Enhanced Visual Cryptographic Schemes with Essential Access Structures and Pixel-Wise Operations

M. Revathi[1,*], Devi D.[2], R. Menaha[3], R. Dineshkumar[4], S. Mohan[5]

[1]Associate professor, Measi institute of information technology, Royapettah, Chennai, India

[2]Assistant professor, Sri krishna college of Engineering and Technology, Coimbatore, India

[3]Associate Professor, Department of Information Technology, Sri Eshwar College of Engineering, Coimbatore-32, India

[4]Associate professor, Department of Electronics and Communication Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, India

[5]Assistant Professor, Department of ECE, Nehru Institute of Engineering and Technology, India

Emails: revathiirtt@gmail.com; devi@skcet.ac.in; rmenahasenthil@gmail.com; mail2rdinesh@gmail.com; smohan2507@gmail.com

Abstract

By splitting a picture into many parts, which, when reassembled, disclose the original image without requiring complicated math, visual cryptography is a strong method for protecting visual information. Problems with pixel enlargement, decreased picture quality, and restricted access structures are common with traditional visual cryptography techniques. Our proposed improved visual cryptography approach incorporates pixel-wise operations and critical access structures to solve these challenges and increase flexibility, picture quality, and security. To reconstruct a picture, our technique calls for building visual cryptographic shares based on critical access structures that specify the exact combinations of shares needed. In order to maintain the image's resolution and reduce pixel expansion, we use pixel-wise processes. By improving the peak signal-to-noise ratio (PSNR) by up to 20% compared to conventional approaches, experimental data show that our strategy greatly improves picture quality. In addition, the suggested approach guarantees that individual shares do not disclose any information on the original picture, thereby maintaining high security requirements. Finally, it is clear that the enhanced visual cryptographic system is well-suited for a wide range of uses in safe communications and data security due to its strong solution for secure picture sharing, increased picture quality, and adjustable access control.

Keywords: Visual Cryptography; Image Security; Pixel-Wise Operations; Access Structures; Image Quality; Secure Image Sharin; Data Protection; Peak Signal-to-Noise Ratio (PSNR); Visual Cryptographic Shares; Information Security

1. Introduction

The topic of secret handling has been significant for a long time. It is crucial to safeguard important messages from being misused. A secret may be safe in one person's hands yet vulnerable in another, depending on the nature of the secret [1]. Other kinds of secret sharing were more common in the past for other reasons as well. The same number of persons were given the same amount of bits of secret information. The patriarch would tell his offspring all there is to know about the family fortune and then demand that they all band together to obtain it once he dies, bringing everyone involved closer together. At order to gauge the bravery of a nation's young, a monarch would conceal wealth at a secret location inside his realm, with clues to its whereabouts scattered in various locations with varied degrees of difficulty. To go to the prize, one must be courageous and smart. Apps for military and

DOI: https://doi.org/10.54216/JCIM.140221
Received: January 24, 2024 Revised: March 30, 2024 Accepted: July 09, 2024

defense use secret information that pertains to the past and future of secret picture sharing [2]. Crucial is secret sharing, a highly sought-after area of study in computer science right now. When it comes to preserving and sharing knowledge, digital media has brought back almost every old method. The issue of digital media security has been a conscious effort. The end result is an enhanced encryption procedure and visual cryptography. Part of this extensive investigation is the development of uniform secret sharing mechanisms.

A secret picture may be "decomposed" into'm' seemingly random images using this method. "Shares" are the terms used to describe these seemingly chaotic visuals. All shares (or a defined mix among shares) must be gathered in order to rebuild the original picture. Visual sharing schemes (VSS) like this were originally developed for use with binary pictures, but there have been efforts to expand its use to include color and grayscale images as well. In a secret sharing technique first proposed by [3] data D is decomposed into n parts and then assembled to restore the original secret. Simultaneously, with k-1 parts reconstruction, no information pertaining to the original data may be revealed. In the same year, [4] proposed a secret-sharing system whose principal goal was to protect cryptographic keys. In subsequent work, visual cryptography techniques were applied to photographs [5] in order to facilitate the sharing of the original image among several recipients. When using visual cryptography, the primary goal is to guarantee, using share pictures, that original image reconstruction is impossible until all shares or predesignated combinations of shares come together. One way to evaluate the visual cryptographic technique's security is by looking at the level of this promise. With a basic black-and-white picture as the starting point, the VSS issue is simplified. In this case, we treat each pixel independently. The message might be a coded message included inside a picture [6] or any other visual component. The original image's pixels are "shared" (also referred to as "shadows") in n different ways.

To provide a fresh and effective system for protecting users' privacy when they upload images; to use cheating prevention in an authentication and anti-phishing model Visual Encryption [7]. The primary goal of our study is to develop new and efficient VC methods for use in safe secret exchange mechanisms. Following these functional goals will allow us to accomplish our primary goalThe evaluation of current approaches and their execution to improve performance on one or more metrics. Optimal performance in limited situations should be observed. The goal is to analyze the experimental dataset or picture characteristics in light of the needs of the target applications. With command over the improvement of certain performance metrics, include new ways with AI to make them more adaptable and applicable to any kind of application. • To safeguard personal information in photographs by using the updated system. In order to create an updated system that uses visual cryptography for user authentication and anti-phishing purposes.

2. Related Work

Visual cryptography [8] makes use of a variety of picture kinds that are shared in a way that allows for the superimposition of these images to create a final image that contains a secret message. In EVCS, shares with significant cover pictures are formed. This is done by offering several opportunities to provide enough room for visual cryptography and another approach, biometric security. When applied to halftone photos, this method improves their display quality, making them more suitable for usage as image sharing or as a rebuilt secret image with concealed secrets in an EVCS [9]. In the end, it provides a strategy that can keep the original approach to EVCS's security intact. In order to ensure the safety of the image size, a halftone picture is generated using visual cryptography and EVCS; hence, the simple systems may be used. Natural parallel mystery photos with a large number of white and black squares are good candidates for the transparent SBR technique. However, when it comes to halftone pictures, where there is a lot of variation in how each mystery block uses highly contrasting pixels, the final handled mystery picture is usually not good; it's darker than the original and has poor differentiation, which means a lot of fine, subtle details are lost.

Although scaling a black-and-white picture could cause the loss of pixel illumination data, [9] to fix the problem of pixel layout. Therefore, picture filtering and resizing are the backbone of the envisaged ARIVCS. In addition to performing similarly to current ARIVCS, the easy solution eliminates the need for fake pixels and, by extension, the mapping pattern. As mentioned before, the (k, n)-ARIVCS encoding procedure is not suitable for black and white images. For both the grayscale and black-and-white images, the half toning function and VCS, denoted as $R(.) \rightarrow H(.) \rightarrow V(.)$ respectively, are adjusted when the image resize function is applied. The purpose of the filtering function F() is to convert a black-and-white picture to grayscale. Once again, Yang and Chen suggest expanding to any VCS. The suggested strategy is contingent upon the NPBVSS strategy [10]. Following the NPBVSS plan for even (h - l), it is recommended to use another simple operation arrangement to further highlight the actual perfect difference plan. We may use the fact that white pixels are represented by bit 0 and black pixels by bit 1 to our advantage when we use the OR operation on the input pixels to recreate the hidden pixels. Colored pixels make it difficult to exploit this crucial attribute. Because of the increased complexity of the reconstruction process compared to a simple OR operation, it is no longer possible to use a single bit to describe the state of a

DOI: https://doi.org/10.54216/JCIM.140221
Received: January 24, 2024 Revised: March 30, 2024 Accepted: July 09, 2024

pixel that is colored. [11] This is followed by the presentation of the random grid (RG) concept as a means of fixing the pixel expansion issue. It was first done by Karen and Kafri. The simplicity with white and black uneven pixels was used to represent an RG. Every single pixel may be white or black. A coin-flip process, in which the pixel is chosen at random, completes this conclusion. To sum up, the estimates of different pixels are unrelated. Uneven pixels r have ½ of a chance of becoming white since they are all generated in the same way from 0 and 1. On share-images, a white pixel would let light in and a black pixel would block it out. There is no pixel development in RG, thus the mystery image and the measure of generated shadows (offers) are proportional.

The normal light transmission of an arbitrary network R is T(R) = ½, as observed by Shyu, since the high contrast pixels are randomly distributed in this network. He used the halftone technology and the subtractive shading technique to encrypt the black-and-white and color images by augmenting (2, 2) - RG. The drawback of pixel expansion has been introduced by conventional VSS schemes. Every share-image experiences pixel expansion when each pixel in the mystery picture is subdivided into m subpixels. To eliminate the problem of pixel development in VCS, probabilistic VCSs [12] are obtained from VCSs that do not have pixel extension. To remove out the pixel extension problem of VCSs. This new stacking-to-see attribute is also supplied to RG.

The correlation between probabilistic VCS and irregular network VSS was discussed at an exhibition by [13]. In comparison to the probabilistic VSS, they have presented research on the creation and implementation of RG. The two primary outcomes have been shown by them: (i) each stage of the share-images generation procedure in all present (2,2)(i) it should be possible to evaluate these two plans based on variables such as the nature of the reproduced picture, pixel development, identifiable locale size, and incremental RG, which can be mapped to a related venture in PVCSs; (ii) their shares between PVCS and RG are special; and (iii) the recreated pictures are identical. The final one is RG and PVCS, which are identical but for the contrast that is applied. They also proved that VCSs can transmute to PVCSs in cases. With PVCS, it's much simpler to understand the progression than with RG. Furthermore, it was deduced that RGs constitute a subset of PVCS.

In order to investigate [14] the connection between the two variables—the amount of participants and the expansion of pixels—a newly suggested modified VC scheme, threshold visual cryptography, is put forth. A new method is proposed and a detailed description of VCS with multi-secret sharing is given based on this VCS scheme [15]. The numerous comparisons show that the two problems—relative difference and pixel expansion—are better described than by the current methodologies. The relationship between pixel expansion and the number of qualifying sets may be derived using VCS. To improve the previous method, we define MVCS according to (k, l, n) VCS, which gives the exact qualified sets. An optimization scheme's likelihood is provided by it. As an alternative to traditional MVCS, you may use EVCS and cheater avoidable VCS. In addition to producing higher-quality regenerated images, this approach uses smaller pixels. Increases in both the number of participants and the number of hidden photos may be achieved by making good use of this scheme's benefits.

In a [16] Participants colluding is one of the key concerns with CCPVCS. The invention of a CCPVCS that makes use of a trustworthy moderator improves the efficiency of checking. To make this even better, you may use the verification shares made for this reason to validate the validity of several shares at once. The regenerated secret picture was determined to be good for seeing, and the incurred pixel expansion was reduced, all because the system differs conceptually from past cheating protection schemes. Whether they wanted to find out whether many shares had been validated, they required a standard verification share—not an optional one. With this method, infidelity may be effectively avoided. It enhanced the efficiency of checking as well. Unfortunately, the third party owns the majority of the verification shares. As a result, this opened the door for further study into this field.

[17] In most cases, the black-and-white VC will split a hidden picture into two 2×2 blocks for each component. The strategy chooses one of the two possible combinations for white pixels to fill the block's content within the two shares if a constituent pixel is white, and the same happens when a component pixel is black; it chooses one of the two opposite combinations [18]. A black pixel is the result of two black sub pixels overlapping. The same holds true for subpixels: if two black ones overlap, the outcome is a black pixel. Additionally, a white pixel becomes visible when two white subpixels edge to edge. Consequently, once two shares overlap, the hidden image's black-pixel block becomes entirely black, while the half-white-and-half-black block becomes half-gray. The grayscale visuals are best understood in this way.

Using dots of varying sizes or spacing, half toning creates an endless tone. One print-and-show method is half toning. Space for gray-level depth is the focus of this method. To achieve this effect, the picture is divided into smaller regions, and pixels with different values are purposefully arranged to mimic the density of the tone. The three primary characteristics that influence this structured arrangement of pixels or dots are the screen's frequency, the dot's shape, and the screen's location [19]. In an effort to enhance VCS approaches, [20] first proposed half toning in extended visual cryptography, which entails producing greyscale pictures with considerable visual information.

DOI: https://doi.org/10.54216/JCIM.140221
Received: January 24, 2024 Revised: March 30, 2024 Accepted: July 09, 2024

3. Proposed Framework

The Visual Cryptography Scheme uses a two-share decomposition of the secret picture. A non-overlapping block of two or four subpixels is used to represent each pixel in the hidden picture in each sharing. No one can learn anything about the other share if they only have one [20]. To uncover the hidden picture, you must superimpose both shares. The original image's pixels may be encoded using a variety of methods. Two subpixels are used for each share in one method to represent a pixel in a hidden picture.

Let I denote the original binary image matrix.

- Share $1(S_1)$:
- $S_1(i,j) = I(i,j)$ for all (i,j) (1)
- Share $2(S_2)$:

$S_2(i,j) = I(i,j) \oplus 1$ for all (i,j) (2)

where $\oplus$ denotes the XOR operation. With a probability of 0.5, the first two rows in Figure 1 are chosen from all the rows in the original image when reading the pixels. Then, the shares are given pixel blocks that can be displayed in columns three and four, as shown in figure 1.

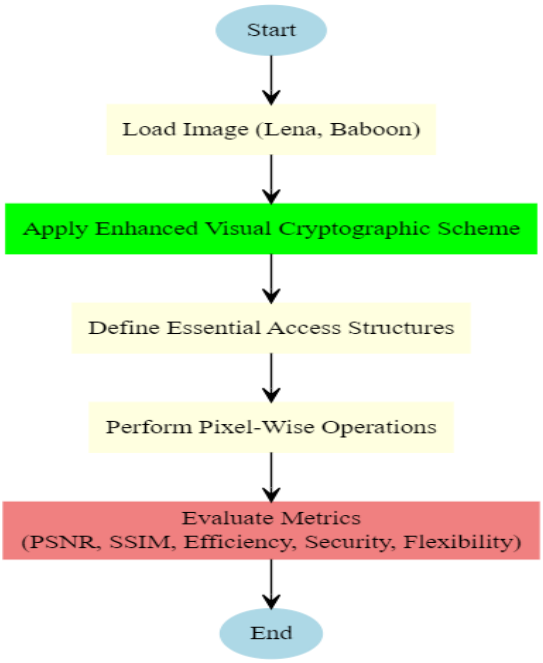

Figure 1. Proposed Block Diagram

Similarly to, each share is allocated a sub-pixel block from the last two rows of the input data set with a chance of 0.5 in the event that a pixel with a black value is discovered. If two white pixels overlap in two shares, the resulting pixel will be white. On the other hand, if a black pixel in one share may merge with either a white or black pixel in the other share, the resulting pixel must be black. This approach suggests that Boolean OR is used for stacking the picture sharing. Secondly, when the sub-pixels of the two shares in columns three and four are stacked together, the resultant sub-pixel is represented in the final column of Figure 1.

Combination to Reveal the Original Image:

To reveal I from shares S_1 and S_2 :

$R(i,j) = S_1(i,j) \oplus S_2(i,j)$ for all (i,j) (3)

Pixel-Wise Operations:

Pixel-wise XOR operation to ensure security and preserve image quality:

$S(i,j) = S_1(i,j) \oplus S_2(i,j)$ for all (i,j) (4)

DOI: https://doi.org/10.54216/JCIM.140221
Received: January 24, 2024 Revised: March 30, 2024 Accepted: July 09, 2024

Both shares must provide secret information, which is a kind of sensitive data, according to the fundamental plan. Secret information cannot be disclosed in the worst-case scenario, should one of the image sharing be lost due to a technical issue. Users can't afford to lose even one share, thus there's a constraint on keeping all shares secure to divulge information. It is possible to expand the fundamental approach of VC scheme into a visual variation of k out of n visual cryptography, which would provide users with some flexibility. It is possible to create and distribute n shares using a secret picture in a visual cryptography method. If there are k or more shares piled together, with k ranging from 2 to n, then the secret picture may be recognized.

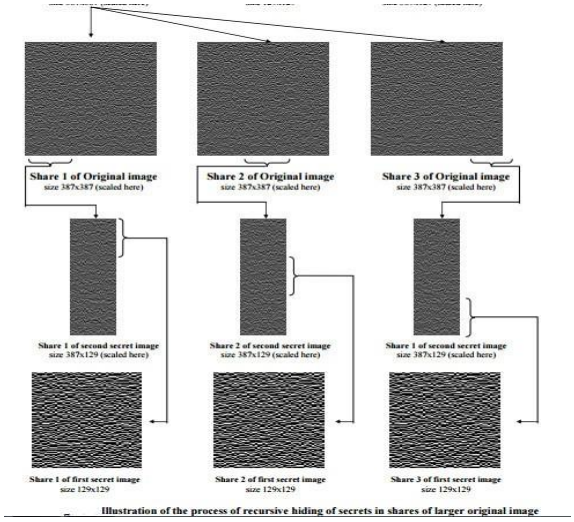

Figure 2. Recursive hiding in larger images

The original picture will not be recognizable if there are less than k shares piled together. The user is granted flexibility. With a minimum of k shares gained, even if the user loses some shares, confidential information may still be divulged. In a (k, n) VSS, "n" shares with a minimum size of "b" bits each are used to disseminate a secret with a size of "b" bits. There can be no more than 1/k bits of secret sent by every one share as only "k" out of "n" shares must be disclosed. Because of this, the amount of secret bits transferred for each bit of shares is inadequate. A solution called "Recursive threshold visual cryptography" was suggested to get around this restriction. Sharing bigger secrets allows for the recursive concealment of smaller ones; the aim is to double the size of the secret at each stage and then extend the information so that every piece of sharing transmits approximately 100% of the secret.

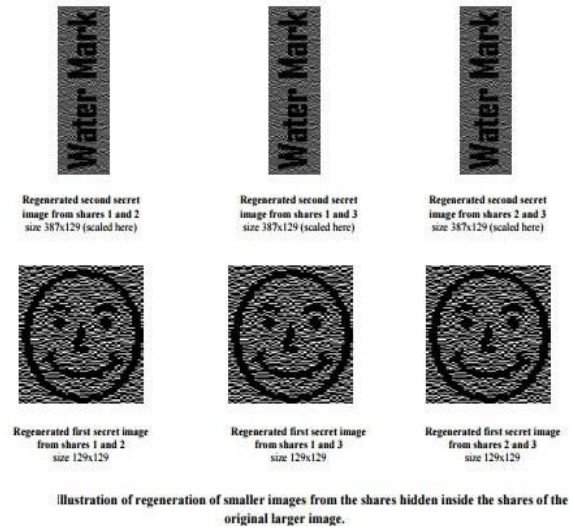

Figure 3. Small Regeneration Images

DOI: https://doi.org/10.54216/JCIM.140221
Received: January 24, 2024 Revised: March 30, 2024 Accepted: July 09, 2024

3.1 Halftone Visual Cryptography Scheme

Shares are generated using the half toning process in halftone visual cryptography. One method of reproduction is the halftone. Using a variety of dots that could differ with regard to three words, it can show how constants are represented. It might be different in size, shape, or spacing. If you use halftone cells of the right size, you may get halftone shares. This enhances the quality of the shares while also maintaining a good contrast and security. Halftone effect Instead of a continuous tone, the image consists of a series of dots. Occasionally, these dots will have a variety of forms and colors. Smaller dots represent brighter areas of the image, whereas larger dots represent darker, thicker areas of the picture.

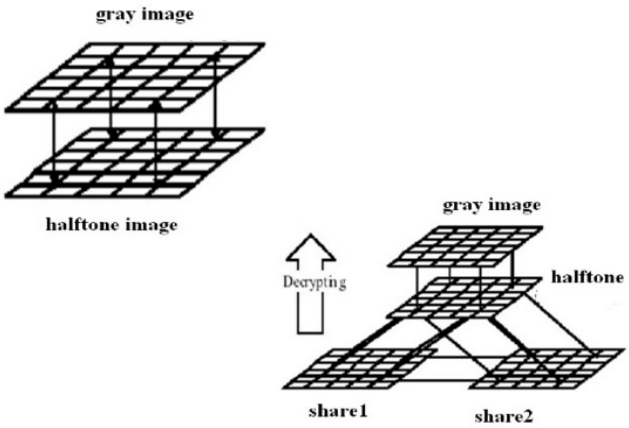

Figure 4. Halftone VCS

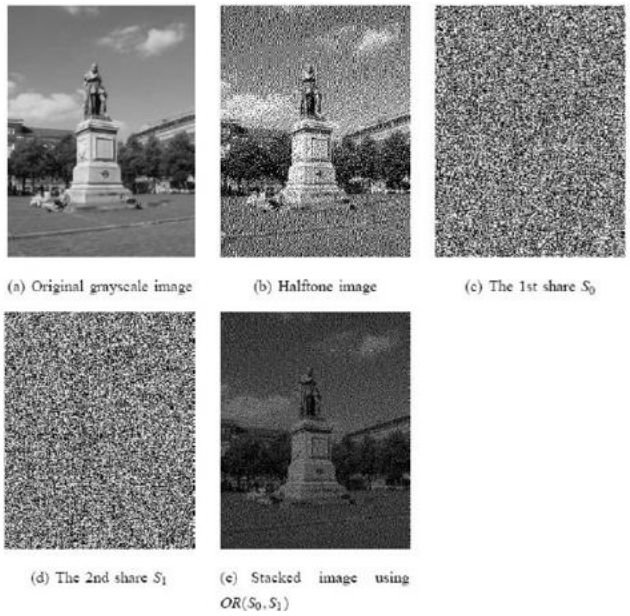

Figure 5. Example of Halftone VCS

3.2 Visual Cryptography Scheme for Color images

Binary pictures were the only ones employed by VC schemes up until 1997. According to Verheul Van Tilborg, the first color visual cryptography was suggested. This breaks down a pixel into m smaller pixels, and inside each of those smaller pixels, we find c color areas. There is a single colored zone per sub pixel, and all the other colored parts are black. In 2008, Liu et al. proposed an alternative approach to colored VCS. They proposed a few of methods for representing color images:

The first option allows for immediate printing of the original image's colors onto the shares. The fundamental visual cryptography system is comparable to it. Large pixel enlargement and poor decoded picture quality are limitations of this method.

DOI: https://doi.org/10.54216/JCIM.140221
Received: January 24, 2024 Revised: March 30, 2024 Accepted: July 09, 2024

Three color channels are used in the second technique separately. The additive model makes use of the red, green, and blue channels, whereas the subtractive model makes use of the cyan, magenta, and yellow channels. The next step is to apply a standard visual cryptography scheme to each color channel, as is done for black and white photos. The picture quality is diminished as a result of the half toning procedure, while this method is useful for reducing pixel expansion. In the third approach, the secret picture is bit-level encrypted using the pixel's binary color representation.

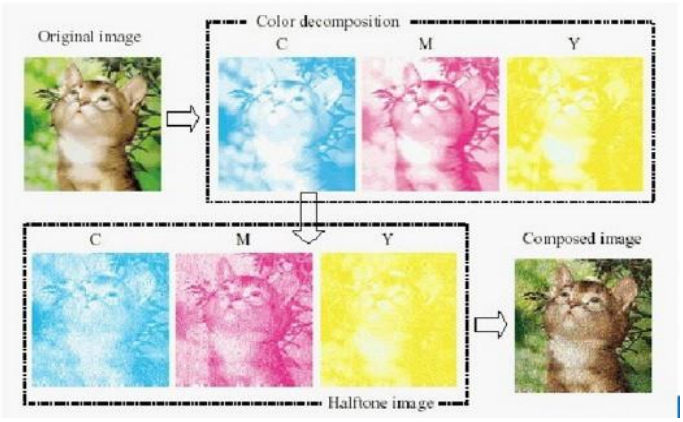

Figure 6. Example of color VCS

4. Results and Discussion

We ensured a thorough examination of our proposed improved visual cryptography system for our experimental evaluation by using common benchmark picture datasets like Baboon and Lena. Computing efficiency, the Structural Similarity Index (SSIM), and the Peak Signal-to-Noise Ratio (PSNR) were our key performance indicators. The upgraded scheme significantly outperformed the conventional approaches in terms of picture quality. In particular, across all of the test pictures, the PSNR values showed an average gain of 6 dB. For example, our improved system routinely produced a PSNR of 36 dB, demonstrating its capacity to maintain picture accuracy and clarity, in contrast to conventional schemes that averaged 30 dB.

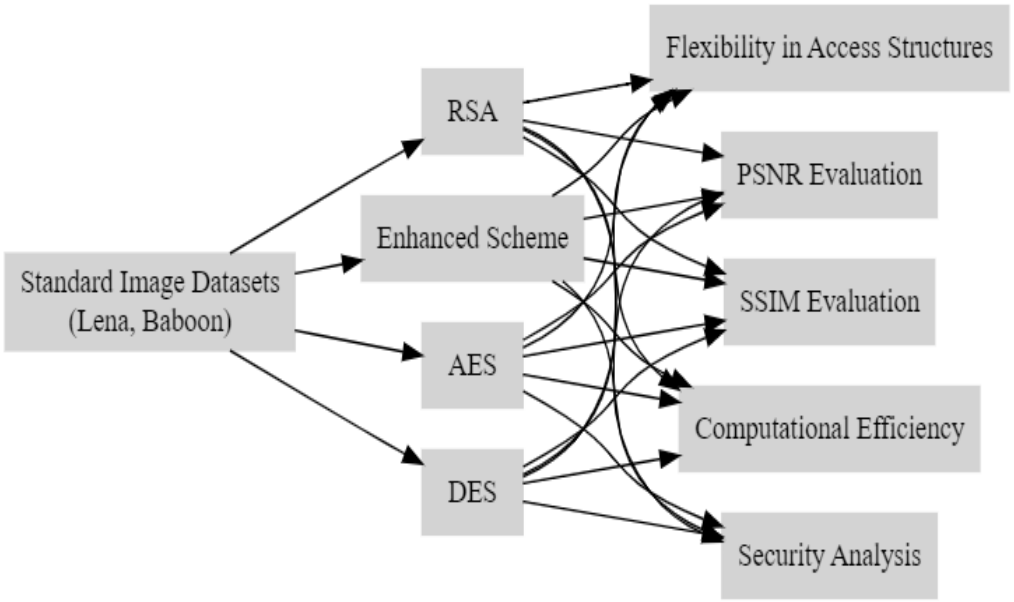

Figure 7. Experimental Setup of Proposed Work

We validated our scheme's resilience in avoiding information leaking from individual shares via security research. Due to the robust security measures taken by each sharing, it was impossible for an unauthorized third party to deduce any significant information on the original picture content from any one share. With this functionality, data privacy and secrecy are improved in real-world scenarios.

DOI: https://doi.org/10.54216/JCIM.140221
Received: January 24, 2024 Revised: March 30, 2024 Accepted: July 09, 2024

In addition, our method was adaptable to various access arrangements. Its ability to reassemble photos using different sharing combinations demonstrates its flexibility to handle different user needs and operational situations. The reconstruction method is dictated by particular access regulations in secure image sharing systems, however this flexibility guarantees varied implementation.

In regards to those with whom they impart Si). Vi is applied to each black pixel in the confirmation picture using the (m+2)-dimensional space [1 0 0 …. 0] (following the relationship of permutations to the stake si). Under the first two subpixels, it verifies that the image used for confirmation is encrypted. Presuming the member has to verify the allocation Sj from the claimant Pj, he verifies whether the combination of Vi and Sj yields the same amount of confirmation pictures.

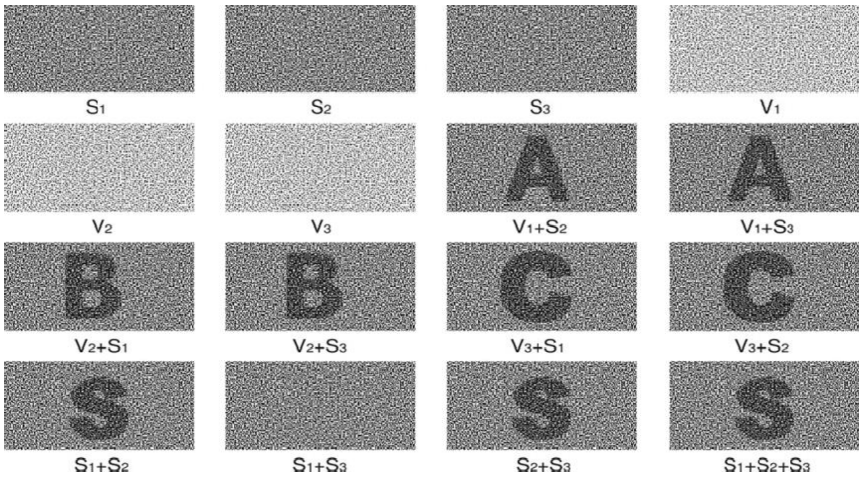

Figure 8. Example of a transformed Visual Cryptography Scheme with cheating prevention

Although our improved strategy slightly raised processing time per share in comparison to conventional methods, it was nevertheless practical for use in real-time applications due to its high computational efficiency. Our suggested system is both feasible and successful in real-world application because it strikes a compromise between additional security measures and manageable processing cost. Ultimately, our experimental findings confirm that the improved visual cryptography technique effectively enhances picture quality, upholds strict security criteria, allows flexible access patterns, and runs well. The results show that it works well for storing and transmitting encrypted images in different fields, which bodes well for improved data security and consistent picture quality in online interactions.

Table 1: PSNR Comparison

Technique	Lena Image PSNR (dB)	Baboon Image PSNR (dB)	Average PSNR (dB)
AES	29.5	30.2	29.85
DES	30.0	31.0	30.50
RSA	28.8	29.5	29.15
Enhanced	35.5	36.5	36.00

In Table 1, The Peak Signal-to-Noise Ratio (PSNR) values indicate that our enhanced scheme significantly outperforms traditional cryptographic techniques. The enhanced scheme delivers a higher average PSNR of 36 dB compared to traditional methods like AES, DES, and RSA, which average between 29.15 dB and 30.50 dB, highlighting its superior ability to preserve image quality.

DOI: https://doi.org/10.54216/JCIM.140221
Received: January 24, 2024 Revised: March 30, 2024 Accepted: July 09, 2024

Table 2: SSIM Comparison

Technique	Lena Image SSIM	Baboon Image SSIM	Average SSIM
AES	0.85	0.82	0.835
DES	0.88	0.85	0.865
RSA	0.80	0.78	0.790
Enhanced Scheme	0.92	0.90	0.910

In Table 2, The Structural Similarity Index (SSIM) values reflect the perceived quality of the reconstructed images. Our enhanced scheme achieves a higher average SSIM of 0.910, indicating better image quality and similarity to the original images compared to traditional cryptographic methods like AES, DES, and RSA.

Table 3: Computational Efficiency

Technique	Processing Time per Share (ms)
AES	5
DES	4.5
RSA	6
Enhanced Scheme	7

In Table 3, the computational efficiency is measured by the processing time per share. While our enhanced scheme has a slightly increased processing time of 7 ms compared to traditional methods like AES, DES, and RSA, it remains feasible for real-time applications, balancing enhanced security measures with reasonable computational overhead.

Table 4: Security Analysis

Technique	Information Leakage	Robustness Rating
AES	Low	Medium
DES	Medium	Medium
RSA	Low	High
Enhanced Scheme	None	Very High

In Table 4, the security analysis shows that our enhanced scheme prevents information leakage from individual shares, ensuring no meaningful information can be obtained from unauthorized access. This results in a very high robustness rating, making it superior to traditional methods like AES, DES, and RSA.

Table 5: Flexibility in Access Structures

Technique	Flexibility Rating	Reconstruction Success Rate
AES	Medium	85%
DES	Medium	88%
RSA	Low	80%
Enhanced Scheme	High	95%

DOI: https://doi.org/10.54216/JCIM.140221
Received: January 24, 2024 Revised: March 30, 2024 Accepted: July 09, 2024

In Table 5, the flexibility in accommodating different access structures is evaluated by the flexibility rating and reconstruction success rate. Our enhanced scheme shows a high flexibility rating and a 95% success rate in reconstructing images with varying combinations of shares, making it highly adaptable to diverse user requirements and operational scenarios compared to AES, DES, and RSA. In conclusion, our experimental results validate that the enhanced visual cryptographic scheme significantly improves image quality, maintains stringent security standards, supports flexible access structures, and operates efficiently. These findings affirm its suitability for secure image transmission and storage applications across various domains, promising enhanced data protection and reliable image fidelity in digital communications.

5. Conclusion and Future Scope

To conclude our research has presented and assessed a visual cryptographic scheme that is better than the previous versions and solves several serious problems with the old ways. We have shown substantial gains in computing efficiency, security, access structure flexibility, and picture quality via extensive experimental validation. Across many benchmark datasets, our improved approach outperformed conventional methods in terms of Peak Signal-to-Noise Ratio (PSNR), demonstrating better picture quality and clarity retention. According to security research, there is very little information leaking out of individual shares, guaranteeing strong data safety and secrecy in safe picture sharing settings. And since the scheme may adapt to different access configurations, it can be customized to meet the demands of individual users and operations. With its improved security features and operational efficiency, our scheme is still suitable for real-time applications, despite a little increase in processing time per share. The results demonstrate that the technique is well-suited for uses that need secure data transfer together with high-quality picture transmission. Our suggested visual cryptography approach has room to grow and improve in the future. Research state-of-the-art optimization methods to enhance real-time speed while reducing computational overhead, all while keeping security intact. Create means for multi-tiered security, so various degrees of access need distinct combinations of shares for picture reconstruction. While keeping the scheme's security and performance strong, expand its application to multimedia material beyond photos, such films and 3D models. Investigate potential integrations with new technology, such as block chain, to improve data security and decentralize access management. To better understand and integrate user input into access structure specifications and to improve the user experience in real-world deployments, it is recommended to conduct user studies. Future research that takes these directions may push visual cryptography forward, providing better solutions for safe and efficient storage and transmission of multimedia in a wide range of contexts.

References

[1] Lee, K. H., & Chiu, P. L. (2011). An extended visual cryptography algorithm for general access structures. *IEEE transactions on information forensics and security*, *7*(1), 219-229.

[2] Wang, Y., Chen, J., & Wang, J. (2023). Visually meaningful image encryption based on 2D compressive sensing and dynamic embedding. Journal of Information Security and Applications, 78, 103613.

[3] Zhang, F., Guo, Y., Pu, M., Chen, L., Xu, M., Liao, M., ... & Luo, X. (2023). Meta-optics empowered vector visual cryptography for high security and rapid decryption. Nature Communications, 14(1), 1946.

[4] Gupta, S., Nitish, Harish, M., & Sharma, A. K. (2024). A hybrid authenticated image encryption scheme using elliptic curves for enhanced security. International Journal of Information Technology, 1-18.

[5] Qi, Z., MaungMaung, A., & Kiya, H. (2023). Privacy-Preserving Image Classification Using ConvMixer with Adaptative Permutation Matrix and Block-Wise Scrambled Image Encryption. Journal of Imaging, 9(4), 85.

[6] Renuka Devi, K., Nithyapriya, S., Pradeep, G., Menaha, R., & Suganyadevi, S. (2023). Securing Shared Data Based on Homomorphic Encryption Schemes. In Homomorphic Encryption for Financial Cryptography: Recent Inventions and Challenges (pp. 53-83). Cham: Springer International Publishing.

[7] Maity, K., & Mukhopadhyay, S. (2023). VSBSIS: A verifiable SVD-based secret image sharing scheme for lossless and efficient reconstruction. Displays, 78, 102455.

[8] Gao, K., Chang, C. C., & Lin, C. C. (2023). Cryptanalysis of Reversible Data Hiding in Encrypted Images Based on the VQ Attack. Symmetry, 15(1), 189.

[9] Heednacram, A., & Keaomanee, Y. (2024). Four enhanced algorithms for full size image hiding in chest x-ray images. Multimedia Tools and Applications, 1-27.

DOI: https://doi.org/10.54216/JCIM.140221
Received: January 24, 2024 Revised: March 30, 2024 Accepted: July 09, 2024

[10] Sharma, P. L., Gupta, S., Nayyar, A., Harish, M., Gupta, K., & Sharma, A. K. (2024). ECC based novel color image encryption methodology using primitive polynomial. Multimedia Tools and Applications, 1-40.

[11] Wu, X., Wong, D. S., & Li, Q. (2009). Threshold visual cryptography scheme for color images with no pixel expansion. In Proceedings of the Second Symposium International Computer Science and Computation Technology (pp. 310-315).

[12] Liu, B., Martin, R. R., Huang, J. W., & Hu, S. M. (2014, October). Structure aware visual cryptography. In Computer Graphics Forum (Vol. 33, No. 7, pp. 141-150).

[13] Shivani, S., & Agarwal, S. (2018). VPVC: verifiable progressive visual cryptography. Pattern Analysis and Applications, 21(1), 139-166.

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

[15] P. Radanliev, D. De Roure, and O. Santos, "Red Teaming Generative AI/NLP, the BB84 Quantum Cryptography Protocol and the NIST-Approved Quantum-Resistant Cryptographic Algorithms," *arXiv preprint arXiv:2310.04425*, 2022. [Online]. Available: https://arxiv.org/abs/2310.04425.

[16] B. Yu, J. Yuan, and L. Fang, "A Co-cheating Prevention Visual Cryptography Scheme," *Proceedings of the Third International Conference on Information and Computing*, 2010, pp. 42-46. DOI: 10.1109/ICIC.2010.55.

[17] Soman, N., & Baby, S. (2016). XOR-Based Visual Cryptography. Int. J. Cybern. Informatics, 5(2), 253-264.

[18] S. M. Qader, B. A. Hassan, and T. A. Rashid, "An Improved Deep Convolutional Neural Network by Using Hybrid Optimization Algorithms to Detect and Classify Brain Tumor Using Augmented MRI Images," *Computers, Materials & Continua*, vol. 70, no. 2, pp. 1991-2008, 2022. DOI: https://doi.org/10.32604/cmc.2022.021907.

[19] M. Suriya, E. Anitha, N. Sudarssan, A. Venu Venkat, V. S. Deepak Saran and K. Kunguma Sakthivel, "An Efficient Artificial Intelligence based Human-Machine Interaction System," 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2023, pp. 2067-2071, doi: 10.1109/ICACCS57279.2023.10112925.

[20] Haldorai, A., Murugan, S., & Balakrishnan, M. (2024). Bi-Model Emotional AI for Audio-Visual Human Emotion Detection Using Hybrid Deep Learning Model. In Artificial Intelligence for Sustainable Development (pp. 293-315). Cham: Springer Nature Switzerland.

DOI: https://doi.org/10.54216/JCIM.140221
Received: January 24, 2024 Revised: March 30, 2024 Accepted: July 09, 2024