
K. Shankar and Dr. P. Eswaran

INTRODUCTION

The term ‘cryptography’ refers to the process of safeguarding the secret data against access by unscrupulous persons in scenarios where it is humanly impossible to furnish physical protection. (Randhir Kumar and Akash Anil, 2011). It deals with the methods which convert the data between intelligible and unintelligible forms by encryption/decryption functions with the management of key(s) (Xuehu Yan et al., 2014). In fact, providing safety competencies to collective, isolated and unreliable storage Systems paves the way for the efficiency deprivation which provides several roadblocks in their deployment. Public-key cryptography techniques represent the orders of magnitude which is much slower than their symmetric key equivalents (Lanxiang Chen and Shuming Zhou, 2010). In this regard, the Visual cryptography symbolizes a brand of secret sharing wherein the secret is an image and the shares are also images printed on transparencies. The strangeness of this kind of secret sharing is that the restoration of the secret is achieved by superposing the shares (transparencies) of the participants (Arco et al., 2014). Visual Cryptography (VC) effectively offers a safe method to deliver confidential images in non-computer-aided decryption scenarios. A comprehensive visual cryptography scheme is offered which creates significant shares by integrating cover images into the noise-like shares (Pei-Ling Chiu and Kai-Hui Lee, 2015). The Visual cryptography techniques are assessed by means of two parameters: the pixel extension, which represents the number of sub pixels that each pixel of the original secret image is programmed into, and the contrast, which exhibits the visual quality of the reclaimed confidential image (Divya and Rama lakshmi, 2011). The VC, also known as the VSS, represents a confidential sharing model for images in which the decryption is carried out by superimposing the stacked shares through the human visual mechanism (Xiaotian Wu et al, 2014). The distinct quality of programming the secret deoid of any computer computation makes the VC a superb device for exchanging confidentialities in scenarios having meager computing skills (Pei-Yu Lin et al, 2015). In this regard, a homo-morphic cryptosystem glistens with the unique quality that when any specific algebraic function is carried out on the data input prior to encryption, the consequential encryption remains same as if an algebraic function is executed on the data input subsequent to encryption (Naveed Islam et al, 2011). The Dynamic
visual cryptography has been effectively employed for optical management of harmonically vibrating mechanisms and vibration generation tools (Vilma Petrauskiene et al., 2014). As opposed to the conventional cryptographic techniques like the Data Encryption Standard (DES) approach and the Advanced Encryption Standard (AES) method, The VC ushers in quicker decryption doing away with the Advanced Encryption Standard (AES) method, The Encryption Standard (DES) approach and the for optical management of harmonically vibrating visual cryptography has been effectively employed conventional cryptographic techniques like the Data secret image sharing has tackled this dilemma as the computational intricacy of the entire secret sharing secret of low dimension vis-à-vis the size of the secret to be communicated, without in anyway altering the computational intricacy of the entire secret sharing function (Kamel Mohamed Faroum, 2014). The secret image sharing has tackled this dilemma as the it encodes the user data into various secret shadows (shares) and allocates them to various participants (Xuehu Yan et al., 2015). The sharing of several secrets, cheating deterrence, sharing of color images, idyllic contrast attainment, provision of the region incrementing property, and provision of progressive recovery were launched later on (Ching-Nung Yang and Che-Yu Lin, 2015). The Elliptic curve cryptography, in essence, employs the elliptic curves which do not represent ellipses wherein the variables and the coefficients are all bound to elements of a restricted field. Generally, the EC is symbolized by a set of points in two dimensional Cartesian coordinate systems (Maria Celestina Vigila and Muneeswaran, 2012). In the modern public key cryptography, factors decomposition hassles dependent on huge numbers are habitually employed, the classic example being the RSA cryptography. With the looming growth of computer hardware and high-performance computing technology, the RSA has found itself plagued with certain insurmountable roadblocks (BAI Qing-hai et al., 2012). The solution of the innovative technique for keeping dishonesty at bay is the acceptance of several secret images in such a way that each qualified subsets will expose the relative secret image only, leaving the other secret images unfamiliar to the prospective hawkers (Du-Shiau Tsai et al., 2007).

RELATED WORKS

In 2015 Srinivasan nagaraj et al. The enlarged size of the internet and vast communication across it and also medical needs digital images require of security plays vital role. New encryption technique

Using elliptic curve cryptography with magic matrix operations for securing images that transmits over a public unsecured channel. There are two most important groups of image encryption algorithms: some are non chaos-based selective methods and chaos-based selective methods (Srinivasan nagaraj et al., 2015).

In 2015 Smithashree et al have proposed the image encryption based on synchronous cipher using Elliptic curve cryptography. The index point was generated using LFSR (Linear Feedback Shift Register) with a polynomial of degree n with an initial value. Take the output from LFSR as index and find the key (Ki) from the points on EC (Elliptic Curve) either y or both x and y coordinates points alternately and an image was encrypted using an additive encryption algorithm using the key (Ki) (Smithashree and Sujatha, 2015).

In 2013, Rupachandra Singh et al came out with an innovative video watermarking technique based on visual cryptography and scene change recognition in discrete wavelet transform domain. The concept was to deploy the various segments of a single watermark into several scenes of a video for the creation of the owner’s share from the original video in accordance with the frame mean in the identical scene and the binary watermark, and the generation of the identification share based on the frame mean of probably attacked video. Experiments are carried out to validate the strength by means of a sequence of investigations. The safety aspect of the proposed algorithm is well-taken care of by means of the visual cryptography (Rupachandra Singh et al., 2013).

In 2013 Credit goes to Peng Li et al for launching the Visual cryptography scheme (VCS) in which shares a binary confidential image into various binary shadows and the confidential image, in turn, can be visually exposed by stacking qualified shadows without the need for calculation. The VCS has failed to achieve efficiency in view of the mega development and inferior visual quality. Hence a universal Grey visual cryptography scheme is envisaged, with the skills to share further data, labeled as the Sharing More Information Grey Visual Cryptography Scheme (SMIGVCS). All the shadow pixels of VCS implant supplementary data for creating the Grey shadows of SMIGVCS, and the entrenched data originates from the shadows of a polynomial-based secret sharing scheme (PSSS). When assessed and contrasted with the two-in-one image secret sharing scheme (TiOISSS), the innovative SMIGVCS is competent to attain minor shadow size with satisfactory visual quality(Peng Li et al., 2013).

In 2013, Ali Soleymani et al were instrumental in envisaging an epoch-making encryption method based on the elliptic curves for protecting the images to be communicated over public channels. An
innovative mapping technique is envisioned to transform an image pixel value to a point on a predefined elliptic curve over finite field GF(p) with the help of a map table. The encryption and decryption procedures are furnished in a detailed manner with implementation. All statistical assessments are carried out on the encrypted image to appraise the power of the novel approach. In terms of the histogram, correlation, entropy and key sensitivity investigation, the novel cryptosystem offers a consistent protection for communicating images over the public channels (Ali Soleymani et al., 2013).

PROPOSED METHODOLOGY

The Visual cryptography method is used to send an original image from the transmitter to the receivers with confidentiality and secrecy. From the secret image the separate matrix is created for the RGB by using their pixel values ($P_i$). From those pixel values shares are created by using the sharing process of the visual cryptography. In the share creation process each share is separately created by utilizing the new Visual Secret Share (VSS) creation procedure to improve the performance of the images. Multiple Shares are divided into blocks for the security purpose of the images utilized the Elliptical Curve Cryptography (ECC) method. This method consists of the encryption and decryption processes, the public key, and the private key generated by using the prime number and the base point of the images. The key generation for the encryption process includes the ECC multiplication process Point addition and Point doubling utilized to generate the public key. Decryption process employs the optimization technique for the private key generation of the ECC method. For improving the performance of the cryptographic image in the ECC method different optimization techniques are used such as the Cuckoo Search (CS), Ant Colony Optimization (ACO), Particle Swarm Optimization (PSO) and Grey Wolf Optimization (GWO) for the private key generation by the ECC method. The performance of the image is taken as the fitness value for the optimization process such as the peak signal to the noise ratio value (PSNR) and correlation coefficient (CC) value. After the decryption process, finally the output image is compared with the original image for evaluating their performance by using the PSNR MSE and CC values. By using this method, the original image is shared securely and its information is maintained with confidentiality.

Block Diagram:

Figure 1 shows the block diagram of the proposed scheme in visual cryptography and its each blocks are explained in the following.

**Secret Image:**

The pixel values of the secret color image (original image) are extracted and take as RGB pixel values and these values are separately indicated as matrix $R_p, G_p$ and $B_p$ the size of the matrix is the same size of the original image size (R*C). The original pixel values of the image is

$$\text{Pixel} = \sum_{i=1}^{R*C} R_i + G_i + B_i$$

Where, $R_i, G_i$ and $B_i$ (R*C) is the size of the original image size and the color is specified as Red, Green and Blue. Every pixel from the secret image is encoded into multiple sub pixels in each share image using a matrix to determine the color of the pixels.

**Visual Secret Sharing (VSS):**

In the Visual Secret Sharing (VSS) procedure, a binary secret image is encoded into n shares known as ‘transparencies’. Each and every share comprises both black and white pixels, in the shape of noise and is exceptionally large in dimension when compared to that of the secret image. The binary secret image can be deciphered with the help of the visual system by overlapping any k of n transparencies.
unaccompanied by any sort of cryptographic calculation. Original pixel of the secret image emerges in ‘n’ adapted versions labeled as ‘shares’ is a compilation of sub-pixels of the RGB image. Now, to overlap the i - th R share with the i - th G share along with the i – th B share, for i=1,2…n, to generate the final i – th share which is home to the related R, G and B segments. Each and every R, G, B share depends on the pixel value of the RGB image. The share for RGB is separately indicated as R, G, and B, indicated as

\[
R_p = \lim_{k \to \infty} R_{ab}
\]

\[
G_p = \lim_{k \to \infty} G_{ab}
\]

\[
B_p = \lim_{k \to \infty} B_{ab}
\]

Where, a and b are the positions in matrix R, G, and B are components of the image pixel. The R, G and B band pixel values are obtained from the original image and considered as the separate matrix. In this investigation, a new visual secret share generation technique is employed process to utilize to produce two shares each of every image. The essential stages of the VSS process are elegantly exhibited below.

Algorithm 1: Visual Secret Share (VSS) Creation process

1. Select an image of size w×h of the image, where w is a width and h is a height of the image.
2. Create two matrices for share 1 and share 2 pixels
3. Initialize variable font color and index value
   Initially set index=1
   For w and h is 1 to width and height
   Image color=Get pixel color from w×h
   Index= Choose random number either 0 or 1
4. If (index==1)
   Set Share 1 pixel (w×h) =Image Color
   Set Share2 pixel (w×h) = Empty
5. else
   Set Share 1 pixel (w×h) = Empty
   Set Share2 pixel (w×h) = Image Color

Above mention process based the shares are created in each band(R, G and B) of the image. Here, the number of basics matrices is 1 and number of shares is 2. For example,

\[
R = \begin{bmatrix}
175 & 209 & 204 \\
122 & 145 & 176 \\
105 & 118 & 131 \\
\end{bmatrix}
\]

G = \begin{bmatrix}
62 & 72 & 69 \\
122 & 145 & 176 \\
123 & 156 & 164 \\
\end{bmatrix}

B = \begin{bmatrix}
63 & 100 & 108 \\
83 & 93 & 94 \\
93 & 109 & 103 \\
\end{bmatrix}

After that, basics matrix based created the share R_{S1}, R_{S2}, G_{S1}, G_{S2}, and B_{S1}, B_{S2} are shown in below matrix. For example R band share creation process initially generate the empty matrix this contain the 255 pixel values and VSS process based shares are created.

\[
R_{S1} = \begin{bmatrix}
255 & 209 & 255 \\
255 & 255 & 255 \\
122 & 145 & 176 \\
\end{bmatrix}
\]

\[
R_{S2} = \begin{bmatrix}
175 & 255 & 204 \\
122 & 255 & 255 \\
105 & 118 & 131 \\
\end{bmatrix}
\]

\[
G_{S1} = \begin{bmatrix}
255 & 72 & 255 \\
68 & 85 & 255 \\
123 & 156 & 164 \\
\end{bmatrix}
\]

\[
G_{S2} = \begin{bmatrix}
62 & 255 & 69 \\
255 & 255 & 85 \\
255 & 255 & 255 \\
\end{bmatrix}
\]

\[
B_{S1} = \begin{bmatrix}
63 & 255 & 108 \\
83 & 255 & 94 \\
93 & 109 & 103 \\
\end{bmatrix}
\]

\[
B_{S2} = \begin{bmatrix}
61 & 50 & 255 \\
255 & 255 & 68 \\
95 & 255 & 255 \\
\end{bmatrix}
\]

Block Creation:

The Secret offering method is intended is to encrypt a confidential image into n trivial offer images. It is not possible to release any data on the preliminary image till the entire shares are attained. The offers are obtained from the distinctive confidential image well-before the encryption. At the outset, it ascertains the number of shares (n) to be generated. The client is given freehand to fix the level of excellence for n. prior to distinguishing the shares, the requisites networks are primarily designed and well-gearied in accordance with the number of shares to be shaped. At this juncture, a random Key is generated which is centered on block size of the confidential image, which habitually is in the dimension of 4x4 or 8x8.

Elliptical Curve Cryptography:

The Elliptic curve cryptography (ECC) is competent to furnish the identical degree and kind of safety as provided by the RSA but with smaller keys. The ECC represents a method for the public-key cryptography according to the algebraic configuration of elliptic curves over finite fields. One of the glittering advantages in relation to the non-ECC cryptography is the identical degree of safety offered by small size keys. The cryptography, in essence, characterizes a mathematical based technique to guarantee unqualified data safety over a public channel and has two primary objectives such as Privacy and Authentication. Thus, because of privacy, no data can be accessed by illegal individuals. Further on account of Authentication, data is not transformed in the changeover and the parties entering into communication are absolutely authenticated entities. The ECC procedure proceeds through certain phases such as……
Select the parameters for ECC process:

In fact, the Elliptic Curve Method (ECM), linked with cryptography, is called the ECC for performing open key cryptography. Elliptic Curve Cryptography (ECC) hitherto enjoys the distinctive brand name. The paramount and well-known strategy which figures it out functions in jam-packed rocking time-frame. Its safety emanates from the Elliptic Curve Logarithm, which represents the Discrete Logarithm Problem (DLP) in a congregation symbolized by concentrating on an elliptic curve over a restricted domain field. For the existing cryptographic objective, an elliptic curve takes the shape of a plane curve over a fixed field, instead of being represented in the real numbers, and it comprises the points which very well meet the equation.

\[ y^2 = x^3 + ax + b \quad (5) \]

The parameter of the ECC process which are the prime number and the two integer value these consequences in a sensational reduction in key size expected to attain to the identical level of security offered in customary public key cryptography plans Let the equation of the curve is

\[ y^2 \mod p = x^3 + ax + b \mod p \quad (6) \]

Where a, b are the integers and p is the prime number.

Base point generation:

It is the general equation of the elliptic curve. In the elliptic curve cryptography, the prime number is selected as k and private key is selected as L. Then, the Elliptic curve cubic equation is the,

\[ P = S(i)^3 + u \cdot S(i) + v \quad (7) \]

Where, u and v are the constants and it is u=v=2.

The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements. If the condition \( X=Y \) is satisfied, the best point is selected for the elliptic curve. The x and y is

\[ x = \text{mod}(P, n_p) \quad (8) \]

\[ y = \text{mod}(S(j)^3, n_p) \quad (9) \]

Where p(i,j) the points of elliptic curves are \( n_p \) the prime number. The doubling process is used to find the x and y values.

Key generation process:

In the confidential image, the secret key \( K_s \) are provided by the user. The column transformation can be worked out on the confidential image prior to the formation of the fundamental matrices to fine-tune the safety level. Two keys are employed in the ECC technique such as the private key \( H \) and the public key \( K_p \). The required vital matrices are configured according to the number of shares to be generated.

The best point \( K_s(k, l) \) and \( K_p \) is a public key. The public key is the \( K_p = H \cdot K_s \quad (10) \)

Let generate the key matrix \( K_{8} \) randomly for examples

\[ K_{8} = \begin{bmatrix} 55 & 134 & 155 & 87 \\ 151 & 133 & 98 & 130 \\ 189 & 102 & 167 & 89 \\ 134 & 38 & 83 & 63 \end{bmatrix} \]

Encryption method:

The encryption is the process of encoding messages or information in such a way that they can be authorized. In the encryption method, each share has block and every block section is encrypted by the encryption method. The number of blocks is represented as b(i, j) where i and j are the row and column of the block of the share. The number of shares the image would be divided (n) and number of shares to reconstruct the image (k) are also taken as input from the user. The encryption, i.e. the division of the image into n number of shares such that k number of shares is sufficient to reconstruct the image. In this process, every two parts of the data is given as input for the encryption process. The public key generation of the encryption point doubling and the point addition process will be used.

Point doubling: Point doubling is similar to point addition, except one takes the tangent of a single point and finds the intersection of the curve with the tangent line. Key generation process selects the base point \( (X_p, Y_p) \) and the prime number. This can be algebraically calculated by:

\[ \lambda = \frac{3 X^2 + a}{2 Y} \quad (11) \]

\[ X_q = \lambda^2 - 2X_p \quad (12) \]

\[ Y_q = \lambda(X_q - X_p) - Y_p \quad (13) \]

Where a is the multiplication factor of X in the elliptic field given by \( X+aX+b \).

Point addition: Point addition is defined as taking two points along a curve \( E \) and computing where a line through them intersects the curve. The operation is denoted as \( P + Q = R \) or \( (X_r, Y_r) = (X_a, Y_a) \).

This can be algebraically calculated by:

\[ \lambda = \frac{Y_r - Y_p}{X_r - X_p} \quad (14) \]

\[ X_s = \lambda^2 - X_p \quad Y_s = \lambda(X_s - X_p) - Y_p \quad (15) \]

These processes based find the public key for the encryption process the data \( X_s(i, j) \)and \( Y_s(i+1, j) \).
the point is
\[ C_1 = H \ast K \]  \hspace{1cm} (16)
\[ C_2 = (X_n, Y_n) + C_1 \]  \hspace{1cm} (17)

The number of keys used if sender and receiver use the same key, the system is referred to as symmetric, single key or secret key conventional encryption. If the sender and the receiver each uses a different key the system is referred to as asymmetric, two key, or public-key encryption.

**Decryption method:**

The Decryption is the converse methodology of encryption which represents the procedure of shifting over the encrypted content into its unique plain content. In this process, the private key (H) is employed to decode the message and the point \( C_1 \) is utilized to decrypt the pixel point.

\[ C_{11} = H \times C \]  \hspace{1cm} (18)

In the decryption procedure, the colors images are regained by modifying the decrypted indexed images back to their RGB (Red-Green-Blue) versions. In the cryptographic method cipher images are communicated after encryption to the decryption technique. Fig 1 illustrates the equation based each share (1 and 2) both of which are discretely encrypted and decrypted in the RGB bands. In the relative decryption task, the secret key H is produced by employing various optimization methods like the Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO) cuckoo search (CS) and the Grey wolf optimization (GWO) algorithm. In this method, the finest optimal key is achieved in the GWO algorithm.

**Grey Wolf Optimization (GWO) algorithm:**

The grey wolf, as a point of fact, is an integral member of the Canidae family. The group of the grey wolves is considered as the summit predators, illustrating their pivotal rank at the summit of the food chain. They often illustrate a unique behavior of surviving as a cluster. The leaders include a male and a female, and are designed as alpha, which are usually entrusted with the function of taking suitable decisions regarding several features like the hunting, sleeping place, time to wake, and the like.

The appropriate decisions taken by the alpha are immediately communicated to the entire group. The Beta signifies the second rank in the chain of command of the grey wolves. In fact, they represent the secondary wolves which efficiently extend assistance to the alpha in the decision-making or other group functions.

The omega lies at the lowest level of the grey wolf family structure and normally works like the scapegoat, submitting to the other dominant wolves on almost all occasions. They are permitted to eat only after all the other wolves have taken their dishes. In our innovative technique, the alpha (\( \alpha \)) is considered as the most suitable solution in order to methodically copy the social hierarchy of wolves at the time the GWO is designed. Consequently, the second and third best solutions are termed as beta (\( \beta \)) and delta (\( \delta \)) correspondingly. The rest of the candidate solutions are considered to be the omega (\( \omega \)). In the GWO method the hunting (optimization) is directed by \( \alpha \), \( \beta \), \( \delta \) and \( \omega \).

<table>
<thead>
<tr>
<th>Algorithm 2: Grey Wolf Optimization Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: Initialize the solution</td>
</tr>
<tr>
<td>( H_i = { H_1, H_2, \ldots, H_n } ) \hspace{0.5cm} Initialize a, A and C</td>
</tr>
<tr>
<td>Step 2: Find the fitness for the initial solution,</td>
</tr>
<tr>
<td>( F_i = \text{Max} ) (PSNR+CC)</td>
</tr>
<tr>
<td>Step 3: Based on the fitness separate the solution</td>
</tr>
<tr>
<td>( H_{a} ) = the best search solution,</td>
</tr>
<tr>
<td>( H_{b} ) = the second best search solution,</td>
</tr>
<tr>
<td>( H_{d} ) = the third best search solution</td>
</tr>
<tr>
<td>Step 4: Update the position of the current search solution</td>
</tr>
<tr>
<td>( H(t+1) = \frac{H_{a} + H_{b} + H_{d}}{3} )</td>
</tr>
<tr>
<td>Step 5: Calculate the fitness for new search solution,</td>
</tr>
<tr>
<td>( F_{i(new)} = \text{Max} ) (PSNR+CC)</td>
</tr>
<tr>
<td>Step 6: Store the best solution so far attained, Iteration=Iteration+1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Initialization process:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initialize the solution as random key values in a decryption process and the host nest population ( (hnp) ) is generated by the given initial solution ( (H_{i}) ) and certain algorithm parameters such as a, A and c as coefficient vectors.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fitness Function:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluate the fitness value of each solution and then calculate the best solution values. In step 2 mentions ( F_{i} ) PSNR is peak signal to noise ratio and CC is correlation factor of each image.</td>
</tr>
</tbody>
</table>
Based on the fitness separate the solution:
Now, we find the fitness separate solution (private key) based on the fitness value. Let the first best fitness solutions be α, the second best fitness solutions β and the third best fitness solutions δ.

Update the position:
Let us presume that the alpha as the best candidate solution along with beta and delta are equipped with the superior awareness about the probable locality of the prey with the intention of scientifically reproducing the hunting character of the grey wolves. Consequently, we accumulate the first three best solutions achieved till now and command the other search agents including the omegas to update their locations in accordance with the location of the best search agent. For the purpose of modification of the innovative solution H(t+1) the following formulas are effectively utilized.

\[ D^\alpha = C.H_\alpha - H_t, \quad D^\beta = C.H_\beta - H_t, \quad D^\delta = C.H_\delta - H_t \]  

\[ H_t = H_t - A.(D^\alpha), H_t = H_t - A.(D^\beta), H_t = H_t - A.(D^\delta) \]  

With the intention of having the hyper-spheres with various random radii the arbitrary constraints such as the A and C extend a helping hand to the candidate solutions. The research and deployment are invariably ensured by the adaptive values of A and C, which allow the GWO to effectively carry out the research and deployment. As A goes on diminishing, almost 50% of the iterations are submitted to the research (|A|<1) and the remainder are dedicated to the deployment. By means of encompassing the character, the succeeding equations are utilized with the intention of mathematical modeling.

\[ D = |C.H_\alpha(t) - H(t)| \]  

For find the coefficient vectors use equation:
A = 2a_1t - a,  \quad C = 2t_r \]  

The GWO has only two main parameters to be adjusted (A and C). However, we have kept the GWO algorithm as simple as possible with the fewest operators to be adjusted. The maximum accuracy obtained in the process will be continued.

It has an infinite variance with an infinite mean. Here the steps essentially form a random walk process with a power law step length distribution with a heavy tail. Then get the maximum fitness and optimal key.

\[ C_{ij} = H_{optimal} \times C_{ij} \]  

\[ C_{ij} = C_2 - C_{11} \]  

The C_{ij} represents the final result of the decryption method.

Stacked Image:
The stacked image is predicted by the enhancement process in the cryptography. The Grey wolf optimization improvement results in key production in the deciphering of the confidential image. In the confidential image each offer is part in block image and the prime number is selected along with the private key, a, b values. Thereafter, the base point production occurs and the key is generated centered on the block size of the confidential image. Finally, the GWO improvement in encryption and decryption is carried out and the output image is attained. Further, all the deciphered shares are amassed together to attain the original image. That means

\[ R_p = R_1 \oplus R_2 \]  

\[ G_p = G_1 \oplus G_2 \]  

\[ B_p = B_1 \oplus B_2 \]

Final decrypted image

\[ F_{water} = R_p + G_p + B_p \]

RESULTS AND DISCUSSION

Visual cryptography process different images are used to evaluate the performance of the proposed scheme. In this process, consider different images such as the Lena, (image1) house (image 2), peppers (image 3), and baboon (image4) are used to split the RGB band to generate the shares. In the encryption process the public key is generated randomly selected from the key matrix and the decryption process generates the private key by using the optimization techniques such as the Particle Swarm Optimization (PSO), Ant colony Optimization (ACO) cuckoo search (CS) and Grey Wolf Optimization (GWO) algorithm. In all these optimization techniques the maximum fitness PSNR and CC is attained in the GWO optimization technique. The performance of the proposed scheme is analyzed by using the PSNR, CC MSE, Variation of Information (VI), Global Consistency Error (GCE) and Random Index (RI) value in all images. And also apply the different attacks in all images, to analyze the proposed scheme.

Experimental results:
The original confidential image divides the RGB band images, each possessing two diverse dependent on the multiple share generation. Subsequently, various images like image 1 (Lena), image 2 (house), image 3 (peppers) and image 4 (baboon) are employed to create the number of shares. Now, two shares are produced for each diverse image of the RGB band. In each band, each share is individually encrypted and decrypted to attain the original image. Thereafter various factors of performance, like the PSNR, MSE and CC, values of each share are
evaluated and the ambushes also included in the shares for assessing the performance.

Table 1, 2, 3 and 4 shows the image 1 (Lena), image 2 (house), image 3 (peppers) and image 4 (baboon) are employed in producing the two different shares. The three band 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. In secret image based generate the RGB band and each band has two shares, these shares are separately encrypted and decrypted to retrieve to the original image.

Table 1: Proposed scheme for image1 (Lena)

<table>
<thead>
<tr>
<th>Original image</th>
<th>Different band images</th>
<th>Two shares</th>
<th>Encrypted image</th>
<th>Decrypted image</th>
<th>Stacked image</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="lena.png" alt="Image 1" /></td>
<td><img src="lena.png" alt="Image 1" /></td>
<td><img src="lena.png" alt="Image 1" /></td>
<td><img src="lena.png" alt="Image 1" /></td>
<td><img src="lena.png" alt="Image 1" /></td>
<td><img src="lena.png" alt="Image 1" /></td>
</tr>
<tr>
<td><img src="lena.png" alt="Image 1" /></td>
<td><img src="lena.png" alt="Image 1" /></td>
<td><img src="lena.png" alt="Image 1" /></td>
<td><img src="lena.png" alt="Image 1" /></td>
<td><img src="lena.png" alt="Image 1" /></td>
<td><img src="lena.png" alt="Image 1" /></td>
</tr>
</tbody>
</table>

Table 2: Proposed scheme for image2 (House)

<table>
<thead>
<tr>
<th>Original image</th>
<th>Different band images</th>
<th>Two shares</th>
<th>Encrypted image</th>
<th>Decrypted image</th>
<th>Stacked image</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="house.png" alt="Image 2" /></td>
<td><img src="house.png" alt="Image 2" /></td>
<td><img src="house.png" alt="Image 2" /></td>
<td><img src="house.png" alt="Image 2" /></td>
<td><img src="house.png" alt="Image 2" /></td>
<td><img src="house.png" alt="Image 2" /></td>
</tr>
<tr>
<td><img src="house.png" alt="Image 2" /></td>
<td><img src="house.png" alt="Image 2" /></td>
<td><img src="house.png" alt="Image 2" /></td>
<td><img src="house.png" alt="Image 2" /></td>
<td><img src="house.png" alt="Image 2" /></td>
<td><img src="house.png" alt="Image 2" /></td>
</tr>
</tbody>
</table>

Performance analysis:
The statistical analytic investigation on the innovative image encryption approach has illustrated its unparalleled complexity and diffusion qualities which categorically combat assessable ambushes. This is revealed by an investigation on the histograms of the enciphered images and on the correspondences of adjoining pixels in the decrypted image. The histograms images have effectively exhibited the decrypted image and distinctive image comparisons. Moreover, it also shows how the pixels of the images are circulated in the encrypted and
decrypted images without causing any reductions the image features.

**Peak Signal to Noise Ratio (PSNR):**

The signal, here, represents the original data, and the noise relates to the flaw triggered by the compression. While analyzing and contrasting the compression codec’s, the PSNR constitutes an approximation to human insight of modernization excellence. Even though a superior PSNR usually reveals the fact that the modernization is of superb quality, though there are exceptions to this trend. Therefore, it is highly essential to take utmost care regarding the extent of validity of this metric.

\[
PSNR = \frac{1}{s} \sum_{i=1}^{s} 20 \times \log_{10} \left( \frac{255}{\text{MSE}_i} \right)
\]

Where \( S \) is the number of shares (i=1,2) and MSE is the mean square error

**Mean Square Error (MSE):**

In statistics, the mean squared error (MSE) of an estimator evaluates the average of the squares of the "errors", in other words, the divergence between the estimator and the subject-matter of estimation. This tool represents a risk function, relating to the "errors", in other words, the divergence between the estimator and the subject-matter of estimation. This tool represents a risk function, relating to the anticipated value of the squared error loss or quadratic loss.

\[
MSE = \frac{1}{S} \sum_{i=1}^{S} \left( \frac{1}{a+b} \sum_{i=1}^{a+b} (O_{ij} - D_{ij})^2 \right)
\]

Where, \( a \) and \( b \) is the width and length of the original image, \( x \) and \( y \) is the row and column value of the pixel, \( O \) is the original image pixel and \( D \) is the decrypted image pixel value. This equation based obtains the MSE value for each shares of each band.

**Correlation Coefficient (CC):**

To assess the correlation between two neighboring pixels throughout plain-image and the ciphered image, this procedure is performed. Here, the correlation coefficient of each set is carried out by means of successive equations,

\[
W(x, y) = \frac{CON(x, y)}{M(x) \times M(y)}
\]

Where

\[
CON(x, y) = \frac{1}{F_x} \sum_{i=1}^{F_x} (x_i - M(x)) \times (y_i - M(y))
\]

\[
M(x) = \frac{1}{F_y} \sum_{i=1}^{F_y} x_i
\]

\[
M(y) = \frac{1}{F_y} \sum_{i=1}^{F_y} (y_i - M(x))^2
\]

Where, \( W(x,y) \) is the correlation coefficient, \( M(x) \) and \( M(y) \) are the mean value of the \( x \) and \( y \) are the two adjacent pixel values; \( F_x \) is the number of pairs \( x,y \). This equation based obtain the CC in each shares.

Global Consistency Error (GCE):

The GCE evaluates the level up to which several images can be deemed as an improvement over the other. The original image represents simply a division of the pixels of an image into sets.

\[
GCE = \frac{1}{n} \min \left\{ \sum_{i=1}^{S} E(S_i, S_{i+1}), \sum_{i=1}^{S} E(S_i, S_{i+2}) \right\}
\]

Where, segmentation error measure takes two different image \( S_1 \) and \( S_2 \) as input, these values contain pixel.

Variation of Information (VI):

The VI metric defines the distance between two diverse images as average conditional entropy of the one image to other.

\[
VI(X; Y) = H(X)+H(Y)−2I(X, Y)
\]

Where, \( H(X) \) is entropy of X and \( I(X, Y) \) is mutual information between X and Y

Random Index (RI):

The Rand index determines the percentages of pairs of pixels category which are consistent among the evaluated image and the decrypted image averaging across several ground truth division. Also labeled as the Rand measure it represents an evaluation of the resemblance between the two categorizations.

\[
RI = \frac{a + b}{a + b + c + d}
\]

Where, \( a + b \) is the number of agreements between X and Y and \( c + d \) is the number of disagreements between X and Y.

In table 5 explains that the different images with the performance of the histogram equalization with the presentation assessment parameters such as PSNR, CC, MSE, VI, GCE and RI for the suggested scheme. For the elliptic curve cryptography strategy the intended system encloses the many share creation, encryption, and decoding scheme. The histogram image shows how the image pixels are divided in the image, in addition presents the contrast among the original image and final image in the wake of applying the suggested approach for examining the images. Through images, by their PSNR values the suggested approach is linked with the image and output images are pointed out. The PSNR value points out the nature of the image to the output image after the suggested scheme linked with it. Now the PSNR value of each image is 69.568. The MSE value as well the GWO process 0.013 and the global constancy error value of the suggested method has a better value that is 0.415 similarly the RI and VI is 1.03 and 1.895. Now the CC parameter is 0.995 and it presents the original image is maintained in the decrypted image after the suggested segment.
Table 5: Performance evaluation of Different images

<table>
<thead>
<tr>
<th>Original image</th>
<th>Histogram for original image</th>
<th>Decrypted image</th>
<th>Histogram for Decrypted image</th>
<th>PSNR</th>
<th>MSE</th>
<th>CC</th>
<th>GCE</th>
<th>VOI</th>
<th>RI</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>68.957</td>
<td>0.010</td>
<td>0.84</td>
<td>0.28</td>
<td>2.22</td>
<td>0.28</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>69.917</td>
<td>0.006</td>
<td>0.99</td>
<td>0.28</td>
<td>2.22</td>
<td>0.84</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>67.194</td>
<td>0.031</td>
<td>0.99</td>
<td>0.27</td>
<td>0.84</td>
<td>2.17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>71.599</td>
<td>0.005</td>
<td>0.99</td>
<td>0.83</td>
<td>2.29</td>
<td>0.83</td>
</tr>
</tbody>
</table>

**Attack:**
The positions of the pixel values are changed in the image for finding the image without changing its image quality. In table 6 shows that the attack applied image and the performance. The attack changed the image information but the proposed scheme retrieves the image with the minimum noise and its PSNR value is nearly 72% retrieved. So it maximums retrieve the information with the minimum distortion.

In table 6 shows that the proposed scheme with the attack applied for the all images the PSNR value will be minimized. For Lena image the attack applied the PSNR is minimized in 3.35% and the MSE value also minimized in 0.023% then the performance analysis parameters are minimum for attack applied for the image compared to the proposed scheme.

Table 6: Attack applied results

<table>
<thead>
<tr>
<th>Original image</th>
<th>Histogram for original image</th>
<th>Attacked image</th>
<th>Histogram for attacked image</th>
<th>PSNR</th>
<th>MSE</th>
<th>CC</th>
<th>GCE</th>
<th>VI</th>
<th>RI</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>65.88</td>
<td>0.0254</td>
<td>0.999</td>
<td>0.292</td>
<td>2.343</td>
<td>0.838</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>66.209</td>
<td>0.024</td>
<td>0.999</td>
<td>0.285</td>
<td>2.287</td>
<td>0.842</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>63.927</td>
<td>0.033</td>
<td>0.994</td>
<td>0.279</td>
<td>2.238</td>
<td>0.840</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>67.088</td>
<td>0.0183</td>
<td>0.999</td>
<td>0.292</td>
<td>2.365</td>
<td>0.837</td>
</tr>
</tbody>
</table>

Table 7 shows that the comparison graph between the with attack and without attack of all images (Lena, house, pepper and baboon). In this graph the X axis takes the with attack and without...
The attack Y axis takes the different images and Z axis shows that the PSNR, MSE and CC values. When the attacks are applied to the different images, the PSNR value of without attack image is a best performance. The PSNR value of the without attack compared to with attack 98.23% retrieved the original image. All the parameter value minimized 95.23%. The correlation coefficient value (CC) is comparatively low in attack applied to all the images and the CC value in all the images in the proposed scheme attained in better value.

Table 7: Comparison between with attack and without attack

<table>
<thead>
<tr>
<th>PSNR</th>
<th>MSE</th>
<th>CC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Comparative Analysis:

Then the decryption process generate the private key various dissimilar optimization techniques are utilized which are PSO, ACO, CS and GWO optimization technique comparison also shown in below table 8. To locate private key to the decryption process these algorithms are employed. The fitness function based high value PSNR and CC is achieved in the GWO algorithm. It gives PSNR value of the all images is 69.56 it’s contrasted to the other optimization technique the PSNR minimized as 9.238% and mean square error value of GWO compared to the ACO the error variation is 5.4% for house image. Likewise the other images as well the performance study factor better for GWO contrasted to the other techniques.

Table 8: Comparison between optimization techniques in different images

<table>
<thead>
<tr>
<th>PSNR</th>
<th>MSE</th>
<th>CC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Convergence Graph:

Different optimization techniques such as Grey Wolf Optimization (GWO), Ant Colony Optimization (ACO), Particle Swarm Optimization (PSO) and Cuckoo Search (CS) are used to the find the private key. The fitness estimation of this process is maximum value of PSNR and CC value attained in GWO algorithm.

Figure 2 shows that the convergence graph is plotted between the iteration and fitness estimations of the various strategies, for GWO, PSO, ACO and CS. This graph basically resolves that the GWO procedure is given the greatest fitness using least possible iteration. Through the graph, the GWO Strategy takes the minimum iteration for providing the ideal result. Subsequently, it is maximized to 69.45 and it’s attained in 94 iterations. Initial iteration the fitness value of GWO is 22.36 and other techniques also the initial fitness value is 15.63. Then the iteration is varied the performance also varying based on the procedure of the techniques. The maximum fitness of GWO compared to the CS the difference is 5.56% similarly the other algorithm also the difference is 11.29%. Through the graph the grey wolf optimization strategy just specifies the ideal fitness value with the efficient results.
CONCLUSION

Visual cryptography process is created by using the visual secret sharing scheme with the elliptic curve cryptography. The shares are separately encrypted and decrypted by means of the encryption and decryption technique in line with the elliptic curve cryptography and the point doubling and addition multiplication process used in key generation. In the decryption process generate the private key by the use of the Grey wolf optimization (GWO) optimization technique. It is clear that the PSNR values of the secret different images are 68.95, 69.917, 67.174 and 71.599. The mean square error value is minimized in all images is 0.010, 0.006, 0.03 and 0.005 then the correlation coefficient value is the almost in all the images are nearly 0.999. The correlation coefficients and histogram estimations have made it clear that the encryption technique was performed on the secret image so as to preserve the confidentiality of the image. In future, the performance increase the secret image by using the other method instead of ECC the peak signal to noise ratio will be improved by using this, the image quality is also improved as well as minimizing its mean square error value.

REFERENCES


Peng Li et al., 2013. Sharing more information in Grey visual cryptography scheme. Journal of visual communication image, 24 :1380-1393.


Xiaotian Wu et al., 2014. Improved tagged visual cryptography by random grids. Signal Processing, 97: 64-82.