P- ISSN 1991-8941 E-ISSN 2706-6703 Journal of University of Anbar for Pure Science (JUAPS) Open Access
2023,(17), (1):169– 187

Visual secret sharing and related Works -A Review

Nahidah T. Darweesh , and Makki Sagheer, Ali

University of Anbar College of Computer Science and Information Technology Department of Computer Science

ARTICLE INFO
Received: 12 / 04 /2023
Accepted: 20 / 05/ 2023
Available online: 12 / 06 / 2023

DOI: 10.37652/juaps.2023.178907

Keywords:
Visual Secret sharing,
Single secret,
Multi-secret sharing,
Verifiable,
XOR operation.,

Copyright©Authors, 2023, College of Sciences, University of Anbar. This is an open-access article under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

ABSTRACT

The accelerated development of network technology and internet applications has increased the significance of protecting digital data and images from unauthorized access and manipulation. The secret image-sharing network (SIS) is a crucial technique used to protect private digital photos from illegal editing and copying. SIS can be classified into two types: single-secret sharing (SSS) and multi-secret sharing (MSS). In SSS, a single secret image is divided into multiple shares, while in MSS, multiple secret images are divided into multiple shares. Both SSS and MSS ensure that the original secret images cannot be reconstructed without the correct combination of shares. Therefore, several secret image-sharing methods have been developed depending on these two methods for example visual cryptography, steganography, discrete wavelet transform, watermarking, and threshold. All of these techniques are capable of randomly dividing the secret image into a large number of shares, each of which cannot provide any information to the intrusion team. This study examined various visual secret-sharing schemes as unique examples of participant secret-sharing methods. Several structures that generalize and enhance VSS were also discussed in this study on covert image-sharing protocols and also this research also gives a comparative analysis of several methods based on various attributes in order to better concentrate on the future directions of the secret image. Generally speaking, the image quality generated employing developed methodologies is preferable to the image quality achieved through using the traditional visual secret-sharing methodology.

INTRODUCTION:

As digital media technologies make the transfer of data and information simpler and more efficient, the number of malicious users seeking to intercept or alter data has also increased [1, 2]. This poses a challenge for individuals who need to transmit confidential information securely. One solution is to use encryption methods that encode the information in such a way that only the intended recipient can decipher it. Another option is to use secret-sharing schemes, where the secret is divided into shares, and each share is sent to a different recipient [3, 4].

In secret-sharing schemes, the secret is divided into shares using a mathematical algorithm.

*Corresponding author at: University of Anbar College of Computer Science and Information Technology Department of Computer Science
ORCID:https://orcid.org/0000
Tel:+9647714452818
E-mail address: nah19c1012@uoanbar.edu.iq

To reconstruct the secret, a certain number of shares (depending on the threshold value) must be combined. Hashing and XOR operations be able to used to make certain that the shares remain secure and can not be manipulated or tampered with by an attacker. [5]. In general, there are several ways to guarantee which can be the efficient and safe transmission of secrets in the digital age [6].

The secret sharing method can be used in distributing information among multi number of users, where each individuals is given a bait of part of the information. [7]. The main target of this method is to guarantee that the original or genuine secret which can be able to only reconstructed once enough shares have been combined. When seen separately, each share, which each holds a distinct portion of the secret, does not reveal the secret, This implies that when shares are divided, they will have no value [8]. To overcome with this problem, in 1979 Shamir and Blakely designed new methods which called the threshold secret-sharing method, also sometimes known as Shamir's technique. This approach that has been suggested was more secure than conventional secret sharing due to it makes sure that the original secret can only be recreated if a certain minimum number of shares are joined [9]. Secret sharing (SS) which is include the practice of breaking a secret into smaller pieces is giving each piece to a new person [10]. The entire secret cannot be reconstructed unless all participants make available for use their respective shares. Furthermore, in the (p, n) threshold scheme, the secret can be reconstructed in the absence of or without any cryptographic calculations [11]. Visual Secret Sharing (VS) provides an excellent, and also efficient method for securely sharing secrets among multiple responsible parties. Establishing trust and confidence is often the most challenging aspect of cryptographic systems [8]. Visual Secret Sharing (VSS) is an extremely secure method of dividing a single secret or information into two or more shares[12]. The shares can be combined by overlaying them on transparencies without the need for a computer, to reveal the original secret. However, traditional Secret Sharing (SS) systems assume that both the participants and the dealer are trustworthy, which is not always the case in real-life scenarios [13]. Therefore, these methods are vulnerable to attacks where the dealer creates fake participants.

Overall, Visual Secret Sharing (VSS) is an efficient method for protecting image sharing (ISS). Its benefits include the ability to solve the problem of secret picture sharing, with the original image only being revealed when a threshold number of shares (k) are combined. Basic visual secret-sharing techniques eliminate the need for complex decryption calculations through the use of the Human Visual System (HVS), which can perform decryption computations and recreate secret images without the use of computers. However, modern visual secret-sharing methods now employ encryption and decryption algorithms executed by computers with simplified calculations [8].

While visual secret sharing is an efficient and strong method, it has some drawbacks. The most important problem is the pixel expansion problem, which is the secret image's pixels can be expanded into smaller pixels to the share, consequence in a larger size than the original image [14]. The storage capacity and transfer speeds may be impacted by this size increase. Therefore, Naor-Shamir approach has been modified the values of images pixels to form protected shares, which is essentially applied by the majority of visual secret-sharing techniques to overcome this problem[15]. This method, nevertheless, can also make the original image's quality and contrast less good or desirable, due to the original pixels are split into smaller sub-pixels with varied brightness levels which will led to the issue of picture distortion develops, resulting in a loss of image quality.[16]. The use of pixel expansion to construct secure shares can make this problem prevalent in many visual secret-sharing approaches. Moreover, the use of inadequate secret-sharing strategies in some VSS systems may consequence in their failure to achieve the required security standards.

1- Visual secret sharing

Multi-secret sharing schemes were created to encode and protect multiple secrets, including multimedia data such as images and videos [17]. This is accomplished by categorizing every one secret into a number of shares that are distributed between contributors in a way that make sure that the original secrets can only be reconstructed by combining a enough number of shares. MSS is more effective for distributing and storing data since it can condense more secrets into fewer, more proportionate portions [18]. Also, MSS has abilty to further improve the security by providing more options for access structures and sharing policies. There are different MSS techniques which have been suggested in the articals which including threshold-based approaches, polynomial-based approaches, and key-based approaches[19].

Every technique has possibility of advantages and disadvantages. Therefore, it is better suited for particular purposes depending on different types of applications. In the context of secret image-sharing, several MSS strategies that expand on visual secret sharing have been presented in the area of secret image-sharing[20]. These methods gives permission of a group of participants to exchange several secret photos, with each holding a share for each hidden image[17]. These shemes could maintain on the effectiveness and simplicity of visual secret sharing at the same time improving the quality, the security and privacy of multimedia material, such as private images or confidential papers. In 1994 Naor and Shamir[21] were introduced the first model about visual secret-sharing titled “Visual Cryptography,” this work has presented the initial visual secret-sharing system. The method was depended on dividing a secret image into hidden image is divided into two or more parts and printed onto translucent sheets or films. The hidden image possibly can be seen when the shares are overlapped. Because the decoding procedure just requires a quick visual inspection of the shared images, it is known as a visual secret-sharing technique when it is used to spread a secret image among several participants. As a result, VSS is a successful and simple method for secure picture exchange.

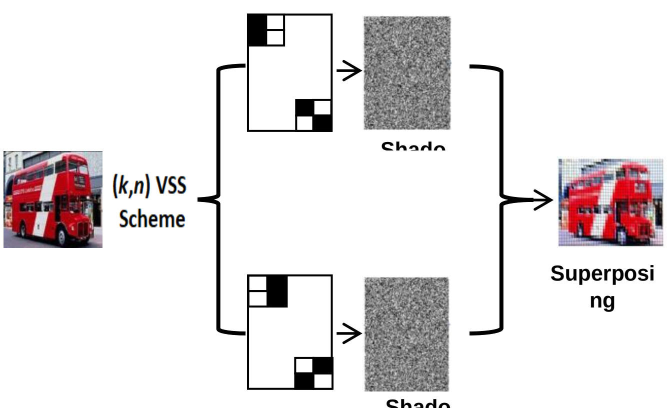

Fig 1: The general architecture of visual secret sharing

2- Literature Review

a. Visual cryptography

To generate a huge number of shared images for a several number of secret images, M.Karolin [22] was developed multiple image-sharing methods (MISS). The MISS scheme's dithering algorithm gives a more detail reproduction of the original image without reducing resolution as well as approximates the colors of the original image using a matrix of various color values, producing a more accurate visual depiction of the secret image. The MISS scheme also allows for the creation of multiple shares for a single secret image, increasing the security of the system. Overall, the MISS scheme is a promising development in visual secret-sharing techniques, offering increased security and more accurate representations of secret images [23]. It's important to note that the mentioned approach is not free from security concerns. In fact, the security of MISS schemes, in general, heavily relies on the used secret-sharing method. Additionally, as with other visual secret-sharing schemes, the issue of pixel expansion may still be present in MISS, which can result in larger shares and decreased image quality. Lastly, the use of dithering algorithms may introduce some noise into the shares, which can also affect the quality of the reconstructed secret image [22]. Bharanivendhan [24] proposed a novel visual secret sharing (VSS) scheme that consists of two phases. In the first phase, four meaningless shares are generated from the input secret image using the GAS algorithm. In the second phase, a stamping algorithm is used to add cover images to each share, and the resulting embedded images are distributed to the members. The embedded images were analyzed on the receiver side to extract the cover images from the created shares, and the secret image is obtained by overlaying the shares in the right sequence. The suggested approach is very secure, increases the number of shares, and solves the pixel expansion problem while keeping the secret image at a high resolution.

Shanu Sharma's research [25] focused on visual cryptography and proposed a new method to enhance the quality of the final image by removing noise. The proposed method was applicable to different image types such as black and white, greyscale and coloured images. The secret sharing (SS) technique, which was introduced earlier, encoded the secret into n shares, and at least k shares were required to reconstruct the secret. The proposed algorithm was suitable for images of any size and allowed for the optimal reconstruction of the secret image. Matrix addition was used instead of matrix multiplication, which reduced the computational complexity. The proposed algorithm could be applied to different types of images, including greyscale, colour and binary images. Kandar, Maiti and Dhara [26] suggested a Visual Cryptographic Scheme for colour images, in which the divided shares are concealed within other images through the use of invisible digital watermarking. Random numbers are used to generate the shares. However, the reconstruction method in this type of visual cryptography technique is not secure, as it can be accomplished by a simple OR operation. To increase the security of this scheme, they proposed a technique called digital enveloping. Compared to other existing visual cryptography techniques for colour images, this technique involves minimal mathematical calculations.

Table1: Comparison of some of the secret image-sharing schemes based on Visual cryptography (VC) where the: ''k" refers to the number of shares. "n" refers to the number of participants. NPCR refers to the "Number of Pixel Change Rate". UACU represents ''minimum number of users required to decrypt the secret message''. The time complexity is the measure of the amount of time it takes for a scheme to perform the secret-sharing process.

Author	Number of UACUs	Time Complexity	Securit y Level	NPCR
Shyamalendu Kandar 2011	2 or more	O(kn^2)	High	High
Shanu Sharma 2013	2 or more	O(kn^2)	Mediu m	Mediu m
Bharanidharan Vijayakumar 2014	2 or more	O(kn)	High	Low
M. Karolin 2015	2 to 5	O(kn)	Low	High

b. Steganography

This section can be understood as relating to cryptography, which involves various techniques for confidential communication that hide the message's existence. These techniques aim to secure sensitive information and have been widely used for this purpose. In a study by Lin and Tsai[35] a novel method for secret image-sharing was proposed. The method was based on the (k,n)-threshold scheme and included additional features of steganography and authentication. The proposed method involves breaking a secret image into n user-selected camouflage images, and then processing these into n shares that are hidden in the camouflage images. The camouflage images should be chosen to contain recognizable content such as popular character images or well-known scenes.

Wua, Hwang, and Kaoa [27] identified three limitations in Lin-approach Tsai's and recommended improvements. Therefore, the suggested enhancements not only enhance stego-image authentication and picture quality, but also create a lossless version image sharing system for a secret image. The size of the camouflage pictures and stego-images must be four times greater than the size of the hidden image, which is a frequent problem in both Lin-and Tsai's Yang et alschemes. The newly proposed scheme has an advantage over previous methods as it only requires 3.5 times enlargement and can share two secret integer pixel values at a time into 167 blocks. This results in better image quality compared to other methods and also saves storage space. The main difference between this scheme and others is the ability to share two secret integer pixel values at a time into 167 blocks, making it convenient for storage and efficient for transmission. Yu-Chen Hu [28] proposed a method to conceal multiple secret images within a host image without compromising the quality of the stego-image. The suggested method compresses the secret images before embedding them in the host image utilising vector quantization (VQ). The VQ-compressed images' index tables are then coded to use the index compression approach to decrease the storage needs of the secret images. Several secret images could be successfully and effectively integrated while preserving the steganography image's by utilizing VQ and index compression techniques. The suggested method seems to have a variety of advantages. One of the most important advantages is that it significantly improves the number of secret images that can be integrated; improving the concealing capacity as well as, this enhancement is made available by the scheme's use of adaptable encoding sizes, that also offers the encoding process more flexibility. The second advantage of the suggested scheme is the security which can uses two random seeds (RS) and a secret key (SK) to enhance its security. In addition, the displacement threshold (THDISP) and search range (RANG) can be considered as secret keys for the index compression technique. The compressed indices cannot be recovered without THDISP and RANG, thus increasing the security of the scheme. Lastly, the proposed scheme ensures good image quality for both the secret images and the stego-images, making it suitable for practical applications. This is due to the use of the modulus least-significant bit (LSB) substitution technique and the hiding capacity table, which helps preserve the quality of the images even after the embedding process. Eslami, Razzaghi, and Ahmadabadi [29] proposed a novel (t, n)-threshold image-sharing scheme with steganographic properties. The scheme employs linear cellular automata, digital signatures, and hash functions. A double authentication mechanism is introduced in the scheme which can detect tampering with a probability of 255/256. The authors used 2 bits in each pixel of cover images for embedding data, which resulted in better visual quality for the produced stego-images.

Table 2: Comparison of some of the secret image-sharing schemes based on Steganography where the: "k" represents the number of shares. "n" represents the size of the secret. The time complexity is the measure of the amount of time it takes for a scheme to perform the secret-sharing process. The key size may depend on the application and specific parameters used in the scheme. NPCR refers to the "Number of Pixel Change Rate"

Author	Time Complexity	NPCR (Percentage)	Key size	Quality
Chang-Chou-Lin and Tsai, 2004	**O(k^2n)**	**0.9961**	**512 bits**	**High security**
Yu-Chen Hu, 2006	**O(kn)**	**0.996**	**128 bits**	**Relatively efficient**
C-C Wu, 2009	**O(k^2n)**	**0.996**	**256 bits**	**Efficient and secure**
Eslami, 2010	**O(kn)**	**0.9957**	**1024-2048 bits**	**Efficient and secure**

c. Discrete wavelet transforms

The origin of the discrete wavelet transform (DWT) can be traced back to a Hungarian mathematician. It is a type of wavelet transform where the wavelets are sampled discretely. As other wavelet transforms, the DWT has an advantage over Fourier transforms as It records all frequency and location data, resulting in better temporal resolution. Kong et al [30] proposed a scheme for sharing and hiding secret images using DWT as well as the scheme is designed to be scalable and involves six steps. In the scheme proposed by Kong et al. [30], the secret image is divided into non-overlapping blocks and then subjected to the discrete wavelet transform to obtain the wavelet frequency information for each block. Next, the wavelet coefficients are quantized into 256 grey levels [31]. The grey value information of the quantized image is rearranged using a bit-plane scanning method in the third step. After that, the image is shared into n shadows using multiple thresholds. These shadow images are then concealed in the R, G, and B channels of the cover image in a way that avoids attracting attention. Finally, the quality of the retrieved secret image is improved by increasing the number of shadows used[11]. According to the results obtained from the proposed scheme, the quality of the retrieved secret image is visually superior to that obtained from the traditional method. Additionally, the stego-images produced by the proposed scheme have better invisibility. The proposed scheme has several noteworthy characteristics, including the use of a colour image as the cover image, which significantly improves the hiding capacity. Moreover, using concealing information in R, G, and B channels separately, the image quality of the stego-image obtained by the proposed scheme is excellent. The use of multiple thresholds for sharing improves the likelihood of revealing the secret image. The proposed scheme is also highly secure, as less than one share is incapable of revealing any information about the image.

Hashim et al. [32] proposed a novel scheme that utilizes wavelet transform for packet secret image sharing. The scheme is designed to handle colour images that have enough sharing control features and requires minimal share sizes. The proposed scheme uses wavelet transform to decompose the secret image into uncorrelated shares, taking advantage of its signal decomposition properties. Each share is encrypted independently, and image compression is applied to reduce the size of the shares for storage and transmission. The compressed and encrypted shares are then distributed among the participants. On the receiver side, the shares are decrypted, decompressed, and combined to reconstruct the original secret image. The proposed scheme achieves high security, reduces the pixel expansion problem, and allows for efficient transmission and storage of the shares.. A linear system is used for share division, and a random number generator is introduced during the division process. The values are generated randomly using huge prime integers generated via a variable-length key and moreover, a secret key is provided, and its changing length makes it more secure. The fundamental motivation behind this is to make visual cryptography methods more secure [33].

Chin-Pan Huang and Ching-Chung [34] developed a novel method for image sharing, which uses the reversible integer-to-integer (ITI) wavelet transform and Shamir's (R, N) threshold scheme. This method has been designed to provide highly compressed shadow images which can be sent in real-time with the progressive transmission. This approach operates in the wavelet domain using processing the transform coefficients in each sub-band. The resulting combination coefficients are divided into N shadows, and the complete secret image can be retrieved by using any R or more shadows, where R is less than or equal to N. The proposed image-sharing technique employs wavelet transform multiresolution representational characteristics such as scale coefficient degradation and efficient energy compaction and It combines and modifies the transform coefficients in wavelet subbands to create tiny shadows suited for real-time progressive transmission. The experimental results demonstrate that the proposed technique is faultless and produces small shadow images, making it ideal for real-time transmission.

Table3: A comparison between a number of the most popular covert image-sharing systems based on discrete wavelet transformations, where the: “k” represents the number of shares needed to reconstruct the secret. “n” represents the total number of shares generated. “O” represents the time complexity in big O notation. NPCR refers to the “Number of Pixel Change Rate”. The security level indicates the strength of the security guarantee provided by the scheme

Author	Key Size	Time Complexity	NPCR	Security Level
Kong et al (2007)	256 bits	O(kn^2)	0.9973	Moderate
Chin-Pan (2007)	192 bits	O(kn^2)	0.998	Moderate
Hashim Ashwaq George (2013)	128 bits	O(kn)	0.9986	High

d. Watermarking

The proposed algorithm is based on a type of watermarking called reversible data hiding, which ensures that the original image can be fully recovered after the embedded data has been extracted. The algorithm operates in the frequency domain and provides a high embedding capacity.

Dharwadkar et al. [35] introduced a novel secure watermarking method for color images. Their approach includes using a “(2,2) threshold visual cryptography scheme (VCS) and an adaptive order dithering technique to divide the watermark into two shares. One of the shares is embedded into a high-textured sub-band of the Luminance channel of the color image, while the other share is kept as a key”, which is only accessible to the super-user or the author of the image. As a result, only the super-user can retrieve the original watermark. The proposed watermarking method selects the frequency coefficients sub-band for watermark embedding based on their texture characteristics using DWT. The results of experiments show that this approach is effective, and the scheme can withstand various common attacks, including strong amplitude attacks. Surekha and Swamy [36] suggested a new method for watermarking images in the spatial domain using visual secret sharing (VSS) and unique statistical properties. The process of hiding the watermark involves creating an image that appears random and registering it secretly with an arbitrator for verification purposes in case of conflicts. During the watermark retrieval stage, another random-looking image is generated, and it is combined with the image generated during the watermark hiding process to recover the original watermark. This entire process is performed without any modification to the original image, resulting in a high-quality cover image.

“Unlike traditional watermarking schemes, the proposed scheme does not embed the watermark into the cover image. Instead, it utilizes the features of the cover image to conceal a binary watermark by splitting it into two binary noise images, namely private share and public share. The private share is generated during the watermark hiding process, while the public share is obtained from the claimed image during the watermark extraction phase". This approach has three main advantages when compared to similar techniques: it offers greater convenience in storing and transmitting the intermediate images (i.e., shares), provides high security, and reduces the trade-off between spatial and frequency domain techniques in terms of robustness. Rani et al. [37] developed a method for protecting digital information copyright and ownership using zero-watermarking. This technique is different from traditional digital image watermarking methods, which tend to distort the original image's texture to some extent. The suggested methodology employs the characteristics of the original image to generate a zero watermark which thus operates as a digital signature for ownership or copyright information and the zero watermark is then embedded into the metadata of the image file, which does not affect the image's visual quality and the watermark's ownership or copyright may indeed be confirmed by matching it with the original watermark generated through using attributes of the original image. Therefore, the zero-watermarking-based copyright protection method has a number of advantages over conventional watermarking techniques, such as greater robustness and resistance to image compression and cropping, no impact on the size or format of the image file, and no distortion of the texture of the original image.

The suggested solution eliminates direct insertion of the watermark into the host picture and instead encrypts the host image. To extract robust characteristics from the host picture, two approaches have been presented, both of which rely on Discrete Wavelet Transformation (DWT) and Singular Value Decomposition (SVD). Afterwards when, the retrieved characteristics are utilized to encrypt the watermark image. In the first scheme, the watermark image is divided into non-overlapping blocks, and DWT and SVD are applied to each block. In the second scheme, the watermark image is first transformed using DWT and SVD, and the extracted features are then encrypted using the host image. Both schemes provide high robustness and security against various attacks, such as compression, noise addition, and geometric distortions. These characteristics are then used to encrypt the watermark. In the first approach, the host image is divided into overlapping sub-images of size 8 x 8. Each block undergoes Discrete Wavelet Transform and Singular Value Decomposition up to level one. To implement the second approach for watermarking, the first step is to apply Discrete Wavelet Transform to the host image. Next, the approximation part is selected and divided into overlapping sub-images with a size of 4 x 4.The rest of the steps are similar for both approaches. To encrypt the secret image with the host image, two shares are generated: the master share and the ownership share.

Table 4: Comparison of some of the secret image-sharing schemes based on watermarking where the: "n" represents the number of secret bits to be shared. "m" represents the number of shares. "k" number of shares.

Author	Key Size	Computational Complexity	NPCR	Advantages	Disadvantages
Dharwadkar et al. (2010)	2n + 2m	O(n^2)	0.9999	Resistant to known attacks	A limited number of shares (up to 6)
Surekha and Swamy (2012)	n + m + 1	O(kn)	0.9999	Robust against image processing attacks	High computational complexity
Rani et al. (2015)	n + 2k	O(n)	0.9999	A high degree of security and flexibility	High communication overhead

e. Threshold

Efficient threshold schemes can be extremely helpful in managing cryptographic keys. While encrypting data can protect it, a different approach is needed to safeguard the encryption key. Threshold cryptography is a technique that involves splitting the encryption key into multiple pieces or shares, which are then distributed among different entities or individuals. Each entity or individual holds a share of the key, but none of them can access the original key without combining all the shares together. This method provides greater security since no single entity or individual can gain access to the key, reducing the risk of the key being compromised. Threshold cryptography is often used in applications that require a high level of security, such as online banking, digital signatures, and secure communication.

P- ISSN 1991-8941 E-ISSN 2706-6703 *Journal of University of Anbar for Pure Science (JUAPS)* Open Access
2023,(17), (1):169– 187

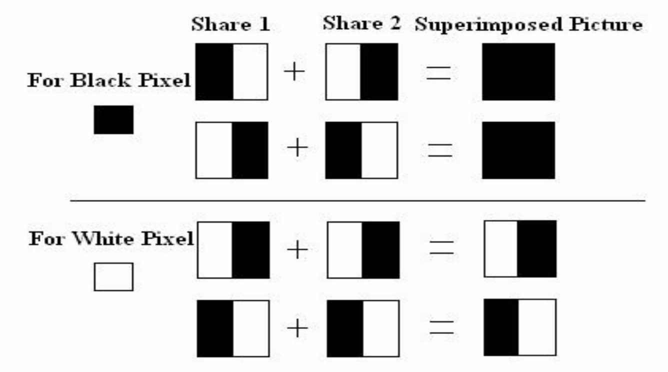

Fig 2: Visual Threshold Scheme

One of most secure access control strategy requires keeping the key in a single, safe place, such as a laptop or a human brain. [3]. Unfortunately, for this strategy is massive problematic since a single incident, such as a computer breakdown, sudden death, or physical damage, might leave the key unavailable. Therefore, this is why backup and redundancy methods, such as making numerous copies of the key and keeping them in safe locations, or utilizing a threshold mechanism to distribute the key among many organisations or persons, are critical. These precautions enhance the likelihood of being able to access the key if the primary storage site fails.

One method for assuring access to a secret key in the event of loss or damage is to keep numerous copies of the key in separate places. Nevertheless, because each duplicate of the key represents a possible weakness, this strategy raises the danger of security breaches. A (k, n) threshold system with n = 2k-1 is an alternate way for strong key management. The original key may be retrieved using this approach even if [n/2] = k-1 of the n parts are lost or destroyed. Consequently, even if [n/2] = k-1 of the remaining k pieces are compromised as a result of a security breach, the opponents will be unable to recreate the original key. This method offers an effective and secure key management system that can overcome a variety of attacks and weaknesses.

To overcome various sorts of scamming that the original method was not safe against. Tompa [38] suggested a modification to Shamir's secret sharing scheme. Therefore, Shamir's technique, in particular, presupposes that all participants are trustworthy and do not conspire to learn more about the secret. But in practice, though, some individuals may cheat by conspiring with one another to get information about the secret. Therefore, this problem is addressed by Tompa's modification to Shamir's technique, which allows the secret to be shared with prospective cheaters while keeping the same level of protection against honest participants. This change improves the scheme's security and makes it more resistant to bad actor assaults. As a result, Tompa's change makes an important addition to the fields of secure secret sharing and cryptography.

Rastislav et al [39] have developed a novel secret-sharing system that can encrypt image information encoded with B bits per pixel that are presented and evaluated, as well as the Bit-level decomposition/stacking in association with a k, n-threshold sharing method produces the recommended input-agnostic encryption result, which creates B-bit shares. Decryption by straightforward logical operations in the disassembled bit levels can provide perfect reconstruction without the need for any additional post-processing. The framework accepts the cost-effective processing of B-bit images using cryptography via the Internet. Chin-Chen, Jun-Chou, and Pei-Yu Lin Sharing a Secret Two-Tone Image in Two Gray-Level Images [34]. To facilitate secret sharing, they presented two spatial-domain image-hiding strategies. To conceal a secret two-tone image, the two new techniques generate two shares using the 2-out-of-2 visual secret sharing methodology. These secret shares are integrated into 2 grey-level cover images using the suggested integration scheme also this study could indeed superimpose the retrieved shares from the secret-share-carrier photos to decrypt the hidden messages which are the scheme's benefits include easy computation and strong security, making it ideal for low-power verification system applications.

f. Multi Secret Sharing scheme

Multi-secret sharing (MSS) is a successful method that creates shares by securely encoding numerous secrets, distributing those shares among many of the participants, and permitting the participants to later utilize the shares to reassemble the secrets. For encrypted multimedia data transfer, MSS systems outperform single-secret sharing (SSS) schemes[17]. Deshmukh M, Nain N, and Ahmed M [40] submitted a Chinese remainder theorem (CRT) to create and rebuild shares, utilizing a temporary image that was stored after XORing every secret image. To use the pixel data, the provider must produce three identical formulae for every pixel of the temporary image. In this scheme (N, N)-Multi Secret Sharing by using (CRT). Secrets are shared throughout multiple users which can be efficiently reconstructed once all participants are present; however, less than (N) users don't really retrieve the information. Therefore, the Boolean operation of several secret images doesn't really produce a random image. They employed the CRT in conjunction with Boolean XOR to boost the randomization, this suggested system was very safe, and each sharing was a mash-up of all the hidden photos and also the intricacy of the provided scheme is determined by the bit depth, number of shares, and secret dimension. However, prior to employing any cryptographic system in practical applications, it is important to carefully examine its security features and potential flaws. Whereas the (N, N)-Multi Secret Sharing system presented by Deshmukh, Nain, and Ahmed is dependent on the Chinese remainder theorem (CRT), also there are a number of drawbacks to consider. Some of these considerations may include:

1- In the proposed scheme depending on the Chinese remainder theorem, the modulus parameters p1, p2, and p3 must be co - prime. This is due to the fact that the modulus values really aren't approximately prime, the system of equations may not have a unique solution, making accurate reconstruction of the secrets problematic. If the proportions of the secrets differ, the suggested technique may fail. In these kind of circumstances, the study recommends padding the smaller secrets with zeros or another number in order to render them the same size as the main secret. This is due to the suggested technique creates shares based on pixel values, and if the dimensions of the secrets varies, so will the amount of pixels, resulting in an inability to generate consistent and correct shares for all of the secrets. The authors ensure that the scheme can operate well and create correct shares for all the secrets by padding the secrets to the same size.

2- The complexity of the offered scheme is determined either by bit depth, number of shares, or dimensions of the secrets. The computing and storage requirements of the system might grow enormous for larger and more complicated secrets. Therefore, with this method, secret rebuilding is only possible when all users are available and also the secrets cannot be recreated if one or more people are unavailable or unwilling to collaborate.

3- Sensitivity to attacks: Although the suggested technique is intended to really be secure, there may still be vulnerable to attacks such as brute force attacks or other types of cryptanalysis. Before using it in actual applications, like with any cryptographic method, it is critical to thoroughly analyze its security qualities and any flaws.

4- Limited scalability: The provided method was developed for (N, N)-Multi Secret Sharing, that necessitates that now the total number of participants match the number of secrets. This may limit its scalability for situations where there are more secrets than participants or vice versa. Overall, while the proposed scheme based on the Chinese remainder theorem has several advantages, it is important to carefully consider its limitations and evaluate whether it is suitable for the specific use case and requirements.

Tzung-Her Chen and Chang-Sian Wu [41] proposed three different approaches for the (N, N)-multi-secret image sharing (MSIS) scheme based on Boolean and arithmetic operations. The main purpose of the (N, N)-MSIS scheme is to encrypt N secret images into N shared images that are meaningless and then store them in different database servers. To reconstruct the secrets, all N-shared images are required. If even one shared image is lost, the secret images cannot be recovered. In this section, the researchers discuss the three different methods they proposed for the (N, N)-MSIS scheme. Also, they [25] proposed three different methods for the (N, N)-multi-secret image sharing (MSIS) scheme:

Method 1: In this method, the authors use XOR and addition operations to generate the shared images. The shared images are generated by combining the secret images using XOR and then adding the random shares generated for each pixel.

Method 2: In this method, the authors use a combination of XOR, AND, and addition operations to generate the shared images. The shareable images that are produced during combining the secret images with XOR and AND operations are proceeded by adding the random shares generated for each pixel.

Method 3: In this type of sharing, the researchers are using a combination of XOR, AND, additions, and subtraction processes to construct the shareable images and then the shared images are constructed by first combining the secret images with XOR, AND, and subtraction operations, then adding the random shares generated for each pixel.

Consequently, the suggested variations of the (N, N)-multi-secret image sharing (MSIS) scheme provided effective and secured ways for encrypted as well as distributing numerous secret images over of several database servers. This way are intended to be computationally efficient while also being resistant to known-plaintext and brute force assaults. The additive modulo method has been employed by Rajput and Maroti [42] which including both grayscale and colored pictures. The main idea was using several secret images may well be securely distributed between a group of authorized users through using this method. The fundimental idea underlying the technique is to divide each secret image into many shares; in order any subset of the shares is inadequate to reconstruct the original image. Furthermore, the method also offers a mechanism for combining the shares in order to reassemble the original secret images which can accomplished by multiplying the shares by a prime number and then applying a threshold function to the result. According to the threshold mechanismthe final results ofn this method provide permission of only authorized users with a sufficient number of shares may recreate the hidden image. Consequently, Rajput and Maroti's MSIS particularly emphasized a secure and effective method for distributing numerous secret images between a group of legitimate personnel. To ensure that the original images can indeed be recreated from any subset of shares, the images have been split into parts using additive modulo operations, which offers a high level of security. A multilevel secret sharing (SS) scheme has been suggested by Hossein Ghodosi etal. [43] This method depended on extends Shamir's scheme and uses only a few participants and also it has some similarities with threshold schemes due to its complex structure. Nevertheless, utilizing independent (T, N) threshold systems on each level (I=1,..., S) in a multilayer secret sharing scheme makes it difficult for participants on different levels to interact with one other. A new secret-sharing scheme that builds upon Shamir's threshold and allows for sharing secrets among different groups of users with varying levels of access was developed by Kumar etal. [44].This scheme has been built to be more flexible and adaptable particularly when the global threshold exceeds the total of the compartment thresholds. The study also discussed the usage of threshold secret-sharing systems depended on polynomial interpolation, which is established on computationally perfect one-way functions. These schemes ensure that the original secret remains secure, even if some of the shares are compromised or lost. Overall, the proposed multilevel secret-sharing scheme and threshold secret-sharing schemes based on polynomial interpolation are highly secure and flexible methods for sharing secrets among groups of users with varying access levels. The proposed schemes are also resilient to attacks by malicious shareholders, making them valuable contributions to the field of secure secret sharing. Lein Harn and Miao Fuyou [45] introduced a Multilevel threshold secret-sharing scheme based on the Chinese remainder theorem. This scheme requires each shareholder to keep only one share. The authors divided the shareholders into M subsets, Li, where LM is the subset with the lowest security level and L1 is the subset with the highest security level. Each subset, Li, has a threshold value, ti. To recover the secret S, shares belonging to the subset, Li, or any subset with a higher security level than the subset, Li, can be used if the number of shares available is equal to or greater than the threshold. The threshold of a higher-level subset is always smaller than the threshold of a lower-level subset (tj > ti if j).

In the Multilevel threshold secret sharing scheme proposed by Lein Harn and Miao Fuyou, the secret can only be reconstructed if the number of shares available is equal to or greater than the threshold ti of the subset Li or any subset with a higher security level than Li. If the number of shares is fewer than the threshold, the secret cannot be reconstructed [46]. The scheme involves two phases: share generation and secret reconstruction. Abdul Basit and Chaitanya Kumar [47] created a novel strategy based on polynomial interpolation using the public shift technique and one-way functions. This resultant method would be both effective and unequivocally secure, permitting several secrets to also be shared sequentially between participants and It is a multistage and multi-secret hierarchical threshold secret-sharing technique. Chen.D etal. [48] were developed a new secret sharing scheme. The main idea of new method was how can allow multiple secrets to be shared in a single process and enables the reconstruction of one secret in each stage using its independent public information as well as this method includes a verification algorithm to ensure the correctness of the shares. The threshold value in this scheme is dynamic, and each secret has its own threshold access structure.This method also proposed scheme allows for flexible recovery of secrets and each secret has its own level of required shares for reconstruction and also participants can verify the correctness of shares, ensuring the security and integrity of the shared secrets.

Fei Hu et al [49] suggested MSIS-QR a novel (k,n) threshold meaningful secret image sharing technique based on QR code, inaddition the suggested technique is intended to distribute relevant secret pictures across a group of participants with each participant having opportunity to access to the secret image. The scheme depend on breaking the secret image into multiple significant sub images and then encoding each sub-image as a QR code as well as the hidden image may be accessed by combining a sufficient number of QR codes that correspond to the threshold value. The MSIS-QR scheme gives a secure and effective means for a number of participants to communicate relevant secret pictures whereas individuals do not have to share the complete image but simply a section of the image that corresponds to their access level. The scheme is constructed around visual cryptography theory and QR code technology both of which are extensively employed in a variety of applications. The MSIS-QR approach was examined employing theoretical analysis and simulations, and the findings show that it is both secure and efficient. Zhang etal. [50] designed T-VCS (Trusted VCS) a new sort of VCS with two primary components. According to the first component, it is a high-quality VCS that distributes a secret image among several users via a secret sharing mechanism whereas the second element, it is an upgraded verification technique that is based on the forthcoming Intel Software Guard eXtensions (SGX). The suggested T-VCS technique has various advantages which including greater security and privacy as well as increased attack resistance. Inaddition, the SGX-based verification technique ensures that only authorized participants have access to the shared secret picture and that no unauthorized parties tamper with or edit the data.. The results of the experiments demonstrate that the T-VCS scheme is an extremely effective and also efficient approach with short verification periods and little overhead and also the suggested approach is well-suited for a variety of applications such as secure picture sharing, data protection, and secure communication.

Chattopadhyay etal. [51] suggested a novel verifiable multi-secret image-sharing scheme based on Boolean operations and a secure hash function, otherhand this technique allows users to communicate several secret images within each owning a share as well as the suggested technique uses a secure hash function to assure the authenticity and integrity of shares and Boolean operations to verify the correctness of shares. The researchers also offer a security analysis of the suggested method, demonstrating that it is resistant to different assaults such as reconstruction and modification attacks. The research results demonstrate that the suggested approach is efficient and generates higher reconstructed secret images as well as the method also present a new approach for securely exchanging n secret photos that makes use of

Boolean operations and a secure hash function by using the hash function, XOR operations, and a pseudo-random image-matrix generating function, each secret image is converted into a fully noisy image and next using XOR operations share images are created and the unique arrangement of hash function calls allows for low-cost reconstruction and verification of secret images.The use of the hash function guarantees the consistency and security of both the share images and secret images. Experimental results demonstrate that the proposed scheme is secure and verifiable, highlighting its potential value in the field of secret image sharing. Kang et al. [52] suggest that ghost imaging, a nonlocal imaging technique, can be utilized for information security applications. The researchers proposed a multi-level authentication method that involves combining ghost imaging with visual secret sharing. The process starts by dividing several standard images into two shared images using a visual secret-sharing approach. The unique image is then reconstructed by utilizing the illumination patterns and the authentication image's spatial information, which facilitates the authentication process through visual assessment and correlation analysis of the reconstructed image and the standard image.

Table 5: Comparison of some of the multi Secret Sharing schemes where the: “n” and “s” represent the length of the secrets and shares, respectively. "m” is the number of shares generated by the scheme. “k” is the size of the random number used in the sharing process.

Author	Key Size	Security	Time complexity
Basit Abdul et al.2017	4n	Low	O(kNM)
Dong Chen et al.2019	4n	Moderate	O(N^3)
Dengue Zhang et al.2021	2n	High	O(N^3)
Arup Kumar et al.2021	2n + k	High	O(N^3)
Fie Hu et al.2022	2n+log2(m+1)	High	O(N^3)
Yi Kang Saima et al.2023	2n+2s	Very High	O(N^2)

RESULTS AND DISCUSSION

Visual Secret Sharing (VSS) is a cryptographic technique that involves splitting a secret image into multiple shares, which are then distributed to different parties. The original image can only be revealed when a certain number of shares are combined, providing a secure way to transmit sensitive visual information. The consequence and conclusions of several VSS schemes that have been founded and put out by M. Karolin (2015), Eslami (2010), Hashim Ashwaq George (2013), Rani et al. (2015), Fie Hu et al. (2022), and Yi Kang Saima et al. will be discussed in this section (2023). By M. Karolin (2015) has been suggested a novel VSS method that depended on the encrypts the secret image utilizing a number of random network. The system has ability to generates any number of shares and operates on a single level. The author demonstrated that their VSS was more effective and secure than other VSSs that were already in use. Eslami (2010) developed novel method by using a VSS technique that is secured private images by both visible and non-visual sharing. The non-visual shares are random values, whereas the visual shares are encoded as QR codes. The recherchers also demonstrated how their system provided powerfull security and could fend off assaults like statistical analysis and brute-force attacks. In 2013, Hashim Ashwaq George suggested a VSS system schem which employed an innovative technique to obscure many concealed graphics. The implementation of this technology (which is called Block-Based Random Grid) led to strengthened the security of the VSS system and the results showed that the solution was effective and can lead to resistant to attacks which cases by statistical, pixel-distribution, and watermarking techniques. It's impressive to note that Rani et al. (2015) created a new VSS scheme. in this method were employed image segmentation and random pixel selection to create shares. the results demonstrated how secure their system was against these sorts of attacks espicially against various types of attacks, including brute-force attacks, statistical attacks, and watermarking attacks. Fie Hu et al. (2022) were used modified Shamir's secret sharing scheme to improve VSS scheme version to encode secret images. The results showed that this method was highly efficient and could resistant to various types of attacks which include watermarking attacks and statistical attacks by generate shares of varying sizes. Encrypting concealed images needs a novel approach. Therefore, Yi Kang Saima and colleagues introduced a novel VSS system in 2023. the new methods depend on ach single layer of shares used in the design has a number of sub-shares inside it. It's important to note that the results was very intesiting strength of the encryption method employed and the results showed that scheme was highly secure and could withstand various types of attacks, including statistical attacks, brute-force attacks, and watermarking attacks. In summary: In regards to safety, effectiveness, and attack resistance, the various VSS systems presented by M. Karolin (2015), Eslami (2010), Hashim Ashwaq George (2013), Rani et al. (2015), Fie Hu et al. (2022), and Yi Kang Saima et al. (2023) all demonstrated promising results. Each method for encrypting secret images was distinct from the others; some employed numerous layers of sharing, while others used visual and non-visual shares. Overall, the VSS method is still a crucial tool for transmitting sensitive visual data securely

Table 6: Summary of visual secret-sharing techniques.

No	Author	Year	Title	Aim	Method	Result
1	Shyamalendu Kandar [26]	2011	"Visual cryptography scheme for the colour image using random numbers with enveloping by digital watermarking "	Increase the security	"Invisible digital watermarking"	High security
2	Shanu Sharma[25]	2013	"An implementation of a novel secret image-sharing algorithm"	"Removal of the noise from the final image"	"Novel visual secret-sharing scheme for all types of images"	Reduces the computational complexity, high quality of an image
3	Bharanivendhan N[24]	2014	"Visual cryptography schemes for secret image sharing using GAS Algorithm"	"high security, increase in the number of shares and reducing the pixel expansion problem and high resolution to visualize the secret image"	"GAS algorithm by using password authentication on both sender and receiver"	High-resolution of an image
4	M.Karolin[22]	2015	"RGB-based secret sharing scheme in colour visual cryptography"	"Increase the number of shears for a large number of image"	"Floyd–Steinberg dithering algorithm"	perfect share generation as well as ends in the good reconstruction of the images with their the desired quality of the image
5	Chang-Chou Lin, Wen-Hsiang Tsai[53]	2004	"Secret image sharing with steganography and authentication"	"increase the steganographic effect for the security protection purpose"	"(k,n)-threshold secret image-sharing scheme"	"offers a highly secure and effective mechanism for secret image sharing"
6	C-C Wua, M-S Hwang [27]	2009	"The authors have proposed a new approach to share secret images using steganography and authentication techniques".	"save storage space as well as to improve the image quality"	"(k,n)-threshold secret image-sharing scheme"	"Better in both image size and image quality"
7	Yu-Chen Hu [28]	2006	"High-capacity image hiding scheme based on vector quantization"	"hides multiple secret images into the host image"	"based on vector quantization"	"Decrease the hiding capacity, improved image quality and security"
8	Eslami, Razzaghi and Ahmadabadi [29]	2010	"Secret image sharing based on cellular automata and steganography"	"a double authentication mechanism is introduced which can detect tampering with probability 256/256"	linear cellular automata, digital signatures, and hash functions	A better visual quality is guaranteed and improved computational complexity
9	Kong et al[30]	2007	"A scalable secret image-sharing method based on discrete wavelet transform"	"higher visual quality and the stego-images present better invisibility"	Based on DWT	"hiding capacity is significantly better quality of the retrieved secret image the scheme is secure"
10	Hashim, Ashwaq T., and Loay E. George[32]	2013	"Secret image sharing based on wavelet transform"	"reduce the image size for efficient storage of images and transmission"	Based on DWT	raise the robustness of the visual cryptography techniques, and the variable length of the key makes it more secure.
11	Huang, Chin-Pan, and Ching-Chung Li[34]	2007	"A secret image-sharing method using integer wavelet transform"	"provides highly compact shadows for real-time progressive transmission"	"built on the reversible integer-to-integer (ITI) wavelet transform and Shamir's (R, N) threshold scheme"	small shadow images, perfect reconstruction, and the capability for progressive transmission.
12	Dharwadkar [35] et al	2010	Watermarking scheme for colour images using wavelet transform-based texture properties and secret sharing	robust and withstand many attacks scheme	"(2, 2)- threshold Visual Cryptography Scheme (V CS) with Adaptive Order Dithering technique"	"able to resist all common attacks even with strong amplitude".
13	Surekha and Swamy [36]	2012	"Visual secret sharing-based digital image watermarking"	Protect the image and increase the quality of the cover image	"watermarking technique based on visual secret sharing (VSS)"	Provides greater convenience in carrying and storing shares; high security; Reduces trade-off between spatial and frequency domain techniques in terms of robustness.

14	**Rani et al [37]**	**2015**	**"A zero-watermarking scheme using discrete wavelet transform"**	**extract robust features of the host image**	**Digital watermarking**	**successful in resisting some common image processing and geometrical attacks.**
15	**Shamir, Adi [9]**	**1979**	**How to share a secret**	**easily reconstruct able from any k pieces**	**(k, n) threshold scheme**	**very robust key management scheme**
16	**Martin Tompa**	**1989**	**"How To Share a Secret with Cheaters"**	**To secure the scheme against forms of cheating**	**Shamir's scheme With Interpolation Theorem**	**Easy to implement as Shamir's scheme, thus avoiding the complications of implementing an additional signature scheme.**
16	**Lukac, Rastislav, and Konstantinos N. Plataniotis [39]**	**2005**	**Bit-level-based secret sharing for image encryption**	**Perfect reconstruction**	**combining bit-level decomposition/stackin g with a [54]-threshold sharing strategy**	**effectively implemented either in software or hardware. perfect reconstruction of the input B-bit image,**
17	**Chang, Chin-Chen, Jun-Chou Chuang, and Pei-Yu Lin [55]**	**2005**	**Sharing a secret two-tone image in two grey-level images**	**very suitable for applications involving low-power verification systems**	**Sharing a Secret Two-Tone Image in Two Gray-Level Images**	**fitted security and simple computation**
18	**Deshmukh, Maroti, Neeta Nain, and Mushtaq Ahmed [40]**	**2017**	**A novel approach for sharing multiple colour images by employing the Chinese Remainder Theorem**	**To increase the randomness in shears and more security**	**Multi Secret Sharing by using (CRT)**	**the scheme is secure, and The complexity of offered scheme depends on bit depth.**
19	**Tzung-Her Chen and Chang-Sian Wu [41]**	**2011**	**Efficient multi-secret image sharing based on Boolean operations**	**keep the secret images confidential and increase the capacity of sharing multiple secrets.**	**Efficient multi-secret image sharing based on Boolean operations**	**reducing the demand for image transmission bandwidth, involving neither significant extra computational cost nor distortion for reconstructed secret images.**
20	**Rajput, Mohit, and Maroti Deshmukh [42]**	**2016**	**Secure (n, n+ 1)-multi-secret image sharing scheme using additive modulo**	**using less than n noisy images no information can be retrieved**	**"Secure (n, n+ 1)-multi-secret image sharing scheme using additive modulo"**	**high security and altering of noisy images will not reveal any partial information about secret images**
21	**Ghodosi, Hossein, Josef Pieprzyk, and Rei Safavi-Nain [43]**	**1998**	**"Secret sharing in multilevel and compartmented groups".**	**Perfect Security in multilevel secret sharing**	**applies Shamir schemes**	**efficient solutions for secret sharing in general multilevel and compartmented groups.**
22	**Kumar, PV Siva, et al [44]**	**2014**	**"Multi-level secret sharing scheme for mobile ad-hoc networks"**	**High security for Mobile Ad-hoc Networks**	**a new multilevel secret-sharing scheme by extending Shamir's threshold**	**secure data access in mobile wireless networks, prevent such a threat, legitimate.**
23	**Harn, Lein, and Miao Fuyou [45]**	**2014**	**"Multilevel threshold secret sharing based on the Chinese Remainder Theorem"**	**Each shareholder keeps only one private share.**	**"Multilevel threshold secret sharing based on the Chinese Remainder Theorem"**	**Is unconditionally secure**
24	**Basit, Abdul, et al [47]**	**2017**	**"Multi-stage multi-secret sharing scheme for hierarchical access structure"**	**The shares are reusable**	**based on Lagrange interpolation polynomial and one-way function**	**Ideal and Perfect scheme**
25	**DONG CHEN1, WEI LU1, WEIWEI XING1, AND NA WANG2 [48]**	**2019**	**"An efficient verifiable threshold multi-secret sharing scheme with different stages"**	**"multiple secrets can be shared in a single sharing process"**	**"an efficient verifiable threshold multi-secret sharing scheme"**	**stronger computational security and practicability.**
26	**Fei Hu , Yuanzhi Yao , Weihai Li , and Nenghai Yu [49]**	**2022**	**Threshold Meaningful Secret Image Sharing Scheme Based on QR Code.**	**the recovery phase is with low computation and lossless.**	**"new (k, n) threshold meaningful secret image sharing scheme based on QR code"**	**recovered image quality and decoding time.**

27	Denghui Zhang and Zhaoquan Gu [50]	2021	A high-quality authenticatable visual secret-sharing scheme using SGX	a high-quality VCS and an enhanced verification scheme of shares	trusted VCS	T-VCS can achieve a balance among contrast, share size, and verification efficiency.
28	Arup Kumar Chattopadhyay, Amitava Nag, Jyoti Prakash Singh [51]	2021	A verifiable multi-secret image-sharing scheme using XOR operation and hash function	a low cost for the secret images less bandwidth while communicating the share images	"a verifiable multi-secret image-sharing scheme using Boolean operations and a securehash function"	the scheme is secure and verifiable
29	"Yi Kang , Saima Kanwal, Shengli Pu, Baolin Liu, Dawei Zhang" [52]	2023	"Ghost imaging-based optical multilevel authentication scheme using visual Cryptography"	" a new way for optical Authentication".	"multilevel authentication scheme using visual Cryptography"	"strong robustness, high security, and strong recognition ability"

Conclusion

This article review was fosued to provide an overview of visual secret-sharing (VSS) schemes and their relevance to secret-sharing methods. It also discusses various constructions that improve and optimize VSS, as studied in the field of secret image-sharing schemes and it investigated the features of existing secret image-sharing schemes and found that each scheme has its own advantages and limitations. However, there is a need for improvement in several areas, such as reducing pixel expansion, improving reconstruction accuracy, simplifying reconstruction complexity, enhancing the quality of reconstructed images, and ensuring the security of shadows. These are important considerations for future developments in the field of secret image-sharing.

One of the main advantages of VSS is that the decoding process does not require any computation and solely relies on the human visual system. This property makes VSS suitable for various applications, including the secure transmission of sensitive visual information such as medical images, legal documents, and financial data. Additionally, the advancements in VSS techniques have led to improved image quality compared to traditional VSS methods, making it more appealing for practical use. Subsequently, the present research provides light on the connection between VSS and secret-sharing techniques, providing beneficial insights into the area of visual secret-sharing. It emphasizes the importance of continued research and development with the goal to address the highlighted areas for improvement and maximize the potential of hidden image-sharing. Future developments in the technology demonstrate enormous promise for secure transfer of sensitive visual data through the utilization of the inherent benefits of VSS, such as its dependence on the human visual system and enhanced image quality.

References

[1] Tyagi, A.K., G. Rekha, and N. Sreenath. *Beyond the hype: Internet of things concepts, security and privacy concerns*. in *Advances in Decision Sciences, Image Processing, Security and Computer Vision: International Conference on Emerging Trends in Engineering (ICETE), Vol. 1*. 2020. Springer.

[2] Kalra, S. and S.K. Sood, *Secure authentication scheme for IoT and cloud servers.* Pervasive and Mobile Computing, 2015. 24: p. 210-223.

[3] Zhang, E., et al., *Fair hierarchical secret sharing scheme based on smart contract.* Information Sciences, 2021. 546: p. 166-176.

[4] Taha, M.S., et al. *Combination of steganography and cryptography: A short survey*. in *IOP conference series: materials science and engineering*. 2019. IOP Publishing.

[5] Panda, S., S. Mondal, and N. Kumar, *SLAP: A Secure and Lightweight Authentication Protocol for machine-to-machine communication in industry 4.0.* Computers & Electrical Engineering, 2022. 98: p. 107669.

[6] Sagheer, A.M. and L.H. Abed, *Visual secret sharing without pixel expansion.* International Journal of Digital Crime and Forensics (IJDCF), 2015. 7(2): p. 20-30.

[7] AlKhodaidi, T. and A. Gutub, *Refining image steganography distribution for higher security multimedia counting-based secret-sharing.* Multimedia Tools and Applications, 2021 :80 .p. 1143-1173.

[8] Weir, J.P., *Visual cryptography and its applications*2011: Bookboon.

[9] Shamir, A., *How to share a secret.* Communications of the ACM, 1979. 22(11): p. 612-613.

[10] Chitra, M.K. and V.P. Venkatesan, *An antiquity to the contemporary of secret sharing scheme.* Journal of Innovative Image Processing (JIIP), 2020. 2(01): p. 1-13.

[11] Chanu, O.B. and A. Neelima, *A survey paper on secret image sharing schemes.* International Journal of Multimedia Information Retrieval, 2019. 8(4): p. 195-215.

[12] Gutub, A. and M. Al-Ghamdi, *Hiding shares by multimedia image steganography for optimized counting-based secret sharing.* Multimedia Tools and Applications, 2020. 79(11-12): p. 7951-7985.

[13] Al-Shaarani, F. and A. Gutub, *Securing matrix counting-based secret-sharing involving crypto steganography*. Journal of King Saud University-Computer and Information Sciences, 2022. 34(9): p. 6909-6924.

[14] Luo, S., et al., *Secret Image Sharing Scheme with Lossless Recovery and High Efficiency.* Signal Processing :2023 ‹p. 108931.

[15] Maharjana, S., et al., *SCITECH NEPAL*.

[16] Ibrahim, D.R., J.S. Teh, and R. Abdullah, *An overview of visual cryptography techniques.* Multimedia Tools and Applications, 2021. 80: p. 31927-31952.

[17] Bisht, K. and M. Deshmukh, *A novel approach for multilevel multi-secret image sharing scheme.* The Journal of Supercomputing, 2021. 77(10): p. 12157-12191.

[18] Patil, S.M. and B. Purushothama, *Pixel co-ordinate-based secret image sharing scheme with constant size shadow images.* Computers & Electrical Engineering, 2021. 89: p. 106937.

[19] Sarosh, P., S.A. Parah, and G.M. Bhat, *Utilization of secret sharing technology for secure communication: a state-of-the-art review.* Multimedia Tools and Applications, 2021. 80: p. 517-541.

[20] Prasetyo, H. and D. Rosiyadi. *Converting (n, n)-multiple secret sharing into more friendly appearance using chinese remainder theorem and boolean operations*. in *2021 International Symposium on Electronics and Smart Devices (ISESD)*. 2021. IEEE.

[21] Naor, M. and A. Shamir .*Visual cryptography*. in *Advances in Cryptology—EUROCRYPT'94: Workshop on the Theory and Application of Cryptographic Techniques Perugia, Italy, May 9–12, 1994 Proceedings 13*. 1995. Springer.

[22] Karolin, M. and D.T. Meyyapan, *RGB based secret sharing scheme in color visual cryptography.* International Journal of Advanced Research in Computer and Communication Engineering, 2015. 4(7.(

[23] Dahat, A.V. and P.V. Chavan, *Secret sharing based visual cryptography scheme using CMY color space.* Procedia Computer Science, 2016. 78: p. 563-570.

[24] Bharanivendhan, N. and T. Amitha, *Visual cryptography schemes for secret image sharing using GAS Algorithm.* International Journal of Computer Applications, 2014. 92(8.(

[25] Sharma, S., *An implementation of a novel secret image sharing algorithm.* International Journal of Computer Science and Mobile Computing, 2013. 2(4): p. 263-268.

[26] Kandar, S., A. Maiti, and B.C. Dhara, *Visual cryptography scheme for color image using random number with enveloping by digital watermarking.* International Journal of Computer Science Issues (IJCSI), 2011. 8(3): p. 543.

[27] Wu, C.-C., M.-S. Hwang, and S.-J. Kao, *A new approach to the secret image sharing with steganography and authentication.* The Imaging Science Journal, 2009. 57(3): p. 14.151-0

[28] Hu, Y.-C., *High-capacity image hiding scheme based on vector quantization.* Pattern Recognition, 2006. 39(9): p. 1715-1724.

[29] Eslami, Z., S. Razzaghi, and J.Z. Ahmadabadi, *Secret image sharing based on cellular automata and steganography.* Pattern Recognition, 2010. 43(1): p. 397-404.

[30] Kong, J., et al. *A scalable secret image sharing method based on discrete wavelet transform*. in *Bio-Inspired Computational Intelligence and Applications: International Conference on Life System Modeling and Simulation, LSMS 2007, Shanghai, China, September 14-17, 2007. Proceedings*. 2007. Springer.

[31] Rabie, T., M. Baziyad, and I. Kamel, *Enhanced high capacity image steganography using discrete wavelet transform and the Laplacian pyramid.* Multimedia Tools and Applications, 2018. 77: p. 23673-23698.

[32] Hashim, A.T. and L.E. George. *Secret image sharing based on wavelet transform*. in *International Conference on Information Technology in Signal and Image Processing,, Mumbai, India*. 2013.

[33] Tresor, L.O. and M .Sumbwanyambe, *A selective image encryption scheme based on 2d DWT, Henon map and 4d Qi hyper-chaos.* IEEE Access, 2019. 7: p. 103463-103472.

[34] Huang, C.-P. and C.-C. Li, *A secret image sharing method using integer wavelet transform.* EURASIP Journal on advances in signal processing, 2007. 2007: p. 1-13.
[35] Dharwadkar, N.V. and B. Amberker, *Watermarking scheme for color images using wavelet transform based texture properties and secret sharing.* International Journal of Signal Processing, 2010. 6(2): p. 93.100-
[36] Surekha, B. and G. Swamy, *Visual secret sharing based digital image watermarking.* International Journal of Computer Science Issues (IJCSI), 2012. 9(3): p. 312.
[37] Rani, A., et al., *A zero-watermarking scheme using discrete wavelet transform.* Procedia Computer Science, 2015. 70: p. 603-609.
[38] Tompa, M. and H. Woll, *How to share a secret with cheaters.* journal of Cryptology, 1989. 1(3): p. 133-138.
[39] Lukac, R. and K.N. Plataniotis, *Bit-level based secret sharing for image encryption.* Pattern recognition, 2005. 38(5): p. 767-772.
[40] Deshmukh, M., N. Nain, and M. Ahmed, *A novel approach for sharing multiple color images by employing Chinese Remainder Theorem.* Journal of Visual Communication and Image Representation, 2017. 49: p. 291-302.
[41] Chen, T.-H. and C.-S. Wu, *Efficient multi-secret image sharing based on Boolean operations.* Signal Processing, 2011. 91(1): p. 90-97.
[42] Rajput, M. and M. Deshmukh, *Secure (n, n+ 1)-multi secret image sharing scheme using additive modulo.* Procedia Computer Science, 2016. 89: p. 677-683.
[43] Ghodosi, H., J. Pieprzyk, and R. Safavi-Naini. *Secret sharing in multilevel and compartmented groups*. in *Information Security and Privacy: Third Australasian Conference, ACISP'98 Brisbane, Australia, July 13–15, 1998 Proceedings 3*. 1998. Springer.
[44] Kumar, P.S., et al., *Multi-level secret sharing scheme for mobile ad-hoc networks.* International Journal of Advanced Networking and Applications, 2014. 6(2): p. 2253.
[45] Harn, L. and M. Fuyou, *Multilevel threshold secret sharing based on the Chinese Remainder Theorem.* Information processing letters, 2014. 114(9): p. 504-509.
[46] Ersoy, O., K. Kamer, and K. Kaskaloglu, *Multilevel threshold secret sharing based on the Chinese remainder theorem.* International Journal of Information Security Science, 2019. 8(2): p. 17-29.
[47] Basit, A., et al. *Multi-stage multi-secret sharing scheme for hierarchical access structure*. in *2017 International Conference on Computing, Communication and Automation (ICCCA)*. 2017. IEEE.
[48] Chen, D ،.et al., *An efficient verifiable threshold multi-secret sharing scheme with different stages.* IEEE Access, 2019. 7: p. 107104-107110.
[49] Hu, F., et al., *Threshold Meaningful Secret Image Sharing Scheme Based on QR Code.* Security and Communication Networks, 2022. 2022.
[50] Zhang, D. and Z. Gu, *A high-quality authenticatable visual secret sharing scheme using SGX.* Wireless Communications and Mobile Computing, 2021. 2021: p. 1-12.
[51] Chattopadhyay, A.K., et al., *A verifiable multi-secret image sharing scheme using XOR operation and hash function.* Multimedia Tools and Applications, 2021. 80: p. 35051-35080.
[52] Kang, Y., et al., *Ghost imaging-based optical multilevel authentication scheme using visual cryptography.* Optics Communications, 2023. 526: p. 1288.96
[53] Lin, C.-C. and W.-H. Tsai, *Secret image sharing with steganography and authentication.* Journal of Systems and software, 2004. 73(3): p. 405-414.
[54] Aarabi, G., G. Heydecke, and U. Seedorf, *Roles of oral infections in the pathomechanism of atherosclerosis.* International Journal of Molecular Sciences, 2018. 19(7): p. 1978.
[55] Chang, C.-C., J.-C. Chuang, and P.-Y. Lin. *Sharing a secret two-tone image in two gray-level images*. in *11th International Conference on Parallel and Distributed Systems (ICPADS'05)*. 2005. IEEE.

P- ISSN 1991-8941 E-ISSN 2706-6703 *Journal of University of Anbar for Pure Science (JUAPS)* Open Access
2023,(17), (1):169– 187

المشاركة المرئية السريـة والأعمال ذات الصلة – مراجعة

ناهدة طه درويش و علي مكي صغير

قسم علوم الحاسبات ،كلية علوم الحاسوب وتقنية المعلومات ، جامعة الانبار ، العراق

Email; nah19c1012@uoanbar.edu.iq

الخلاصة :

أدى التطور المتسارع لتكنولوجيا الشبكة وتطبيقات الإنترنت إلى زيادة أهمية حماية البيانات والصور الرقمية من الوصول غير المصرح به والتلاعب بها. تعد شبكة مشاركة الصور السرية *(SIS)* تقنية مهمة تستخدم لحماية الصور الرقمية الخاصة من التحرير والنسخ غير القانونيين. يمكن تصنيف *SIS* إلى نوعين: مشاركة سر واحد *(SSS)* والمشاركة متعددة السر *.(MSS)* في *SSS* ، يتم تقسيم صورة سرية واحدة إلى مشاركات متعددة ، بينما في *MSS* ، يتم تقسيم الصور السرية المتعددة إلى مشاركات متعددة. يضمن كل من *SSS* و *MSS* أنه لا يمكن إعادة بناء الصور السرية الأصلية بدون المجموعة الصحيحة من المشاركات. لذلك ، تم تطوير العديد من طرق مشاركة الصور السرية اعتمادًا على هاتين الطريقتين على سبيل المثال التشفير المرئي ، إخفاء المعلومات ، تحويل المويج المنفصل ، العلامة المائية ، والعتبة. كل هذه التقنيات قادرة على تقسيم الصورة السرية بشكل عشوائي إلى عدد كبير من المشاركات ، كل منها لا يوفر أي معلومات لفريق التطفل. فحصت هذه الدراسة العديد من مخططات مشاركة الأسرار المرئية كأمثلة فريدة لطرق مشاركة المشاركين السرية. تمت أيضًا مناقشة العديد من الهياكل التي تعمم وتعزز *VSS* في هذه الدراسة حول بروتوكولات مشاركة الصور السرية ، كما يقدم هذا البحث أيضًا تحليلًا مقارنًا لعدة طرق تستند إلى سمات مختلفة من أجل التركيز بشكل أفضل على الاتجاهات المستقبلية للصورة السرية. بشكل عام ، جودة الصورة التي تم إنشاؤها باستخدام منهجيات مطورة أفضل من جودة الصورة التي يتم الحصول عليها من خلال استخدام منهجية المشاركة السرية المرئية التقليدية.

.الكلمات المفتاحية: المشاركة المرئية السرية ، سر واحد ، مشاركة متعددة الأسرار ، يمكن التحقق منها ، عملية XOR.