International Journal of Engineering Sciences & Emerging Technologies, Oct. 2023.
ISSN: 22316604 Volume 11, Issue 2, pp: 242-247 ©IJESET

A REVIEW: SECRET SHARING COUNTING BASED TECHNIQUES AND IT'S APPLICATIONS

Meenakshi Yadav[1], Varsha Sharma[2], Jayati Bhardwaj[3], Zoya[4]
[1,3]Asst. Prof., CSE Department,
MIT Moradabad, UP, India
[1]meenakshiyadav2309@gmail.com,[3]jayatibhardwaj2@gmail.com
[2] Asst. Prof., CSE Department,
KITPS Moradabad, UP, India
vs55840@gmail.com
[4] Student, CSE Department
KITPS Moradabad, UP, India
[4] saydzoya@gmail.com

ABSTRACT

Secret sharing counting based is a simple, flexible and secure technique that can be used to protect sensitive data. A secret can be dividing into multiple parts and distributing them among different parties. The SSCB technique ensure that no single party has access to the secret and that the secret can only be reconstructed if a certain number of parties collaborate. As such, secret sharing counting based scheme has become an important tool for individuals, organizations and government that need to protect sensitive information. Secret sharing counting based secret sharing is also relatively easy to implement and understand to other secret sharing schemes. This makes it a more accessible solution for many users, particularly those who may not have advanced cryptographic knowledge. This survey paper contributes to providing the review of existing procedures, comparisons, categorizing and applications.

KEYWORDS: *Secret sharing, access structure, threshold scheme, secret sharing applications, SSCB.*

1. INTRODUCTION

The history of secret sharing counting sharing is closely related to the history of threshold-based secret sharing. The threshold-based scheme was first introduced by Adi Shamir in 1979, who presented a method for splitting a secret into multiple shares and distributing them among participants [1]. The secret can be recreated only if a certain number of shares are combined. Secret sharing counting based technology is a variant of the threshold-based scheme that was proposed by S. Halevi and A. Shamir in 2002. In the threshold-based scheme, the secret is divided into n shares, and a minimum of t shares is required to reform the secret. In the counting-based scheme, the shares are assigned count values, and a minimum of t shares with a specific count value is required to reconstruct the secret [2]. The motivation for developing the counting-based scheme was to provide more flexibility in the distribution of secret shares. The secret counting based technology permit for a greater variety of access structures, where access is granted to participants based on their assigned count values. In today's digital age, data security has become a critical issue for individuals, organizations, and governments. Sensitive information such as personal data, financial records, and classified government documents need to be protected from unauthorized access, theft, or tampering. Cryptography is a technique that can be used to protect such data. Cryptography involves using mathematical algorithms to convert data into a secret code that can only be deciphered by those who have the key to unlock it. One area of cryptography that has received significant attention in recent years is secret sharing. Secret sharing is a technique that allows a secret

to be divided into multiple parts, which are then distributed among different parties. This ensures that no single party has access to the secret, and that the secret can only be reconstructed if a certain number of parties collaborate. One type of secret sharing scheme that has gained prominence is the SSCB scheme [3]. SSCB is a category of secret sharing scheme that is based on arithmetic operations. In secret sharing counting based, a secret is divided into multiple parts, and each part is assigned a value based on a pre-determined set of rules. These values are then distributed among different parties, who collaborate to reconstruct the secret. The most common form of secret sharing counting based is the (k, n)-threshold scheme, where k is the minimum number of parties required to reconstruct the secret, and n is the total number of parties [4].

2. FLOW CHART OF SECRET SHARING COUNTING BASED

In this flow chart secret is first divided into n parts, and each part is assigned a random value. The assigned values are then distributed among the n parties. To reconstruct the secret, at least k parties must collaborate and share their assigned values.

For example, let's say that a company wants to protect its financial records using a (3, 5)-threshold schemes. The company's financial records are first divided into five parts, and each part is assigned a random value. The assigned values are then distributed among five different parties, such as the CEO, CFO, and three board members. To reconstruct the financial records, at least three parties must *collaborate* and share their assigned values.

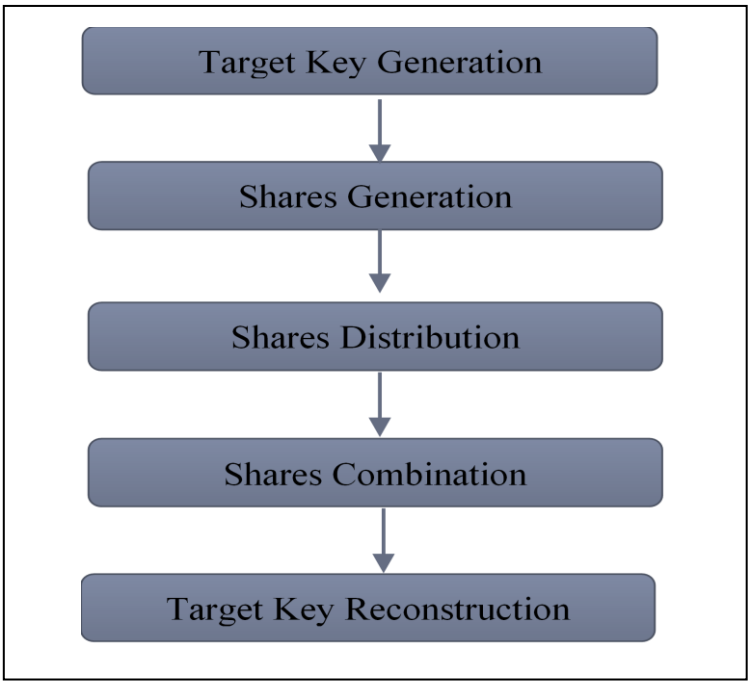

Figure 1. Flowchart of secret sharing counting based

3. ADVANTAGES OF SECRET SHARING COUNTING BASED

Secret sharing counting based has several advantages over other kinds of secret sharing schemes.

A. First, secret sharing counting based is simple and easy to understand. Unlike other schemes that involve complex mathematical operations, secret sharing counting based involves basic arithmetic operations that can be easily understood by anyone with a basic understanding of mathematics.
B. Second, secret sharing counting based is highly secure. Since the values assigned to each part of the secret are randomly generated, it is virtually impossible for an attacker to guess the

assigned values and reconstruct the secret without collaborating with the required number of parties.

C. Third, secret sharing counting based is highly flexible. The (k, n)-threshold scheme can be adapted to suit different requirements by adjusting the values of k and n. For example, a company that wants to protect highly sensitive data may choose a (5, 7)-threshold schemes, while a company that wants to protect fewer sensitive data may choose a (2, 4)-threshold schemes.

4. LITERATURE REVIEW

Taghreed M. Alkhodaidi, Adnan A. Gutub, [5] the research paper titled "Scalable shares generation to increase participants of secret sharing counting based technique" proposes a novel method for generating scalable shares in SSCB scheme. The proposed method is designed to increase the number of participants who can access the shared secret in an efficient and secure manner. In secret sharing scheme can change the ownership of the target key among participants by assigning part of the target to each of them. Thus, participants cannot reconstruct the target key when they lose some of these parts. When share keys are being created, the dealer can determine one of them to be necessary to reconstruct the target key. The authors introduce the concept of secret sharing counting based, which is a variant of the threshold-based secret sharing technology. The SSCB allows for the secret to be divided into multiple shares, each assigned to a different participant, and each share is associated with a count value. To retrieve the secret, a minimum number of shares with a specific count value must be gathered.

The authors introduce a novel approach of appending parity bits (either a series of 0's or 1's to Target key (TK). The most important part about this approach is the dynamic approach, by simply padding the bits and changing single bit each time to generate a share key. For example, let's say a Target is 110011 then first share key could be: 111011, second share key could be: 110111, third one would be: 11001100000, fourth would be 11001110000 and so on. Hence one problem of scaling can be addressed. But as the authors were able to solve one problem, another problem of "security" makes its way, since it is easier to now guess the process and ultimately the target keys. To improve the overall security one approach suggested by authors is to append larger parity bits (>10 bits). This will thus increase the overall time to crack a share key or series of share keys. The second way is to randomize the process a bit. For example, appending series of 0's or 1's and changing at least 2 bits randomly and then applying bitwise operations like and or a modulo operator to recreate the target key.

Adnan Gutub, Taghreed Alkhodaidi, [6] The research paper "Smart expansion of target key for more handlers to access multimedia secret sharing counting based" proposes a method to improve the efficiency and security of multimedia secret sharing counting based schemes. Multimedia SSCB is a method for distributing a secret message among a group of participants, where each participant receives a share of the secret. The secret can only be rebuilt when an appropriate number of shares are combined together, and the combination threshold can be customized based on the specific requirements of the application.

The proposed method in the paper involves expanding the target key, which is used to encrypt the secret message before it is distributed. By expanding the target key, more handlers can access the secret message without compromising its security. The expansion is achieved using a Random Number Generator or in simple terms RNG. The authors proposed to have half bits of the target key as a part of the target key while the other half is produced using RNG. The random number produced must have at least one zero else the system discards the number and again recreates the random part. If the random number produced has a low number of zeros, that means zeros are not enough for all participants, the half size of the target key bits become modified. These improved bits of the target key have additional zeros helping to create as many share keys as possible.

Following is an example for expansion of the target key (TK):

RNG= 1111 1101

Block of Zeros (Z)= 0000 0000

TK1= 0000 0000 1111 1101 (Add zeros at first)

TK2= 1111 1101 0000 0000 (Add zeros at last)

TK3= 1111 0000 0000 1101 (Add zeros in the middle)

TK4= 1010 1010 1010 1010 (Skip 1 bit and add 1 zero)

TK5= 1100 1100 1100 0100 (Skip 2 bits and add 2 zeros and vice versa)
As one can imagine many numbers of combinations are possible. Hence the problem of expansion is solved here. To evaluate the randomness authors made use of the following tests by NIST 800-22 standard.
Frequency test: This method counts the number of zeros and ones in the sequence.
Frequency test within a block: This method divides the entire sequence into blocks and then calculates the number of ones and zeros
Runs test: The purpose of this test is to make sure that the sequence of binary digits is not too repetitive or too predictable, which could indicate that it is not random.
The paper presents a detailed analysis of the security and efficiency of the proposed method and compares it to other existing systems. The proposed technique outperforms existing methods in terms of security and efficiency, making it a promising solution for multimedia secret sharing counting based technology.
Adnan Abdul, Aziz Gutub, [7] Watermarking is a method used to insert a single identifier or signature into digital content, such as images or videos. The embedded identifier can be used to track the distribution and usage of the content and to identify the original owner or creator of the content.
The proposed method in the paper uses secret sharing counting based, which is a technique for splitting a secret message into multiple shares that can be distributed amongst different participants. The secret message in this case is the watermark that is embedded into the digital video content. The method allows for "fractional invalidation", which means that if the watermark is found to be compromised in a portion of the video, only that portion needs to be invalidated, rather than the entire video. This reduces the impact on the legitimate use of the video and allows for more targeted and efficient invalidation. The paper addresses the current watermarking challenge where ownership proof needs to be addressed whenever slight tampering occurs in the video file. CBSS is simply used for this watermarking as identity proofing data-bits scheme. At time of verification, these embedded secret bits are recollected again forming the shares, which are combined providing possible regeneration of the owner password. In other term, as the owner password is semi-verified, the watermarking is proving that the copyright claim as authentic work, announcing the percentage of suitable ownership situation. The authors showcase the effectiveness and trade-offs between 1-LSB, 2-LSB and 3-LSB techniques (least significant bit)
The authors propose to first convert the video file to binary and use SSCB system target key. Then the system produces shares as watermarking stream bits which are then embedded to the video file. The authors also proposed that the embedding process can be done partially and not for all video frames. To verify the watermark one can, compare the shares with the target key. The percentage of verification allows the application and user to either accept or refuse them. In summary, the paper proposes a method for protecting the copyright of digital video content through watermarking using secret sharing counting based. The method allows for fractional invalidation, which reduces the impact on the legitimate use of the video. The proposed method is shown to outperform existing methods in terms of security and efficiency, making it a promising solution for digital video watermarking.
Adnan Gutub, Maimoona Al-Ghamdi, [8] Steganography is a technique for hiding secret messages within other non-secret data, such as images in the proposed method, steganography is used to hide the shares of the secret message within images. This enhances the security of the proposed scheme by making it more strong and less prone to the attacker identification. The paper presents a detailed analysis of the security and efficiency of the proposed method and done comparison with the existing methods. In the paper the authors use a 1 bit/2-bit method to create a secret share preserving the security. The shares are hidden within LSB of the image using steganography technique. This done to find out the maximum share's opportunities with different length so that share security can be increased. The paper tries to relate between different steganography approaches according to the factors of the security, the robustness and the capacity. Standard measures, such as histogram, peak signal to noise ratio (PSNR), and bit per pixel (bpp) are used to evaluate the security, robustness and capacity respectively.
The outcomes show that the proposed method outperforms existing methods in terms of security and efficiency, making it is a best solution for improving the security of secret sharing counting based schemes. In summary, the paper proposes a method for improving the security and efficiency of image/data security using steganography and SSCB. The method involves hiding the shares of the secret

message within images, which enhances the security of the scheme by making it more difficult for attackers to identify and retrieve the shares.

Faiza Al-Shaarani, Adnan Gutub, [9] The research paper "Securing matrix counting-based secret-sharing involving crypto steganography" explores the combination of two security techniques: matrix counting-based secret-sharing and cryptographic steganography. The purpose of this combination is to enhance the security of data transmission and storage in cloud computing environments. Matrix secret-sharing counting-based is a method of distributing a secret message across multiple shares, where each share contains a subset of the secret message. The shares are generated using a matrix counting algorithm, which involves counting the number of ones in each row and column of a binary matrix. To reconstruct the secret message, a minimum number of shares must be combined using a threshold scheme.

Cryptographic steganography involves hiding a secret message within an innocuous-looking carrier message, such as an image or audio file. The carrier message is modified in a way that is imperceptible to the human eye or ear but can be decoded by a recipient who knows the encryption key. The research article proposes a combination of these two techniques, where the shares generated by the matrix counting-based secret-sharing technique are embedded within a carrier message using cryptographic steganography. The resulting stego-image or stego-audio file can then be transmitted or stored in a cloud computing environment with a higher level of security than either technique alone. The authors of the paper also propose a novel approach for selecting the threshold value in the matrix secret-sharing counting based scheme. This approach involves using a genetic approach to optimize the threshold value based on the desired level of security and the available computational resources.

5. APPLICATIONS OF SECRET SHARING COUNTING BASED

- **A. Multimedia content protection:** Secret sharing counting based can be used to protect multimedia content such as images, audio, and video from unauthorized access. The secret can be shared among a group of authorized users, and the content can be accessed only when a minimum number of shares with a specific count value are gathered.
- **B. Cloud computing:** Secret sharing counting based can be used to protect delicate information in cloud computing environments. The secret can be shared among multiple cloud servers, and the data can be accessed only when a minimum number of shares with a specific count value are gathered.
- **C. Cryptography:** Secret sharing counting-based can be used to create secure cryptographic keys that are shared among multiple parties. The key can be accessed only when a minimum number of shares with a specific count value are gathered.
- **D. Access control:** Secret sharing counting-based can be used to control access to delicate information in a distributed system. The secret can be shared among multiple nodes, and the data can be accessed only when a minimum number of shares with a specific count value are gathered.
- **E. Secure voting:** Secret sharing counting based can be used to implement secure voting systems. The secret can be shared among voters, and the votes can be accessed only when a minimum number of shares with a specific count value are gathered.

6. CONCLUSIONS

Secret sharing counting based is a powerful cryptographic technique that allows for the sharing of a secret message between groups of participants. The method has several advantages over other secret sharing schemes, including its simplicity, efficiency, and flexibility. Secret sharing counting based can be used in a variety of applications, including cloud sharing, watermarking, and digital rights management. One of the key benefits of secret sharing counting based is its flexibility. The scheme allows for customization of the combination threshold, which determines how many shares are required to reconstruct the secret message. This means that the combination threshold can be adjusted based on the specific requirements of the application, allowing for a fine balance between reliability and efficiency. Another benefit of secret sharing counting based is efficiency. The method requires only a small number of cryptographic operations to generate and distribute the shares, making it an efficient

solution for many applications. In addition, the shares can be generated and distributed in parallel, further improving the efficiency of the scheme. Despite its many benefits, secret sharing counting based is not without its limitations. The scheme relies on the assumption that the participants in the sharing scheme are honest and will not collude to retrieve the secret message. In addition, the scheme is vulnerable to certain types of attacks, such as side-channel attacks. Overall, secret sharing counting based is a powerful cryptographic technique that offers a flexible, efficient, and accessible solution for secure message sharing. With continued research and development, secret sharing counting based has the potential to be applied in a wide range of applications, from cloud sharing to digital rights management and beyond.

7. FUTURE WORK

One area of research where secret sharing counting based can be used is cloud computing. SSCB or secret sharing counting based can be used to improve the scalability of parallel computing and distributed systems. Specifically, the research could investigate how the use of parallel and distributed computing can enable the secret sharing counting based technique to handle larger amounts of data more efficiently and with lower computational costs. Cloud computing involves breaking down a computational task into smaller sub-tasks that can be executed concurrently on multiple processing units. In the context of secret sharing counting based, parallel computing could be used to distribute the computation of shares and reconstruction of the secret message across multiple processing units, thereby reducing the overall computation time. One could potentially develop a highly scalable countingbased secret-sharing scheme that can handle large amounts of data efficiently and with low computational costs. However, there are also challenges associated with this approach, such as ensuring consistency and integrity of the shared data across systems and managing the communication and coordination between multiple processing units. Overall, exploring the use of cloud computing in secret sharing counting based has the potential to significantly enhance the scalability of the scheme in cloud computing applications, enabling it to handle larger amounts of data and support more users with lower computational costs.

REFERENCES

[1] A. Shamir. How to share a secret. Communications of the ACM, 22:612–613, 1979.
[2] G. R. Blakley, “Safeguarding cryptographic keys”, Proc. of AFIPS National Computer Conference, vol. 48, pp. 313-317, 1979.
[3] A. Gutub, N. Al-Juaid, E. Khan, “Secret sharing counting based Technique for Multimedia Applications”, Multimedia Tools and Applications, Springer, pp. 1-29, 2017.
[4] Zahra Ahmadian, Sadegh Jamshidpour, “Linear Subspace Cryptanalysis of harn’s Secret Sharing-Based Group Authentication Scheme”, IEEE Transactions on Information Forensics and Security, pp. 502 – 510, September 2017.
[5] Taghreed M. Alkhodaidi, Adnan A. Gutub,” Scalable shares generation to increase participants of counting- based secret sharing technique “, International Journal of Information and Computer Security Volume 17 Issue 1-2, pp 119–146,2022.
[6] Adnan Gutub, Taghreed Alkhodaidi,” Smart expansion of target key for more handlers to access multimedia secret sharing counting based”, multimedia tools and applications, vol. 79, pages17373–17401, 2020.
[7] Adnan Abdul, Aziz Gutub, “Adopting counting-based secret-sharing for e-Video Watermarking allowing Fractional Invalidation”, multimedia tool and application, pages 9527–9547, February 2022.
[8] Gutub, Adnan, Al-Ghamdi, Maimoona, “Image Based Steganography to Facilitate Improving Secret sharing counting based”, 3D Display Research Center, Kwangwoon University and Springer-Verlag GmbH Germany, part of Springer Nature, 2019.
[9] Faiza Al, Shaarani, Adnan Gutub, “Securing matrix counting-based secret-sharing involving crypto steganography”,Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 9, Pages 6909-6924, October 2022