

Visual Cryptography with RSA Encryption for Secure Image Communication

Praveen Chouksey¹, Rohit Miri², Konda Srinivas³

¹Research Scholar, Dr. C.V. Raman University, Kota, Bilaspur (C.G.), India.

²Professor and Head, Department of Computer Science & Engineering, Dr. C. V. Raman University, Kota, Bilaspur (C.G), India.

³Professor & Head, Department of CSE (Data Science), CMR Technical Campus, Kandlakoya, Hyderabad, Telangana, India

Abstract

In visual cryptography, many shares are generated that are seemingly random but contain a hidden message within themselves. When all the shares are combined, they reveal the secret image. The concept of visual secret sharing is to encrypt a secret image into multiple illogical share images. It ensures that no data about the original image is revealed unless at least one of the shares is obtained. The original image can be reconstructed by directly overlapping all the shares, allowing the human visual system to identify the complete secret image without the need for complex computational tools. Therefore, they can be communicated securely as a set of shares. The Rivest-Shamir-Adleman (RSA) approach is employed to enhance the privacy and safety of the image. This technique is used to generate multiple shares, which are then encrypted and decrypted using the RSA technique. The test results have demonstrated a peak signal-to-noise ratio of 58.0025, a mean square error value of 0.1164, and a correlation coefficient of 1 for the decrypted image, indicating no distortion from the original image.

Keywords: Visual cryptography, visual secret sharing, RSA encryption, privacy, safety, image communication, peak signal-to-noise ratio, mean square error, correlation coefficient.

1. Introduction

Information security is critical for a great number of applications ranging from anti-counterfeiting to telecommunications [1]. Various digital cryptography techniques have been investigated to prevent information leakage, pursuing a high-security level of information. For computer-based techniques, long latency and high computational power are two main challenges. Compared with their electronic counterparts, optical cryptography techniques generally have the advantages of low-power consumption [2], high-speed parallel processing, and multi-dimensional capabilities, opening a gate for securing information. The past decades have seen significant advances in optical cryptography, including optical watermarking, steganography, and visual cryptography (VC) [3]. Nevertheless, the early efforts rely on the complex combination of multiple optical components for signal processing in the Fourier realm, leading to a large form factor. Furthermore, owing to the limited vector optical-field manipulation capabilities of conventional optical devices, the abundant degrees of freedom of light, such as amplitude, phase, frequency, polarization, etc., have not been fully exploited in early optical cryptography, leading to a limited safety performance. In recent years, meta surfaces, one kind of ultrathin optical elements consisting of an array of subwavelength nanostructures, have been developed to manipulate all the fundamental properties of light [4]. By combining multiple meta-atoms or different phase shift mechanisms, a single meta surface can be engineered to achieve independent multi-dimensional optical-field manipulation [5]. The compactness and versatile functionalities make meta surfaces perfect candidates for optical encryption [6] through various mechanisms such as multichannel vector hologram by exploiting Malus's law, the combination of grayscale/colour printing and the holographic image, as well as tuneable meta-holograms based on phase-change materials or spatial light modulators [7]. However, the spatially varying polarization property of vector light is not well exploited in optical cryptography until now, leading to a limited security level. Most holographic cryptography techniques can be potentially cracked by adjusting the polarization state of the input and output light or the incidence wavelength. A pioneering work that combines meta surface with ghost imaging or single-pixel imaging provides a framework to solve the integration problem and enhance the security level. In recent investigations, the security level has been improved by integrating meta surface imaging, visual cryptography, and computational imaging [8]. Generally, owing to the indirect imaging

manner of computational imaging, multiple optical measurements or additional digital post-processing are required for hidden image restoration. Essentially, these approaches deviate from the original intention of all-optical encryption, leading to the loss of the merits of parallel, high-speed, and low-power consumption properties to some extent. Here, we propose the concept of high-security vector VC, whose ciphertexts are coded based on the vector imaging process of a spin-decoupled dual-axis meatless [9]. Since the spatial degree is theoretically unlimited and the encryption is combined with other degrees (e.g., incident wavelength, polarization, orbital angular momentum, and spatial dislocation of spin states) [10], our approach enables much higher security.

The original picture may be rebuilt by immediately overlaying all the shares, which enables the human visual system to recognize the whole hidden picture without the need of using complicated computing methods. As a result, they can be shared safely as a collection of information. The RSA method is used to further improve the image's level of privacy and security. This method is used to produce several shares, which are then encrypted and decrypted using the RSA method. The RSA method is used to construct multiple shares.

2. Literature Survey

Almalkawi, et al. [11] proposed a lightweight and efficient security scheme based on chaotic algorithms to efficiently encrypt digital images. The proposed algorithm handles digital images in two different phases. digital images are split into blocks and compressed by processing them in frequency domain instead of Red-Green-Blue (RGB) domain. AL-Hashemy, et al. [12] proposed a simple and effective new algorithm for image encryption using a chaotic system which is based on the magic squares. This novel 3D chaotic system is invoked to generate a random key to encrypt any colour image. Bisht, et al. [13] proposed an approach to encrypt the color images using bit-level permutation and alternate logistic map. The proposed method initially segregates the color image into red, green, and blue channels, transposes the segregated channels from the pixel-plane to bit-plane, and scrambles the bit-plane matrix using Arnold cat map (ACM). Shah, et al. [14] proposed the S-box based image encryption algorithms. The authors improved the S-box based image encryption algorithms by the usage of all 16 distinct degree 8 primitive irreducible polynomials over \mathbb{Z}_2 and by introducing a new role of the ring of integers modulo n in the permutation steps. Kumari, et al. [15] proposed a block cipher that ensures confidentiality and secrecy for secure data communication network. A high-quality cryptographic process ensures high entropy, high key sensitivity, ability to resist known plaintext and chosen-plaintext attack, high speed of execution, high key space, high randomness, and resistance towards differential attack. Sridhar, et al. [16] proposed the several kinds of image encryption and decryption strategies. In the advanced computerized world, the transmitting and storing of multimedia content is more. However, the security level of computerised data while transmitting is an enormous issue.

Ghebleh, et al. [17] proposed an efficient and secure color and grayscale image encryption scheme that utilizes a chaining of skew tent maps as its pseudorandom number generator. The proposed scheme convolves the shuffling and mixing operations into several rounds for enhanced security. Mondal, et al. [18] proposed A contemplator on topical image encryption measures. Image encryption contributes a preeminent bite to charter security for secure sight data communication over the internet. The work illustrates a survey on image encryption in different domains providing concise exordium to cryptography, moreover, furnishing the review of sundry image encryption techniques. Rehman, et al. [19] proposed a novel way of confusion by introducing intra-permutation and Exclusive-OR operation with complementary DNA rules that brings randomness in the image. The proposed algorithm requires only single round of confusion/diffusion operation to achieve high quality of encryption results Chanu, et al. [20] proposed a comprehensive survey from over 100 papers which explains the new approaches and challenges. This paper also provides a comparative analysis of different methods based on different properties.

Raghav, et al. [21] proposed Security and Cryptography in Images and Video Using Elliptic Curve Cryptography (ECC). The proposed method shows that more powerful modern encryption techniques based upon Shannon theory. Image encryption techniques vary from region selection algorithms to spatial and frequency domain algorithms. Nithyakalyani, et al. [22] proposed fingerprint image encryption scheme based on DNA encoding and chaotic Logistic map. using the Logistic map chaotic sequences are generated and scrambled them by performing route cipher method. Rajendran, et al. [23] proposed an update on medical data

steganography and encryption. Steganography is the method of protection of files such as images, videos, or text messages by concealing their information from unauthorized users using methods of encryption and masking of data and embedding them into different images or text files. Farri, et al. [24] proposed a robust blind and secure video watermarking method based on integer wavelet transform and the generalized chaotic sine map. In this method, integer wavelet transform is applied to each main frame of the standard video. Ismael, et al. [25] proposed a new technique for encryption called DNA-DES that is more robust than traditional data encryption standard (DES). The proposed technique integrates concepts derived from DNA, ribonucleic acid, and nucleic acids to increase the key space and number of available permutations of traditional DES.

3. Proposed Methodology

The proposed visual cryptography method is used to send the image to the receiver as securely and confidentially. The image is transferred as shares and all shares are stacked together to get back the original image. The proposed method is used to create the shares from their pixel values. The pixel values of the colour image (RGB image) are extracted from the original image and represent as matrix (P*Q). The extracted pixels values are used to create the multiple shares (share1, share2... share n) and the shares are divided into blocks. The blocks of the shares are encrypted by using the elliptical curve cryptography method and the encrypted image is decrypted by using the decryption of the RSA method. Finally, the output image is compared with the original image for evaluating their performance by using the peak signal noise ratio (PSNR) value, Mean square error (MSE) and correlation coefficient (CC).

3.1 Block Diagram

Figure 1 shows the block diagram of the proposed method of the visual cryptography and its each block are explained in the following. The pixel values of the secret colour image (original image) are extracted and take as RGB pixel values, and these values are separately indicated as matrix and the size of the matrix is the same size of the original image size (P*Q). The original pixel values of the image are

$$Pixel = \sum R + G + B \tag{1}$$

Here, *pixel* is the total values of the Red, Green, and Blue.

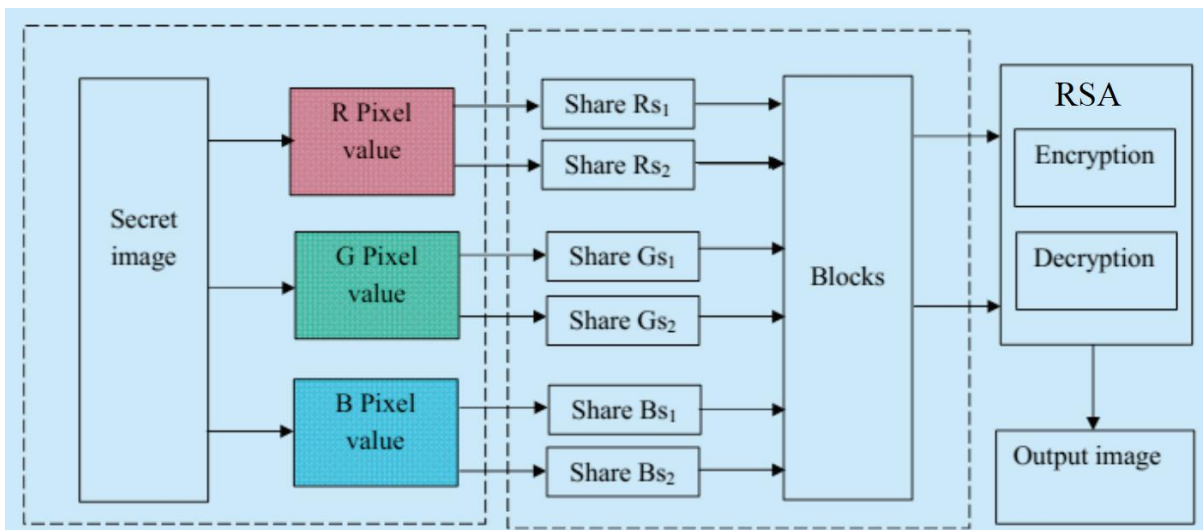


Figure 1. Block diagram of proposed method.

3.2.1 Share creation

Each original pixel of the secret image is appeared in ‘n’ modified versions called shares. Each share is a collection of sub-pixels of the RGB image. Each R, G, B shares are based on the pixel values of the RGB image. The share for RGB is separately indicated as R_s , G_s and B_s and indicated as

$$R_s = \int_l^k \lim_{k \rightarrow 1} \text{ton} R_{ab} \tag{2}$$

$$G_s = \int_l^k \lim_{k \rightarrow 1ton} G_{ab} \tag{3}$$

$$B_s = \int_l^k \lim_{k \rightarrow 1ton} B_{ab} \tag{4}$$

Here, a and b are the positions in matrix, R_s , G_s and B_s are the shares of the RGB. The R_{ab} , G_{ab} and B_{ab} are components of the image pixel. The R, G and B band pixel values are extracted from the original image and take as the separate matrix. The shares are created based on the splitting the image into various regions. The secret sharing scheme is to encrypt a secret image into n meaningless share images. It cannot leak any information about the original image unless all the shares are obtained. Shares are obtained from the original secret image Before the encryption, first it is finding the number of shares(n) to be generated. The user can give any value for n. Before separating the shares, the basic matrices are first constructed based upon the number of shares to be created. A random Key is generated based on block size of the secret image. Usually, the block size will be 4 x 4 or 8 x 8. The numbers of shares are created based on the number of basic matrices if the number of shares is 2S, where S is the number of basic matrices and the S is greater than or equal to 2($S \geq 2$). The basic matrices are obtained by dividing every pixel value in R, G and B by S. For example, let the pixel value in R is 123, S is 2. $123 / 2 = 61.5$. So, the corresponding pixel value in the first and second basic matrix is 42 and the third basic matrix is 43. Therefore $61+62 = 123$. If $S=3$, then the number of shares to be produced are $2 \times 3 = 6$. Then, the shares can be constructed by XORing basic matrices on different combination. Here, the number of basics matrices is 2 and number of shares is 4. The basic matrices construct from the pixel value of the R, G, and B divide by two. For example,

$$R = \begin{bmatrix} 227 & 227 & 228 & 225 \\ 227 & 226 & 227 & 223 \\ 226 & 225 & 227 & 225 \\ 226 & 226 & 226 & 227 \end{bmatrix} \tag{5}$$

$$G = \begin{bmatrix} 134 & 134 & 136 & 133 \\ 133 & 133 & 134 & 130 \\ 130 & 129 & 132 & 130 \\ 130 & 130 & 130 & 131 \end{bmatrix} \tag{6}$$

$$B = \begin{bmatrix} 125 & 123 & 122 & 116 \\ 121 & 118 & 117 & 112 \\ 113 & 111 & 111 & 107 \\ 110 & 107 & 106 & 105 \end{bmatrix} \tag{7}$$

Let generate the key matrix K_m randomly.

$$K_m = \begin{bmatrix} 53 & 132 & 254 & 83 \\ 161 & 134 & 108 & 209 \\ 191 & 105 & 248 & 89 \\ 128 & 32 & 224 & 73 \end{bmatrix} \tag{8}$$

After that, the basic matrices are created above mentioned method and they are denoted as R_{b1} and R_{b2} .

$$R_{b1} = \begin{bmatrix} 113 & 113 & 114 & 112 \\ 113 & 113 & 113 & 111 \\ 113 & 112 & 113 & 123 \\ 113 & 113 & 113 & 113 \end{bmatrix} \tag{9}$$

$$R_{b2} = \begin{bmatrix} 114 & 114 & 114 & 113 \\ 114 & 113 & 114 & 112 \\ 113 & 113 & 114 & 123 \\ 113 & 113 & 113 & 114 \end{bmatrix} \tag{10}$$

Before share creation, the following operation is performed with the R_{b1} and R_{b2} matrices.

$$B_{R1} = 128 - R_{b1} \tag{11}$$

$$B_{R2} = R_{b2} \tag{12}$$

$$B_{R2} = \begin{bmatrix} 114 & 114 & 114 & 113 \\ 114 & 113 & 114 & 112 \\ 113 & 113 & 114 & 123 \\ 113 & 113 & 113 & 114 \end{bmatrix} \tag{13}$$

The red band shares are created by using the XOR operation with the basic matrices and the key matrices.

$$RS_1 = B_{R1} \oplus K_m(5) RS_2 = B_{R1} \oplus B_{R2}(6) \tag{14}$$

$$RS_3 = B_{R2} \oplus RS_1(7) \tag{15}$$

$$RS_4 = RS_1 \oplus R(8) \tag{16}$$

From that above process apply other two-pixel values of the green (GS1, GS2, GS3, GS4, Km) and blue (BS1, BS2, BS3, BS4, Km) bands used for creating the multiple shares. In the share reconstruction process multiple shares are stacked together to get the original image. That means

$$R = R_{S1} \oplus R_{S2} \oplus R_{S3} \oplus R_{S4} \oplus K_m \tag{17}$$

$$G = G_{S1} \oplus G_{S2} \oplus G_{S3} \oplus G_{S4} \oplus K_m \tag{18}$$

$$B = B_{S1} \oplus B_{S2} \oplus B_{S3} \oplus B_{S4} \oplus K_m \tag{19}$$

After shares are reconstructed and then the encryption and decryption method based on RSA method applied on each colour bands of the reconstructed shares. Each colour band images are divided into blocks before the encryption and decryption operation. The blocks are divided into 4*4 as block size. From that above operations the numbers of multiple shares are created and then the encryption and decryption method based on RSA method applied on that share. The shares are divided into blocks before the encryption and decryption operation. The blocks are divided into 4*4 as block size.

3.2.2 RSA Encryption

RSA is the most used public key encryption algorithm. RSA computation occurs with integers modulo $n = p \cdot q$. It requires keys of at least 1024 bits for good security. Keys of size 2048 bit provide best security. Widely used for secure communication channel and for authentication to identity service provider. RSA is too slow for encrypting large volumes of data. but it is widely used for key distribution Following steps are followed in RSA to generate the public and private keys

Step 1: Consider two large prime numbers p and q such that $p \sim q$.

Step 2: Compute $n = p \cdot q$

Step 3: Compute $\varphi(pq) = (p - 1) \cdot (q - 1)$

Step 4: Consider the public key k_1 such that $gcd(\varphi(n), k_1) = 1; 1 < k_1 < \varphi(n)$

Step 5: Select the private key k_2 such that $k_2 \cdot k_1 \text{ mod } \varphi(n) = 1$

Step 6: Calculate cipher text C from plaintext P such that, $C = P^{k_1} \text{ mod } n$

Step 7: Encryption and Decryption are done as follow Encryption:
 $P = C^{k_2} \text{ mod } n = P^{k_1 k_2} \text{ mod } n$

4. Results and Discussions

4.1 Experimental Results

Figure 2 shows the original image RGB bands image, and its share images. Each band has four different shares based on the multiple share creation. The shares are created based on the above-mentioned multiple share creation method. Here, four shares are generated for each different original input image and shares are shown in Figure 2. The overall performance of the proposed method is analysed by using the peak signal noise to ratio value, mean square error and correlation coefficient value. Also, different attacks are used such as salt and pepper noise, filtering noise and blurring noise to analyze the proposed method effectiveness. In Figure 2, various input images are employed for producing the different shares and aggregate four separate shares are

made. At the point when all shares are stacked together, they will get the primary secret image. From this anyone of the shares of the multiple shares is the insignificant image which does not give any data of the primary image. The three distinctive images are demonstrated in the share images and they are indicated as R, G, and B band share images. The initial column of the image is demonstrated in the original image before the creation of the share. At that point the segments 2, 3, 4 and 5 are demonstrated the shares of the original secret image. Each one band has its own shares by utilizing the shares creation strategy.


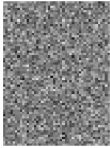




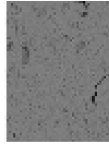






| Original image | Share 1 | Share 2 | Share 3 | Share 4 |
|---|---|---|---|---|
|  |  |  |  |  |
| |  |  |  |  |
| |  |  |  |  |

Figure 2. VC results of Lena image.

In Figure 3, the encrypted images and its stacked images are shown in the table for different images. The stacked images are taken from the shares of the images and this stacked image is given as input to the encryption method. So, the given image is encrypted clearly in the encryption process. The encrypted images are shown for the encrypted images for R, G and B with their stacked images. The encrypted image is taken after the encryption method applied on it the image and it is not given any information about the image. So, the secrecy of the image is maintained without any deviation the image. Only the blurred images are getting after the image encryption method. After encryption, the decryption process is used to retrieve the original image without any deviation of the image.















| Original image | Stacked images | | | Encrypted images | | |
|---|---|---|---|--|---|---|
| | R | G | B | R | G | B |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Figure 3. Encrypted results of various images.

Figure 4 shows the proposed method with their PSNR, MSE and CC values. In Figure 4, the row 1, 2, 3 and 4 demonstrates the analysis results of the original images. Here, the four separate images are employed to dissect the proposed strategy. The proposed system contains the numerous share creation and encryption and decoding technique for the RSA strategy. In Figure 4, it has the original image with its histogram image, final output

image with its histogram image and its execution test qualities like PSNR, MSE and CC. The histogram image demonstrates how the image pixels are dissected in the image, which gives the contrast between the original image and final image in the wake of applying the proposed strategy for analysing the images. Through images, the proposed strategy relates to the image and output images are indicated by their PSNR values. The PSNR value indicates the nature of the image to the output image after the proposed technique connected with it. Here, the PSNR qualities are 58.0025, 57.4297. Also, the MSE values and CC values are shown in Figure 4. From the MSE values, it gives the original image and decrypted image differences, and it should be minimum for any images. Here, the MSE values are nearly 0.1 and it gives the original image is retained in decrypted image after the proposed part.


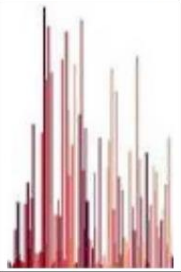
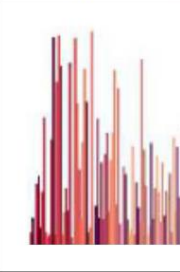


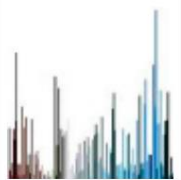
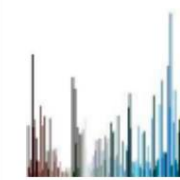

| Original image | Histogram | | Final Image | PSNR value | MSE | CC |
|--|--|--|--|------------|--------|----|
| | Original image | Decrypted image | | | | |
|  |  |  |  | 58.0025 | 0.103 | 1 |
|  |  |  |  | 57.4297 | 0.1176 | 1 |

Figure 4. Performance evaluation of proposed method

4.2 Attacks

The different types of attacks applied on the image for stealing the information of the image or blurring the image for reducing its quality of the image. The positions of the pixel values are changed in the image for finding the image without changing its image quality. The following tables are shown the attacks applied image and its encrypted images and stacked images. In Figure 5, the salt and pepper attack are applied on the encrypted image and the encrypted image is shown in table. The attack is changed the image information, but the proposed method is retrieving the image with the minimum noise and its PSNR value is nearly 60% retrieved. So, it is maximum retrieve the information with the minimum distortion. Figure 5 shown the proposed method with the attack applied on it and after attack is applied on the image, the proposed method is effectively retrieving the original image nearly 70% of the original image values is retrieved without affecting the image quality.

4.3 Performance comparison with existing methods

From the table 1, the PSNR value of the proposed method is higher than the existing method and mostly it is 35% to 40% improved from the exiting method. So, the image quality is improved by the proposed method. In MSE value, the mean square error is minimized by the proposed method compared with the existing method. Because the MSE value shows the how the pixels are exchanged and shuffled within the image and how it is retrieved by the method. From that, the image quality also improved, and it has very low error value in proposed method. In the Correlation Coefficient value, the proposed method has the maximum CC value which is 1. It indicates that all pixels are retrieved by the proposed method. So, the image quality is improved. It is comparatively low in the existing method. The PSNR value graph is clearly shown that the proposed method is given better result and it retrieves the maximum the original image quality and the existing method compared with the proposed method values. From that, the proposed method is given best result






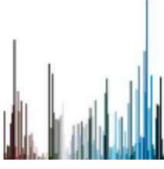


| Original image | Histogram | | Final output | PSNR value | MSE | CC |
|---|---|---|--|------------|--------|--------|
| | Original image | Decrypted image | | | | |
|  |  |  |  | 39.0097 | 9.2797 | 0.9976 |
|  |  |  |  | 38.3616 | 9.939 | 0.9987 |

Figure 5. Performance evaluation of proposed method in presence of attacks.

Table 1. Performance comparison with existing methods

| Method | Proposed Method | | | Existing Method [13] | | |
|--------|-----------------|--------|----|----------------------|--------|--------|
| | PSNR | MSE | CC | PSNR | MSE | CC |
| Lena | 58.0025 | 0.1030 | 1 | 42.8116 | 3.4281 | 0.9745 |
| House | 57.4297 | 0.1176 | 1 | 42.7093 | 3.485 | 0.9641 |
| Pepper | 56.684 | 0.1454 | 1 | 42.7888 | 3.4249 | 0.9729 |
| Baboon | 58.1437 | 0.0997 | 1 | 42.9096 | 3.3378 | 0.992 |

5. Conclusion

In this work, the utilization of RSA encryption and decryption for visual cryptography has demonstrated exceptional performance. A multitude of seemingly random shares are generated, which are effectively encrypted and decrypted using the RSA technique. Notably, the PSNR values achieved are 58.0025, 57.4297, 56.684, and 58.1438, indicating the preservation of image quality even in the presence of attacks on the secret image. The correlation coefficient values reveal that the images exhibit a high degree of similarity, with values approaching 1, while the mean square error values are 0.103, 0.1176, 0.1454, and 0.0997. These results affirm that the proposed method successfully retains the quality of the original image without significant variation. Through correlation coefficient analysis and histogram estimations, it is evident that the encryption technique effectively safeguards the confidentiality of the secret image. Consequently, the image confidentiality is consistently upheld, and the recovered image is an accurate representation of the original image, with no adverse impact on its quality. In future research, further enhancements can be made by employing optimization techniques to improve the performance of the PSNR. This approach will not only enhance image quality but also minimize the mean square error value.

References

[1] Sun, Elaine Y-N., et al. "Efficient recoverable cryptographic mosaic technique by permutations." IEEE Transactions on Circuits and Systems for Video Technology 31.1 (2020): 112-125.
 [2] Sahu, Aditya Kumar, and Monalisa Sahu. "Digital image steganography and steganalysis: A journey of the past three decades." Open Computer Science 10.1 (2020): 296-342.
 [3] Favorskaya, Margarita N., Lakhmi C. Jain, and Eugenia I. Savchina. "Perceptually tuned watermarking using non-subsampled shearlet transform." Computer Vision in Control Systems-4: Real Life Applications (2018): 41-69.

- [4] Ud Din, Shams, et al. "Secure exchange of medical data using a novel real-time biometric-based protection and recognition method." *Electronics* 9.12 (2020): 2013.
- [5] Begum, Mahbuba, and Mohammad Shorif Uddin. "Digital image watermarking techniques: a review." *Information* 11.2 (2020): 110.
- [6] Sarmah, Dipti Kapoor, Anand J. Kulkarni, and Ajith Abraham. *Optimization models in steganography using metaheuristics*. Springer International Publishing, 2020.
- [7] Chao, Jin, et al. "CaRENets: Compact and resource-efficient CNN for homomorphic inference on encrypted medical images." *arXiv preprint arXiv:1901.10074* (2019).
- [8] Bhandari, Vijay, et al. "Development of secure image transposal algorithm using 16* 16 quantization table." *International Journal of Scientific Research & Engineering Trends* 4 (2018).
- [9] Aharoni, Ehud, et al. "Tile Tensors: A versatile data structure with descriptive shapes for homomorphic encryption." *arXiv preprint arXiv:2011.01805* (2020).
- [10] Ahmed, Kareem, and Ibrahim El-Henawy. "Increasing robustness of data encryption standard by integrating DNA cryptography." *International Journal of Computers and Applications* 39.2 (2017): 91-105.
- [11] Almalkawi, Islam T., et al. "A lightweight and efficient digital image encryption using hybrid chaotic systems for wireless network applications." *Journal of Information Security and Applications* 49 (2019): 102384.
- [12] AL-Hashemy, Rageed Hussein, and Sadiq A. Mehdi. "A new algorithm based on magic square and a novel chaotic system for image encryption." *Journal of Intelligent Systems* 29.1 (2019): 1202-1215.
- [13] Bisht, Ankita, et al. "A color image encryption technique based on bit-level permutation and alternate logistic maps." *Journal of Intelligent Systems* 29.1 (2019): 1246-1260.
- [14] Shah, Dawood, and Tariq Shah. "A novel discrete image encryption algorithm based on finite algebraic structures." *Multimedia Tools and Applications* 79 (2020): 28023-28042.
- [15] Kumari, Manju, Shailender Gupta, and Anjali Malik. "A superlative image encryption technique based on bit plane using key-based electronic code book." *Multimedia Tools and Applications* 79 (2020): 33161-33191.
- [16] Sridhar, B. "Performance Evaluation of Different Encryption Techniques." *Research Journal of Engineering and Technology* 9.3 (2018): 227-232.
- [17] Ghebleh, Mohammad, and Ali Kanso. "A novel efficient image encryption scheme based on chained skew tent maps." *Neural Computing and Applications* 31 (2019): 2415-2430.
- [18] Mondal, Jayanta, and Debabala Swain. "A contemplator on topical image encryption measures." *Cryptography: Breakthroughs in Research and Practice*. IGI Global, 2020. 556-573.
- [19] Rehman, Aqeel Ur, and Xiaofeng Liao. "A novel robust dual diffusion/confusion encryption technique for color image based on Chaos, DNA and SHA-2." *Multimedia Tools and Applications* 78.2 (2019): 2105-2133.
- [20] Chanu, Oinam Bidyapati, and Arambam Neelima. "A survey paper on secret image sharing schemes." *International Journal of Multimedia Information Retrieval* 8.4 (2019): 195-215.
- [21] Raghav, Piyush, and Amit Dua. "Security and Cryptography in Images and Video Using Elliptic Curve Cryptography (ECC)." *Cryptographic and Information Security*. CRC Press, 2018. 141-170.
- [22] Nithyakalyani, M. R., V. Palanisamy, and R. Anandhajothi. "Fingerprint template encryption scheme based on chaotic map and DNA sequence." *International Journal of Pure and Applied Mathematics* 118.7 (2018): 297-305.
- [23] Rajendran, Sindhu, et al. "An update on medical data steganography and encryption." *Recent Trends in Image and Signal Processing in Computer Vision* (2020): 181-199.
- [24] Farri, Elhameh, and Peyman Ayubi. "A blind and robust video watermarking based on IWT and new 3D generalized chaotic sine map." *Nonlinear Dynamics* 93 (2018): 1875-1897.
- [25] Ismael, Ahmed Yousif. *Construct a Strong and High Performance Algorithm to Generate Pseudorandom Number Generator (PRNG) for Stream Cipher*. Diss. University of Baghdad, 2019.