

Enhanced Visual Cryptography for Color Images using Error Diffusion based AES Encryption

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

Visual cryptography is a technique that allows visual information to be encrypted in such a way that the decrypted information appears as a visual image. To enhance visual cryptography for color images, the proposed technique utilizes the RGB color space. The process involves several steps, including color decomposition and error diffusion. Color decomposition breaks down the color image into its constituent color channels (red, green, and blue). Each color channel is then treated as a separate grayscale image and undergoes visual cryptography individually. Error diffusion is a technique used in half-toning, where the quantization residual (the difference between the original pixel value and the quantized value) is distributed to neighboring pixels that have not been processed yet. This helps in maintaining the overall visual quality of the decrypted image. In the proposed technique, the image is encrypted using four shares: cyan, magenta, yellow, and a mask. The mask is generated using a random function and consists of half-black and half-white pixels in each block. To review the secret image, all the shares are stacked together. By combining the shares, the original image can be visually decrypted. The addition of the AES algorithm can further enhance the security of the encryption process. Advanced Encryption Standard (AES) is a widely used symmetric encryption algorithm that provides strong cryptographic protection. By incorporating the AES algorithm at an appropriate stage in the visual cryptography process, the security of the encrypted shares can be strengthened. The specific details of where and how the AES algorithm is incorporated would depend on the implementation and design choices of the visual cryptography system.

Keywords: Visual cryptography, transparent shares, security, RGB color space, color decomposition, error diffusion, quantization residual, half-toning.

1. Introduction

An image provides a lot of information. Almost one-third of our cortical brain region is dedicated to the visual processing of the perceived information. Images are a significant source of information. Images have various applications in a variety of fields such as storing patient medical information, capturing aerial images by satellite imagery, capturing interplanetary motion images by telescopes, storing an individual's identity in the form of

fingerprints, or iris images, etc. [1]. Digital communication generates millions of digital data in the form of digital images. Cryptography is an efficient way to safeguard sensitive information. Cryptography is a method of storing and transmitting data in a form intended for reading and processing the information. The advancement of encryption and decryption leads to an infinite future. Security analysis depicts the schematic encryption the scheme can endure numerous crypt analytical attacks. Reliability and protection of information are equally critical to obtain respect from the recipient for the information obtained [2]. Encryption of images plays a key role if the images are to be kept private and transmitted securely. The encryption task involves distorting the pixel intensity of the image input to create a cipher image that is completely different from the image input. Using the secret keys, the receiver decrypts the images and returns the original image. There are various private keys used by the sender and receiver in asymmetric key cryptography which are further used to generate the shared secret key. On the other hand, symmetric-key cryptography involves encryption and decryption with a single key that the sender and receiver are secretly known to have [3]. Most common processes involve symmetric approaches such as AES, DES, Hill cipher, etc. to protect the information stored in the images. While they are easy to implement and fast to process, the amount of security given to the image is lacking for these methods. This is overcome by incorporating asymmetric techniques such as RSA, ECC, ElGamal, etc. that provide more security but a trade-off in ease of implementation and feasibility of computations [4]. This paper used an artificial neural network (ANN) algorithm in encryption/decryption based on specific characteristic features. However, these processes become more difficult to deploy with time complexity when communicating several encryptions and decrypting parameters through an unsecured channel. Elliptic curve and ElGamal cryptosystems include asymmetric key cryptography, while Hill Cipher, AES, and Double Playfair Cipher are symmetric key algorithms [5]. Asymmetric key cryptography is highly secure but requires significant computational complexities that are further eased using asymmetric key cryptography algorithms in addition to asymmetric key cryptography [6]. The RGB model is a widely used model for representing and storing digital color images. In this model, the image is represented by three independent channels. Each channel is a 2D matrix. The first matrix represents the red colour, the second matrix represents the green colour, and the third matrix represents the blue colour. The three matrices are of the same width and height. Each pixel in the colour image is represented by three values that are the three corresponding values on the three matrices. Each value can range from 0 to 255. In this way, the RGB model can represent more than 16 million distinct colours. Many recent scientific papers have shown that combining DNA cryptography and chaotic sequences leads to very efficient and promising results with respect to nonlinearity, randomness and resistance to common attacks. This paper presented an encryption technique based on 4D Lorenz hyperchaos and DNA encoding [7]. First, an integer wavelet transform IWT is applied to produce approximation and detail bands of the input image. Then, the LL band is permuted using chaotic sequences, and then they are encoded using DNA. Finally, an operation called DNA-XOR is performed to produce the encrypted image. This paper presented a color image encryption technique that uses a 2D hyperchaotic map to scramble the initial image and then uses a logistic-tent map to produce a cover image [8]. Then, SHA-2 is applied to this cover image to produce a mask image, and the two images are encoded using DNA, followed by

Enhanced Visual Cryptography for Color Images using Error Diffusion based AES Encryption

many diffusions to produce cipher image. In this paper, a novel RGB image encryption technique is proposed, based on a logistic chaotic function and several rounds of DNA encoding. First, the logistic function is used to generate 16 randomly generated round keys. The chaotic sequences are then employed in a Feistel structure over different rounds to change individual pixels by performing key-based random nonlinear DNA encoding, transpositions, diffusions and substitutions. An initial 16×16 DNA matrix is built up, where the entries of this matrix are four sequential DNA symbols [9]. The matrix is first permuted according to the round key, and then Playfair is used to perform the substitution of each four DNA symbols from the bit representation of the image with the corresponding patterns, according to the common rules of Playfair. The nonlinearity of the generated matrix ensures the robustness of the technique against differential attacks [10]. The basic Playfair substitution is preceded and followed by several transpositions and substitutions to increase the randomness of the intermediate representations. To decrypt, the encryption steps are repeated in reverse.

2. Literature Survey

Melkemi, et al. [11] proposed Voronoi-based image representation applied to binary visual cryptography. The proposed Voronoi-based Visual Cryptography (VVC) technique permits to drastically reduce the amount of encoded and transmitted information by comparison with a traditional VC scheme. Geetha, et al. [12] proposed Multiple share creation based visual cryptographic scheme using diffusion method with a combination of chaotic maps for multimedia applications. The proposed visual cryptographic method is divided into three phases namely, i) Separation of color bands, ii) Generation of several shares and iii) Encryption & Decryption. Anwar, et al. [13] proposed A pixel permutation-based image encryption technique using chaotic map. The authors presented an overview of the different encryption algorithms in details, analyzing its effect in the field of image cryptography. Chowdhary, et al. [14] proposed an analysis for performing image encryption and decryption by hybridization of Elliptic Curve Cryptography (ECC) with Hill Cipher (HC), ECC with Advanced Encryption Standard (AES) and ElGamal with Double Playfair Cipher (DPC). Fatahbeygi, et al. [15] proposed a new robust image watermarking algorithm based on blocks classification and visual cryptography (VC). The VC technique is used to generate two image shares: A master share that is constructed according to the block classification results and an owner share generated by using the master share together with a binary watermark. Kaur, et al. [16] proposed A new image encryption method based on permutation–diffusion architecture. Permutation and diffusion operations are performed row-wise and column-wise on input image. To permute and diffuse the pixels, Lorenz-like chaotic system with varying bifurcation parameter is used to generate six random sequences. Singh, et al. [17] proposed a secure way of obscuring the information based on XOR based Visual Cryptography (VC). It obscures the secret information into multiple meaningful shares prior to outsourcing which reduces the vulnerability of random looking shares to cryptanalysis. Dawahdeh, et al. [18] proposed A new image encryption technique that combines Elliptic Curve Cryptosystem with Hill Cipher (ECCHC) to convert Hill cipher from symmetric technique to asymmetric one and increase its security and efficiency and resist the hackers.

Geetha, et al. [19] proposed an OGWO based ECC (Elliptic Curve Cryptographic) approach. The proposed visual cryptographic scheme is divided into three phases namely, (a) Separation of color bands, (b) Generation of numerous shares and (c) Optimal Encryption and Decryption. Shankar, et al. [20] proposed Adaptive Elephant Herding Optimization (AEHO). This proposed image safety model signcryption with elephant-based optimization method used. This technique Signcryption is the technique that mixes the functionality of encryption and digital signature in a single logical step. Guo, et al. [21] proposed a new simple image encryption technique using the Beta chaotic map for performing the confusion and diffusion of input plain image. This image encryption is further applied to the multiple secret sharing (MSS). Ye, et al. [22] proposed a new meaningful image encryption algorithm based on compressive sensing and information hiding technology, which hides the existence of the plain image and reduces the possibility of being attacked. Zhang, et al. [23] proposed a new optical color image encryption scheme. Because of the spatial nonlinear coupling which replaces traditional adjacent coupling, the 2DNLCML system contains good features such as ergodic pseudo-random sequence, less periodic windows in bifurcations and larger range of parameters in chaotic dynamics, which is more suitable for image encryption. Dolendro Singh, et al. proposed [24] An approach for the generation of visually meaningful multiple-image encryption scheme. The noise-like image lures an adversary to carry out attacks. Multiple cipher image data are embedded in the insignificant real data of a host image. Mahmud, et al. [25] proposed a new symmetric image encryption method using the concepts of ribonucleic acid (RNA) sequence and genetic algorithm (GA), called RNA-GA. The proposed method starts by generating specified number of initial cipher images using logistic map function.

3. Proposed Methodology

The proposed technique determines that the secret sharing scheme with CMY colour space is visual cryptography. Visual cryptography is an algorithm that is used to encrypt and decrypt the image. The flowchart of the proposed system is shown in Figure 1. Visual Cryptography involves image processing, dividing the original image to few halftone images for encryption and later combining all the images for decryption. A method for image processing is performed on the image in order to obtain increase image certain operation or to pick up some beneficial information. Import image for doing analyzing and processing of the image. The output can change the image or image analysis-based reports. Convert an image from RGB to the CMY color space through the image processing. For the encryption, separate the original image to halftone image using color decomposition. Then, use the error diffusion to encrypt the halftone image with a pair of pixels. This kind of component image is like a transparent, and no one can see the image behind the scheme. For the decryption, combine all of the sharing images to reveal the confidential image. In additional to this, image histogram was also created. It was used to show the difference between the original image and decryption image. First, user needs to load a new image, and the image type must be JPG or PNG. Then, image will direct convert to Qt format. Second, choose the scheme which is RGB or CMY to generate the shares. If the user does not select the scheme, system will pop up an error message and continue at the same step. Third, generate the shares according to the user's choice. In this step, system will split the red, green, and blue components of the image.

Enhanced Visual Cryptography for Color Images using Error Diffusion based AES Encryption

Then, convert these three colours to cyan, magenta, and yellow when the user chooses the CMY scheme. The conversion is given by the formulae $\text{cyan} = 225 - \text{red}$, $\text{magenta} = 225 - \text{green}$, and $\text{yellow} = 225 - \text{blue}$. After that, system will convert CMY to halftone with the error diffusion. Using the middle intensity which is 128 to do the calculation until each pixel becomes 255 or 0, besides, generate a mask with the random half white and half black pixel. Fourth, combine all of the shares and masks to display the secret image. In this step, user needs to click the checkbox to combine all the shares. Then, system will do the calculation. Set the intensity of the shares that becomes 128 when the pixel value of mask is 0, otherwise, minus by 255. Lastly, click the save button to create a file and save the output of the image and the shares with the PNG image type.

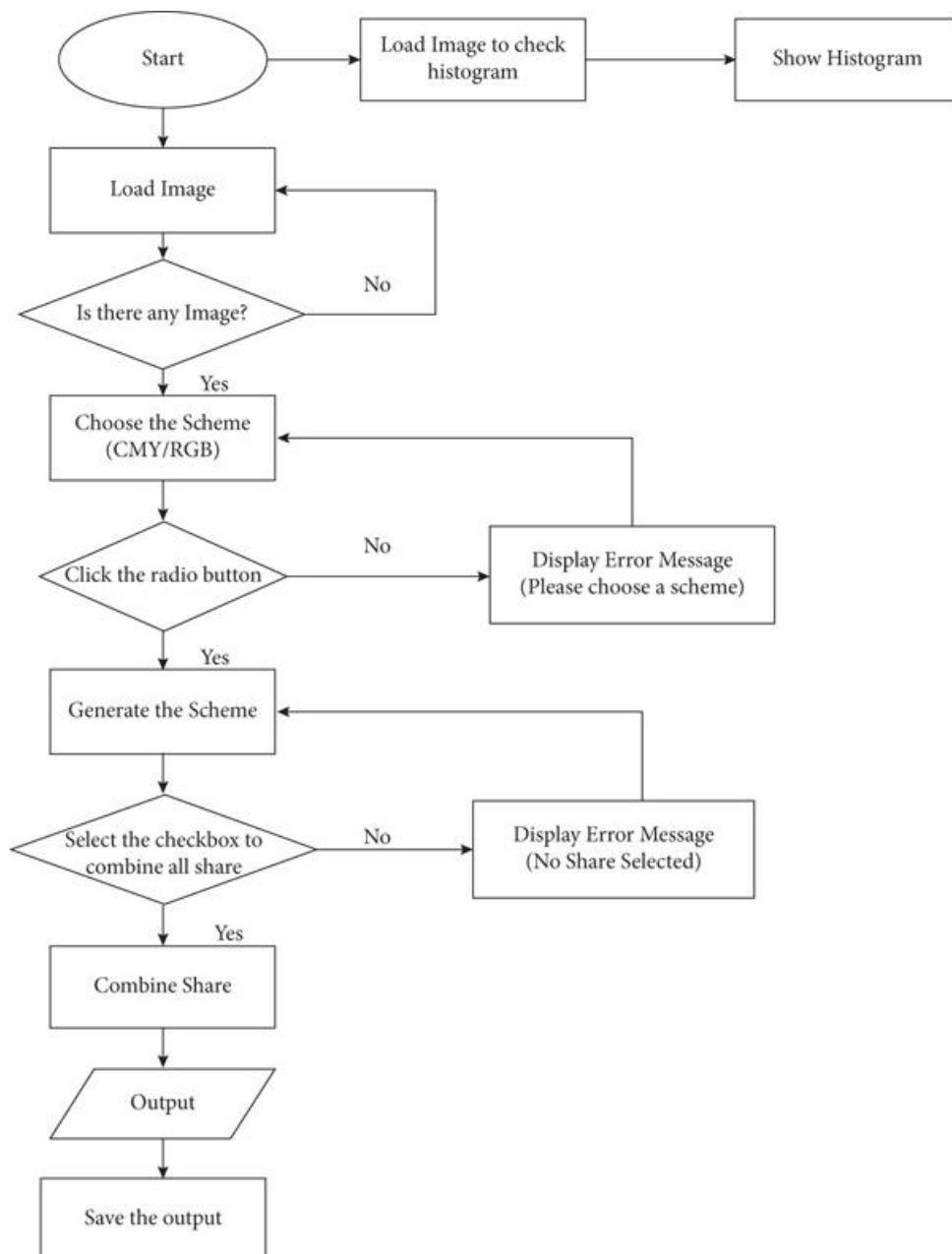


Figure 1. Flow chart of the proposed system.

3.1 Image Processing

The image is a description of the visual perception of artifacts. For example, it is a picture made using a camera or other two-dimensional picture. Images is the magnitude of the distribution of one or more colours. It can capture by optical equipment, for instance, microscopes, telescopes, lenses, mirrors and camera. There are many kinds of images use in the visual cryptography such as grayscales images, binary image, and colour images. But in this research, the colour image will be chosen to do the visual cryptography. It was because the CMY components will separate from a colour image. The image file format will be JPG and PNG. They are the most popular file format that can easily get from the online resource. In the image processing, the imported image will convert from an RGB to CMY colour space. Afterward, do the colour decomposition for the import image before converting it to the halftone image. The cyan, magenta, and yellow colours will separate from the image for each pixel through the colour decomposition. The following relationships of CMY and RGB: $C=225-R$, $M=225-G$, and $Y=225-B$. Thus, in the (x,y,z) representation, $(0, 0, 0)$ represents full white, and $(255, 255, 255)$ represents full black.

3.2 Error Diffusion

Error diffusion is a kind of halftone in which quantized residuals are distributed to neighbouring pixels that have not been processed. The main purpose is converting multilevel images to binary images; although, it has other application. It is different with other half toning methods, and it is classified as a regional operation because the operations performed by the algorithm at one location affect the operations that occur at other locations. Error diffusion with edge enhanced image tendency. Compared to other halftone techniques, this can make the image's text more readability. This method captures monochrome or colour images and decreases the amount of quantization levels. The general application of error diffusion related reducing the number of quantized states to only two per channel which is 255 or 0. There are many types of error diffusion, but only one-dimension error diffusion is used. The simplest form of this algorithm is to scan one pixel and one row with an image at a time, compared the current pixel with the half gray value. If it is higher than this value, white pixels will be generated in the generated image. If the pixel is less than half the brightness, black pixels are generated. The resulting pixels are completely bright or completely black; so, there are errors in the image. Then, add the error to the next pixel in the image and repeat the process. For example, the greyscale value is 100 of a pixel. This value is closer 0 than 255; so, it will automatically become 0, and 100 (the error) will be add into the next value.

3.3 Encryption and Decryption

Encryption is a way to hide the information into the true meaning of the information through the secret code method. An encryption data is also called cipher text, and it looks like a plaintext. The encrypted algorithms are formulas use to encode the information. Then, the visual image will be displayed by the decrypted information. The process of converting encrypt data to its original format is called decryption. Choose all of the shared images for doing the combination. Only by overlaying all the images can more clearly restored the secret image. The algorithms use in encryption and decryption is visual cryptography. Before starting to encrypt and encrypt an image, choose an image and import the image from the file

Enhanced Visual Cryptography for Color Images using Error Diffusion based AES Encryption

directory to the system. After that, image processing is done to convert the RGB to CMY colour space. After converting to CMY colour space, the visual cryptography process is as follows:

Step 1: Divide the image to three colour component images

Step 2: Error diffusion will be used to generate the halftone image. All the pixel of the halftone image will be expanded to block. Therefore, each block of the shared image contains two transparent (white) pixels and two-colored pixels

Step 3: Create a black and white share, known as a mask, which is double the size of the secret image in each direction. The block of pixels will randomly assign half black and half white in this mask

Step 4: Selecting the mask for check the pixel value, if cyan component is revealing, fill the positions corresponding to the position of the white pixels in the mask with a cyan pixel and the color to the opposite way

Step 5: According with (IV), do the same thing to check the magenta and yellow pixel value

Step 6: Repeating the steps (IV and V) until all pixel in the image is decomposed, then get the four-sharing image which is cyan, magenta, yellow, and black

Step 7: Lastly, using the four-sharing image and stack together, the value of pixel in mask is 0 will become 128; otherwise, it will be minus by 255, and the confidential image will be decrypted by human visual system.

3.4. Histogram Analysis

The image histogram is a histogram that can be used as graphical representation of the distribution of tones. The amount of contrast will describe by a histogram. It will calculate the brightness and darkness in a scene. In the program, it loads an image to do testing. Using Open CV function "Split", the image is divided into R, G, and B planes, hence three different colour lines will be shown in the histogram image. Third, using OpenCV function "calcHist" to calculate each R, G, and B planes of the histogram, the important things in here are BINS, DIMS, and RANGE. BINS means the number of pixels. Normally, it will be 256. DIMS means the number of parameters for data collect. In the program, DIMS value is always 1 as it refers to the intensity value of the data collected. RANGE means the intensity value. Normally, it will be [0, 256]. Lastly, plot the three lines of histogram in a new window.

3.5 AES 128-bit encryption

AES is an iterative instead of Feistel cipher. It is based on two common techniques to encrypt and decrypt data known as substitution and permutation network (SPN). SPN is a number of mathematical operations that are carried out in block cipher algorithms. Figure 2 shows the structure of AES, which can deal with 128 bits (16 bytes) as a fixed plaintext block size. These 16 bytes are represented in 4x4 matrix and AES operates on a matrix of bytes. In addition, another crucial feature in AES is number of rounds. The number of rounds is relied on the length of key. There are three different key sizes are used by AES algorithm to encrypt and decrypt data such as (128, 192 or 256 bits). The key sizes decide to the number of rounds such as AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.

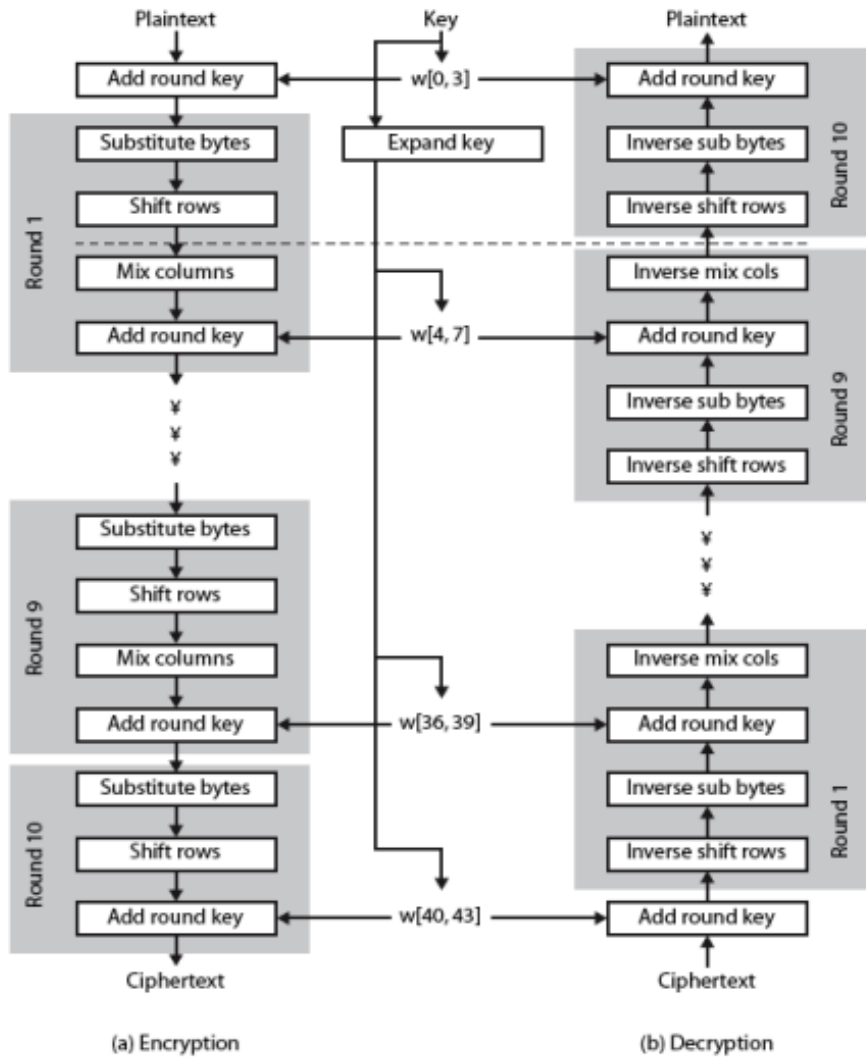


Figure 2. Structure of AES.

AES key Expansion: AES algorithm is based on AES key expansion to encrypt and decrypt data. It is another most important steps in AES structure. Each round has a new key. In this section concentrates on AES Key Expansion technique. The key expansion routine creates round keys word by word, where a word is an array of four bytes. The routine creates $4 \times (Nr+1)$ words. Where Nr is the number of rounds. The process is as follows: The cipher key (initial key) is used to create the first four words. The size of key consists of 16 bytes (k_0 to k_{15}) as shown in Figure 3 that represents in an array. The first four bytes (k_0 to k_3) represents as w_0 , the next four bytes (k_4 to k_7) in first column represents as w_1 , and so on. AES can use equation to calculate and find keys in each round easily as follows:

$$K[n]: w[i] = k[n-1]: w[i] XOR k[n]: w[i] \tag{1}$$

This equation uses to find a key for each round rather than w_0 . For w_0 must use equation that is different from above equation.

$$K[n]: w_0 = k[n-1]: w_0 XOR SubByte(k[n-1]: w_3 \gg 8) XOR Rcon[i] \tag{2}$$

Enhanced Visual Cryptography for Color Images using Error Diffusion based AES Encryption

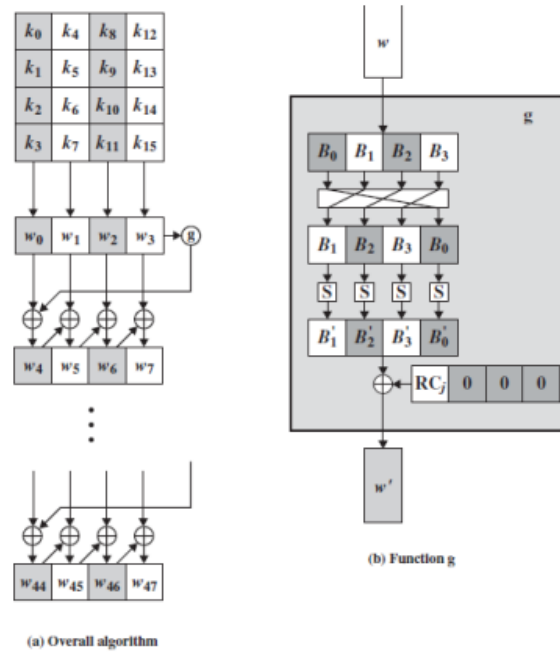


Figure 3. AES Key Expansion.

4. Results and Discussions

4.1 Experimental Results

Figure 4 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 4. 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 analyses the proposed method effectiveness. In Figure 4, 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. In Figure 5, 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.


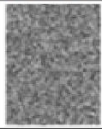











Original image	Share 1	Share 2	Share 3	Share 4
				
				
				

Figure 4. Visual cryptography results of Madrid image.





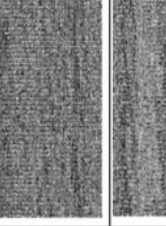
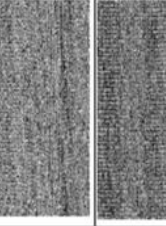





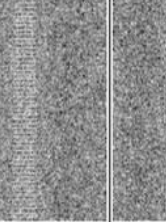


Original image	Stacked images			Encrypted images		
	R	G	B	R	G	B
						
						

Figure 5. Encrypted results of various images.

Figure 6 shows the proposed method with their PSNR, MSE and CC values. In Figure 6, 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 6, 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 56.684 and 58.1438. Also, the MSE values and CC values are shown in Figure 6. From

Enhanced Visual Cryptography for Color Images using Error Diffusion based AES Encryption

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.

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 7, 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 7 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.



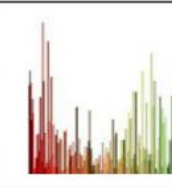


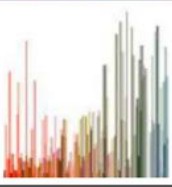
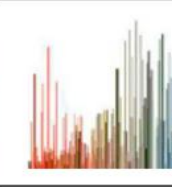
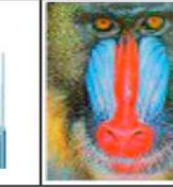
Original image	Histogram		Final Image	PSNR value	MSE	CC
	Original image	Decrypted image				
				56.684	0.1454	1
				58.1438	0.0997	1

Figure 6. Performance evaluation of proposed method


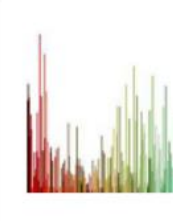
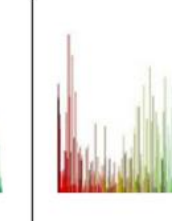


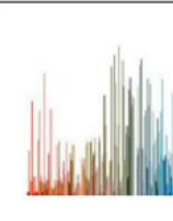
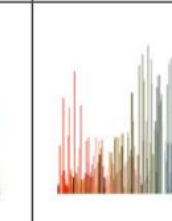
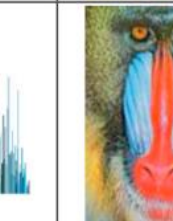
Original image	Histogram		Final output	PSNR value	MSE	CC
	Original image	Decrypted image				
				36.3878	17.584	0.9968
				42.8698	3.3988	0.9993

Figure 7. Performance evaluation of proposed method in presence of attacks.

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 existing 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

Table 1. Performance comparison with existing methods

Method	Proposed Method			Existing Method [13]		
	PSNR	MSE	CC	PSNR	MSE	CC
Lena	59.0025	0.09030	1	42.8116	3.4281	0.9745
House	59.4297	0.0876	1	42.7093	3.485	0.9641
Pepper	60.684	0.1254	1	42.7888	3.4249	0.9729
Baboon	51.1437	0.0797	1	42.9096	3.3378	0.992

5. Conclusion

Due to the widespread application of Internet technology, data security has become a crucial factor. In comparison to traditional cryptographic methods, human-based visual cryptography offers advantages such as reduced computational complexity and avoidance of complex encryption techniques. Visual cryptography provides a secure means of transferring images while hiding the information within them. The AES based visual encryption technology based on CMY color space and secret sharing has gained attention due to its ability to maintain secrecy and conceal color information. The generated and distributed secrets cannot be deciphered easily. Although the accuracy of CMY color space is superior to RGB color space, the resulting image may appear darker. Future work in this field could focus on reducing the overall time required for image encryption and decryption. To enhance security, digital watermarking and steganography techniques can be combined with visual cryptography, such as hiding information within the image and then encrypting it using visual cryptography. Additionally, video files can be divided into individual frames and encrypted using the proposed algorithm for each frame.

References

- [1] Zhang, Yong. "The fast image encryption algorithm based on lifting scheme and chaos." *Information sciences* 520 (2020): 177-194.

Enhanced Visual Cryptography for Color Images using Error Diffusion based AES Encryption

- [2] Ramasamy, Priya, et al. "An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic—Tent map." *Entropy* 21.7 (2019): 656.
- [3] Shivani, Shivendra, and Suneeta Agarwal. "VPVC: verifiable progressive visual cryptography." *Pattern Analysis and Applications* 21.1 (2018): 139-166.
- [4] Asgari-Chenaghlu, Meysam, Mohammad-Ali Balafar, and Mohammad-Reza Feizi-Derakhshi. "A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation." *Signal Processing* 157 (2019): 1-13.
- [5] Patro, K. Abhimanyu Kumar, and Bibhudendra Acharya. "An efficient colour image encryption scheme based on 1-D chaotic maps." *Journal of Information Security and Applications* 46 (2019): 23-41.
- [6] Naskar, Prabir Kumar, et al. "A robust image encryption scheme using chaotic tent map and cellular automata." *Nonlinear Dynamics* 100 (2020): 2877-2898.
- [7] Chen, Junxin, Lei Chen, and Yicong Zhou. "Cryptanalysis of a DNA-based image encryption scheme." *Information Sciences* 520 (2020): 130-141.
- [8] Liu, Bo-Cheng, et al. "Arm-embedded implementation of a novel color image encryption and transmission system based on optical chaos." *IEEE Photonics Journal* 12.5 (2020): 1-17.
- [9] Nematzadeh, Hossein, et al. "Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices." *Optics and Lasers in Engineering* 110 (2018): 24-32.
- [10] Sivakumar, T., and Pu Li. "A secure image encryption method using scan pattern and random key stream derived from laser chaos." *Optics & Laser Technology* 111 (2019): 196-204.
- [11] Melkemi, Mahmoud, and Karim Hammoudi. "Voronoi-based image representation applied to binary visual cryptography." *Signal Processing: Image Communication* 87 (2020): 115913.
- [12] Geetha, P., V. S. Jayanthi, and A. N. Jayanthi. "Multiple share creation based visual cryptographic scheme using diffusion method with a combination of chaotic maps for multimedia applications." *Multimedia Tools and Applications* 78 (2019): 18503-18530.
- [13] Anwar, Shamama, and Solleti Meghana. "A pixel permutation based image encryption technique using chaotic map." *Multimedia tools and applications* 78 (2019): 27569-27590.
- [14] Chowdhary, Chiranjil Lal, et al. "Analytical study of hybrid techniques for image encryption and decryption." *Sensors* 20.18 (2020): 5162.
- [15] Fatahbeygi, Ali, and Fardin Akhlaghian Tab. "A highly robust and secure image watermarking based on classification and visual cryptography." *Journal of information security and applications* 45 (2019): 71-78.
- [16] Kaur, M., and V. J. E. L. Kumar. "Efficient image encryption method based on improved Lorenz chaotic system." *Electronics Letters* 54.9 (2018): 562-564.
- [17] Singh, Priyanka, Balasubramanian Raman, and Manoj Misra. "A (n, n) threshold non-expansible XOR based visual cryptography with unique meaningful shares." *Signal Processing* 142 (2018): 301-319.

- [18] Dawahdeh, Ziad E., Shahrul N. Yaakob, and Rozmie Razif bin Othman. "A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher." *Journal of King Saud University-Computer and Information Sciences* 30.3 (2018): 349-355.
- [19] Geetha, P., V. S. Jayanthi, and A. N. Jayanthi. "Optimal visual cryptographic scheme with multiple share creation for multimedia applications." *computers & security* 78 (2018): 301-320.
- [20] Shankar, K., et al. "An efficient image encryption scheme based on signcryption technique with adaptive elephant herding optimization." *Cybersecurity and Secure Information Systems: Challenges and Solutions in Smart Environments* (2019): 31-42.
- [21] Guo, Jing-Ming, Dwi Riyono, and Heri Prasetyo. "Improved beta chaotic image encryption for multiple secret sharing." *IEEE Access* 6 (2018): 46297-46321.
- [22] Ye, Guodong, et al. "Image encryption and hiding algorithm based on compressive sensing and random numbers insertion." *Signal processing* 172 (2020): 107563.
- [23] Zhang, Ying-Qian, et al. "A new color image encryption scheme based on 2DNLCML system and genetic operations." *Optics and Lasers in Engineering* 128 (2020): 106040.
- [24] Dolendro Singh, Laiphraipam, and Khumanthem Manglem Singh. "Visually meaningful multi-image encryption scheme." *Arabian Journal for Science and Engineering* 43 (2018): 7397-7407.
- [25] Mahmud, Maqsood, Malrey Lee, and Jae-Young Choi. "Evolutionary-based image encryption using RNA codons truth table." *Optics & Laser Technology* 121 (2020): 105818.