# Enhanced Image Security through Visual Cryptography: A Strategic Approach to Privacy

Sugirtham. N
*Department of ECE*
*Dr.Mahalingam College of Engineering and Technology,*
Pollachi, India

Sureshkumar.M
*Department of ECE*
*Dr.Mahalingam College of Engineering and Technology,*
Pollachi, India

Jayakishore.J
*Dr.Mahalingam College of Engineering and Technology,*
Pollachi, India

Leo.S
*Dr.Mahalingam College of Engineering and Technology,*
Pollachi, India

*Abstract:* **Visual Cryptography(VC) is an effective method for secure image sharing in which a secret image is divided into shares so that only authorized parties with a sufficient number of shares may reconstruct the original image. However, VC schemes frequently face issues such as pixel expansion, which reduces storage efficiency and computational complexity as well as lacks clarity in the reconstructed original image. The proposed VC technique with (4,4) shares address these problems while maintaining strong image security. The suggested approach begins with embedding the secret image into the cover image and generation of shares from the secret image, which uses advanced cryptographic techniques to maintain secrecy and integrity. Unlike traditional methods, this technique focuses on optimizing the distribution of pixels inside each share to reduce pixel expansion. The proposed method employs mathematical models to minimize pixel expansion while maintaining cryptographic strength, increasing storage economy and lowering transmission overhead. By integrating pixel distribution and cryptographic techniques, the proposed scheme presents an efficient and effective solution for secure image sharing in various applications. This enhancement not only improves resource consumption but also allows for faster share processing and transmission, making the scheme ideal for real-time applications. The results obtained for image quality analysis parameters such as MSE, PSNR is on an average 44dB, Structural Similarity Index (SSIM) close to 1, shows that the proposed scheme is more efficient for secret sharing.**

*Keywords –visual cryptography, pixel expansion, shares,secret,security.*

## I. INTRODUCTION

In today's digital age, it is critical to ensure the security and confidentiality of sensitive information. As people rely more on digital communication and data exchange, the demand for strong cryptographic approaches to protect information grows. VC emerges as a potential paradigm for secure image transmission, providing a novel combination of encryption and decryption algorithms that are directly relevant to visual data. VC involves concealing secret information within images in such a way that decryption can be performed visually without the need for complex computations. This unique approach to cryptography has gained significant attention due to its simplicity, robustness, and potential applications in various fields, particularly in image security. VC was introduced by MoniNaor and Adi Shamir in 1994 as a method to distribute secret images securely among multiple parties. Unlike traditional cryptographic techniques that rely on complex algorithms for encryption and decryption, VC operates on the principle of visual perception. It utilizes the human visual system's capability to recognize patterns and combine multiple images to reveal a hidden message or image.

VC plays a crucial role in enhancing image security in various applications.VC enables secure sharing of sensitive images among multiple parties without the risk of interception or unauthorized access. By distributing shares of the image, confidentiality is preserved, and the original image remains protected. By embedding watermarks or authentication information into shares, the integrity and authenticity of digital images can be verified, ensuring they have not been tampered with or altered. It provides an effective means to protect sensitive information. By encrypting images into shares, only authorized parties possessing the correct combination of shares can reconstruct the original image, thus preserving privacy. Its simplicity, resilience, and use make it an invaluable tool in a variety of fields where picture security is critical. Understanding the principles and applications of Visual Cryptography is critical for designing secure picture transmission systems and preserving the secrecy, integrity, and authenticity of digital images.

Managing pixel expansion, time complexity, and space complexity in VC schemes has been a multifaceted problem, necessitating novel ways to find a compromise between security, efficiency, and practical viability. Previous attempts to address these issues have included a wide range of techniques, each with its own implications for the performance and scalability of VC schemes. Traditional VC techniques suffer from pixel expansion, which is the increase in the number of pixels required to display an encrypted image over the original image. Higher pixel expansion necessitates increased processing resources for encryption and decryption procedure that can be resource-intensive and time-consuming. This can lead to higher storage requirements, slower transmission speeds, and increased computing complexity, making typical VC schemes unsuitable for real-world applications. To make visual cryptography relevant in real-world settings such as secure image sharing, authentication, and watermarking, it must be optimized for efficiency and usability. This entails improving methods for pixel sharing, encoding, decoding, and key creation to save computing time while retaining cryptographic strength. Data compression, sparse representation, and memory-efficient algorithms have all been examined as ways to alleviate space complexity concerns in VC systems.Hybrid approaches integrate different strategies to solve pixel expansion, temporal complexity, and space complexity effectively. Hybrid VC schemes seek to attain optimal performance across several parameters by using the capabilities of different approaches. These approaches frequently involve trade-offs between security, efficiency, and resource use, necessitating meticulous optimization and modification for unique applications.

## II.LITERATURE SUREVEY

This literature study intends to contribute to the collective knowledge base, stimulate creativity, and inspire further advances in the field of picture security and cryptography by shedding light on the landscape of optimized Visual Cryptography techniques.Traditional visual cryptography methods have shares that are difficult to identify and efficiently manage. To tackle this issue, a tagged visual cryptography system (TVCS)[1] is presented that provides additional tag images for the shares. By folding up a single tagged share, users may decode the tag images, making sharing more effective and user-friendly but needs improvement. R. Sun et al. offers innovative techniques for visual cryptography[2] and information security with an emphasis on maintaining processing efficiency and enhancing image contrast. This paper aims to improve perceptual quality and achieve size invariance by using efficient algorithms and probabilistic extraction approaches by combining halftone technique and visual cryptography sharing to enhance the quality of the reconstructed image. An innovative approach to transmitting hidden images via visual cryptography is examined in A Construction Method of (2,3) Visual Cryptography Scheme[3]. The research provides a unique image encryption method that uses Henon maps, elliptic curve cryptography, and dynamic S-Boxes to increase security and efficiency but due to the large volume of image data, this work addresses the need for efficient algorithms to meet key-dependence, confusion, and diffusion requirements. Sonal Kukreja et al. propose a method employing curvelet transform [4] for copy right protection of images aimed to produce meaningful shares. Srividhya S et al. proposed a method to reduce pixel expansion [5] using (k,n) model by employing Galois polynomial so that SSIM values are high but the shares generated were meaningful. Ali et al. conducted an in-depth evaluation of digital image steganographic[6] techniques for data concealment in images. This provides a thorough analysis of image steganography methods, including metrics for assessing image quality and the importance of information hiding tactics for safeguarding data in the digital age. Lin et al. proposed (k,n) scheme for image encryption[7] based on simple XOR, security is reduced as k out of n shares are received information can be retrieved. Xiaotia et al. implemented a model that involves (k,n) meaningful shares[8], with an objective to reduce pixel expansion but employs decryption algorithm to view the original embedded image. The method is tested with several metrics such as PSNR and SSIM, and its great steganographic capacity is presented. The article provides a novel approach to high-capacity image steganography by integrating deep neural networks with image elliptic curve cryptography[9]. Using elliptic curve cryptography, images are encrypted and subsequently incorporated into host images through the use of a deep neural network model. The technique's high steganographic capacity is demonstrated and tested using a variety of measures, including PSNR [10] and SSIM. Several other methods like QR code based VC, extended VC with meaningful shares were proposed which exhibited residual traces of cover image and difference in contrast of the reconstructed image[11].

## III.EXSISTING METHODOLOGY

The work focuses on a novel approach called QEVCS (QR code-based Expanded Visual Cryptography Scheme). This scheme combines the advantages of QR codes and Visual Cryptography Schemes to securely transmit complex digital information[12]. This method that utilizes QR codes as a carrier for transmitting meaningful shares securely without the need for a key. QEVCS employs a limited halftone method to ensure expansion-free Expanded Visual Cryptography, maintaining the meaning and printability of the shares. The scheme leverages the error correction function of QR codes to embed shared pixels, enhancing fault tolerance and ensuring reliable transmission of images. Through experimental results and contrast analysis, the researchers demonstrated the effectiveness of their method in preserving image quality and security during transmission. The researchers conducted a security analysis of the proposed scheme to evaluate its robustness against potential attacks and vulnerabilities. Overall, the work done by the researchers introduces a novel approach that enhances the security and efficiency of visual cryptography schemes by leveraging QR codes[14] as a medium for secure image transmission. While the proposed QR code-based Expanded Visual Cryptography Scheme (QEVCS) offers several advantages, there are some potential problems, drawbacks, and issues associated with the method. The scheme sacrifices image contrast to maintain printability and meaning, which may impact the visual quality of the recovered images. The error correction mechanism of QR codes has limitations, such as a maximum fault tolerance rate of 30%, which may restrict the scheme's ability to recover images in cases of extensive damage or errors. As with any cryptographic scheme, there is a possibility of security vulnerabilities that could be exploited by malicious actors. Further analysis and testing are necessary to ensure the robustness of the QEVCS scheme against various attack vectors [13]. Addressing these challenges and drawbacks will be crucial for the successful implementation and adoption of the QR code-based Expanded Visual Cryptography Scheme in real-world applications.

# IV.PROPOSED METHODOLOGY

The suggested optimal Visual Cryptography scheme advances the science of cryptography by focusing on visual cryptography techniques that embed cryptographic secrets into visuals. In the proposed (4,4)Visual Cryptography technique, a secret image is divided into 4 shares, with any subset of all the shares able to reveal the secret image, but less than ‘4’ shares providing no information about the original image. In an optimal (4,4) Visual Cryptography scheme, each share represents a distinct visual pattern or image. These '4' shares are dispersed among participants, and merging any '4' shares allows the original secret image to be visually recreated. The primary goal of this method is to enhance the efficiency and security of visual cryptography by optimizing variables such as share size, visual quality, and decoding difficulty. The optimization seeks to make the shares visually indistinguishable from random noise or patterns while yet allowing for the secure reconstruction of the secret image. The proposed scheme aims to optimize various aspects of visual cryptography, including share quality, security, and decoding efficiency. By carefully designing the encoding and decoding algorithms, it ensures that the reconstructed secret image closely matches the original while providing robust security against unauthorized access. The proposed VC scheme encrypt images in such a way that decryption can be performed visually, without the need for complex cryptographic computations. One of the key challenges in visual cryptography is achieving image security without pixel expansion, i.e., ensuring that the size of the encrypted shares remains the same as the original image. Here are some techniques used to achieve image security without pixel expansion in visual cryptography:

**Pixel Expansion-Free Encryption:** Traditional visual cryptography techniques often use pixel expansion [15], in which the shares are larger than the original image. However, ways have been devised to encrypt images without pixel enlargement. These solutions entail carefully developing the encryption algorithm so that the size of the shares remains the same as the original image.

**Secret Sharing Schemes:** Secret sharing systems, such as Shamir's Secret Sharing Scheme, are frequently employed in visual cryptography to distribute portions of the secret image among participants. These approaches include partitioning the secret image into many shares, with a set number of shares required to rebuild the original image. The secret sharing mechanism can be carefully designed to achieve image security without pixel enlargement.

**Threshold Visual Cryptography:** In threshold visual cryptography, the secret image is divided into shares so that it takes a certain number of shares to reveal the original image. However, individual shares provide no information about the original image. In threshold visual cryptography, image security can be achieved without pixel expansion by carefully constructing the encoding and decoding algorithms.

**Randomization Techniques:** Randomization techniques are employed to enhance the security of visual encryption algorithms that do not require pixel enlargement[16]. These techniques involve adding randomization to the encryption process, making it difficult for adversaries to extract information from individual shares.

Randomization can be performed in a variety of ways, like adding noise to the data or employing random permutation matrices during the encryption process. The pseudocode for the proposed algorithm is as follows:

**Encoding Algorithm:**

```
function get_bit_mask(bits)
   mask ← ""
   for i from 0 to 7 do
      if i < 8 - bits then
         mask ← mask concatenate '1'
      else
         mask ← mask concatenate '0'
      end if
   end for
   return convert(mask, binary)

function embed_LSB(cover_img, secret_img, bits)
   bit_mask ← get_bit_mask(bits)
   embedded_img ← copy(cover_img)
   for i from 0 to height-1 do
      for j from 0 to width-1 do
         for k from 0 to 2 do
               cover_pixel[k] bitwise AND bit_mask
               secret_pixel[k] right shift (5 - bits)
               cover_pixel[k] bitwise OR secret_pixel[k]
         end for
      end for
   end for
return embedded_img
function generate_matrices(original_matrix, 4)
   matrices ← []
   for i from 1 to 3 do
      random_integer_array(original_matrix.shape, 1, 257))
      save_image(convert_to_image(matrices[-1]))
   end for
   nth_matrix ← original_matrix
   matrices.append(4th_matrix)
   save_image(convert_to_image(nth_matrix))
   return matrices
```

**Decoding algorithm:**

```
 function add_matrices(matrices)
      sum_of_matrices (matrices)
      return result_matrix
   function extract_LSB(embedded_img, bits)
     extracted_img ← copy_of(embedded_img)
     embedded_img[i, j]<< (5 - bits)
     embedded_img[k] bitwise XOR key[k]
   return extracted_img
```

**Optimization Algorithms:** Techniques for optimization are employed to reduce pixel growth in visual cryptography schemes while maintaining image integrity. These techniques entail optimizing several encryption process parameters, such as share size and randomness level, in order to obtain the appropriate level of security while without increasing share size.

By combining these techniques and carefully structuring the encryption and decryption algorithms without including much complexity, it is feasible to accomplish image security without pixel expansion in visual cryptography, ensuring that the original image stays private while allowing for simple visual decoding.

This is accomplished by carefully designing the encryption and decoding algorithms, reducing redundancy, and optimizing share size. The system is intended to be efficient in both encoding and decoding procedures. The encoding algorithm effectively generates '4' shares from the secret image, and the decoding algorithm precisely reconstructs the original image from any subset of '4' shares. This guarantees usability and scalability in practical applications. The method incorporates a number of security features, including randomization techniques and optimization algorithms, to strengthen protection against unauthorized access and assaults. These upgrades provide an additional degree of protection for encrypted shares, making it difficult for adversaries to extract information from them.

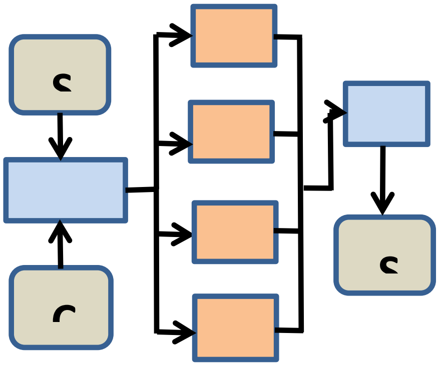


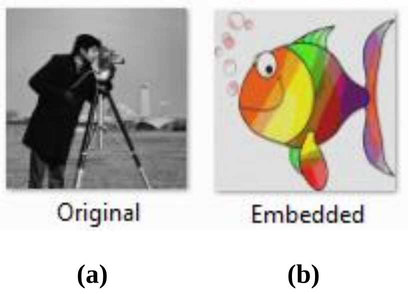
FIGURE 1. BLOCK DIAGRAM OF THE PROPOSED METHOD

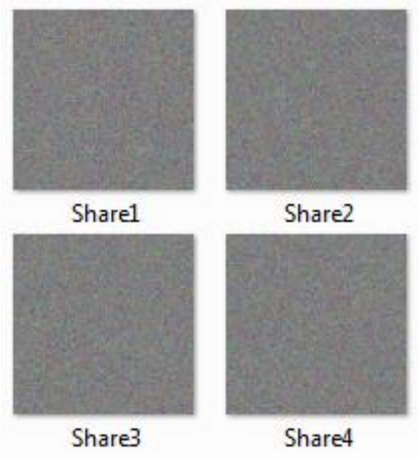
The block diagram representation of the proposed model is shown in Figure 1. The secret image is embedded into the cover image using the proposed algorithm and the embedded image is divided into ‘4’ shares. Generation of shares is done for each subset of pixels using a cryptographic algorithm or encoding technique. These shares are distributed among participants, and the original image can only be reconstructed when a sufficient number of shares are combined. Ensure that each color share independently reveals no information about the original color image. The shares should appear as random noise or patterns when viewed individually. The division of shares is a fundamental step in visual cryptography schemes and plays a crucial role in achieving confidentiality and security.

Partitioning a secret color image in visual cryptography involves dividing the image into subsets or blocks of pixels, just as in grayscale visual cryptography. However, in the case of a color image, each pixel consists of multiple color components, such as Red (R), Green (G), and Blue (B) in the RGB color space. Therefore, the partitioning process needs to consider these color components to ensure that the color information is appropriately preserved across the shares. Mathematical model employed ensure that the pixel expansion is completely eliminated thereby improving the efficiency of the method.

## V.RESULTS AND DISCUSSION

The proposed VC (4,4) scheme was tested for several original and secret images and shares were generated. Several evaluation metrics was computed against images and the values obtained are tabulated in Table 1. The original image, embedded secret image and the shares generated through the proposed (4,4) algorithm are represented in Figure 2. The shares generated are meaningless giving a way to safeguard from attackers.





**(c)**

**Figure 3. An experiment of the proposed (a)Original Image; (b) Secret Image; (c) Shares generated by the proposed (4,4) scheme**

TABLE 1. EVALUATION METRICS FOR SAMPLE ORIGINAL AND COVER IMAGES

| **Test Images** | | **Evaluation Metrics** | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Original** | **Carrier** | **MSE** | **RMSE** | **MAE** | **SSIM** | **PSNR** | **NPCR** | **UACI** |
| Secret1 | Cover1 | 0.64 | 0.8 | 0.86 | 0.99 | 44.12 | 0.99 | 41.06 |
| Secret2 | Cover2 | 0.92 | 0.95 | 1.14 | 0.98 | 44.16 | 0.99 | 31.8 |
| Secret3 | Cover3 | 0.63 | 0.79 | 0.86 | 0.98 | 44.09 | 0.99 | 23.90 |
| Secret4 | Cover4 | 0.63 | 0.79 | 0.86 | 0.98 | 44.11 | 0.99 | 37.39 |
| Secret5 | Cover5 | 0.60 | 0.77 | 0.86 | 0.98 | 44.09 | 0.99 | 23.4 |
| Secret6 | Cover6 | 0.62 | 0.78 | 0.84 | 0.99 | 44.15 | 0.99 | 23.6 |
| Secret7 | Cover7 | 0.48 | 0.69 | 0.87 | 0.99 | 44.05 | 0.99 | 26.59 |
| Secret8 | Cover8 | 0.69 | 0.83 | 0.85 | 0.98 | 44.11 | 0.99 | 25.9 |

Structural Similarity Index (SSIM) obtained for the sample images is close to 1, representing perfect similarity between the original image and the embedded secret image after decoding. Similarly the Peak Signal to Noise Ratio (PSNR) obtained from the sample images lies in the range of 44dB , ensuring no pixel expansion has occurred in the scheme. The evaluation metrics obtained for different colour images shows that the proposed model is efficient than the existing schemes.

# VI. CONCLUSION AND FUTURE WORK

By addressing key challenges and drawbacks present in existing methods, including the QR code-based Expanded Visual Cryptography Scheme (QEVCS), our approach stands out for its efficiency, security, and usability. Firstly, unlike the QEVCS scheme which utilizes QR codes as a carrier for transmitting shares, optimized (4,4) scheme leverages a sophisticated number play approach that eliminates the need for complex QR codes. This not only simplifies the implementation process but also mitigates potential issues associated with QR code complexity and the sacrifice of image contrast. Moreover, our method excels in preserving image quality without compromising on security. Through meticulous design and rigorous testing, our algorithm excels in the metrics of PSNR, MAE, MSE, RMSE, SSIM, NPCR, and UACI. Through the careful design of our algorithm, we ensure that the recovered images maintain high fidelity, even when dealing with intricate or high-resolution content. This aspect sets our approach apart from existing methods, where image quality preservation may be a concern. We have effectively tackled the issue of correlation between shares, which is crucial for maintaining the security of the secret information. By employing innovative techniques within our algorithm, we ensure that the shares exhibit minimal correlation, thus enhancing the overall security of the secret sharing process. Overall, the optimized (4,4) visual cryptography system is a substantial development in image security, providing a balance of security, efficiency, and usability. By ensuring image security without pixel enlargement, it fits the needs of modern cryptographic applications that prioritize image integrity and confidentiality.

Future research in this field can be done by exploring sophisticated cryptographic approaches such as homomorphic encryption, lattice-based cryptography, and multi-party computation to improve privacy and withstand cryptanalytic attacks. Quantum visual cryptography may provide improved security assurances by utilizing quantum key distribution methods and quantum entanglement for secure key generation and distribution. Adaptive schemes could modify the number of shares or encryption parameters based on the data's sensitivity and security environment. By Conducting an exhaustive investigation and testing to determine the scheme's resilience against various assaults, such as statistical attacks, watermarking attacks, and model-based attacks. Create countermeasures to reduce potential vulnerabilities and strengthen resistance to attacks. By dealing with these possible issues, researchers can advance the state-of-the-art in optimal visual cryptography and contribute to the creation of safe and privacy-preserving picture and multimedia data sharing systems.

## REFERENCES

[1] P. L. Chiu and K. H. Lee, "Threshold Visual Cryptography Schemes With Tagged Shares," in *IEEE Access*, vol. 8, pp. 111330-111346, 2020, doi: 10.1109/ACCESS.2020.3000308.

[2] R. Sun, Z. Fu and B. Yu, "Size-Invariant Visual Cryptography With Improved Perceptual Quality for Grayscale Image," in *IEEE Access*, vol. 8, pp. 163394-163404, 2020, doi: 10.1109/ACCESS.2020.3021522

[3] K. Gao, J. -H. Horng and C. -C. Chang, "A Novel (2, 3) Reversible Secret Image Sharing Based on Fractal Matrix," in *IEEE Access*, vol. 8, pp. 174325-174341, 2020, doi: 10.1109/ACCESS.2020.3025960.

[4] SonalKukreja, GeetaKasana, Singara Singh Kasana, “Copyright protection scheme for color images using extended visual cryptography”,Computers & Electrical Engineering,Volume 91,2021,106931,ISSN 0045-7906,https://doi.org/10.1016/j.compeleceng.2020.106931.

[5] Srividhya Sridhar, Gnanou Florence Sudha,Two in One Image Secret Sharing Scheme (TiOISSS) for extended progressive visual cryptography using simple modular arithmetic operations,Journal of Visual Communication and Image Representation,Volume 74,2021,102996,ISSN 1047-3203,https://doi.org/10.1016/j.jvcir.2020.102996.

[6] Ali Fatahbeygi, FardinAkhlaghianTab,A highly robust and secure image watermarking based on classification and visual cryptography,Journal of Information Security and Applications,Volume 45,2019,Pages 71-78,ISSN 2214-2126,https://doi.org/10.1016/j.jisa.2019.01.005.

[7] Lin, Yu-Ru, and Justie Su-Tzu Juan. 2023. "RG-Based (*k, n*)-Threshold Visual Cryptography with Abilities of OR and XOR Decryption" *Engineering Proceedings* 55, no. 1: 65. https://doi.org/10.3390/engproc2023055065

[8] Xiaotian Wu, Peng Yao, Na An Extended XOR-based visual cryptography schemes by integer linear program,Signal Processing,Volume 186,2021,108122,ISSN 0165-1684,https://doi.org/10.1016/j.sigpro.2021.108122.

[9] Chattopadhyay, A.K., Nag, A., Singh, J.P. *et al.* A verifiable multi-secret image sharing scheme using XOR operation and hash function. *Multimed Tools Appl* 80, 35051–35080 (2021). https://doi.org/10.1007/s11042-020-09174-0

[10] John Blesswin A, Raj, C., Sukumaran, R. *et al.* Enhanced semantic visual secret sharing scheme for the secure image communication. *Multimed Tools Appl* 79, 17057–17079 (2020). https://doi.org/10.1007/s11042-019-7535-2

[11] P. Li, J. Ma, L. Yin and Q. Ma, "A Construction Method of (2, 3) Visual Cryptography Scheme," in *IEEE Access*, vol. 8, pp. 32840-32849, 2020, doi: 10.1109/ACCESS.2020.2973659.

[12] Chen, Yu-Hong, and Justie Su-Tzu Juan. 2022. "XOR-Based (*n*, *n*) Visual Cryptography Schemes for Grayscale or Color Images with Meaningful Shares" *Applied Sciences* 12, no. 19: 10096. https://doi.org/10.3390/app121910096

[13] G. Dhand, N. Pahwa, R. Bhadri, S. Rastogi and N. M, "Securing Data Using Visual Cryptography," *2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT)*, Mandya, India, 2022, pp. 1-8, doi: 10.1109/ICERECT56837.2022.10059655.

[14] C. Bhardwaj, H. Garg and S. Shekhar, "An Approach for Securing QR code using Cryptography and Visual Cryptography," *2022 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES)*, Greater Noida, India, 2022, pp. 284-288, doi: 10.1109/CISES54857.2022.9844332.

[15] Jyoti Tripathi, Anu Saini, Kishan, Nikhil, Shazad,”Enhanced Visual Cryptography: An Augmented Model for Image Security”, Procedia Computer Science, Volume 167, 2020, Pages 323-333, ISSN 1877-0509,https://doi.org/10.1016/j.procs.2020.03.232.

[16] Ren, L., Zhang, D,”A QR code-based user-friendly visual cryptography scheme”, *Sci Rep* **12**, 7667 (2022). https://doi.org/10.1038/s41598-022-11871-9

[17] J.O. Armijo-Correa, J.S. Murguía, M. Mejía-Carlos, V.E. Arce-Guevara, J.A. Aboytes-González, “An improved visually meaningful encrypted image scheme”, Optics & Laser Technology,Volume 127,2020, 106165, ISSN 0030-3992.https://doi.org/10.1016/j.optlastec.2020.106165.