International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Survey on Secret Share Creation Scheme for Image Security

Dr Saravanan R[1]*, Ramya K*[2]*, Ranjeetha J*[3]*, Shalini E*[4]

[1,2,3,4]***Department of Information Technology,*** *Sri Manakula Vinayagar Engineering College, Puducherry, India,2023*

ABSTRACT-

Visual secret sharing (VSS) also called visual cryptography is a technique of protecting secret images from unauthorized access through the generation of few shares or shadow images. VSS has been widely used in secure communications. Secret image sharing (SIS) allows a secret image to be divided into several shares and the secret image can only be recovered through the collaboration of the shares. Even if some of the participants fail to give their share or are unavailable, the secret can still be reconstructed as long as the minimum number of required participants is available. Secret-sharing schemes use a threshold parameter that specifies the minimum number of participants required to reconstruct the secret. This threshold can be adjusted to balance security and usability. This survey paper presents a brief overview of various types of techniques used in secret share creation schemes.

Keywords: Secret image sharing, data hiding, Visual cryptography

1. INTRODUCTION

Nowadays, with the massive development of the Internet, the digitization of multimedia data has brought great convenience to people's lives. The development of multimedia information has been unstoppable. Despite the broad applications available on the Internet, the information security and privacy issues that come with it are very crucial.

Illegal organizations and network viruses that steal digital information provide serious threats to information security. Thus, the security and privacy of information transmission have become particularly important, especially in the political, healthcare, military, and commercial fields. Although traditional encryption can ensure information security only to a certain extent, this type of traditional technology does not conceal the content of the information. This has become the biggest weakness of traditional encryption algorithms. To rectify the series of above-mentioned problems information-hiding technique was introduced.

Several threats can arise when transmitting images over the internet. It includes Unauthorized access: Hackers may intercept and access the images being transmitted over the internet, and use them for malicious purposes such as identity theft, cyberstalking, or blackmail. Malware infection: Images transmitted over the internet can be used as a carrier for malware, which can infect the recipient's device and cause various types of damage, including data loss or theft. Data interception: Images transmitted over the internet can be intercepted by attackers, who can steal the data contained in them, such as personal information, financial data, or sensitive business data. Image alteration: Attackers may modify images during transmission, altering their content or introducing malware or other malicious code. Lack of privacy: Images transmitted over the internet may be viewed by unauthorized persons, leading to a violation of privacy and potential legal consequences.

The secret share creation scheme choice depends on the specific requirements and constraints of the application. Some of the different secret-sharing schemes used are:

1. Shamir's Secret Sharing System (SSS): This approach is frequently used in applications that require a high level of adaptability and scalability. SSS, for example, can be used to disseminate the secret keys of a large cryptographic system, such as a distributed database system or secure cloud storage. It is also used in applications that require dynamic or adaptive access control, where the required number of shares and the set of participants can change over time.

2. Blakley's Secret Sharing Scheme: This method is used in high-security applications such as military or government applications. The secret can only be pieced together with all n shares because it provides perfect secrecy. As a result, reconstructing the secret necessitates all n shares.

3. The Asmuth-Bloom Secret Sharing System is frequently used in applications that require simple and effective secret sharing. Because the amount of each share is proportional to the size of the secret, it is especially useful when the secret is small.

4. Krawczyk's Secret Sharing Scheme: Krawczyk's Secret Sharing Scheme is a popular option for applications that require quick and efficient secret sharing. Because the size of each share is unrelated to the size of the secret, Krawczyk's system is advantageous when the size of the secret is enormous.

5. Threshold Cryptography: This method is frequently used in applications that require safe access control and decentralised information control. The secret keys can be distributed using threshold cryptography when a computation is performed by several parties who do not completely trust one another. Threshold cryptography can also be used in applications requiring fault tolerance, where the system must continue to function even if some of the participants are compromised or fail.

2. RELATED WORKS

1. **A High-quality authenticatable Visual secret-sharing scheme using SGX:**

A visual cryptography scheme (VCS) is a secret-sharing method that can decrypt shares without the use of digital devices and encodes images as shares. Even though a member can simply stack enough shares to reveal the secret image, hostile opponents can defraud participants by providing fake shares. This paper includes, If someone fakes a sharing, the victim won't be able to decrypt the secret image or will think that the decoded fake image is the real one. If both participants in the 2-out-of-2 VCS are truthful, they can recover the real hidden image. To trick A into thinking the secret image is false, Share1+fakeshare exposes, a malicious participant can create a Fake Share if he knows details about Share1 that Participant A owns.

2. **A Common Method of Share Authentication in Image Secret Sharing:**

Image secret sharing (ISS) is receiving more and more attention due to the significance of digital images and their broad application to digital watermarking, blockchains, access control, identity authentication, distributive storage in the cloud, and other areas. In its actual implementation, share authentication is a crucial problem. An ISS with a separate common share authentication capability is discussed in this study and is appropriate for both dealer participatory authentication and dealer non-participatory authentication. To achieve the extra features of distinct share authentication, no pixel expansion, low encryption and decryption (authentication) complexity, lossless decryption, and auxiliary encryption, the designed ISS integrates the principles of polynomial and VSS. To demonstrate the benefits of our method, feature comparisons were made with similar schemes.

3. **A Novel Hierarchical Secret Image Sharing Scheme with Multi-Group Joint Management:**

The secret image would typically be encrypted into several shares and then stored in a cloud as part of the secret image-sharing method. But, if this cloud is assaulted, there is a chance that the secret will leak. The fact that the produced shares are distributed and stored across several clouds is a way to remedy the issue. Each cloud is autonomous, yet they can work together to manage the secret image. To overcome this issue, a method for distributed storage across multiple clouds that can protect the security of the secret image is proposed in this study. Many groups with various thresholds would each receive the secret image. A series of thresholds determines how many shareholders each group will have. In this hierarchical approach for sharing secret images, the secret image can only be recreated if the total number of shares satisfies all threshold requirements. Also, the produced shares all have the same weight, making them better suited for universal use.

4. **An Efficient (n, n) Visual Secret Image Sharing using Random Grids with XOR Recovery:**

While transmitting data (images) over the internet, security and ease of use must be taken into account. Encrypting data is one approach. Visual secret-sharing systems are an additional method. By its very name, visual cryptography relates to image-based cryptography. It is a subfield of cryptography that focuses on the encoding and decoding of visual data. By dividing an image into n shares, visual cryptography shows a visual secret-sharing system that can be used to decrypt the original image with little to no computational work. This study suggested employing random grids to create an effective (n, n) visual secret image-sharing mechanism. With the help of XOR stacking and this approach, a secret image can be fully retrieved without the use of a decoder. No pixel expansion occurs when using visual cryptography based on a random grid.

5. A secure Boolean-based multi-secret image-sharing scheme:

An (n, n) multi-secret image sharing scheme shares N secret images among N shared images. With this kind of technique, all n secret images can be recovered using n shared images, but if any shared image is lost, all secret images cannot be recovered. These covert strategies outperform other image-sharing methods since they just call for an XOR calculation. This paper proposes a safe Boolean-based secret image-sharing technique that creates a random image from shared or secret images using a random image-generating function. The random image generating function creates a random image to satisfy the random criterion by using a bit shift subfunction. To distribute or recover secret images, this approach only needs a small amount of CPU processing time. Nearly as much time is needed to transmit n secret images as it does to recover n secret images. More computation is required for the bit shift subfunction than for XOR.

6. A comparative study of Symmetric key algorithms DES, AES, and Blowfish: Cryptography is the science of protecting data and keeping information private and secure from unauthorized users. Encryption and decryption of data are done by using a secret key to provide data confidentiality, data integrity, and authentication. The process of transforming plaintext to ciphertext is called encipherment and the reverse process of transforming ciphertext to plaintext is called decipherment. Both the encipherment and decipherment processes are controlled by a cryptographic key. This paper analyzed the comparison of DES, AES, and Blowfish algorithms for video encryption and decryption considering certain parameters such as time and file size.

3. ALGORITHM

Security is the most important factor in the evaluation of cryptographic algorithms. Security encompassed features such as randomness of the algorithm output, security, key size, and speed as compared to other algorithms.

3.1 OVERVIEW OF THE ALGORITHM

DES:

In 1977, IBM developed the Data Encryption Standard, often called DES. The DES encryption process divides plaintext into two halves, and it uses a 64-bit plaintext and a 56-bit key to produce a 64-bit ciphertext, which is encrypted data. The key length of the DES algorithm is 56 bits, while the block size is 64 bits (the remaining 8 bits are checked bits). There are 16 rounds of identical procedures in DES, regardless of the length of the key. Due to the fixed number of operations in DES and the absence of permutation combinations, we are less likely to be able to break the encryption.

AES:

Vincent Rijmen and Joan Daemen created the symmetric key block cipher known as the Advanced Encryption Standard (or AES) in 2001. AES is used to encrypt sensitive data all around the world in hardware and software. AES is frequently utilized for sending data via computer networks, especially wireless networks. AES creates a 128-bit block from a 128-bit plaintext and a 128-bit secret key, which is then processed to yield 16 bytes (128 bits) of ciphertext. AES keys can have a length of 128 bits, 192 bits, or 256 bits, with 10 rounds (128 bits), 12 rounds (192 bits), or 14 rounds (256 bits). On the other hand, AES encryption, which has replaced DES as the de facto international standard, is more secure.

Blowfish:

Bruce Schneier designed the Blowfish algorithm to be a symmetric-key block cipher in 1993. The Blowfish algorithm uses a variable key size that can be anywhere between 32 and 448 bits. This allows for a high degree of flexibility and makes it possible to use Blowfish in applications that require different levels of security.

Below is the explanation of how the blowfish algorithm works

1. A key schedule with 18 32-bit subkeys is created from the 64-bit key.

2. The initialization of P and S, two 32-bit values, by the Blowfish algorithm is based on a predetermined string of hexadecimal digits.

3. A 64-bit block is used to partition the plaintext information.

4. A Feistel network with 16 rounds is used to encrypt each 64-bit block. The right half of the block is XORed with a subkey from the key schedule after being split into two 32-bit halves in each round. The key schedule also determines a set of four substitution boxes, or S-boxes, through which the result is then transmitted. The two 32-bit halves are then switched, and the procedure is again repeated.

5. The length of the resulting ciphertext is equal to the initial plaintext.

6. The same procedure is used to decrypt the ciphertext using the same key schedule and S-boxes but in reverse order.

3.2. EVALUATION METRICS

3.2.1 Encryption Time:

Encryption time is the time an encryption algorithm takes to convert plaintext data to ciphertext. It is an indicator of the efficiency of the algorithm. In the analysis, the encryption time is expressed in milliseconds and is taken into consideration when determining the encryption speed.

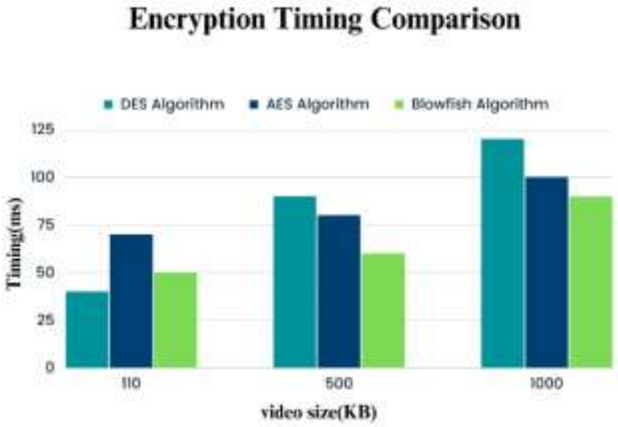

Figure 1: Shows the encryption time of DES, AES, and Blowfish algorithm

3.2.2 Decryption Time:

The time taken by an encryption algorithm to convert ciphertext data to plaintext data refers to decryption time. Lesser the decryption speed, more is the efficiency of the algorithm. Similar to how encryption time is measured in milliseconds, decryption time is likewise used to determine wireless network speed.

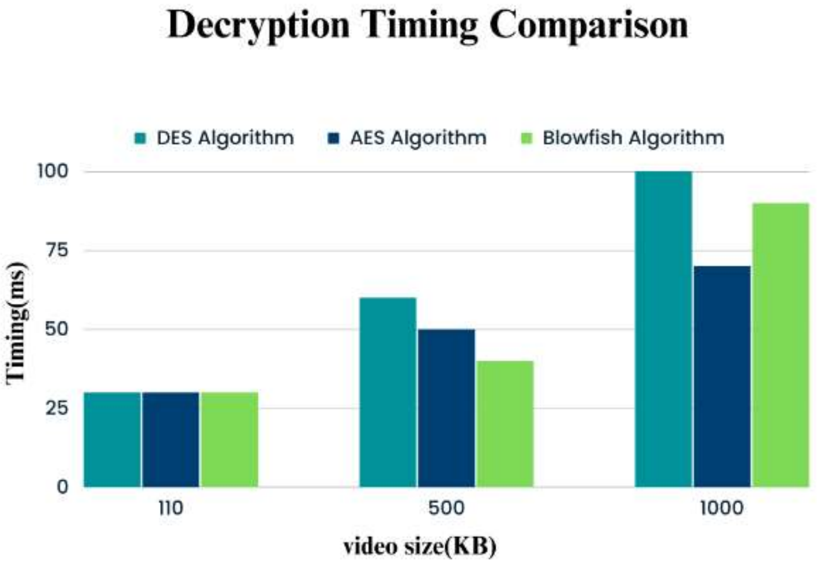

Figure 2: Shows the decryption time of DES, AES, and Blowfish algorithm

3.2.3 Throughput:

The throughput of a cryptosystem is defined as the megabytes of plaintext encrypted by the algorithm per millisecond. A greater throughput is indicative of a more efficient system. The unit of measurement is Mbps.

4. CONCLUSION

Illegal organizations and network viruses that steal digital information provide serious threats to information security. Thus, the security and privacy of information transmission have become particularly important, especially in the political, healthcare, military, and commercial fields. In this work, we have collected different schemes that are used in the shared creation of an image. In this study, we have established the share creation scheme that provides high security to the images. And also, various encryption algorithms are compared to provide additional security to the shares. In this study, we also provide a suitable algorithm that can be used by the user to encrypt and decrypt the image.

5. REFERENCES

[1] Denghui Zhang and Zhaoquan Gu, "A High-Quality Authenticatable Visual Secret Sharing Scheme Using SGX",2021

[2] Xuehu Yan, Yuliang Lu, Ching-Nung Yang, Senior Member, Xinpeng Zhang, and Shudong Wang," A Common Method of Share Authentication in Image Secret Sharing",2021.

[3] Zhen Wu, Yining Liu, and Xingxing Jia," A Novel Hierarchical Secret Image Sharing Scheme with Multi-Group Joint Management",2020.

[4] Ram Gopal Sharma and Dr. Hitendra Garg and Dr. Priti Dimri," An Efficient (n, n) Visual Secret Image Sharing using Random Grids with XOR Recovery",2019.

[5] Archisman Ghosh," Comparison of encryption algorithms: AES, Blowfish, and Twofish for the security of wireless Networks",2020.

[6] Pankaj Kumari, Manju Bala, Ankush Sharma," A comparative study of Symmetric key algorithm DES, AES and Blowfish",2019.

[7] Chien-Chang Chen and Wei-Jie Wu, "A secure Boolean-based multi-secret image sharing scheme",2015.