ENHANCING SECURITY BY APPLYING LSB STEGANOGRAPHY AND HYBRID CRYPTOGRAPHY FOR IMAGE TRANSMISSION

[1]M.J. Bheda,[2]Prof.Amita Shah
[1]M.E. Student,[2]Assistant Professor,
[1,2]Department of Computer Engineering
[1,2]L.D. College of engineering, Ahmedabad-380015, India

Abstract:* In this aeon, with the quick improvement of numerous multimedia technologies thousands of multimedia information are created and transmitted within the Government Agencies (CID, FBI), research organization, E-commerce and military fields, medical, so they want to secure such applications are increased. Due to the development in the field of multimedia applications, every minute thousands of messages which can be images, text, videos, audios are created and transmitted over a communication network, So Security of image and video data has become increasingly important. To ensure the security of image transmission, people have proposed many security algorithms using steganography, cryptography, and visual cryptography. Secret information can be secured using steganography which is data hiding method. We have proposed an improved LSB technique to incorporate large data here. Encryption technique is integrated with steganography technique to give added security. Symmetric encryption uses shared secret key but secrecy can be compromised as keys may be intercepted or listened over a medium. To deal with this issue, Elliptic Curve Cryptography (ECC), an asymmetric key encryption method is used which is secure with smaller keys for the same level of security, especially at high levels of security. To give a deeper level of security and randomness to process, Visual Cryptography is used which scramble a secret image into n meaningless shares of the image. So proposed approach will Increase data hiding capacity and Enhancing security with improving the visual quality of image for transmitting it over the public communication channel.

***Index Terms* - LSB, Visual cryptography, ECC, HVS**

I. Introduction

A tremendous development in the field of multimedia technologies has taken place in recent decades [11]. Due to the popularity of smart phones, android applications, as well as the rapid growth and extensive internet availability, acquisition, manipulation and communication of digital images has been effectively used in this cybernetic world. Consequently, information security and confidentiality has become a fundamental and important communication requirement.
We use digital data such as images,videos, texts,audios in our daily lives with the rapid development of the Internet and multimedia techniques. Large information can be transmitted via computer networks. However, the security of many information on the web is not up to date or to the mark, and the information can be capturing by an unlawful or unauthorized user. Subsequently guaranteeing the Security and Secrecy of information transmission is exceptionally imperative and current need. This necessity can be accomplished by distinctive methods like Steganography and Cryptography.

In the area of digital data security, there are two domains namely information hiding and cryptography. Information hiding deals with steganography. Steganography is the scientific discipline of inconspicuous communication by concealing information in some other media. It refers to the process of hiding the presence of the secret message. It is an art of covert writing. It does not keep the message secret but it provides the secrecy of the message. Steganography hides a secret message from the third party. It does not arouse an eavesdropper's attention. According to Dictionary.com- "Steganography is hiding a secret message within a larger one in such a way that others cannot discern the presence or contents of the hidden message" [18]. The Steganography term is deducted from the Greek words “stegos” implying “cover” and “grafia” implying “writing” and literally means “Cover writing” [18]. Cryptography is an effective approach for secure communications which is an art of writing in the form of secret codes. Hence, the method of cryptography becomes vital for any secured communication over an untrustworthy medium such as the web. The strategy of cryptography preserves information from burglary and modification as well as gives user authentication. Within the event that anyone ought to talk about safely with somebody else at that point, they utilize the cryptography. there are two sorts In cryptography: (a) symmetric key cryptography (b) Asymmetric key cryptography. Sender and receiver both are sharing the same secret key In symmetric key cryptography. Firstly sender encodes the data or message by utilizing key and encryption calculation at that point send to the beneficiary. A receiver will get the message or information and unscramble by utilizing the same key and decoding algorithm. There are many symmetric cryptographic algorithms are as: DES, 3DES, Twofish, Blowfish, RC2, RC5, RC4, AES, CAST5, IDEA, TEA. In asymmetric key cryptography, two different keys are used to encrypt and decrypt the message i.e. a public key and private key. For the process of encryption public key and encryption algorithm used, an output of this encryption process is called as ciphertext and these cipher text sends over the network to the receiver. A receiver will receive the ciphertext and decrypt it by using the decryption algorithm and private key [1]. Here, a sender using the public key of receiver and receiver using his private key for the encryption and decryption process. There are various asymmetric key algorithms as: RSA, Digital Signature, Diffie- Hellman, Elgamal key, ECDSA, and ECC. The study methods for decoding cipher messages is called as cryptanalysis and methods for recognizing hidden messages within the stego-media is called as steganalysis. The former pertains to the set of methodologies to acquire the meaning of encrypted information, whereas the latter is the art of uncovering secretive messages [1]. In the area of digital data security, Shamir proposed the most widely used cryptographic approach so as to share the input (sophisticated) images, based on visual secret sharing (VSS) scheme and another algorithm was introduced by Naor and Shamir [24] known as visual cryptography (VC). Visual cryptography algorithm encodes the secret data in order to generate different meaningless shares and then distributing them to a receiver. Finally, all generated shares are stacked up in order to recover the secret image. Because of speedy decoding or recovering properties and perfect cipher, VC method has drawn the attention towards research. The visual cryptographic scheme is extensively employed for secure transmission of sophisticated images and passwords in military, intelligence, E-bill and tax payments, confidential video conferencing, medical imaging system, and internet banking [22]. This paper is focusing on a strategy for combining together cryptography and steganography for images.

This paper is organized into five sections. Section I gives the introduction of this paper. Section II shows the survey of different existing methods of cryptography, steganography and visual cryptography. Section III explains the proposed modified least significant bit steganography method. Section IV, V show elliptic curve cryptography and visual cryptography respectively. Section VI shows the proposed flow and algorithm. Section VII shows the implementation and results. Finally, section VIII gives the conclusion of this paper.

II. Literature Review

In the case of steganography, cryptography and visual cryptography, different methods are performed. Improvements can be made after a survey of such existing methods in these existing strategies.

An algorithm has been proposed in [18] to exchange the data between sender and receiver using variable block size symmetric encryption algorithm which is content based. This method performs xoring between ASCII value of information and key which is generated using the folding method. The resultant value is again xored with the length of text information. In the second phase, encrypted text is hidden behind an image to give more security using raster scan steganography. The experiments show that the encryption approach is capable of effectively fulfilling the image encryption by drawing the best parameters to achieve the best effect of image encryption. For encrypted security, this proposed method has a strong sensitivity to the three - digit key that can break under various key combinations using the brute force method.

In [19] dual layer for the security of data is given, The first layer is to encrypt data using the AES encryption algorithm and then encrypt the key used for encryption using RSA.After dividing data into ' n ' blocks and embedding it into ' n ' images using LSB. Then the random nature in which the image is sent increases the chaos factor further. The first layer is done by encrypting data using the AES encryption algorithm and then encrypting the key used for the encryption using RSA. After that divide data in to ‘n' block and embed them in ‘n' images using LSB. Then further increasing the chaos factor by the random nature in which the image is sent. The three layers may increase the time to send the data, but potentially increases the time needed to decrypt the information. The method proposed is much more efficient than the LSB method standard.

This paper [23] introduced new visual cryptography for a color image by proposing a special table for initial permutation as well as initial inverse permutation to increase diffusion. Then divide the plain image into blocks, each block represents share; These operations result in nine shares. after that apply the encryption algorithm like RSA & Elgamal, Some shares encrypted with RSA and others encrypted with Elgamal, creating multiple shares to increase image security during network transfer.

Authors in [24] proposed randomized visual secret sharing which utilizes block-based progressive visual secret sharing and discrete cosine transform (DCT) based reversible data embedding technique to recover a secret image. The method of recovery is based on incremental visual secret sharing, which recovers block by block the secret image. The proposed scheme accomplishes a contrast level of 70–90% for noise-like and 70–80% for meaningful shares. Experimental results appeared that the proposed scheme reestablishes the secret image with better visual quality in terms of human visual system based parameters.

Author has proposed [21] progressive visual cryptography in which it creates nine number of shares of a secret image. Progressive Visual Cryptography (PVC) means recovering the secret image progressively by superimposing the n shares of a specific secret image. The structure of the scheme is given to make n shares of any secret image. This structure of the scheme may give matrices for sharing that give the idea of how a secret image can be distributed among n shares. With the help of determination of various types of pixels the watermark embedding technique is implemented in this paper after finding the prediction error using those pixels. For both color and grayscale images, this visual cryptography scheme with watermark embedding technique works.

In [20] dual layer for the security of data is given, the first layer is done by scrambling information utilizing the Blowfish encryption algorithm and after that scrambled information is partitioned into ‘n' pieces. After that ‘n' piece information is embedded in ‘n' images utilizing LSB. The proposed algorithm takes somewhat more time to execute as three extra features are included to the algorithm specifically: encryption utilizing Blowfish algorithm, breaking of blocks and information of a hash table. The proposed algorithm, since it uses more images, uses lesser information per image than the standard LSB and subsequently gives a better PSNR value per image, which means the viewer will discover it harder to distinguish even more than the standard LSB.

In [26], In this system, SHA2 is one of the strongest hash function technique which generate a 256-bit string of registered user data. This 256-bit string is then embedded into an image using the LSB data hiding technique. Two shares of this image are created using (2,2) visual cryptography algorithm. votes are encrypted by AES encryption algorithm to provide the security. AES encryption algorithm is faster so, encryption is done in minimum time. So, it saves time and improves the performance of the system.

In [25], a novel approach is proposed for multimedia data security by integrating Steganography and Visual Cryptography. The proposed method contains two phases. The first phase, by changing the number of bits hidden in RGB channels based on the indicator value, dynamically hides the message in a Cover Image 1.VC schemes conceal the Cover Image2 into two or more images which are called shares. In the second phase, two shares are created from a Cover Image2 and the stego image created in the first phase is hidden in these two shares. The shares are safe as they reveal nothing about the multimedia content. The Cover Image2, stego image, and the hidden message can be recovered from the shares without including any complex computation. More amount of data can be transmitted by increasing the number of VC shares.

In this paper[22], the author has proposed a highly secured visual cryptography scheme which uses AES encryption algorithms and error diffusion halftoning technique as intermediate steps in cryptography work. In the first step create the shares of halftone images of each channel and after that AES encryption is applied to protect the shares from malware exercises which can alter the bit arrangements to create the unauthenticated shares.

According to the literature survey, the steganography methods incorporated the data hiding techniques that provide less embedding capacity. Next, the extraction of the secret data from stego-media does not ensure 100 percent recovery of the secret data. The combined techniques of steganography and cryptography use traditional encryption algorithms with a shared secret key which may compromise the secrecy of multimedia data over communication channel if shared secret key listened over an unsecured communication channel. All these challenges solved by implementing a proposed approach which protects data from hackers.

III. Modified least significant bit steganography algorithm

In modified least significant bit steganography algorithm, XOR operation is performed between 4-4-4Least Significant Bits of the cover image and bits of the secret image. Resultant values of XORing are replaced in cover image bits. With the use of a modified steganography method, no one can get original secret image bits from cover image bits.

Cover image bits: 10011101 11101110 01110010 01111111
Secret image bits: 0011 0011 0111 0010
LSB substitution: 1001110**0** 1110111**0** 0111001**1** 0111111**1**
XOR LSB substitution: 1001**0101** 1110**1101** 0111**0101** 0111**1101**

IV. ECC Asymmetric encryption algorithm

Elliptic Curve Cryptography (ECC), public key cryptography is developed by Victor Miller and Neal Koblitz independently in the year 1985. Elliptic Curve Cryptography provides higher security with smaller key size if it will be compared with other asymmetric encryption algorithms. Elliptic Curve Cryptography 160-bits offers an equivalent level of security to information as RSA 1024-bit does. High level of security is achieved using a small key size. In Elliptic Curve Cryptography, we will be using the curve equation of the form [33]:

$$y2 \bmod P = x3 + ax + b \bmod P \qquad (1)$$

$$\text{with } 4a3 + 27b2 \neq 0.$$

Where a and b are the constant and P is prime. Here the elements of the finite field are integers between 0 and p – 1. All the operations such as addition, subtraction, division, multiplication involve integers between 0 and p – 1.

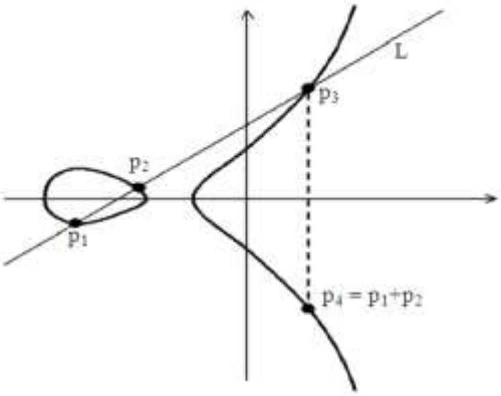


Figure 1: Graph of Elliptic curve[1]

To encrypt a message, sender and receiver chose an elliptic curve and took an affine point (G) that lies on the curve. Plaintext M is encoded into a point P_M. Sender chose a random prime integer x and Receiver chose a random prime integer y. x and y are sender and Receiver's private keys, respectively. To generate the public key, sender computes (2) and receiver computes (3).

$$Pa = xG \quad (2)$$

$$Pb = yG \quad (3)$$

To encrypt a message point P_M for Receiver, Sender chooses another random integer k and computes the encrypted message P_C using the Receiver's public key (P_B). P_C is a pair of points (4):

$$P_C = [(kG), (P_M + k\,P_B)] \quad (4)$$

Sender Sends the encrypted message P_C to Receiver. He receives the ciphered message and multiplying his private key, y, with kG and subtract it from the second point in the encrypted message to compute P_M. The result corresponds to the plaintext message M (5):

$$P_M = (P_M + k\,P_B) - [ykG\,] \quad (5)$$

The strength of an ECC-based cryptosystem depends on the difficulty of finding the number of times *G* is added to itself to get Pa. the cryptographic strength of elliptic curve encryption lies in the difficulty for a cryptanalyst to determine the secret random number *k* from *k*P and P itself.

V. Visual cryptography

Visual cryptography, introduced by Naor and Shamir in 1995, is a cryptographic scheme based on the human visual system. Visual Cryptography doesn't require complex mathematical algorithms to encrypt and decrypt data. The main idea of this approach is to encrypt any message (text, image, etc..) into a number of different images called shares. Only, when the shares are overlapped together in order to match the transparency among the subpixels, the secret message can be seen and recovered. One of the simplest implementations of this approach is the 2 out of 2 sharing scheme, where the message to be encrypted is divided into 2 shares using exclusive or operation where both shares needed for a successful decryption. However, even if only one share is present, no information about the message can be revealed. When cryptanalysis of the above schemes is considered, the divisions or shares exist in unencrypted form during the transmission and retrieval over a connected network. However, a man in the middle attack cannot predict the secret message with a single share, but if the attackers are able to grab all the available shares, there is a possibility of recovering the plain text by using certain normal brute force attacks [10].

Algorithm for visual cryptography:

1. Input the image with a secret image.
2. Initialize two collections of n x m Boolean matrices S0 and S1. S0 acts as a pool of matrices from which to randomly choose matrix S to represent a white pixel while S1 acts as a pool of matrices from which to randomly choose matrix S to represent a black pixel.
3. Using the permutated basis matrices, each pixel from the secret image will be encoded into two sub pixels on each participant's share. The secret image with black pixel will be converted on the ith participant's share as the ith row of matrix S1, where a 1 represents a black sub pixel and a 0 represents a white sub pixel. Similarly, The secret image with white pixel will be converted on the ith participant's share as the ith row of matrix S0.
4. Stacking the entire qualified participant's shares to reconstruct the secret image.

VI. Proposed methodology

This system provides an enhanced blend of image steganography along with cryptography. This method proposes modified LSB technique for color image steganography which enhances the data hiding capacity of cover image and uses elliptic curve cryptography for encryption of stego-image after that to give more randomness in pixel values and dipper level of security, visual cryptography is used which creates two shares of the encrypted image. The block diagram for the proposed method is shown in figure(2).

The proposed system has subsequent six modules (three at the sender and three at the receiver):

1. Stegano Encoding using modified LSB steganography
2. ECC encryption
3. share generation using visual cryptography
4. share merging in visual cryptography
5. ECC decryption
6. Stegano Decoding

In the first module, the 24-bit cover image is chosen and split into three planes: Red, Green, and Blue. 24-bit Secret image is taken. In the module, secret image is embedded in a cover image using 4-4-4 data hiding technique of modified least significant bit steganography. Bits of a secret image are xored with 4-4-4 least significant bits of cover image and a resultant value stored in cover image 4-4-4 least significant bits. In the second module, the stego image is encrypted using elliptic curve cryptography asymmetric encryption technique which uses receivers public key to generate an encrypted image. ECC's main advantage is that you can use smaller keys for the same level of security, especially at high levels of security (AES-256 ~ ECC-512 ~ RSA-15424). In the third module, To give dipper level of security, shares of an encrypted image are generated using (2,2) visual cryptography technique. With a single share, any intruder cannot get secret information. Shares of the secret image are then transmitted from sender to receiver. In the fourth module, receiver overlap shares of the secret image using (2,2) visual cryptography technique. In the fifth module, decrypt secret encrypted image using receivers private key using elliptic curve cryptography decryption process. In the sixth module, Secret image extracted from the cover image using a modified lest significant bit steganography method.

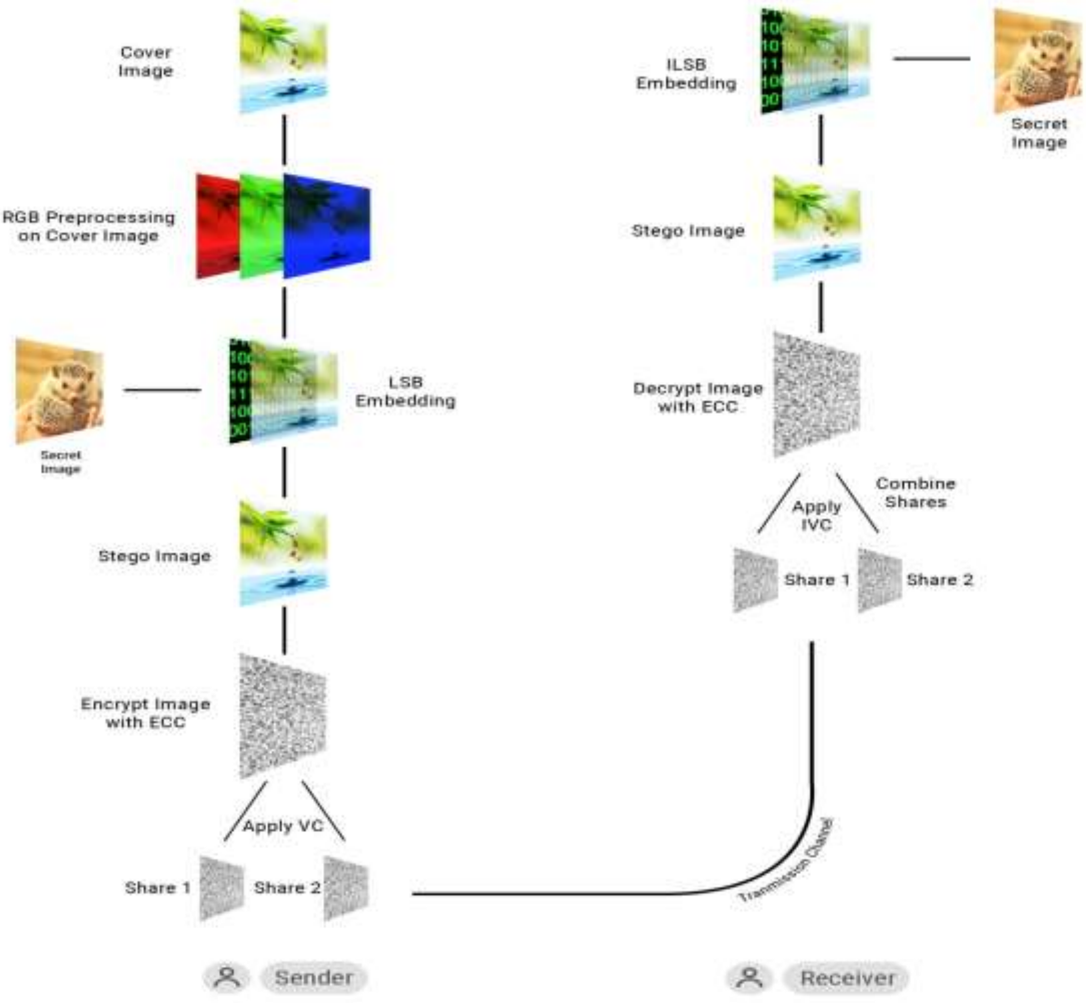


Figure 2: Block diagram of the proposed system

VII. Implementation and Results

The simulation has been done in MATLAB 2018a using a variety of images and the results of 4 images have been represented here. Both cover image and secret image are of a color image. The images are taken from SIPI database [32]. The Mean Square Error, Peak Signal to Noise Ratio and hiding capacity are the parameters used for the proposed technique. These two parameters (MSE and PSNR) are basically error matrices to compare the original cover image with the output Stego image. The third parameter hiding capacity is the size of the data in a cover image that can be modified without deteriorating the integrity of the cover image.

1) Mean Square Error

MSE measured the error between the original and Stego image [18].

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j)-g(i,j)\|^2 \qquad (6)$$

Where **f** represents the matrix data of our cover image, **g** represents the matrix data of our degraded image in question, **m** represents the numbers of rows of pixels of the images and I represent the index of that row, **n** represents the number of columns of pixels of the image and **j** represents the index of that column. In Steganography low value of MSE required so output image looks similar to the input image.

2) Peak Signal to Noise Ratio

It is defined as the ratio between the maximum possible power of a signal and the power of corrupting noise. It is the ratio of peak square value of pixels by mean square error (MSE). It is expressed in decibel (db) [18]. The PSNR is defined as:

$$PSNR = 20 \log_{10} (((\max (f)) / ((MSE) \hat{}0.5)) \qquad (7)$$

Where, **max(f)** represents the maximum value of a pixel of the image that exists in our original "known to be good" image.

MSE measures error between original and stego image; it computes a positive value from o to 1.

3) Data hiding capacity

It is the size of the data in a cover image that can be modified without deteriorating the integrity of the cover image.

The below table(1) shows PSNR value calculation of cover image and stego image for the proposed algorithm and existing algorithm; this is done using Matlab 2018a.

Sr. No.	Input size (Image Size, Secret Size)	An output of the Existing Method	An output of the proposed method (Average)
1	512 X 512, 2 KB	69.70	71.04
2	512 X 512, 20 KB	67.07	69.77
3	512 X 512, 200KB	65.11	67.19
4	512 X 512, 280 KB	64.58	65.72

Table 1: PSNR value calculation

The below table(2) shows MSE value calculation of cover image and stego image for the proposed algorithm and existing algorithm; this is done using Matlab 2018a.

Sr. No.	Input size (Image Size, Secret Size)	An output of the Existing Method	An output of the proposed method (Average)
1	512 X 512, 2 KB	0.0069	0.0051
2	512 X 512, 20 KB	0.0128	0.0068
3	512 X 512, 200KB	0.0200	0.0124
4	512 X 512, 280 KB	0.0226	0.0174

Table 2: MSE value calculation

Following are the images before and after the execution of the proposed algorithm. As can be seen, the difference is not visually perceptible. However, the image on the right i.e. 3(b) contains data that has been embedded in it using the modified Least Significant Bit Algorithm. On further experimenting, the PSNR value can be found out to be different. This, however, is something not visible to the naked eye, which in turn tells us about the entire efficiency of steganography.

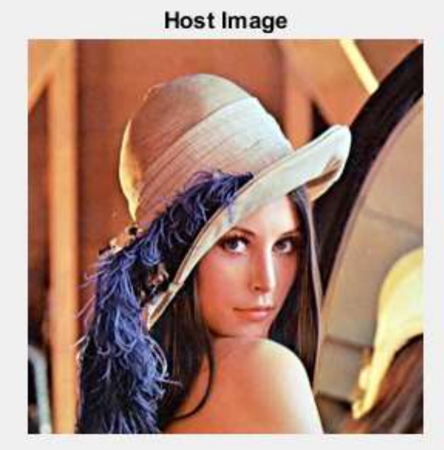


Figure 3a: cover Image

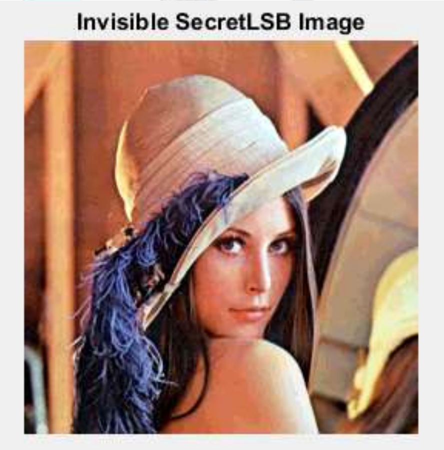
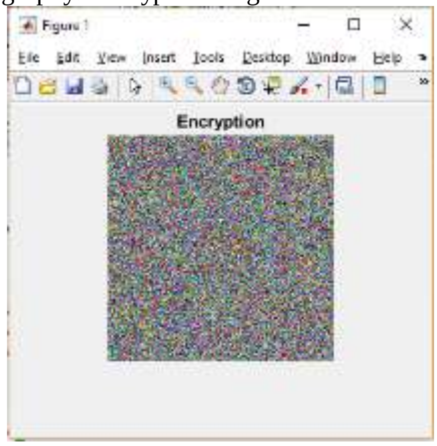


Figure 3b: Output stego Image

In the second module, to protect the image from steganalysis elliptic curve cryptography encryption algorithm is applied to generate stego image, which provides better security with small key size that RSA provides with a longer key. To provide a dipper level of security and randomness in pixel value, shares of an encrypted image are generated using (2, 2) color visual cryptography. Encrypted image and shares of the encrypted image shown below:



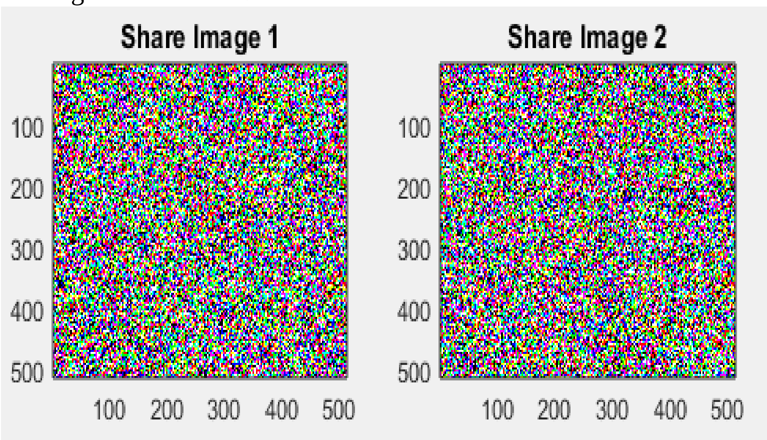


Figure 4: Encrypted Stego Image Figure 5: Two Shares of Encrypted Image

Both Share images are then sent to the receiver. The receiver applies the reverse process in order to decrypt and extract the secret images. The final output is obtained at the receiver side. The secret image is recovered at the receiver end without any data loss.

VIII. Conclusion

The focus of this paper is the security and confidentiality of data. A new method of image steganography and hybrid cryptography is implemented in order to enhance the security and also the data embedding capacity of the image. An image is hidden inside another image with the help of 4-4-4 XOR least significant bit steganography, a data hiding technique. Hence the embedding capacity of a 24-bit image is improved as compared to that of existing LSB methods. The security of the image is further enhanced by implementing elliptic curve cryptography encryption of stego images. The method ensures the high security of the secret image as it is split into two parts called shares. The two images are then sent separately over the network. If the intruder intercepts one image and tries to extract the secret data then he/she will not be able to recover the data. Hence this method enhances the data embedding capacity, ensures 100 percent recovery of secret data, and also ensures the security of data at three levels: Steganography, Cryptography, and splitting image by visual cryptography.

IX. Acknowledgment

I would like to thank my honorable teachers, fellow students, supportive friends and especially my family. I would also like to say thank to that person who guides me through the way, she continually and persuasively conveys a spirit of adventure in regards to my work Ms. Amita Shahmam.

X. REFERENCES:

[1] William Stallings, Cryptography and Network Security, Principles and Practice. Fifth edition.

[2]Artz, Donovan. "Digital steganography: hiding data within data." internet computing, IEEE 5.3 (2001): 75-80.

[3]https://www.ukessays.com/essays/computer-science/the-types-and-techniques-of-steganography-computer-science-essay.php

[4]Mansi S. Subhedara, Vijay H. Mankarb. Current status and key issues in image steganography: A survey. COMPUTER SCIENCE REVIEW 13–14 (2014) 95–113

[5]Hill, Douglas W., and James T. Lynn. "Adaptive system and method for responding to computer network security attacks." U.S. Patent No. 6,088,804. 11 Jul. 2000.

[6] Kaufman, Charlie, Radia Perlman, and Mike Speciner. Network security: private communication in a public world. Prentice Hall Press, 2002.

[7]Alfalou, Ayman, and C. Brosseau. "Optical image compression and encryption methods." Advances in Optics and Photonics 1.3 (2009): 589-636

[8]http://users.telenet.be/d.rijmenants/en/visualcrypto.htm

[9]Kenneth H Rosen. Cryptography: theory and practice. CRC press, 2005.

[10] Denning, Dorothy E. "Cryptography and data security." (1982).

[11]Manju Kumari . Shailender Gupta. Pranshul Sardana; "A Survey of Image Encryption Algorithms", _ 3D Research Center, Kwangwoon University and Springer-Verlag GmbH Germany, part of Springer Nature 2017

[12]Matsui, M. (1994). The first experimental cryptanalysis of the Data Encryption Standard. Advances in cryptology—CRYPTO'94 (pp. 1–11). https://doi.org/10.1007/3-540-48658-5_1.

[13]Schneier, B. (1994). The Blowfish encryption algorithm.Dr. Dobb's Journal, 19, 38–40. http://www.drdobbs.com/security/the-blowfish-encryption-algorithm/184409216.

[14]Neeta, D., Snehal, K., & Jacobs, D. (2007). Implementation of LSB Steganography and Its Evaluation for Various Bits. 2006 1st International Conference on Digital Information Management.

[15]"A Survey on different techniques of steganography" Harpreet Kaur, Jyoti Rani, MATEC Web of Conferences DOI: 10.1051/matecconf/20165702003 ICAET 2016

[16]Naor, M., & Shamir, A. (1995). Visual cryptography. Lecture Notes in Computer Science, 1–12. doi:10.1007/bfb0053419

[17]A Arjuna Rao1, K Sujatha1, A Bhavana Deepthi1, L V Rajesh1 (2017), "Survey paper comparing ECC with RSA, AES and Blowfish Algorithms", International Journal on Recent and Innovation Trends in Computing and Communication, IJRITCC

[18]Shivani Chauhan, Jyotsna, Janamejaya Kumar, Amit doegar"Multiple layer Text security using Variable block size Cryptography and Image Steganography" 2017 International Conference on "Computational Intelligence and Communication Technology (IEEE-CICT).

[19]Shreyank N Gowda" Advanced Dual Layered Encryption for Block-Based Approach to Image Steganography" 2016 International Conference on Computing, Analytics and Security Trends (CAST) © 2016 IEEE

[20]Shreyank N Gowda " Using Blowfish Encryption to Enhance Security Feature of an Image" International Conference on Information Communication and Management © 2016 IEEE

[21]Swati Narkhede, Mahesh Shirole" New watermark embedding technique using visual cryptography" International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017) © 2017 IEEE

[22]Prachi Khokhar and Debasish Jena"Color Image Visual Cryptography Scheme with Enhanced Security" 2016 International Conference on Frontiers in Intelligent Computing: Theory and Applications © 2017 Springer

[23]Alaa kadhim, Rand Mahmoud Mohamed" Visual Cryptography For Image Depend on RSA & ElGamal Algorithms" International Conference on Multidisciplinary in IT and Communication Science and Applications © 2016 IEEE

[24]Nikhil C. Mhala, Rashid Jamal, Alwyn R. Pais "Randomised visual secret sharing scheme for grey-scale and color images" IET Image Process; The Institution of Engineering and Technology 2017© 2017 IET

[25]M. Mary Shanthi Rani, G. Germine Mary and K. Rosemary Euphrasia "Multilevel multimedia security by integrating visual cryptography and steganography techniques" 2016 cybersecurity and computational models, Advances in Intelligent © 2016 Springer

[26]Mrs. Nilam Kate, Mrs. J. V. Katti "Security of remote voting system based on visual cryptography and SHA" International Conference on Advances in Computing, Communications, and informatics © 2016 IEEE

[27]Rubeena Jabi, Punyaban Patel, Deepty Dubey, "An Efficient Secure Data Transmission Based on Visual Cryptography", IEEE International Conference on Research Advances in Integrated Navigation Systems (RAINS - 2016).

[28]Venkata Krishna Pavan Kalubandi, Hemanth Vaddi, Vishnu Ramineni, Agilandeeswari Loganathan, "A novel image encryption algorithm using AES and visual cryptography", International Conference on Next Generation Computing Technologies (NGCT-2016) IEEE.

[29]Tapan Kumar Hazra, Anisha Mahato, Arghyadeep Mandal, Ajoy Kumar Chakraborty," A Hybrid Cryptosystem of Image and Text Files Using Blowfish and Diffie-Hellman Techniques", IEEE 2017

[30] https://www.techopedia.com/definition/1770/cryptography

[31] https://www.slideshare.net/PratikshaPatil/visual-cryptography1

[32] http://sipi.usc.edu/database/.

[33] https://docslide.net/documents/the-advantages-of-elliptic-curve-cryptography-for-advantages-of-elliptic-curve.html