Seminar Report

on

CRYPTO-WATERMARKING

Submitted by

Fathima Farhath PA (20420038)

In partial fulfillment of the requirements for the award of the Degree of
Bachelor in Technology in Information Technology

DIVISION OF INFORMATION TECHNOLOGY SCHOOL OF
ENGINEERING COCHIN UNIVERSITY OF SCIENCE AND
TECHNOLOGY KOCHI-682022

MARCH 2024

DIVISION OF INFORMATION TECHNOLOGY
SCHOOL OF ENGINEERING
COCHIN UNIVERSITY OF SCIENCE AND TECHNOLOGY

CERTIFICATE

Certified that this is a Seminar Report titled

CRYPTO-WATERMARKING

Submitted by

Fathima Farhath PA(20420038)

in partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in Information Technology of Cochin University of Science and Technology, Kochi during the academic year 2023-24, is a bonafide record of work carried out under our guidance and supervision.

Dr. Daleesha M Vishwananthan   Ms. Sariga Raj
Head of Division   Seminar Guide

Acknowledgement

Declaration

I Fathima Farhath PA hereby declare that the Seminar Report entitled "CRYPTO-WATERMARKING" is an original one and has neither been submitted earlier to this institution nor submitted by me to any other institution for fulfillment of the requirement of a course of study.

Abstract

The digital landscape presents a constant challenge: protecting the authenticity and ownership of valuable content amidst widespread copying and manipulation. In the digital realm, safeguarding content authenticity and ownership is ever-pressing. While traditional watermarking methods offered some protection, their limitations – namely, detectability and vulnerability to attacks – were significant shortcomings. This abstract introduces crypto-watermarking, a revolutionary approach that leverages the strengths of both watermarking and cryptography to address these limitations.

Cryptographic watermarking emerges as a promising solution by embedding imperceptible digital signatures within digital content, enabling robust ownership verification and authentication. Unlike its predecessors, crypto-watermarking integrates the data-hiding power of watermarking with the robust security of cryptography of the Advanced Encryption Standard (AES). This innovative approach entails embedding encrypted watermarks into digital assets, ensuring imperceptibility and resilience against tampering attempts. By leveraging AES as the encryption algorithm, crypto-watermarking fortifies content protection, mitigating risks associated with unauthorized distribution and piracy. This abstract serves as a concise yet informative guide, Unveiling the potential of crypto-watermarking to revolutionize digital content security for creators, security professionals, and anyone concerned with safeguarding valuable data.

Contents

8 References

List of Figures

Abbreviations

AES - Advanced Encryption Standard

DES - Data Encryption Standard

3DES - Triple Data Encryption Standard

RSA - Rivest–Shamir–Adleman

DSA - Digital Signature Algorithm

DCT - Discrete Cosine Transform

Chapter 1

Introduction

The report titled "Crypto-Watermarking" addresses the critical need for safeguarding digital content in an age dominated by the widespread transmission of information. With concerns surrounding the protection, authentication, and ownership verification of digital assets escalating across various domains, the integration of cryptography with digital watermarking emerges as a pivotal solution. Specifically, this report focuses on the utilization of Advanced Encryption Standard (AES) encryption within the realm of crypto watermarking. By harnessing AES encryption techniques, this approach aims to embed imperceptible marks into digital media, fortifying them with robust and tamper-evident identifiers or signatures. Through an exploration of AES-based crypto watermarking methodologies, encompassing encryption during watermark embedding and decryption during extraction, this report elucidates how AES enhances the security and resilience of watermarking schemes. Moreover, it examines the effectiveness of AES encryption in thwarting common attacks on watermarking systems, thereby mitigating threats such as signal processing manipulations and malicious tampering.

1.1 Scope

This method focuses on the integration of Advanced Encryption Standard (AES) encryption within the domain of crypto watermarking. It delves into the theoretical foundations and practical methodologies involved in employing AES encryption techniques to enhance the security and robustness of watermark embedding and extraction processes. The scope encompasses an exploration of AES-based crypto watermarking methodologies, including

the encryption of watermark data prior to embedding and decryption during extraction. Furthermore, it examines the efficacy of AES encryption in mitigating common attacks on watermarking systems, such as signal processing manipulations and malicious tampering. While emphasizing the specific application of AES encryption in crypto watermarking, the report also touches upon broader cryptographic principles and their implications for digital content protection and authentication.

1.2 Objectives

- Enhance the security of digital content by embedding imperceptible marks or signatures using cryptographic techniques.

- Provide robust authentication and verification mechanisms to combat unauthorized duplication, manipulation, and distribution of digital media.

- Enable the protection of intellectual property rights by facilitating the identification and ownership verification of digital assets.

- Support digital rights management (DRM) systems by embedding tamper-evident identifiers for tracking and controlling the usage of copyrighted materials.

- Foster trust and integrity in digital transactions by ensuring the authenticity and integrity of digital content across various domains and applications.

Chapter 2

Background and Fundamentals of Research

2.1 Digital Watermarking

Digital watermarking is a technique used to embed imperceptible information, known as a watermark, into digital media such as images, audio, video, or documents. The primary purpose of digital watermarking is to provide a means of identifying and protecting digital content from unauthorized use, distribution, or tampering, without significantly degrading the quality or perceptibility of the original media. It is a pattern or signal embedded within digital content that is typically invisible to the human eye or ear, but can be detected and extracted using specialized algorithms or software. This watermark often contains information about the content's origin, ownership, copyright status, or other relevant metadata. Digital watermarking techniques vary depending on the type of media and the desired application, but they generally involve modifying the content in a way that is robust to common signal processing operations and compression algorithms.

Types of Watermarking

There exists different types of watermarking techniques, such as:

- Visible watermarking: Visible watermarking involves embedding visible marks or logos directly onto the surface of digital media. Visible watermarks are commonly used for branding, copyright notices, or ownership

identification. While visible watermarks are easily detectable, they may also degrade the visual quality of the content and can be removed or tampered with by malicious users.

- Invisible watermarking: Invisible watermarking, also known as digital or imperceptible watermarking, embeds imperceptible information within digital media. Unlike visible watermarks, invisible watermarks are not visually apparent to viewers and do not degrade the quality of the content. These watermarks are primarily used for copyright protection, authentication, and content tracking without interfering with the user's viewing experience.

- Robust watermarking: Robust watermarking is a technique used to embed imperceptible information within digital media in such a way that the watermark remains detectable even after the content undergoes various transformations or attacks. Unlike fragile watermarking, which is highly sensitive to modifications, robust watermarks are designed to withstand common signal processing operations, compression algorithms, and intentional attacks.

- Fragile watermarking: Fragile watermarking techniques are designed to detect any modifications or tampering to the digital content. Fragile watermarks are embedded in a manner that makes them highly sensitive to any alterations in the content, such as image cropping, resizing, or compression. Fragile watermarking is commonly employed in applications where the integrity and trustworthiness of the content are paramount

2.2 Cryptography

Cryptography is the art of protecting information by transforming it into an unreadable form, called ciphertext. This ciphertext can only be retrieved back to its original form, called plaintext, using a secret key or a combination of keys. Cryptography plays a vital role in securing communication channels and storing sensitive data in today's digital world.

Cryptographic algorithms
- Symmetric Encryption Algorithm:Also Known as private key Enccryption. It uses a single secret key for both encrypting and decrypting data.

eg:AES (Advanced Encryption Standard),DES (Data Encryption Standard),3DES (Triple DES)

- Asymmetric Encryption algorithm: Also known as public key Encryption.Asymmetric encryption utilizes a mathematically linked pair of keys: a public key and a private key. Public Key: This key is freely available for anyone to encrypt messages with. Private Key: This key is kept secret by the receiver and is used to decrypt messages encrypted with the corresponding public key.eg:RSA,DSA

2.3 Crypto-Watermarking

Crypto-watermarking builds upon the principles of both cryptography and digital watermarking to provide a more secure way to embed hidden information within digital content.

Instead of simply hiding information within digital content, crypto-watermarking uses cryptographic functions (like hashing or digital signatures) to secure the watermark data itself. This offers stronger protection against tampering and unauthorized extraction of the watermark. It enhances security in applications like copyright protection, content authentication, and tamper detection for important documents. While balancing imperceptibility, robustness, and processing overhead presents challenges, advancements in algorithms and potential integration with blockchain technology promise a future of even more secure and reliable crypto-watermarking solutions.

Chapter 3

Comparison of Traditional Watermarking and Cryptographic Watermarking Approaches

3.1 Traditional watermarking method (Without Cryptography)

In traditional watermarking, imperceptible marks or identifiers are embedded into digital content to provide ownership or copyright information.

- Objective: Traditional watermarking aims to embed imperceptible marks or identifiers into digital content to provide ownership or copyright information, but it doesn't involve cryptographic techniques.

- Visibility: Traditional watermarks can be visible or invisible, depending on the application. Visible watermarks may include logos or text overlaid on images or videos, while invisible watermarks modify the data itself without affecting its visual appearance.

- Robustness: Traditional watermarking techniques may lack robustness against various signal processing operations, such as compression, cropping, or scaling. As a result, the watermark may be easily removed or altered without detection.

- Security: Without cryptographic techniques, traditional watermarks may not provide strong security against unauthorized removal or tampering. They may serve as a deterrent but are not necessarily tamper-evident.

- Applications: Traditional watermarking finds applications in various fields, including copyright protection, content authentication, and digital foren-

sics. It's commonly used in media distribution, stock photography, and document authentication.

3.2 Current Crypto-Watermarking method

In crypto watermarking, cryptographic techniques are incorporated to embed imperceptible marks into digital content, enhancing security and robustness against tampering or removal.

- Objective: Crypto watermarking incorporates cryptographic techniques to embed imperceptible marks into digital content, enhancing security and robustness against tampering or removal.

- Incorporation of Cryptography: Crypto watermarking typically involves encrypting the watermark data before embedding it into the content. This ensures that the watermark remains secure and tamper-evident, even if the content is manipulated.

- Robustness and Security: Crypto watermarking is designed to be highly robust against various attacks, including signal processing operations, compression, and malicious tampering. The cryptographic techniques used ensure the integrity and authenticity of the watermark.

- Detection and Authentication: Crypto watermarking allows for reliable detection and authentication of watermarked content, even in the presence of sophisticated attacks. The embedded watermark can be extracted and verified using cryptographic methods, providing strong evidence of ownership or origin.

- Applications: Crypto watermarking is well-suited for applications requiring high levels of security and tamper resistance, such as digital rights management (DRM), content authentication, and forensic analysis. It's commonly used in industries like entertainment, publishing, and document management, where protecting intellectual property is critical.

While traditional watermarking without cryptography serves as a basic method for embedding marks into digital content, crypto watermarking enhances security and robustness through the integration of cryptographic techniques. Crypto watermarking provides tamper-evident protection and reliable authentication, making it suitable for applications requiring strong security guarantees.

Chapter 4

The Crypto-Watermarking Process

4.1 Steps Involved in Crypto-Watermarking

Figure 4.1: Crypto Watrmarking Process

article

1. **Preparation of Watermark:**

   - This step involves creating the information to be embedded as a watermark. It could be a:
     - Hash function output: A cryptographic hash (e.g., SHA-256) of the original content for tamper detection.
     - Digital Signature: A digital signature created using the private key of an authorized entity (e.g., doctor) for authentication.

2. **Encryption of Watermark:**

   - An additional layer of security can be achieved by encrypting the watermark itself with a separate key before embedding.

3. **Content Preparation:**

   - The digital content (e.g., X-ray image) where the watermark will be embedded is prepared. This might involve pre-processing steps like format adjustments for optimal watermark embedding.

4. **Watermark Embedding:**

   - The chosen watermark (hashed data or encrypted signature) is then embedded into the digital content using a robust watermarking technique. This technique should be imperceptible and not degrade the content's quality.
   - **Tamper Detection Methods:**
     - **Images:** Spatial Domain Embedding
       * In this technique, the watermark is directly embedded into the pixel values of the image.
     - **Videos:** Wtermark Embeddng Techniques for different content types
       * For videos, temporal characteristics are considered for watermark embedding.
     - **Audio:** Frequency Domain Embedding
       * Audio signals are often transformed into the frequency domain using techniques like Fourier Transform.

5. **Crypto-watermarked Asset:**

   - The final output is the digital content with the embedded crypto-watermark.

6. **Watermark Verification:**

   - Apply Watermark Extraction:
     - When verification is needed, the embedded watermark is extracted from the crypto-watermarked content using the watermark extraction technique.

- Decryption of Watermark:
  - If the watermark was encrypted during preparation, it's decrypted using the corresponding key to retrieve the original watermark data.
- Watermark Content Retrieval:
  - The extracted watermark (hash or signature) is retrieved.

7. **Tamper Detection and Authentication:**

- Compare:
  - The retrieved watermark content (hash or signature) is compared with the original watermark (generated in step 1) or its verification information (e.g., public key for signature validation).
- If Changed:
  - If the comparison fails, it indicates tampering with the content, as the watermark would have been altered.
- Else (Not Tampered):
  - If the comparison succeeds, it suggests a high probability that the content hasn't been tampered with (for hash-based) or the content is authentic (for digital signatures).

Chapter 5

Use Case:Secure Embedding of Patient Data in Medical Images

Scenario: A healthcare facility needs to securely store and transmit a patient's medical data along with their X-ray image. This data could include demographics, medical history, and details about the X-ray itself. To comply with regulations like HIPAA and enhance patient privacy, the facility wants to embed the data directly within the X-ray image.

Proposed Approach: The use case leverages the following steps:

1. **Data Preprocessing:**

   - Patient data undergoes various transformations to prepare it for embedding. This might involve converting it to a binary sequence and potentially compressing it for efficient integration.

2. **Watermark Creation:**

   - A watermark is generated containing two parts(Fig 5.1):
     - Digital Signature: A signature (e.g., using SHA-1) is created using the hospital's private key to ensure data authenticity.
     - Patient Data: The remaining patient data is converted into a binary sequence. These parts are concatenated to form the complete watermark.

3. **Watermark Embedding:**

   - The Discrete Cosine Transform (DCT) is applied to divide the X-ray image into subblocks. The watermark bits are then strategically embedded into the medium frequency bands of these subblocks using a visibility factor to balance imperceptibility and robustness.
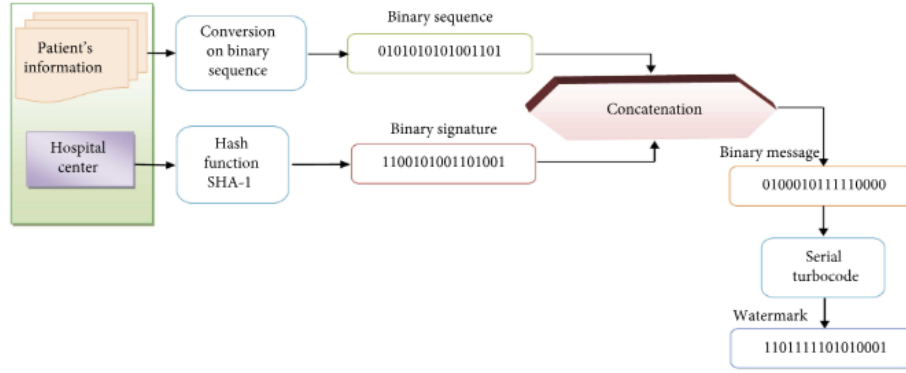
Figure 5.1: Watermark Creation

4. **Encryption:**

- For enhanced security, the watermarked image is encrypted using the AES algorithm(Fig 5.2). Additionally, chaotic techniques like Arnold's cat map and Henon map are employed for key generation and shuffling to further strengthen the encryption process.
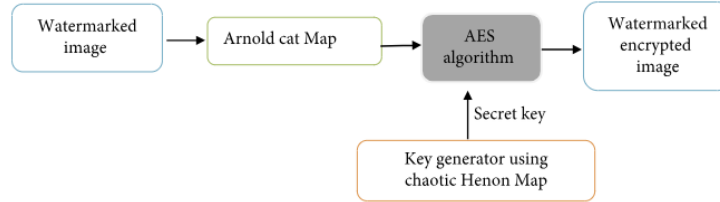

Figure 5.2: AES Encryption

5. **Watermark Extracction:**

- The extraction process reverses the embedding steps. This involves decrypting the watermarked image with the AES algorithm and undoing the encryption's shuffling using Arnold's cat map in reverse.Next, the medium frequency bands of subblocks in the decrypted image are analyzed to extract the embedded bits based on the watermark embedding equation. The extracted bits are then combined to form a complete binary message. Optionally, error correction techniques can be applied to account for potential errors. Finally, the binary message is decoded back to its original format, separating the signature for verification and retrieving the complete set of patient information.

The below figure(Fig:5.3) depicts different types of watermarks using in medical imaging:

Figure 5.3: Watermarks in medical imaging

Chapter 6

Crypto Watermarking Analysis

6.1 Advantages

- Enhanced Security: The algorithm utilizes cryptographic techniques and watermark embedding to ensure the security of digital content.

- Tamper Detection: It provides tamper detection capabilities, allowing content owners to verify the authenticity and integrity of their digital assets.

- Copyright Protection: Crypto watermarking helps protect intellectual property rights by providing a means to identify and trace ownership of digital content.

- Robustness: Watermarks embedded using cryptographic techniques are often robust against common signal processing operations, compression algorithms, and malicious attacks.

- Versatility: Crypto watermarking can be applied to various types of digital media, including images, audio, video, and documents, making it a versatile solution for content protection.

6.2 Limitations

- Computational Overhead: The encryption and watermark embedding processes may introduce computational overhead, particularly for large datasets.

- Sensitivity to Image Modifications: The algorithm's effectiveness may be reduced if the medical image undergoes significant modifications or transformations after watermark embedding.

- Vulnerability to Attacks: While robust, crypto watermarking methods may still be vulnerable to sophisticated attacks, such as collusion attacks or watermark removal techniques developed by adversaries.

6.3 Applications

- Medical Data Security: The algorithm can be applied in healthcare settings to securely store and transmit patient data along with medical images, ensuring compliance with privacy regulations.

- Brand Protection: Organizations use crypto watermarking to protect their brand assets, such as logos and images, from misuse or unauthorized use on the internet or in print media.

- Forensic Analysis: In forensic investigations, the algorithm can be used to embed metadata within digital images, providing valuable information for analysis and authentication.

Chapter 7

Conclusion

In this seminar report, we embarked on an in-depth exploration of crypto watermarking which stands as a robust solution for safeguarding digital content integrity, enhancing security, and protecting intellectual property rights. By embedding imperceptible watermarks using cryptographic techniques, this method enables tamper detection, content authentication, and traceability, crucial in various domains such as digital rights management, media forensics, and brand protection. While offering significant advantages in content protection, it's essential to acknowledge its limitations, including potential quality degradation and susceptibility to sophisticated attacks. Nonetheless, with ongoing advancements in cryptography and signal processing, coupled with its versatile applications, crypto watermarking remains a valuable tool for ensuring the authenticity, integrity, and ownership of digital assets in an increasingly digitalized world.

Chapter 8

References

1. Sondes Ajili, Mohamed Ali Hajjaji and Abdellatif Mtiba, "Crypto-Watermarking Algorithm Using Weber's Law and AES: A View to Transfer Safe Medical Image " 2021

2. Surekha Borraa and Rohit Thanki b, "Crypto-watermarking scheme for tamper detection of medical images" 2018

3. B. Sridhar1 , V.Syambabu, "An Importance of Crypto-Watermarking Techniques for Secure Transmission of Multimedia Information" 2021

4. Jana Dittmann, Petra Wohlmacher,Klara Nahrstedt,"Using Cryptographic and Watermarking Algorithms" 2001

5. Dalel Bouslimi, Gouenou Coatrieux , "A crypto-watermarking system for ensuring reliability control and traceability of medical images" 2016

6. Ali Al-Haj, Ahmad Mohammad Alaa' Amer "Crypto-Watermarking of Transmitted Medical Images" 2016

7. B. Sridhar; V. Syambabu, An Importance of Crypto-Watermarking Techniques for Secure Transmission of Multimedia Information 2021