Analysis and Implementation of Secret Image Sharing for Secure Distribution of Pre-Release Digital Media Assets

Rafli Dwi Nugraha - 18223038

Information System & Technology Study Program

School of Electrical Engineering and Informatics

Institut Teknologi Bandung, Jalan Ganesha 10 Bandung

E-mail: raflidwin322@gmail.com , 18223038@std.stei.itb.ac.id

***Abstract*—The increasing number of digital media leaks involving unreleased games, films, trailers, and promotional assets has become a significant challenge for the entertainment industry. Existing protection mechanisms, such as access control, digital rights management (DRM), and watermarking, primarily focus on restricting access or identifying the source of a leak after it occurs. However, these approaches do not prevent authorized individuals from viewing or distributing complete digital assets. This study analyzes and implements a secret image sharing framework based on a (3,3) XOR secret-sharing scheme for securing the distribution of confidential digital media during the pre-release phase. Secret image sharing is a cryptographic technique that divides an image into multiple shares, where each share independently reveals no meaningful information and the original image can only be reconstructed when all required shares are combined. The proposed framework applies a (3,3) XOR-based secret image sharing scheme to sensitive media assets, ensuring that no single stakeholder possesses the complete content before authorized reconstruction. This research contributes to the development of preventive cryptographic controls for protecting confidential digital media assets and reducing the risk of pre-release leaks.**

Keywords—component; Secret Image Sharing, XOR Secret Sharing, Digital Media Security, Leak Prevention, Secret Sharing, Information Security, Digital Asset Protection.

I. INTRODUCTION

A. Background

The digital entertainment industry has experienced significant growth in recent years, resulting in the widespread production and distribution of digital assets such as movie posters, trailers, game artwork, promotional materials, and other pre-release content. These assets are often shared among multiple stakeholders, including development teams, marketing departments, publishers, and external partners throughout the production and release process. While digital collaboration improves efficiency, it also increases the risk of unauthorized disclosure and information leakage.

Several high-profile incidents involving leaked game footage, unreleased trailers, and confidential promotional materials have demonstrated the challenges of protecting sensitive digital media. Such leaks can negatively affect marketing strategies, reduce the impact of official announcements, expose unfinished content to public scrutiny, and potentially cause financial and reputational damage to organizations. As a result, ensuring the confidentiality of pre-release digital assets has become an important concern for content creators and distributors.

Various security mechanisms have been employed to address this issue, including access control systems, digital rights management (DRM), non-disclosure agreements (NDAs), and digital watermarking. Although these solutions can restrict access, monitor user activities, or identify the source of a leak after it occurs, they generally allow authorized users to view the complete digital asset. Consequently, the risk of insider threats remains a significant challenge, as individuals with legitimate access may intentionally or unintentionally disclose confidential information.

Secret image sharing offers an alternative approach to protecting sensitive visual information. Secret image sharing is derived from the concept of secret sharing, where confidential information is divided into multiple shares and distributed among authorized participants. In image-based secret sharing, the original image is transformed into several independent shares, each of which reveals no meaningful information when viewed individually. The original image can only be reconstructed when all required shares are combined. By ensuring that no single party possesses the complete asset, secret image sharing has the potential to reduce the risk of unauthorized disclosure during the distribution of confidential digital media.

B. Objectives

This research aims to analyze the applicability of secret image sharing as a security mechanism for protecting confidential digital media assets during the pre-release phase. The study seeks to design and implement a secret image

sharing-based framework that enables sensitive visual content to be distributed among multiple stakeholders without granting any individual party access to the complete asset. Furthermore, this research evaluates the effectiveness of the proposed approach in preventing unauthorized disclosure by ensuring that individual shares do not reveal meaningful information about the original media. In addition, the study assesses the accuracy of the reconstruction process to determine whether the original media can be successfully recovered when the required shares are combined. Ultimately, this research aims to examine the potential of secret image sharing as a preventive security mechanism for reducing the risk of digital media leaks while preserving the integrity of the protected content.

II. LITERATUR REVIEW

A. Digital Media Leaks

Digital media leaks refer to the unauthorized disclosure of confidential digital assets before their intended public release. In the entertainment industry, such assets may include movie trailers, promotional posters, game footage, concept art, scripts, and other proprietary materials. The increasing reliance on digital collaboration platforms and cloud-based storage systems has expanded the attack surface for unauthorized access and distribution of sensitive content.

Pre-release leaks can negatively impact organizations in various ways. Leaked content may reduce the effectiveness of marketing campaigns, diminish audience anticipation, expose unfinished products to public criticism, and potentially cause financial and reputational losses [1]. Furthermore, leaks originating from internal stakeholders present a significant challenge because authorized users often require access to confidential materials as part of their responsibilities.

As a result, organizations continuously seek methods to protect digital assets during development, review, and distribution processes to minimize the risk of unauthorized disclosure [1].

B. Existing Digital Media Protection Methods

Various security mechanisms have been developed to protect confidential digital media assets. Some of the visual data leak prevention mechanisms in use today include:

a. Access Control

Access control mechanisms restrict access to authorized users through authentication and authorization policies. While effective in limiting access, authorized users can still view and potentially distribute the complete asset.

b. Digital Rights Management (DRM)

Digital Rights Management (DRM) technologies provide content protection through encryption, usage restrictions, and device-specific controls. DRM is widely used for protecting distributed media but is generally focused on controlling consumption after content has been released.

c. Digital Watermarking

Digital watermarking embeds identifiable information within digital content, enabling organizations to trace the source of unauthorized distribution. Although watermarking assists in leak attribution, it does not prevent users from accessing the protected content.

d. Non-Disclosure Agreements (NDAs)

Non-Disclosure Agreements (NDAs) serve as legal instruments that discourage unauthorized disclosure. However, they rely primarily on deterrence and legal consequences rather than technical prevention.

Despite their effectiveness in specific scenarios, these methods generally assume that authorized individuals can access the complete media asset, leaving organizations vulnerable to insider threats and unauthorized redistribution.

C. Secret Sharing

Secret sharing is a cryptographic technique that enables a secret to be divided into multiple pieces, known as shares, and distributed among a group of participants [3]. The concept was formally introduced by Shamir in 1979 as a method for protecting sensitive information while ensuring that no individual participant can access the complete secret independently. In a secret-sharing scheme, the original secret can only be reconstructed when a predefined number of shares are combined, while possession of fewer shares provides insufficient information to recover the secret [3].

Secret sharing schemes are commonly represented using a threshold notation (k,n), where n denotes the total number of generated shares and k represents the minimum number of shares required for reconstruction [3]. For example, in a (3,3) scheme, all three shares are required to recover the original secret, whereas in a (2,3) scheme any two out of three shares can reconstruct the secret. This threshold property provides both confidentiality and fault tolerance, making secret sharing suitable for applications involving distributed trust and collaborative access control.

The security of secret sharing relies on the principle that individual shares reveal no meaningful information about the original secret [3]. As a result, an adversary who obtains fewer than the required number of shares cannot reconstruct or infer the protected information. Due to these characteristics, secret sharing has been widely applied in cryptographic key management, secure data storage, distributed systems, and confidential information protection.

In the context of digital media protection, secret sharing offers a mechanism for distributing sensitive assets among multiple stakeholders while preventing any individual party from obtaining the complete content. This characteristic makes secret sharing particularly relevant for mitigating insider threats and unauthorized disclosure during the distribution of confidential digital media assets.

D. Secret Image Sharing

Secret Image Sharing (SIS) is an extension of traditional secret-sharing techniques that applies the concept of share generation and reconstruction to digital images [4]. Instead of dividing numerical secrets or cryptographic keys, secret image sharing divides an image into multiple shares that can be distributed among authorized participants. Similar to conventional secret sharing, each share independently reveals no meaningful information about the original image, and reconstruction is only possible when the required shares are combined.

Secret image sharing techniques can be broadly categorized into polynomial-based schemes, visual cryptography schemes, and XOR-based schemes [5]. Polynomial-based approaches extend traditional secret-sharing algorithms to image data, while visual cryptography focuses on reconstructing images through visual superimposition of shares. XOR-based secret image sharing utilizes the properties of the exclusive OR (XOR) operation to generate shares and recover the original image.

Among these approaches, XOR-based secret image sharing offers several advantages, including simplicity, computational efficiency, and lossless reconstruction. In a typical XOR-based scheme, random shares are generated and combined with the original image using XOR operations to produce additional shares. During reconstruction, all required shares are combined through the XOR operation, resulting in an image that is identical to the original image.

The security of XOR-based secret image sharing relies on the randomness of the generated shares. Because individual shares appear as random noise and contain no meaningful visual information, unauthorized parties cannot recover the original image without possessing all required shares. Furthermore, the lossless reconstruction capability makes XOR-based secret image sharing particularly suitable for protecting digital media assets where preserving image quality is essential.

Due to its confidentiality properties and reconstruction accuracy, secret image sharing has been applied in secure image transmission, medical image protection, cloud storage security, and confidential multimedia distribution. These characteristics make it a promising approach for protecting pre-release digital media assets from unauthorized disclosure.

E. XOR-based Secret Image Sharing

XOR-based Secret Image Sharing is a category of image protection techniques that utilize the exclusive OR (XOR) operation to generate and reconstruct image shares. In a (3,3) XOR scheme, two shares are generated randomly, while the third share is computed by applying the XOR operation between the original image and the generated shares. The original image can only be reconstructed when all three shares are combined using the same XOR operation.

Let S represent the original image, and R_1 and R_2 represent randomly generated shares. The third share R_3 is generated as:

$$R_3 = S \oplus R_1 \oplus R_2$$

To reconstruct the original image:

$$S = R_1 \oplus R_2 \oplus R_3$$

Because XOR is a reversible operation, the reconstructed image is identical to the original image. Furthermore, individual shares reveal no useful information regarding the secret image, ensuring confidentiality during distribution. These properties make XOR-based secret image sharing suitable for applications requiring both strong confidentiality and perfect reconstruction accuracy.

F. Related Works

Numerous studies have explored the application of secret sharing and secret image sharing techniques for protecting sensitive information. One of the foundational works in this field was proposed by Shamir, who introduced the concept of threshold secret sharing as a method for dividing confidential information into multiple shares while preventing unauthorized access to the original secret. The proposed scheme demonstrated that a secret could only be reconstructed when a sufficient number of shares were available, establishing the basis for subsequent secret-sharing research.

Building upon traditional secret-sharing schemes, researchers have extended these concepts to image data through Secret Image Sharing (SIS). Thien and Lin proposed an image-sharing method that applies secret-sharing principles to digital images, enabling secure image distribution while preserving confidentiality during transmission and storage. Their work demonstrated the practicality of secret-sharing techniques for multimedia data and inspired further developments in image protection mechanisms.

Another major research direction involves Visual Cryptography, introduced by Naor and Shamir, which enables image reconstruction through the superimposition of multiple shares. Visual cryptography provides a simple and intuitive approach to image protection; however, many traditional visual cryptography schemes suffer from pixel expansion and image quality degradation during reconstruction [2]. These limitations may reduce their suitability for applications requiring accurate recovery of digital media assets.

To address reconstruction quality issues, researchers have proposed XOR-based secret image sharing schemes. Unlike traditional visual cryptography, XOR-based approaches utilize bitwise XOR operations to generate and reconstruct image shares. These schemes offer several advantages, including computational simplicity, low implementation complexity, and lossless reconstruction of the original image [5]. As a result, XOR-based secret image sharing has been widely adopted in applications requiring accurate image recovery and strong confidentiality guarantees.

Although previous studies have demonstrated the effectiveness of secret image sharing for secure image transmission, cloud storage protection, medical image security, and confidential information sharing, limited attention has been given to its application in preventing leaks of pre-release digital media assets. Existing protection mechanisms in the entertainment industry primarily rely on access control, digital rights management (DRM), digital watermarking, and legal agreements, which generally assume that authorized users can access the complete content.

Therefore, this research investigates the application of a (3,3) XOR-based Secret Image Sharing scheme as a preventive security mechanism for protecting confidential digital media assets during the pre-release phase. By distributing independent image shares among multiple stakeholders, the proposed approach aims to reduce the risk of unauthorized disclosure while maintaining accurate reconstruction of the original media when all required shares are combined.

III. Design And Implementation

A. System Architecture

The proposed framework consists of three main stages: share generation, share storage, and image reconstruction. The original image is processed by the share generation module to produce three independent shares using a (3,3) XOR-based Secret Image Sharing scheme. The generated shares are stored as separate image files and can subsequently be loaded by the reconstruction module to recover the original image. This architecture allows the confidentiality and reconstruction properties of the proposed scheme to be evaluated in a controlled environment.

The process can be visually seen through the diagram below

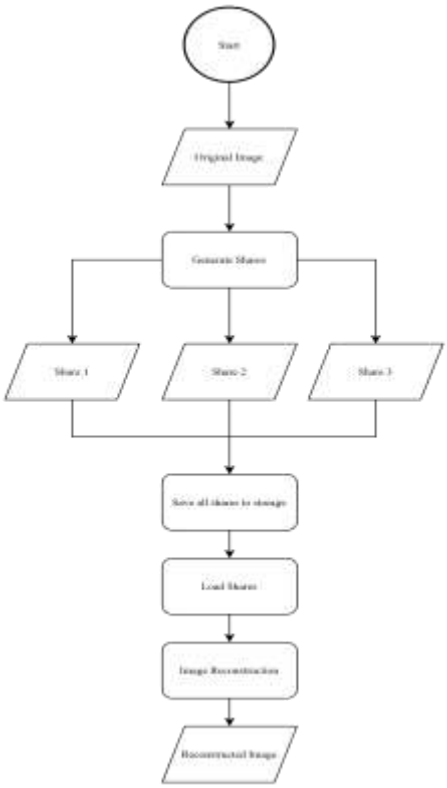

Fig. 1. System Process Flowchart

B. System Implementation

The system is built with the XOR-based secret sharing as a foundation. The implementation is built in python.

a. Share Generation

The share generation process begins by converting the original image into a numerical pixel array. Two random shares are generated using a cryptographically secure random number generator. A third share is then produced using the XOR operation between the original image and the generated random shares.

Let:

S = Original image

R_1 = Random share 1

R_2 = Random share 2

The third share is computed as

$$R_3 = S \oplus R_1 \oplus R_2$$

The generated shares appear as random noise and do not reveal meaningful information regarding the original image.

b. Share Storage

After the share generation process is completed, all generated shares are stored as separate image files. Each

share is saved independently while preserving its original dimensions and pixel values.

The storage phase enables the generated shares to be retained for subsequent reconstruction and evaluation. Since each share contains only partial information and appears as random noise, storing an individual share does not expose the original image content.

In this research, all generated shares are stored locally within the experimental environment to facilitate reconstruction and performance evaluation.

c. Image Reconstruction

The reconstruction process aims to recover the original image using all generated shares. The reconstruction module loads the three stored shares and applies the XOR operation to each corresponding pixel.

The original image is reconstructed using:

$$S = R_1 \oplus R_2 \oplus R_3$$

Because XOR is a reversible operation, the reconstruction process restores the exact pixel values of the original image. As a result, the recovered image is identical to the original image without information loss.

The reconstructed image is subsequently saved for comparison and evaluation purposes.

IV. Result And Analysis

A. Experimental Setup

Several digital media images were selected as test samples to evaluate the proposed framework. For each image, three shares were generated using the XOR-based Secret Image Sharing algorithm. The generated shares were analyzed individually to determine whether meaningful visual information could be extracted. Subsequently, all shares were combined to reconstruct the original image.

The evaluation focuses on two aspects:

a. Confidentiality of individual shares.

b. Accuracy of reconstructed images.

B. Leak Prevention Analysis

Fig. 2. Original Image

Fig. 3. Generated Share 1

Fig. 4. Generated Share 2

Fig. 4. Generated Share 3

Fig. 5. Reconstructed Image

The generated shares were visually inspected to evaluate whether confidential information from the original image could be inferred. The results indicate that all generated shares appear as random noise and do not reveal recognizable objects, text, colors, or structural features from the original media asset.

Consequently, possession of a single share does not provide sufficient information to reconstruct or infer the protected content. These findings demonstrate that the proposed framework effectively reduces the risk of unauthorized disclosure by ensuring that complete access to the media asset requires all generated shares.

C. Reconstruction Accuracy

Because the XOR-based that used in this implementation is a lossless, the reconstructed image is evaluate by how exactly it is to the original image. Evaluation is done by calculating MSE, PSNR, and SSIM.

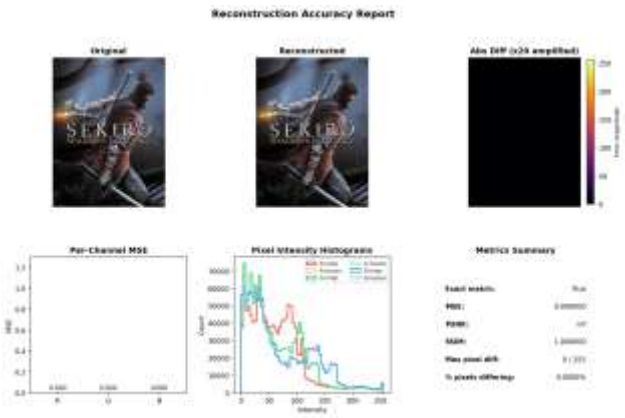

Fig. 6. Image Evaluation

The visual comparison shown by the figure above prove that he reconstructed image was identical to the original image without observable degradation or information loss.

The results confirm that the XOR-based Secret Image Sharing scheme provides lossless reconstruction, ensuring that the protected media can be recovered accurately when all required shares are available.

V. CONCLUSION

This research analyzed and implemented a (3,3) XOR-based Secret Image Sharing scheme as a security mechanism for protecting confidential digital media assets during the pre-release phase. The proposed framework divides an original image into three independent shares, where each share individually contains no meaningful information about the protected media. The original image can only be recovered when all generated shares are combined through the reconstruction process.

The experimental results demonstrate that the generated shares effectively preserve the confidentiality of the original image. Visual inspection shows that each share appears as random noise and does not reveal recognizable visual features, text, or structural information from the original media asset. Consequently, possession of a single share is insufficient to infer or reconstruct the protected content, indicating that the proposed approach can reduce the risk of unauthorized disclosure.

Furthermore, the reconstruction process successfully recovered the original image without visible degradation or information loss. By utilizing reversible XOR operations, the proposed scheme achieved lossless reconstruction, ensuring that the recovered image was identical to the original image. This characteristic is particularly important for digital media assets, where preserving image quality and content integrity is essential.

Based on the obtained results, it can be concluded that the proposed XOR-based Secret Image Sharing scheme is a viable approach for protecting confidential digital media assets. The scheme provides strong confidentiality through share

separation while maintaining accurate reconstruction of the original image when all required shares are available.

SOURCE CODE REPOSITORY AT GITHUB

https://github.com/Raflind/Sundre

ACKNOWLEDGEMENT

The author would like to express sincere gratitude to Dr. Ir. Rinaldi Munir, M.T. for his invaluable guidance and insightful lectures. Finally, I want to thank to the gaming community that inspired me to write this topic.

REFERENCES

[1] Ma, L., Montgomery, A. L., Singh, P. V., & Smith, M. D. (2014). An empirical analysis of the impact of pre-release movie piracy on box office revenue. Information Systems Research, 25(3), 590–603.

https://doi.org/10.1287/isre.2014.0530

[2] Bhatnagar, R., & Kumar, M. (2018). Visual cryptography: A literature survey.

https://doi.org/10.1109/ICECA.2018.8474649

[3] R Shamir, A. (1979). How to Share a Secret.

https://web.mit.edu/6.857/OldStuff/Fall03/ref/Shamir-HowToShareASecret.pdf

[4] Thien, C. C., & Lin, J. C. (2002). Secret Image Sharing.

https://doi.org/10.1016/S0097-8493(02)00131-0

[5] Chen, T. H., & Tsao, K. H. (2011). *Visual Secret Sharing by Random Grids Revisited*.

https://doi.org/10.1016/j.patcog.2008.11.015

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 19 Juni 2026

Rafli Dwi Nugraha 18223038