A Literature Review on Various Recent Steganography Techniques

Anupriya Arya
M-tech Student
Computer Science, BBAU Central University,
Lucknow, UP, India
anu.arya.0110@gmail.com

Sarita Soni
Assistant Professor
Computer Science, BBAU Central University,
Lucknow, UP, India
saritasoni90@gmail.com

Abstract—In this paper we review different Steganography techniques which not only hides the message behind the image but also provides security. Data is generally in the form of text, audio, video and image steganography algo can be applied to audio, video, and image file. Hiding secret information in image file is known as image steganography and in video file is known as video steganography. In tis paper have been discussed various techniques & steganography like spatial domain transform domain, vector embedding, and statistical technique, distortion technique, masking and filtering techniques.

Index Terms*—Steganography, Data hiding; Audio; Video; Text; spatial domain, transform domain, Security; LSB; Encryption, Cover writing.*

*****

I. INTRODUCTION

In recent trends in the world, the communication is the basic necessity of every growing area. The growth of modern communication technologies imposes a special means of security mechanisms especially in case of data networks. Everyone wants the secrecy and safety of their communicating data. Information security is a major issue of concern while exchanging a data in an open network, as internet is not only a single network it is worldwide collection of loosely network. The network security is becoming more important as the volume of data being exchanged over the Internet increases day by day. The two important techniques for providing security are cryptography and steganography. Both are well known and widely used methods in information security. Steganography and Cryptography both plays a very important role in information security [1].

In cryptography, the message is modified in an encrypted form with the help of encryption key which is known to sender and receiver only. The message cannot be accessed by anyone without using the encryption key. However, the transmission of encrypted message may easily arouse attacker’s suspicion, and the encrypted message may thus be intercepted, attacked or decrypted violently. In order to overcome the shortcomings of cryptographic techniques, steganography techniques have been developed. Steganography is the art and science of communicating in such a way that it hides the existence of the communication. Thus, steganography hides the existence of data so that no one can detect its presence [2]-[3].

In steganography the process of hiding information content inside any multimedia content like image, audio, video is referred as a “Embedding”. For increasing the confidentiality of communicating data both the techniques may be combined. So, steganography (hiding information) and cryptography (protecting information) are totally different from one another. Due to invisibility or hidden factor it is difficult to recover information without known procedure in steganography. Detecting procedure of steganography known as Steganalysis. Good imperceptibility and sufficient data capacity (efficiency of hidden information) are two properties which should be possessed by all the steganography techniques. Some shared secret – key known as Stego-key is used in steganography algorithm. *Figure (1)* Shows Block Diagram of Steganography

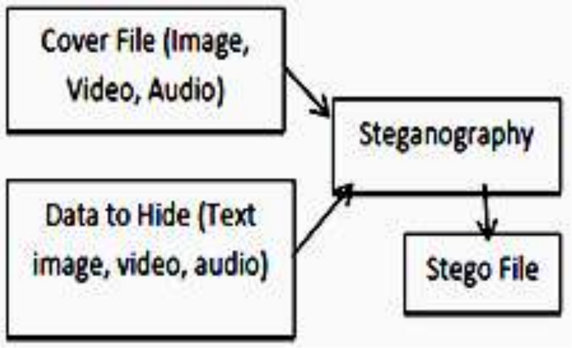
Cover File (Image, Video, Audio)
Data to Hide (Text image, video, audio)
Steganography
Stego File

Fig. 1 Block Diagram of Steganography

The survey was conducted on various steganography techniques which are very helpful and useful for providing better information security along with some cryptography techniques and some other techniques such as LSB, LSBM, LSBMR, SSHDT, RSTEG, OPA, Genetic-X mean algorithm, VSS, SDSS, FDSS, BPCS, GLM algorithm, SDS, Transform domain techniques, Distortion techniques etc. In this paper, includes the various papers on steganographic techniques. All the papers which are discussed in the literature review were taken from IEEE explore.

This paper is organized as follows: Section II discusses the concept and definitions regarding steganography with techniques. Section III presents the review of phase controlled of 3-phase IM drive. Section IV presents the summary of the paper. Section V presents the conclusion and future work of research work.

II. STEGANOGRAPHY OVERVIEW

Steganography is a Greek word which means concealed writing. The word “steganos” means “covered “ and “graphial “ means “writing”. The origin of steganography is the biological and physiological. The term “steganography” came into use in 1500’s after the emergence of Trithemius’ book on the subject “Steganographia”.. But today’s most of the people transmit the data in the form of text, images, video, and audio over the medium. In order to safely transmission of confidential data, the multimedia object like audio, video, images are used as a cover sources to hide the data The overview of steganography field can be divided into three parts in given table –I [4]-[5].

Table-I

Past	Present	Future
It’s very older origins can be traced back to 440 BC.	The majority of today’s steganographic systems uses the multimedia objects like image; audio; video etc	Nowadays, “Hacking” is very famous term
In early times, messages were hidden on back of the wax writing tables, written on the stomachs of the rabbits, or the tattooed on the scalp of slaves	Its cover media because people often broadcast digital pictures over email and other Internet communication	It is nothing but an unauthorized access of data which can be collected at the time of the data transmission
Invisible ink has been in use for centuries-for fun by children and students and for serious espionage by spies & terrorists [7].	in present world of steganography various steganographic techniques have been proposed	Steg analysis is a process in which a steganalyzers cracks the cover object to get the hidden data
Cryptography became very common place in the middle periods	There are certain cases in which a combination of Cryptography & Steganography is used to achieve data privacy over secrecy	It is hoped that Steganography along with Cryptography may improve the privacy as well as secrecy.

III. TYPES OF STEGANOGRAPHY

The various types of steganography include, Depending on the type of the cover object there are many suitable steganographic techniques discussed section-III-IV, which are followed in order to obtain security as shown in figure (2) [6]-[8].

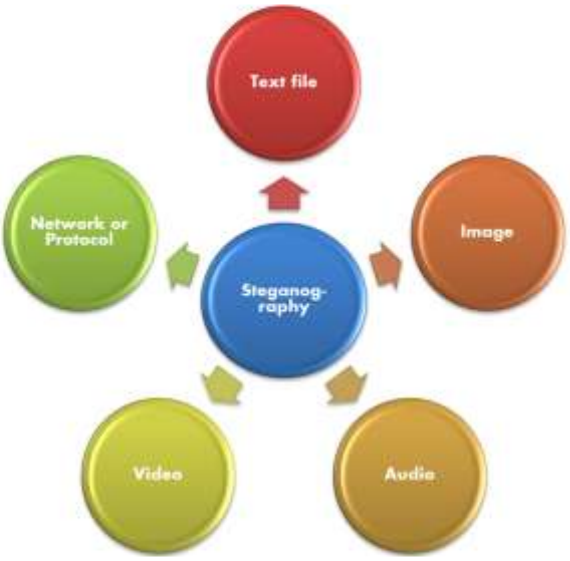

Fig. 2 Digital Medium to Achieve Steganography

3.1 Text file Steganography:

Secret Data is hided in a text file. In this method, the secret data is hidden behind every nth letter of every words of text message. Text steganography requires less memory as it can only store text files. It provides quick communication or transfer of files from one computer to another. Text steganography is not commonly used as text files containing large amount of redundant data. Numbers of methods are available for hiding data in text file. These methods are i) Format Based Method; ii) Random and Statistical Method; iii) Linguistics Method [8].

3.2 Image Steganography:

The process of concealing the secret message in an image file is known as image steganography, hiding the data by taking the cover object as image is referred as image steganography It has certain limitations like you cannot embed a large amount of data in an image because it may distort which may arise suspicion that the image might contain any information.. The conventional image steganography algorithm is LSB embedding algorithm.

3.3 Audio Steganography:

The method of hiding secret information in an audio is known as audio steganography. It is also very robust in nature but with limitation of the amount of data one can hide. This method hides the data in WAV, AU and MP3 sound files. There are different methods of audio steganography. These methods are

i) ***Low Bit Encoding*** **ii)** ***Phase Coding*** **iii)** ***Spread Spectrum.***

3.4 Video Steganography:

Steganography methods have mostly two types, spatial domain and frequency domain technique.

- ***Spatial Domain Based Method:***
- ***Transform Domain Based Method:***

The method of hiding secret information in a video is known as video steganography. In this case video (combination of pictures) is used as carrier for hiding the data. Generally discrete cosine transform (DCT) alter the values (e.g., 8.667 to 9) which is used to hide the data in each of the images in the video, which is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI are the formats used by video steganography.

3.5 Network or Protocol Steganography:

Network or protocol Steganography methods are uses Modification of a single network protocol. It involves hiding the information by taking the network protocol such as TCP, PDU (Protocol Data Unit), UDP, ICMP, IP etc, as cover object. It is highly secure and robust [8].

IV. TECHNIQUES OF STEGANOGRAPHY

There are various steganography techniques used based on the information to be hidden. In this paper we describe brief review of several image steganography techniques are as follows. *Figure 3* shows the various steganography techniques are broadly classified into different categories:

A. Spatial Domain Technique*:*

In spatial domain steganography method, for hiding the data some bits are directly changed in the image pixel values. Most used method in this category is least significant bit .Spatial domain techniques are classified into following [9]-[12]:

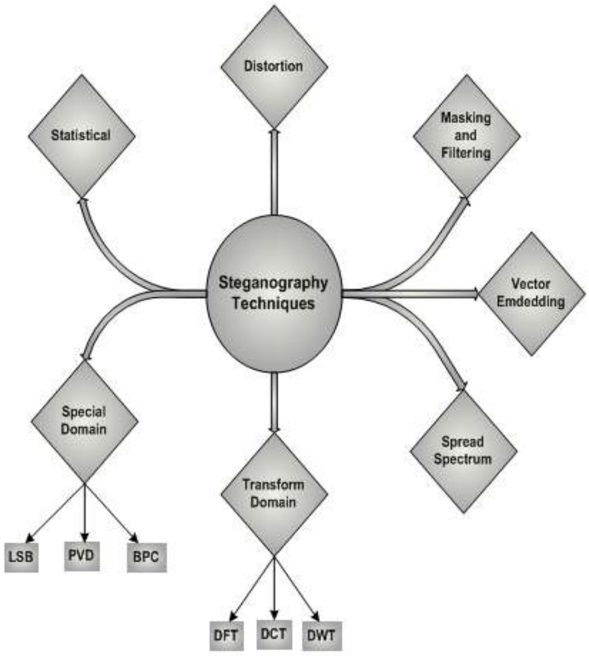

Fig. 3 Techniques of Steganography

a1. Least Significant Bit Insertion (LSB):

In this technique a simple approach to embedding is done by replacing the least significant bits of cover-image pixels with the bits of secret data. The image obtained after embedding is almost similar to original image because the change in the LSB of image pixel does not bring too much differences in the image.

a2. **Binary Pattern complexity (*BPC)*:**

In this segmentation of image are used by measuring its complexity. Complexity is used to determine the noisy block. In this method noisy blocks of bit plan are replaced by the binary patterns mapped from a secret data

a3. Pixel Value Differencing (PVD): In this method, two consecutive pixels are selected for embedding the data. Payload is determined by checking the difference between two consecutive pixels and it serves as basis for identifying whether the two pixels belongs to an edge area or smooth area.

B. Transform Domain Based Technique:

These techniques try to encode message bits in the transform domain coefficients of the image. Data embedding performed in transform domain is widely used for robust watermarking. Transform domain techniques are classified into various categories such as

b1. The Discrete Fourier Transform (DFT): *in this technique a* Discrete Fourier transform is the transform that are purely discrete: discrete-time signals are converted into discrete number of frequencies. These techniques are converting a finite list of equally spaced samples of a function into the list of coefficients of a finite combination of complex sinusoids ordered by their frequencies. It can be said to convert the sampled function from its original domain often time or position along a line to the frequency domain [12].

b2. The Discrete Cosine Transform (DCT): In this technique is similar to the Discrete Fourier Transform. DCT transform the signal or image from spatial domain to the frequency domain. The mathematical transforms convert the pixels in such a way as to give the effect of "spreading" the location of the pixel values over part of the image.

b3. Discrete Wavelet Transform (DWT): In this technique is used to transform the image from a spatial domain to the frequency domain. In the process of steganography DWT identifies the high frequency and low frequency information of each pixel of the image. It is mathematical tool for decomposing an image hierarchically. It is mainly used for processing of non-stationary signals.

C. Vector Embedding:

A vector embedding method that uses robust algorithm with codec standard (MPEG-1 and MPEG -2) .This method embeds audio information to pixels of frames in host video. It is based on the H.264/AVC Video coding standard. The algorithm designed a motion vector component feature to control embedding, and also to be the secret carrier. The information embedded will not significantly affect the video sequence's visual invisibility and statistical invisibility. The algorithm has a large embedding capacity with high carrier utilization, and can be implementing fast and effectively [13].

D. Spread spectrum:

In this technique is used a secret data spread over a wide frequency bandwidth. The ratio of signal to noise in every frequency band must be so small that it becomes difficult to detect the presence of data. Even if parts of data are removed from several bands, there would be still enough information is present in other bands to recover the data. Thus it is difficult to remove the data completely without entirely destroying the cover .It is a very robust approach used in military communication [13]-14].

E. Statistical Technique:

In this technique message is embedded by changing several properties of the cover. It involves the splitting of cover into blocks and then embedding one message bit in each block. The cover block is modified only when the size of message bit is one otherwise no modification is required [15].

F. Distortion Techniques:

In this Technique is used to store the secret data by distorting the signal. An encoder applies a sequence of modifications to the cover image and the decoder phase decodes the encrypted data to the original data with the secret data by using some secret key [16].

G. Masking and Filtering:

In this technique is used to hides the data by marking an image. This approach is valuable where watermarks become a portion of the image. The data will be embedded where the more significant part of the image rather than hiding it into the noisy portion. The watermarking techniques are more integrated into the image and it can be applied without the fear of destruction of the image. This technique is used in 24 bit and grey scale images [15], [16].

V. A LITERATURES SURVEY REGARDING WITH VARIOUS RECENT STEGANOGRAPHY TECHNIQUES

The several characteristics of information hiding discussed [17], has been suggested Steganography is the art of passing information in a manner that the very existence of the message is unknown. The goal of steganography is to avoid drawing suspicion to the transmission of a hidden message. The recent growth in computational power and technology has propelled it to the forefront of today's security techniques of contemporary steganography techniques for image in spatial and transform domains and steganalysis techniques for the detection of secret message in the image, authors explore the steganography, its history, features, tools and various techniques like LSB, masking, filtering and other transformations used for hiding messages in an image. The paper also describes various methods to hide the secret or confidential message in an original file so that it is unintelligible to an interceptor [18], addressed the concept of embedding the secret message into an image using LSB technique and then applied AES algorithm to provide better security. Has been presented [19], proposes a reverse procedure described in paper by using an alteration component method. In addressed [20] user enters username, password and a key. A key is taken from automatic key generator device which generates a unique key after some specific time. After this the secret message and key is encrypted and encrypted message is embedded into cover image and stego image is produced. In paper [21] the secret message is first compressed then the message is hashed and encrypted using encryption key. This method results in robust model and achieves two important principles of security i.e. privacy and authenticity. In [22], a review used for hiding a secret message or image in spatial and transform domain. at [23] introduced a method where secret message is first compressed using wavelet transform technique and then embeds into cover image using LSB where the bits of secret message is inserted into image by using random number generator. In [24], A. Joseph Raphael introduces basic terminologies of cryptography and steganography and ensures that the combination of both gives multiple layers of security and will achieve requirements like capacity, security and robustness [25] introduced a method based on image ranking. Firstly, secret data is encrypted using RSA encryption algorithm and then users selects any image suited for hiding particular data. This will make difficult for attacker to succeed an attack. In [26], it is proved in this paper that using these techniques, data can be made more secure and robust. Have introduced [27], the method for embedding the secret image into cover image using LSB technique and then encrypts using DES algorithm and used the key image. In [28], authors first embed the secret data within cover image using LSB technique and then apply DES encryption method for encrypting the data which provides better security. In [29], authors first encrypts the data with RC4 encryption algorithm and then embeds in BMP cover image using three different steganographic methods. In [30], embeds the secret image into 24 bit or 8 bit image by using LSB and then evaluated results for 2, 4, 6 LSB for a .png file and a .bmp file. In [31], authors proposed a new technique called metamorphic cryptography where secret image is encrypted and transformed into a cipher image using key and this cipher image is embedded into a cover image by converting it into an intermediate text and finally transformed once again into an image. In the paper at [32], have been suggested basic terminologies of steganography, steganography techniques, classifications and review of previous work done by researchers. In the paper at [33], has discussed a method of hiding information on the billiboard. This method can be used for announcing a secret message in public place. In paper [34], user selects secret image in BMP format and encrypts using BLOWFISH cryptography Algorithm because BLOWFISH is faster, stronger and gives good performance when compared with DES, 3DES, AES, RC6, RC4. Has been discussed [35], approach to hide an image i.e. Hide behind Corner (HBC) algorithm is used to place a key at the image corners. All the keys at the corners are encrypted by generating Pseudo Random Numbers. Then the hidden image is transmitted. The receiver should know all the keys that are used at the corners while encrypting the image. Reverse Data Hiding (RDH) is used to get the original image and the original image is produced when all the corners are unlocked with proper secret keys used for hiding the image. In [36], user enters username, password to login into the system. After successful login, user can embed secret message into an image using a key and produces stego image. Same key is used at receiver site for retrieving the hidden data. Here the secret message is transferred into text file first. Then the text file is compressed into zip file, the zip text file then is used for converting it into binary codes. Zipping the text file is more secured and is hard to detect.

In [37], authors present a new technique for hiding information based on Huffman encoding. The gray level image of size m*n and p*q is taken as cover image and secret image respectively. The Huffman encoding is performed over secret image and each bit of Huffman code of secret image or a message is embedded into cover image by using LSB. The paper at [38] is similar to where secret data is encrypted using RSA encryption algorithm and then user selects any image suited for hiding particular data and then this secret data is embedded into cover image using LSB. Finally, a stego image has been produced. In [39], paper presents a method for encrypting and decrypting a secret file which embeds into image file using random LSB insertion method in which bits of secret message are spread into image bits randomly. These random numbers are generated by using a key. In [40], the secret message or data can be hidden in any image, audio or video which provides more security. The secret data is first encrypted using AES algorithm and key is hashed using SHA-1 to prevent from attacks then user can hide the cipher data in image, audio or video using LSB technique [41]-[42].

VI. CONCLUSION AND FUTURE WORK

In this paper provides literature reviews on conventional approaches and technique used in the security & transmitted data over the data networks. As steganography becomes widely used in computing, there are issues that need to be resolved. Every technique have its own importance and use for hiding the data in image. After the study of the all techniques it is easy to decide a particular one for secret communication. Future work can be done in way to combining the concepts of cryptography and steganography, to provide more security to the secrete message.

REFERENCES

[1] Sofyane Ladgham Chikouche and Noureddine Chikouche, “An improved approach for lsb-based image steganography using AES algorithm”, 5th International Conference on Electrical Engineering - Boumerdes (ICEE-B), IEEE Xplore, 14 December 2017.

[2] Provos N. and Honeyman P, “Hide and Seek: An Introduction to Steganography”, IEEE Security and Privacy, vol. 01, issue 3, pp. 32-44, May-June 2003.

[3] F. Piper, “Basic Principles of Cryptography”, IEEE Colloquium on Public uses of Cryptography, pp. 2/1-2/3, April 1996.

[4] I.J. Cox, M.L. Bloom, J.A. Fridrich, and T. Kalkert, “Digital watermarking and Steganography”, USA: Morgan Kaufman Publishers, pp. 1-591, 2008.

[5] Ashish T. Bhole and Rachna Patel, “Steganography over video File using Random Byte Hiding and LSB Technique”, IEEE international conference on computational intelligence and computing research. 2012

[6] R.Nivedhitha, Dr.T.Meyyappan, “Image Security using Steganography and Cryptographic Techniques”, International Journal of Engineering Trends and Technology, Vol.7, pp. 366-371, 2012.

[7] Anjali A. Shejul, Prof. U. L. Kulkarni, “A DWT based Approach for Steganography using Biometric”, International Conference On Data Storage and Data Engineering, IEEE, pp. 39-43, 2010.

[8] K. Gopalan. , “Audio steganography using bit modification”, IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP ’03), vol 2, pp. 6-10, April 2003.

[9] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das “A Tutorial Review on Steganography” International conference on contemporary computing, volume 101, 2008/8/7.

[10] Mehdi Hussain, Mureed Hussain, “A Survey of Image Steganography Technique”, International Journal of Advanced Science and Technology, Vol. 54, pp. 113-124, 2013.

[11] C. Science and B. Bridgeport, “A Novel Video Steganography Algorithm in the Wavelet Domain Based on the KLT Tracking Algorithm and BCH Codes,” (2015).

[12] Neil F. Johnson, Sushil Jajodia, “Exploring Steganography: Seeing the Unseen”, IEEE, pp. 26-34, Feb1998.

[13] Dr. R. Sridevi, Vijaya Lakshmi Paruchuri, K.S. Sadasiva Rao, “Image Steganography combined with Cryptography”, International Journal of Computers & Technology, Vol.9, pp. 976-984, July 2013.

[14] Lokesh Kumar, “Novel Security Scheme for Image Steganography using Cryptography Technique”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, pp. 143-146, April 2012.

[15] Mihir H Rajyaguru, “Crystography-Combination of Cryptography and Steganography with Rapidly Changing Keys”, International Journal of Emerging Technology and Advanced Engineering, Vol.2, pp. 329-332, October 2012.

[16] H.Al-Barhmtoshy, E.Osman and M.Ezzaand, “A Novel Security Model Combining Cryptography and Steganography”, Technical Report, pp. 483-490, 2004.

[17] S.Ashwin, J.Ramesh, K.Gunavathi, “Novel and Secure Encoding and Hiding Techniques Using Image Steganography: A Survey”, IEEE Xplore International Conference on Emerging Trends in Electrical Engineering and Energy Management, pp. 171-177, Dec 2012.

[18] Humanth Kumar, M.Shareef, R. P. Kumar, “Securing Information Using Steganography”, IEEE Xplore International Conference on Circuits, Power and Computing Technologies, pp. 1197-1200, March 2013.

[19] A. Joseph Raphael, Dr. V.Sundaram, “Cryptography and Steganography-A Survey”, International Journal of Computer and Technology Applications, Vol.2 (3), pp. 626-630, 2010.

[20] Armin Bahramshahry, Hesam Ghasemi, Anish Mitra, Vinayak Morada, „„„Design of a Data Hiding Application Using Steganography”, Databases, pp. 1-6, 2007.

[21] Vipula Madhukar Wajgade, Dr. Suresh Kumar, “Stegocrypto - A Review of Steganography Techniques using Cryptography”, International Journal of Computer Science & Engineering Technology, Vol. 4, pp. 423-426, 2013.

[22] Dhawal Seth, L. Ramanathan, Abhishek Pandey, “Security Enhancement: Combining Cryptography and Steganography”, International Journal of Computers Applications, Vol. 9(11), pp. 3-6, 2010.

[23] Wai Wai Zin, “Implementation and Analysis of Three Steganographic Approaches”, IEEE Xplore International Conference on Computer Research and Development, pp. 456-460, March 2011.

[24] D. Jacobs, Snehal Kamalapur, Neeta Sonawane, “Implementation of LSB Steganography and its Evaluation for Various Bits”, IEEE Xplore International Conference on Digital Information Management, pp. 173-178, Dec 2006.

[25] N.V Rao, J.TL Philjon, “Metamorphic Crypto- A Paradox between Cryptography and Steganography using Dynamic Encryption”, IEEE Xplore International Conference on Recent Trends in Information Technology, pp. 217-222, June 2011.

[26] S. Channalli, A. Jadhav, “Steganography an Art of Hiding Data”, International Journal on Computer Science and Engineering, Vol.1(3), pp. 137-141, 2009.

[27] Ms. Hemlata Sharma,Ms. MithleshArya, Mr. Dinesh Goyal , “Secure Image Hiding Algorithm using Cryptography and Steganography”, IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 13(5), pp. 1-6, August 2013.

[28] Hemalatha M., Prasanna A., Dinesh Kumar R., Vinoth kumar D., “Image Steganography using HBC and RDH Technique”, International Journal of Computer Applications Technology and Research, Vol.3, pp. 136-139, 2014.

[29] Rosziati Ibrahim, Teoh Suk Kuan, “Steganography Algorithm to Hide Secret Message inside an Image”, Computer Technology and Application, pp. 102-108, 2011.

[30] Rig Das, Themrichon Tuithung, “A Novel Steganography Method for Image Based on Huffman Encoding”, IEEE, 2012.

[31] M.Juneja, P.S. Sandhu, “Data Hiding with Enhanced LSB Steganography and Cryptography for RGB Color Images”, International Journal of Applied Research, Vol. 3(5), pp. 118-120, May 2013.

[32] M.S Sutaone., M.V. Khandare, “Image Based Steganography using LSB Insertion Technique”, IEEE Xplore, , pp. 146-151, Jan 2008.

[33] Shery Elizabeth Thomas, Sumod Tom Philip, Sumaya Nazar, Ashams Mathew, Niya Joseph, “Advanced Cryptographic Steganography using Multimedia Files”, International Conference on Electrical Engineering and Computer Science (ICEECS), pp. 239-242, May 2012.

[34] Ajit Singh, Swati Malik, “Securing Data by using Cryptography with Steganography”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3(5), pp. 404-409, May 2013.

[35] M. Sitaram Prasad, S. Nagan Janeyulu, Ch. Gopi Krishna, C. Nagaraju, “A Novel Information HidingTechnique for Security by using Image Steganography”, Journal of Theoretical and Applied Information Technology, pp. 35-39, 2005-2009.

[36] Khalil Challita, Hikmat Farhat, “Combining Steganography and Cryptography: New Directions”, International Journal on New Computer Architectures and their Applications (IJNCAA), Vol. 1(1), 2011, pp. 199-208.

[37] Jidagam Venkata Karthik, B.Venkateshwar Reddy, “Authentication of Secret Information in Image Steganography”, International Journal of Latest Trends in Engineering & Technology, ISSN: 2278-621X, Vol. 3(1), pp. 97-104, Sep 2013.

[38] Vipula M.Wajgade, Nagesh D. Matharia, Dr. Suresh Kumar, “Enhancing Data Security with Advanced Digital Image Steganography”, International Journal of Pure and Applied

Research in Engineering and Technology, Vol. 1(8), pp. 228-238, 2013.

[39] M. Pavani, S. Naganjaneyulu, C. Nagaraju, "A Survey on LSB Based Steganography Methods", International Journal of Engineering and Computer Science (IJECS), Vol. 2 (8), pp. 2464-2467, August, 2013.

[40] Shilpa Gupta, Geeta Gujral, Neha Aggarwal, "Enhanced Least Significant Bit algorithm for Image Steganography", International Journal of Computational Engineering & Management (IJCEM), Vol. 15(4), pp. 40-42, July 2012.

[41] Aprajita, Ajay Rana, "Steganography-The Art of Hiding Information- Comparison from Cryptography", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 1(5), pp. 1308-1312, May 2013.

[42] Atul Kahate, "Cryptography and Network Security", Tata McGraw-Hill, 2006.