Enhanced Blend of Image Steganography and Cryptography

Radha S. Phadte
Department of Computer Engineering
Goa College of Engineering
Goa, India
radha0128phadte@gmail.com

Rachel Dhanaraj, Asst. Professor
Department of Computer Engineering
Goa College of Engineering
Goa, India
racheldhanaraj@gmail.com

***Abstract*— As there is large advancements in internet technology, there has been huge text as well as multimedia data transfer over the internet. Due to this data security is a vital necessity. Steganography and Cryptography are the sets of techniques to provide security to data. Steganography is an art of hiding secret information into another cover medium like image, audio, video, etc. Cryptography is an art of converting plain data into unreadable format. Steganography can be integrated with Cryptography in order to enhance the security of data. In this paper, a new method is proposed to provide security to 24 bit color images, by integrating Steganography and Cryptography. In this method, randomized LSB based method is used to hide an image in another image. The resulting stego image is then encrypted using chaotic theory. This new integrated method ensures the enhancement in the data hiding capacity, the security of the image and lossless recovery of the secret data.**

***Keywords*— Image, Steganography, Cryptography, LSB, Encryption, Decryption, Chaos Theory, Data hiding, key, Security.**

I. INTRODUCTION

There has been a tremendous development in the communication field in recent time. Hence the security and confidentiality of information has become a very essential and important requirement for communication. With the speedy development and enhancement of the Internet Science and multimedia technology, we use various forms of digital data such as texts, images, videos, audios in our day to day life. Huge information can be transmitted through the network of computers and mobile devices. However, the security and confidentiality of data over the internet is not up to the mark, and the data can be captured by an unauthorized user. Hence ensuring the Security and Confidentiality of data transmission is very important and current necessity. This requirement can be achieved by different techniques like Steganography and Cryptography [1].

Cryptography and Steganography are the most popular and widely used technologies for the purpose of data security in communication. Steganography is an art and science of hiding the secret data into another data. However Cryptography is an art of changing the appearance of data in order to make it unreadable. In other words, Steganography hides the existence of the data, while Cryptography hides the readable and meaningful contents of the data.

Cryptography techniques can be basically classified into two types. Symmetric-key cryptography and Asymmetric-key cryptography. In Symmetric-key, only one key is used by the sender as well as the receiver. In Asymmetric-key, two different keys are used: a public key which is disclosed to all and a private key which is secretly known only to the authorized recipient of data. In Cryptography, even though the secret data is sent in the unreadable format, it gives the hint of existence of secret data to the unauthorized recipient. However in Steganography, such hint is not given to the unintended recipient as the secret data is hidden inside another data. Therefore, Steganography can be more useful and advantageous when the use of cryptography is risky or prohibited [2].

Steganalysis is a study or set of techniques for extracting the secret data which is hidden in some stego-media. Cryptanalysis is a set of techniques for finding the meaningful secret data from the cipher data. The work done in this paper is focusing on the methodology for combining together Steganography and Cryptography for images.

II. THEORY

A. LSB Steganography

LSB (Least Significant Bit) is one of the spatial domain steganography techniques. LSB technique is used to embed the data inside another data called as cover-media. The cover media can be image, audio or video. 8-bit or 24-bit images can be used as cover image to hide the secret data. The MSBs of image pixels carry the most significant data of the image and the LSBs carry the least significant data of the image. The desired number of MSBs (Most Significant Bit) of secret data can be embedded behind the LSBs (Least Significant Bit) of the cover image. Therefore the stego image obtained by embedding the secret data in cover image looks similar to the original cover image. But the similarity between Cover image and stego image decreases as the number of embedded bits of secret data increases [3].

978-1-5090-4890-8/17/$31.00 ©2017 IEEE

B. Chaos Theory

Digital images have some peculiar properties that make images and other multimedia data different from text. Some of these properties are, high correlation among pixels, large data redundancy and mass data capacity. Due to such properties, image encryption becomes different from texts encryption. Therefore, encryption algorithms used for text encryption like DES, AES, RSA, Blowfish are inappropriate for encryption of images or other multimedia data. Therefore the chaos based encryption techniques are proved to be most suitable and advantageous for encryption of multimedia data. In common words, chaos means randomness or a state of disorder. Chaotic systems have the following properties: 1) They are deterministic i.e. they have several mathematical equations or formulation which rule their behavior. 2) They are sensitive to initial conditions. 3) They are unpredictable and non-linear that is a small change can produce large or huge effects. 4) They appear to be random and disorderly. Chaos based encryption techniques give high speed, complexity, less computational overheads, computational power and high security [4].

This paper basically consists of six sections. Section I gives the introduction of this paper. Section II gives the theory of the techniques used in this proposed method. Section III shows the survey of different existing methods of cryptography and steganography. Section IV explains the proposed methodology. Section V shows the Test results and Analysis. Finally section VI gives the conclusion of this paper.

III. Literature Review

There are various methods implemented in case of Steganography and Cryptography. Enhancements in these existing methods can be done after a review of such existing methods.

Authors in [5] proposed two methods of combined cryptography and steganography. In first method an image is secured by converting it into an encrypted form using S-DES algorithm and a secret key and then the encrypted image is concealed in another image. In the second method, an image is secured by encrypting it using S-DES algorithm and an image key. The resulting image is then concealed inside another image so as to hide its very existence. Both these techniques have been tested and it has been observed that they prevent the possibilities of steganalysis also.

Authors in [6] have proposed a new method to improve the security of data that incorporates LSB based data hiding technique along with cryptography and digital signature. Authors have incorporated the randomness in data embedding positions with the help of a control message. This control message decides the LSB positions of cover image to hide the secret data. The control message is provided with digital signature by sender's private key and then again encrypted with receiver's public key and then sent to the receiver. So the secret data can be extracted from the stego image only by decrypting and authenticating the control message sent by the sender, with the help of corresponding private and public keys.

Authors in [7], have proposed a hybrid approach which uses combination of image encryption and image hiding, to provide higher security. Image encryption is done using Blowfish Algorithm and for image hiding LSB technique is used.

Authors in [8], have proposed a method that combines the techniques of cryptography and steganography. Here the secret data to be sent is first encrypted by AES algorithm. The encrypted data is then embedded in the cover image using LSB data hiding technique with randomness. The resulting stego-image is then split into different parts depending upon the intensity values of pixels. These parts are again encrypted and sent to the receiver. Receiver receives each part and decrypts it. All the decrypted parts are then combined in order to obtain the stego image. Then the secret data is extracted from the stego-image.

Authors in [9], have proposed a method for image encryption using chaos based technique. This method basically has two steps. In the first step a chaotic sequence is generated using Henon map. And in the second step, each pixel of the plain image is encrypted using the chaotic sequence generated in the first step.

Authors in [10], have proposed a new method for image encryption. This method is based on chaos based theory. Here, the logistic map is used to create chaotic sequences. These chaotic sequences which act as confusion key and diffusion key, are then used to perform chaotic confusion and diffusion of image pixels in order to obtain the encrypted image. Confusion and Diffusion are performed by applying Ex-OR operation between intensity of pixels and chaotic sequences.

Authors in [11], have proposed a new encryption method for image encryption. In this method, first the image is encrypted using chaotic diffusion. The diffused image is then passed through a wavelet transform to convert the image into frequency domain. The resulting image is then encrypted using chaotic confusion. Then the inverse wavelet transformed is applied to get the image back from frequency domain. Then the encrypted image is sent to the receiver along with the fingerprint of the image. Here the privacy as well as integrity of the image is maintained.

Authors in [12], have proposed a new image encryption method which is based on chaos theory. Here the image is split into three different color planes i.e. Red, Green, Blue. Chaotic confusion and diffusion is performed on each color plane of the image separately. Then these encrypted color planes are combined to form final encrypted image.

Authors in [13] have presented a new method of image steganography in spatial domain on gray images, blend with cryptography. By this method, the data is first encrypted using

978-1-5090-4890-8/17/$31.00 ©2017 IEEE

Vernam cipher algorithm and then the encrypted data is embedded inside an image using the new image steganography method i.e. LSB with Shifting (LSB-S). In LSB-S method authors have used four LSB of the pixel and performed circular Left shift operation and XOR operation.

Authors in [14] have introduced a new LSB based steganography method. In this, secret information is hid in cover image in a random order with the help of a secret key. Here, a secret key word is taken and it is converted into stream of ASCII values and then into a stream of binary bits. This stream of binary bits is then XORed with the binary bits of Red color plane. The result is then used to decide whether the secret data bits are to be stored in LSBs of green plane or blue plane.

Authors in [15] have proposed LSB based image steganography method in order to improve image security and quality. Here, RC4 algorithm is used to achieve randomization in hiding secret data bits in LSBs of Cover image pixels instead of sequential embedding. After embedding, certain LSBs of Stego image are inverted in order to reduce the number of modified LSBs. Thus, less number of least significant bits of cover image is altered in comparison to plain LSB method, improving the PSNR of stego-image. By storing the bit patterns for which LSBs are inverted, message image can be obtained correctly.

IV. Proposed Methodology

This system provides the enhanced blend of image steganography along with cryptography. This method proposes an improved randomized LSB technique for color image steganography and uses chaotic theory for encryption of stego-image. The block diagram for the proposed method is shown in Fig.1a and Fig.1b.

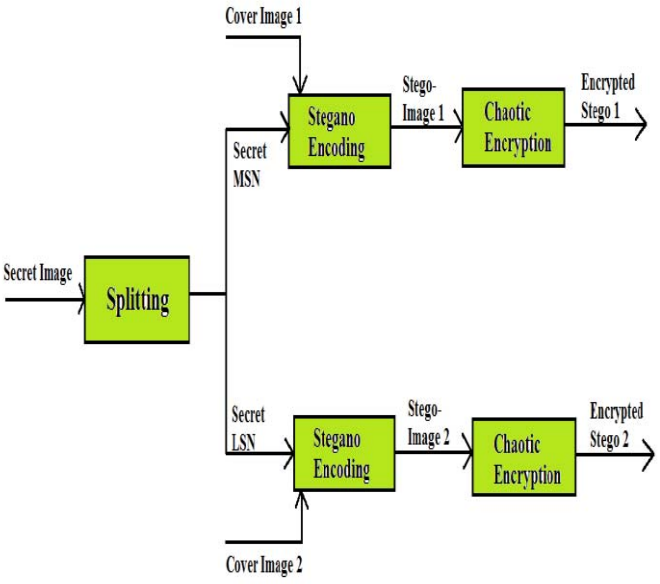

Fig 1a. Block Diagram of Proposed Method at Sender

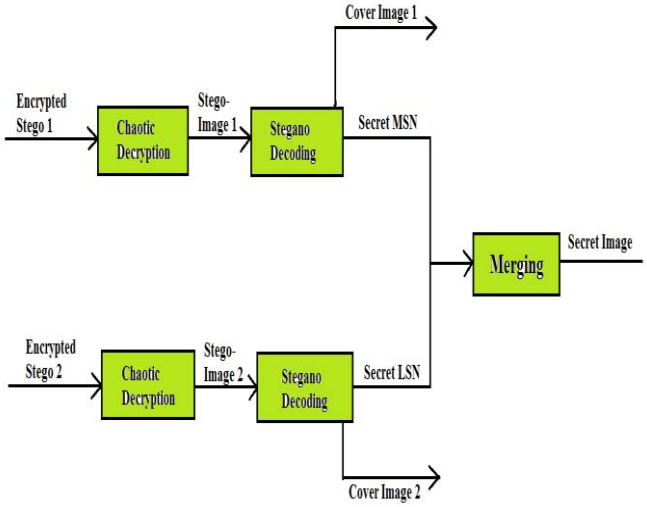

Fig 1b. Block Diagram of Proposed Method at Receiver

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

1. Splitting
2. Stegano Encoding
3. Chaotic Encryption
4. Chaotic Decryption
5. Stegano Decoding
6. Merging

In the first module, the 24 bit secret image is taken and split into three planes: Red, Green and Blue. Each plane is then split into two parts at bit level of each pixel. The two parts are named as Secret MSN (Most Significant Nibble) and Secret LSN (Least Significant Nibble). In the second module, two 24 bit cover images are chosen. Both secret MSN and secret LSN are embedded in randomized order, in two different cover images using 4-4-4 data hiding technique of steganography. In the third module, both the stego images are encrypted using chaotic theory and a secret key. Here the encryption is applied by number of confusion and diffusion rounds on stego images. Confusion is applied to shuffle the pixel positions of the stego images. Diffusion is applied to change the intensity values of pixels of stego images. Both the encrypted stego images are then transmitted from sender to receiver. In the fourth module, receiver decrypts both the images using reverse process and the same secret keys. In the fifth module, secret MSN and secret LSN are extracted from both the stego images. In the sixth module, Secret MSN and secret LSN are merged together to obtain final secret image. Same set of secret keys are used at the sender as well as the receiver. Sender informs the receiver about the secret keys through email.

A. Algorithm

1) Splitting of Secret image into two secret images

978-1-5090-4890-8/17/$31.00 ©2017 IEEE

- Split each pixel of Red, Green and Blue planes of the image into two sub-pixels to form two different images as : MSN Secret and LSN Secret.
- MSN : Most Significant Nibble
  LSN : Least Significant Nibble
- Following steps are applied on both images (Secret MSN and Secret LSN).

2) Stegano Encoding

- Secret image is embedded in randomized order in the Cover image using 4-4-4 hiding technique.
- For Example
  Cover Image Pixel : [1101**1100** 1100**0110** 1000**0111**]
  Secret image Pixel : [1100 1001 1010]
  Stego image Pixel : [1101**1100** 1100**1001** 1000**1010**]

3) Chaotic Encryption

- Basically consists of two main steps.
- 2D Chaotic Confusion
- 1-D Chaotic Diffusion.

2D Chaotic Confusion

- Confusion is performed in the proposed method with the help of secret encryption keys called as Confusion keys.
- Initially, random transposition of image pixels is performed. For this, a system generated Confusion key matrix (of image size) is created with the help of which the image pixels are transposed. Confusion is then performed on this randomly transposed image.
- Three different Confusion keys are used for Confusion of Red, Green and Blue plane of the image.
- 1 Confusion round is created by: 1 column-wise shuffle and 1 row-wise shuffle.
- Pixel P(a,b) is interchanged with pixel P(a',b') for all $1 \leq a \leq r$ and $1 \leq b \leq c$ (where r*c is the size of the plain image).
- In Row-wise Confusion,
  $a' = a$ (1)
  $b' = b + key \bmod (c)$ (2)
- In Column-wise Confusion
  $a' = a + key \bmod (r)$ (3)
  $b' = b$ (4)

1-D Chaotic Diffusion (Using Logistic Map)

- Diffusion is performed on Confused Image.
- Diffusion is performed by using logistic map. It is defined as:
  $$Y_{n+1} = e\, Y_n\, (1 - Y_n) \quad (5)$$
  Where Y_0 and e are two real numbers, such that: $Y_0 \epsilon [0,1]$ and $e \epsilon [0,4]$.
  For $3.57 < e < 4$, the logistic map becomes chaotic.
- In Diffusion, pixel intensity values of each and every pixel are changed.
- P(a,b) is replaced with P'(a,b), for all $1 \leq a \leq r$ and $1 \leq b \leq c$ where r*c is the size of the plain image.
- Create an array X from each color plane of the confused image.
- Each element in the array is the intensity value of one of the color components of a pixel.
- The dimension 's' of this array is equal to r*c, where r is the number of rows and c is the number of columns of the image.
  $$X = [x_1, x_2, \ldots, x_s]$$
- Generate the Diffusion Key 'DiffKey' as an array of chaotic sequence $K=\{k_1, k_2, \ldots k_s\}$, using equation (5).
- Conduct a chaotic diffusion of the image pixels stored in the array X, one by one, using the chaotic sequence K, for $i = 1, \ldots, s$
  $$X_i = X_i \text{ XOR } K_i \quad (7)$$
- Perform the following operation on the resulting array obtained in the previous step,
  $$X_i = X_i * K_i \quad (8)$$
- Build the encrypted image by combining arrays X (of each color component) obtained after all the previous steps.
- The secret key of the algorithm consists of the system generated Confusion key matrix, three Confusion keys, and the initial conditions y_0 and e for Diffusion key.
- For Decryption, all the steps are performed in the reverse order and with the same secret keys.

V. Test Results And Analysis

The proposed model in this paper is implemented in Matlab. Both Secret image and cover images are of 24 bits. The size of secret image should be lesser than or equal to the size of cover image. Here the images with different sizes are tested. The secret image of Squirrel.jpg and the two cover images of Tiger.jpg and Feather.jpg are shown in Fig 2a, 2b and 2c. These images have the size 1024*640.

In Stegano-Encoding both secret MSN and secret LSN are embedded in two different cover images using LSB based 4-4-4 data hiding technique of steganography. The output of this module is stego-images which are shown in Fig.3a and 3b.

In the third module both the stego images are encrypted using chaotic confusion and diffusion. The output of this module is shown in Fig.4a and 4b.

978-1-5090-4890-8/17/$31.00 ©2017 IEEE

Fig 2a. Secret Image

Fig 2b. Cover Image 1

Fig.2c Cover Image 2

Fig.3a. Stego-Image 1

Fig.3b. Stego-Image 2

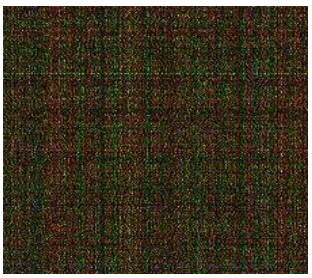

Fig.4a. Encrypted Stego 1

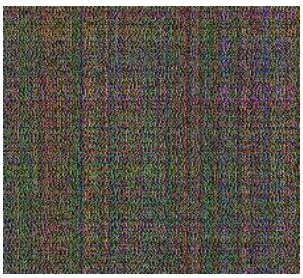

Fig.4b.Encrypted Stego 2

Both the encrypted stego images are then sent to the receiver. The receiver applies the reverse process in order to decrypt and extract the secret images i.e. secret MSN and secret LSN. Then both the secret parts are merged to get the final secret image. The final output obtained at the receiver side is shown in Fig. 5. The secret image is recovered at the receiver end without any data loss.

Fig.5 Secret Image

A. Histogram Analysis

Histogram of an image is a graphical view of the pixel intensity distribution in a digital image. It plots the number of pixels for each intensity value. Fig 6 shows the histograms for Red, Green and Blue plane of Cover, Stego and Encrypted image. It shows that the histograms for cover image and Stego image are almost same. Hence it does not encourage for steganalysis. The histogram for Cover image and Encrypted image are completely dissimilar which gives no hint about the original image. Hence it prevents statistical attack.

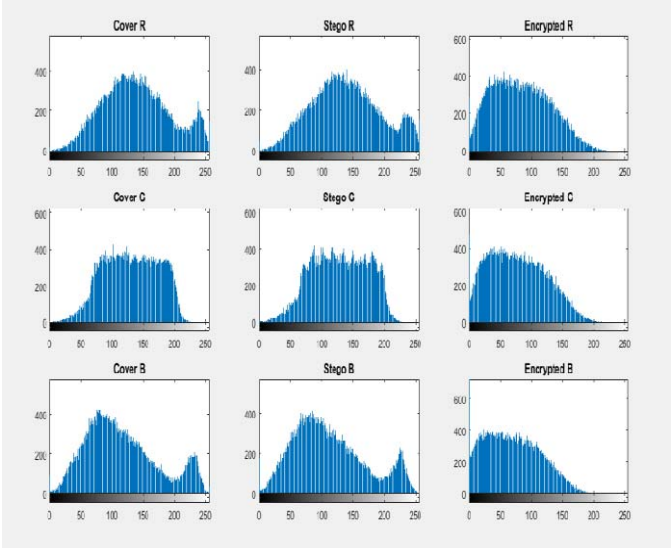

Fig 6 Histograms for Cover, Stego and Encrypted Images

Fig 7 shows the histogram for the Red, Green and Blue plane of the secret image and the recovered image. It shows that both the histograms are exactly same. Hence this method ensures lossless recovery of secret image.

978-1-5090-4890-8/17/$31.00 ©2017 IEEE

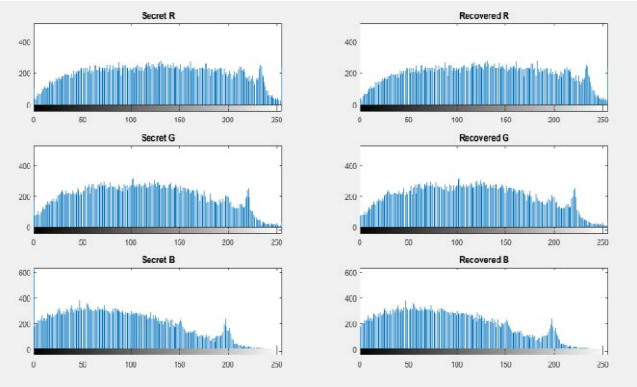

Fig 7 Histograms for Secret and Recovered Image

B. Key Sensitivity Analysis

Three different Confusion keys are used for Red, Green and Blue Planes: 3564102789476583, 4664102789476583, 5764102789476583. And the Diffusion parameters: 3.89012563468327, 0.45673028132475.

The encrypted image is decrypted using the same keys to obtain the secret image shown in Fig 5. If the image is decrypted using the Diffusion parameters as: 3.89012563468321, 0.45673028132479 (only the last single digit is changed) then the Secret image obtained is shown in Fig 8. This proves that the proposed algorithm is very sensitive to the change in the secret key, which makes it impossible to recover the original data through cryptanalysis attack.

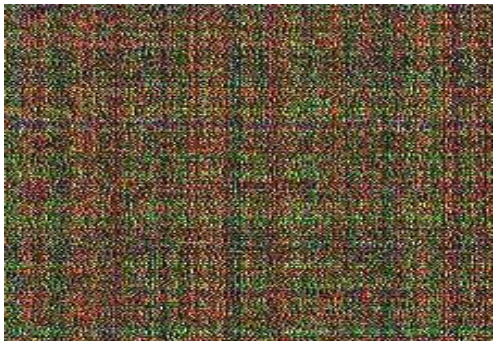

Fig.8 Secret Image obtained with wrong key

VI. CONCLUSION

The focus of this paper is security and confidentiality of data. A new method of image steganography and 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 data hiding technique. Hence the embedding capacity of 24 bit image is improved as compared to that of existing LSB methods. The security of the image is further enhanced by implementing chaotic encryption of stego images. The method ensures the high security of the secret image as it is split into two parts and embedded in two different cover images. 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 be able to recover the data only partially. Hence this method ensures the lossless recovery of the secret image at the receiver end; it enhances the data embedding capacity and also ensures the security of data at three levels: Steganography, Cryptography, and Transmission by splitting.

REFERENCES

[1] Shahzad Alam, S M Zakariya, M Q Rafiq, "Analysis of Modified LSB Approaches of Hiding Information in Digital Images", 2013 5th International Conference on Computational Intelligence and Communication Networks, @ 2013 IEEE.

[2] A. Joseph Raphael, Dr. V. Sundaram, "Cryptography and Steganography–A Survey", Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630.

[3] Rupali Jain, Jayshree Boaddh, "Advances in Digital Image Steganography", 2016 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016), ©2016 IEEE.

[4] Ephin M, Judy Ann Joy, N. A. Vasanthi, "Survey of Chaos based Image Encryption and Decryption Techniques", Amrita International Conference of Women in Computing (AICWIC'13).

[5] Vipul Shanna, Madhusudan, "Two New Approaches for Image Steganography Using Cryptography", 2015 Third International Conference on Image Information Processing, © 2015 IEEE.

[6] Xinyi Zhou, Wei Gong, WenLong Fu, LianJing Jin, "An Improved Method for LSB Based Color Image steganography Combined with Cryptography", copyright 2016 IEEE ICIS 2016, June 26-29, 2016, Okayama, Japan.

[7] Moresh Mukhedkar, Prajkta Powar, Peter Gaikwad, "Secure non real time image encryption algorithm development using cryptography & Steganography", ©2015 IEEE.

[8] Jitha Raj.T, E.T Sivadasan, "Secure Transmission of Data by Splitting Image", 2015 Intl. Conference on Computing and Network Communications (CoCoNet'15), Dec. 16-19, 2015, Trivandrum, India, ©2015 IEEE.

[9] Joshi Rohit A, Joshi Sumit S, G. P. Bhole, "Improved Image Encryption Algorithm using Chaotic Map", International Journal of Computer Applications (0975 – 8887) Volume 32– No.9, October 2011.

[10] Fadia TALEB, "A New Chaos Based Image Encryption Scheme Using Chaotic Logistic Maps", ©2014 IEEE.

[11] Manish Mishra, Shraddha Pandit, "Image Encryption Technique Based on Chaotic System and Hash Function", 2014 IEEE International Conference on Computer Communication and Systems(ICCCS '14), Feb 20-21, 2014, Chennai, INDIA, ©2014 IEEE.

[12] Nikhil Debbarma, Lalita Kumari, Jagdish Lal Raheja, "2D Chaos Based Color Image Encryption Using Pseudorandom Key Generation", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 4, July – August 2013.

[13] Kamaldeep Joshi, Rajkumar Yadav, "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication", 2015 Third International Conference on Image Infonnation Processing, © 2015 IEEE

[14] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, "A New Approach for LSB Based Image Steganography using Secret Key", 14th International Conference on Computer and Information Technology (ICCIT 201 I) 22-24 December, 201 I, Dhaka, Bangladesh, @ 2011 IEEE.

[15] Nadeem Akhtar, Pragati Johri, Shahbaaz Khan, "Enhancing the Security and Quality of LSB based Image Steganography", 2013 5th International Conference on Computational Intelligence and Communication Networks, © 2013 IEEE.