Journal of Computer Science

Original Research Paper

Primary Color Based Numerous Image Creation in Visual Cryptography with the Help of Grasshopper Algorithm, Artificial Neural Network and Elliptic Curve Cryptography

[1]Surajit Goon, [1]Debdutta Pal and [2]Souvik Dihidar

[1]*Department of Computer Science and Engineering, Brainware University, India*
[2]*Department of Computer Application, Eminent College of Management and Technology, India*

Article history
Received: 01-03-2022
Revised: 05-05-2022
Accepted: 06-05-2022

Corresponding Author:
Surajit Goon
Department of Computer
Science and Engineering,
Brainware University, India
Email: goon_surajit@yahoo.co.in

Abstract: The two primary restrictions of visual cryptography methods, contract, and security are well-known. Visual cryptography is considered secure if no share reveals information about the secure picture and this image is unreachable when shares are combined. Recursion can be used in a visual cryptography method to ensure the integrity of both arguments. Sometimes, the many shares are generated illogically in such a manner that they sometimes reveal the actual image. The model proposed in the paper has been proved beneficial in reducing the computation, noise, or distortion in the recreated image and helps in providing amended contracts. The suggested scheme uses unique pixel patterns to create a contract for the decrypted image. The contract for the recursion visual cryptography scheme is alterable from the white pixel pattern to new pixel patterns. The elliptic curve cryptography approach is used to ensure the privacy and security of the image. This study has taken a four-share mechanism in which each component is divided into four shares for each color segment. The proposed algorithm uses the Grasshopper algorithm to select the bit's positions where the encryption must be done. Neural Networks have been used as a cross validator in the proposed work model. A new fitness function is designed for the Grasshopper algorithm. The proposed algorithm is compared based on Mean Square Error and Peak Signal to Noise Ratio.

Keywords: Contract, Visual Cryptography, Decryption, Security, Recursion, Elliptic Curve

Introduction

The new-age transformation in technology has opened many doors for research. Sharing heterogeneous data over the internet has been a trend (Wang *et al.*, 2019). With this growing technology, it becomes crucial to handle loopholes like data security, privacy and safety properly. Cryptography is one such area that has caught the attention of researchers (Li *et al.*, 2018). Keeping this area in mind, Naor and Shamir (1994) proposed a new model for cryptography, namely Visual Cryptography. In this model, decryption is not computerized and can be performed by human sight. The scheme divides the unique image into K parts, where any S parts can reconstruct the unique image. The primary function of Visual Cryptography is to decode the secret colored image without any mechanical intervention (Kashyap *et al.,* 2018). The recursive secret hiding invented by Gnanaguruparan and Kak (2002) in the current scheme allows the different secret patterns to be embedded within the image without overloading the network.

Naor and Shamir (1994) introduced a visual secret sharing scheme based on the concept that a person having all n parts of share can decode the image. Even if a single sub-part of the image goes missing, the decryption process won't be carried out. In the case of two shares, it is noticed that when two black sub-pixel appear, the images are overlaid together, then p is black, but when p is white, the black sub-pixel and white pixel appear solitary. Therefore the distinction can be quickly made whether p is white or back. Visual Cryptography can be utilized for copyright safety for legal ownership. In such cases, the host share remains the same during embedding. Hyper graphic colorings can be used to execute a visual cryptography scheme (Yang *et al.*, 2016). The method accompanies the (K, K)-threshold best for pixel development.

Related Works

Pande and Shukla (2013) introduced a visual cryptography scheme by which we can generate n number of shares of reduced sizes and keep the contrast level. This model also supports various image types and is applied to binary, grey, and color images.

Das *et al*. (2019), proposed that the unnecessary shares in VCS can grab the hacker's attention while performing transactions, thus posing a threat by revealing the secret image. To avoid undue attention, Shamir's (k, m) scheme can be used for encoding meaningless images. The proposed scheme uses the 3D vector quantization method to minimize the volume of encoded data.

Shankar and Elhoseny (2019a) suggested different strategies for securing digital images on communication channels through Homomorphic Encryption with the ideal key section. To enhance the security aspect, ant lion optimization is considered. The experimental outcomes were then analyzed and compared with other strategies. They employ a visual secret share creation technique to create three shares, as well as a hash function to improve security. They also use the Grey Wolf Optimization (OGWO) method to choose the best keys. As a result, compared to previous ways, it generates a more secure system with less computing time. However, because of significant computational resource overheads, WSN as encryption instruments may be impracticable.

Shankar and Elhoseny (2019b) proposed Discrete Wavelet Transform implemented on images to produce sub-images. In this, multiple shadows are constructed and then encrypted and decrypted using Homomorphic Encryption and for the generation of optimal key, Oppositional based Harmony Search algorithm is used. Comparative studies showed the system performed better in comparison to other systems. Furthermore, the secret key values may differ from one image to the next, giving attackers even more ambiguity regarding the key. Its system's security can be improved by incorporating some unique swarm optimization techniques into its framework.

Jia *et al*. (2019), proposed chaotic cat mapping for two scheme encryption. Later these algorithms are analyzed. The results show that the system resists cipher attacks and is effective in encryption. However, the data also demonstrates that the bigger the number of pixels, the longer the two techniques take. As a result, various 3D point cloud comparison techniques may be necessary for the future before encryption.

Elhoseny *et al*. (2020), studied the security of medical images on the Internet of Things. They use an optimized technique with the cryptographic model. To date, all the hospital data was secured on the cloud, which is venerable, so another framework is required for the security aspect. The optimal key was opted by using grasshopper optimization and particle swarm optimization in elliptic curve cryptography. The proposed model was further compared to check the reliability. This study proposes a hybrid IoT security encryption method, in the recommended computation, even using the optimal key, which has unique encryption and speed decoding features. However, this procedure is not safe enough since it has never been highly impalpable, which requires further investigation to increase the level of safety.

Mhala and Pais (2019), proposed a Visual Secret Sharing (VSS) scheme to recover the image by considering many shares in which meaningful information has been embedded and noise-like shares have been reduced. In addition, a random VSS scheme recovers the image by hiding the random data into shares so that redundancy in the image is avoided to a great extent. The different embedded techniques used to retrieve the image enhance the contrast. The proposed results ensure that 70 to 80% shares have been obtained with 99% shares for the noise. To boost the contrast of the reconstructed image, this strategy employs the reversible data hiding technique. The suggested approach has the advantage of recovering images without any blocking artifacts. To employ additional embedding sites inside the shares, the author may introduce some data embedding approaches.

Gibert *et al.* (2019) presented a deep learning approach to categorize the malware efficiently into families using discriminated patterns to visualize the image. The developed method uses two benchmarks: The Malimg dataset and the Malware classification dataset. The experimental results are compared with state-of-the-art techniques to validate the proposed model. Even though comparable patterns can be detected in the visualization of malware programs from the same family, this approach has issues with compressed or encrypted samples, which may have an entirely different general structure.

Jisha and Monoth (2019), retained the image forgeries using visual cryptography schemes, which improved integrity, authenticity, confidentiality, and robustness. The proposed model presents an overview of the active digital images in which authenticating the image and detecting tampering are the primary considerations. In addition, the proposed model is compared with the existing models to determine the drawbacks. For the production of the original image, this research employs XOR-based processes, which yields a better outcome in terms of loss of contrast. However, there is no solution for a color image in this study.

Dalvi and Wakde (2018), use visual cryptography techniques to fragment the image into different shares to decrypt the image. The decryption process is performed using the bitwise operation on every pixel using the key. A novel sterilization algorithm has been used for multiple sharing and generating a key. The proposed system combines the shares to simulate the results finally. This technique is exceptionally safe because shares are encrypted many times using keys that can never be decrypted without knowing them. However, this strategy failed to convey the meaningful shares, which are commonly utilized in this sort of communication.

To secure the anonymity and availability of crucial commercial or military images, Ahmadian and Amirmazlaghani (2019), employed hidden image sharing techniques. These schemes have some basic security features that can emerge from key elements. In this article, researchers eliminate these vulnerabilities and use the Optimally Asymmetric Encryption Padding (OAEP) technique and Information Dispersal Algorithms (IDA). The proposed scheme provides better performance in computing security, small shadow size and generation, and hidden redundancy. The results have been analyzed using the proposed security scheme and prove that the secret image is confined to the limited number of enemies that have been calculated.

Shankar *et al*. (2020) secured Digital Images (DI) with an encryption algorithm. To ensure security, the images were selected using the Chinese Remainder Theorem (CRT) model, the image was encoded in many shares and Stream Encryption (SE) algorithms encrypted the stream. A meta-logic algorithm has been introduced to encrypt the selection using the best public and private keys and decrypt the image into a secure transmission. With an improved Cuckoo Search algorithm, the optimal key has been selected as a fitness feature that consumes less time. The simulation results of the proposed algorithm improved with DI security in comparison to the defined algorithms in all the images. Though a full description of various encryption techniques will be necessary, a hybrid optimization approach using numerous metrics will be studied.

Using information theory and other stochastic optimization approaches, Chhikara and Kumar (2021), suggested a modified grasshopper optimization method to shrink the feature set in the steganalysis process.

In their suggested work, Chaturvedi and Shukla (2020), employed a modified grasshopper method to optimize one position bits at the encryption end to secure data communication through optimal discrete wavelet transform and sanitization technique.

Significant Contribution of Proposed Work

In today's world, sensitive data transmission plays a crucial part in multimedia transmission. Security measures are an essential component of such systems. For this type of transmission, visual cryptography is a great solution and elliptic curve cryptography adds even more security to the mix. The existing methodology (Shankar and Eswaran, 2017), explains the main element, but we could use specific optimization techniques to get a more accurate result. When two shares are overlaid in visual cryptography methods, two black sub-pixels occur if the resultant pixel p is black. If the final pixel p is white, however, a single black and a single white sub-pixel appear. As a result, we can tell if p is black or white. The proposed method is used to construct the shares, which are dependent on their image pixels. The color image's pixel values are retrieved and represented as a matrix from the original image. This study not only uses the recursive visual cryptographic scheme for sharing a secret image but also applies elliptic curve cryptography for generating more secure shares and also uses a grasshopper optimization algorithm to reduce the computational overheads. This model also uses an artificial neural network to analyze the bit pattern provided by the grasshopper algorithm. Two significant contributions to our proposed work are listed below:

1. To optimize the pixels for encryption, comparably new technology is used, which is a swarm intelligence GOA over current methods
2. It also employs an artificial neural network to cross-verify the pixels patterns generated by the GOA and determine whether they are suitable for encryption

Mathematical Background

Elliptical Curve Cryptography (ECC)

Elliptic curve cryptography is used in public-key cryptography because it allows lower-key sizes to be employed, which reduces storage and transmission needs. A 256-bit ECC public key system can replace a 3072-bit RSA public key system. The prime number is chosen as n_p and the private key is chosen as H in Elliptic curve cryptography (Kapoor *et al.,* 2008). Then the equation is represented by:

$$E = (p(i))^3 + u * p(i) + v \tag{1}$$

where the constants *u* and *v* are equal to two. If X = mod (E, n_p) and Y = mod ($(p(\mathrm{j}))^2$, n_p) then the criterion X = Y is fulfilled and the best point is chosen. The points of the Elliptic curve are denoted by $p(i,j)$. The best point $P_e(k, l)$ and P_f is the public key then $P_f = H*P$.

Recursive Visual Cryptography Schemes

In any system, security has always been a primary concern. As discussed earlier in the paper, security has been one of the primary features of VCS. The model is considered secure if no image is decoded and no information is leaked from any number of shares. To make VCS a secure system recursive visual cryptography scheme has been proposed for a secure system. In the recursive method, the security image has two segments i.e., share and sub share. With the implementation of this scheme, the system's security can be enhanced. In recursive visual cryptography, the components of the shares have been assigned to mediocre zones. To appropriately combine the arbitrary bits in the shares, the entire use of d-sequences or corresponding randomized sequences is used.

Grasshopper Algorithm

The proposed algorithmic architecture uses the Grasshopper Algorithm (GOA) to find the relevant bits where the encryption can be performed.

Population-based meta-heuristic algorithms are what swarm intelligence approaches are classed as and they generate a large number of solutions in each run. This GOA algorithm was described by Saremi *et al.* (2017). The foraging and swarming activities of grasshoppers are mimicked by this approach. The life cycle of a grasshopper (Meraihi *et al.*, 2021) is separated into two phases: Nymph and adults, with the nymph phase defined by modest steps and languid movements and the adulthood phase marked by long-range and rapid movements. The grasshopper swarming behaviors algorithm is built using these two phases. It employs basic mathematical formulas:

$$P_i = S_i + G_i + A_i \qquad (2)$$

where, P_i defines the position of the i^{th} grasshopper, S_i denotes grasshopper social interaction, G_i denotes the gravitational force on the i^{th} grasshopper and A_i denotes wind advection. The GOA is a social interaction-based Swarm Intelligence method (Steczek *et al*., 2020) in which grass insects, also known as grasshoppers, eat all the green crops based on the interaction index. The interaction index is calculated using the selection and interaction's upper and lower bound. If the interaction value goes below the lower or higher bound, the grasshopper leaves the leaf.

The Neural Networks

An artificial neural network is made up of artificial neurons and is organized similarly to a biological network. It sends signals to other neurons in the same way that a biological brain does. In a machine learning process, supervised learning uses a function that maps an output based on sample input-output pairings. The optimization algorithm is the procedure utilized to carry out the learning process in a neural network (or optimizer). There are numerous optimization algorithms to choose from. In terms of memory needs, computing speed and numerical precision, they all have various characteristics and performance. Because it provides a numerical solution to the problem of minimizing a function across a space of parameters, the Levenberg-Marquardt technique was chosen. The learning problem is expressed as the reduction of a loss index. It's a function that determines how well a neural network performs on a given data set. In general, the loss index is made up of error and regularization terms. The error term assesses how well a neural network fits a given set of data. By regulating the model's complexity, the regularization term prevents overfitting. The Levenberg-Marquardt algorithm was created to cope with loss functions that are expressed as a sum of squared errors. It works even if the exact Hessian matrix isn't computed. Instead, it uses the Jacobian matrix and the gradient vector. Consider a loss function that is expressed as a sum of squared errors:

$$f = \sum_{i=1}^{m} e_i^2 \qquad (3)$$

The number of training samples is denoted by them. The derivatives of the errors affecting the parameters are contained in the Jacobian matrix of the loss function:

$$J_{ij} = \frac{\partial e_i}{\partial w_j} \qquad (4)$$

For i = 1,…,m and j=1,…,n. Where n is the number of parameters in the neural network and m is the number of samples in the data set. It's worth noting that the Jacobian matrix has a size of m x n. The gradient vector of the loss function a can be calculated as:

$$\nabla f = 2J^T.e \qquad (5)$$

The vector of all error terms is denoted by e. Finally, we may use the following expression to approximate the Hessian matrix:

$$Hf \approx 2J^T.J + \lambda I \qquad (6)$$

where, λ is the identity matrix and is a damping factor that ensures the Hessian is positive. The Levenberg-Marquardt parameter improvement procedure is defined by the following expression:

$$W^{(i+1)} = W^{(i)} - (J^{(i)}T.J^{(i)} + \lambda^i I)^{-1}(2J^{(i)T}.e^{(i)}) \qquad (7)$$

For i = 0, 1,……

Proposed Method

The proposed method is used for maintaining security. It helps send the image to the receiver without affecting its confidentiality and maintains its security. The image is divided into shares and then transmitted. All the shares need to be stacked together to get back the original image. In this method, their pixel values are used to construct the shares. Let's suppose the pixel value to be P_v for the primary (RGB) color images. P_v is taken from the original image and then represented as a matrix ($P*Q$). These pixel values are further used to create sub shares and later these shares are clubbed in blocks. After compiling the shares in blocks, these blocks are encrypted using Elliptical Curve Cryptography (ECC) Method, Grasshopper Algorithm, Artificial Neural Network, and decryption is done through the ECC method. After encryption and decryption, the final product is compared to the original. The results can be compared by peak signal-noise ratio value, correlation coefficient, and mean square error. The notations that have been discussed in our proposed model are given in Table 1.

Table 1: Notation table

Notation	Description
R_m, G_m, and B_m	Matrices represent Red, Green and Blue pixel values respectively.
n	Total number of pixels in the secret image.
$R_{S1...4}$, $G_{S1...4}$ and $B_{S1...4}$	Four shares each from Red, Green, and Blue pixels' values respectively.
R_{ab}, G_{ab}, and B_{ab}	They are components of the respective image pixels where a and b indicate the position in that particular matrix.
Imag	Represent the qualifying set.
Bidn	Represent the forbidden set.
J	Reconstructed image.
S	Number of participants in the reconstructed image.

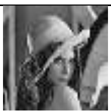
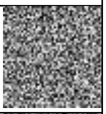
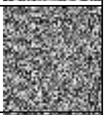
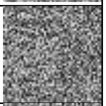
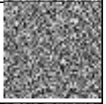
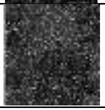
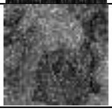
Table 2: Ordinal measures of GOA

Iteration T	Total number of search simulations for optimal bit selection
Population P	The total number of pixels to be optimized
Lower Bound LB	Lower limit of the pixel (0)
Upper Bound UB	Upper limit of pixel (256)
Fitness function	The selection criteria of the pixel

Table 3: Fitness function of GOA

1	If CBV < ABV
0	Otherwise

Table 4: The encryption scheme's results

Original image	Stacked images		Share images				Encrypted images
			Share 1	Share 2	Share 3	Share 4	
	Red						
	Green						
	Blue						
	Red						
	Green						
	Blue						
	Red						

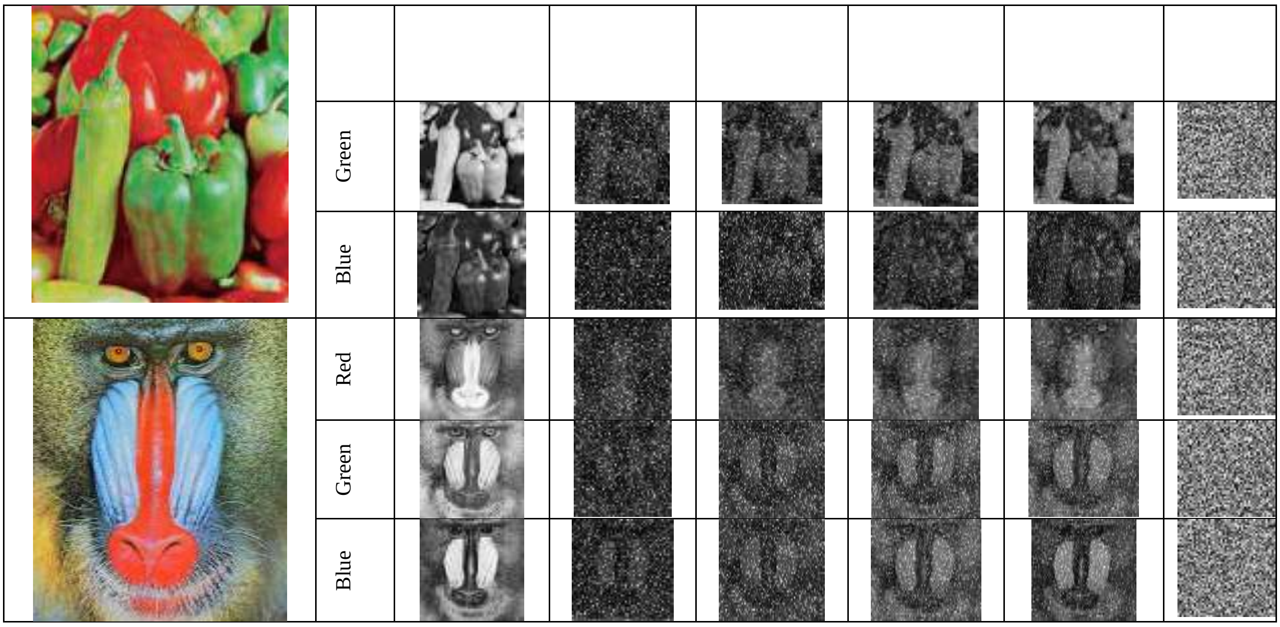


Table 5: Parameters of proposed methods without attacks

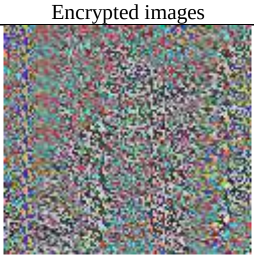
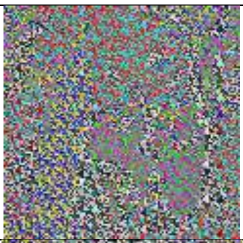
Original image	Encrypted images	Final images	PSNR	MSE	CC
			65.37	0.0932	1
			66.82	0.0738	1
			64.96	0.0983	1
			67.83	0.0648	1

Table 6: Parameters of proposed methods with attacks

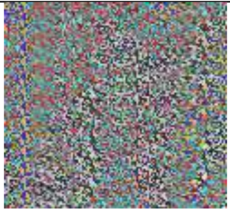
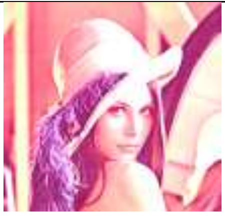
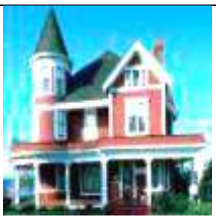
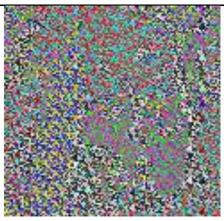
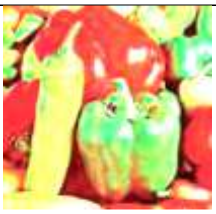
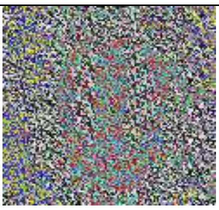
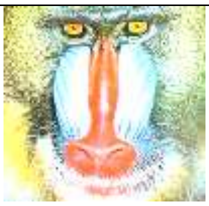
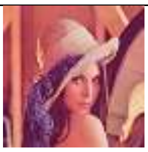
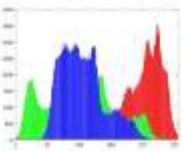
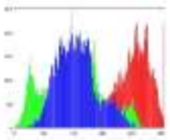
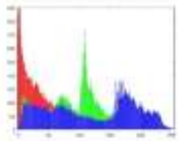
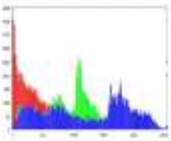
Original image	Encrypted images	Final images	PSNR	MSE	CC
			43.82	6.593	0.9928
			44.83	5.577	0.9953
			43.29	7.682	0.9964
			45.88	4.474	0.9983

Table 7: Comparison of proposed work with existing work

S No.	Images	Proposed work ---------------------------------			Existing work (Shankar and Eswaran, 2017) --		
		PSNR	MSE	CC	PSNR	MSE	CC
1	Lena	65.37	0.0932	1	58.0025	0.1030	1
2	House	66.82	0.0738	1	57.4297	0.1176	1
3	Pepper	64.96	0.0983	1	56.684	0.1454	1
4	Baboon	67.83	0.0648	1	58.1437	0.0997	1

Table 8: Histogram comparisons of original, encrypted, and decrypted images

Original image	Original image histogram	Encrypted image	Decrypted image	Decrypted image histogram
				
				

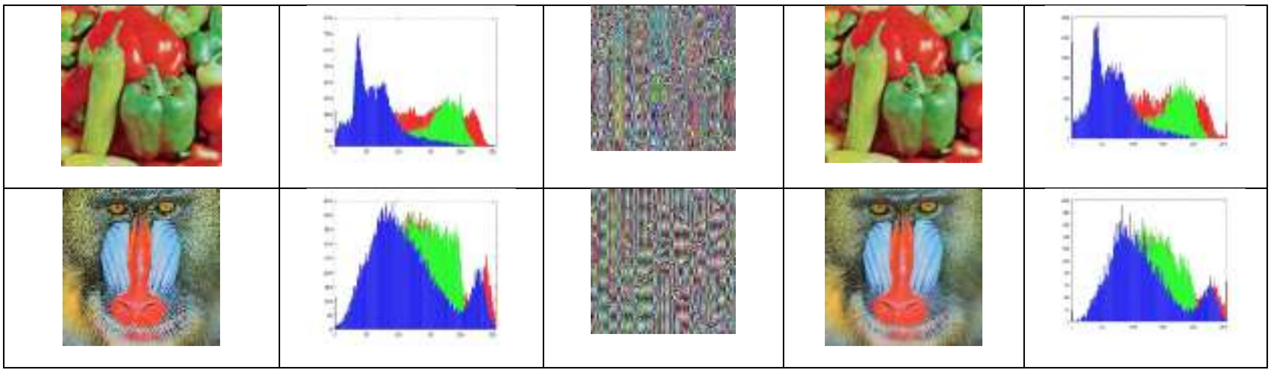


Table 9: Histogram variance results of the proposed scheme.

Images	Color channels	Original	Encrypted
	Red	860223.71	1182.48
Lena	Green	395349.66	1116.30
	Blue	1200884.16	1096.45
House	Red	23719.00	652.47
	Green	11696.81	616.46
	Blue	4911.72	665.86
Pepper	Red	6933.80	1451.08
	Green	9085.84	1431.82
	Blue	26690.23	1465.09
Baboon	Red	14638.67	1165.27
	Green	25265.27	1162.85
	Blue	14877.12	2285.21

Block Diagram

The secret image is divided into sub-image using three primary colors, RGB (Red, Green, and Blue). Figure 1 reflects the bifurcation of the secret image into primary colors (RGB) as per pixel value. These values are represented in matrix R_m, G_m, and B_m, and the matrix size is kept as the size of the original image, i.e., ($P*Q$). The pixel value is computed using the given equation coefficient and mean square error. A description block diagram is mentioned below.

Pixel = value of (R_m +G_m + B_m) ($P*Q$) denotes the size of the original image.

The Equation to Calculate Pixel:

$$Pixel = \sum_{i=1}^{n} (R + G + B) \tag{8}$$

where, n is a total number of pixels in the image.

Now, these sub-images are further divided into more subcategories.

Figure 2 reflects the subdivision of the shares, which are further accumulated in blocks. All the sub shares of primary colors are collected together in the blocks to get a compiled image.

The final blocks that accumulate sub-images are clubbed together to get the output image.

Figure 3 shows after the compiled bock, the image is encrypted using Elliptical Curve Cryptography (ECC) Method, Grasshopper Algorithm, Artificial Neural Network, and decryption is done through ECC method.

The actual image is compared to the final output image so that the results can be compared by peak signal to noise ratio value, correlation coefficient, and mean square error.

Creation Techniques for Share

The pixels from the original image appear in several modified forms known as shares. A share is a combination of RGB image pixels. The primary color shares are determined by the image's pixel value. Now, these shares are separately indicated as:

$$R = kl \int limk - 1tonR_{ab} \tag{9}$$

$$G = kl \int limk - 1tonG_{ab} \tag{10}$$

$$B = kl \int link - 1tonB_{ab} \tag{11}$$

Equations for Model

Suppose a number of participants be v and 2^l be subsets of v:

$$Equation1\text{: let v = } \{v_1, v_2, v_3 \ldots\ldots, v_n\} \tag{12}$$

Phase 1: Encryption process
Imag represents the qualifying sets and Bidn represents the forbidden sets:

$$Equation2: Imag \subseteq 2^1, Bidn \subseteq 2^1 and Imag \cap Bidn = \varnothing \tag{13}$$

Phase 2: Encryption process
Value of i = 1 to n
The value of n can be different at any phase.

Equation 3**:** let $ri = \{ri_1, ri_2, ri_3 \ldots\ldots\ldots\ldots\ldots\ldots ri_n\}$ then Imag⊆2ri, Bidn⊆2ri and Imag ∩Bidn = Ø.

The procedure can be repeated for any number of contracts and security.

Phase 3: Decryption process
In this phase the secret image J can be recreated:

a) $$J = \sum_{h=1}^{S} ri \tag{14}$$

S is the number of participants used to reconstruct the image. The value will vary for different VCSs, in this case, a new equation is given for the reconstruction of each participant:

b) $$ri = \sum_{h=1}^{S} ri.h \, where 1 \le i \le v \tag{15}$$

RVCS Construction

The scheme has been explained with two levels of encryption. This means that the image encryption is done in two stages. At first 2 out of 2 VCS and following, each code is subdivided into 2 out of 2 VCS. The replicating tree diagram further explains the encryption process better. Figure 4 and 5 represents the VCS with recursion in a tree representation. J is encrypted into two shares J_1 and J_2 which are further encrypted into two more shares of each subgroup. In decryption J is represented as:

$$J = J_1 + J_2$$

$$J = J_1 + J_{22} + J_{33}$$

$$J = J_2 + J_{16} + J_{17}$$

$$J = J_{16} + J_{17} + J_{22} + J_{23}$$

(Different Manner Decryption using VCS with Recursion)

Most of the research articles focus on the encryption part, but apart from how to encrypt the data, it is equally important to know what to encrypt and what to not. This will reduce the computation time and the sophistication in the architecture of processing.

Algorithm 1 is designed to implement GOA for position selection following the same concept.

Algorithm 1: The GOA

```
Input: Oimg → Original Image, Key → Encryption Key,
                N → Number of Share
Output: Eimg with S1, S2, S3 and S4 →
          Encrypted Image with Share 1,2,3 and 4
Red Component = Oimg. Red//Red Component of the
                    Image
Green Component = Oimg. Green//Green Component of
                    the Image
Blue Component = Oimg. Blue//Blue Component of the
                    Image
[Row,Col] = size (Oimg)//Calculating total number of
               rows and columns
Create Share Image = []; //Creating an empty share array
For i = 1 → Row
          For j = 1 → Col
               PIX1 = Create Share (Red Component)
                    //Creating empty red components
               PIX2 = Create Share (Green Component)
                    //Creating empty green components
               PIX3 = Create Share (Blue Component)
                  //Creating empty blue components       End
End
```

The GOA algorithm takes the following ordinal measure to compute the bit pattern.

GOA algorithm processes the pixel pattern row by row and each row is considered one unit of Grasshoppers. The pixel selection of each unit depends upon the pixel value and the pixel density in each part. A fitness function is designed that separately intakes the Red, Green, and Blue pixel values. The pixel value of a lower bit of the grasshopper unit is selected as the bit to be encrypted. Cross-validation is required for all selected bit pattern values to ensure the correct bit pattern to encrypt the data. The Fitness Function of GOA uses two elements, Current Bit Value (CBV) and Average Bit Value (ABV). The fitness function of GOA is as follows.

GOA provides the bit pattern where the encryption can be done but requires cross-validation, ensuring that the selected bits are appropriate to encrypt. Gibert *et al.* (2019) used Convolution Neural Network as a classifier for the malware-represented image. He uses training with associated labels to identify the malware images. The conditions are a little different in the proposed work, but the proposed work applies a supervised neural network considering each identified bit pattern as one group. A supervised learning algorithm examines training data and generates an inferred function that may be used to map fresh samples. The Levenberg-Marquardt approach was chosen because it provides a numerical solution to the problem of minimizing a function across a space of parameters. For example, if the pattern value as per their identified position is [22, 45,66,78,98,392; 24 44 22 11 44] then the associated group would be [1:2]. As the learning method is supervised, the test data will be similar to the training data. If the classified labels' results are similar to that of the training labels or group, the selected pattern is suitable for the encryption.

Algorithm 2 represents the work architecture of the applied neural network.

Algorithm 2: The neural networks

```
Input: Bit Pattern Output: Classified Positions
Initialize Neural Networks with Training Data as Bit Pattern
Associated_Labels = BitRow_Number
Start Training.
Store Training Results
Test-Data = Training_Data
Classify Test_Data with Training Results
Store Classified Labels to Database
Subtract Classified Labels from Training Labels
Find Zeros and Identify Positions
Return Positions
```

Simulation Results and Analysis

The simulation of our proposed system was performed on MATLAB 2018b. We used an i3 intel processor and 8 GB of RAM system. We took four secret original images, Lena, Baboon, Pepper, and House, each size 128 X 128 for our simulation.

Imperceptibility and Robustness Analysis

Using the PSNR value, we compare the original image to the decrypted output image. PSNR (Peak Signal Noise Ratio) is one of the most often used measures for Image Quality Assessment (IQA). PSNR is a mathematical metric that compares the intensity of distortion between the original and deformed images. The higher the PSNR, the more comparable they are and the better the reproduction quality. The following metric Correlation Coefficient (CC) is used to evaluate the algorithm's robustness.

The PSNR is represented by:

$$PSNR = 10 * log ?\left(\frac{255^2}{MSE}\right) \tag{16}$$

where the average square of error in certain images is called MSE (Mean Square Error) and is represented by:

$$MSE = 1/(M * N)\sum\sum\ [I(i, j) - I'(i, j)]^2 \tag{17}$$

Here M is the width of the original image, N is the length of the original image, $I(i, j)$ represent the original image pixel and $I'(i, j)$ represent the decrypted image pixel values.

Correlation is a measure of a relationship between two or more variables. When the image and its encryption are the two variables, they are usually highly correlated and when they are almost identical, the correlation coefficient equals one. This technique has been carried out to examine the correlation between two neighboring pixels in both plain and ciphered images.

The results are as follows listed in Table 4. The encrypted images were obtained from the proposed algorithm**.** Table 4 depicts the results of the proposed algorithm in which the original image of size 128 × 128 has been considered which is segmented into three different components such as red, green, and blue. The obtained images were further encrypted for security reasons. After that, we used recursive visual cryptography and ECC to construct four numbers of transparent shares for each component, ensuring that no single share can compromise the original secret. The ECC approach was combined with GOA to improve the performance of image pixels. As a result, the black and white pixels of each encrypted image is distributed evenly.

Table 5 lists the original image, encrypted image, and final image with its PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error), and CC (Correlation Coefficient) without attacks. In the Lena image, it is seen that the obtained PSNR value is 65.37, which shows that the image has been enhanced without attacks. The MSE is also very low, which means that the error between the original and without attack encrypted image is low. The unity vale of the CC shows that both images are almost unique. The house, pepper, and encrypted baboon image also show similar results as the low MSE value explicit that there is the minimum error between the original and encrypted image. As a result, the recovery of the encrypted image is very good in the absence of an attack. The PSNR, MSE, and CC parameters all yielded outstanding results. For all the sample images, PSNR values ranged from 64.96 to 67.87, MSE values ranged between 0.0648 to 0.0983, and CC values were all 1.

Table 6 lists the results of the proposed mechanism with attacks. Each output image is attacked by noises like Salt-and-Pepper, Blurring, and Filtering. Salt-and-pepper noise is a sort of noise that occasionally appears on images. Impulsive noise is a term used to describe this type of noise. The correlation coefficient value changes for all the images. The low PSNR value for the different images depicts that there must be a change between the original and attached image. For Lena's image, the PSNR value reduces to 43.82 from 65.37 and the error also increases from 0.0932 to 6.593. In addition, the CC value changes from 1 to 0.9928, which depicts a slight change between the encrypted without attack image and the final attacked image. For the house image, the PSNR value reduces to 44.83 from 66.82 and the error also increases from 0.0738 to 5.577. In addition, the CC value changes from 1 to 0.9953. The CC value clearly shows a slight change in the encrypted and final image. For the pepper image, the PSNR value diminishes to 43.29 from 64.96. The error also increases from 0.0983 to 7.682. In addition, the CC value changes from 1 to 0.9964. The low CC value shows that there is not much difference as the attackers attack the image. In the case of the Baboon image, the PSNR value changes from 67.83 to 45.88, which shows that signal quality loses. The low MSE value 0.0648 to 4.474 shows some error introduced in the final image. The low CC value finally clears only a slight change between the original and final image.

It is seen in the given figure that the PSNR value with and without attacks changes as the signal quality of the image loses. The without attacks bar graph for the different images shows a high peak value. However, it is low when intruders attack the image from outside.

Figure 6 depicts the MSE of different images. The error rate without attacks almost converges to low. When the intruders attacked the images, the error rate increased for all the other images. The MSE rate for Lena and Pepper images has been more than for house and baboon images. The more the error rate shows the change between the original and final image.

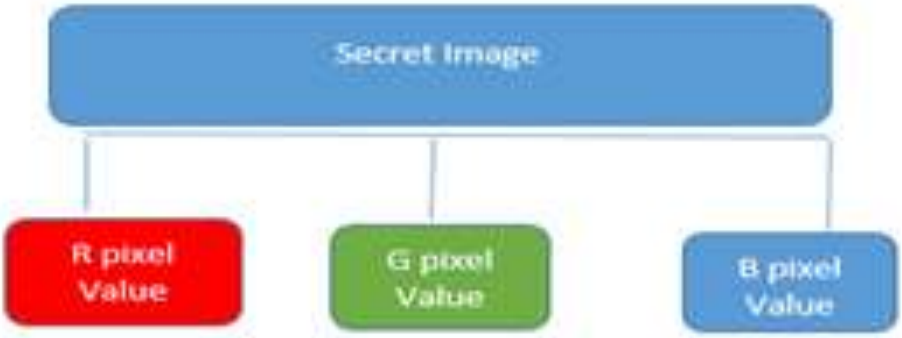


Fig. 1: Secret image

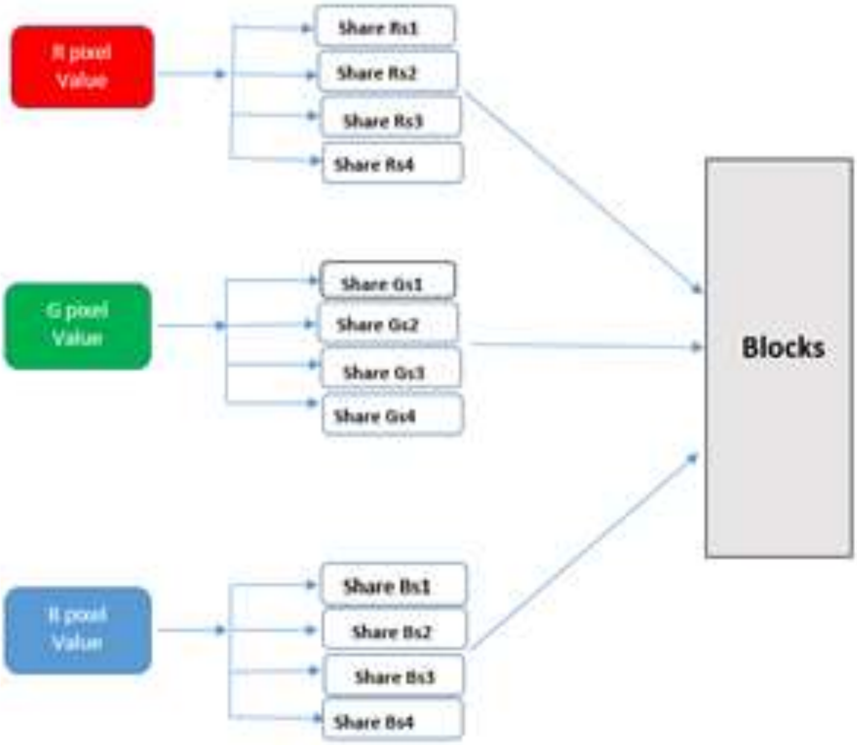


Fig. 2: Subdivisions of the image

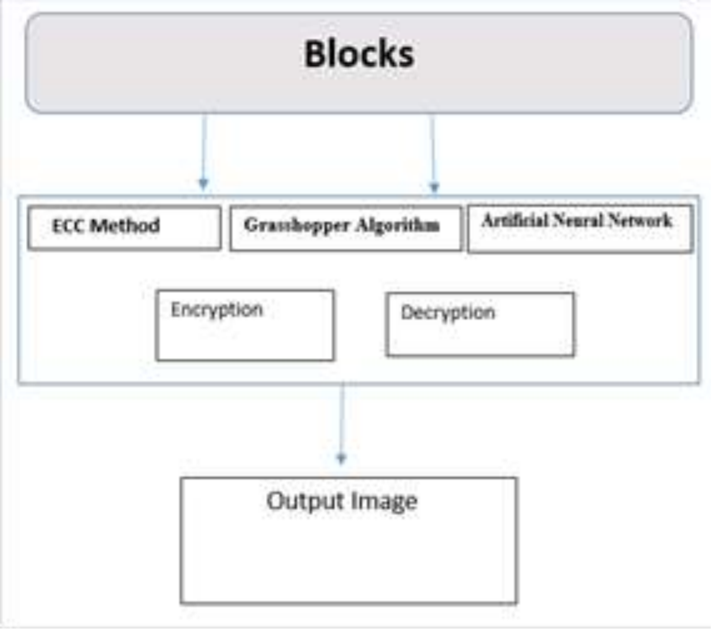


Fig. 3: Compiled diagram for final output

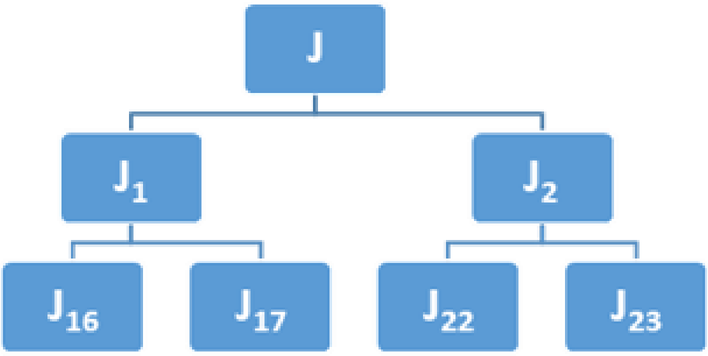


Fig. 4: 2-out-of-2 RVCS with encryption

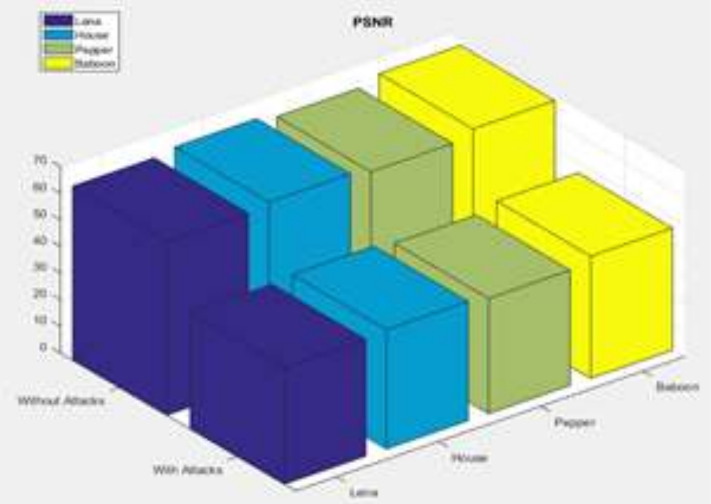


Fig. 5: PSNR value of different images with and without attack

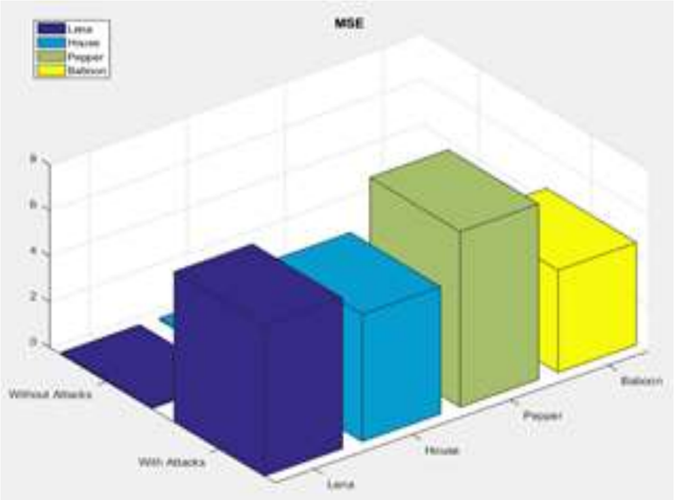


Fig. 6: MSE of different images with and without attack

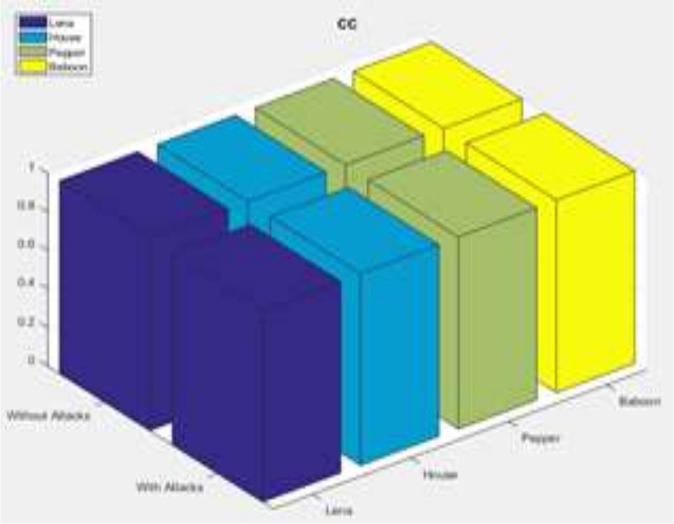


Fig. 7: Correlation coefficient of different images with and without attack

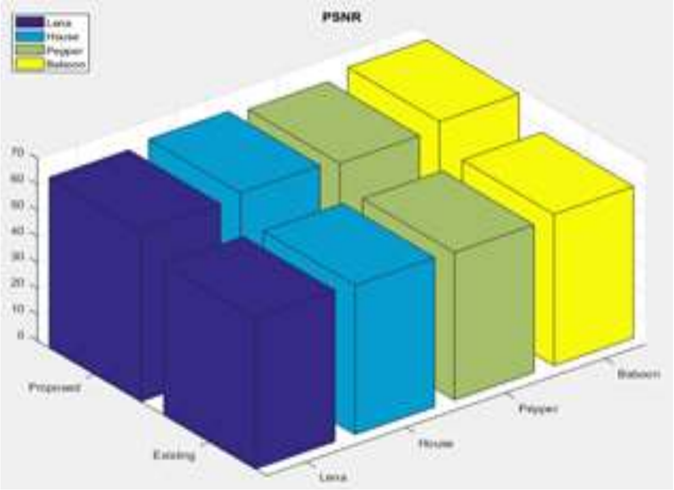


Fig. 8: PSNR value of proposed and existing one (Shankar and Eswaran, 2017)

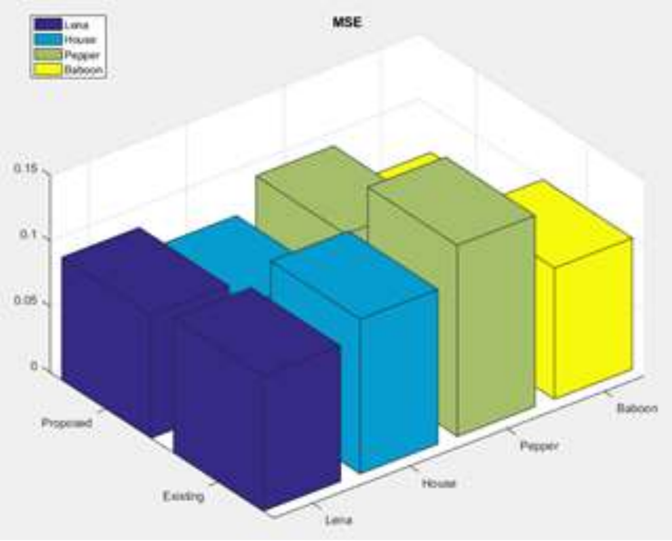


Fig. 9: MSE value of proposed and existing one (Shankar and Eswaran, 2017)

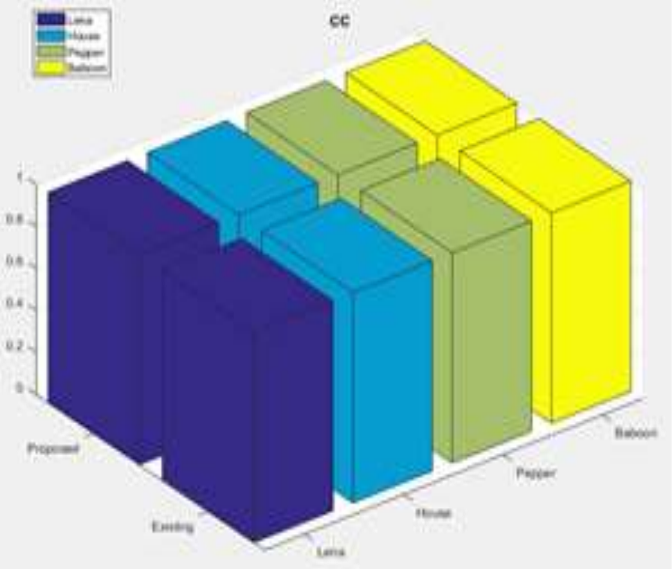


Fig. 10: CC value of proposed and existing one (Shankar and Eswaran, 2017)

The given Fig. 7 clearly shows that the value of CC for the different images changes vary slightly from the unity. This indicates the relationship between the original and final image. The different correlation values between attacked and without attack images show that the processed images have different pixel values from the original image.

The proposed work has been compared with the past results in Table 7, as explained by Shankar and Eswaran (2017). The tabular data shows the result of the proposed and past results. The PSNR value of the proposed approach is clearly shown in the table which is improved by 14% for baboon and house images. However, it is revamped by 11% for Lena and 12% for pepper image. In the case of MSE, the error is reduced by the proposed method is contrary to the past studies.

The low PSNR value of the previous state of art techniques and the high PSNR value of the proposed one show (Fig. 8 and 9) that results have been improved. The Lena image is improved by 14%. Similarly, the other images improved by 11, 12, and 14% for the house, pepper, and baboon image respectively.

In the case of MSE, the proposed method minimizes the error for the different images compared to existing work. The MSE value depicts how to exchange pixels within the image and its extraction for the prescribed image. The proposed method shows that the error value is very low and image quality is finally improved. Overall, the MSE was enhanced by

9% for the Lena image, 37% for the house image, 32% for the pepper image and 35% for the baboon image.

The given Fig. 10 indicates the CC value of the proposed and existing method. In both cases, it is 1, which indicates that the image pixel value correlates with the original image in all points of view. The unity value shows that the proposed mechanism has retrieved all the image's pixel values.

Statistical Analysis

The original image histogram must differ from the encrypted image histogram as the initial criterion for histogram analysis. The encrypted image histogram should also maintain a uniform. Individually, the red, green, and blue components of our sample images meet the aforementioned two criteria. The original and decrypted image histograms also have a visual representation. Table 8 compares each image's composite histograms (red, green, and blue channels). We can observe from the histogram graphs of both the original and decrypted images that they are nearly identical for all of the sample images. The histogram graphs for the Red, Green and Blue channels for both the original and decrypted images are provided in Table 8.

In histogram analysis, variance is a quantitative metric. The formula for calculating variance is:

$$Variance(X)=\frac{1}{n^2}\sum\nolimits_{i=1}^{n}\sum\nolimits_{j=1}^{n}\frac{(x_i-x_j)^2}{2} \qquad (18)$$

where, n denotes the number of greyscale values and x_i and x_j denote the number of pixels for color scale values i and j.

Table 9 illustrates the variance findings of our sample test images, demonstrating that the variance of the original image differs significantly from the variance values of encrypted images for each color channel. We can also see that the variance values of encrypted images are rather low, indicating that they preserve their uniformity. The encrypted images' histogram variance values also indicate that no original image features can be tracked through the encrypted images. Without a proper decryption technique, it is impossible to fetch any information from the encrypted one.

Conclusion and Future Works

This study secures the image by implementing a four share mechanism to encrypt the image using elliptical cryptography. The proposed method is used to build shares that are based on their image pixels. The pixel values of the color image are extracted from the original image and represented as a matrix. The proposed method uses the Grasshopper algorithm to process the image in terms of encryption and decryption in line with the cryptography technique. To alleviate the computational overheads, the Grasshopper optimization algorithm is applied. The encryption has been done using Elliptical Curve Cryptography (ECC) Method, Grasshopper Algorithm, Artificial Neural Network, and decryption is done through the ECC method. The recursive visual cryptographic approach is also used in this study to share a secret. The proposed method has been further cross-validated using the neural network. The bit pattern given by the grasshopper method is analyzed using an artificial neural network. The proposed work has been compared with the past studies to determine its efficiency. So, different parameters such as PSNR, MSE, and CC have been considered and compared with the existing methods Eswaran (2017). The experimental results show that the PSNR value of the proposed method improved by 14% and MSE was revamped by 37%, contrary to the previous techniques. The proposed method's robustness is also further enhanced by incorporating features of optimizing methodologies such as neural networks and grasshopper algorithms. The proposed technique's imperceptibility and resilience are aided by the usage of neural networks and bio-inspired algorithms in conjunction with it. Other bio-inspired algorithms can be used in the future to improve peak signal-to-noise ratio performance. The image quality can be increased as well as the mean square error value reduced by using ensemble approaches. Furthermore, CNNs (Convolutional Neural Networks) may use in the future, which are the most common method for analyzing the bit pattern offered by other bio-inspired algorithms.

Acknowledgment

We'd like to show our gratitude to everyone who assisted us during this research.

Author’s Contributions

Surajit Goon: Carried out the research, conducted the experiments and prepared the article under the guidance of the experts.

Debdutta Pal: Supervised the study and made suggestions for improvements.

Souvik Dihidar: Helped with the analysis and generated the tables and graphs.

Ethics

This is an original scientific article, and no part of it has been previously published. All the authors have examined and approved the work, and there are no ethical concerns.

References

Ahmadian, A. M., & Amirmazlaghani, M. (2019). A novel secret image sharing with steganography scheme utilizing Optimal Asymmetric Encryption Padding and Information Dispersal Algorithms. Signal Processing: Image Communication, 74, 78-88. doi.org/10.1016/j.image.2019.01.006

Chaturvedi, A. K., & Shukla, P. K. (2020). An effective watermarking technique using optimal discrete wavelet transform and sanitization technique. Multimedia Tools and Applications, 79(19), 13161-13177. doi.org/10.1007/s11042-020-08639-6

Chhikara, S., & Kumar, R. (2021). Image steganalysis with entropy hybridized with chaotic grasshopper optimizer. Multimedia Tools and Applications, 80(21), 31865-31885. doi.org/10.1007/s11042-021- 11118-1

Dalvi, G. D., & Wakde, D. G. (2018). An Improved Multi-secret Sharing Visual Cryptography Technique for Color Images Using Sterilization Algorithm. In Advanced Computational and Communication Paradigms (pp. 443-452). Springer, Singapore. doi.org/10.1007/978-981-10-8237-5_43

Das, S. S., Sharma, K. D., Chandra, J. K., & Bera, J. N. (2019). Secure image transmission based on visual cryptography scheme and artificial neural network-particle swarm optimization-guided adaptive vector quantization. Journal of Electronic Imaging, 28(3), 033031. doi.org/10.1117/1.jei.28.3.033031

Elhoseny, M., Shankar, K., Lakshmanaprabu, S. K., Maseleno, A., & Arunkumar, N. (2020). Hybrid optimization with cryptography encryption for medical image security in Internet of Things. Neural computing and applications, 32(15), 10979-10993. doi.org/10.1007/s00521-018-3801-x

Gibert, D., Mateu, C., Planes, J., & Vicens, R. (2019). Using convolutional neural networks for classification of malware represented as images. Journal of Computer Virology and Hacking Techniques, 15(1), 15-28. doi.org/10.1007/s11416-018-0323-0

Gnanaguruparan, M., & Kak, S. (2002). Recursive hiding of secrets in visual cryptography. Cryptologia, 26(1), 68-76. doi.org/10.1080/0161-110291890768

Jia, C., Yang, T., Wang, C., Fan, B., & He, F. (2019). Encryption of 3D point cloud using chaotic cat mapping. 3D Research, 10(1), 1-13. doi.org/10.1007/s13319-018-0212-9

Jisha, T. E., & Monoth, T. (2019). Authenticity and integrity enhanced active digital image forensics based on visual cryptography. In Smart Intelligent Computing and Applications (pp. 189-196). Springer, Singapore. doi.org/10.1007/978-981-13-1927-3_19

Kapoor, V., Abraham, V. S., & Singh, R. (2008). Elliptic curve cryptography. Ubiquity, 2008(May), 1-8. doi.org/10.1145/1386853.1378356

Kashyap, P., Rai, B., Kar, C., Kar, S. K., & Banerjee, S. (2018). An approach for visual cryptography scheme on color images. In Advances in Electronics, Communication, and Computing (pp. 501-508). Springer, Singapore. doi.org/10.1007/978-981-10-4765-7_53

Li, P., Yang, C. N., & Kong, Q. (2018). A novel two-in-one image secret sharing scheme based on perfect black visual cryptography. Journal of Real-Time Image Processing, 14(1), 41-50. doi.org/10.1007/s11554-016-0621-z

Meraihi, Y., Gabis, A. B., Mirjalili, S., & Ramdane-Cherif, A. (2021). Grasshopper optimization algorithm: Theory, variants, and applications. IEEE Access, 9, 50001-50024. doi.org/10.1109/access.2021.3067597

Mhala, N. C., & Pais, A. R. (2019). Contrast enhancement of Progressive Visual Secret Sharing (PVSS) scheme for gray-scale and color images using super-resolution. Signal Processing, 162, 253-267. doi.org/10.1016/j.sigpro.2019.04.023

Naor, M., & Shamir, A. (1994, May). Visual cryptography. In Workshop on the Theory and Application of Cryptographic Techniques (pp. 1-12). Springer, Berlin, Heidelberg. doi.org/10.1007/bfb0053419

Pande, L. N., & Shukla, N. (2013). Visual cryptography schemes using compressed random shares. International Journal of Advanced Research in Computer Science and Management Studies, 1(4).

Saremi, S., Mirjalili, S., & Lewis, A. (2017). Grasshopper optimisation algorithm: theory and application. Advances in Engineering Software, 105, 30-47. doi.org/10.1016/j.advengsoft.2017.01.004

Shankar, K., & Elhoseny, M. (2019a). Multiple Share Creation with Optimal Hash Function for Image Security in WSN Aid of OGWO. In Secure Image Transmission in Wireless Sensor Network (WSN) Applications (pp. 131-146). Springer, Cham. doi.org/10.1007/978-3-030-20816-5_9

Shankar, K., & Elhoseny, M. (2019b). Optimal Stream Encryption for Multiple Shares of Images by Improved Cuckoo Search Model. In Secure Image Transmission in Wireless Sensor Network (WSN) Applications (pp. 147-161). Springer, Cham. doi.org/10.1007/978-3-030-20816-5_10

Shankar, K., & Eswaran, P. (2017). RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography. China Communications, 14(2), 118-130. doi.org/10.1109/cc.2017.7868160

Shankar, K., Elhoseny, M., Kumar, R. S., Lakshmanaprabu, S. K., & Yuan, X. (2020). Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique. Journal of Ambient Intelligence and Humanized Computing, 11(5), 1821-1833. doi.org/10.1007/s12652-018-1161-0

Steczek, M., Jefimowski, W., & Szeląg, A. (2020). Application of grasshopper optimization algorithm for selective harmonics elimination in low-frequency voltage source inverter. Energies, 13(23), 6426. doi.org/10.3390/en13236426

Wang, P., He, X., Zhang, Y., Wen, W., & Li, M. (2019). A robust and secure image sharing scheme with personal identity information embedded. Computers & Security, 85, 107-121. doi.org/10.1016/j.cose.2019.04.010

Yang, C. N., Chen, C. H., & Cai, S. R. (2016). Enhanced Boolean-based multi secret image sharing scheme. Journal of Systems and software, 116, 22-34. doi.org/10.1016/j.jss.2015.01.031