Image Transmission Secretly by means of Symmetric Key, Encryption, Visual Cryptography And Steganography

[1]Mrs. Shalaka Dange, [2]Prof. R. M. Mukhedkar
[1]M.E.Student, [2]HOD
Department of E&Tc Engineering
Dr. D.Y.Patil college of Engineering,Ambi, Pune,India.

***Abstract*— The data security is a very important issue nowadays. Confidential data, financial documents, military information, secret data etc. is transmitted on the Internet. Internet is the primary source to transmit such secure information. In such cases, many techniques are involved to transmit data securely such as Encryption with the key, visual cryptography, Steganography. These techniques devoted to protect such kind of information and they play an important role in providing confidential and secure transmission over network. In this paper, we are suggesting one new method in which the symmetric secret key is used to encrypt the image and then cipher image is produced. Divide this cipher image into different unique parts and apply Novel secret sharing algorithm of steganography. Each unique part will conceal by another innocent image i.e. steganography. Use of secret key will ensure the security of scheme. At the receiver side among n parts only k (threshold) parts or greater than k parts are needed to reconstruct the original secret image.**

***Keywords*—Visual cryptography, symmetric key, Secret sharing steganography**

I. Introduction

Among all popular communication network Internet plays very vital role. Where the distribution of secret data, military information, financial documents, authorized documents, multimedia content etc. has become a regular task. As most of human being using internet to transmit the secret information many user can see the secret information. Hence, now it is very important to provide security or confidentiality to the visual information which is available on the internet. So, to satisfy such an increasing demand of security, many security providing tools are available. Visual cryptography is one of them which are introduced by Naor & Shamir in 1979 to provide security and confidentiality. This technique is mostly used when visual information is transmitted on the unsecure, untrusty communication channel. Adi Shamir and G. Blakley proposed concept of secret sharing .In which secret image is encrypted using a key and encrypted image is divided into n different unique parts. These parts are transmitted over a internet or any unsecure channel. The unsecure channel means where multiple user can see any visual information. So these shares are transmitted on such unsecure channel and after stacking of all these parts the information can revealed otherwise not. In 1983 one new method of secret sharing was proposed by Asmuth-Bloom named Asmuth-Bloom secret sharing scheme which is based on Chinese Remainder theorem. There are many methods to protect data and Steganography is also one of them.Steganography technique hides secret information under the innocent cover such as image, audio, video etc. Accordingly steganography technique falls under different categories like image steganography, text steganography, video steganography etc. But, flaw of this technique is that all secret information is kept under only one cover medium and if this cover medium get lost or corrupted then there are chances that hidden data may get lost or corrupted. Lin and Tsai proposed a method in 2004, in that Steganography was used to hide meaningful shares of secret image in image sharing concept. In this scheme polynomial-based secret sharing approach is used which is proposed by Shamir, it leads to high computational complexity. In the decryption process human visual system approach is used. Secret information can be retrieved by anyone who will get at least k number shares of image among n shares. Hence visual cryptography is also became insecure to transmit secure data. So, in this paper a new idea is suggested which provides extra security and confidentiality to the secure information. In this new method, encryption is done with the help of symmetric key and then cipher image is created which is divided into different unique parts. These unique parts are concealed under another innocent image i.e. steganography. Novel secret sharing algorithm of steganography is used.

II. Previous work

Some of visual cryptography schemes described in the previous papers are as follows. Previously, in 1979 Shamir and Naor proposed a secret sharing approach. Shamir proposed the secret sharing approach which is based on Langrange’s interpolation theorem. According to these scheme secret data can be divided into n number of shares share1, share2 , . . . share n. Secret data image is divided into n number of shares share1, share2……share n and these shares are distributed among n users, one for each user. So to reconstruct the original image at least k share is required. Less than k shares are not able to reconstruct the secret image. This technique is called (k, n) threshold secret sharing. As among n number shares threshold value k number is fixed by programmer here. Blakley Secret sharing scheme proposed a sharing approach based on hyper plane geometry. As non-parallel planes intersect at one single specific point, this secret sharing scheme says that: i) In m-dimensional space secret is a single point. ii) Share corresponds to a hyper plane. iii) Secret is intersection point of threshold plane. iv) Less than threshold planes will not reveal secret [1].

Asmuth-Bloom stated the secret sharing scheme in which shares are created on the basis of Chinese Remainder theorem. Reduction modulo operation is used to create shares and the secret is recovered by solving the system of congruence using the Chinese Remainder Theorem. In past few years visual cryptography was restricted to binary images and because of this; it became inefficient in real time applications. So, Chang- ChouLin, Wen-Hsiang Tsai proposed visual cryptography for gray level images by dithering techniques. This technique converts gray level images into approximate binary images. Then to generate shares existing visual cryptography schemes is applied for binary images. The limitation in this is that all generated shares are random patterns, look like noisy images.

El-Tigani B. Abdelsatir, Sahar Salahaldeen proposed a new encryption algorithm restricted to grayscale images based on (k,n) threshold secret sharing . Quadratic residues theorem is used for encryption. In the proposed scheme, the pixels of the secret image are first permuted and then encrypted by using quadratic residues. Then the encrypted image is shared into n shadow images using polynomials of Shamir scheme. In Shamir secret sharing scheme the secret partition is done by the following polynomial [2].

$$F(x_i) = y + m_1.x_i + m_2.x_i^2 + \cdots + m_{(k-1).}x_i^{(k-1)}.mod(p)$$

. . . . equation (1)

where y is the secret share S1, p is a prime number and the coefficients of the k-1 degree polynomial m_i are chosen randomly and then the shares are evaluated as S1=F(1), S2 = F(2).......Sn=F(n).

Given any k pairs of the share pairs (i, Si), where i=1,2,3.....k we can obtain the coefficients m_i of F(x) by Lagrange interpolation as follows:

$$S=(-1)^{(k-1)}\begin{bmatrix} F(x_1).\frac{(x_2)(x_3).....(x_k)}{(x_1-x_2)(x_1-x_3).......(x_1-x_k)} + F(x_2).\frac{(x_1)(x_3)......(x_k)}{(x_2-x_1)(x_2-x_3).......(x_2-x_k)} + \\ .....F(x_k).\frac{(x_1)(x_2).....(x_{(k-1)})}{(x_k-x_1)(x_k-x_2)......(x_k-x_{(k-1)})} \\ \end{bmatrix}$$

. .. . equation (2)

Pallavi Vijay Chavan and Dr. Mohammad Atique proposed Novel idea of hierarchical visual cryptography. Visual cryptography encrypts secret information into two pieces called as shares. These two shares are stacked together by logical XOR operation to reveal the original secret [3].

III. PROPOSED CONCEPT

There are three possible approaches with it we can transmit our secret information : first is hiding the secret data under another media like text, image, audio, video, this method is called as steganography, second is encrypt the secret data with the help of key and third is divide the secret data in different parts and then transmit that parts. After receiving all parts original information can be opened. This technique is called visual cryptography. These three major approaches can be combined. When any image is encrypted with the key or if image is divided into parts the image which is produced after process contained noise. So this image looks noisy or textured image. By watching this image carefully any unauthorized person will get know about the hidden information. And he will try to get information and if he fails then maybe he will try to destroy or damage it .So to overcome such problems, steganography can be used as it hides all the information under innocent cover image. If incase that image get corrupted or lost then there is huge possibility that all the secret hidden information may get lost or corrupted. To avoid such a problem one new approach is stated in this paper which reduces chances of hiding all the information under single cover and also provides no harm to quality of image. Objective of proposed scheme is to design an encryption/decryption algorithm that efficiently provides high level security for visual information from illicit attacks.

A. Encryption Process:

The encryption process involved in our proposed scheme is as shown in Fig.1. At first step secret image is read and then in second step symmetric key is generated. By using this key secret image which is read in first step is encrypted in this third step. The output of this step is cipher image. In the next step cipher image is divided into parts. Suppose cipher image is divided into n number of shares. These shares are concealed with the help of another image this method is called steganography. After masking of these shares, are transmitted to the receiver side. Advantage of this combined version of two schemes is that key encryption before secret sharing of image will give additional security and use of steganography in secret sharing can provide additional security as it befools the attacker's eye without computational overhead.

B. Secret Sharing of the Encrypted Image:

The input for this step is encrypted image i.e. cipher image. If cipher image is seen by the attacker then he may come to know that this is encrypted image and something is hidden behind it and he will try to achieve that information. So, to deal with such cases this proposed scheme uses the steganography technique to hide cipher image. Cipher image is divided into different shares and different masks are to be generated for different shares. Cipher image share is hidden under the mask.

a) Algorithm for designing the masks for n shares with threshold k:

1. The value of n and k is entered by the user and then matrix is formed of dimension nCk-1 × n by listing all row vectors of size n having the combination of (k-1) numbers of 0's and (nCk+1) numbers of 1's.

2. The matrix generated in step-I is transposed to perform further operations. Each row of this matrix will represent the individual mask for n different shares. Thus the size of each mask is nCk-1 bits, i.e. the size of the mask varies with the value of n and k. Now, use each row of this matrix for generation the corresponding share.

3. The shares of cipher image are masked by different mask pattern. The bits corresponding to 1 in the mask are kept as it is and the bits corresponding to 0 in the mask are replaced by 0.

4. Select a pixel (say A) from cover image consisting of three bytes for RGB values from the corresponding cover image then insert eight bits of masked byte (say B) into pixel After repeating these steps with all other mask patterns other stego share images will produced. So, finally Shares of key encrypted Cipher Image covered with innocent covers will be created by above mentioned algorithms and they will be ready to send to intended receiver.

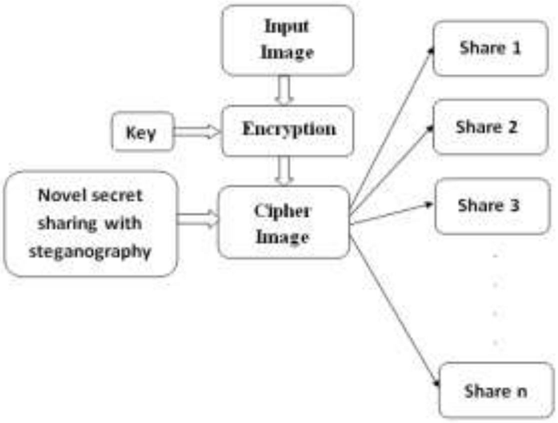

Fig 1. Encryption process

C. Decryption Process:

At the receiver side at least k number of stego share images has to be stacked to reconstruct the original secret image. The fig. 2 shows process of decryption.

a). Extraction of share bytes from stego share images:

Input: k number of stego share images

Output: Recovered Cipher Image.

Step I: First select any k or more no of stego share images. Select the corresponding pixel and extract the share bytes Bi where i= 1, 2, k from the selected k stego share images.

Step II: Perform OR operation between these k extracted share bytes we get the corresponding secret byte.

Step III: Repeat Steps with all pixels of k stego images to get back the secret image of dimension n*m. Finally, the original lossless Cipher Image will get recovered by this algorithm**.**

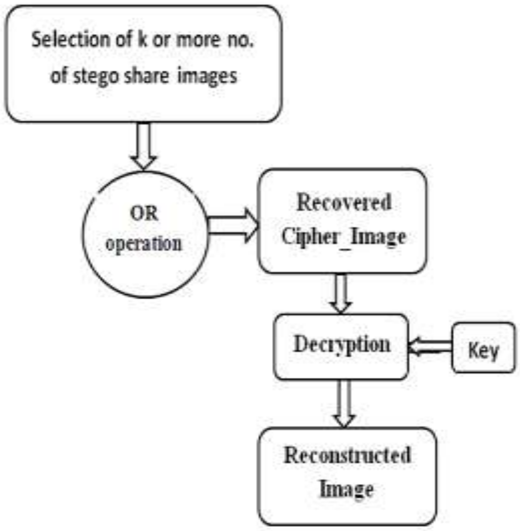

Fig.2. Decryption Process

b) Decryption using key:

Input: Recovered Cipher image, Symmetric Key

Output: Original secret image

Step I: The input taken is cipher image and symmetric key is generated again for decryption process. This retrieves Final Key array back.

Step II: Perform XOR operation in between recovered Cipher Image pixel array and Final Key array. By this finally we will get the original secret image at receiver side.

IV. EXPERIMENTAL RESULT

As per proposed scheme, in encryption process, the original secret image is treated with symmetric key in first step. Leena.png is used as test image for verifying productivity of algorithm. Input to encryption can be any secret image either gray scale, bitmap or color image. For example we considered Leena image of dimension 150x150 as shown below in Fig.3 for conducting experiments. We consider block size of 4x2 and temp value of 0.5155 for key generation. After performing bitwise XOR operation between input secret image i.e. leena.png in our experiment and generated key the output Cipher Image is as shown below in Fig.4. For evaluating results we had done bitwise XOR between Cipher image and Key array at this phase of encryption process. By this we got original secret image back. These algorithms are implemented by using MATLAB R2010a software. Now in the next step, stego shares are created after applying Novel secret sharing algorithm with steganography as like shown below. In decryption process, get the value of no. of shares (n) and threshold (k) as input from user. Then after this perform operations as per the algorithm discussed in section III to get Cipher Image. Output of this step is recovered Cipher Image which will be like this as shown below in Fig.4

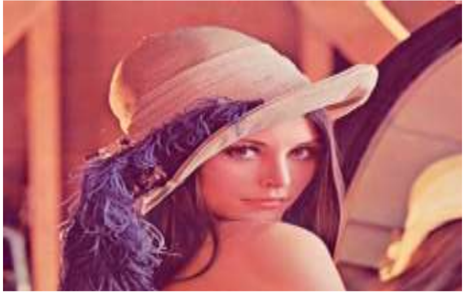

Fig 3. Input secret image

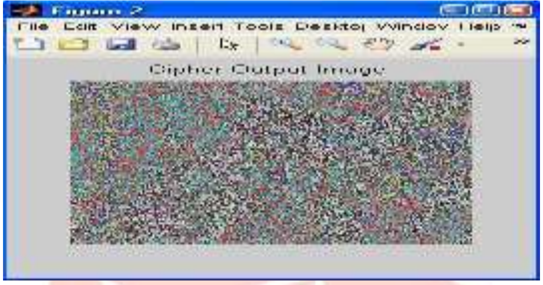

Fig 4. Cipher image

For e.g. consider, No. of shares created n=4. For example, stego share images that will be created can be like these as shown below (see Fig 5 to Fig.8). These images are the example of Stego share images that will be output of Encryption process and will be given as input to decryption process.

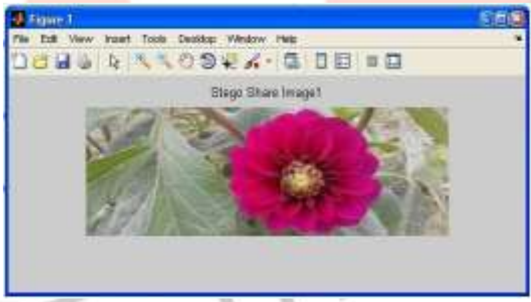

Fig 5. Stego share image 1

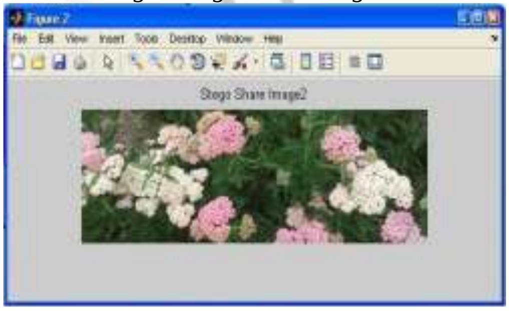

Fig.6 Stego share image 2

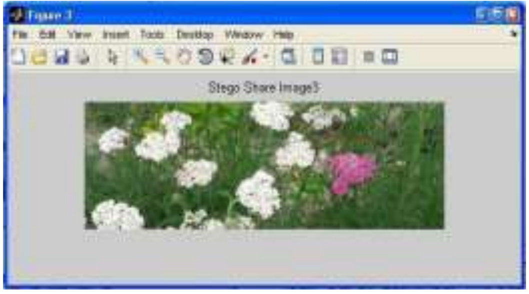

Fig 7 Stego share image 3

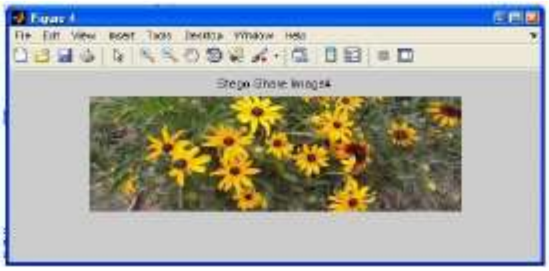

Fig 8. Stego share image4

Now, consider, at this stage, take input data from user for Example: Minimum No. of shares required (threshold) =3, Shares inputted: Share1, Share3, and Share4. Then, Reconstructed Cipher Image from shares will be like this as shown in Fig.9. Now, final step of decryption will be decryption with key. Generate the key and then after performing XOR operation between recovered Cipher image pixel values and final key array we will get original secret image as shown in fig.10

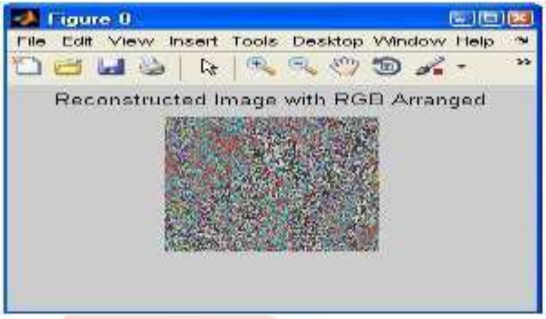
File Edit View Insert Tools Desktop Window Help
Reconstructed Image with RGB Arranged

Fig 9: Recovered cipher image

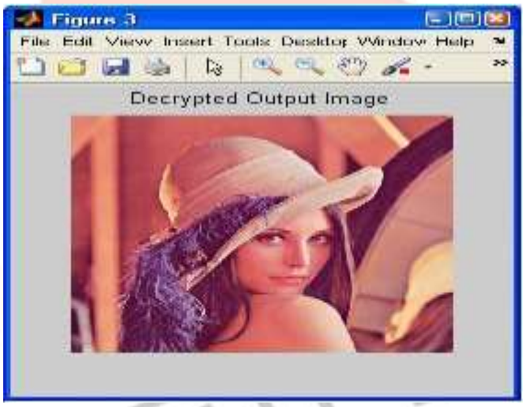

Fig 10: Recovered secret image

V. CONCLUSION

Visual Cryptography is an exciting area of research where exists a lot of scope. We have proposed a new method for visual cryptography different from any other previous schemes. In this new proposed scheme, use of Symmetric key is suggested in first level of encryption process of secret image which will offer additional security. And then we used novel secret sharing with steganography for the creation of shares of this encrypted image which will be meaningful shares instead of having noise like shares. So, because of meaningful shares implicit attack chances are reduced. To best of our knowledge this scheme can be a very effective solution in providing security to secret images from illicit attacks. Use of secret key makes it more secure and reliable.

ACKNOWLEDGMENT

The authors gratefully acknowledge all those who have helped in making of this review paper successfully. As, this review process of this paper was carried out at Dr. D. Y. Patil COE, Ambi, Pune. So, special thanks to Head of E&TC Department, Principal and Management.

REFERENCES

1. Shamir, “How to share a secret,” Proc. Comm. ACM, vol (2), 612-613, 1979.
2. El-Tigani B. Abdelsatir, Sahar Salahaldeen, Hyam Omar and Afra Hashim, “ A novel secret sharing scheme from quadratic residues for grayscale images ” , International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.4, J.uly 2014.

3. Pallavi Vijay Chavan, Dr. Mohammad Atique and Dr. Latesh Malik , “Design and Implementation of Hierarchical Visual Cryptography with Expansionless Shares”, International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.
4. Ilker Nadi Bozkurt, Kamer Kaya, Ali Aydın Selcuk, Ahmet M. Guloglu, “Threshold Cryptography Based on Blakley Secret Sharing”.
5. Kamer Kaya , Ali Aydın Sel ̧cuk, Zahir Tezcan,, “Threshold Cryptography Based on Asmuth-Bloom Secret Sharing”.
6. John Justin.M , Alagendran.B , Manimurugan.S ,“A Survey on Various Visual Secret Sharing Schemes with an Application”, International Journal of Computer Applications (0975 – 8887) Volume 41– No.18, March 2012.
7. Shanu Sharma,” An Implementation of a Novel Secret Image Sharing Algorithm”, IJCSMC, Vol. 2, Issue. 4, April 2013, pg.263 – 268.
8. Harinandan Tunga and Soumen Mukherjee,” Design and Implementation of a Novel Authentication Algorithm for Fool-Proof Lock-Key System Based On Steganography and Key based Visual Cryptography using Novel secret sharing method Visual Secret Sharing Scheme”, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012.
9. Nayan A. Ardak Prof. Avinash Wadhe,” Visual Cryptography Scheme for Privacy Protection”, Nayan A. Ardak et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 2026- 2029.
10. Poonam Bidgar, Neha Shahare,” Key based Visual Cryptography Scheme using Novel Secret Sharing Technique with Steganography”, IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) eISSN: 2278- 2834,p- ISSN: 2278-8735.Volume 8, Issue 2 (Nov. - Dec.2013), PP 11-18
11. Sonam Soni,”, A Road Map to Visual Cryptography, Volume 5, Issue 4, 2015 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.