NEW STEGANOGRAPHY CONCEPT WITH SYMMETRIC ENCRYPTION

Swati Gupta[1], Gajendra Singh[2], Kailash Patidar[3]

[1]PG Student, [2]HOD, [3]Assistant Professor
Department of CSE, SSSITS, Sehore, M.P. (India)

ABSTRACT

This Paper falls under the scope of "Information Image Hiding". The objective of this paper is to provide a secret and secured communication between users. This proposed concept of steganography initially encrypts the color image (that contains the secret image) using the proposed design encryption algorithm and hides the encrypted image in a cover image. So user on seeing the stego image is also cannot predict that there is something hidden information inside it. Thus the concept mainly has three phases. The first phase is the Displacement Phase which deal with the process of changing the original position of pixel of the confidential image by using horizontal, vertical, reverse and diagonal displacement process. The second phase is the Encrypting Phase, which deals with the process of converting the actual secret image into cipher image using the self design encryption algorithm. The Third phase is the Embedding Phase, where the cipher image is embedded into the cover image. This proposed concept uses the standard LSB (Least Significant Bit) technique. Here bits of the cipher image are replaced by the LSBs of the pixel values of the cover image. When the LSBs are alone changed then normal human eyes cannot predict in easily way the difference between the resulting image and original image. Also the algorithm used in the encryption process is the self design Encryption Algorithm. The proposed algorithm uses keys of higher size (128 bits) than its predecessor, so this will ensure higher security.

Keywords: - Cryptography, Decryption, Encryption, Internet, Steganography, Security

I INTRODUCTION

In digital Communication, security and privacy is problematic and challenging task. Privacy priority can be differs from user to user and their needs. Various techniques have been investigated and design to protect confidential privacy. Cryptography can be the best one of them and then steganography comes. The word steganography referred to the covert communications art [11, 12].The aim of steganography is to hide information into a cover media, such as digital image, audio and video. Among evaluation criterions for steganography, the most important are imperceptibility and embedding capacity, that is to say, the stego media should be visually and statistically similar to the corresponding cover media under certain payload. Certainly, these two properties are contradictory. On the other hand, steganalysis aims to discover the existence of hidden secret information in the stego media. Universal blind

detection is an important method in image forensics, and the essence of it is a statistical classified problem of original image and stego image. And the focus is finding some effective features to classify the two classes of images. According to the embedding positions, steganography is generally categorized into spatial and transform domain methods. Least-significant-bit substitution (LSB) [12], only the LSB plane of the cover image is overwritten with the information bits, is a well-known and large capacity spatial method. The secret information is often encrypted before embedded, so it can be seen as random distributed bit stream of 0 and 1. Thus, LSB replacement happening to the whole image will produce structural asymmetry which can be analyzed using histogram analysis such as the Chi-squared attack [12] or regular/singular groups (RS) analysis [13].

II RELATED WORK

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data [9].

In [1] I have observed that authors propose an approach for Image steganography based on LSB using X-box mapping where they have used several Xboxes having unique data. The embedding part is done by Steganography algorithm where they use four unique X-boxes with sixteen different values (represented by 4-bits) and each value is mapped to the four LSBs of the cover image. In [2] we have observed that a technique for image steganography based on Huffman Encoding is presented. In which two 8 bit gray level image of size M X N and P X Q are using as a cover image and secret image respectively. Huffman Encoding is performing over the secret image/message before embedding and each bit of Huffman code of secret image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. The size of the Huffman encoded bit stream and Huffman Table are also embedding inside the cover image. In [3] secret sharing refers to a method of distributing a secret among a group of participants, each of whom is allocated with a share of the secret. The participant's shares are used to reconstruct the secret. Single individual participants share is of no use. The reversible image sharing approach and threshold schemes are used achieve the novel secret color image sharing. The secret color image pixels will be transformed to m-ary notational system. The reversible polynomial function will be generated using (t-1) digits of secret color image pixels. Secret shares are generated with the help of reversible polynomial function and the participant's numerical key. The secret image and the cover image is embedded together to construct a stego image. The reversible image sharing process is used to reconstruct the secret image and cover image. The secret is obtained by the lagrange's formula generated from the sufficient secret shares. Quantization process is applied to improve the quality of the cover image. Peak signal to noise ratio is applied to analyze the quality of the stego images. The simulation results show that the secret and cover are reconstructed without loss [3]. In [4] we have analyzed that author proposes three indigenous methods as a variant of Cipher Block Chaining (CBC) mode for image encryption by considering three different traversing paths (Horizontal, Vertical and Diagonal). In method one simple Raster Scan has been employed to scramble the confidential Image

called Horizontal Image Scrambling (HIS). Method two is a variant of method one called Vertical Image Scrambling (VIS), here traversing path would be top to bottom left to Right. Third method employs diagonal traversing path called Diagonal Image Scrambling (DIS). Later Image Steganography has been adapted to send these Scrambled Images in an unnoticeable manner.

In [5] a tutorial review of the steganography techniques appeared. Various image steganography techniques have been proposed. In this we investigate of founded steganography techniques and steganalysis techniques. We state a set of criteria to analyze and evaluate the strengths and weaknesses of the previous techniques. The least-significant bit (LSB) insertion method is the most common and easiest method for embedding messages in an image with high capacity, while it is detectable by statistical analysis such as RS and Chi-square analyses. In [6] focused on the combination of cryptography and steganography methods and a new technique – Metamorphic Cryptography has suggested. The message is transformed into a cipher image using a key, concealed into another image using steganography by converting it into an intermediate text and finally transformed once again into an image. Hence, in [7] described and reviewed the different research that has done toward text encryption and description in the block cipher. Moreover, in this suggests a cryptography model in the block cipher. There are many security issues in data communication. Cryptography is a substantially safe method to provide protection in data receiving and sending. In [8] expressed a novel algorithm of data hiding using cryptography named as ASK algorithm. Sensitive data is hided in a color image using cryptography. This shows how data can be send using a color image without ignorance of third party. Algorithm described a method for vanishing data in a color image.

III PROPOSED CONCEPT

This proposed concept of steganography initially encrypts the color image (that contains the secret image) using the proposed design encryption algorithm and hides the encrypted image in a cover image. So user on seeing the stego image is also cannot predict that there is something hidden information inside it. Thus the concept mainly has three phases. The first phase is the **Displacement Phase** which deals with the process of changing the original position of pixel of the confidential image by using horizontal, vertical, reverse and diagonal displacement process. The second phase is the **Encrypting Phase**, which deals with the process of converting the actual secret image into cipher image using the self design encryption algorithm. The Third phase is the **Embedding Phase,** where the cipher image is embedded into the cover image. This proposed concept uses the standard LSB (Least Significant Bit) technique. Here bits of the cipher image are replaced by the LSBs of the pixel values of the cover image. When the LSBs are alone changed then normal human eyes cannot predict in easily way the difference between the resulting image and original image. Also the algorithm used in the encryption process is the self design Encryption Algorithm [9, 10]. The proposed algorithm uses keys of higher sizes (128 bits) than its predecessor, so this will ensure higher security. Thus this proposed concept will ensure a more secured communication in unsecured networks.

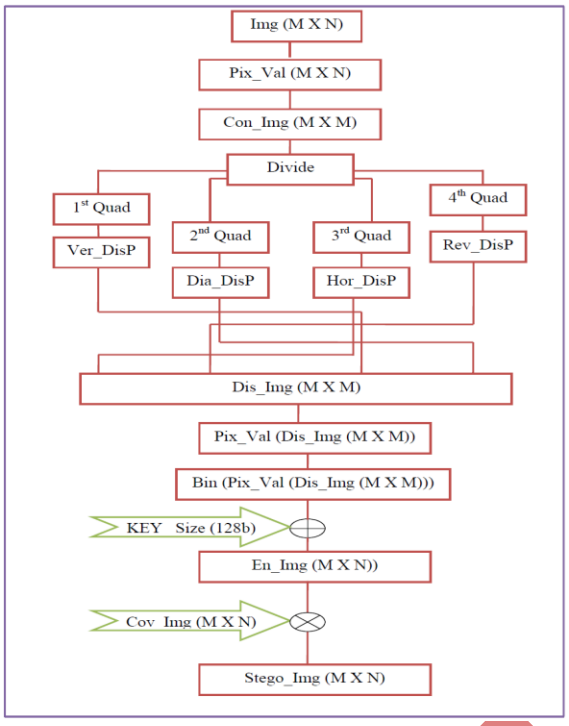


Fig 1: Block Diagram of Proposed steganography at one side

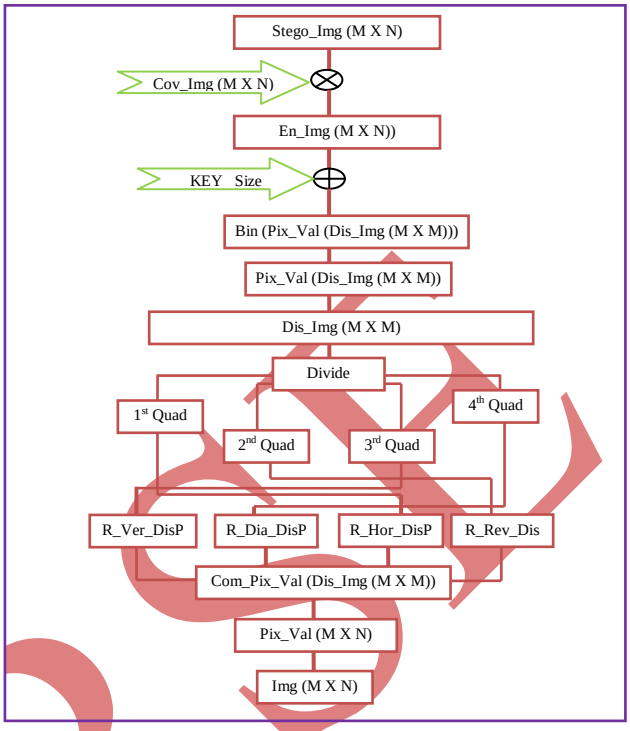


Fig 2: Block Diagram of Proposed Steganography at another Side

3.1 Proposed Divide and Displacement Approach

Fig 3 is showing the general view of proposed divide and displacement process for a confidential image. Initially confidential image of size "MXN" will be converting into size of MXM then it will divide into four equal sub parts as shown in Fig 3. After that displacement process will apply on each sub part of the image individually. In this total four type of displacement has used. One is vertical displacement, this type of displacement applying on the first sub part of the confidential image where pixel of the image is moving toward in upward direction. Second is diagonal displacement, this type of displacement applying on the second sub part of the confidential image where pixel of the image moving toward in diagonal left or diagonal right direction. Third is horizontal displacement, this type of displacement applying on the third sub parts of the confidential image where pixel of the image is moving toward in right or left directions? And fourth displacement is the reverse displacement, this type of displacement applying on the fourth sub part of the confidential image where all the pixel value of the image are moving in the reverse direction.

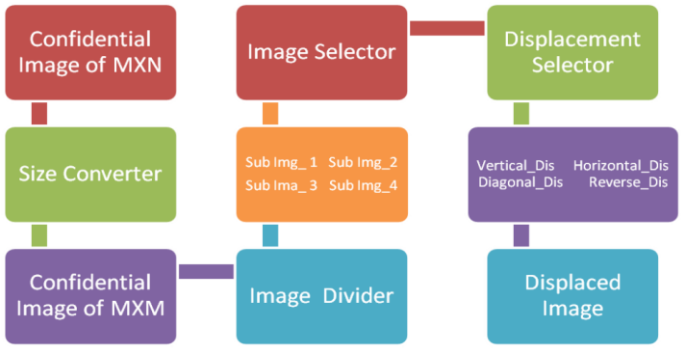


Figure 3: Divide and Displacement of Confidential Image Model

The details of each displacement process are defined below-

Process:

1. In Vertical Displacement moved the entire pixel two columns ahead.
2. In Horizontal Displacement moved the entire pixel two rows ahead.
3. In Diagonal Displacement interchange all the diagonal pixel red to green and green to red.
4. In Reverse Displacement reverse the image.
5. for ex if a image is of 20*20
    a. Replace pixel (1,1) with (20,20)
    b. Replace pixel (2,1) with (19,20) and so on.

For Example 1, 2, 3 …….14, 15, 16 are pixel value of the image and these values are changing during displacement process in following way.

Vertical Displacement of First Sub Part

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

9	10	11	12
13	14	15	16
1	2	3	4
5	6	7	8

Diagonal Displacement of Second Sub Part

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

4	2	3	1
5	7	6	8
9	11	10	12
16	14	15	13

Horizontal Displacement of Third Sub Part

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

3	4	1	2
7	8	5	6
11	12	9	10
15	16	13	14

Reverse Displacement of Fourth Sub Part

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

16	15	14	13
12	11	13	9
8	7	6	5
4	3	2	1

3.2 Proposed Encryption Approach

Architecture of the proposed encryption process is shown in Fig 4. In this architecture shuffling process are defining during encryption/decryption processing.

3.3 Proposed Decryption Approach

Architecture of the proposed decryption process is shown in Fig. 5. In this architecture shuffling process are defining during encryption/decryption processing.

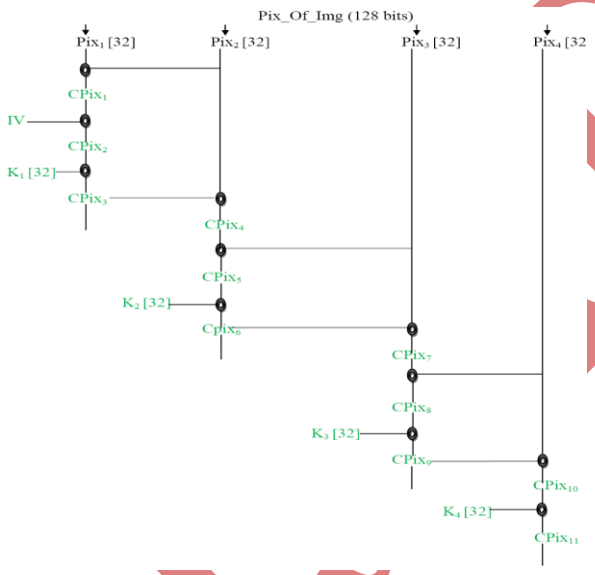


Figure 4: Architecture of Proposed Encryption

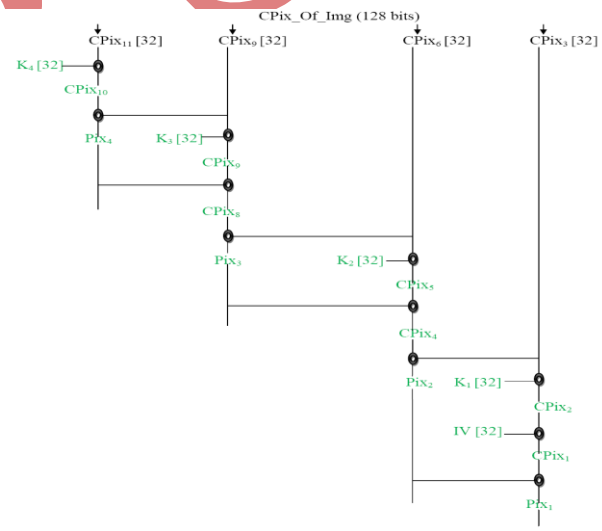


Figure 5: Architecture of Proposed Decryption

3.4 Algorithm Step

Proposed encryption algorithm Step are defining in section 3.5.1 and proposed decryption algorithm step are defining in section 3.5.2.

3.4.1 Algorithm of Proposed Encryption Algorithm

1. Read Pixel Value from Displaced Image

2. Read Binary value of pixels from displaced image.
3. Read 128 bits binary value sequentially.
4. Divide 128 bit binary value of displaced pixels into four equal sub parts of 32 bits each.
5. Input 128 bits value as a key (K)
6. Divide key (k) into four parts with equal in size. 32 bits each (K_1, K_2, K_3, K_4).
7. Input Initialization Vector IV of 32 bits.
8. Perform XOR between First part and Second part binary value of displaced image.
9. Perform XOR operation between Initialization Vector and output of 8^{th} step.
10. Perform XOR between first part of key value (K_1) and output of the step of 9^{th}.
11. Perform XOR between second part and output of 10^{th} step binary value as an Initialization Vector.
12. Perform XOR between output of 11^{th} step and third part binary value
13. Perform XOR between second part of key value (K_i) and output of the step of 12^{th}
14. Repeat step 11 to 13 for third and four sub part of displaced image except 12 step operation in fourth sub part. In each loop i will increase by 1.
15. For Initialization Vector (IV) in second, third and fourth sub part use output of 8^{th} step.
16. Repeat steps 1 to 11 for all displaced pixel in a displaced image.

3.4.2 Algorithm of Proposed Decryption Algorithm

1. Read Pixel Value from Encrypted Image
2. Read 128 bits binary value sequentially
3. Divide 128 bit binary value of encrypted pixels into four equal sub parts of 32 bits each.
4. Rearrange these sub part in following way

   Sub part 4 will become sub part 1

   Sub part 3 will become sub part 2

   Sub part 2 will become sub part 3

   Sub part 1 will become sub part 4
5. Perform XOR between first sub part of encrypted image and fourth sub part of K_4
6. Perform XOR between output of step 5^{th} and 2^{nd} sub part of encrypted image
7. Perform XOR between second sub part of encrypted image and third sub part of K_3
8. Perform XOR between output of step 6^{th} and output of step 7^{th}
9. Perform XOR between output of step 8^{th} and third sub part of encrypted image
10. Perform XOR between third sub part of encrypted image and second sub part of key K_2
11. Perform XOR between output of step 10^{th} and output of step 9^{th}
12. Perform XOR between output of step 11^{th} and fourth sub part of encrypted image
13. Perform XOR between fourth sub part of encrypted image and first sub part of key K_1

14. Perform XOR between output of step 13th and Initialization Vector (IV)
15. Perform XOR between output of step 14th and output step 12th
16. Repeat step 1 to 15 to all pixel value of encrypted image

3.5 Proposed Steganography Algorithm Steps

Proposed steganography algorithm steps at sender end is in section 3.2.1 and proposed steganography algorithm step at receiving end is in section 3.2.2.

3.5.1 Proposed Steganography Algorithm Steps

1. Select an Image as a Cover Image.
2. Select an Encrypted Image as a Confidential Image.
3. Read Pixel Value of Both Images.
4. Read Least Significant Bit (LSB) Pixel Value from Cover Image.
5. Replace LSB pixel Value with Encrypted Image Pixel Value to Form Stego Image.
6. Repeat step 1 to 5 to All Encrypted Pixel Value.

3.5.2 Proposed Reverse Steganography Algorithm Steps

1. Select an Image as a Stego Image.
2. Read Pixel Value of Stego Images.
3. Read Least Significant Bit (LSB) Pixel Value from Stego Image.
4. Combine All LSB pixel Value in One Array to Form Encrypted Image.
5. Repeat step 1 to 4 to All LSB Pixel Value.

IV RESULTS AND CONCLUSION

4.1 Performance Analysis

This section shows the results in which the efficiency and effectiveness of the proposed technique based on selected parameters proving. Selected parameter is entropy, histogram and Peek Signal to Noise Ration (PSNR) [1, 2, 3, 6]. In the experiments, the system encrypts/decrypt images. There are four parameters are calculating by the proposed system one is entropy, second is histogram and third and important parameter is peek signal to noise ratio (PSNR) and last one is execution time which is shown in table 2 and graph 1 The proposed system has run hundred times approximately. In each time, same images are respectively encrypted by existing algorithm and **"Proposed algorithm"**. Size of the selected key was same in each time. Finally, the outputs of the comparison system are

execution time, entropy, histogram and PSNR value which are noted in numeric form. For Results Evolution proposed system has selected three Input Images and one Cover Image which is shown in Table 1. In this Input Image-1having 47 X 23 pixels image where input image-2, 3 having 43 X 25, 57 X 39 pixels and the cover image-1 having 200 X 200 pixels.

Table 1: Input Images and Cover Image

Input Image -1,2,3	Cover Image -1
	

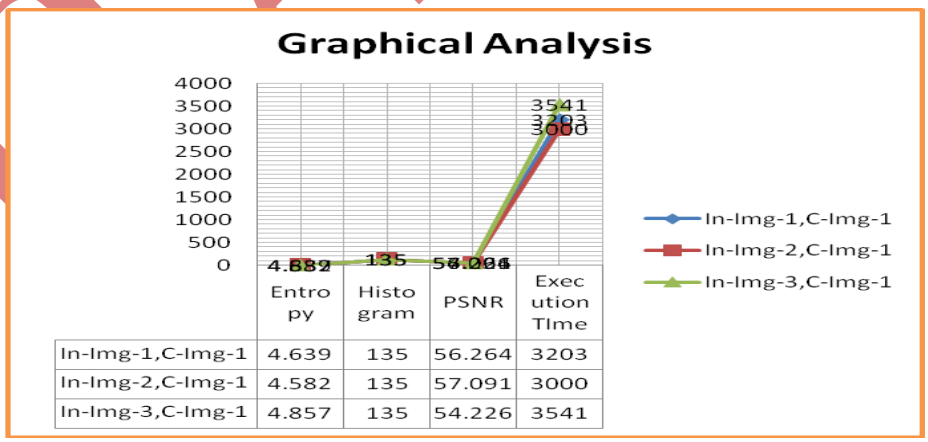
4.2 Encrypted Image Entropy

"The Proposed Algorithm" and existing algorithm have been implemented on a number of images varying types of content and sizes of a wide range. Encrypted image entropy of various images comparisons shown in table 5.2.

Table 2: Entropy, Histogram, PSNR, Execution Time Analysis of Stego Images through Proposed Algorithm

S. No.	Images	Entropy (Approx)	Histogram	PSNR	Execution Time
1	In-Img-1,C-Img-1	4.639	135	56.264	3203
2	In-Img-2,C-Img-1	4.582	135	57.091	3000
3	In-Img-3,C-Img-1	4.857	135	54.226	3541

GRAPH 1: Entropy, Histogram, PSNR, Execution Time Graphical Analysis of Stego Images through Proposed Algorithm



4.3 Results Analysis

During the result evolution it is seen and analyzed that calculated results through earlier techniques are batter in terms of PSNR, Execution time, Histogram, entropy. Table 2 and Graph 1 is showing the PSNR, Execution time, Histogram, entropy result evaluation for various images ie. Input Image -1 with Cover Image producing entropy is 4.639. Other parameters also like histogram is 135, PSNR is 56.264. Execution time is 3203 millisecond.

V CONCLUSION

Steganography is used for security. Steganography is complementary of cryptography which is used for images. Hiding image with suggested steganography technique reducing the detection chance of a secret/confidential image. Initially secret image are encrypting by the suggested encryption technique this is another level of protection with the help of this nobody can cracked the original information if it is discovered. There are an so many applications of steganography. This proposed work explores a small art of steganography technique. It work well simply LSB embedding secrete image pixels in a cover image. Suggested Steganography does not simply pertain to color images but it can also to other medial but this is our future work. In and of itself, suggested steganography is not a good solution to secrecy, but either is simple substitution and short blocking permutation for self design proposed encryption algorithm. But if these methods are combined, it has a much stronger encryption routines.

REFERENCES

[1] Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar "An Image Steganography Technique using X-Box Mapping" IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

[2] RigDas and Themrichon Tuithung "A Novel Steganography Method for Image Based on Huffman Encoding" IEEE 2012

[3] L.Jani Anbarasi and S.Kannan "Secured Secret Color Image Sharing With Steganography" IEEE 2012

[4] Rengarajan Amirtharajan\ Anushiadevi .R2, Meena .y2, Kalpana. y2 and John Bosco Balaguru "Seeable Visual But Not Sure of It" IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

[5] G.Karthigai Seivi, Leon Mariadhasan, K. L. Shunmuganathan "Steganography Using Edge Adaptive Image" IEEE International Conference on Computing, Electronics and Electrical Technologies [ICCEET] 2012

[6] Thomas Leontin Philjon. and Venkateshvara Rao. "Metamorphic Cryptography - A Paradox between Cryptography and Steganography Using Dynamic Encryption" IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011

[7] Ashwak M. AL-Abiachi, Faudziah Ahmad and Ku Ruhana "A Competitive Study of Cryptography Techniques over Block Cipher" UKSim 13th IEEE International Conference on Modelling and Simulation 2011

[8] Abhishek Gupta, Sandeep Mahapatra and, Karanveer Singh " Data Hiding in Color Image Using Cryptography with Help of ASK Algorithm" 2011 IEEE

[9] Guy-Armand Yandji, Lui Lian Hao, Amir-Eddine Youssouf and Jules Ehoussou RESEARCH ON A NORMAL FILE ENCRYPTION AND DECRYPTION" IEEE 2011

[10] Akhil Kaushik, AnantKumar and Manoj Bamela " Block Encryption Standard for Transfer of Data " IEEE International Conference on Networking and Information Technology 2010

[11] Rosziati Ibrahim and Teoh Suk Kuan "Steganography Algorithm to Hide Secret Message inside an Image" Computer Technology and Application 2 (2011) 102-108

[12] Danah boyd and Alice Marwick "Social Steganography: Privacy in Networked Publics" ICA 2011

[13] Luis von Ahn, Nicholas J. Hopper., Public-Key Steganography