Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 12, December 2014, pg.624 – 632

RESEARCH ARTICLE

Hide and Encryption Fingerprint Image by using LSB and Transposition Pixel by Spiral Method

Hyder Yahya Atown
Department of Computer sciences, College of Education for Pure Sciences, Thi-Qar University, Iraq
Haideryhy@yahoo.com

Abstract— The communication provides many methods to distribute information to the people, especially after the growth of multiple applications. Consequently, the security of information has become a fundamental issue. There are two techniques for protect the data: Steganography and cryptography, the combination of these two methods will enhance the security of the data embedded. This paper is about encryption and decryption of fingerprint image using transposition pixel by spiral method that designed to increase security and to improve performance. The process begins when encrypted the fingerprint image by using transposition method and then embed inside an image using LSB method. A comparative analysis is made to demonstrate the effectiveness of the proposed method by computing MSE and PSNR by using MATLAB.

Keywords— Cryptography, Steganography, LSB, Transposition pixel, Spiral method, MATLAB

I. INTRODUCTION

In the past few years, the information is transferred over computer networks and which later became vulnerable to attack and for integrity of data, because of the increasing demand for information security. The information security can achieved by using encryption and hide the information before it is transmitted or stored [1]. Steganography is hiding a secret message or information inside some other digital media in such a way that others cannot discover the presence or contents of the hidden message [2]. Cryptography is a method of storing and transmitting data in a form that only authorized people can be read this information [3]. It is an effective way of protecting the secret information that it is transmitted through network communication or stored on media. The encryption methods for enhancing the security of digital contents has gained high significance in the current era of breach of security and misuse of the confidential information intercepted and misused by the unauthorized parties. Steganography and cryptography are both used to ensure data confidentiality. However, steganography differs from cryptography in the sense that the cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [1]. Thus, with cryptography anybody can see that both parties are communicating in secret. Steganography hides the existence of a secret message in such a way that nobody can see that both parties are communicating in secret [4]. Hide and encryption the image has become an important research area and it has broad application prospects [5]. Many image content encryption algorithms have been proposed. To make the data secure from various attacks and for the integrity of data we must encrypt the data before it is transmitted or stored.

The research aims is to improve the security of the data by combining two techniques steganography and cryptography. The process begins when encrypted the image by using transposition pixel by spiral method and

then embed inside an image using LSB steganography technique. This combinational methodology will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel. The resulting hide-image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker detects the information from the hide-object, it would still require knowledge of image encryption algorithm to decipher the encrypted image [6]. The image hide are tested by transmitting them and the embedded data are successfully extracted by the receiver. The main aim behind the design of this proposal is to get the best security performance over existing Web images by developing a spiral cipher algorithm for image encryption of n*n size by transposition the pixel values. The algorithm ultimately makes it possible for encryption and decryption of the images based on the pixel. The algorithm was implemented and tested by using MATLAB.

II. ENCRYPTION IMAGE

The security of information can be achieved by using cryptography and Steganography. In cryptography, encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge [7]. Where cryptography merely obscures the integrity of the information so that it does not make sense to anyone except the creator and the recipient [1]. Cryptography has evolved from the classical such as Caesar, Vigenère, Trifid ciphers to modern day cipher and public key systems such as symmetric and asymmetric encryption [8]. Cryptography today involves the use of advanced mathematical procedures during encryption and decryption processes. Encryption algorithms have varied such as Advanced Encryption Standard (AES), Blowfish, Triple Data Encryption Standard (3DES) and Serpent [3].

The cryptography in digital computing has been applied to different kinds of digital file formats such as text, images video etc. One of the best-known techniques of visual cryptography has been credited to Moni Naor and Adi Shamir, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image [9]. The chaotic confusion and pixel diffusion methods was proposed by Friedrich perform the permutations using a chaotic combined with alterations of Grey-Level values of each pixel in a sequential manner [10].

III. STEGANOGRAPHIC TECHNIQUE

Data is the backbone of today's communication. To ensure that data is secured and does not go to unintended destination, the concept of data hiding came up to protect a piece of information [11]. Digital data can be delivered over computer networks with little errors and often without interference. The Internet provides a communication method to distribute information to the masses. Steganography is the art of passing information in a manner that the very existence of the message is unknown [12]. All digital file formats can be used for steganography [13]. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. The most popular cover objects used for steganography are digital images. The following Figure shows steganography technique [14].

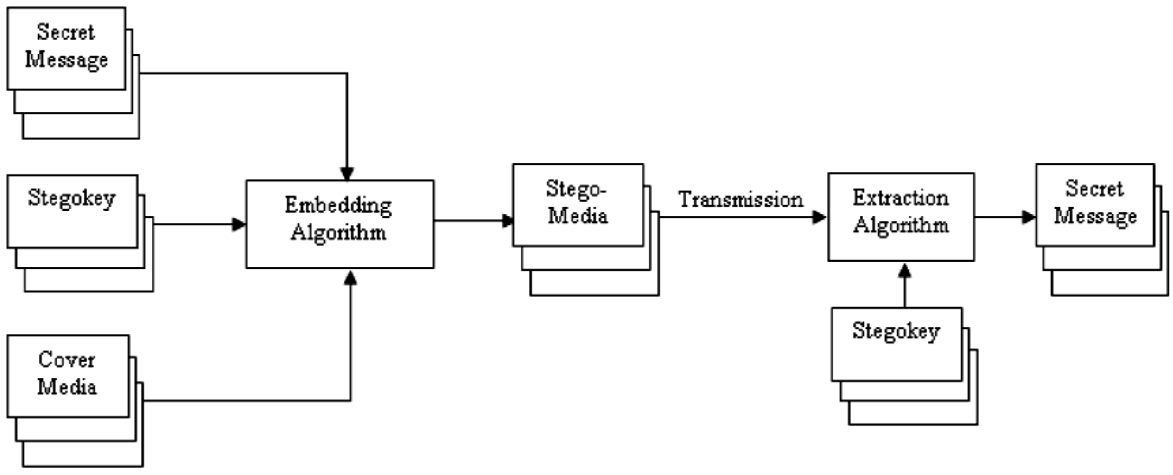


Figure 1. Steganography technique [14].

A simple way of steganography is based on modifying the least significant bit layer of images, known as the LSB technique. This embedding method is based on the fact that the least significant bits in an image can be thought of as random noise, and consequently they become not responsive to any change on the image [15]. LSB is the most commonly used type of insertion scheme used currently in digital steganography [16]. This method is probably the easiest way of hiding information in an image [17, 18]. The secret message is hidden by altering least significant bit in a certain layer of the image file. Altering the LSB will only cause minor changes in color, and thus is not usually noticeable to the human eye. In the LSB technique, the least significant bits of the pixels is replaced by the message which bits are permuted before embedding. In some cases [19], LSB of pixels visited in random or in certain areas of image and sometimes increment or decrement the pixel value. The implementation of LSB method is quite easy and it is a popular method. To hide a secret message inside an image, a proper cover image is needed, because this method uses bits of each pixel in the image. Digital image steganography is accomplished by using a common principle called least significant bit insertion. Each pixel contains a number of bytes that describe the color and appearance of the pixel. Depending on the resolution of that image, there are a set number of bytes for each pixel [20].

Digital images often have a large amount of redundant data and for this reason it is possible to hide message inside image file [21]. An image in a computer is an array of numbers that represent light intensities at various points (pixels). The advantages of LSB based data hiding method is that it is simple to embed the bits of the message directly into the LSB plane of image and many techniques use these methods [21]. The LSB modification does not result in image distortion and thus the resulting stego-image will look identical to the cover-image [22]. These pixels make up the image's raster data. Digital images are stored in either 24-bit (true color images) or 8-bit per pixel files. Grayscale images are preferred because the shades change very gradually between palette entries. This increases the image's ability to hide information [23]. These hide information in a way similar to watermarks on actual paper and are sometimes used as digital watermarks [24].

IV. RELATED WORKS

Nowadays, the issue of security has become one of the most important problems in the field of information technology. Many users want their information and their data to be safe and confidential. The use of cryptography and steganography techniques together can solve this issue. Image encryption have been increasingly studied to meet the demand for real-time secure image transmission. With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks. The security of images has become more and more important due to the rapid evolution of the internet in the world today.

Mamta et al presented a technique for LSB steganographic insertion [25]. They described a technique to embed data through compression 24 bit bitmap file by 8 bit color map. They discussed that this 8 bit color insertion technique provide a good starting point for anyone interested in learning about steganography. The other authors explained LSB embedding technique and presented the evaluation for various file formats [26]. They don't analyze their techniques with other steganographic techniques. According to Neha Sharma et al. proposed a system that combines the effect of two methods such as cryptography and steganography to enhance the security of data [27].

A new cryptographic proposed for securing color image based on visual cryptography was done by Krishnan et al. A binary image was used as the key input to encrypt and decrypt a color image. The secret color image which needs to be communicated was decomposed into three monochromatic images based on YCbCr color space. Then these monochromatic images were then converted into binary image, and finally the obtained binary images were encrypted using binary key image [28]. Christy et al proposed a method that uses Back Propagation Network (BPN) for extended visual cryptography. The size of the image produced was the same as that of the original image [29].

Kester proposed a cryptographic algorithm based on matrix and a shared secrete key [30]. He further applied encryption and decryption of the images based on the RGB pixel [31]. Xu et al, proposed a novel image encryption based on a nonlinear chaotic map (NCM) and only by means of XOR operation. There were two rounds in the proposed image encryption scheme. In each round of the scheme, the pixel gray values were modified from the first pixel to the last pixel firstly, and then the modified image was encrypted from the last pixel to the first pixel in the inverse order [32].

Ruisong et al, proposed two novel schemes to shuffle digital images. Different from the conventional schemes based on Standard map, they disordered the pixel positions according to the orbits of the Standard map. The proposed shuffling schemes didn't need to discretize the Standard map and own more cipher leys compared with the conventional shuffling scheme based on the discretized Standard map. The shuffling schemes were applied to encrypt image and disarray the host image in watermarking scheme to enhance the robustness against

attacks [33]. Amnesh et al, proposed contrastive methods to encrypt images by introducing a new image encryption method which first rearranges the pixels within image on basis of RGB values and then forward intervening image for encryption [34].

V. TRANSPOSITION SPIRAL METHOD

The security of images has attracted more attention recently, and many different image encryption methods have been proposed to enhance the security of these images. Image encryption techniques try to convert an image to another one that is hard to understand. There are various image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types.

The proposed method depicts a typical cryptographic system based on classical encryption techniques i.e. substitutions and transpositions and they are regarded as building blocks for encryption [38]. Transposition technique changes the order of the pixel in image [36]. This cipher just changes the order of the pixel with another pixel in the same image [35]. Such encrypt image could be transmitted across a network or stored within a file system with the objective of providing confidentiality [4]. A transposition cipher keeps the same image, but rearranges their order according to a specific algorithm. You still write the image in row and columns, but instead of reading of the pixel secret image normaly, you read it by using a predetermined pattern. In this research we present transposition pixel by spiral method.

Often the transposition method is of a geometrical nature. Matlab [37] is a matrix based mathematical programming language and widely used in fields such as engineering and the computer sciences including image processing. In this transposition cipher spiral, the image is written pixel (row, column) as matrix of image [38], but is read row and column in a specific order depending on a method and direction. To accomplish this algorithm must follow the following steps:

- Convert the fingerprint image to square image N*N.
- Determine the first pixel to read, for example (1,1) or (1, n) or (n,1) or (n,n).
- Determine the encrypt method, to encrypt the image from outside the image to inside the image (OtI for example from (1,1) pixel to (N/2 , N/2) pixel), or an inverse (ItO).
- Determine the direction, to encrypt the image by clockwise or anticlockwise.

For an example, if we try to encrypt the fingerprint image by using OtI from (1,1) pixel and clockwise as shown in Figure 2. Minimum and maximum coordinates on the spiral method are used to determine the number of rows and columns for the encrypt the image.

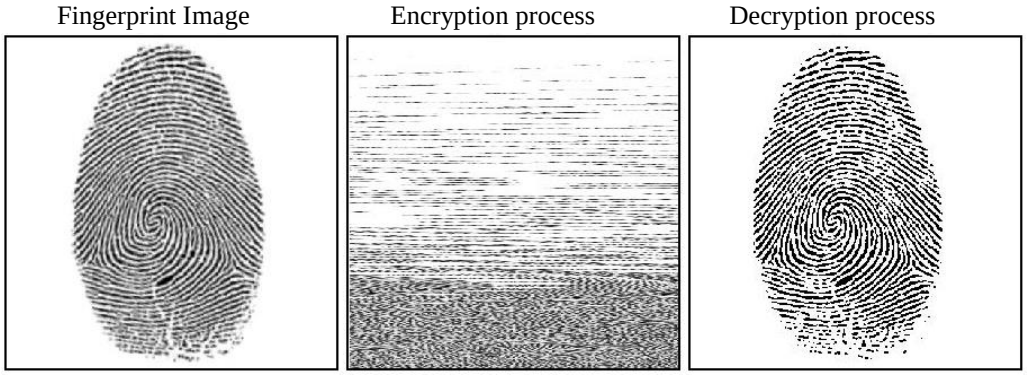


Figure 2. Encrypt and Decrypt process.

VI. PROPOSED METHOD

To enhance the embedding capacity of image steganography and provide an imperceptible hide-image for human vision. Proposed method introduces a method for hiding fingerprint in landscape image by combining cryptography and steganography. The main idea of this method is to use the new algorithm to encrypt the image then cover it by using LSB technique. In this method, there were no changes of the bit values of the original images. Therefore there was no change in the total size of the image during encryption and decryption process.

The first step in this method, encrypt the image by using transposition cipher by spiral method (by using function (Image2Spiral) proposed) and then embed this image inside another image by using LSB technique. The resulting the hide-image can be transmitted without revealing that secret information is being exchanged. The original image is recovered by using inverse LSB technique and then use the inverse of the encryption process (by using function (Spiral2Image) proposed). This approach is illustrated in details in the following steps (algorithm):

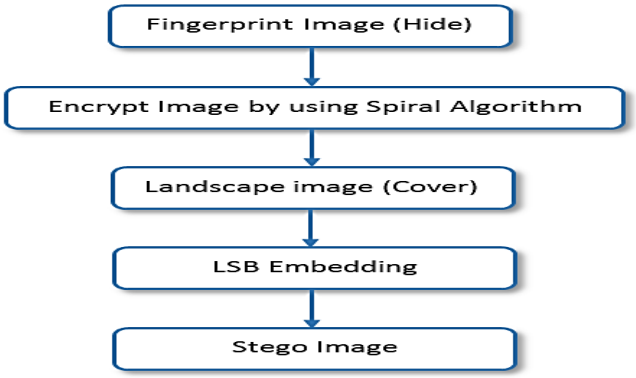


Figure 3. Block Diagram for the Encryption and Embedding process.

The Algorithm:

Step 1. Import data from secret fingerprint image (hide).

Step 2. Extract the secret image size (row, column).

Step 3. Determine the first pixel to read image.

Step 4. Determine the encrypt method, to encrypt the image from outside to inside (O2I), or an inverse (I2O).

Step 5. Determine the direction, to encrypt the image by clockwise or anticlockwise.

Step 6. Apply encryption algorithm (Apply Image2spiral).

Step 7. Import data from Landscape image (Cover).

Step 8. Resize the Landscape image (row, column) to the same size secret image.

Step 9. Apply LSB (Landscape image and the secret image).

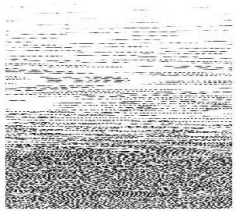
Step 10. Finally the image will be converted into stego-image format.

The inverse of the algorithm will decrypt the encrypted image back into the secret fingerprint image.

VII. EXPERIMENTAL RESULTS

In this research we would be obtaining our results by hide and encryption fingerprint image in simulating the image processing in MATLAB for better security. A comparative analysis is made to demonstrate the effectiveness of the proposed method by computing Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR) [39]. In proposed method, firstly we would be obtaining the matrix and pixels of the chosen image and then we would be encrypting the image using spiral algorithm. The result shows the fingerprint image, encrypted image and the decrypted image as shown in Table 1. We will clearly see that the decrypted image is same as the original image.

Table 1. Fingerprint Image before and after Encryption.

Fingerprint Image	Fingerprint Image	Encrypted Image	Decrypted Image
Fingerprint Image 1			
Fingerprint Image 2			
Fingerprint Image 3			

After enciphering the fingerprint image, these encrypted image are embedded in JPG image file by using LSB steganographic technique. In order to minimize the visible effect of changes to pixel values, the value of PSNR of stego image must be as high as possible. The MATLAB code for the spiral algorithm was written and tested. They are used three landscape with three fingerprint images in simulation proposed method as in Table 2. From Table 2 cannot observation the change between cover image and stego image.

Table 2. Cover and Stego image.

Cover Image	Cover Image	Stego Image
Cover Image 1		

Cover Image 2	 
Cover Image 3	 

To analyze the quality of the embedded texture image, with respect to the original, the measure of PSNR has been employed [39]. Generally speaking, when the payload increases, the MSE will increase, and this will affect the PSNR inversely [39]. So, from trade-off it was found that MSE decrease causes PSNR increase and vice-versa. PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values falling below 30 dB indicate a fairly low quality, i.e., distortion caused by embedding can be obvious; however, a high quality stego-image should strive for 40 dB and above [39]. Our results indicate that embedding process introduces less perceptual distortion and higher PSNR [40]. The obtained results of the experiments are summarized in the Table 3.

Table 3. MSE and PSNR values for the Cover and Stego images.

Fingerprint Image size (Before Encryption)	**Fingerprint Image size (After Encryption)**	**MSE**	**PSNR**
Fingerprint image 1 (62.1 kb)	Fingerprint image 1 (52.9 kb)	0.4212	55.7968
Fingerprint image 2 (58.3 kb)	Fingerprint image 2 (51.7 kb)	0.4150	55.8610
Fingerprint image 3 (79.5 kb)	Fingerprint image 3 (64.6 kb)	0.4384	55.6225

To measure the distortion introduced by the embedding in the cover-image, the PSNR after embedding was observed for some images. It was found that the PSNR is constantly above 55 dB as seen in Table 3 which means that the quality degradations could hardly be perceived by a human eye.

VIII. CONCLUSION

Steganography is not a good solution to secrecy, but neither is encryption. But if these methods are combined, we will have two layers of protection. If a fingerprint image is encrypted by transposition spiral algorithm and hidden with a LSB steganographic method thus we can hide large volume of data. In this paper, we described well known steganographic techniques used to hide image in stego image that use the least significant bit insertion method. This paper presents a spiral algorithm for encryption fingerprint image and embed in color image. The swapping of fingerprint image pixel has increased the security of the image against all possible

attacks available currently. The main focus of the paper is to develop a system with extra security features where a meaningful piece of image can be hidden by combining two basic data hiding techniques. The method can further be extended with taking into account other data hiding and encryption techniques. The proposed method satisfies the requirements such as capacity, security and robustness which are intended for data hiding. The obtained experimental results show that, the proposed method will be a good and acceptable.

REFERENCES

[1] Raphael, A. J. and Sundaram, V. "*Cryptography and Steganography – A Survey*", Int. J. Comp. Tech. Appl., Vol 2 (3), pp. 626-630 , ISSN:2229-6093.

[2] S. Craver, *On Public-key Steganography in the Presence of an Active Warden*, IBM Research Report RC 20931, July 23, 1997.

[3] Nicolas Courtois, Josef Pieprzyk, "*Cryptanalysis of Block Ciphers with Overdefined Systems of Equations*". pp267–287, ASIACRYPT 2002.

[4] Younes, M.A.B. and Jantan, A. (2008), "*Image Encryption Using Block-Based Transformation Algorithm*" International Journal of Computer Science, Vol. 35, Issue.1, pp.15-23.

[5] Pia Singh , Karamjeet Singh "*IMAGE ENCRYPTION AND DECRYPTION USING BLOWFISH ALGORITHM IN MATLAB*", International Journal of Scientific & Engineering Research, Vol 4 (7), pp 150-154, July-2013.

[6] D.Stinson, "*Cryptography: Theory and Practice*", second edition, CRC Press, Boca Raton, 1995.

[7] Abraham Sinkov, "*Elementary Cryptanalysis: A Mathematical Approach"*, Mathematical Association of America, 1966. ISBN 0-88385-622-0.

[8] Kester, Quist-Aphetsi. *"A cryptosystem based on Vigenère cipher with varying key."* International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 1, no. 10 (2012): pp-108.

[9] Visual cryptography retrieved from: http://en.wikipedia.org/wiki/Visual_cryptography.

[10] M. Salleh, S Ibrahim and I.F. Isnin, *"Image encryption algorithm based on chaotic mapping"*, Jurnal Teknologi, 39(D) Dis. 2003: 1–12 Universiti Teknologi Malaysia.

[11] Petitcolas, F.A.P., Anderson, R. J. and Kuhn, M.G. (1999) *"Information Hiding -A Survey"*, Proceedings of the IEEE, Special issue on Protection of Multimedia Content, vol. 87, no. 7, pp.1062-1078.

[12] W. Bender, D. Gruhl, N. Morimoto, A. Lu, "*Techniques for Data Hiding"*, IBM Systems Journal v 35 no 3-4 (96) pp 313-336.

[13] Laskar, S.A. and Hemachandran, K. (2012), *"An Analysis of Steganography and Steganalysis Techniques"*, Assam University Journal of Sscience and Technology, Vol.9, No.II, pp.83-103, ISSN: 0975-2773.

[14] Samer H. Atawneh, *"A New Algorithm for Hiding Gray Images using Blocks"*, the proceedings of ICTTA '06: IEEE - 2nd International Conference on Information & Communication Technologies: From Theory to Applications, Damascus, Syria, 24-28 April, 2006, ISBN: 0-803-9521-2.

[15] Kharrazi, M., Sencar, H. T. and Memon, N. (2004), *"Image Steganography: Concepts and Practice"*, WSPC/Lecture Notes Series: 9in x 6in, pp.1-31.

[16] Chandramouli, R. and Menon, N. (2001), *"Analysis of LSB based image steganography techniques"*, IEEE Proceedings on Image Processing, Vol.3, pp.1019-1022.

[17] Tiwari, N. and Shandilya, M. (2010), *"Evaluation of Various LSB based Methods of Image Steganography on GIF File Format"*, International Journal of Computer Applications (0975 – 8887) Vol. 6, no.2, pp.1-4.

[18] Deshpande, N., Kamalapur, S. and Daisy, J. (2006), *"Implementation of LSB steganography and Its Evaluation for Various Bits"*, 1st International Conference on Digital Information Management, pp.173-178.

[19] J. Fridrich and M. Goljan, *"Digital image steganography using stochastic modulation"*, SPIE Symposium on Electronic Imaging, San Jose, CA,2003.

[20] Kevin Curran, Karen Bailey, "An Evaluation of Image Based Steganography Methods", International Journal of Digital Evidence, Fall 2003 Volume 2, Issue 2.

[21] R., Chandramouli, and Nasir Memon.(2001), "Analysis of LSB based image steganography techniques." In Image Processing, 2001. Proceedings. 2001 International Conference on, IEEE, vol. 3, pp. 1019-1022.

[22] Karen, Bailey, and Kevin Curran.(2006) "An evaluation of image based steganography methods" Multimedia Tools and Applications, Springer Vol.30, no. 1, pp. 55-88.

[23] E. Franz, A. Jerichow, S. Moller, A. Pftizmann, I. Stierland, "*Computer Based Steganography"*, in Information Hiding, Springer Lucture Notes in Computer Science v 1174 (1996) pp 7-21.

[24] B. Pfitzmann, "*Information Hiding Termonology"*, Proc. First Int'l Workshop Information Hiding. Lecture Notes in Computer Science No. 1,174, Springer- Verlag, Berline, 1996, pp. 347-356.

[25] Mamta Juneja, Parvinder Singh Sandhu, *"Designing of Robust Image Steganography Technique Based on LSB Inssertion and Encryption",* 2009 IEEE.

[26] V. Lokeswara Reddy, A. Subramanyam, P. Chenna Reddy, *" Implementation of LSB Steganography and its Evaluation for Various File Formats"*, Int.J.Advanced Networking and Applications, Volume: 02, 2011.

[27] Neha Sharma, Mr.J.S.Bhatia, Neena Gupta, *"An Encrypto Setgo Technique based secure data transmission system"*, PEC, Chandigarh, May, 2005.

[28] Krishnan, G.S.; Loganathan, D.; , "*Color image cryptography scheme based on visual cryptography,"* Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011 International Conference on , vol., no., pp.404-407, 21-22 July 2011.

[29] Christy, J.I.; Seenivasagam, V.; , *"Construction of color Extended Visual Cryptographic scheme using Back Propagation Network for color images,"* Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on , vol., no., pp.1101-1108, 21-22 March 2012.

[30] Kester, Quist-Aphetsi; , *"A public-key exchange cryptographic technique using matrix,"* Adaptive Science & Technology (ICAST), 2012 IEEE 4th International Conference on , vol., no., pp.78-81, 25-27 Oct. 2012.

[31] Kester, Quist-Aphetsi; Koumadi, Koudjo M; , *"Cryptographie technique for image encryption based on the RGB pixel displacement,"* Adaptive Science & Technology (ICAST), 2012 IEEE 4th International Conference on , vol., no., pp.74-77, 25-27 Oct. 2012.

[32] Shujiang Xu,Yinglong Wang,Yucui Guo,Cong Wang, *"A Novel Image Encryption Scheme based on a Nonlinear Chaotic Map"*, IJIGSP, vol.2, no.1, pp.61-68, 2010.

[33] Ruisong Ye,Huiqing Huang, *"Application of the Chaotic Ergodicity of Standard Map in Image Encryption and Watermarking"*, IJIGSP, vol.2, no.1, pp.19-29, 2010.

[34] Amnesh Goel,Nidhi Chandra,"*A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based On Sorting Group-Wise Of RGB Values and Explosive Inter-Pixel Displacement"*, IJIGSP, vol.4, no.2, pp.16-22, 2012.

[35] Sokouti, M., Sokouti, B. and Pashazadeh, S. (2009), *"An approach in improving transposition cipher system"*, Indian Journal of Science and Technology, Vol.2 No. 8, pp. 9-15, ISSN: 0974- 6846.

[36] Giddy, J.P. and Safavi- Naini, R. (1994), *"Automated Cryptanalysis of Transposition Ciphers"*, The Computer Journal, Vol.37, No.5, pp. 429-436.

[37] Mathworks, 2014 Website: http://www.mathsworks.com.

[38] Kahate, A. (2008), "*Cryptography and Network Security*", 2nd Edition, Tata McGraw-Hill.

[39] Kaur, R., Singh, B. and Singh, I. (2012), "*A Comparative Study of Combination of Different Bit Positions In Image Steganography*", International Journal of Modern Engineering Research, Vol.2, Issue.5, pp-3835-3840.

[40] Ulutas, G., Ulutas, M. and Nabiyev,V. (2011), *"Distortion free geometry based secret image sharing"*, Elsevier Inc, Procedia Computer Science 3, pp.721–726.

