียบกับ feature code ของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ ตามกระบวนการ SIMILARITY MEASURE ในหัวข้อที่ 4.2.3

4.4.2 การตรวจสอบความถูกต้องของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ $n \neq 0$ เมื่อมีการเพิ่มขนาดของรูปภาพย่อย

สำหรับวิธีการตรวจสอบความถูกต้องของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ $n \neq 0$ เมื่อมีการลดความละเอียดในการตรวจสอบจะมีขั้นตอนคือ

1. ถอดรหัสลายเซ็นดิจิตอลที่ได้จากเฮดเดอร์ของแต่ละเฟรมของวีดีโอที่นำมาตรวจสอบด้วย public key ที่เป็นคู่กับ private key ที่ใช้เข้ารหัสตามอัลกอริทึมต่อไปนี้

```
for a = n to 0
        d_{a,c} = D_{a^th public key}(S_{a,c})
end
```

ผลลัพธ์ที่ได้จะมี 2 กรณีคือ

- c = 'I'

ผลลัพธ์ที่ได้คือ feature code ของวีดีโอต้นฉบับและ differential feature code ของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1,2,3,….,n $(f^{*}_{0,c} f'_{1,c},..., f'_{n-1,c}, \vec{f}'_{n,c})$

- c = 'P' หรือ c = 'B'

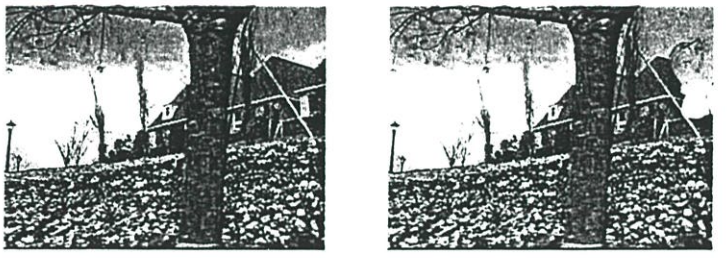
ผลลัพธ์ที่ได้คือ differential feature code ของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 0,1,2,….,n $(f'_{0,c}, f'_{1,c},..., f'_{n-1,c}, \vec{f}'_{n,c})$

2. นำผลลัพธ์ที่ได้จากขั้นตอนที่ 1 มาคำนวณหาค่า feature code ของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 0,1,2,…,n-1 ตามกระบวนการ SUM ในหัวข้อที่ 4.2.2
3. นำ $f^{*}_{n-1,c}$ มาคำนวณหาค่า $\vec{f}^{*}_{n-1,c}$ ตามสมการที่ 4.10, 4.14 และ 4.15 ตามลำดับ แล้วแทนค่าด้วยเลขฐานสองขนาด 2 บิต ตามตารางที่ 4.1
4. นำผลลัพธ์ที่ได้ $(\vec{f}'_{n,c}, \vec{f}^{*}_{n-1,c})$ มาคำนวณหาค่า $\vec{f}^{*}_{n,c}$ ตามกระบวนการ SUM ในหัวข้อที่ 4.2.2
5. คำนวณหาค่า feature code ของเฟรมของวีดีโอที่นำมาตรวจสอบ โดยกำหนดให้ขนาดของรูปภาพย่อยเท่ากับขนาดของรูปภาพย่อยที่ใช้กับเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ

6. นำ feature code ที่ได้ในขั้นตอนที่ 5 ไปเปรียบเทียบกับ feature code ของเฟรมของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ ตามกระบวนการ SIMILARITY MEASURE ในหัวข้อที่ 4.2.3

4.5 ประสิทธิภาพของการตรวจสอบ

จากผลการตรวจสอบความถูกต้องโดยวิธีที่ได้นำเสนอนี้ ผู้วิจัยได้ทำการวัดประสิทธิภาพของวิธีการตรวจสอบเพื่อให้เห็นความถูกต้องของผลการทดลองได้อย่างชัดเจน โดยใช้การเปรียบเทียบระหว่างพิกเซลของบริเวณที่ระบุได้จากขั้นตอนการตรวจสอบ กับพิกเซลของบริเวณที่ได้รับการแก้ไขจริงในรูปภาพ และเปรียบเทียบระหว่างรูปภาพย่อยที่ระบุได้จากขั้นตอนการตรวจสอบ กับรูปภาพย่อยของบริเวณที่ได้รับการแก้ไขจริงในรูปภาพ โดยรูปที่ 4.9 จะแสดงรูปภาพที่ใช้เป็นตัวอย่างรูปภาพต้นฉบับและรูปภาพที่ถูกแก้ไขในหัวข้อนี้



(a) (b)

รูปที่ 4.9 (a) รูปภาพต้นฉบับ, (b) รูปภาพที่ถูกแก้ไข

4.5.1 จุดเปลี่ยนแปลงที่ตรวจพบ

จุดเปลี่ยนแปลงที่ตรวจพบ หมายถึงรูปภาพย่อยตำแหน่งที่ i,j ใดๆ ที่ $A_{i,j}= 1$ ส่วนพิกเซลทั้งหมดของรูปภาพที่ทำการตรวจสอบความถูกต้องจะใช้สัญลักษณ์ $p_{x,y}$ โดยที่ $x \in \{1,...,M\}$, $y \in \{1,...,N\}$ ซึ่งพิกเซลที่อยู่ในรูปภาพย่อยที่ $A_{i,j}= 1$ จะมีค่าเป็น 1 ($p_{x,y} = 1$ คือ พิกเซลที่เป็นจุดเปลี่ยนแปลงที่ตรวจพบ) แต่ถ้าอยู่ในรูปภาพย่อยที่ $A_{i,j}= 0$ จะมีค่าเป็น 0 ($p_{x,y} = 0$ คือ พิกเซลที่ไม่ใช่จุดเปลี่ยนแปลงที่ตรวจพบ) ดังรูปที่ 4.10

รูปที่ 4.10 ผลการตรวจสอบรูปภาพ

4.5.2 จุดเปลี่ยนแปลงจริง

จุดเปลี่ยนแปลงจริง หมายถึงจุดที่ได้รับการแก้ไขจริงในรูปภาพพิจารณาเฉพาะจุดที่ถูกแก้ไขแล้วทำให้ความหมายของรูปภาพเปลี่ยนแปลงไป ซึ่งจุดเปลี่ยนแปลงจริงเกิดจากการนำรูปภาพต้นฉบับมาเปรียบเทียบกับรูปภาพที่นำมาตรวจสอบ รูปภาพย่อยที่มีค่าความสว่างของพิกเซลใดไม่เหมือนรูปภาพต้นฉบับจะนับเป็นรูปภาพย่อยที่ได้รับการแก้ไขจริง จะใช้สัญลักษณ์ $B_{i,j}$ โดยที่ $B_{i,j} \in \{0,1\}$ ค่า 0 หมายถึงไม่มีการเปลี่ยนแปลง และค่า 1 หมายถึงมีการเปลี่ยนแปลง ส่วนพิกเซลของบริเวณที่ได้รับการแก้ไขจริงในรูปภาพเกิดจากการนำรูปภาพต้นฉบับมาเปรียบเทียบกับรูปภาพที่นำมาตรวจสอบ พิกเซลที่มีค่าความสว่างไม่เหมือนกับรูปภาพต้นฉบับจะนับเป็นพิกเซลที่ได้รับการแก้ไขจริง จะใช้สัญลักษณ์ $q_{x,y}$ โดยที่ $q_{x,y} \in \{0,1\}$ ค่า 0 หมายถึงไม่มีการเปลี่ยนแปลง และค่า 1 หมายถึงมีการเปลี่ยนแปลง ดังรูปที่ 4.11 บริเวณที่แรเงาของรูปภาพที่ถูกแก้ไขเป็นบริเวณที่มีพิกเซลแตกต่างไปจากรูปภาพต้นฉบับ

รูปที่ 4.11 จุดเปลี่ยนแปลงจริง

4.5.3 สมการหาค่าความแม่นยำ (Precision)

ขั้นตอนต่อไปนี้เป็นการนำข้อมูลของพิกเซลที่มีการเปลี่ยนแปลง ทั้ง 2 ประเภทมาทำการคำนวณหาเปอร์เซ็นต์ความแม่นยำในการระบุตำแหน่งของรูปภาพที่ถูกแก้ไขเปลี่ยนแปลง โดยใช้สมการที่ 4.17 หาอัตราส่วนระหว่าง จำนวนสมาชิกพิกเซลของพื้นที่ระบุได้จากการตรวจสอบที่ตรง

กับพิกเซลที่เปลี่ยนแปลงจริง ต่อจำนวนสมาชิกของพิกเซลที่เปลี่ยนแปลงจริง คิดเป็นเปอร์เซ็นต์ ความแม่นยำมีค่าตั้งแต่ 0% ถึง 100%

$$\text{Precision} = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N} p_{x,y} \cdot q_{x,y}}{\sum_{x=1}^{M}\sum_{y=1}^{N} q_{x,y}} \times 100 \qquad (4.17)$$

จากสมการข้างต้นในกรณีที่รูปภาพมีพิกเซลที่เปลี่ยนแปลงจริงตรงกับพิกเซลที่ระบุได้จากการตรวจสอบ $p_{x,y} \cdot q_{x,y} = q_{x,y}$ ค่าความแม่นยำจะเป็น 100% ซึ่งหมายความว่าสามารถระบุพิกเซลบริเวณที่ถูกแก้ไขเปลี่ยนแปลงได้ทั้งหมด แต่ถ้าพิกเซลที่ระบุได้จากการตรวจสอบไม่ตรงกับพิกเซลที่เปลี่ยนแปลงจริงค่าความแม่นยำเป็น 0 %

4.5.4 สมการหาค่าความถูกต้อง (Accuracy)

การคำนวณหาเปอร์เซ็นต์ความถูกต้องโดยใช้สมการที่ 4.18 หาอัตราส่วนระหว่าง จำนวนสมาชิกของรูปภาพย่อยที่ระบุได้จากการตรวจสอบที่ตรงกับรูปภาพย่อยที่เปลี่ยนแปลงจริง ต่อจำนวนสมาชิกทั้งหมดของรูปภาพย่อยที่เปลี่ยนแปลงจริง คิดเป็นเปอร์เซ็นต์ความถูกต้องมีค่าตั้งแต่ 0% ถึง 100%

$$\text{Accuracy} = \frac{\sum_{i=1}^{\lfloor M/b \rfloor}\sum_{j=1}^{\lfloor N/b \rfloor} A_{i,j} \cdot B_{i,j}}{\sum_{i=1}^{\lfloor M/b \rfloor}\sum_{j=1}^{\lfloor N/b \rfloor} B_{i,j}} \times 100 \qquad (4.18)$$

จากสมการข้างต้นในกรณีที่รูปภาพมีรูปภาพย่อยที่เปลี่ยนแปลงจริงตรงกับรูปภาพย่อยที่ระบุได้จากการตรวจสอบ $A_{i,j} \cdot B_{i,j} = B_{i,j}$ ค่าความถูกต้องจะเป็น 100% ซึ่งหมายความว่าสามารถระบุรูปภาพย่อยบริเวณที่ถูกแก้ไขเปลี่ยนแปลงได้ทั้งหมด แต่ถ้าไม่สามารถตรวจพบรูปภาพย่อยที่เปลี่ยนแปลงจริงได้ ค่าความถูกต้องจะเป็น 0%

4.5.5 สมการหาค่าความผิดพลาด (False alarm)

การคำนวณหาเปอร์เซ็นต์ความผิดพลาดโดยใช้สมการที่ 4.19 หาอัตราส่วนระหว่าง จำนวนสมาชิกของรูปภาพย่อยที่ระบุได้จากการตรวจสอบแต่ไม่ใช่พื้นที่ของรูปภาพย่อยที่ถูกเปลี่ยนแปลง

จริง ต่อจำนวนสมาชิกทั้งหมดของรูปภาพย่อยที่ไม่ถูกแก้ไขจริง คิดเป็นเปอร์เซ็นต์ความถูกต้องมีค่าตั้งแต่ 0% ถึง 100%

$$\text{False alarm} = \frac{\sum_{x=1}^{\lfloor M/b \rfloor}\sum_{y=1}^{\lfloor N/b \rfloor} A_{i,j} \cdot (1 - B_{i,j})}{(\lfloor M/b \rfloor \cdot \lfloor N/b \rfloor) - \sum_{i=1}^{\lfloor M/b \rfloor}\sum_{j=1}^{\lfloor N/b \rfloor} B_{i,j}} \times 100 \qquad (4.19)$$

จากสมการข้างต้นในกรณีที่รูปภาพมีรูปภาพย่อยที่ระบุได้จากการตรวจสอบตรงกับรูปภาพย่อยที่มีการแก้ไขจริง ค่าความผิดพลาดจะเป็น 0% ในทางตรงกันข้ามถ้ารูปภาพย่อยทั้งหมดคือจุดเปลี่ยนแปลงที่ตรวจพบแต่ไม่ใช่จุดเปลี่ยนแปลงจริง ค่าความผิดพลาดจะเป็น 100%

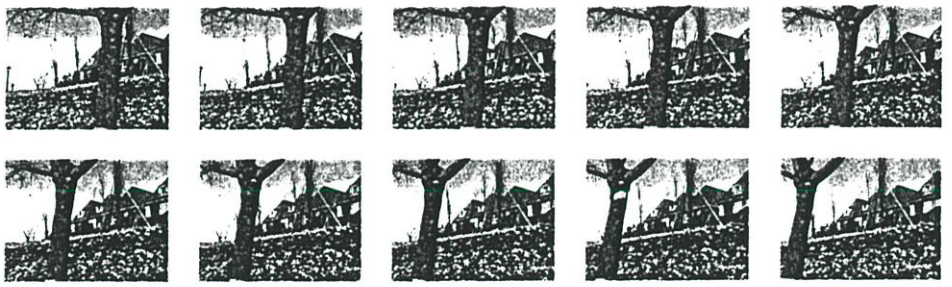
บทที่ 5
ขั้นตอนการทดลองและผลการทดลอง

5.1 ขั้นตอนการทดลองและการตรวจสอบผล

การทดลองในงานวิจัยนี้ ผู้วิจัยได้นำวีดีโอมาทำการตรวจสอบความถูกต้อง ซึ่งผู้วิจัยได้ทำการจำลองกระบวนการรับส่งข้อมูลวีดีโอระหว่างเจ้าของลิขสิทธิ์ ผู้ที่มีกรรมสิทธิ์ในการทำสำเนาวีดีโอลำดับที่ 1 และผู้รับ โดยทำการทดสอบและแสดงผลการเปรียบเทียบระหว่างวีดีโอที่มีการแก้ไขโดยผู้ที่ประสงค์ร้ายกับวีดีโอต้นฉบับและวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1

การสร้างระบบกุญแจสาธารณะ (Public Key Cryptography) สำหรับการเข้าและถอดรหัสเพื่อสร้างลายเซ็นดิจิตอล จะใช้ระบบของ PGP ซึ่ง PGP นอกจากจะใช้สร้างคู่กุญแจคือ public key และ private key แล้วยังมีระบบในการจัดเก็บกุญแจให้มีความปลอดภัยและระบบในการกระจาย public key และการตรวจสอบความถูกต้องของ public key อีกด้วย โดยกำหนดให้ขนาดของคู่กุญแจของเจ้าของลิขสิทธิ์วีดีโอและคู่กุญแจของผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 มีขนาด 1024 บิต

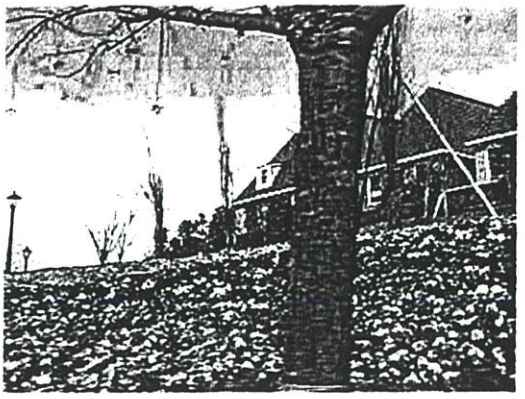
วีดีโอที่นำมาทดลองนี้ใช้การบีบอัดและเก็บบันทึกตามมาตรฐาน MPEG-1 โดยมีความละเอียดที่ 320×240 พิกเซล และมีอัตราการแสดงภาพ 30 เฟรมต่อวินาที ดังรูปที่ 5.1



รูปที่ 5.1 ลำดับของเฟรม

5.1.1 การสร้างลายเซ็นดิจิตอลสำหรับเฟรมต้นฉบับ

แบ่งเฟรมออกเป็นรูปภาพย่อยขนาด 16×16 พิกเซล แล้วทำการคำนวณหาค่า DC coefficient ของแต่ละรูปภาพย่อยเพื่อนำมาหาค่า feature code ตามสมการที่ 4.1, 4.2 และ 4.3 (ในบทที่ 4) โดยใช้ค่า α_1 = -0.02880, α_2 = 0.03070, β = 0.00020 และทำการแทนค่า feature code ด้วยข้อมูลขนาด 2 บิตตามตารางที่ 4.1 ซึ่งจะได้ feature code ที่มีขนาด 1200 บิต แล้วนำ feature code ที่ได้มาเข้ารหัสด้วย private key ของเจ้าของลิขสิทธิ์วีดีโอ ก็จะได้ลายเซ็นดิจิตอลสำหรับเฟรมต้นฉบับ

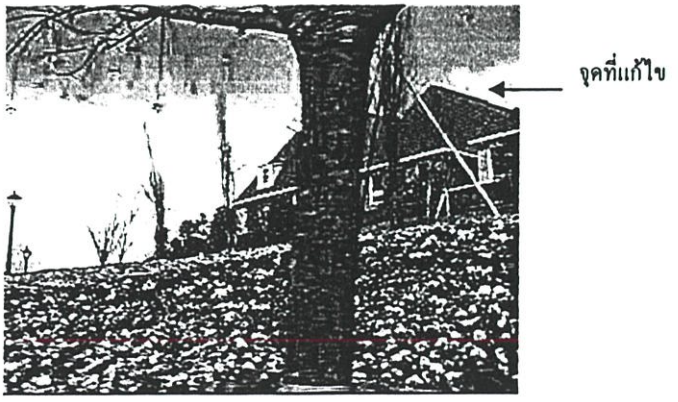


รูปที่ 5.2 เฟรมต้นฉบับ

5.1.2 การสร้างลายเซ็นดิจิตอลสำหรับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1

5.1.2.1 รูปภาพย่อยขนาด 8×8

เฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 สามารถแสดงได้ดังรูปที่ 5.3 ซึ่งการสร้างลายเซ็นดิจิตอลจะมีขั้นตอนเหมือนกับการสร้างลายเซ็นดิจิตอลสำหรับเฟรมต้นฉบับ แต่ขนาดของรูปภาพย่อยที่ใช้สำหรับการคำนวณหาค่า feature code จะมีขนาดเล็กลงคือ 8×8 พิกเซล โดยกำหนดค่า α_1 = -0.02100, α_2 = 0.02370, β = 0.00047 จะได้ feature code ที่มีขนาด 4800 บิต และนำ feature code ที่ได้มาเรียงต่อกับลายเซ็นดิจิตอลของเฟรมต้นฉบับ แล้วเข้ารหัสด้วย private key ของผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 ก็จะได้ลายเซ็นดิจิตอลสำหรับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1



รูปที่ 5.3 เฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1

5.1.2.2 รูปภาพย่อยขนาด 16×16

การสร้างลายเซ็นดิจิตอลจะมีขั้นตอนเหมือนกับการสร้างลายเซ็นดิจิตอลสำหรับเฟรมต้นฉบับ ซึ่งขนาดของรูปภาพย่อยที่ใช้สำหรับการคำนวณหาค่า feature code จะมีขนาดเท่าเดิมคือ 16×16 พิกเซล โดยกำหนดค่า α_1 = -0.02880, α_2 = 0.03070, β = 0.00020 จะได้ feature code ที่มีขนาด 1200 บิต และนำ feature code ที่ได้มาเรียงต่อกับลายเซ็นดิจิตอลของเฟรมต้นฉบับ แล้วเข้ารหัสด้วย private key ของผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 ก็จะได้ลายเซ็นดิจิตอลสำหรับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1

5.1.2.3 รูปภาพย่อยขนาด 32×32

การสร้างลายเซ็นดิจิตอลจะมีขั้นตอนเหมือนกับการสร้างลายเซ็นดิจิตอลสำหรับเฟรมต้นฉบับ แต่ขนาดของรูปภาพย่อยที่ใช้สำหรับการคำนวณหาค่า feature code จะมีขนาดใหญ่ขึ้นคือ 32×32 พิกเซล โดยกำหนดค่า α_1 = -0.03110, α_2 = 0.04470, β = 0.00001 จะได้ feature code ที่มีขนาด 280 บิต และนำ feature code ที่ได้มาเรียงต่อกับลายเซ็นดิจิตอลของเฟรมต้นฉบับ แล้วเข้ารหัสด้วย private key ของผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 ก็จะได้ลายเซ็นดิจิตอลสำหรับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1

5.1.3 การสร้างลายเซ็นดิจิตอลแบบสมทบส่วนต่างสำหรับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1

5.1.3.1 รูปภาพย่อยขนาด 8×8

ทำการคำนวณหาค่า feature code ของเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 โดยกำหนดให้รูปภาพย่อยมีขนาด 8×8 พิกเซล และนำลายเซ็นดิจิตอลที่ได้จากเฮดเดอร์ของเฟรมมาถอดรหัสด้วย public key ของเจ้าของลิขสิทธิ์วีดีโอ แล้วนำ feature code ของเฟรมต้นฉบับ (รูปภาพย่อยมีขนาด 16×16 พิกเซล) มาคำนวณหาค่า feature code ของเฟรมต้นฉบับที่มีขนาดของรูปภาพย่อยเท่ากับ 8×8พิกเซล ตามสมการที่ 4.10, 4.11 และ 4.12 ตามลำดับ เพื่อนำมาคำนวณหาค่า differential feature code ของเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 ตามกระบวนการ SUBTRACT ในหัวข้อที่ 4.1.3 จะได้ differential feature code ที่มีขนาด 4538 บิต จากนั้นนำ differential feature code ไปเรียงต่อกับลายเซ็นดิจิตอลของเฟรมต้นฉบับ แล้วเข้ารหัสด้วย private key ของผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 ก็จะได้ลายเซ็นดิจิตอลแบบสมทบส่วนต่างสำหรับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1

5.1.3.2 รูปภาพย่อยขนาด 16×16

ทำการคำนวณหาค่า feature code ของเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 โดยกำหนดให้รูปภาพย่อยมีขนาด 16×16 พิกเซล และนำลายเซ็นดิจิตอลที่ได้จากเฮดเดอร์ของเฟรมมาถอดรหัสด้วย public key ของเจ้าของลิขสิทธิ์วีดีโอ จะได้ feature code ของเฟรม

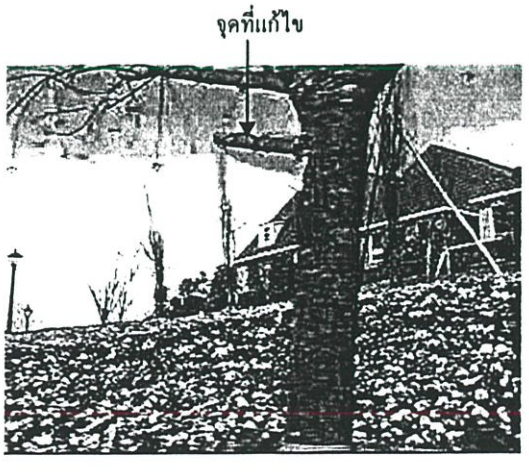
ต้นฉบับ แล้วคำนวณหาค่า differential feature code ของเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 ตามกระบวนการ SUBTRACT ในหัวข้อที่ 4.1.3 จะได้ differential feature code ที่มีขนาด 606 บิต จากนั้นนำ differential feature code ไปเรียงต่อกับลายเซ็นดิจิตอลของเฟรมต้นฉบับ แล้วเข้ารหัสด้วย private key ของผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 ก็จะได้ลายเซ็นดิจิตอลแบบสมทบส่วนต่างสำหรับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1

5.1.3.3 รูปภาพย่อยขนาด 32×32

ทำการคำนวณหาค่า feature code ของ เฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 โดยกำหนดให้รูปภาพย่อยมีขนาด 32×32 พิกเซล และนำลายเซ็นดิจิตอลที่ได้จากเฮดเดอร์ของเฟรมมาถอดรหัสด้วย public key ของเจ้าของลิขสิทธิ์วีดีโอ แล้วนำ feature code ของเฟรมต้นฉบับ (รูปภาพย่อยมีขนาด 16×16 พิกเซล) มาคำนวณหาค่า feature code ของเฟรมต้นฉบับที่มีขนาดของรูปภาพย่อยเท่ากับ 32×32 พิกเซล ตามสมการที่ 4.10, 4.14 และ 4.15 ตามลำดับ เพื่อนำมาคำนวณหาค่า differential feature code ของเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 ตามกระบวนการ SUBTRACT ในหัวข้อที่ 4.1.3 จะได้ differential feature code ที่มีขนาด 236 บิต จากนั้นนำ differential feature code ไปเรียงต่อกับลายเซ็นดิจิตอลของเฟรมต้นฉบับ แล้วเข้ารหัสด้วย private key ของผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 ก็จะได้ลายเซ็นดิจิตอลแบบสมทบส่วนต่างสำหรับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1

5.1.4 การแก้ไขเฟรมวีดีโอโดยผู้ที่ประสงค์ร้าย

เฟรมที่ถูกแก้ไขโดยผู้ที่ไม่มีกรรมสิทธิ์ในการทำสำเนาสามารถแสดงได้ดังรูปที่ 5.4



รูปที่ 5.4 เฟรมที่มีการแก้ไขโดยผู้ที่ประสงค์ร้าย

5.1.5 การตรวจสอบความถูกต้องของเฟรมที่สร้างลายเซ็นดิจิตอล

นำลายเซ็นดิจิตอลที่ได้มาถอดรหัสด้วย public key ของผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 จะได้ feature code ของเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 และลายเซ็นดิจิตอลของเฟรมต้นฉบับ ซึ่งจะต้องนำมาถอดรหัสด้วย public key ของเจ้าของลิขสิทธิ์ ก็จะได้ feature code ของเฟรมต้นฉบับ จากนั้นคำนวณหาค่า feature code ของเฟรมที่นำมาตรวจสอบ โดยกำหนดให้รูปภาพย่อยมีขนาด 16×16 และรูปภาพย่อยที่มีขนาดเท่ากับขนาดของรูปภาพย่อยที่ใช้กับวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 ซึ่งจะได้ feature code 2 กลุ่ม ตามลำดับ แล้วนำ feature code กลุ่มแรกไปเปรียบเทียบกับ feature code ของเฟรมต้นฉบับ ส่วน feature code กลุ่มที่ 2 จะเปรียบเทียบกับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 ตามกระบวนการ SIMILARITY MEASURE ในหัวข้อที่ 4.2.3

5.1.6 การตรวจสอบความถูกต้องของเฟรมที่สร้างลายเซ็นดิจิตอลแบบสมทบส่วนต่าง

5.1.6.1 รูปภาพย่อยขนาด 8×8 (ขนาดที่ใช้กับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1)

นำลายเซ็นดิจิตอลที่ได้มาถอดรหัสด้วย public key ของผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 จะได้ differential feature code ของเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 และลายเซ็นดิจิตอลของเฟรมต้นฉบับ ซึ่งจะต้องนำมาถอดรหัสด้วย public key ของเจ้าของลิขสิทธิ์ แล้วนำ feature code ของเฟรมต้นฉบับ (รูปภาพย่อยมีขนาด 16×16 พิกเซล) มาคำนวณหาค่า feature code ของเฟรมต้นฉบับที่มีขนาดของรูปภาพย่อยเท่ากับ 8×8 พิกเซล ตามสมการที่ 4.10, 4.11 และ 4.12 ตามลำดับ เพื่อนำมาคำนวณหาค่า feature code ของเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 ตามกระบวนการ SUM ในหัวข้อที่ 4.2.2 จากนั้นคำนวณหาค่า feature code ของเฟรมที่นำมาตรวจสอบโดยกำหนดให้รูปภาพย่อยมีขนาด 16×16 และ 8×8 พิกเซล แล้วนำไปเปรียบเทียบกับ feature code ของเฟรมต้นฉบับ (รูปภาพย่อยมีขนาด 16×16 พิกเซล) และ feature code ของเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 ตามกระบวนการ SIMILARITY MEASURE ในหัวข้อที่ 4.2.3

5.1.6.2 รูปภาพย่อยขนาด 16×16

นำลายเซ็นดิจิตอลที่ได้มาถอดรหัสด้วย public key ของผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 จะได้ differential feature code ของเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 และลายเซ็นดิจิตอลของเฟรมต้นฉบับ ซึ่งจะต้องนำมาถอดรหัสด้วย public key ของเจ้าของลิขสิทธิ์ ก็จะได้ feature code ของเฟรมต้นฉบับ แล้วคำนวณหาค่า feature code ของเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1จากกระบวนการ SUM ในหัวข้อที่ 4.2.2 จากนั้นคำนวณหาค่า feature code ของเฟรมที่นำมาตรวจสอบโดยกำหนดให้รูปภาพย่อยมีขนาด 16×16 พิก

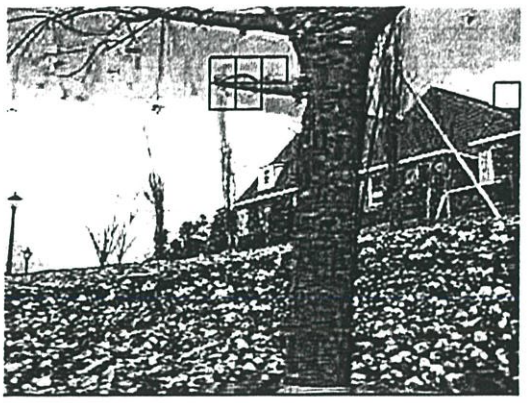
เซล แล้วนำ feature code ที่ได้ไปเปรียบเทียบกับ feature code ของเฟรมต้นฉบับและ feature code ของเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 ตามกระบวนการ SIMILARITY MEASURE ในหัวข้อที่ 4.2.3

5.1.6.3 รูปภาพย่อยขนาด 32×32

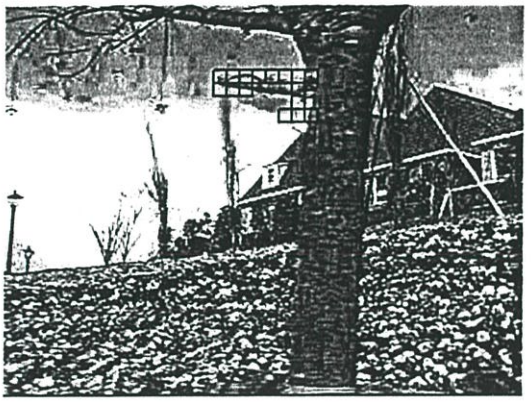
นำลายเซ็นดิจิตอลที่ได้มาถอดรหัสด้วย public key ของผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 จะได้ differential feature code ของเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 และลายเซ็นดิจิตอลของเฟรมต้นฉบับ ซึ่งจะต้องนำมาถอดรหัสด้วย public key ของเจ้าของลิขสิทธิ์ แล้วนำ feature code ของเฟรมต้นฉบับ (รูปภาพย่อยมีขนาด 16×16 พิกเซล) มาคำนวณหาค่า feature code ของเฟรมต้นฉบับที่มีขนาดของรูปภาพย่อยเท่ากับ 32×32 พิกเซล ตามสมการที่ 4.10, 4.14 และ 4.15 ตามลำดับ เพื่อนำมาคำนวณหาค่า feature code ของเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 ตามกระบวนการ SUM ในหัวข้อที่ 4.2.2 จากนั้นคำนวณหาค่า feature code ของเฟรมที่นำมาตรวจสอบโดยกำหนดให้รูปภาพย่อยมีขนาด 16×16 และ 32×32 พิกเซล แล้วนำไปเปรียบเทียบกับ feature code ของเฟรมต้นฉบับ (รูปภาพย่อยมีขนาด 16×16 พิกเซล) และ feature code ของเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 ตามกระบวนการ SIMILARITY MEASURE ในหัวข้อที่ 4.2.3

5.2 ผลการทดลอง

เมื่อนำเฟรมที่มีการแก้ไขโดยผู้ที่ประสงค์ร้ายมาตรวจสอบความถูกต้องของเฟรมโดยเปรียบเทียบกับเฟรมต้นฉบับและเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 ซึ่งถ้ากำหนดให้รูปภาพย่อยที่ใช้กับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 มีขนาดลดลงจากขนาดของรูปภาพย่อยที่ใช้กับเฟรมต้นฉบับ คือมีขนาด 8×8 พิกเซล จะได้ผลดังรูปที่ 5.5 และถ้ากำหนดให้รูปภาพย่อยที่ใช้กับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 มีขนาดเท่ากับขนาดของรูปภาพย่อยที่ใช้กับเฟรมต้นฉบับ คือมีขนาด 16×16 พิกเซล จะได้ผลดังรูปที่ 5.6 และถ้ากำหนดให้รูปภาพย่อยที่ใช้กับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 มีขนาดเพิ่มขึ้นจากขนาดของรูปภาพย่อยที่ใช้กับเฟรมต้นฉบับ คือมีขนาด 32×32 พิกเซล จะได้ผลดังรูปที่ 5.7



(a)



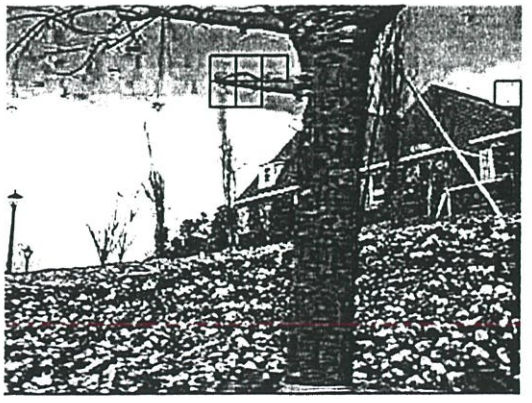
(b)

(c)

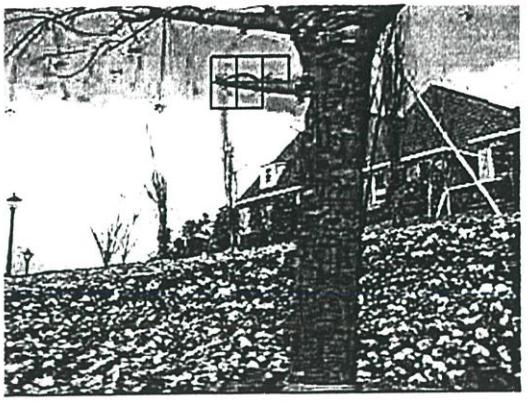
รูปที่ 5.5 (a) ภาพการตรวจสอบเฟรมเมื่อเปรียบเทียบกับเฟรมต้นฉบับ

(b) ภาพการตรวจสอบเฟรมเมื่อเปรียบเทียบกับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1

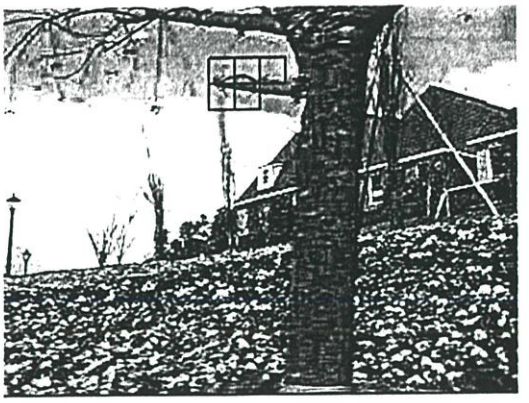
(c) ภาพการตรวจสอบเฟรมเมื่อเปรียบเทียบกับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 (ลายเซ็นดิจิตอลแบบสมทบส่วนต่าง)



(a)



(b)

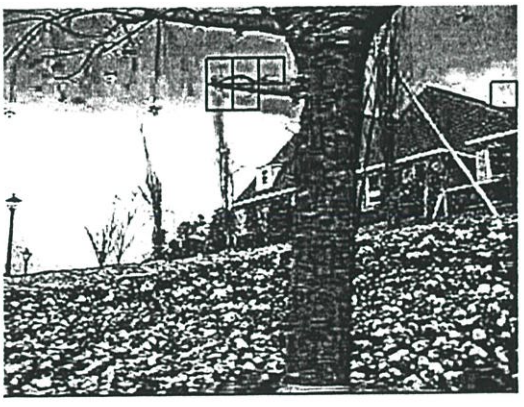


(c)

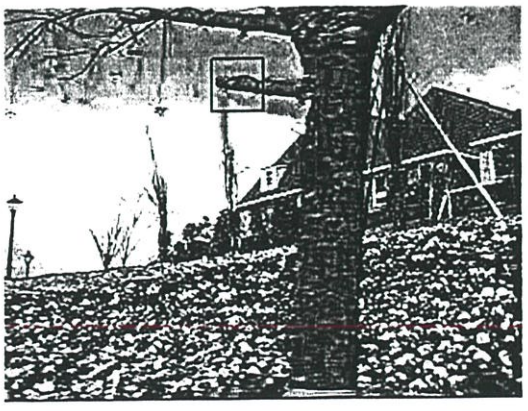
รูปที่ 5.6 (a) ภาพการตรวจสอบเฟรมเมื่อเปรียบเทียบกับเฟรมต้นฉบับ

(b) ภาพการตรวจสอบเฟรมเมื่อเปรียบเทียบกับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1

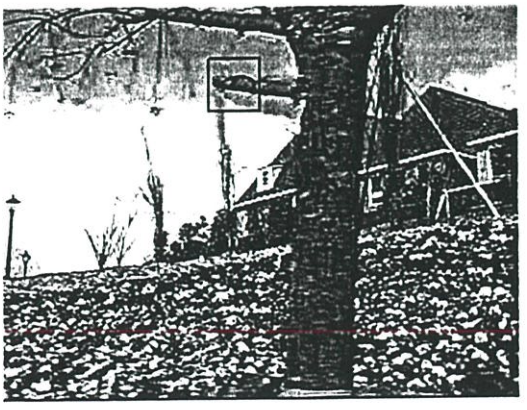
(c) ภาพการตรวจสอบเฟรมเมื่อเปรียบเทียบกับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 (ลายเซ็นดิจิตอลแบบสมทบส่วนต่าง)



(a)



(b)



(c)

รูปที่ 5.7 (a) ภาพการตรวจสอบเฟรมเมื่อเปรียบเทียบกับเฟรมต้นฉบับ

(b) ภาพการตรวจสอบเฟรมเมื่อเปรียบเทียบกับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1

(c) ภาพการตรวจสอบเฟรมเมื่อเปรียบเทียบกับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 (ลายเซ็นดิจิตอลแบบสมทบส่วนต่าง)

5.3 การวัดประสิทธิภาพของวิธีการตรวจสอบความถูกต้อง

ในหัวข้อนี้จะเป็นการวัดประสิทธิภาพของวิธีการตรวจสอบความถูกต้อง โดยทดลองกับวีดีโอทั้งหมด 5 เรื่อง และ รูปภาพจำนวน 5 ภาพ (ดูในภาคผนวก ข) ซึ่งจะมีวิธีการทดลองดังนี้

1. นำวีดีโอแต่ละเรื่องมาคำนวณหาค่า feature code และ differential feature code เพื่อวัดจำนวนบิตของ differential feature code ของเฟรม P,B ว่ามีการลดลงของจำนวนบิตเท่าใดเมื่อเปรียบเทียบกับจำนวนบิตของ feature code ของเฟรม P,B นั้นๆ โดยจะแสดงค่าเฉลี่ยของจำนวนบิตที่ลดลง
2. นำรูปภาพทั้งหมดมาทำการแก้ไขรูปภาพโดยพื้นที่ที่ถูกแก้ไขจะแบ่งเป็น 3 ขนาด คือ 128×160 พิกเซล 64×80 พิกเซล และ 32×40 พิกเซล ส่วนตำแหน่งของพื้นที่ที่ถูกแก้ไขจะสุ่มเลือก 3 ครั้ง เพื่อวัดค่าเฉลี่ยของความแม่นยำ ความถูกต้อง และความผิดพลาด
3. นำรูปภาพทั้งหมดมาผ่านกระบวนการแก้ไขรูปภาพพื้นฐานประเภทต่างๆ คือ การปรับค่าความสว่าง การปรับค่าความแตกต่างของความสว่าง การบีบอัดแบบ JPEG และการเพิ่มสัญญาณรบกวน ในระดับการแก้ไขต่างๆ กัน เพื่อวัดค่าเฉลี่ยของความผิดพลาด

จะได้ผลลัพธ์ดังต่อไปนี้

ในการสร้างลายเซ็นดิจิตอลแบบสมทบส่วนต่างสำหรับเฟรม P,B โดยกำหนดให้รูปภาพย่อยมีขนาด 16×16 พิกเซล และ unknown band = 1% จะทำให้ differential feature code ที่ใช้สร้างลายเซ็นดิจิตอลมีขนาดลดลง 20.13%

ในการสร้างลายเซ็นดิจิตอลแบบสมทบส่วนต่างสำหรับเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1 โดยกำหนดให้รูปภาพย่อยมีขนาด 16×16 พิกเซล และ unknown band = 1% จะทำให้ differential feature code ที่ใช้สร้างลายเซ็นดิจิตอลมีขนาดลดลงดังตารางที่ 5.1

ตารางที่ 5.1 เปอร์เซ็นต์ของจำนวนบิตที่ลดลงของ differential feature code ของเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับที่ 1

จำนวนรูปภาพย่อยที่ถูกแก้ไข	เปอร์เซ็นต์ของจำนวนบิตที่ลดลงของ differential feature code
1×1	49.67%
2×2	48.67%
3×3	47.00%
4×4	44.67%
5×5	41.67%

ตารางที่ 5.2 การวัดประสิทธิภาพของการตรวจสอบรูปภาพที่ถูกแก้ไขจำแนกตามพื้นที่ของบริเวณที่ถูกแก้ไข โดยกำหนดขนาดของรูปภาพย่อย (b×b) ต่างๆ

(a) : ค่าความแม่นยำ

ขนาดของพื้นที่ที่ถูกแก้ไข	Unknown band = 1%			Unknown band = 10%		
	b = 8	b = 16	b = 32	b = 8	b = 16	b = 32
128×160	58.41%	56.63%	47.62%	37.86%	37.86%	36.87%
64×80	54.61%	42.11%	23.92%	37.84%	30.48%	21.57%
32×40	52.79%	39.43%	20.54%	37.78%	28.58%	20.54%

จากผลการทดลองพบว่าขนาดของรูปภาพย่อยที่ใช้คำนวณหาค่า feature code มีผลต่อค่าความแม่นยำ กล่าวคือ ถ้ารูปภาพย่อยมีขนาดใหญ่ขึ้นหรือ unknown band สูงขึ้น ค่าความแม่นยำจะลดลง ส่วนขนาดของพื้นที่ที่ถูกแก้ไขก็มีผลต่อค่าความแม่นยำกล่าวคือ ถ้าขนาดของพื้นที่ที่ถูกแก้ไขมีขนาดใหญ่ขึ้น ค่าความแม่นยำจะเพิ่มขึ้น

(b) : ค่าความถูกต้อง (เมื่อกำหนดให้รูปภาพย่อยที่ถูกแก้ไขจริง คือ รูปภาพย่อยที่มีพิกเซลที่ถูกแก้ไขมากกว่า 1 พิกเซล)

ขนาดของพื้นที่ที่ถูกแก้ไข	Unknown band = 1%			Unknown band = 10%		
	b = 8	b = 16	b = 32	b = 8	b = 16	b = 32
128×160	57.25%	63.05%	66.67%	35.22%	45.81%	50.83%
64×80	55.31%	59.91%	64.79%	34.93%	35.19%	48.33%
32×40	45.32%	49.72%	62.50%	32.76%	33.05%	42.50%

(c) : ค่าความถูกต้อง (เมื่อกำหนดให้รูปภาพย่อยที่ถูกแก้ไขจริง คือ รูปภาพย่อยที่มีพิกเซลที่ถูกแก้ไขมากกว่า 25%)

ขนาดของพื้นที่ที่ถูกแก้ไข	Unknown band = 1%			Unknown band = 10%		
	b = 8	b = 16	b = 32	b = 8	b = 16	b = 32
128×160	69.46%	77.31%	78.84%	49.16%	54.75%	64.59%
64×80	63.09%	70.83%	75.00%	48.31%	54.04%	62.43%
32×40	52.67%	66.67%	71.21%	40.11%	48.61%	57.28%

(d) : ค่าความถูกต้อง (เมื่อกำหนดให้รูปภาพย่อยที่ถูกแก้ไขจริง คือ รูปภาพย่อยที่มีพิกเซลที่ถูกแก้ไขมากกว่า 50 %)

ขนาดของพื้นที่ที่ถูกแก้ไข	Unknown band = 1%			Unknown band = 10%		
	b = 8	b = 16	b = 32	b = 8	b = 16	b = 32
128×160	73.18%	78.38%	80.43%	51.54%	59.30%	66.08%
64×80	69.49%	73.29%	75.00%	49.29%	56.25%	62.92%
32×40	57.32%	68.75%	71.24%	46.46%	53.70%	58.11%

จากผลการทดลอง (ตารางที่ 5.2 (b) – 5.2 (d)) พบว่าขนาดของรูปภาพย่อยที่ใช้คำนวณหาค่า feature code มีผลต่อค่าความถูกต้อง กล่าวคือ ถ้ารูปภาพย่อยมีขนาดใหญ่ขึ้น หรือ unknown band ลดลง ค่าความถูกต้องจะเพิ่มขึ้น ส่วนขนาดของพื้นที่ที่ถูกแก้ไขก็มีผลต่อค่าความถูกต้องกล่าวคือ ถ้าขนาดของพื้นที่ที่ถูกแก้ไขมีขนาดใหญ่ขึ้น ค่าความถูกต้องจะเพิ่มขึ้น และถ้าจำนวนเปอร์เซ็นต์ของพิกเซลที่ถูกแก้ไขในแต่ละรูปภาพย่อยที่ถูกแก้ไขจริงเพิ่มขึ้น ค่าความถูกต้องจะเพิ่มขึ้น

(e) : ค่าความผิดพลาด

ขนาดของพื้นที่ที่ถูกแก้ไข	Unknown band = 1%			Unknown band = 10%		
	b = 8	b = 16	b = 32	b = 8	b = 16	b = 32
128×160	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
64×80	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
32×40	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%

จากผลการทดลองพบว่าไม่ว่าจะกำหนดขนาดของรูปภาพย่อยหรือ unknown band เท่าใด ค่าความผิดพลาดจะเป็น 0% ส่วนขนาดของพื้นที่ที่ถูกแก้ไขไม่มีผลต่อค่าความผิดพลาด

ตารางที่ 5.3 เปรียบเทียบอัตราส่วนการตรวจสอบที่ผิดพลาดสำหรับรูปภาพที่ผ่านกระบวนการปรับค่าความสว่าง โดยกำหนดขนาดของรูปภาพย่อย (b×b) ต่างๆ

ระดับการปรับค่าความสว่าง	Unknown band = 1%			Unknown band = 10%		
	b = 8	b = 16	b = 32	b = 8	b = 16	b = 32
1. ± 5 ระดับความสว่าง	0.08%	0.00%	0.00%	0.07%	0.00%	0.00%
2. ± 10 ระดับความสว่าง	0.13%	0.01%	0.00%	0.08%	0.00%	0.00%
3. ± 20 ระดับความสว่าง	0.22%	0.19%	0.04%	0.12%	0.09%	0.00%
4. ± 30ระดับความสว่าง	0.40%	0.40%	0.19%	0.18%	0.12%	0.00%
5. ± 40 ระดับความสว่าง	0.63%	0.63%	0.31%	0.25%	0.19%	0.00%

ตารางที่ 5.4 เปรียบเทียบอัตราส่วนการตรวจสอบที่ผิดพลาดสำหรับรูปภาพที่ผ่านกระบวนการปรับค่าความแตกต่างของความสว่าง โดยกำหนดขนาดของรูปภาพย่อย (b×b) ต่างๆ

ระดับการปรับค่าความแตกต่างของความสว่าง	Unknown band = 1%			Unknown band = 10%		
	b = 8	b = 16	b = 32	b = 8	b = 16	b = 32
1. ± 5 ระดับความสว่าง	0.03%	0.00%	0.00%	0.00%	0.00%	0.00%
2. ± 10 ระดับความสว่าง	0.17%	0.09%	0.00%	0.02%	0.00%	0.00%
3. ± 20 ระดับความสว่าง	0.37%	0.34%	0.16%	0.14%	0.12%	0.00%
4. ± 30ระดับความสว่าง	1.78%	1.00%	0.52%	0.33%	0.23%	0.10%
5. ± 40 ระดับความสว่าง	2.03%	1.98%	1.94%	0.61%	0.55%	0.33%

ตารางที่ 5.5 เปรียบเทียบอัตราส่วนการตรวจสอบที่ผิดพลาดสำหรับรูปภาพที่ผ่านกระบวนการบีบอัดแบบ JPEG โดยกำหนดขนาดของรูปภาพย่อย (b×b) ต่างๆ

ระดับการบีบอัดรูปภาพแบบ JPEG	Unknown band = 1%			Unknown band = 10%		
	b = 8	b = 16	b = 32	b = 8	b = 16	b = 32
1. JPEG 60	0.06%	0.00%	0.00%	0.05%	0.00%	0.00%
2. JPEG 50	0.10%	0.00%	0.00%	0.08%	0.00%	0.00%
3. JPEG 40	0.31%	0.00%	0.00%	0.25%	0.00%	0.00%
4. JPEG 30	0.40%	0.00%	0.00%	0.30%	0.00%	0.00%
5. JPEG 20	0.86%	0.05%	0.00%	0.34%	0.02%	0.00%

ตารางที่ 5.6 เปรียบเทียบอัตราส่วนการตรวจสอบที่ผิดพลาดสำหรับรูปภาพที่มีการเพิ่มสัญญาณรบกวนแบบเกาส์เซียน โดยกำหนดขนาดของรูปภาพย่อย (b×b) ต่างๆ

ระดับสัญญาณรบกวน (SNR)	Unknown band = 1%			Unknown band = 10%		
	b = 8	b = 16	b = 32	b = 8	b = 16	b = 32
1. 75.96 dB	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
2. 72.95 dB	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
3. 65.96 dB	0.12%	0.05%	0.00%	0.01%	0.00%	0.00%
4. 62.95 dB	0.30%	0.09%	0.00%	0.13%	0.09%	0.00%
5. 55.96 dB	1.65%	0.46%	0.00%	0.28%	0.09%	0.00%

จากผลการทดลอง (ตารางที่ 5.3-5.6) พบว่าขนาดของรูปภาพย่อยหรือ unknown band มีผลต่อความสามารถในการรองรับกระบวนการแก้ไขภาพด้วยวิธีการต่างๆ คือ การปรับค่าความสว่าง การปรับค่าความแตกต่างของความสว่าง การบีบอัดรูปภาพแบบ JPEG และการเพิ่มสัญญาณรบกวน กล่าวคือ ถ้าขนาดของรูปภาพย่อยใหญ่ขึ้นหรือ unknown band สูงขึ้น ค่าความผิดพลาดจะลดลง

ตารางที่ 5.7 เปรียบเทียบความสามารถในการตรวจสอบความถูกต้องของวีดีโอด้วยวิธีการต่างๆ

ความสามารถในการตรวจสอบ	วิธีการ					
	[5]	[6]	[7]	[8]	[9]	[*]
ระบุได้ว่าส่วนใดของวีดีโอที่มีการแก้ไข	/	/	×	×	/	/
ระบุได้ว่าเฟรมใดถูกตัดหรือถูกแทรกเข้ามา	/	/	×	/	/	/
ตรวจพบว่าวีดีโอมีการแก้ไขเมื่อวีดีโอมีการเปลี่ยนแปลงระดับความเข้มของแสงสว่างเฉพาะบางส่วนของเฟรม	/	×	/	×	/	/
ตรวจพบว่าวีดีโอที่นำมาตรวจสอบเป็นวีดีโอต้นฉบับหรือวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ	×	×	×	×	×	/
ระบุความแตกต่างของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ	×	×	×	×	×	/

หมายเหตุ : * คือ วิธีการที่นำเสนอในงานวิจัยนี้

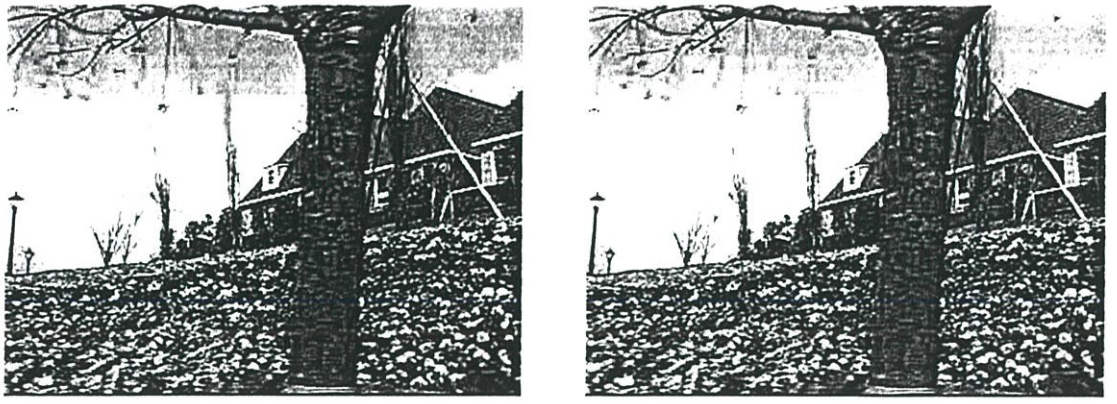
5.4 ตัวอย่างของภาพที่ผ่านกระบวนการแก้ไขภาพด้วยวิธีการต่างๆ

5.4.1 การปรับค่าความสว่าง (Brightness adjustment)

การแก้ไขความสว่างของภาพโดยการเพิ่มค่าความสว่างที่จะทำให้ผลลัพธ์ที่ได้จากการตรวจสอบด้วยวิธีการที่นำเสนอนี้ไม่มีและมีข้อผิดพลาดเกิดขึ้นเมื่อกำหนดให้รูปภาพย่อยมีขนาด 16×16 พิกเซล และ unknown band = 1% สามารถแสดงได้ดังรูปที่ 5.8 (a) และ 5.8 (b) ตามลำดับ ส่วนการลดค่าความสว่างที่จะทำให้ผลลัพธ์ไม่มีและมีข้อผิดพลาดเกิดขึ้นสามารถแสดงได้ดังรูปที่ 5.9 (a) และ 5.9 (b) ตามลำดับ

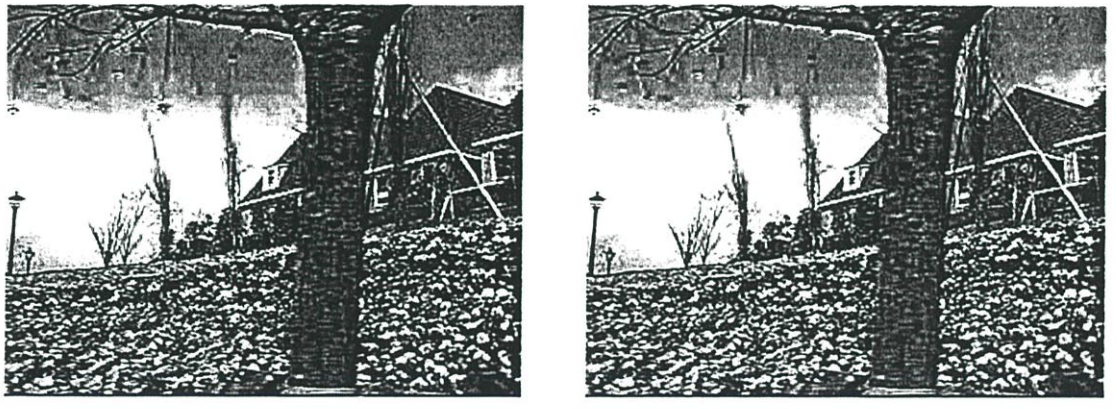
5.4.2 การปรับค่าความแตกต่างของความสว่าง (Contrast adjustment)

การแก้ไขความแตกต่างของความสว่างของภาพโดยการเพิ่มค่าความแตกต่างของความสว่างที่จะทำให้ผลลัพธ์ที่ได้จากการตรวจสอบด้วยวิธีการที่นำเสนอนี้ไม่มีและมีข้อผิดพลาดเกิดขึ้นสามารถแสดงได้ดังรูปที่ 5.10 (a) และ 5.10 (b) ตามลำดับ ส่วนการลดค่าความแตกต่างของความสว่างที่จะทำให้ผลลัพธ์ไม่มีและมีข้อผิดพลาดเกิดขึ้นสามารถแสดงได้ดังรูปที่ 5.11 (a) และ 5.11 (b) ตามลำดับ



(a) (b)

รูปที่ 5.8 (a) การเพิ่มค่าความสว่างแล้วผลการตรวจสอบไม่มีข้อผิดพลาดเกิดขึ้น
(b) การเพิ่มค่าความสว่างแล้วผลการตรวจสอบมีข้อผิดพลาดเกิดขึ้น

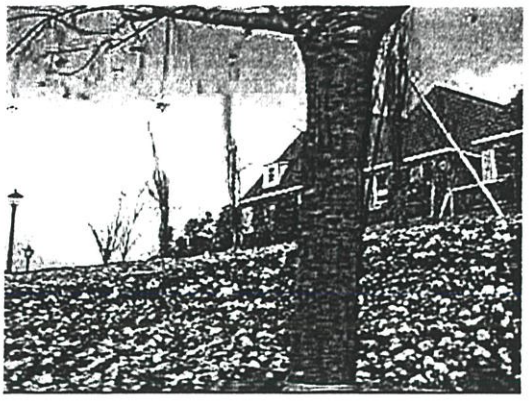


(a) (b)

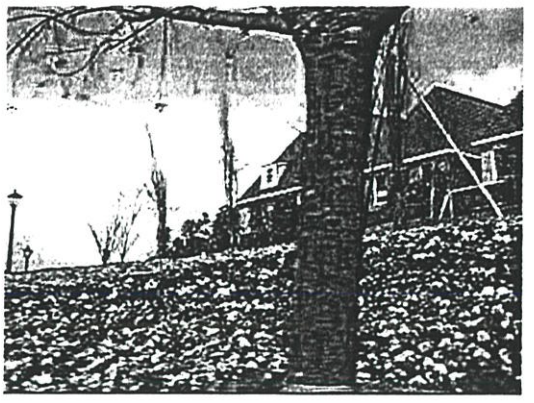
รูปที่ 5.9 (a) การลดค่าความสว่างแล้วผลการตรวจสอบไม่มีข้อผิดพลาดเกิดขึ้น
(b) การลดค่าความสว่างแล้วผลการตรวจสอบมีข้อผิดพลาดเกิดขึ้น

(a) (b)

รูปที่ 5.10 (a) การเพิ่มค่าความแตกต่างของความสว่างแล้วผลการตรวจสอบไม่มีข้อผิดพลาดเกิดขึ้น
(b) การเพิ่มค่าความแตกต่างของความสว่างแล้วผลการตรวจสอบมีข้อผิดพลาดเกิดขึ้น



(a)

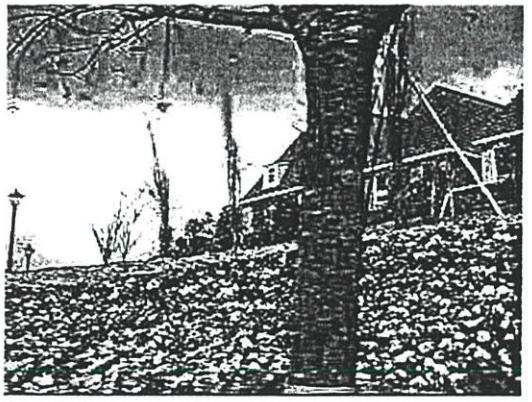


(b)

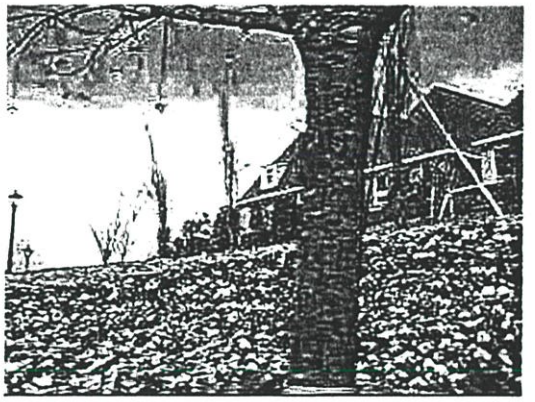
รูปที่ 5.11 (a) การลดค่าความแตกต่างของความสว่างแล้วผลการตรวจสอบไม่มีข้อผิดพลาดเกิดขึ้น
(b) การลดค่าความแตกต่างของความสว่างแล้วผลการตรวจสอบมีข้อผิดพลาดเกิดขึ้น

5.4.3 การบีบอัดแบบ JPEG (JPEG Compression)

การบันทึกภาพเป็นไฟล์ประเภท JPEG ที่จะทำให้ผลลัพธ์ที่ได้จากการตรวจสอบด้วยวิธีการที่นำเสนอนี้ไม่มีและมีข้อผิดพลาดเกิดขึ้นสามารถแสดงได้ดังรูปที่ 5.12 (a) และ 5.12 (b) ตามลำดับ



(a)



(b)

รูปที่ 5.12 (a) การบีบอัดแบบ JPEG แล้วผลการตรวจสอบไม่มีข้อผิดพลาดเกิดขึ้น
(b) การบีบอัดแบบ JPEG แล้วผลการตรวจสอบมีข้อผิดพลาดเกิดขึ้น

5.4.4 การเพิ่มสัญญาณรบกวน (Noise adding)

การเพิ่มสัญญาณรบกวนแบบสุ่มเทียมที่มีการแจกแจงแบบเกาส์เซียน (Gaussian) ที่จะทำให้ผลลัพธ์ที่ได้จากการตรวจสอบด้วยวิธีการที่นำเสนอนี้ไม่มีและมีข้อผิดพลาดเกิดขึ้นสามารถแสดงได้ดังรูปที่ 5.13 (a) และ 5.13 (b) ตามลำดับ

(a) (b)

รูปที่ 5.13 (a) การเพิ่มสัญญาณรบกวนแล้วผลการตรวจสอบไม่มีข้อผิดพลาดเกิดขึ้น
(b) การเพิ่มสัญญาณรบกวนแล้วผลการตรวจสอบมีข้อผิดพลาดเกิดขึ้น

บทที่ 6
สรุปผลการวิจัยและข้อเสนอแนะ

เนื่องจากเทคโนโลยีคอมพิวเตอร์และสื่อประสมมีการพัฒนาไปมาก การแก้ไขตัดต่อวีดีโอโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ หรือผู้ที่ประสงค์ร้ายสามารถทำได้ง่ายขึ้น ทำให้ในปัจจุบันนี้ได้มีความพยายามในการพัฒนาวิธีการตรวจสอบความถูกต้องของวีดีโอ ซึ่งสามารถแบ่งวิธีการต่างๆ ออกเป็น 2 ประเภท คือ เทคนิคของลายเซ็นดิจิตอล และเทคนิคของลายน้ำดิจิตอล

งานวิจัยนี้ได้นำเสนอวิธีการสร้างลายเซ็นดิจิตอลสำหรับวีดีโอต้นฉบับและวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ โดยใช้หลักการของ Incremental-based digital signature เพื่อให้สามารถตรวจสอบความถูกต้องของวีดีโอที่ถูกแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ โดยลายเซ็นดิจิตอลจะสร้างขึ้นสำหรับแต่ละเฟรมของวีดีโอ ซึ่งมีวิธีการดังต่อไปนี้

1. คำนวณหาค่า feature code สำหรับเฟรม I หรือ differential feature code สำหรับเฟรม P,B และเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับใดๆ
2. เข้ารหัส feature code ของเฟรม I หรือ differential feature code ของเฟรม P,B และเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับใดๆ ซึ่งก่อนการเข้ารหัสเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับใดๆ นั้นจะต้องนำ differential feature code ที่ได้ไปเรียงต่อกับลายเซ็นดิจิตอลของเฟรมที่มีการแก้ไขโดยผู้มีกรรมสิทธิ์ในการทำสำเนาลำดับก่อนหน้า
3. แนบลายเซ็นดิจิตอลของแต่ละเฟรมเข้าไปในเฮดเดอร์ของเฟรมนั้นๆ

6.1 สรุปผลการวิจัย

การตรวจสอบความถูกต้องของวีดีโอที่มีการบีบอัดแบบ MPEG-1 โดยใช้ลายเซ็นดิจิตอลแบบสมทบส่วนต่างที่ได้นำเสนอนี้ เมื่อทำการทดลองแล้วผลการทดลองเป็นที่ยอมรับได้ตามเป้าหมายที่วางไว้ กล่าวคือสามารถบอกได้ว่าวีดีโอที่นำมาตรวจสอบมีการแก้ไขโดยผู้ที่ประสงค์ร้ายหรือไม่ และถ้ามีการแก้ไขโดยผู้ที่ประสงค์ร้ายก็สามารถระบุได้ว่าเกิดการแก้ไขที่ส่วนใดของวีดีโอเมื่อเปรียบเทียบกับวีดีโอต้นฉบับหรือวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ นอกจากนี้ยังสามารถตรวจสอบได้ว่าวีดีโอที่นำมาตรวจสอบเป็นวีดีโอต้นฉบับหรือวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนา และสามารถระบุถึงความแตกต่างของวีดีโอที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ ได้ โดยขนาดของรูปภาพย่อยที่ใช้คำนวณค่า feature code จะมีผลต่อการตรวจสอบความถูกต้อง ซึ่งถ้าขนาดของรูปภาพย่อยใหญ่ขึ้นจะทำให้

ความแม่นยำและข้อผิดพลาดในการตรวจสอบลดลง แต่ความถูกต้องจะเพิ่มขึ้น ปัจจัยที่มีผลต่อการตรวจสอบนั้นได้แก่ความทนทานต่อการแก้ไขเปลี่ยนแปลงรูปภาพด้วยวิธีการต่างๆ คือ การปรับความสว่างของรูปภาพ การปรับความแตกต่างของความสว่างของรูปภาพ การบีบอัดรูปภาพ และการเพิ่มสัญญาณรบกวน โดยวิธีการนี้สามารถรองรับกระบวนการเปลี่ยนแปลงต่างๆ ได้ ซึ่งถ้ากำหนดให้มี unknown band มาก ก็จะมีความคงทนต่อกระบวนการเปลี่ยนแปลงต่างๆ ได้ดีกว่าการกำหนดให้มี unknown band น้อย และการใช้ differential feature code ในเฟรม P,B และเฟรมที่มีการแก้ไขโดยผู้ที่มีกรรมสิทธิ์ในการทำสำเนาลำดับต่างๆ จะทำให้จำนวนบิตที่ใช้สร้างลายเซ็นดิจิตอลลดลง

6.2 ข้อเสนอแนะสำหรับการพัฒนาในอนาคต

จากผลการทดลอง พบว่าวิธีการที่ได้พัฒนานี้มีข้อจำกัดบางประการ และมีจุดที่ควรปรับปรุงให้มีประสิทธิภาพมากขึ้นต่อไปอีกดังนี้

1. รูปภาพย่อยที่ใช้ในการสร้าง feature code มีขนาดตายตัวเท่ากันหมดทั้งเฟรม ซึ่งอาจไม่เหมาะสมเมื่อนำไปใช้กับเฟรมที่มีรายละเอียดสูง ซึ่งบางบริเวณของเฟรมอาจจะมีรายละเอียดที่เล็กหรือใหญ่ไม่เท่ากัน อาจจะต้องมีการปรับขนาดของรูปภาพย่อยให้แปรผันกับเนื้อหาของเฟรม ซึ่งเฟรมหนึ่งๆ สามารถแบ่งรูปภาพย่อยให้มีขนาดต่างๆ ได้ เพื่อให้สามารถตรวจสอบรายละเอียดของเฟรมได้ยืดหยุ่นมากขึ้น
2. การแทนค่า feature code ด้วยเลขฐานสองขนาด 2 บิต ทำให้ความละเอียดในการตรวจสอบน้อย และจำนวนบิตของ differential feature code ก็ลดลงไม่มากนัก อาจจะต้องมีการแทนค่า feature code ด้วยจำนวนบิตที่มากขึ้น
3. ควรมีการพัฒนาขั้นตอนการตรวจสอบความถูกต้องของวีดีโอ ที่ทำให้ผู้ใช้สามารถพิจารณาและตัดสินได้ว่าวีดีโอถูกแก้ไขไปมากน้อยในระดับใดได้ง่ายและชัดเจนยิ่งขึ้น อาจมีการสร้างแบบจำลองหรือสมการในการวัดค่าความเปลี่ยนแปลงของวีดีโอออกมาเป็นตัวเลขเป็นค่ามาตรฐานใช้ในการเปรียบเทียบกับวีดีโอต่างๆ ได้
4. การแนบลายเซ็นดิจิตอลเข้าไปในเฮดเดอร์ของเฟรมอาจถูกทำลายหรือสูญหายเมื่อมีการเปลี่ยนแปลงฟอร์แมตของวีดีโอหรือมีการแก้ไขวีดีโอ ซึ่งในปัจจุบันยังไม่มีวิธีการแก้ไขที่ดี ดังนั้นคงต้องรอให้มีมาตรฐานทั่วไปที่จะทำให้ลายเซ็นดิจิตอลคงอยู่แม้ว่าจะมีการเปลี่ยนแปลงฟอร์แมตของวีดีโอหรือมีการแก้ไขวีดีโอก็ตาม
5. วีดีโอและรูปภาพที่นำมาทดลองวัดประสิทธิภาพของวิธีการตรวจสอบความถูกต้องมีจำนวนไม่มากนัก อาจจะต้องมีการทดลองกับวีดีโอและรูปภาพจำนวนมากขึ้น เพื่อให้ได้ผลการทดลองที่ถูกต้องและครอบคลุมรูปภาพในลักษณะอื่นๆ ได้

เอกสารอ้างอิง

[1] Peter D. Symes. Video Compression : Fundamental Compression Techniques and an Overview of the JPEG and MPEG Compression Systems. Mc Graw – Hill. 1998.

[2] Ming-Ting Sun and Amy R. Reibman. Compressed Video over Networks. Marcel Dekker,Inc. 2001.

[3] Ingemar J. Cox. et. al. Digital Watermarking. Morgan Kaufmann. 2002.

[4] James F. Kurose and Keith W. Ross. Computer Networking : A Top-Down Approach Featuring the Internet. Addison Westley Longman. 2001.

[5] Ching-Yung Lin. "Watermarking and Digital Signature Techniques for Multimedia Authentication and Copyright Protection." Doctor of Philosophy in the Graduate School of Arts and Science, Columbia University. 2000.

[6] Jana Dittmann. et. al. "Content-based Digital Signature for Motion Pictures Authentication and Content-Fragile Watermark." IEEE International Conference on Multimedia Computing and Systems., vol.2, 1999. pp.209-213.

[7] Marc Schneider and Shih-Fu Chang. "A Robust Content Based Digital Signature For Image Authentication." International Conference on Image Processing., vol.3, 1996. pp.227-230.

[8] Bijan G. Mobassseri. et. al. "Content Authentication and Tamper detection in Digital Video." International Conference on Image Processing., vol.1, 2000. pp.458-461.

[9] Min Wu and Bede Liu. "Watermarking For Image Authentication." International Conference on Image Processing., vol.2, 1998. pp.437-441.

[10] Celik, M. et. Al. "Hierarchical Watermaking for Secure Image Authentication With Localization." IEEE Transaction on Image Processing., vol.11, 2002. pp.585-595.

[11] Sangiamkun, W. and Chotikakamthorn, N. "Digital watermarking technique for image authentication by neighbouring block similarity measure." IEEE Region 10 International Conference on Electrical and Electronic Technology., vol.2, 2001. pp.743-747.

[12] Bellare, M. et. al. "Incremental Cryptography:The Case of Hashing and Signing." Crypto'94, Lecture Note in Computer Science., vol.839, 1994. pp.216-233.

[13] Fischlin, M. "Lower Bounds for the Signature Size of Incremental Schemes." In 38th Annual Symposium on Foundations of Computer Science., 1997. pp.438-447.

[14] Rafael C. Gonzalez And Richard E. Woods. Digital Image Processing. Addison Wesley Longman. 1997.

[15] Gregory K. Wallace. "The JPEG Still Picture Compression Standard." IEEE Transactions on Consumer Electronics., vol.38, 1992.

[16] Bender, W. et. al. "Techniques for Data Hiding." IBM System Journal., vol.35, 1996. pp.313-336.

[17] Ingemar J. Cox. et. al. "Secure Spread Spectrum Watermarking for Multimedia." IEEE Transactions on Image Processing., vol.6, 1997. pp.1673-1678.

[18] Maria Paula Queluz. "Towards Robust, Content Based Techniques for Image Authentication." IEEE Second Workshop on Multimedia Signal Processing., 1998. pp.297-302.

[19] Jiri Fridrich. "Image Watermarking for Tamper Detection." International Conference on Image Processing., vol.2, 1998. pp.404-408.

[20] Chiou-Tung Hzu and Ja-Ling Wu. "Digital watermarking for video." International Conference on Digital Signal Processing., vol.1, 1997. pp.217-220.

[21] Min Wu and Hong Heather Yu. "Video Access Control Via Multi-level Data Hiding" IEEE International Conference on Multimedia & Expo 2000., vol.1, 2000. pp.381-384.

[22] Chiou-Ting Hsu and Ja-Ling Wu. "DCT-Based Watermarking for Video" IEEE Transactions on Consumer Electronics., vol.44, 1998. pp.206-216.

[23] Liu Tong and Qiu Zheng-ding. "The Survey of Digital Watermarking-based Image Authentication Techniques." International Conference on Signal Processing., vol.2, 2002. pp. 1556-1559.

ภาคผนวก

ภาคผนวก ก.

อภิธานศัพท์

ตัวแปร	ความหมาย
M×N	ขนาดของรูปภาพหรือเฟรมของวีดีโอ
n	ลำดับชั้นของสำเนาวีดีโอ
c	ชนิดของเฟรม
b×b	ขนาดของรูปภาพย่อย
$g(x, y)$	ระดับความเข้มของแสงสว่างของรูปภาพหรือเฟรมของวีดีโอ
$g_{i,j}(x_1, y_1)$	ระดับความเข้มของแสงสว่างของรูปภาพย่อยตำแหน่งที่ i,j
$g_{u,v}(x_2, y_2)$	ระดับความเข้มของแสงสว่างของรูปภาพย่อยตำแหน่งที่ u,v เมื่อมีการเพิ่มหรือลดขนาดของรูปภาพย่อย
$DC_{n,c,i,j}$	DC coefficient ของรูปภาพย่อยตำแหน่งที่ i,j ของเฟรม c และของสำเนาวีดีโอลำดับที่ n
$f^{(r)}_{n,c,i,j}$	feature code ที่มีค่าเป็นจำนวนจริงของรูปภาพย่อยตำแหน่งที่ i,j โดยได้จากการเปรียบเทียบกับรูปภาพย่อยที่อยู่ติดกันทางด้านขวา (i,j+1)
$f^{(b)}_{n,c,i,j}$	feature code ที่มีค่าเป็นจำนวนจริงของรูปภาพย่อยตำแหน่งที่ i,j โดยได้จากการเปรียบเทียบกับรูปภาพย่อยที่อยู่ติดกันทางด้านล่าง (i+1,j)
$f^{(z)}_{n,c,i,j}$	feature code ที่มีค่าเป็นจำนวนจริงของรูปภาพย่อยตำแหน่งที่ i,j ($f^{(r)}_{n,c,i,j}$ หรือ $f^{(b)}_{n,c,i,j}$), $z \in \{ r,b\}$
$f^{*(r)}_{n,c,i,j}$	feature code ที่มีค่าเป็นจำนวนเต็มของรูปภาพย่อยตำแหน่งที่ i,j โดยได้จากการเปรียบเทียบกับรูปภาพย่อยที่อยู่ติดกันทางด้านขวา (i,j+1)
$f^{*(b)}_{n,c,i,j}$	feature code ที่มีค่าเป็นจำนวนเต็มของรูปภาพย่อยตำแหน่งที่ i,j โดยได้จากการเปรียบเทียบกับรูปภาพย่อยที่อยู่ติดกันทางด้านล่าง (i+1,j)
$f^{*(z)}_{n,c,i,j}$	feature code ที่มีค่าเป็นจำนวนเต็มของรูปภาพย่อยตำแหน่งที่ i,j ($f^{*(r)}_{n,c,i,j}$ หรือ $f^{*(b)}_{n,c,i,j}$), $z \in \{ r,b\}$
$f^{*}_{n,c}$	feature code ที่มีค่าเป็นจำนวนเต็มของเฟรม c ของสำเนาวีดีโอลำดับที่ n
$f'^{(r)}_{n,c,i,j}$	differential feature code ของรูปภาพย่อยตำแหน่งที่ i,j (feature code ได้จากการเปรียบเทียบกับรูปภาพย่อยที่อยู่ติดกันทางด้านขวา (i,j+1))

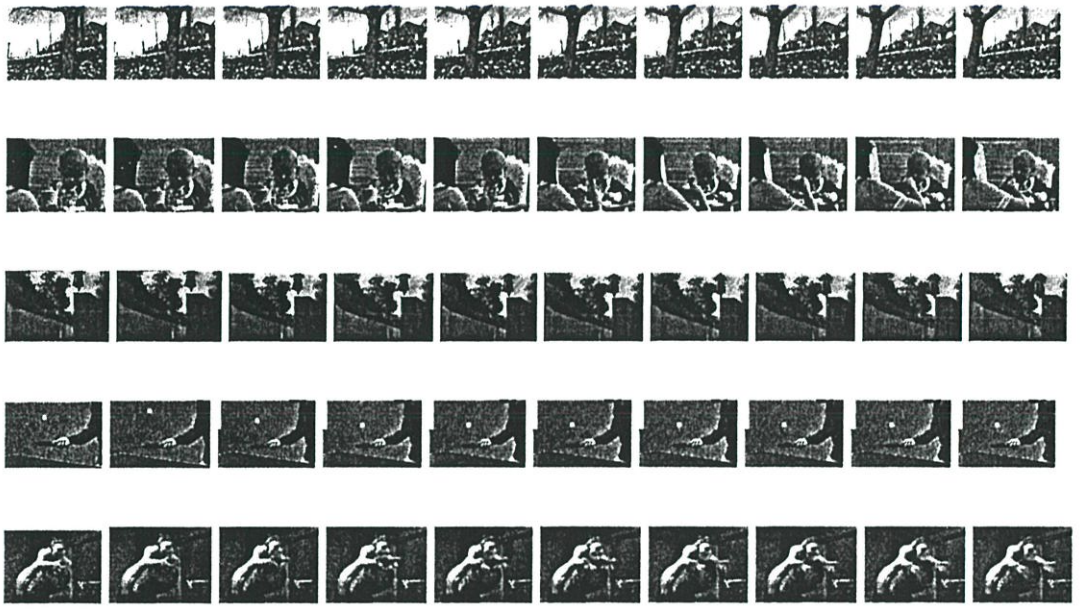
ตัวแปร	ความหมาย
$f'^{(b)}_{n,c,i,j}$	differential feature code ของรูปภาพย่อยตำแหน่งที่ i,j (feature code ได้จากการเปรียบเทียบกับรูปภาพย่อยที่อยู่ติดกันทางด้านล่าง (i+1,j))
$f'^{(z)}_{n,c,i,j}$	differential feature code ของรูปภาพย่อยตำแหน่งที่ i,j ($f'^{(r)}_{n,c,i,j}$ หรือ $f'^{(b)}_{n,c,i,j}$)
$f'_{n,c}$	differential feature code ของเฟรม c ของสำเนาวีดีโอลำดับที่ n
$d_{n,c}$	ข้อมูลที่ใช้สร้างลายเซ็นดิจิตอลของเฟรม c ของสำเนาวีดีโอลำดับที่ n
$S_{n,c}$	ลายเซ็นดิจิตอลของเฟรม c ของสำเนาวีดีโอลำดับที่ n
$\overleftarrow{f}^{(r)}_{n,c,u,v}$	feature code ที่มีค่าเป็นจำนวนจริงของรูปภาพย่อยตำแหน่งที่ u,v โดยได้จากการเปรียบเทียบกับรูปภาพย่อยที่อยู่ติดกันทางด้านขวา (u,v+1) เมื่อมีการลดขนาดของรูปภาพย่อย
$\overleftarrow{f}^{(b)}_{n,c,u,v}$	feature code ที่มีค่าเป็นจำนวนจริงของรูปภาพย่อยตำแหน่งที่ u,v โดยได้จากการเปรียบเทียบกับรูปภาพย่อยที่อยู่ติดกันทางด้านล่าง (u+1,v) เมื่อมีการลดขนาดของรูปภาพย่อย
$\overleftarrow{f}^{(z)}_{n,c,u,v}$	feature code ที่มีค่าเป็นจำนวนจริงของรูปภาพย่อยตำแหน่งที่ u,v เมื่อมีการลดขนาดของรูปภาพย่อย ($\overleftarrow{f}^{(r)}_{n,c,u,v}$ หรือ $\overleftarrow{f}^{(b)}_{n,c,u,v}$), $z \in \{ r,b\}$
$\overleftarrow{f}^{*(r)}_{n,c,u,v}$	feature code ที่มีค่าเป็นจำนวนเต็มของรูปภาพย่อยตำแหน่งที่ u,v โดยได้จากการเปรียบเทียบกับรูปภาพย่อยที่อยู่ติดกันทางด้านขวา (u,v+1) เมื่อมีการลดขนาดของรูปภาพย่อย
$\overleftarrow{f}^{*(b)}_{n,c,u,v}$	feature code ที่มีค่าเป็นจำนวนเต็มของรูปภาพย่อยตำแหน่งที่ u,v โดยได้จากการเปรียบเทียบกับรูปภาพย่อยที่อยู่ติดกันทางด้านล่าง (u+1,v) เมื่อมีการลดขนาดของรูปภาพย่อย
$\overleftarrow{f}^{*(z)}_{n,c,u,v}$	feature code ที่มีค่าเป็นจำนวนเต็มของรูปภาพย่อยตำแหน่งที่ u,v เมื่อมีการลดขนาดของรูปภาพย่อย ($\overleftarrow{f}^{*(r)}_{n,c,u,v}$ หรือ $\overleftarrow{f}^{*(b)}_{n,c,u,v}$), $z \in \{ r,b\}$
$\overleftarrow{f}^{*}_{n,c}$	feature code ที่มีค่าเป็นจำนวนเต็มของเฟรม c ของสำเนาวีดีโอลำดับที่ n เมื่อมีการลดขนาดของรูปภาพย่อย
$\overleftarrow{f}'_{n,c}$	differential feature code ของเฟรม c ของสำเนาวีดีโอลำดับที่ n เมื่อมีการลดขนาดของรูปภาพย่อย
$\overrightarrow{f}^{(r)}_{n,c,u,v}$	feature code ที่มีค่าเป็นจำนวนจริงของรูปภาพย่อยตำแหน่งที่ u,v โดยได้จากการเปรียบเทียบกับรูปภาพย่อยที่อยู่ติดกันทางด้านขวา (u,v+1) เมื่อมีการเพิ่มขนาดของรูปภาพย่อย

ตัวแปร	ความหมาย
$\vec{f}^{(b)}_{n,c,u,v}$	feature code ที่มีค่าเป็นจำนวนจริงของรูปภาพย่อยตำแหน่งที่ u,v โดยได้จากการเปรียบเทียบกับรูปภาพย่อยที่อยู่ติดกันทางด้านล่าง (u+1,v) เมื่อมีการเพิ่มขนาดของรูปภาพย่อย
$\vec{f}^{(z)}_{n,c,u,v}$	feature code ที่มีค่าเป็นจำนวนจริงของรูปภาพย่อยตำแหน่งที่ u,v เมื่อมีการเพิ่มขนาดของรูปภาพย่อย ($\vec{f}^{(r)}_{n,c,u,v}$ หรือ $\vec{f}^{(b)}_{n,c,u,v}$), $z \in \{ r,b\}$
$\vec{f}^{*(r)}_{n,c,u,v}$	feature code ที่มีค่าเป็นจำนวนเต็มของรูปภาพย่อยตำแหน่งที่ u,v โดยได้จากการเปรียบเทียบกับรูปภาพย่อยที่อยู่ติดกันทางด้านขวา (u,v+1) เมื่อมีการเพิ่มขนาดของรูปภาพย่อย
$\vec{f}^{*(b)}_{n,c,u,v}$	feature code ที่มีค่าเป็นจำนวนเต็มของรูปภาพย่อยตำแหน่งที่ u,v โดยได้จากการเปรียบเทียบกับรูปภาพย่อยที่อยู่ติดกันทางด้านล่าง (u+1,v) เมื่อมีการเพิ่มขนาดของรูปภาพย่อย
$\vec{f}^{*(z)}_{n,c,u,v}$	feature code ที่มีค่าเป็นจำนวนเต็มของรูปภาพย่อยตำแหน่งที่ u,v เมื่อมีการเพิ่มขนาดของรูปภาพย่อย ($\vec{f}^{*(r)}_{n,c,u,v}$ หรือ $\vec{f}^{*(b)}_{n,c,u,v}$), $z \in \{ r,b\}$
$\vec{f}^{*}_{n,c}$	feature code ที่มีค่าเป็นจำนวนเต็มของเฟรม c ของสำเนาวีดีโอลำดับที่ n เมื่อมีการเพิ่มขนาดของรูปภาพย่อย
$\vec{f}'_{n,c}$	differential feature code ของเฟรม c ของสำเนาวีดีโอลำดับที่ n เมื่อมีการเพิ่มขนาดของรูปภาพย่อย
$\tilde{f}^{*(r)}_{i,j}$	feature code ที่มีค่าเป็นจำนวนเต็มของรูปภาพย่อยตำแหน่งที่ i,j ของเฟรมวีดีโอที่นำมาตรวจสอบ โดยได้จากการเปรียบเทียบกับรูปภาพย่อยที่อยู่ติดกันทางด้านขวา (i,j+1)
$\tilde{f}^{*(b)}_{i,j}$	feature code ที่มีค่าเป็นจำนวนเต็มของรูปภาพย่อยตำแหน่งที่ i,j ของเฟรมวีดีโอที่นำมาตรวจสอบ โดยได้จากการเปรียบเทียบกับรูปภาพย่อยที่อยู่ติดกันทางด้านล่าง (i+1,j)
$A_{i,j}$	ตัวบ่งชี้ว่ารูปภาพย่อยตำแหน่งที่ i,j ถูกตรวจพบว่ามีการแก้ไขหรือไม่
$B_{i,j}$	ตัวบ่งชี้ว่ารูปภาพย่อยตำแหน่งที่ i,j มีการแก้ไขจริงหรือไม่
$p_{x,y}$	ตัวบ่งชี้ว่าพิกเซลตำแหน่งที่ x,y ถูกตรวจพบว่ามีการแก้ไขหรือไม่
$q_{x,y}$	ตัวบ่งชี้ว่าพิกเซลตำแหน่งที่ x,y มีการแก้ไขจริงหรือไม่

ภาคผนวก ข.

วีดีโอและรูปภาพที่ใช้ในการทดลอง

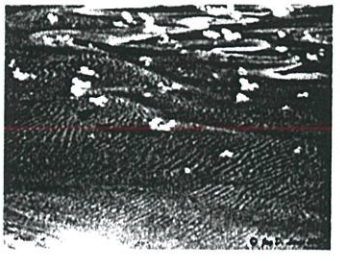
1. วีดีโอ



2. รูปภาพ

2.1 รูปภาพที่มีความละเอียดและค่าความแตกต่างของความสว่างปานกลาง

2.2 รูปภาพที่มีความละเอียดและค่าความแตกต่างของความสว่างต่ำ



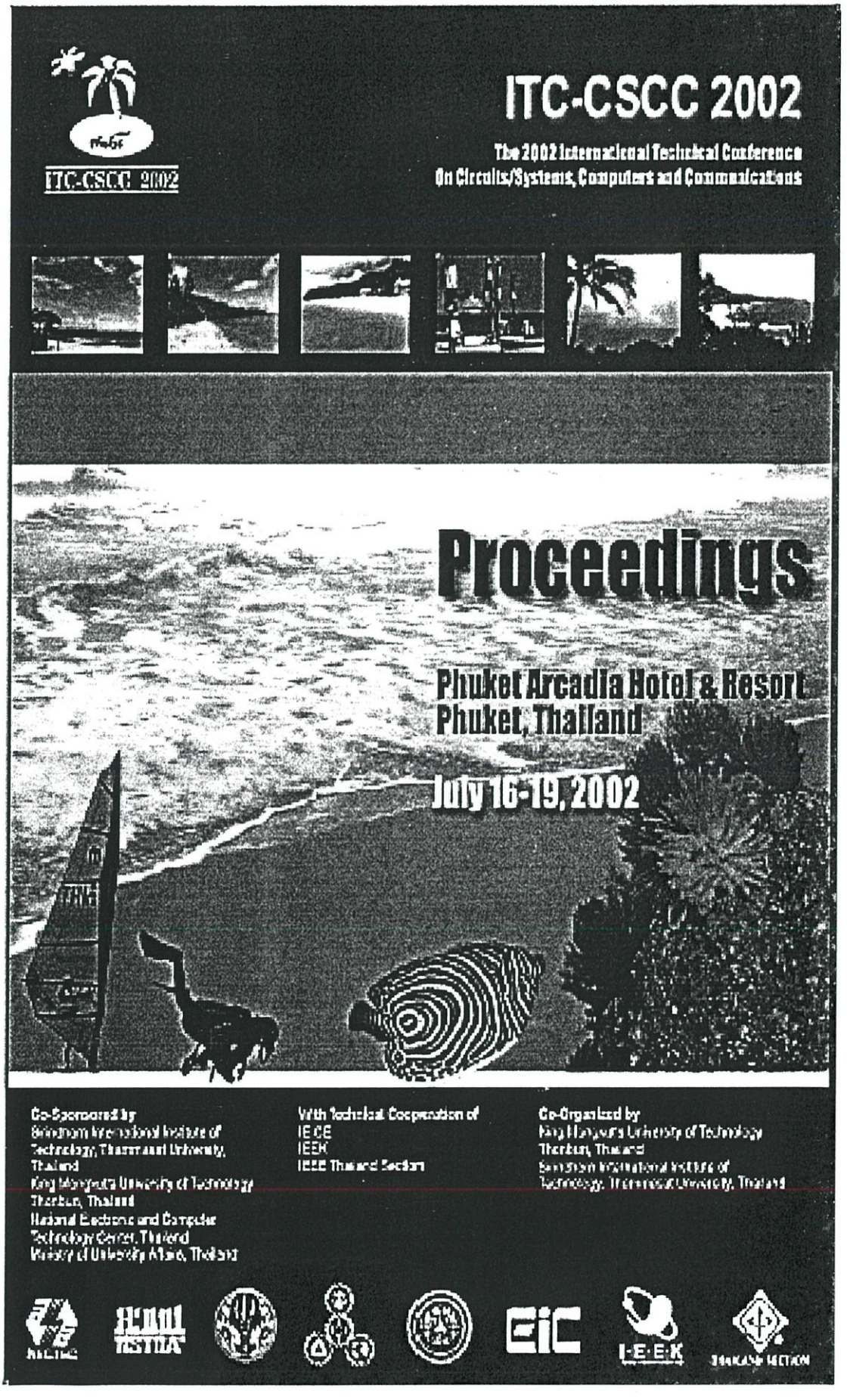
2.3 รูปภาพที่มีความละเอียดต่ำแต่ค่าความแตกต่างของความสว่างสูง

2.4 รูปภาพที่มีความละเอียดสูงแต่ค่าความความแตกต่างของความสว่างต่ำ

2.5 รูปภาพที่มีความละเอียดและค่าความแตกต่างของความสว่างสูง

ภาคผนวก ค.
บทความและผลงานวิจัยที่ได้รับการตีพิมพ์

1. Wilaiporn Kultangwattana and Nopporn Chotikakamthorn. "Incremental-based Digital Signature with Neighbouring Block Similarity Measure for Video Authentication" The 2002 International Technical Conference On Circuits/System, Computers and Communications (ITC-CSCC 2002). pp.1412-1415.


ITC-CSCC 2002
ITC-CSCC 2002
The 2002 International Technical Conference
On Circuits/Systems, Computers and Communications
Proceedings
Phuket Arcadia Hotel & Resort
Phuket, Thailand
July 16-19, 2002
Co-Sponsored by
Sirindhorn International Institute of
Technology, Thammasat University,
Thailand
King Mongkut's University of Technology
Thonburi, Thailand
National Electronic and Computer
Technology Center, Thailand
Ministry of University Affairs, Thailand
With Technical Cooperation of
IECE
IEEK
IEEE Thailand Section
Co-Organized by
King Mongkut's University of Technology
Thonburi, Thailand
Sirindhorn International Institute of
Technology, Thammasat University, Thailand
EIC
I·E·E·K

Incremental-based Digital Signature with Neighbouring Block Similarity Measure for Video Authentication

Wilaiporn Kultangwattana and Nopporn Chotikakamthorn
Faculty of Information Technology &
Research Center for Communications and Information Technology,
King Mongkut's Institute of Technology Ladkrabang.
Chalongkrung Road, Bangkok 10520, Thailand
Tel.: +66-2-326-8020, Fax.: +66-2-326-9074
e-mail: wilaiporn17@yahoo.com, nopporn@it.kmitl.ac.th

Abstract: This paper describes a digital signature-based method for original and updated video authentication. The method uses multiple digital signatures in dealing with video data undergoing multiple change/updating. In addition, a feature based on neighbouring block similarity measure is applied to deal with certain image/video modification. The proposed method can cope with wide range of image/video tampering. It is suitable for practical use of video data, where updating may be performed by more than one legal parties. Experimental results are included with concluding remarks.

1. Introduction

Recently, the problem of video authentication has been addressed. There are two approaches which have been suggested for achieving the task of authenticating digital video. The first one is based on the use of a digital signature technique, and the second one is based on digital watermarking techniques. A digital signature method as proposed by Ching-Yung Lin [2] can detect and localize alterations of the original video. Difference between DCT coefficients of the first image-block group and those of the second group is computed to construct a feature. Another method was proposed by Jana Dittmann [3]. The method uses edge-based feature code for digital signature so it can not detect color alterations. Another work includes that of Marc Schneider[4], which proposed a hashing method for video data. Digital watermarking method proposed by Bijan G. Mobasseri [1] has a watermark inserted into each frame of video, to detect unauthorized cut-and-splice or cut-insert-splice. Min wu [5] proposed an insertion of a watermark in a frequency domain of an I-frame.

This paper deals with the digital signature-based approach, due to the lack of enough embedding capacity when the watermarking approach is applied. The proposed method uses a feature based on similarity measure between two adjacent blocks of image. In addition, by applying the concept of incremental-based digital signature, video data undergoing multiple updating from more than on legitimated owners, can be authenticated in a hierachical manner. The paper is organized as follows. First, a general framework of authenticating digital video is described. In Section 2 Section 3 describes the proposed incremental-based digital signature for video authentication. In Section 4, some experimental results of image authentication are given. Discussion and concluding remarks are provided in Section 5.

2. Digital Signature for Video Authentication

Just as with human signatures, digital signing should be done in such a way that a signature is verifiable, non-forgible, and non-repudiable. In a processing of generating a digital signature, a private key is used to encrypt a message (or the feature or hashed data corresponding to the original image). This encrypted message is called a "digital signature". The authentication process of this message needs the public key associated with the private key used to generate a signature, to decrypt the digital signature. The message to be authenticated is then compared with the decrypted digital signature. If they are identical, then the received message is authentic.

Given the overheads of encryption and decryption, signing and verifying data can be overkill. Using a message digest, computational complexity can be greatly reduced due to data size reduction. For image and video data authentication, however, use of a hashing function is not suitable. Because, with a slight change in image data due, for example, to compression, the image/video may be regarded as invalid. A general process of digital signature method for image/video authentication, such as that described in [2] is shown in Figure 1.

When a user needs to authenticate the image or video received, a signature needs to be decrpyted and compares with the corresponding feature value extracted from the test image. If the two data sets match (or closely match), the image is said to be "authentic". The authentication process is shown in Figure 2.

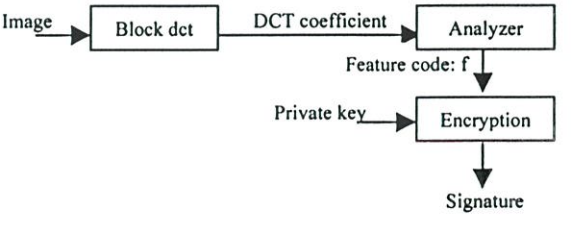


Figure 1. Digital Signature Generation

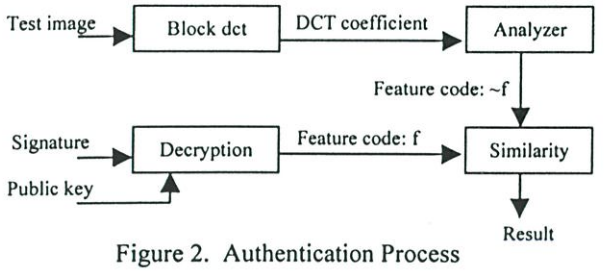


Figure 2. Authentication Process

3. Incremental-based Digital Signature for Video Authentication

The method described here is based on the digital signature approach, as detailed in [2]. However, unlike the method in [2], similarity between each block to the adjacent one on the right, and to another block below, is used (see. Figure 3). In addition, we introduce the concept of incremental-based digital signature. The method was inspired by [6, 7], but its main principle bears no relationship with [6, 7]. In this scheme, for the video I-frame, digital signature is generated from an extracted feature with complementary information (which includes information regarding to day, month, year, hour, minute, second, frame number, and frame rate). For the video P-frame and B-frame, digital signature is generated from the feature obtained as the difference between the feature corresponding to the nearest I-frame and P-frame.

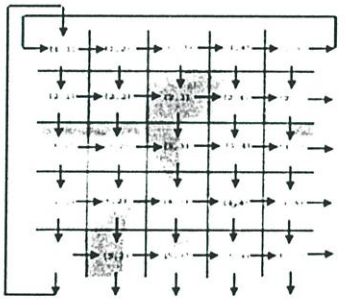


Figure 3. Use of neighbouring blocks for feature extraction

In feature extraction process, an image (or video frame) is divided into blocks of size 8×8. For each block pair, says block (i,k) and $(i,k+1)$, a local histogram equalization is performed. From the pair of equalized blocks, DC coefficient (mean) of the block (i,k), denoted by $f_{i,k}$, is computed. Normalized difference between the coefficients corresponding to the two adjacent blocks is then calculated as given by

$$\tilde{f}^{r}_{i,k} = \frac{f_{i,k} - f_{i,k+1}}{f_{i,k} + f_{i,k+1}} \qquad (1)$$

for the feature corresponding to the block on the right, and

$$\tilde{f}^{b}_{i,k} = \frac{f_{i,k} - f_{i+1,k}}{f_{i,k} + f_{i+1,k}} \qquad (1)$$

for the feature corresponding to the block below the current one. For the blocks at the image edge, the adjacent blocks are chosen as described in Figure 3. Next, $\tilde{f}^{r}_{i,k}$ and $\tilde{f}^{b}_{i,k}$ are quantized, so that they can be represented by a finite number of binary bits. Here, two bits are used for representing each feature. Therefore, there are at most 4 different quantization levels. In this case, the quantized data is given by

$$\breve{f}^{*}_{i,k} = \begin{cases} 1 & \tilde{f}^{*}_{i,k} \geq \alpha+\beta \\ 2 & \alpha-\beta < \tilde{f}^{*}_{i,k} < \alpha+\beta \\ 0 & -\alpha+\beta \leq \tilde{f}^{*}_{i,k} \leq \alpha-\beta \\ 2 & -\alpha-\beta < \tilde{f}^{*}_{i,k} < -\alpha+\beta \\ -1 & \tilde{f}^{*}_{i,k} \leq -\alpha-\beta \end{cases} \qquad (2)$$

where $\tilde{f}^{*}_{i,k}$ ($\breve{f}^{*}_{i,k}$) represents either $\tilde{f}^{r}_{i,k}$ ($\breve{f}^{r}_{i,k}$) or $\tilde{f}^{b}_{i,k}$ ($\breve{f}^{b}_{i,k}$). From Eq. (2), α is a threshold parameter for quantization. It should be chosen such that the quantized data represents well the difference between image blocks. One criterion for choosing α is to select the parameter such that the probabilities of $\breve{f}^{*}_{i,k}$ having values 0, 1, and –1, are approximately the same. In addition, from Eq. (2), β is a parameter used to create an unknown band. This allows for the detection process to be reliably performed with the image or video suffered from noise and distortion.

For a video I-frame, the resulting quantized data $\breve{f}^{r}_{i,k}$ and $\breve{f}^{b}_{i,k}$ are combined with those from other blocks to construct a digital signature. For a video P-frame and B-frame, $\breve{f}^{r}_{i,k}$ (and $\breve{f}^{b}_{i,k}$) is compared with the corresponding $\breve{f}^{r}_{i,k}$ (and $\breve{f}^{b}_{i,k}$) of the I-frame. Difference between the two is then used for signature creation. Use of feature obtained as a difference between I-frame and P- or B-frame can reduce the number of bits required to code a feature. The same process is applied for the case where there is a need to create a signature of an image/video which is a result of rightful modification to an original content. Here, a variable-length coding scheme is used to code the difference of I-frame block and that of P-frame block (as well as the difference between blocks from the original and the rightful modified image/video). For example, in our experiment, if the two blocks are considered identical (the difference is below a certain threshold), a single bit of value '0' is used to code the difference. On the other hand, if the difference is above the threshold, two data bits are used. In this latter case, the first bit set as '1', while the second bit value reflects the direction of the difference.
Figure 4 describes how signatures are created for the case of multiple image/video updating.

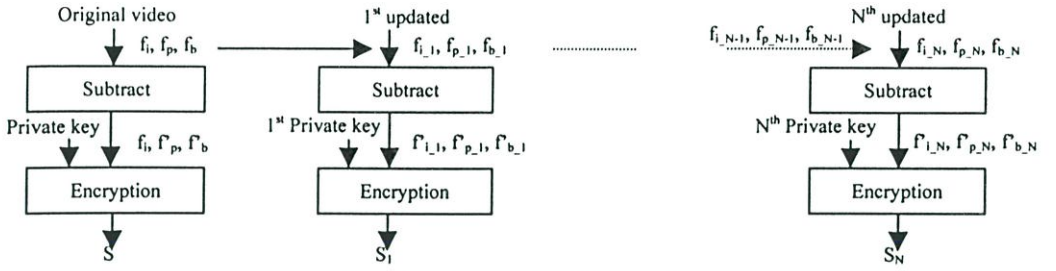


Figure 4. Updated digital signature

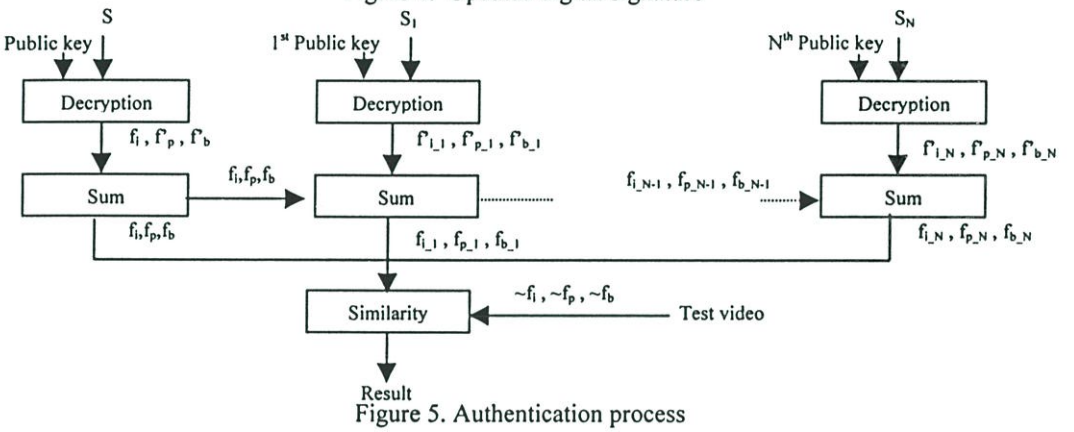


Figure 5. Authentication process

To authenticate an image/video content, a signature corresponding to each image frame is first decoded. For the I-frame case, the decoded signature is used to compare with the feature extracted from the image/video frame under consideration. For the P-frame and B-frame, the feature difference between that of the frame under consideration and the corresponding one of the I-frame must be first computed. The resulting feature difference is then used to compare with the decoded signature corresponding to the same block pair. In any case, any block pair of which the extracted feature is different from that of the decoded signature is regarded as dissimilar. The exception is when the decoded signature corresponding to any block pair has its value, which represents an unknown case (=2, see Eq. 2). In this special case, the two feature sets corresponding to that block pair are always considered identical. The authentication process for multiple updating is shown in Figure 5.

Setting the detection threshold is a classical decision estimation problem. If the threshold is set to be too high, it creates missed detection more often, while setting the threshold too low results in more false alarm.

4. Experiment Results

Experiment have been carried out to test the performance of the proposed method. The test image (frame) size is 240×320. We divided it into blocks of size 8×8. In the experiment, a local histogram equalization is performed with the window size of 16×16. In addition, $\alpha =$ 0.12 and $\beta =$ 0.05 were chosen. Figure 6 shows a video sequence used.

By using the proposed incremental-based method, it has been found that the obtained feature required less bit to encode to code. As a result, on avergage, the signature size is reduced by 33.74% per frame.

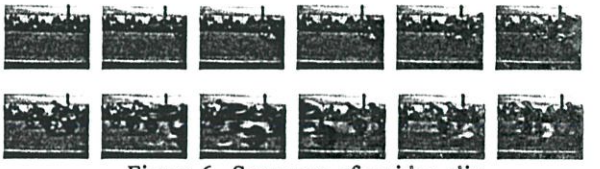


Figure 6. Sequence of a video clip.

Next, various image manipulations were performed. The results are given below.

Cropping: Parts of the image on the right and bottom were cropped is shown in Figure 7(b), as compared with the orignal one shown in Figure 7(a). Borders of blocks of which their relation to neighbouring ones differ from those of the original were marked by a white line in the figure.

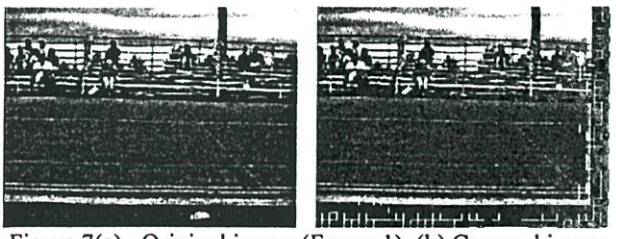


Figure 7(a). Original image (Frame 1), (b) Cropped image

Brightness adjustment : Figure 8(a) shows original image with 20% increase in brightness level and Figure 8 (b) shows original image with 20% decrease in brightness level. The percentage of feature mismatches found for the case of Figure 8(a) is 1.67%, and 3.17% for Figure 8(b). The errors found are due to pixel intensity saturation as a result of brightness adjustment.

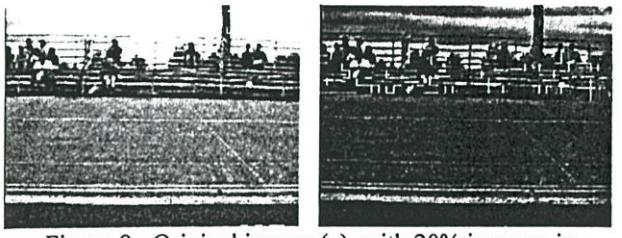


Figure 8. Original image: (a) with 20% increase in brightness level, (b) with 20% decrease in brightness level

Contrast adjustment: Figure 9(a) shows original image with a global histogram equalization. The percentage of feature mismatches is 0.08 %.

JPEG compression: Figure 9(b) shows 60% JPEG compression image. The number of feature mismatches found is 0.96%.

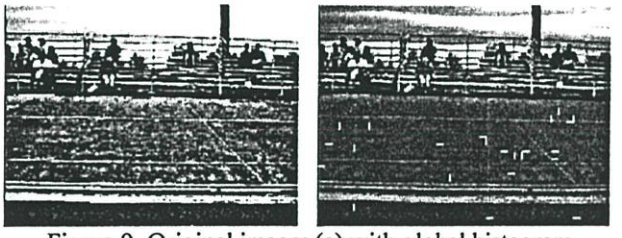


Figure 9. Original image: (a) with global histogram equalization, (b) with 60% JPEG compression

Noise: Figure 10(a) shows image adds "salt & pepper" noise, where the noise density is 0.04. And Figure 10(b) shows image adds "gaussian" SNR = 67.41 dB. In Figure 10(b) the percentage of feature mismatches is 1.83%.

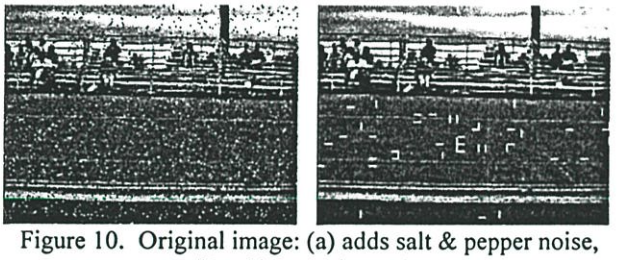


Figure 10. Original image: (a) adds salt & pepper noise, (b) adds gaussian noise

Updated and Manipulation: Figure 11(a) shows updated image. The digital signature is generated from the different feature, obtained as difference between the feature of the original image and updated image. Length of feature is 4800 bits and length of different feature is 2424 bits so, it decrease 49.50%. Experiment is made by manipulating the updated image, is shown in Figure 11(b). The authentication result, when compared with the updated image is shown in Figure 12(a). The authentication result, when compared with the original image is shown in Figure 12(b).

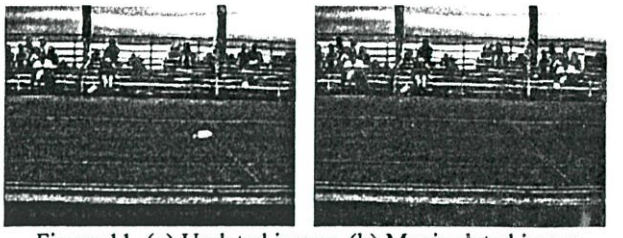


Figure 11. (a) Updated image, (b) Manipulated image

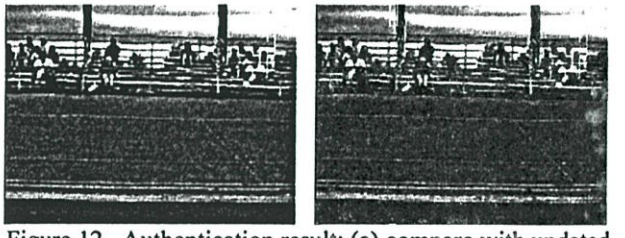


Figure 12. Authentication result: (a) compare with updated image, (b) compare with original image

5. Conclusion

In this paper, the video authentication method based on relative similarity of neighboring block features has been proposed. The proposed scheme has the advantages of being able to identify a modified portion of image/video, as compared with either the original image/video or an updated image/video. The use of incremental-based signature approach reduces the size of a signature. In addition, it allows for P-frames and B-frames of the original video, and video frames from the updated or modified video, to be treated in a unified manner.

References

[1] G. Bijan Mobassseri, J. Michale Sieffert, J. Richard Simard. "Content Authentication and Tamper detection in Digital Video," *Proc. Int. Conf. on Image Processing,* Vol.1, pp.458-461, 2000.

[2] Ching-Yung Lin. "Watermarking and Digital Signature Techniques for Multimedia Authentication and Copyright Protection," *Doctor of Philosophy in the Graduate School of Arts and Science, Columbia University,* 2000.

[3] Jana Dittmann, Arnd Steinmetz, Ralf Steinmetz. "Content-based Digital Signature for Motion Pictures Authentication and Content-Fragile Watermark," *IEEE Int. Conf. on Multimedia Computing and Systems,* Vol.2, pp.209-213, 1999.

[4] Marc Schneider and Shih-Fu Chang. "A Robust Content Base Digital Signature For Image Authentication," *Proc. Int. Conf. on Image Processing,* Vol.3, pp.227-230, 1996.

[5] Min Wu and Bede Liu. "Watermarking For Image Authentication," *Proc. Int. Conf. on Image Processing,* Vol.2, pp. 437-441, 1998.

[6] M. Bellare, O.Goldreich, S.Goldwasser. "Incremental Cryptography:The Case of Hashing and Signing," *Crypto '94, Lecture Note in Computer Science,* Vol. 839, pp.216-233, 1994.

[7] M. Fischlin. "Lower bounds for the signature size of incremental schemes." *In 38th Annual Symposium on Foundations of Computer Science,* pp. 438-447, 1997.

ประวัติผู้เขียน

ชื่อผู้เขียน	นางสาววิไลพร กุลตังวัฒนา
วัน/เดือน/ปี เกิด	17 พฤศจิกายน 2521
วุฒิการศึกษาระดับปริญญาตรี	วิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยหอการค้าไทย ปีการศึกษา 2542
	นิติศาสตรบัณฑิต มหาวิทยาลัยสุโขทัยธรรมาธิราช ปีการศึกษา 2545