Al-Nahrain Journal of Science
ANJS, Vol.27(3), September, 2024, pp. 97-108

Exploring Visual Cryptography Techniques: A Comprehensive Review

Hajir Alauldeen Al-Bayati[1,*], Lahieb M. Jawad[2], Dalal N. Hamod[1]

[1] Department of Computer Science, College of Science, Al-Nahrain University, Baghdad, Iraq
[2] Department Network Engineering, College of Information Engineering, Al-Nahrain University, Baghdad, Iraq

Article's Information

Received: 26.02.2024
Accepted: 12.05.2024
Published: 15.09.2024

Keywords:
Visual cryptography.
Image encryption.
Shares.
Encryption /Decryption.

Abstract

The backdrop: visual cryptography represents a contemporary encryption technology valued for its ease of implementation and comprehensibility, eliminating the need for a secure channel for key transmission and similar requirements. This paper aims: delve into the diverse methods employed in optical encryption, exploring their advantages and drawbacks, with a particular focus on image encryption techniques and the outcomes documented in various research studies. The objective is to identify the strengths and weaknesses inherent in these methodologies, paving the way for potential solutions in the future of optical encryption research. Notably, challenges persist in effectively handling color images and utilizing multiple shares (n, n), impacting both the security and the restoration aspects. The time computation aspects, encompassing creation, encryption, and restoration of these shares, also present challenges. Consequently, ongoing improvements are necessary to address these intricacies and enhance the robustness and applicability of visual cryptography technologies in diverse contexts.

http://doi.org/10.22401/ANJS.27.3.12

*Corresponding author email: hajaralaa110@gmail.com

1. Introduction

Nowadays, the networking scenario is changing rapidly, the use of electronic devices and mobile has increased, and transmitting the secret information over the Internet has become a popular and challenging medium so the process of encryption has become important for security. Eavesdroppers who attempt to hack data or secret information while transmitting over the Internet pose a dangerous position. As technology develops, it can provide a lot of information that the user needs appropriately and quickly, but the security issue may hinder the data transfer process, for instance, the interception of a data can occurs during a transmission process [1]. At the same time, a growing number of individuals are advocating for additional security measures to safeguard their privacy. Also, despite visual cryptography technology introduction by Naor and Shamir in 1994, Visual Cryptography has grown into a hot study area. As its name shows that it may recover visual information using the human eye or via stacking lots of images together [2]. Figure (1) demonstrates the Naor-Shamir technique by describing an algorithm for encrypting a single pixel in an image, in order to create the two shares [3]. Two cryptographic mechanisms are available: symmetric key cryptography employs the usage of the same key for encryption and decryption. Asymmetric key cryptography employs two distinct keys for encryption /decryption [4].

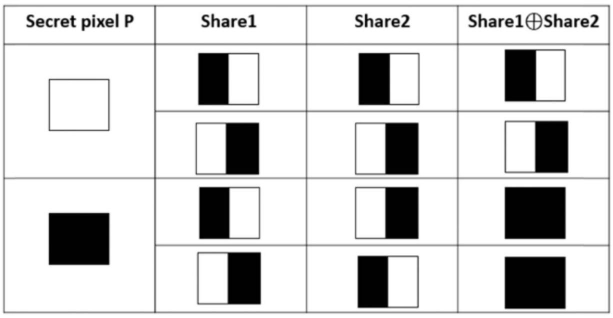

Figure 1. Naor-Shamir technique

2. Visual Cryptography

Visual Cryptography (VC) a new type of cryptographic scheme, allows us to encrypt images, video, text, and other data in a completely secure manner that can be immediately decoded by human visual senses [5]. It is one of the most effective cryptography schemes, using merely encryption, means that there is little requirement for decryption and no large calculations are required to decrypt the image. As a result, anyone may use the system without knowing anything about cryptography (encryption or decryption), since no computations are required, since decoding happens when the shares are visually stacked or overlapped. This is the benefit of VC over traditional cryptographic techniques, which are often conditionally secure. Considering its unique properties, VC has a wide range of applications, including protecting online transactions, digital watermarking, authentication, steganography, and others [6]. Figure 1 depicts the steps for a VC encryption. Furthermore, Visual Secret Sharing (VSS) is a VC-specific application in which a secret image is separated into shares, each giving partial information. VC is often associated with images because it relies on the human visual system to decrypt the information. Some of the primary methods utilized in VC:

- Pixel Duplication: This approach duplicates pixels from the original image to produce several shares.
- Random Pixel Patterns: This approach generates random patterns of pixels for representing noise or data.
- Pixel Expansion: The original image pixels are extended into a larger grid in shares.
- Threshold method: These strategies require a threshold number of shares to get various shares.

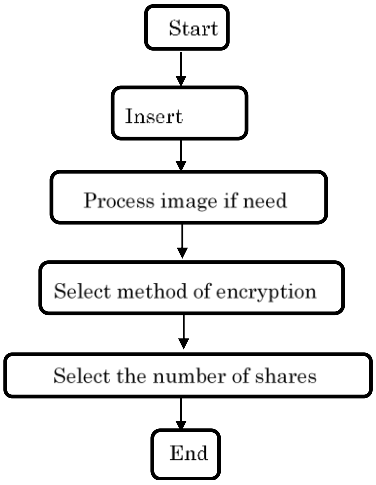

Figure 2. VC flowchart.

3. Literature review

Authors in [4] proposed a new approach is based on two existing algorithms: visual cryptography and Harris Hawks optimization (HHO). Based on (2, 2) secret sharing. The method involves several steps, including color quantization, color level determination using the hybrid optimization algorithm, grouping of segments, and share generation for each color channel. The proposed approach aims to eliminate pixel expansion also improve the quality of image retrieval. The outcomes show that the approach provides high-quality reconstructed images, but setting the parameter of pixel expansion to $m \geq 1$ will result in a decrease in the quality of shared and reveal images, and it appear this scheme un-expandable. In reference [7] The QR code-based expansion-free and meaningful visual cryptography scheme (QEVCS) generates visually appealing Codes with QR codes that are used to transmit significant portions of images while retaining image security. They proposed Instead of encrypting each individual pixel by a pixel, they utilize a block-based halftoning procedure, this to preserve each of the dimensions of the share and secret blocks. QEVCS embeds shares of the hidden image into QR codes, in addition, the approach employs block encryption & limited halftoning this to allow for the reuse of current expanded visual cryptography scheme (EVCS) techniques for creating encryption matrices with no pixel expansion. The method is used to control the flow via the limit gray-level halftoning method, and observed the value of peak signal-to-noise ratio (PSNR) has small, about 20dB with difficulty to reveal the original image. So, will be distributed via public networks. The proposed work has found in [8] the image and text are encrypted and decrypted using the Advanced Encryption Standard (AES) algorithm, this for secures sensitive information while it is being transported and stored. It used 128-bit key employed to encrypt. With little modified by an encryption key in each round during encryption. With the assistance of Python code implementation. Phase One: Stego Image Creation Upon the encryption procedure in this phase, the secret input is placed in random pixels within Cover Image1. Phase two: Hiding stego picture in VC shares the stego image developed in Phase 1 is inserted within Cover Image2's VC shares. The Cover Image2 is divided into three colour channels (RGB), & two shares are formed based on the intensity of pixel values (more than or below 128) for each colour channel. Here the data concealed in the secret image after a hybrid steganography and visual cryptography. It seems reconstructed the encrypted image/text without distortion.

Authors in [9] work many shares (share1, share2, … share n) is created using retrieved pixel values, and the shares are then separated into blocks. The Rivest-Shamir-Adleman (RSA) technique effectively encrypts and decrypts a multitude of seemingly random shares that are generated. The proposed method maintains the original image quality, and in the situation of security, the approach falls short, as seen by the near to 1 correlation value generated. It was also observed that their technique might provide secure image data, though the high key space size (2048 bit) so it becomes slow, but provided better security. In [10] Halftone Visual Cryptography (HVC) represents an encoding approach which employs Visual Cryptography Schema VCS and halftoning techniques to produce meaningful shares in order to increase the level of safety of share pictures. In order to prevent the residual image effect, they suggested a novel approach known as "Color Halftone Visual Cryptography (CHVCs)" for retrieving color secret images of the same size utilizing a dynamic codebook plus error diffusion mechanism. The experimental findings based on imagery metric values demonstrated an improvement in visual quantity, and security for the recovered secret image. In other hand observe generated random shares, which decreased the security level and made share management difficult.

In [11] proposed system, Image steganography and visual cryptography are combined. 24-bit color images are employed. First, a binary matrix is built from the secret and share1 images to form the red, green, and blue layers. Then XOR operation is carried out on each layer corresponds. Secret messages and cover object are encoded with text and images using this method. They did to enhance the tool's durability and resistance to detection. Apparently, it’s observed that because of the obtained correlation value of 1.0, the original image is independent of the encrypted image and has less protection against various attacks.

Authors in [12] proposed a new lossless secret color image sharing scheme allows for the transformation of any RGB secret color image into multiple shadow images based on chaotic map. In this novel used a set of multiple shares, these shadow pictures may be utilized to recreate the original hidden image with no distortion. For their method, do not have the preprocessing stage when the secret image is converted into a random image employing the Arnold Cat map or other chaotic maps. The secret color picture is separated into parts of (k-1) pixels each. Then shared pixels are created for each segment via a mathematical transformation across a finite field of choice. Their approach generates shadow pictures that smaller than the original image. The algorithm has medium speed, as seen by the encryption time of 3:4133s. However, because peak signal-to-noise ratio (PSNR) has a perfect value, it is robust to statistical attacks.

Suggest in [13] a novel color image 2-out-of-2 visual cryptography (VC) schema utilizing Block Diagonalization Algorithm (BDA). The two fundamental stages of optimization—exploration and exploitation—are comparable to these swarming tendencies. In their work reliant (2, 2) color Visual Cryptography scheme exhibits several advantageous features. The innovation capitalizes on BDA's optimization capabilities for color level determination, enhancing the quality of reconstructed images Without having to sacrifice computational speed or introduce pixel expansion. Nonetheless, it may be said that the method in [13] is anti-differential in terms of security given the high entropy value 7.9989 achieved.

In [14] the objective is to introduce an innovative digital image encryption method based on the Lorenz chaotic system. The encryption algorithm comprises three phases. Firstly, Black Mask Algorithm applied to the original image, this algorithm generates four shares (C, M, Y, K). Next, the shares' pixels generated by the black mask algorithm pass the Scrambling Process. Lastly, made Lorenz System the Lorenz chaotic system is then product the new secret keys via a logistic map and the use of chaotic sequences generated by the Lorenz system to encrypt the four shares produced from previous stages (C, M, Y, and K), the outcome is satisfactory, and the program has been found to be resistant to differential attacks it was 33.92%. the Pixel to Signal Noise Ratio PSNR values achieved is 58.39, mean square error (MSE) was 0.09 and Unified average changing intensity (UACI) was 33.92.

Authors in [15] Presented an Optimized Color Halftone Visual Cryptography (OCHVC) schema utilized a hybrid of the Hash codebook and halftone Floyd–Steinberg error diffusion algorithm. Their method involves two primary stages: construction and reconstruction. Participants receive six meaningful and secure shares through public communication channels during the construction stage. The reconstruction stage employs XOR-

Boolean operations to recover the halftone color secret image. Random share images are generated by dividing them into mask cells with a size of [4 × 4]. Their method can be said to be successful recovery of the halftone color secret image underscores the efficacy of the proposed OCHVC methods.

Authors in [16] A novel encryption strategy, are Profile Hidden Markov Model (PHMM), has been developed. The key elements of this design are probability vector (PV), initialization vector (IV) and substitution-box (S box). PV is created from the original image using the RGB chance model and the PHMM theory. By obtaining random values along the lengths of the initial image, IV is produced. Values 0 through 255 are randomly inserted into a 16-by-16 matrix, each of which is used just once, to create the S-Box. The suggested block-based encryption approach yielded the PV, IV, S-BOX, and encrypted image output. All four of these elements are used to get the original image with minimal loss. Otherwise, the decryption procedure results in useless data. Their work has strong against statistical attack because peak signal-to-noise ratio (PSNR) has high value. And from the performance study presented in [16], it can be said that the method met the requirements for a high degree of security while maintaining an acceptable encryption efficiency for varying sizes.

In [17] the Block-based Progressive VSS (BPVSS) mechanism for share generation is examined. There are two kinds of shares that they can produce: meaningful shares and noise-like shares. A halftone picture is the BPVSS algorithm's input. The algorithm then displays generates binary shares and an extracted pixel as output after receiving n shares as input. Similar to the embedding approach, they separate the shares into non-overlapping 8 × 8 blocks in order to extract the data. They formulated the restoration problem as a classic model and applied the MAP estimator to recover the high-resolution image. These multiple shares for the secret image using basis matrices and then restoring the original image using the embedded data and SR techniques. We observe from [17] that there is a near relationship between the original image and recovered image, which is confirmed by the Structural Similarity Index (SSIM) value (0.8005) obtained.

In [18] the separated red, green, and blue color pictures are used in the proposed way to use visual cryptography. In the current system, each share formed is encrypted separately utilizing Visual Secret Share creation (VSS) methods. In their novel XOR-Based Visual Cryptography was created the share1 and ahare2. Suggested technique uses share1 encryption plus share2 encryption, both of which are included in the RSA algorithm. The decryption share1 and ahare2 processes enable hidden picture sharing and stacking.

Found in [19] Four color shares: cyan, magenta, yellow, and a mask is used to encipher the image. And they employed an Advanced Encryption Standard (AES) algorithm for encryption and decryption that was based on an artificial neural network (ANN). In their suggested the security of the encryption process can be further enhanced by incorporating the AES algorithm. There are multiple steps involved in the process, such as color decomposition and error diffusion. And they used color decomposition to split the original image toward a halftone image for encryption purposes. The halftone image can be encrypted using a pair of pixels using error diffusion. Although CMY color space is more accurate than RGB color space in the AES-based visual encryption technology, the image may be darker. Observed that it provides a tiny degree of black pixel, which provides a small sensitivity to size changes. While the maximum correlation value which is 1 found that all pixels are retrieved confirms the theory that this approach good in the security domain.

Authors in [20] Used a mix of secret management of keys and Shamir's hidden sharing algorithm, they offer a reliable and secure private image sharing technique. They have designed an ideal encryption technique along with an efficient secured (k, k) multiple secret color pictures-based sharing (SKMSS) system. After every share is formed, it is encrypted using special keys produced by the Hybrid Optimal (SIMON). SIMON cipher keys for encryption are created utilizing a Cuckoo Search Optimization Algorithm, which relies on Hybrid Particle Swarm Optimization. That scheme's achievement is assessed using metrics like peak signal-to-noise ratio (PSNR), mean square error (MSE), & CC, of findings show that their method offers close to be a poor degree of security, with a PSNR value of 47.0056dB.

In [21] RGB pixel values of the secret image, an individual matrix is generated. The Visual Cryptography approach is used in the share generation process based on the pixel values. Each share is produced independently throughout the share creation process utilizing Visual Secret Sharing (VSS). The Rivest-Shamir-Adleman (RSA) algorithm is used to encrypt and decrypt the multiple shares of secret images that were created. Key generation is done using the multiplication technique during the encryption process. Encryption is done using the public key, while decryption is done using the private key. Their proposed method was observed to have a higher level of security according to experimental results and quality for sharing secret images, and it also runs faster with encryption time is 1.108 and decryption time is 0.0132 with comparison of the AES algorithm. This RSA algorithm offers both high-security image encryption and fast decryption. In the proposed RSA method Lena image peak signal-to-noise ratio (PSNR) values is 156.32, mean square error (MSE) values is 0.4931, however AES method values are 152.42, 0.4891 for peak signal-to-noise ratio (PSNR) and mean square error (MSE) respectively.

In [22] A Modulo Encryption based VSS system (MEVSS) is suggested for encrypting a secret picture shared by n individuals. proposed Instead of converting the secret color image to a binary or grayscale form first, they proposed (n, n) MEVSS technique directly encrypts it with the modulo encryption technique. The input image is separated into two noise images and/or four noise images, means they introduced (2,2) MEVSS and (4,4) MEVSS for comparison. Then the encryption of the secret image is generated by XOR operation, resulting in meaningless shares. The MEVSS algorithm, color images are encrypted using modulo encryption without being converted into any other form, such as binary or grayscale. By their approach demonstrated the efficiency and real-time encryption, as evidenced by the near standard values of 99.604% and 33.4469% for the Number of Pixel Change Rate (NPCR) and Unified average changing intensity UACI, respectively. Further, the correlation value (0.00007) indicates that the neighboring pixels within the original image are closer together than those in the encrypted image, indicating less predictability by third parties.

The work in [23] presents an Extended Visual Cryptography Strategy (EVCT) for the security of medical images. The confidential medical image is first encrypted using a Cryptography Method: Circular Shift Encryption (CSE) technique, after which three shares are formed using cover photos. Cover pictures might be binary, grayscale, or color. They made the size of the hidden picture as the cover image is the same. At the recipient's end, the rebuilt encrypted secret picture is decoded using the encryption technique: Circular Shifting Decryption (CSD) technique, and the retrieved secret image is acquired during the decryption phase. Based on their performance research presented in [23], it can be said that the method met high security requirements.

In [24] Visual Cryptography and Elliptic Curve Cryptography (ECC) is employed to generate individual red and green and blue shares utilizing the Visual Secret Sharing (VSS) Scheme, their research introduces the application of the ECC method for both image encryption and decryption, leveraging the Rubik's cube image encryption algorithm. They used for public key cryptography generation of encryption method, while the ECC method's secret key generates the decryption process. The process involves dividing each RGB pixel value toward three shares, with subsequent encryption and decryption using the Rubik's cube encryption algorithm applied to Elliptic Curve Cryptography shares. The encrypted image's 0.02 error rate rating indicates that it is a good quality.

Authors in [25] proposed Multiple grayscale Secret Image Sharing (MSIS) approach for safe sharing is suggested in their research. They suggested MSIS performs three essential tasks: signification, share production, and share disclosing. The secret pictures are processed in this step to have meaningful values for pixels so that during the Share Construction step, the image having the least amount of pixel error will be split into shares. The stage of Reveal part of the suggested MSIS algorithm. This reconstructs the original secret picture as the output after receiving the shares as input, and their results are recovered out the channels employing the LSB extracting method. Their experimental findings, which include a recorded error rate of 1169.232 and a peak signal-to-noise ratio (PSNR) value of 7.48579dB, demonstrate that the approach offers low security and low quality.

Authors in [26] employed a meaningful visual cryptography scheme (QEVCS) centered around QR codes. In their QEVCS strategically divides the image encryption process toward two stages. Initially, it proposes a gray-level limited EVCS, which segments a secret image into two equally sized and cover images. Subsequently, these cover images are seamlessly integrated into corresponding QR code images using gray decoding. In lieu of pixel-by-pixel encryption, a block-based halftoning operation is employed to uphold consistent sizes in both the secret and share blocks. According to the PSNR values which roughly 21, whereas standard halftone pictures have PSNR values of approximately 27. So observed this work is fulfill security needs.

Presenting in [27] a novel picture encryption technique that combines 3D chaotic systems, public-key cryptography, DWT, and Schur decomposition. Proposed to create the random sequence, the chaotic system's starting values are first created using the RSA technique. The pre-encrypted picture is then obtained by performing both diffusion and scrambling procedures on the plain image. To produce the upper triangular and orthogonal matrices, the pre-encrypted plain picture is subjected to the Schur decomposition method. Secondly, a DWT procedure is performed once the cover picture has been jumbled. Eventually, the visually significant cover picture embedded with hidden plain image may be generated by using the inverse DWT and inverse scrambling procedure. Due to the standardized correlation values among the primary cover image that the final visual meaningful cover pic is close to 0.9997, the proposed encryption approach is unnoticeable for secret image transmission. Based on the performance study shown in [27], it can be said that the method achieved the requirements with a high security level and a sufficient encryption speed for varying picture sizes.

In [28] the encryption process uses fuzzy random grids and a meta-heuristic approach to generate shares which can encrypt gray and color images. So, creates two random grids of fuzzy values by performing the encryption operation on the first values associated with the image's pixels without using binary conversion. The values of the 2nd fuzzy random grid are set utilizing the color connections between the initial fuzzy random grid & the original picture, while the decimal values of this first fuzzy random grid being set randomly during the encryption process. Furthermore, random grids are created in a way that prevents them from displaying any information about the original image individually. The original image is only visually evident when the random grids are piled on top of one another, which is accomplished using the fuzzy OR operator. Here, we may conclude that the quality of recovered images has reached a good level because of the suggested relationship the color combination for the suggested encrypting and decrypting stages which the value got from the peak signal-to-noise ratio (PSNR)= 327.2931dB, however the correlation coefficient of less than 0.09 indicates no correlation.

Authors in [29] A novel method is introduced that combines steganographic techniques with deep learning and visual cryptography to address inherent security concerns in this approach. Notably, the vulnerability where anyone familiar with the concealed information location can easily retrieve it is mitigated. In this method, a secret image is concealed within a cover picture using steganography. The secret image is first processed using an autoencoder and then undergoes visual cryptography through an exclusive OR (XOR) operation with a randomly generated image known as mask1. Empirical findings indicate that both the cover image and the stego image demonstrate negligible distortion. Based on the correlations between the encrypted and unencrypted pixels, their approaches will be determined to be vulnerable to attack.

In [30] proposed integrated hybrid lightweight and transfer deep learning algorithms to establish a resilient and effective framework for image retrieval. Furthermore, the incorporation of visual cryptography based on the 3D Lotka-Volterra chaos map to produce four shares. Empirical results demonstrate that not only achieves an elevated level of protection for visual cryptography but also ensures accurate image retrieval. In [30] it can be concluded with a stated encryption time of 0.1587315 to 0.159732 seconds; the method's performance seems reasonable. Due to the four shares are cloud-stored, along with their distinctive features. And may be considered robust against exhaustive assault, and the likelihood of danger is low, with an entropy value of 7.990869063 to 7.989623688.

In summary, all of the works covered in the literature review have benefits and disadvantages when it comes to conveying hidden images across a communication channel. Based on the features specified in Table 1, the corresponding table compares numerous previously presented approaches.

Table 1. Comparative analysis of various techniques based on objective metrics

Ref.	**Algorithms**	**Problem**	**Aim (objective)**	**Shares**	**Result**	**PSNR**	**MSE**	**CC**	**UACI (%)**	**NPCR (%)**	**SSIM**
[4]	Harris hawks optimization algorithm (HHO)	The pixel expansion set to parameter $m \geq 1.1$ results in a decrease in the quality of recovered images.	Address the troubles related to pixel enlargement, excessive processing costs, and the impact of subpar decryption quality.	(2, 2) secret sharing	Enhances the quality of the recovered image without impacting the calculation or adding additional pixels.	6.1811	4.2012	0.0009	32.00	99.90	—
[7]	QR code-based expansion-free	Quality of the restored images	Solve the issue with noise-like shares		The recovery picture is the same size like the secret image, eliminating mistrust in possible attackers	21.01	515.32	—	—	—	6.23
[8]	AES algorithm	Planning for a different encryption key in each round to perform encryption	Image security from an unauthorized person	2 shares	key space security and prevent common attacks	89.9	0.014	—	—	—	—
[9]	RSA	Employing optimization techniques to improve the performance of the PSNR.	(RSA) approach is employed to enhance the privacy and safety of the image.	N shares	Correlation coefficient of 1 for the decrypted image, indicating no distortion from the original image.	58.0025	0.1030	1	—	—	—
[10]	CVCS algorithm	pixel expansion, made share management difficult	enhancing the size, visual quality, and security of the retrieved secret image	2 shares	flexibility in managing share images, control to check the authentication of each share	27.582 to 27.758	108.96 to 113.46	—	—	—	0.901 to 0.996
[11]	XOR operation And other technique	can exposed key.	developing a technique that uses text and images as secret messages, with an additional layer of security	2 shares	Achieves enhanced security. The cover image and stego image have a minimal amount of distortion	51 to 57	0.07 to 0.5	1.00	—	—	0.9 to 0.8
[12]	chaotic maps & XOR operation	The scheme needs to be tested and optimized for larger image sizes, computational complexity	achieve lossless recovery of the original secret image without distortion	n shadow images	produces shadow images that are smaller in size compared to the original image	inf	0	0.00256	33.4797488942	99 : 6047973633	—

[13]	Binary dragonfly algorithm (BDA).	to produce valuable shares or color images format.	Pixels expanding, large computational complexity, and poor-quality decryption.		Memory requirements are reduced and image quality is enhanced.	6.1315d B	0.09	0.0011	32.66	99.68	—
[14]	image encryption algorithm called black mask	Complex features, pseudo unpredictability, and severe sensitivity to their initial values	To add encryption using keys to the action of decrypting images in order to make it more difficult.	four shares	Secure encryption/decryption file, according to statistical simulation.	58.39	0.09	—	33.92	—	—
[15]	Hash codebook and Floyd–Steinberg algorithm And bat optimization algorithm	Work to Ensure that the data is secure while being transmitted from attacks like Gaussian attacks.	Enhance the quality of share images to avoid pixel expansion and cross-interference issues.	6 meaningful shares	more robust against different attacks and security levels have been enhanced	28.3456 %	95.1748%	0.9933	—	—	—
[16]	Profile Hidden Markov	—	Create a simple, powerful, and efficient technique for encrypting digital photographs	—	increased encryption security, decryption process is very fast,	∞	0	0.9	34.11	100	1
[17]	MAP and SR techniques	around improving the contrast, reducing artifacts, maintaining security	Propose a super-resolution based visual secret sharing (VSS) scheme	Four shares	achieved an improvement in the contrast of the secret image	75.4609 to 66.731	0.0018 to 0.014	—	—	—	0.80 to 0.309
[18]	RSA Algorithm	—	confidential, authentication integrity and non-reputation	2 shares	Privacy, honesty, authenticity, and not being repudiated are all required.	69.91	93.44 %	—	18.070	92.16	—
[19]	artificial neural network (ANN) / AES algorithm	Time complexity, resulting image appear darker. So reducing the time required and enhance security.	retrieves the maximum the original image quality	four shares	All pixels are retrieved and it has very low error value.	59.0025	0.090	1	—	—	—

[20]	Hybrid Optimal SIMON (HOS) ciphers	security analysis and security characterization of Secret Image Sharing (SIS) methods	Provide low computational complexity, lossless secret reconstruction, and no pixel expansion.	'k' shares	Development of a secure and optimal secret sharing scheme for color images.	47.0149	1.2930	0.9997	—	—	—
[21]	RSA algorithm	Another approach may be used to improve the performance of the hidden image.	This is very much need secrecy protecting the messages and transmission medium also.	Two shares	The clarity of images is enhanced, and the level of security is high.	156.32	0.4931	—	13.88	69.44	—
[22]	XOR	Key Management, Lossy Sharing, Robustness against Attacks	improve security, reduce complexity, flexibility in the number of participants	2 shares 4 shares	The recovered secret image is lossless, faster, and its complexity is low	100.00 dB	—	0.000073	33.4469	99.604	—
[23]	CSE and CSD algorithm	May can Secret images are noticed.	Achieve medical image security	3 shares	Lossless and less complex.	Infinity	0.0	—	—	—	1.0
[24]	Elliptic Curve (ECC) Rubik's Cube Algorithm	Optimizing the encryption algorithm for Rubik's cube images.	evaluate performance of these algorithm	—	Improved the image quality and minimized error values.	92.05	0.0277	—	13.88	44.44	—
[25]	MSIS algorithm	—	Enhance the security and reduce the complexity.	1 share	reduced Pixel expansion, decreasing the likelihood of guessing the availability to secret image	7.485	1169.2	—	—	—	-0.00351
[26]	Halftone algorithm	enhance the visual quality of recovered images	The privacy of images is preserved by eliminating noise-like in traditional VCS.	—	The recovery image is identical in size to the secret images, keeping the images' privacy intact.	21	502.4	—	—	—	6.23
[27]	3D chaotic system and the RSA algorithm	Fast encryption of images	effectively hide the secret image	—	final visual cover image more imperceptible with an increased NC value	Inf	0	0.99	33.47	99.60	—
[28]	Fuzzy random grids, Genetic algorithm, OR operator	Don't have an appropriate run time.	To protect gray and color images with genuine values, without transforming them into binary or color images, or using pixel expansions.	Two shares	High-quality images were displayed after decrypting while respecting image security. Also robust against attacks.	326.78 dB	—	0.09	32.261	97.356	1.0

[29]	Least Significant Bit (LSB) technique XOR	this system's compatibility and performance can be tested on more recent datasets	Enhance the quality of Stego images and safeguard private images.	—	provide good protection for the secret image	59.52	0.14	1	—	—	0.97
[30]	Lotka_Volterra chaos system	need for exploration and integration of the image retrieval model with other applications	propose a secure and efficient content-based image retrieval system	four shares	Achieves a higher level of protection and provides accurate image retrieval.	7.30 dB	12764.2	0.001	—	—	—

4. Results and Discussion

After conducting an extensive survey on various visual cryptography schemes, this section synthesizes a discussion on the results of these methods, reinforcing the insights gleaned throughout the paper. Additionally, several metrics commonly employed for assessing image quality have been introduced:

a. **Peak Signal-to-Noise Ratio, or PSNR:** Higher PSNR readings are typically indicative of better image quality. Results from experiments [12], [16], [22], [23], [27] and so on are noteworthy since they exceed 60 dB, which is a positive consequence.

b. **MSE (Mean Squared Error):** Depending on the pixel intensity levels, a lower MSE value translates to improved image quality. Research like [8], [12], [17], and [23] have shown reduced MSE values, emphasizing enhanced image quality.

c. **The correlation coefficient, or CC:** determine the similarity between the associated pixels for the original image. has a range of -1 to 1, with positive values nearer 1 being preferred for evaluating the quality of a picture. Nonetheless, research [6], [13], and [22] produced values that were almost -1, indicating some variation in the outcomes.

d. **SSIM (Structural Similarity Index):** Values around 1 suggest strong similarity and great picture quality. The index ranges from -1 to 1. Research [27], [28] produced outstanding image quality with an SSIM score of 1.

e. **UACI (Universal Assessment picture Quality):** used to investigate differential assaults. Study [14] achieved the highest UACI at 33%, suggesting somewhat the level of quality. This scale is based on percentages, which allows for a more natural evaluation of image quality.

f. **Number of Pixel Change Rate (NPCR):** Comparing the pixel values among the original and encrypted images. The resultant number is returned as a percentage. If the value exceeds 99%, then the evaluation is positive.

In summary, these criteria offer a thorough assessment of the image's quality attained by various visual cryptography techniques. Notably, each metric contributes unique insights, and the selection of the most appropriate method may depend on the specific requirements of a given application or scenario.

5. Conclusions

This paper conducts a comprehensive examination of the application of visual cryptography methods in concealing actual information. The methods are categorized based on the outcomes reported in each study and the number of generated shares. Essentially, creating multiple shares demands additional time for generation and distribution to subscribers, but it offers enhanced security compared to a smaller number of shares. The study presents diverse visual cryptography approaches for implementing authentication. Specifically, Our review reveal that the methods utilizing chaotic maps and XOR operations, as discussed in [12], demonstrated exceptional results in term of security metrics such as PSNR, MSE, CC, UACI and NPCR (inf, 0, 0.0025618, 33.4797488942, 99:6047973633) respectively. These metrics indicate a high level of image quality, correlation between shares, and resistance against unauthorized decryption attempts. Additionally, [16] presents another promising approach using Profile Hidden Markov models, which also yielded excellent results across various metrics. The reported metrics include an infinite PSNR value, indicating negligible distortion in the reconstructed image, along with high CC, UACI, NPCR, and SSIM values, signifying strong security and fidelity in the decrypted information. Our study underscores the importance of choosing appropriate encryption algorithms and methodologies in visual cryptography to achieve robust security and reliable decryption outcomes. While the creation of multiple shares may entail increased generation and distribution time, it offers a trade-off for enhanced security, making it a worthwhile consideration in cryptographic implementations. Additionally, ensuring security against advanced cryptographic attacks remains an ongoing concern. Furthermore, we analyze encryption algorithms and their outcomes using various metrics. Notably, [12], [16], [21], [23], [27] exhibit superior results based on metrics such as PSNR, MSE, CC, UACI, NPCR, and SSIM.

References

[1] Ahamed, S. A.; Sarkar, I.; Molla, M.A.; Roy, S.; Bose, R.; “Utilizing the RGB Color Model and Halftone Technique for Color Segregation in Visual Cryptography”, (2023).

[2] Wang, L.; Yan, B.; Yang, H.M.; Pan, J.S.; “Flip extended visual cryptography for gray-scale and color cover images”. Symmetry, 13(1), 65, 2020.

[3] Sahni, G.K.; Hari, K.V.; "Schemes and Applications of Visual Cryptography". International Journal of Emerging Technologies in Engineering Research (IJETER) 8.6, 2020.

[4] Ibrahim, D.; Sihwail, R.; Arrifin, K.A.Z.; Abuthawabeh, A.; Mizher, M.A.; “Novel Color Visual Cryptography Approach Based on Harris Hawks Optimization Algorithm”. Symmetry 15(7): 1305, 2023.

[5] Somwanshi, D.R.; Vikas, T.H.; "An Optimal (2, 2) Visual Cryptography Schemes For Information Security". First International Conference on Advances in Computer Vision and Artificial Intelligence Technologies (ACVAIT 2022). Atlantis Press 2023.

[6] Bachiphale, P.; Nitish, Z.; "Review Based on Visual Cryptographic Scheme and Applications". Rivista Italiana di Filosofia Analitica Junior 14.2: 81-87, 2023.

[7] Ren, L.; Zhang, D.; “A QR code-based user-friendly visual cryptography scheme”. Scientific Reports 12(1): 7667, 2022.

[8] Patel, D.D.; Subhashchandra, D.; “Securing textual information with an image in the image using a visual cryptography AES algorithm”. Int. J. Enh. Res. Manag. Comp. Appl. 12(6), 2319-7471, 2023.

[9] Chouksey, P.; Miri, R.; Srinivas, K.; “Visual Cryptography with RSA Encryption for Secure Image Communication.” 2021.

[10] Hameed, R.S.; Ibrahim, A.W.S.; “Color halftone visual cryptography scheme using dynamic codebook and error diffusion technique”. Iraqi J. Info. Technol. 9(4), 2019.

[11] Islam, M.; A.; Riad Md Al-Amin K.; Pias, T. S.; “Enhancing security of image steganography using visual cryptography”. In 2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST) (pp. 694-698). IEEE. 2021.

[12] Sardar, M.K.; Adhikari, A.; “A new lossless secret color image sharing scheme with small shadow size”. J. Visu. Commun. Imag. Repr. 68: 102768, 2020.

[13] Dyala, R.I.; Rosni A.; Je Sen T.; “An enhanced color visual cryptography scheme based on the binary dragonfly algorithm”. Int. J. Comp. Appl., 2020.

[14] Fadhil, S.A.; Farhan, A.K.; “Color Visual Cryptography Based on Three Dimensional Chaotic Map”. Iraqi J. Comp. Comm. Cont. Sys. Eng. 22(2): 2022.

[15] Aswad, F.M.; Ihsan, S.; Salama, A.M.; “An optimization of color halftone visual cryptography scheme based on Bat algorithm”. J. Intell. Sys. 30(1): 816-835, 2021.

[16] Özcan, H.; Gülağiz, F.K.; Altuncu, M.A.; İlkin, S.; Şahin, S.; “A new visual cryptography method based on the profile hidden Markov model”. Adv. Elect. Comp. Eng. 21(1): 21-36, 2021.

[17] Mhala, N.C.; Pais, A.R.; “Contrast enhancement of progressive visual secret sharing (pvss) scheme for gray-scale and color images using super-resolution”. Signal Processing 162: 253-267, 2019.

[18] Karolin, M.; Meyyappan, T.; “Image encryption and decryption using RSA algorithm with share creation techniques”. Int. J. Eng. Adv. Tech. 9(2): 2797-2800, 2019.

[19] Chouksey, P.; Miri, R.; Srinivas, K.; “Enhanced Visual Cryptography for Color Images using Error Diffusion based AES Encryption”. Turkish Online Journal of Qualitative Inquiry: 13: 1, 2022.

[20] Shankar, K.; Taniar, D.; Yang, E.; Yi, O.; “Secure and optimal secret sharing scheme for color images”. Mathematics 9(19): 2360, 2021.

[21] Karolin, M.; Meyyappan, T.; “Authentic secret share creation techniques using visual cryptography with public key encryption”.

Multimedia Tools and Applications 80(21-23): 32023-32040, 2021.

[22] Saini, P.; Kumar, K.; Kashid, S.; Negi, A.; "MEVSS: Modulo Encryption Based Visual Secret Sharing Scheme for Securing Visual Content". In International Conference on Deep Learning, Artificial Intelligence and Robotics (pp.24-35). Cham: Springer International Publishing. 2022.

[23] Maurya, R.; Kannojiya, A.K.; Rajitha, B.; "An extended visual cryptography technique for medical image security". In 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 415-421). IEEE. 2020.

[24] Karolin, M.; Meyyappan, T.; "Visual Cryptography Secret Share Creation Techniques with Multiple Image Encryption and Decryption Using Elliptic Curve Cryptography". IETE Journal of Research 1-8: 2022.

[25] John, B.A.; Selva, M.G.; Manoj, K.S.; "Multiple secret image communication using visual cryptography". Wireless Personal Communications 122(4): 3085-3103, 2021.

[26] Ren, L.; Zhang, D.: "A QR code-based user-friendly visual cryptography scheme". Scientific Reports 12(1): 7667, 2022.

[27] Dong, Y.; Huang, X.; Ye, G.; "Visually meaningful image encryption scheme based on DWT and schur decomposition". Security and Communication Networks: 1-16, 2021.

[28] Mokhtari, A.M.,; Ramezani, R.; Latif, A.M.; "High-quality visual cryptography of real-value images without pixel expansion using fuzzy random grids". Iranian Journal of Fuzzy Systems, 2023.

[29] Seuti, T.; Al-Mamun, M.; Sarowar, S.A.H.M.; "Enhanced Steganography Technique via Visual Cryptography and Deep Learning". In Proceedings of the International Conference on Big Data, IoT, and Machine Learning: BIM 2021 (pp. 623-636). Springer Singapore. (2022).

[30] Al-Ta'i, Z.T.M.; Sadoon, S.M.; "Securing Privacy: Encrypted Image Retrieval with CNNs and Chaos-Based Visual Cryptography on Cloud Computing". International Journal of Intelligent Engineering & Systems 16(6): 2023.