Dynamic Key based LSB Technique for Steganography

Bhanupriya Katre
M.Tech Scholar
Dept. of Electronics and Communication
SISTech, Bhopal

Bharti
Assistant Professor
Dept. of Electronics and Communication
SISTech, Bhopal

ABSTRACT

Steganography refers to the branch of computer science which deals with the covering up message in the format which cannot be detectable by any intruder. The secret message or the confidential data can be sent over internet with security using various steganography techniques. This technique has overcome many drawbacks of traditional method of cryptography in which data is encoded and sent over the internet which can be seen by the intruders and they can make attack on it. It is possible for the intruder to make the intrusion sometimes when the cryptographic algorithm is not sufficient enough but in case of steganography no one knows except the receiver that the message sent is confidential or hidden in some kind of picture, audio or video. So it makes it lot secure to send the message over internet with the use of steganography. In the proposed paper the detail information of image steganography is presented along with the applications and methods used for this process.

Keywords

Stagnography, Cover image, Stego image, LSB, PSNR

1. INTRODUCTION

New technologies are growing very fast these days so security issues are on the boom. Many algorithms and methods are made to provide security to the information or message in the communication system. The data can be accessed by the authorized user for this reason the mechanism is build. Data transfer on internet is being done every day in form of thousands of messages from one place to another. So the prime concern of the user is its data security. The need is to send the message in such a way that no one else can read it accept the receiver[3]. Cryptography was the only technique before which was used to send the data from one person to another over communication network using Internet. In cryptography the message was encrypted using key by at the sender ends and decrypted at the receiver's end using the key. The only problem with cryptography is that the unauthorized user knows that the message has been sent using any encryption algorithm. So to overcome with this drawback of cryptography, steganography came in to light where the message is sent in a way different pattern that no one can understand that some important message is in that format [5]. Use of internet has increased over some decades and the transfer of data has also increased, there is rapid growth in the information and communication media which increase the demand of security in the communication network system. This demand of security encourages the researcher and software developers to develop some new techniques of security protection.

2. STEGANOGRAPHY

Steganography is the art of computer science which deals with the hiding or concealing of the text file, message, video or image with in another text file, image, video or message[1]. The word steganograph is derived from the Greek word which means 'covered writing'. Hiding of the message in steganography is done in such a way that the message is undetectable[3]. If the good capacity media is chosen in Steganography then the better results can be achieved in image quality. The main objective of steganography is to provide security to the communication. There are many techniques used to secure the data like cryptography but sometimes there is a need to secure the message in it so there used a technique known as steganography. Steganography are of different types applied to various media of communication which will be discussed in detail in this paper [1][2].

Steganography was first introduced in the year 1499 by Johannes Trithemiu. It was the time when the word is a combination of two: first 'Stegano' which means to COVERED and 'Graphos' which means to WRITE so the combination means covered writing. It is a very exclusive technique of covering data into different medium that there would be no awaken doubt to the intruders [2]. The main concept of the steganography is that the data sent is not detectable to anyone's eye except the receiver. The message in the steganography is embedded in the form of audio, video, image or text file. Invisible ink and microdots are the very conventional technique of steganography. There was also some methods in which the wooden tablets are used to send message covered with wax, the message was engrave in the wooden tablet[3].

2.1 Steganography Types

There are many steganography techniques depending upon the type of cover object which needs to be steganography. They are as follows [4][5]:

2.1.1 Network Steganography

In steganography where the network protocol like TCP, UDP, IP or ICMP are used as carrier to cover object is known as network steganography. In the unused bits of the header of TCP/IP steganography can be achieved[8].

2.1.2 Video Steganography

When the information is hiding or covered in the form of video is known as video steganography. In this steganography both the combination of image and audio is present. It covers the file or information into a digital format. Video format is used as a carrier in hiding the data. For each image in the video there uses a discrete cosine function transform (DCT) value from 8.667 to 9 to hide the information. Video formats used in video steganography are Mp4, MPEG, AVI, H.264 etc [8].

2.1.3 Audio Steganography

This is the technique in which the message is hidden in the audio format. Least Significant Bit (LSB) and Phase coding are the most popular audio steganography techniques. Audio is used a s carrier in this steganography and it has become more popular due to it VOIP (voice over IP) medium. The audio formats used in audio steganography are AVI, MIDI, WAVE, MPEG etc [11].

2.1.4 Text File Steganography

Hiding information or data in the form of text file is known as text steganography. It requires less memory storage as it stores only text files. The transfer of information from one system to another is very fast in this technique. It does not use the large amount of redundant data text file for hiding. Information hiding in text steganography is achieved by the general techniques like whitespaces, capital letters, number of tabs etc [5].

2.1.5 Image Steganography

Hiding of the data in the image format is known as image steganography. LSB is the most popular technique of image steganography used in which the original image cannot be changed. In these technique pixels intensity is used to hide the information [6].

3. GENERAL IMAGE STEGANOGRAPHY TERMS

General terminologies used in the image steganography are mentioned below[6][7].

- **Message**-

  In image steganography message is the general information or actual data which is used to be steganography, it can be a text file or anything in a specified format.

- **Cover Image**-

  This is the carrier image which is used in which the data or information will be hided.

- **Stego Image**-

  This is the image in which the message or actual information is hided and ready to be sent to desired location.

- **Stego Key**-

  This is just like the key used in cryptography which is used to extract the original or actual data from the stego image.

4. IMAGE STEGANOGRAPHY METHODS

It is the method in with the cover image is embedded with the information or message to be send and converted into stego image. This stego image is now be ready to send to the receiver along with the stego key so that the message can be cracked by the receiver. There are various properties of the image steganography such as:

- Large amount of data can be embedded into the image that means it has a very high capacity.
- It is robust which means if the stego image is cropped or modified it should not affect the original message.
- It is a temper resistant that does not let intruder to alter the data once embedded into the stego image.
- Computational capacity of the image steganography is however low if the data is large and extracting of it needs time.

The various techniques used for image steganography are as follows[8].

4.1 Spatial Domain Technique

Every version of spatial domain technique of image steganography changes the image pixel value by some or all bits for hiding the message. The very simplest technique in this domain is Least Significant Bit (LSB) in which the value of the pixels change without many distortions. The human eye cannot see that imperceptible changes [9]. The main advantage of using spatial domain technique in image steganography is that a large amount of data can be stored in the image and original message cannot be degraded easily in this method. But there are some limitation to this method as the data can be lost if the image is manipulated in the LSB technique and the data can easily be destroyed by very simple attacks or intrusions[10]. The broad classification of the spatial domain methods are as follows:

a. Least Significant Bit (LSB)

b. Edges Based Data Embedded Method (EBE)

c. Pixel Value Differencing (PVD)

d. Mapping Pixel to Hidden Data Method

e. Labeling or Connectivity Method

f. Histogram Shifting Method (HSM)

g. Texture Based Method (TBM)

h. Pixel Intensity Based Methods (PIBM)

4.2 Transform/Frequency Domain Method

Covering or hiding the message in this method is more complex. There are various techniques and methods are built to provide the hiding of data into image. For the domain of embedding techniques, many algorithms and method has been suggested in the transform domain techniques [3]. Embedding data in the frequency domain is stronger rather that embedding the data in time domain signal. Most of the data in today’s system is embedded in the time or frequency domain of image steganography rather than spatial domain as it provides various advantages over spatial technique. In this technique the message or the actual data is hided in that part of the image which is less exposed to cropping, compression and processing. Transform or frequency domain techniques can further be classified into following groups.

a. Discrete Fourier Transformation Technique (DFT)

b. Discrete Wavelet Transformation Technique (DWT)

c. Discrete Cosine Transformation Technique (DCT)

d. Discrete Fourier transformation technique (DFT)

e. Embedding in Coefficient Bits

f. Reversible Method or Lossless (DCT)

4.3 Distortion Technique

The message knowledge of the cover image is need by the distortion technique of image steganography method during the decrypting process [1]. The decoder function checks the difference between the cover image and stego image to restore the secrete information or message. In the cover image, the encoder adds the sequence of changes. So, the data or message is described by the signal distortion. This produced sequence of modifications in cover image is added in the stego image. To match the secret message in the stego object, the produced sequence of modification is used for transmitting the data[10]. The encoding of the data or message is done at the pseudo-randomly chosen pixels. The message or data at the given data pixel bit is "1" if the stego image is different from the cover image and "0" is the difference is same. But there is a limitation to the benefits if the cover image is send along the stego image. As in the other techniques of image steganography the cover image is not used more than once because if the intruder tries to modify, crop, rotate the image, it can be easily detected by the receiver. The original message can be recovered in some cases as the message or data if encoded with error correcting information or data[13].

5. FILTERING AND MASKING METHOD

In this technique the paper watermark kind of logic is used in which image is marked in the same way. This technique does not hide the information in the noise are but in the more significant areas. In this technique the covered or hidden message is more integrated than the cover Image. Since the compression is lossy in this technique, the destruction of the image cannot be done in watermarking method [11]. There advantage of using watermarking techniques in masking and filtering is that it is more robust and secure than LSB in respect to compression as the data is hided in the invisible area of the image. This masking and filtering technique of image steganography technique has some limitations also which is that it can be applied only to the gray scale images and they are being restricted to 24 bits.

6. APPLICATIONS OF IMAGE STEGANOGRAPHY

There are various applications of image steganography, they are mentioned below [9][1]0:

- **Copyright Protection**-

  The secret message is embedded and hidden in the image which would be identified as the intellectual property or the watermark. This is in relating to the watermarking technique and the property is posses by the owner.

- **Secret Communication**-

  Image steganography provides secret communication between the sender and the receiver of the message which in cryptography is not present as the message sent there is encoded but not hidden.

- **Feature Tagging**-

  Name of the individuals, capitations or annotations even map can be tagged in the photo which can be sent to the receiver. In the stego image is copied, the information and tagging is also copied but the authorized user which has the stego key can extract the features out of it.

- **Digital Watermarking-**

  It is used in the steganograph image to verify the authenticity and integrity of the carrier signal message in the cover image. Digital watermark is embedded in the cover image. It is most commonly used for banknote authentication and copyright infringements.

7. LITERATURE SURVEY

The new Steganography algorithm is proposed in this paper in which compression mechanism is used to increase the capacity of the data to be hidden in the image. In this algorithm the text file is hided inside the image by compressing 1bit to 8 bit per pixel ratio. This method will be used to efficiently hide the user data [9]. There are various algorithms and techniques in image steganography which have been studied in this proposed paper. Steganography is the technique in which the message or data is hided in the image so that no one except the desired authenticate user can see it using stego key. In this paper detail overview of the steganography and its concepts has been discussed. All the method of steganography like image, video, audio and text steganography is explored which are used to embed the message in digital carrier. The quality of the stego image and the capacity of the cover image are the two most important things of image based steganography [11].

Importance to steganography gaining the exponential growth as the secret and confidential communication over the internet has been increased in few decades. It is an invisible mode of communication which deals with the hiding or covering of the confidential message. Data embedding in steganography is achieved in image, video, audio, voice or multimedia, communication, text file, military communication, authentication and content for copyright purposes. The secret communication in image based steganography is achieved by embedding the message in cover image and generating the stego image which is carrying the hidden message. All the techniques used for steganography along with the classification, applications and types are discussed in this paper [12].

Invisible communication with the help embedding the message into an image, video, audio or text file is known as steganography. The message cannot be attacked by intruders or attackers if the applied steganography is succussed. The main purpose of using steganography is to provide robustness and undetectability to the data which makes it hidden in other format. The factors effecting the steganography and comparison to various other techniques are studied in this paper and also the various method used for steganography [13].

Digital communication in the recent years has a rapid growth in the information technology branch, to provide security to the data and robustness various techniques are used and one of them recently very popular is steganography. Steganography deals with the embedded of data into another format for transmitted between sender and the receiver so that no one can detect the data or message in the very new format. Steganography can be done using various methods like image, video, audio, text and network steganography. In the presented paper new method for image steganography is introduced in which large amount of data can be hidden by use of secrete colour image. The proposed algorithm or method is based on two methods that is Different Size Image Segmentation (DSIS) and Modified Least Significant Bits (MLSB). The secret message is embed using DSIS instead of sequentially or randomly. The simulated result for the proposed algorithm shows that it provides high payload capacity [14].

Steganography means to hide the data in different format from the original one. The main objective of steganography is to cover the data behind the images. In steganography it means to encrypt the data in image form. Security is the main issue in sending the data over the Internet these days, for the communication between the sender and the receiver in the wireless communication network steganography plays a major important role for the confidential data to be sent with security. There are many techniques which are developed for this process of hiding or embedded the data in the image form in steganography which will be discussed in brief in this paper.

LSB-Hash, RSA encryption and decryption and various other algorithms are studied deeply in this paper [15].

Secret communication can be done with the help of steganography. In steganography the message in hidden in the form of image, video, text or network media which do not let anyone knows the actual message. It is the study of invisible communication which deals with covering or hiding of the data in different format. The message or data can be in the form of audio, video, text or image file. In image steganography the message is first embed in the cover image and then the stego image is produced to be sent to the receiver. The data is hided in such a way that no one can detect the hidden message. To decrypt or to get the original image or message out of stego image the key is used known as stego key. It is very similar to cryptography wher the message is encoded but in steganography instead of encode the message, it is hidden which provides more security and robustness to the message. In this paper briefly classification of steganography technique for hiding the data is proposed [16].

8. PROPOSED WORK

This section describes about the proposed algorithm along with the proposed flow chart. Figure 1 is showing the architecture of proposed encryption technique. Here secrete information dived into its binary value and at a time 128 bits block selected to perform operation during whole process. Now selected 128 bits value divide into two sub parts of 64-64 bits as a left and right sub parts respectively. Then apply series of operation like circular shifting (left and right) followed by XOR operation between selected dynamic key value and other sub part. The proposed work is having two parts. In first part, we are discussing about the key generation process as follows:

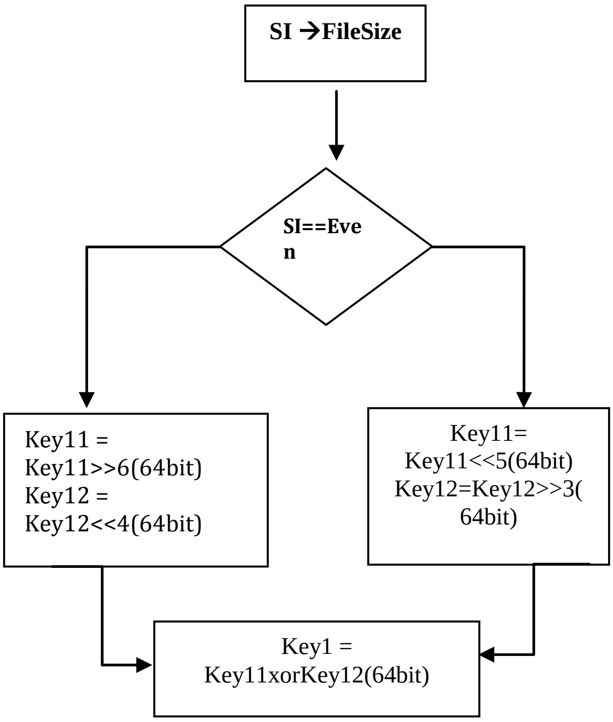


Figure 1: Key Generation of the proposed work

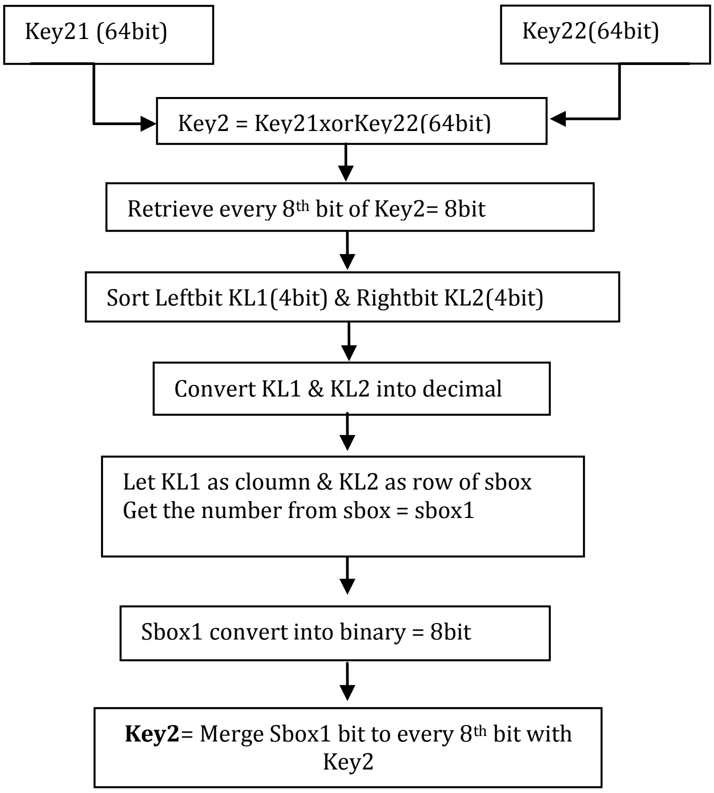

Key21 (64bit)
Key22(64bit)
Key2 = Key21xorKey22(64bit)
Retrieve every 8th bit of Key2= 8bit
Sort Leftbit KL1(4bit) & Rightbit KL2(4bit)
Convert KL1 & KL2 into decimal
Let KL1 as cloumn & KL2 as row of sbox
Get the number from sbox = sbox1
Sbox1 convert into binary = 8bit
Key2= Merge Sbox1 bit to every 8th bit with Key2

Figure 2: Steganography of the proposed work

1. Input Secret Image
2. Convert SI into binary
3. Measure file size
4. Input Alphanumeric Key Key11 of 8character 64bit
5. Input Alphanumeric Key Key12 of 8character 64bit
6. If File Size==even

Key11<< 6 Time Right Circular Shift
Key12>>4 Time Left Circular Shift
Key1 = xor (Key11,Key12)
  else
Key11>>5 Time Left Circular Shift
Key12<<3 Time Right Circular Shift
Key1 = xor(Key11,Key12)
End

7. Input Alphanumeric Key Key21 of 8character 64bit
8. Input Alphnumeric Key Key22 of 8character 64bit
9. KL1 = xor(Key21,Key22)
10. Key2 = KL1(8 16 24 32 40 48 56 64)
11. Half Key2 left and right
12. Bin2dec Key2 left & right
13. Key2 left as column and Key2 right as row
14. Get Key2 cordinate number from SBOX
15. Dec2bin SBOX output
16. Key2 (8 16 24 32 40 48 56 64)= SBOX output(1 2 3 4 5 6 7 8)
17. For loop i = 1: filesize/128

Divide SI quarterly
Divide Key1 & Key2 into half

18. SI1 = SI11>>5 xor Key11
19. SI2 = SI12<<3 xor SI1 xor Key11xorKey12
20. SI3 = SI21>>5 xor SI2 xor Key22
21. SI4 = SI22<<3 xor SI3 xor Key21 xor Key 22

22. Concanate SI bits
23. Apply Huffman Coding on SI bits
24. Loop End
25. Write Encrypted image
26. Input Cover Image
27. Merge Encrypted image with secret image with one bit sequence
28. Write stego image

9. RESULT ANALYSIS

We have taken two cover images. First cover image is of Lena and another cover image is of cape. These are shown in figure 4(a) and 4(b).

(A)

(B)

Figure 4: Cover images

2(A)

2 (B)

Figure 5: Stego images

Performance Evaluation

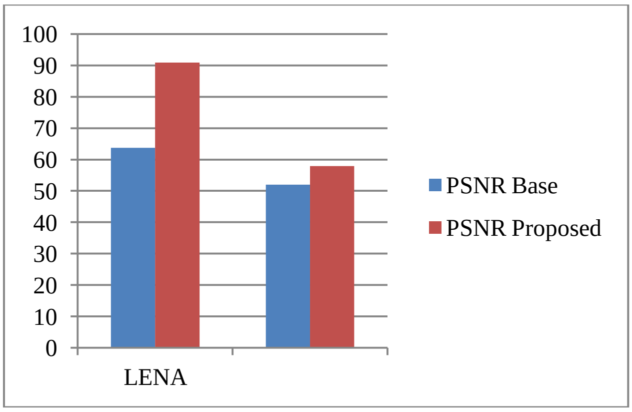
This section presents the Evaluated results through Existing as well as proposed technique by using selected performance parameters analysis. Analysis is done on Peek Signal to Noise Ratio (PSNR) analysis. There is text information which has selected to find Performance of the proposed system. During evaluation proposed system has run on number of several text and image information and captured overall performance on selected parameters like PSNR. Here results is based on selected cover Images which is cited above.

Peek Signal to Noise Ratio (PSNR) Analysis: PSNR is defined as assume that N is the total number of pixels in the input or output image, MSE (Mean Squared Error) is evaluated as

$$PSNR = 10log_{10}\frac{(L-1)^2}{MSE}$$

Table 1: Various Values Of PSNR of Various Images

	PSNR	
	Base	Proposed
LENA	63.7037	90.878
Cape	52.0359	57.8736



Graph1: Various Values of PSNR of various Images

The value of PSNR should be greater for the better of the output image quality

10. CONCLUSION

In this paper presented a detail review on Image Steganography. All the applications and algorithms or methods of image steganography are discussed in this paper. The paper also shows how steganography is better than various other methods used for secure communication over Internet. Steganography provides high standard security than cryptography in which message is encoded to be sent to the receiver where as in steganography the message is embedded in the cover image and sent to the receiver using stegno key to decrypt the stegano image. In this paper we have implemented the proposed work in MATLAB and verify the results. PSNR parameter to evaluate the performance of the proposed work.

11. REFERENCES

[1] G Prabakaran, R. Bhavani, P.S. Rajeswari, “Multi secure and robustness for medical image based steganography scheme” International Conference on Circuits, Power and Computing Technologies (ICCPCT), Publication Year: 2013 , Page(s): 1188 – 1193.

[2] N. Akhtar, ; P. Johri, ; S Khan, “Enhancing the Security and Quality of LSB Based Image Steganography” 5th International Conference on Computational Intelligence and Communication Networks (CICN), Publication Year: 2013 , Page(s): 385 – 390.

[3] R.P Kumar, V. Hemanth, M “Securing Information Using Sterganoraphy” International Conference on Circuits, Power and Computing Technologies (ICCPCT), Publication Year: 2013 , Page(s): 1197 – 1200.

[4] M.K Ramaiya. ; N.Hemrajani, A.K Saxena. “Security improvisation in image steganography using DES” IEEE 3rd International on Advance Computing Conference (IACC), Publication Year: 2013 , Page(s): 1094 – 1099.

[5] 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.

[6] L.Jani Anbarasi and S.Kannan “Secured Secret Color Image Sharing With Steganography” IEEE 2012.

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

[8] 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.

[9] RigDas and Themrichon Tuithung ”A Novel Steganography Method for Image Based on Huffman Encoding” IEEE 2012.

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

[11] Navdeep and Ms Neha Goyal, "Hide Text in Images Using Steganography and a Review of Methods and Approach for Secure Stegnography", IJRIM Volume 6, Issue 5 (May, 2016) (ISSN 2231-4334), International Journal of Research in IT & Management (IMPACT FACTOR – 5.96).

[12] Dr. Rajkumar L Biradar and Ambika Umashetty, "A Survey Paper on Steganography Techniques", International Journal of Innovative Research in Computer and Communication Engineering (A High Impact Factor, Monthly, Peer Reviewed Journal) Vol. 4, Issue 1, January 2016.

[13] Shikha Sharda and Sumit Budhiraja, "Image Steganography: A Review", International Journal of Emerging Technology and Advanced Engineering, (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 1, January 2013).

[14] Odai M. Al-Shatanawi and Nameer N. El. Emam, "A New Image Steganography Algorithm Based On Mlsb Method With Random Pixels Selection", International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.2, March 2015.

[15] Ashadeep Kaur, Rakesh Kumarand Kamaljeet Kaint, "Review Paper on Image Steganography", Volume 6, Issue 6, June 2016 International Journal of Advanced Research in Computer Science and Software Engineering.

[16] Divyanshu Triapthi, Yash Kumar Singh and Rohit Singh, "A Review on Digital Image Steganography with its Techniques and Model", IJSART – Volume 2 Issue 4– APRIL 2016 ISSN [ONLINE]: 2395-1052.