ENHANCED VISUAL CRYPTOGRAPHY NETWORK (EVCN) FOR SECURED DATA TRANSMISSION COMBINING DES AND ELLIPTIC CURVE CRYPTOGRAPHY

Surajit Goon

Department of Computer Science & Engineering, Brainware University
Barasat, 700125, India
goon_surajit@yahoo.co.in
https://www.brainwareuniversity.ac.in

Debdutta Pal

Department of Computer Science & Engineering, Brainware University
Barasat, 700125, India
ddp.cs@brainwareuniversity.ac.in
https://www.brainwareuniversity.ac.in

Souvik Dihidar

Department of Computer Science, Eminent College of Management & Technology
Barasat, 700126, India
souvik@ecmt.in
https://www.ecmt.in

Abstract

Internet usage has shown an enormous increase in recent decades. Textual data, images and even videos are transmitted across the globe through emails, chat applications, virtual meet applications and many more. Visual cryptography, being renowned for encryption, can guarantee the protection of image data to a great extent. Visual cryptography concentrates on secret sharing, which encrypts a secret image into shares that will not disclose any information regarding the original confidential image. This research work proposes an Enhanced Visual Cryptography Network (EVCN) with an encryption-decryption strategy that combines the Data Encryption Standards (DES) Algorithm and Elliptic Curve Cryptography (ECC) algorithm for encrypting input images, followed by the addition of a secret text to the input image. Finally, the Long Short Term Memory Network (LSTM) is used for evaluating the performance of the proposed system.

***Keywords*: authentication, Data Encryption Standards, encrypted image, elliptic curve cryptography, Internet, long short term memory, Visual Cryptography, Signal to noise ratio, Bit Error rate.**

1. Introduction

Due to enormous growth in the digitization of multimedia, image security evolved as the major plan related to the secure transmission of data over unsecured channels [Kalimuthu *et al*. (2021)]. Images are often applied in diverse domains like medical imaging, business, advertising, marketing, online teaching, and even certain confidential messages. The last few decades have shown growing use of technologies in various multidisciplinary domains like science, entertainment, inspections, border control and military operations. In some specific areas of applications, there arises a need for hiding strategic information like the data acquired or the relevant details regarding the same. The insurance of data protection and privacy seems to be struggling to be effectively solved. As a result, many security schemes and algorithms keep evolving rapidly. Internet of Things (IOT) devices has simple data processing targets like sensors, smart watches, mobile applications and many more [Basavaiah *et al*. (2021)]. These devices are accompanied by very small memory and limited computational abilities [Rathee *et al*. (2020)]. Because of this reason, IOT devices do not have the special memory provision for storing and processing

security functions. Some techniques need to be imposed on this issue, leading to the evolution of lightweight cryptography [Jadhav (2019)].

The important concern related to this in the real-time scenario is data security when transmitting these images through the internet and storing them on multiple platforms; protecting the confidentiality, authenticity and integrity of the images is a major concern [Abroshan (2021)]. This drives the need for highly secure encryption algorithms. Recently various approaches have been intelligently presented to overcome the related challenges of image security requirements. Based on the key distribution, the cryptosystems are broadly classified as symmetric and asymmetric encryptions. Symmetric encryption employs the usage of the same key for both encryption and decryption [Mansoor *et al.* (2029)]. With the knowledge of one of the keys, the calculation of the other seems to be pretty easier. These types of encryption schemes are still in use in various fields owing to the less computational complexity and speed of encryption [Alaya (2021)]. The management and distribution of keys remain a barrier that needs proper attention. When the symmetric key algorithm is employed multiple times, it dramatically increases the number of keys that will be employed. Intruders may also intercept the process of key distribution. As a result of this, the symmetric algorithms are most often not being used individually. On the other hand, a combination of two or more symmetric or asymmetric algorithms is believed to guarantee improved security.

Modernization in biomedical image-related pieces of equipment and their related processing technologies led to the increase in usage of image-based medical data rapidly [Vodnala *et al.* (2021)]. These data need to be transmitted over a public network among hospitals or doctors in providing telemedicine services and, at times, even need to be used by a telemedicine database center to upload it. Owing to limited local storage and computing resources, they may also be needed to be stored in the cloud storage or databases [Palevicius *et al*. (2018)]. These images may involve sensitive and confidential patient information details, which increases the need for confidentiality technology that can protect the privacy credential of patients.

To overcome the problems posed by the symmetric encryption systems, asymmetric encryption ensures the usage of different keys for encryption and decryption [Hao *et al.* (2021)]. The most important aspect of this is that the knowledge of the encryption key will not favor the knowledge in calculating the key for decryption. Secure data communication among multiple sophisticated users is the added advantage of this approach, followed by the prevention of key distribution through unsecure internet channels. The asymmetric encryption scheme requires two different types of keys, likely the private and the public key. The public key can be made open to everyone while the private key remains to be kept confidential by the receiver. The receiver keeps hold of the key pair initially which is followed by the transmission of the public key. The data to be transferred is encrypted with the public key, which can only be decrypted on the receiver side using the private key known to the receiver alone [Sethuraman *et al.* (2019)].The private key remains to be held by the receiver, greatly facilitating key distribution and management. Some efficient asymmetric encryption algorithms worth mentioning are the Diffie- Hellman Algorithm, Elliptic curve cryptography, El Gamal, Digital Signature Algorithm (DSA) and the Rivest, Shamir. Adleman (RSA) [Gong *et al.* (2019)] algorithm.

Visual cryptography, a cryptographic system based on the human visual system, decrypts the encrypted data using the human vision system [Kumar *et al*. (2021)]. The main task behind this approach is to encrypt text or images into multiple images called shares [Gurunathan (2020)]. When they split up, shares get aligned together to match the transparency found in the sub-pixels, and the original image gets revealed. This scheme was extended to k out of n schemes in which the original message was split to n shares, out of which only k shares will be sufficient for decryption. The availability of k-1 shares cannot guarantee the retrieval of the original image or text. Initially, this method was applied to only grey-scale images, but gradually it began to be used on color images, too [Fatahbeygi (2019)]. The activities of hackers in retrieving highly confidential data on multimedia based applications creates security related concerns towards human life.VC makes the task of intruders complex in retrieving the confidential information. Moreover, to increase the privacy and confidentiality of the transmitted information there is increased demand in making use of encryption algorithms in addition to visual cryptography concept.

The rest of the paper is outlined as follows: Section 2 elaborates an overview of the existing work relevant to the proposed work, the research gap and the objectives of the research work. The methodology used in the proposed work is presented in Section 3 and the experimental results are pictured in section 4 with comparative analysis. Finally section 5 discusses the conclusion and gives suggestions applicable for proceeding future work.

2. Literature Review

Visual cryptography makes use of combinational techniques for encoding images to n shares and then decoding it by simply stacking the shares without the use of any complex or traditional algorithms[Selva Mary (2020)]. The significant approach of visual cryptography aims in transferring the images related to real time applications with high data security and with no compromise in the image quality. This study was implemented to be used in (n,n) scheme and the (k,n) scheme and can be used for real time medical images and important images that requires quick responses. This study elaborated a technique for error abatement using two filtering methodologies that are value discretization based and reduced error based [Abdullah (2020)]. This approach showed PSNR of 21% and reduced mean square error up to 77%. The PSNR value remained as a motivation for selecting the proposed

research work. Old style cryptographic technique costs high in computation in both decryption and encryption. An original image is encrypted into many called as Shares in VC. The original picture is termed as SI which is encrypted using VC methods. Encrypted version of SI is shares. These shares are circulated to many participants. The SI can't be disclosed from only one share. The original image is recovered when these shares are arranged concurrently.

Another study [Wu (2020)] concentrated on Color and normal cryptography scheme and utilized colors in alleviating the problem of pixel expansion. Two constructs were proposed for (k,n) threshold probability related color and normal non-expansible shares that satisfied contrast and security conditions. Evaluation of results showed better performance. This study [Jisha (2020)] concerned both XOR and OR related random grid VC schemes for black and white images. It was for (t,k,n) access structure which is a generalized version of the threshold(k,n) structure where t participants were strictly required for successful recovery of original secret image. This work concentrated on finding the closed representation of light contrasts which was mathematically very challenging problem. In visual cryptography there is very high probability of dishonest shareholders presenting faked shares while reconstructing the original image. This actually results in damage to honest shareholders. To overcome this, the proposed work [Jia *et al.* (2019)] devised a secure approach that verified the cheating shares and achieved fair amount of reconstruction of original secret image. Among the XOR based original shares, an image for verification was also used. This work motivated in using additional algorithms along with the usual visual cryptographic schemes for enhancing data security.

[Li *et al.* (2020)] This study is a variation of the usual (k, n) share VC. The motivation for this is that some of the participants may play important roles than others. So this work proposed a (t, s, k, n) VC scheme with additional information regarding essential participants. The secret original image was shared with essential (s) and non-essential (n-s) shadows out of total n shadows. The researchers had proposed a physical scheme for visual cryptography that required only two shares without demanding a pixel expansion.[Melgar (2019)]. A colored and transparency printed share on polyvinyl chloride base of 3 mm was used as one of the share and colored image that was displayed in a smartphone was used as the alternate share. The method was tested using practical examples and found to produce better results [Kumari *et al.* (2019)] In order to enhance the level of security in visual cryptography, this research combines the Blowfish algorithm with visual cryptography concept. User-friendly, effective and powerful tool for enhanced data security is the crucial need of the hour. In this regard, this research work highlights a block encryption framework using the Hidden Markov model [Ozcan *et al.* (2021)], which made use of three components like initial probability vector, vector for initialization and the substitution box. The rate of encryption was 0.774 Mbits/s and 1.0535 Mbits/s for normal gray-scale images. This was a good encryption rate but which can still be further improved. Cryptography and steganography are the two main techniques that can guarantee secure data transmission. This work [Gambhir (2019)], combines a cryptographic technique, RSA algorithm [Abid *et al.* (2021)] with steganography and DES algorithm with audio and image steganography [Saravanan (2019)].

This study [Zhang *et al.* (2019)], proposed ECC with weak matrix to more cracks for being initiated, retaining high strength, ductility and light weight. It was found that the proposed ECC produced increased tensile strength on addition of light weight-based filter. [Ibrahim *et al.* (2020)] Visual cryptography decomposes images into shares and supports data transmission with added security, thereby generating the decrypted image with a reasonable quality. In spite of all these advantages, these systems also face shortcomings like pixel expansion, poor quality of decrypted images and even high computational complexity. With the aim of overcoming some of these limitations, the proposed work in this study gives a novel 2 out of 2 scheme for secret sharing for color images with the use of dragonfly algorithm. This algorithm helps supporting in the determination of optimal color gradient levels in encryption, generating decrypted images of very high quality. The overall complexity of the data security system was found to be comparatively less.

2.1. *Research Gap*

This research work is proposed with the motivation of overcoming some of the limitations that the literature review have projected.

- Visual cryptographic schemes still needs to address the problem of efficiently encrypting multiple secrets and pixel expansion [Ibrahim *et al.* (2021)].
- Visual cryptography based schemes needs further improvements in optimization of the designing schemes ,algorithms and further applying them in real-time applications [Goon *et al.* (2022)].
- The widespread use of high speed networks and smart devises the threats on data transmission is on the raise and this makes investigators to focus on securing applications related to digital images and data.
- The main drawback of visual cryptographic techniques is that if the split up share happens to be changed or modified by intruders ,the integrity of the reconstructed image cannot be verified [Mary (2019)]. This can be overcome by encrypting the original image and then using the resultant encrypted image for splitting and using it in visual cryptographic schemes.

- Existing schemes based on visual cryptography show witness issues like high computational complexity, pixel expansion and poor quality of decrypted images [Goon (2019)].

2.2. *Objectives*

The main objectives of the EVCN is

- To implement an enhanced data security visual cryptography mechanism for real time applications.
- To implement a secure data transmission scheme for high data confidentiality and integrity
- To improve the PSNR in secured data transfer by integrating two efficient encryption algorithms like DES and ECC. A high signal-to-noise ratio value can guarantee the high quality of images on retrieval on the receiver side.
- To implement a non-expansible data security scheme in which the share images take the same size as that of the secret input image. This reduces the memory requirements and can also generate images of very high quality.

3. Proposed System

The true purpose of the proposed architecture was to implement a novel hybrid approach for efficient encryption and decryption of images concerned with visual cryptography. As part of pre-processing, the images of the selected dataset were resized. The original input image was encrypted using the DES algorithm and then with the ECC algorithm. A hidden text was then added to this encrypted image, and the resultant was then split into two shares. This confidential share was transmitted securely through the internet. On the receiver side, the multiple shares were overlapped, and then the resultant image was subjected to decryption with the ECC and DES algorithm, respectively, to get the original image. The performance of the proposed system was evaluated using the Long Short Term Memory (LSTM) network. Figure 1 shows the architectural framework of the proposed image encryption system.

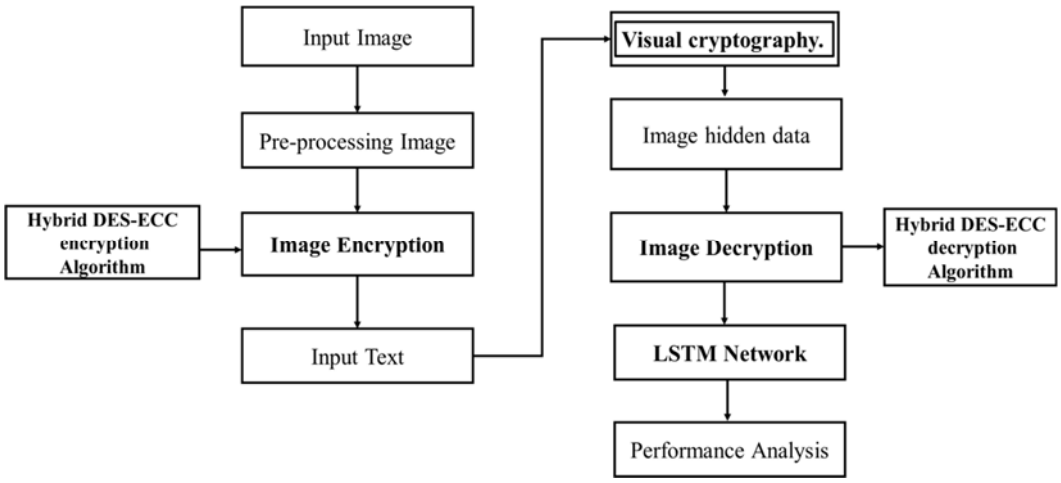

Fig.1. The architecture of the proposed image encryption system using LSTM

3.1. *Dataset Description*

The images from the C4L dataset (512 X 512) were used to evaluate the efficiency of the proposed EVCN. The cameraman image was resized as part of pre-processing and used by the hybrid algorithm for encryption.

3.2. *DES Algorithm*

In the proposed EVCN, the input image is initially encrypted using the DES algorithm. The overall strength of any block cypher is based on the size of the key, the number of iterations or rounds and the ability of the algorithm to protect data against security attacks. DES has shown worldwide acceptance for three decades. It uses a block size of 64 bits and a key of size 64 bits. The working of a DES algorithm is pictured in figure 2. The first step is the initial permutation of the original 64 bits to produce left and right permuted blocks of 32 bits each. This is followed by 16 iterations of encryption using 56 bits of the key. After 16 rounds, the left and the right permuted block are combined again to generate 64-bit cipher text related to the image.
The same algorithm will be used for decrypting the original image from the encoded one but in the reversed form. The initial and final permutations will be reversed along with the sub-key sequence used in the 16 rounds. The outline of the overall operations carried out by the DES algorithm is portrayed in figure 2.

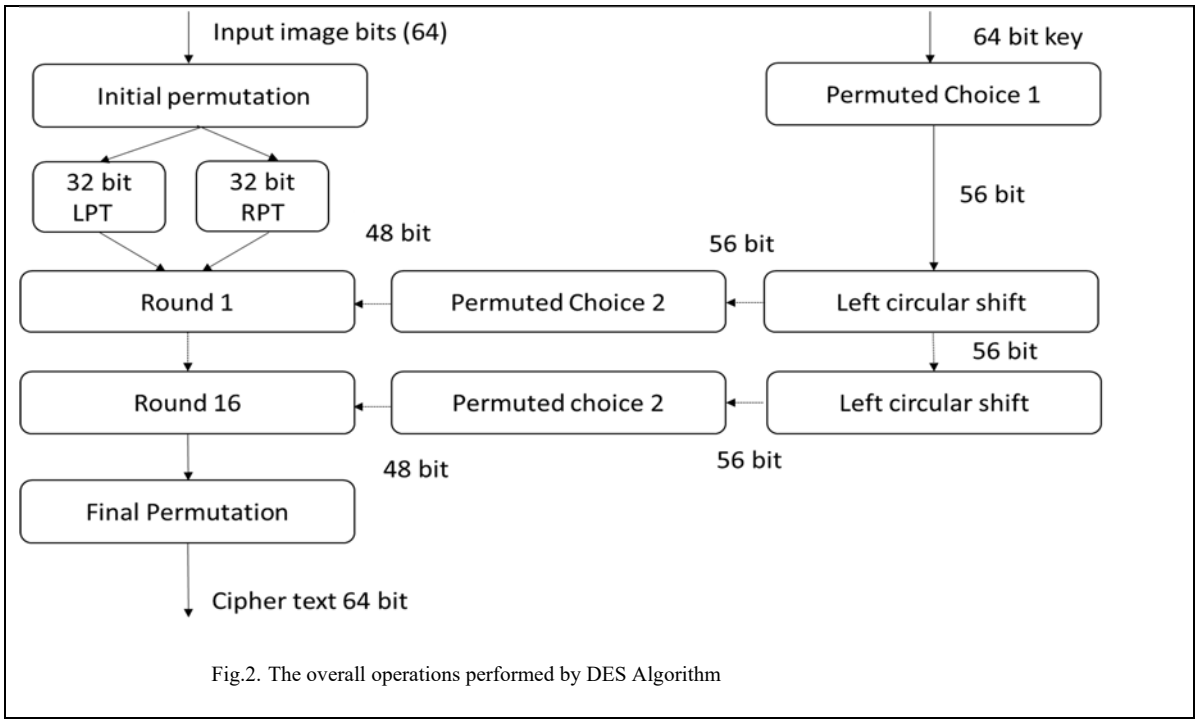

Fig.2. The overall operations performed by DES Algorithm

Each round in the DES algorithm is a combination of the following steps i) key transformation, ii) expansion permutation, iii) S-box substitution followed by iv) p-box substitution, and finally, v)XOR operation and swap.

Key Transformation: The 56-bit key gets split up into two 28 bits keys which are then subjected to left circular shift individually. The number of bits shifted depends on the rounder number. Then both the shifted halves get integrated, and the resultant is permuted to get a 48-bit sub-key, and the process tends to be named compression permutation.

Expansion permutation: Here, the 32-bit left and right permuted halves of the input are processed. The right permuted text (RPT) is expanded to 48 bits, while the left permuted text (LPT) remains the same. Thirty-two bits of the RPT gets split into 4 blocks of 6 bits each. Each 4 bit block gets expanded to 6 bits which yields a resultant 48 bit block on combination. The expanded 48 bit RPT is now XORed with 48 bits of the key followed by passing the result to the S-box.

S-box substitution: The input block which is 48 bit gets divided into eight 6 bit groups. This goes as input to the corresponding eight S boxes which substitutes 4 bits for each 6 bits taken as input with the help of the S-box lookup table.

P-box permutation: The 32 bits retrieved from the s boxes are just permuted in this step and passed by.

XOR and swap: The 32 bits of LPT which remains untouched so far is XORed with the 32 bit output of the P box. This becomes the RPT for the successive round and the previous RTP gets swapped with the LPT. Now the old value of RTP becomes the new LTP that will be used for round that follows. After 16 such rounds the output undergoes a permutation which is the resultant 64 bit value output

3.3. *ECC Algorithm*

ECC is a data encryption technique based on pairs of private and public key. It produces public key based security among key pairs using elliptic curve mathematics. It produces keys which are mathematically difficult to crack being the reason for considering ECC as an efficient algorithm. An elliptic ECC curve is a curve of points over finite field that obeys the equation

$Y^2=X^3 + aX + b$

Private keys of this algorithm are normal integers that fall within the range of the field size of the elliptic curve. It will generally be integers of 256 bits. The ECC algorithm generates keys using the random number synthesis technique. The p key is then calculated using this and thereby supports the creation of the secure cipher text to be transmitted.

The public keys in ECC are generally EC points which is a pair of coordinates {a, b} that lies on the curve. The special properties of EC points allow them to get compressed to a single coordinate plus a single bit that is even or odd. Thus the public key that is compressed, corresponding to ECC private key, which is 256 bits, is an integer that is 257 bits. The overall working of the ECC algorithm in generating the cipher text is elaborated on in detail.

Algorithm for ECC

ENCRYPTION:

1. Let 'Mesg' be the source message.
Consider 'Mesg' as having the point 'M_{11}' on the ECC curve.
2 .Let '$K1_{ran}$' be the n random number we have that is
Taken within (1 to (n-1)).
3.'$p1_{curv}$' is the point found on the ECC curve.

Choose the private key as '$d1_{priv}$ to be in the range of selected 'n.'
4. Calculate the public key.'$Q1_{pub}$' =$d1_{priv} * p1$.
Cipher texts get generated which is '$C_{11} and\ C_{22}$.

$$\boldsymbol{C_{11} = k1_{ran} * p1_{curv}}$$
$$\boldsymbol{C_{22} = M_{11} + (K_{1rand} * Q1_{pub})}$$

DECRYPTION:

The original message 'Mesg' needs to be retrieved

$$\boldsymbol{M_{11} = \left(\left(M_{11} + K1_{rand} * Q1_{pub}\right)\right) - (\, d1_{priv} * (K1_{ran} * P1_{curv}))}$$
$$\boldsymbol{M_{11} = C_{22} - \left(d1_{priv} * C_{11}\right)}$$

'M_{11}' is the required original message needed to be retrieved.

In the given algorithm, Mesg is the source message that we have send which is having the point M_{11}on the curve. The random number chosen is $K1_{ran}$ is the n random number that we have chosen .$P1_{curv}$ is the point on the curve and then we chose the private key to be $d1_{priv}$ within the range n. The public key $Q1_{pub}$ is then calculated as

$$\boldsymbol{'Q1_{pub}' = d1_{priv} * p1.} \quad (1)$$

This will yield the cipher text C_{11} and C_{22} which is calculated as

$$\boldsymbol{C_{11} = k1_{ran} * p1_{curv}} \quad (2)$$
$$\boldsymbol{C_{22} = M_{11} + (K_{1rand} * Q1_{pub})} \quad (3)$$

On the decryption side, the original text is retrieved as M_{11} which is given as

$$\boldsymbol{M_{11} = \left(\left(M_{11} + K1_{rand} * Q1_{pub}\right)\right) - (\, d1_{priv} * (K1_{ran} * P1_{curv}))} \quad (4)$$

$$\boldsymbol{M_{11} = C_{22} - \left(d1_{priv} * C_{11}\right)} \quad (5)$$

This guarantees the generation of the original text on the receiver side.

3.4. *Combined DES and ECC Algorithm*

The novel algorithm for the combined DES and ECC generates more data security when used in visual cryptography which is highlighted as the prime novelty of this research work.

Key expansion algorithm
Input: Key_i- input key given for expansion K_i -output expanded key n- number of rounds **Algorithm**: for i= 0 to n $K_i \leftarrow key_{4i} + key_{4i+1} + + key_{4i+2} = key_{4i+3}$ If (i mod4 $\neq$0) $k_i \leftarrow k_{i-1} \oplus K_{i-4}$ Subword(rotword(k_i-1))

The novel key expansion algorithm takes the key key_i as input key to be expanded and generates the expanded key Ki using the equation

$$K_i \leftarrow key_{4i} + key_{4i+1} + + key_{4i+2} = key_{4i+3} \quad (6)$$

3.5. *Encryption Algorithm (DES and ECC Combined)*

The algorithm for encryption of the original image by the combined DES and ECC is elaborated which takes the original image as input and generates encrypted image.

Encryption algorithm (Combined DES-64 and ECC)
Input: S_e -DES encryption key Input_block- Input image block for the combined algorithm **Output:** Output_block – output image block of DES algorithm Encryption function (input_block [16], output_block [16]) encrypt(input_block , S_e) $S_e \leftarrow$addroundkey(S_e, input_block[0..n]) $\sum_{round=1}^{10} S_e \leftarrow subbytes(s), S_e \leftarrow shiftrows(s)$ If (round$\neq$0), $S_e \leftarrow$mixcolumn(S_e) $S_e \leftarrow$ addroundkey (S_e, k[4 x round, 4 x round +3]) encrypt(S_e, output_block) **Encryption algorithm ECC** **Input:** Output_block – input for ECC encryption S_c- key for ECC encryption **Output:** Output_block- output encrypted image block. Encryption function encrypt (s_c, output_block[16]) encrypt (input_block, s_c)

S_{c_i}←addroundkey (s_c, input_block [0...n])

$$\sum_{\text{round}=1}^{10} \text{Sc}_i \leftarrow \text{subbytes}(s_{c_i}), \text{Sce} \leftarrow \text{shiftrows}(s_{c_i})$$

If (round≠0), Sc_i ←mixcolumn (S_e)$key_{cc} = \sum_{round=1}^{10} Sc_i * \text{Se}$

s_{c_i} ←addroundkey (s_{c_i}, key_{cc} [4 x round, 4 x round +3])
Encrypt (s_{c_i}, output block)

The algorithm for encryption and decryption of the image using the combined approaches for DES and ECC takes the image block input_block as input using the key S_e .the equation for key generation is given as

$$\sum_{\text{round}=1}^{10} \text{Se} \leftarrow \text{subbytes(s)}, \text{Se} \leftarrow \text{shiftrows(s)} \quad (7)$$

The key gets multiplied with the columns in the image using the following equation and generates the encrypted image block which is then passed to the ECC algorithm for encryption.

S_e ← addroundkey (S_e, k [4 x round, 4 x round +3]) (8)

The ECC algorithm takes the image data in the array output_block as input and encrypts it further. The public key S_{ci} is used by this algorithm for key generation in each round using the equation given as

s_{c_i}←addroundkey (s_c, k [0...n]) (9)

$$\sum_{\text{round}=1}^{10} \text{S}_{ci} \leftarrow \text{subbytes}(s_{c_i}), \text{Sce} \leftarrow \text{shiftrows}(s_{c_i}) \quad (10)$$

The combined key key_{cc} for final encryption is generated as

$$key_{cc} = \sum_{round=1}^{10} Sc_i * \text{Se} \quad (11)$$

The encrypted image is then generated using the equation

s_{c_i} ←addroundkey (s_{c_i}, key_{cc} [4 x round, 4 x round +3]) (12)

3.6. *Decryption Algorithm (DES and ECC Combined)*

The decryption algorithm takes the combined shares of visual cryptography as input and gives the original decrypted image.

Decryption algorithm (combined ECC and DES Algorithm)

Input:

Output_block[16]-encrypted image

S_{cid} – decryption key

Output:

Output_block[16] –the output of ECC decrypted message

Decryption function ($s_{c_{id}}$, output_block[16])

Decrypt (input_block, $s_{c_{id}}$)

$s_{c_{id}}$←addroundkey ($s_{c_{id}}$, output_block [0...n])

$\sum_{round=1}^{10}$ Sd ← inv_subbytes$(s_{c_{id}})$, $s_{c_{id}}$ ← inv_shiftrows$(s_{c_{id}})$

If (invround≠0), $s_{c_{id}}$←mixcolumn ($s_{c_{id}}$)

$ECC_{c_{id}}$ ←addroundkey ($s_{c_{id}}$, k [4 x invround, 4 x invround +3])

Decrypt ($ECC_{c_{id}}$,output_block)

Decryption algorithm DES-64

Decryption function ($ECC_{c_{id}}$,output_block[16])

decrypt(input_block,S_{ed})

S_{ed}←addroundkey(S_{ed}, output_block [0..n])

$\sum_{round=1}^{10} S_{ed} \leftarrow$ inv_subbytes(S_{ed}), $S_{ed} \leftarrow$ inv_shiftrows(S_{ed})

If (invround≠0), S_{ed} ←mixcolumn(S_{ed})

S_{ed}←addroundkey(S_{ed},k[4 x invround, 4 x invround +3])

decrypt(S_{ed},output_block)

The round key S_{cid} for decryption is generated using the equation

$$S_{c_{id}} \leftarrow \text{addroundkey}\ (s_{c_{id}}, \text{output\_block}\ [0...n]) \quad (12)$$

The inverse of the key used for encryption is used for decryption. This key S_{ed} is generated using the equation

$$\sum_{round=1}^{10} S_{ed} \leftarrow \text{inv\_subbytes}(s_{c_{id}}), s_{c_{id}} \leftarrow \text{inv\_shiftrows}(s_{c_{id}}) \quad (13)$$

$$ECC_{c_{id}} \leftarrow \text{addroundkey}\ (s_{c_{id}}, k\ [4 \text{ x invround}, 4 \text{ x invround} +3]) \quad (14)$$

The reverse of encryption operation is carried out in the decryption side which is given by the equation Where ECC_{cid} Is the resultant image key. The key for decryption using the DES is given by the equation

$$S_{ed} \leftarrow \text{addroundkey}\ (S_{ed}, \text{output\_block}\ [0..n]) \quad (15)$$

$$\sum_{round=1}^{10} S_{ed} \leftarrow \text{inv\_subbytes}(S_{ed}), S_{ed} \leftarrow \text{inv\_shiftrows}(S_{ed}) \quad (16)$$

The decrypted image retrieved is the original image with the the expected quality as that of the original image.

3.7. *Visual Cryptography*

Without any prior understanding of cryptography and computational work, Visual Cryptography Scheme (VCS) permitted to decrypt images. Using the VCS's hidden image sharing, the original image was partitioned to relevant and meaningless shares. The shares were circulated between participants and the original hidden image was retrieved by assembling the shares using the human visual system through decryption. Diverse methods of VC were created primarily for binary images which were then improved to steer color or gray scale images. The secret picture was separated and concealed in distinct image during encryption, making it hard to find the secret data. Until the shares are differentiated it's puzzling and difficult to comprehend. Retrieving the secret data was attainable when the shares were collected and positioned consecutively. Hidden sharing assisted in dispersing of dissimilar shares among different persons and ensured that only legalized person had the access to them. The individuality and advantage of VC than other secret methods was which required extremely few computational works.

3.8. *LSTM for Evaluation*

LSTM is a recurrent unit which is capable of remembering past knowledge seen by the network so far and can forget data that is irrelevant. This is achieved by the introduction of various layers of activation function named gates for different activities. Each unit of LSTM network maintains the internal cell state (ISC) vector that conceptually gives description about the chosen information selected for retaining by the preceding LSTM unit. LSTM constitute four different gates, each for dedicated purpose.

Forget gate (f): This gate is to determine the extent to which the network has to forget previous data.
Input gate (i): This gate determines the extent to which the network has to write the information on to the internal cell state.
Input modulation gate (g): This is probably a sub-part of input gate used in modulation of the data that will be written on to the ISC by the input gate. This is done on the addition of non-linearity with the information and converting the information to zero-mean. As zero-mean information converges faster, it reduces the learning time.
Output gate (o): This gate is to determine the output to be generated from each internal cell state to the succeeding hidden state.

The workflow of a LSTM network is same as that of a recurrent neural network and varies from it in the sense that , in addition to the hidden state being passed forward, the ICS also gets forwarded.

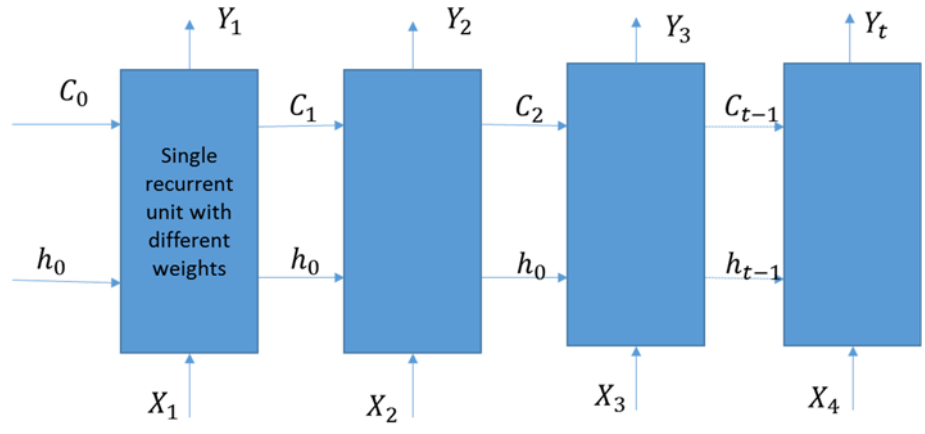

Fig.3. LSTM –Architecture

The architecture of LSTM is shown in figure 3. C_0, C_1, C_2 are the current states and h_0 ,h_1 ,h_2 are the hidden states.X_1,X_2,X_3 are the inputs and Y_1,Y_2,Y_3 are the corresponding outputs to the LSTM network. The algorithm used to evaluate the accuracy of the EVCN is given below

LSTM Algorithm
For the given $P1_i$ =the value 1 to P1 To generate the subset $P1_i$, Step 1: Attain Q bootstrapped instances out of the entire training set. Step 2: Half the number of variables is randomly chosen. The individual LSTM network is trained For the $P1_i$ the LSTM classifier, FP1i is trained. A prediction is made. The outcome with the expected score $soc_k \sim (P1_i)$is predicted for given input End.

The network takes the current values of the input, the initial hidden state and the internal cell state as the inputs for each stage and then calculates the values for the available four gates. For every gate, parameterized vectors of the preceding hidden state and current input are calculated as the element-wise multiplication of the corresponding vector with respective weights. The activation function of every gate is applied on parameterized vectors element-wise. Then CIS is calculated by element-wise vector multiplication of input and modulation gate and preceding ICS and forget gate. Both the vectors are then added. The present hidden state is then calculated by taking the hyperbolic tangent of the CIS vector and multiplying it with the output gate. Like the Recurrent neural networks, the LSTM also produces output at each stage which is used in training the network with the gradient descent. The LSTM network was used for evaluating the performance. The decrypted image was taken as the input by LSTM, and the similarity between the decrypted and the input image in terms of accuracy was calculated.

4. Results and Discussions

The proposed EVCN was evaluated using real-time data, and the results were used in analyzing the performance of the EVCN.

4.1. *Input Image*

To evaluate the performance of the EVCN, the image shown in figure 4 was used, and the results were analyzed. The cameraman image was used for analyzing the proposed EVCN in real-time.

Fig.4. Input image used by the EVCN for encryption

4.2. *Encrypted Image Generated By DES and ECC*

The input image was initially encrypted using the combined DES and the ECC algorithm that disclosed no information about the input image.

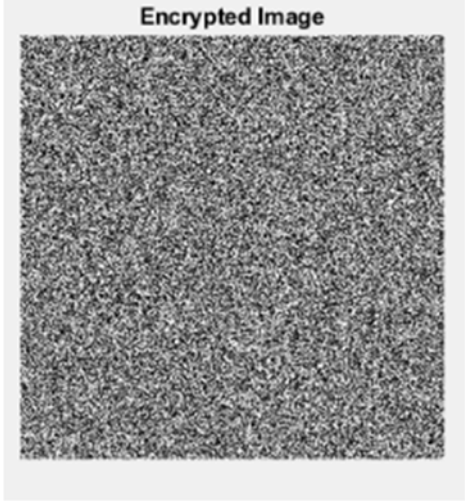

Fig.5. Image after encryption by the DES and ECC

The input image, after being resized, was processed by the combined DES and ECC algorithm and the combination yielded the encrypted image shown in figure 5. This step guarantees added data security with the use of two effective algorithms. These images did not show any information related to the input. This was an added advantage that helped to attain high confidentiality of the data transmission.

4.3. *Visual Cryptography Shares*

Visual cryptography aims to split the images into shares so that it discloses no information about the original image. It is an efficient image transfer approach that can guarantee secured data transfer.

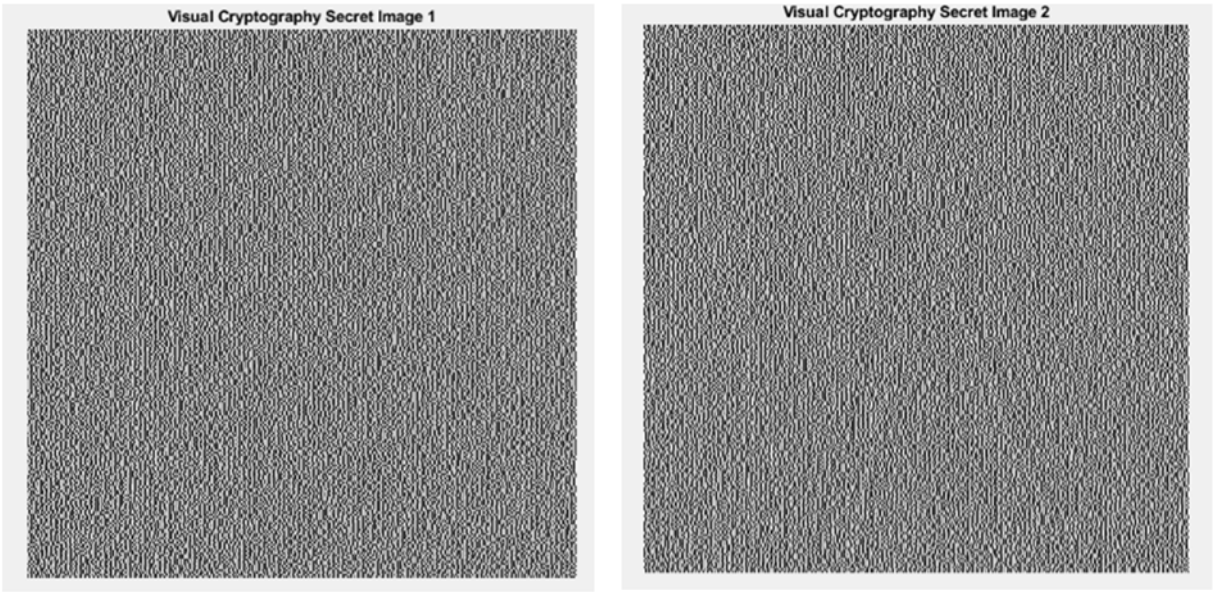

Fig 6: Image of share1 and share two generated by EVCN

The image shown in figure 6 is the representation of shares 1 and 2 of the original encrypted image. The image was encrypted using a combined DES and ECC algorithm. On further addition of a hidden text, the resultant was subjected to VC.

4.4. *Decrypted Image*

The confidential image data transferred through transmission channels on the receiver side needs proper handling for decrypting the same using the private key share.

Fig 7: Original Cameraman image(2017) after decryption using EVCN

The image in figure 7 is the original image retrieved after decryption using the EVCN on using the key pair from the DES and ECC algorithms. The input image and the received output image were compared using the LSTM network. The results of comparison showed that the decrypted image on the receiver side was of very high quality and showed a comparison accuracy of 99%.

4.5. *Performance Evaluation of the EVCN*

Least Mean Square Error (LMSE): This measures the cumulative squared error between the original image and the compressed image. This represents the minimum possible error value if the image is scaled concerning intensity.

Peak Signal to Noise Ratio (PSNR): This metric measures the ratio of the maximum value of the signal and the amount of distorting added noise that adversely affects the representation quality of the image.

Bit Error Rate (BER): This metric measures the ratio between the counts of available bit errors to the count of the bits transferred.

Universal Quality Index (AQI): This metric highlights the image quality using correlation loss contrast-related and luminance distortions.

Normalized Cross-Correlation (NCC): The value of this metric is given by the inverse convolution of the Fourier transform of the images normalized with local sums and sigmas.

Contrast to Noise Ratio (CNR): Before calculating the PSNR, a term gets subtracted and yields CNR in the presence of bias in the image.

Root Mean Square Error (RMSE): This term is used to measure the error difference between the segmented and the source message. Smaller values of RMSE show better performance.

Metrics	Values
PSNR	52.9073
LMSE	0.0017
BER	0.3329
UQI	0
NCC	0.9967
CNR	1.4859
RMSE	0.5770

Table 1: Performance analysis of the proposed EVCN

Table 1 shows the values of the performance metrics of EVCN with PSNR value of 52.9073, LMSE value of 0.0017, BER of 0.3329, UQI value 0, NCC value 0.9967, CRR 1.4859 and RMSE value 0.5770.

4.6. *Performance Metrics for LSTM*

The proposed EVCN was tested for accuracy, recall, precision, sensitivity, specificity and F1Score as metrics using the LSTM network.

Accuracy: Accuracy gives a measure of the model's efficiency, which is calculated as the ratio of the count of predictions made correctly to the count of the total number of predictions.

$$\text{Accuracy}=\frac{TP+TN}{TP+TN+FP+FN} \quad (17)$$

Where,

TP – True Positive
TN- True Negative
FP- False Positive
FN-False Negative

Precision: Precision is the ratio of the count of outcomes that are correctly predicted s positive to the total of the predictions that are correctly predicted as positive and the ones that are wrongly predicted to be positive.

$$\text{Precision}=\frac{TP}{TP+FP} \quad (18)$$

Recall: This metric reveals the model's ability to detect positive instances. It is the ratio between the total numbers of predictions that are correctly detected as positive to the count of all available positive samples.

$$\text{Recall}=\frac{\boldsymbol{TP}}{\boldsymbol{TP+FN}} \quad (19)$$

Sensitivity: Sensitivity gives a measure of the efficiency of a model in predicting positive instances, also termed the rate of true positivity.

$$\text{Sensitivity}=\frac{\boldsymbol{TP}}{\boldsymbol{TP+FN}} \quad (20)$$

Specificity: This metric measures negative samples that are correctly predicted. It is the ratio of true negative samples and the sum of true negative and false-positive samples**.**

$$\textbf{Specificity}=\frac{\boldsymbol{TN}}{\boldsymbol{TN+FP}} \quad (21)$$

F1-Score: The F1 Score is the weighted average of precision and recall.

$$\textbf{F1 Score}=\frac{2*(recall*precision)}{(recall+precision)} \quad (22)$$

Metrics	Values
Accuracy	98
Sensitivity	92
Specificity	93
Precision	92
Recall	98
F-score	94.96

Table 2: LSTM Performance

The results of testing the proposed EVCN showed an accuracy of 98%, recall of 98%, precision of 92%, the sensitivity of 92%, specificity of 93% and F1 score of 94.96%.

Algorithm	Precision	Recall	F-score	Accuracy
CVC Algorithm	0.82	0.79	0.55	0.67
Siamese network	0.7	0.75	0.5	0.69
Hybrid Approach	0.95	0.93	0.94	0.93
LSTM	0.97	0.98	0.99	0.99

Table 3: Comparison of LSTM performance [Mohan (2021)]

Table 3 compares the performance of the LSTM that was used for evaluating the results. When other networks were used for real-time evaluation, it was found that expected accuracy was not generated. The EVCN generated an accuracy of 0.99, a precision of 0.9, a recall of 0.98 and an F-Score of 0.99.

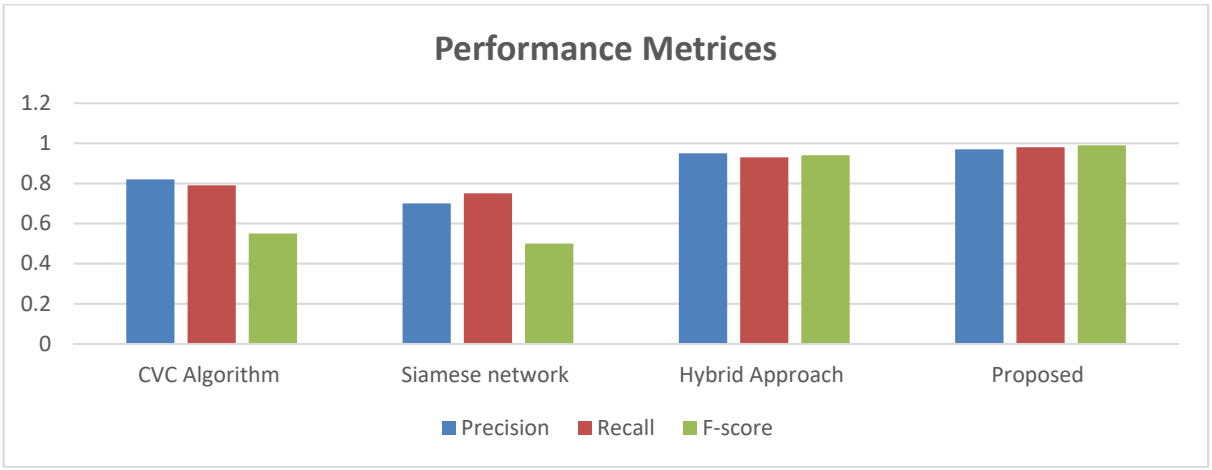

Fig 8: comparing evaluation performance of EVCN with other approaches.

The comparison of evaluation of performance is depicted in figure 8, which concludes that the EVCN outperforms the other existing models in performance evaluation.

5. Conclusion

A secret image can securely be transmitted with the EVCN using the proposed hybrid algorithm without information loss. Encryption of the original data and its decryption is made as complex as possible by integrating two effective algorithms that can improve data security against statistical and differential attacks. The proposed hybrid algorithm can be used for images of any high dimension. The work can competently be used in transmitting confidential medical images, spatial images, geographic maps, military information, satellite image-based applications and many more. The effective approach that is proposed takes less amount of time to be implemented and tested, which is an added advantage. This enables the system to be used in many real-time applications. Further, the same approach can be extended and enhanced to the general (k,n) –EVCN with additional security features. Future work can also concentrate on sharing multiple secret images simultaneously.

References

[1] Abdullah R. and Fakieh B. (2020), "Health care employees' perceptions of the use of artificial intelligence applications: survey study," Journal of medical Internet research, vol. 22, p. e17620.
[2] Abid R., Iwendi C., Javed A. R., Rizwan M., Jalil Z., Anajemba J. H., et al. (2021), "An optimised homomorphic CRT-RSA algorithm for secure and efficient communication," Personal and Ubiquitous Computing, pp. 1-14.
[3] Abroshan H. (2021), "A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms," International Journal of Advanced Computer Science and Applications, vol. 12.
[4] Alaya B. and Sellami L. (2021), "Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban VANET networks," Journal of Information Security and Applications, vol. 58, p. 102779 .
[5] Basavaiah J., Anthony A. A., and Patil C. M. (2021), "Visual Cryptography Using Hill Cipher and Advanced Hill Cipher Techniques," in Advances in VLSI, Signal Processing, Power Electronics, IoT, Communication and Embedded Systems, ed: Springer, pp. 429-443.
[6] Fatahbeygi A. and Tab F. A. (2019), "A highly robust and secure image watermarking based on classification and visual cryptography," Journal of information security and applications, vol. 45, pp. 71-78.
[7] Gambhir A. and Arya R. (2019), "Performance analysis and implementation of DES algorithm and RSA algorithm with image and audio steganography techniques," in Computing, Communication and Signal Processing, ed: Springer, pp. 1021-1028.
[8] Gong L., Qiu K., Deng C., and Zhou N. (2019), "An optical image compression and encryption scheme based on compressive sensing and RSA algorithm," Optics and Lasers in Engineering, vol. 121, pp. 169-180.
[9] Goon S (2019) Major developments in visual cryptography. Int J Eng Adv Technol, 9(1S6), pp 81–88.
[10] Goon, S., Pal, D. & Dihidar, S. (2022). "Primary Color Based Numerous Image Creation in Visual Cryptography with the Help of Grasshopper Algorithm, Artificial Neural Network and Elliptic Curve Cryptography". Journal of Computer Science, 18(5), 322-338. https://doi.org/10.3844/jcssp.2022.322.338
[11] Gurunathan K. and Rajagopalan S. (2020), "A stegano-visual cryptography technique for multimedia security," Multimedia Tools and Applications, vol. 79, pp. 3893-3911.
[12] Hao X., Ren W., Xiong R., Zhu T., and Choo K.-K. R. (2021), "Asymmetric cryptographic functions based on generative adversarial neural networks for Internet of Things," Future Generation Computer Systems, vol. 124, pp. 243-253.
[13] Ibrahim D. R., Abdullah R., and The J. S. (2020), "An enhanced color visual cryptography scheme based on the binary dragonfly algorithm," International Journal of Computers and Applications, pp. 1-10.
[14] Ibrahim D. R., The J. S., and Abdullah R. (2021), "An overview of visual cryptography techniques," Multimedia Tools and Applications, vol. 80, pp. 31927-31952.
[15] Jadhav S. P. (2019), "Towards light weight cryptography schemes for resource constraint devices in IoT," Journal of Mobile Multimedia, pp. 91–110-91–110.
[16] Jia X., Wang D., Chu Q., and Chen Z. (2019), "An efficient XOR-based verifiable visual cryptographic scheme," Multimedia Tools and Applications, vol. 78, pp. 8207-8223.
[17] Jisha T. and Monoth T.,(2020) "Recent Research Advances in Black and White Visual Cryptography Schemes," Soft Computing for Problem Solving, pp. 479-49.
[18] Kalimuthu S., Naït-Abdesselam F., and Jaishankar B. (2021), "Multimedia Data Protection Using Hybridized Crystal Payload Algorithm With Chicken Swarm Optimization," in Multidisciplinary Approach to Modern Digital Steganography, ed: IGI Global, pp. 235-257.
[19] Kumar M., Aggarwal J., Rani A., Stephan T., Shankar A., and Mirjalili S., (2021), "Secure video communication using firefly optimization and visual cryptography," Artificial Intelligence Review, pp. 1-21.
[20] Kumari P., Kaur A., and Kaur S., "Security Enhancement of Visual Cryptography Using Blowfish Algorithm."
[21] Li P., Yin L., and Ma J. (2020), "Visual cryptography scheme with essential participants," Mathematics, vol. 8, p. 838.
[22] Mansoor K., Ghani A., Chaudhry S. A., Shamshirband S., Ghayyur S. A. K., and Mosavi A. (2019), "Securing IoT-based RFID systems: A robust authentication protocol using symmetric cryptography," Sensors, vol. 19, p. 4752.
[23] Mary G. S. and Kumar S. M. (2019), "A self-verifiable computational visual cryptographic protocol for secure two-dimensional image communication," Measurement Science and Technology, vol. 30, p. 125404.
[24] Melgar M. E. V. and Farias M. C. (2019), "A (2, 2) XOR-based visual cryptography scheme without pixel expansion," Journal of Visual Communication and Image Representation, vol. 63, p. 102592.
[25] Mohan J. and Rajesh R. (2021), "Enhancing home security through visual cryptography," Microprocessors and Microsystems, vol. 80, p. 103355.
[26] On alternatives to Lenna, Journal of Modern Optics (2017), 64:12, 1119-1120, DOI: 10.1080/09500340.2016.1270881.
[27] Özcan H., Gülağiz F. K., Altuncu M. A., İlkin S., and Şahin S. (2021), "A New Visual Cryptography Method Based on the Profile Hidden Markov Model," Advances in Electrical and Computer Engineering, vol. 21, pp. 21-36.
[28] Palevicius A., Janusas G., Ragulskis M., Palevicius P., and Sodah A.,(2018), "Design, analysis and application of dynamic visual cryptography for visual inspection of biomedical systems," in Nanostructured materials for the detection of CBRN, ed: Springer, pp. 223-232.
[29] Rathee G., Sharma A., Saini H., Kumar R., and Iqbal R. (2020), "A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology," Multimedia Tools and Applications, vol. 79, pp. 9711-9733.
[30] Saravanan M. and Priya A. (2019), "An algorithm for security enhancement in image transmission using steganography," Journal of the Institute of Electronics and Computer, vol. 1, pp. 1-8.

[31] Selva Mary G. and Manoj Kumar S., (2020), "Secure grayscale image communication using significant visual cryptography scheme in real time applications," Multimedia Tools and Applications, vol. 79, pp. 10363-10382.
[32] Sethuraman P., Tamizharasan P., and Arputharaj K., (2019), "Fuzzy genetic elliptic curve Diffie Hellman algorithm for secured communication in networks," Wireless Personal Communications, vol. 105, pp. 993-1007.
[33] Vodnala S., Majumdar S., and Nath P. K. (2021), "Region of Interest-Based Encryption of Biomedical Image," in Data Intelligence and Cognitive Informatics, ed: Springer, pp. 851-861.
[34] Wu X. and Yang C.-N. (2020), "Probabilistic color visual cryptography schemes for black and white secret images," Journal of Visual Communication and Image Representation, vol. 70, p. 102793.
[35] Zhang Z., Yuvaraj A., Di J., and Qian S. (2019), "Matrix design of light weight, high strength, high ductility ECC," Construction and Building Materials, vol. 210, pp. 188-197.

Authors Profile

Surajit Goon is presently doing his PhD in Computer Science & Engineering at Brainware University, Barasat, WB, India. He works in Eminent College of Management & Technology, Barasat, WB, India as assistant professor since 2016. He got his M.Tech degree in Computer Science & Engineering from BIT, Mesra, India and M.C.A. from B.P.U.T, India. His research interest includes Image Processing, Network Security and Visual Cryptography

Debdutta Pal is currently working as associate professor in Brainware University, Barasat .She had been an associate professor in Calcutta Institute of Engineering and Management, Kolkata, India, since February 2017. She joined academia as assistant professor in the same institute in 2008. Debdutta completed her PhD from University of Calcutta in 2014. She has been associated with organising many conference in India as member of Technical Program Committee. She has supervised two granted project for undergraduate students. She has published more than 20 research papers in reputed journal and peer reviewed conference proceedings. She has also contributed chapters in a book published by CRC press in 2013. She has authored one text book. Her research interest is on Adhoc Network and it's Security. She is a professional member of Institute of Engineers (India).

Souvik Dihidar received his B.Tech degree in Electronics and Electrical Communication Engineering from Indian Institute of Technology, Kharagpur. He got his M.S. and Ph.D. degrees in Electrical and Computer Engineering from Georgia Institute of Technology, Atlanta, USA. He worked for Marvell Semiconductor in Santa Clara, California in the area of Wireless Communications. He is currently with Eminent College of Management and Technology, Barasat, where he is an Associate Professor in the Computer Science Department. His research interests include error control coding, digital signal processing, and cryptography.