A Crypto-Steganography: A Survey

Md. Khalid Imam Rahmani[1]
[1]Associate Professor, Deptt. of Computer Sc. & Engg.
Echelon Institute of Technology
Faridabad, INDIA.

Kamiya Arora[2], Naina Pal[3]
[2,3]M.Tech. Scholar, Deptt. of Computer Sc. & Engg.
Echelon Institute of Technology
Faridabad, INDIA.

***Abstract*—The two important aspects of security that deal with transmitting information or data over some medium like Internet are steganography and cryptography. Steganography deals with hiding the presence of a message and cryptography deals with hiding the contents of a message. Both of them are used to ensure security. But none of them can simply fulfill the basic requirements of security i.e. the features such as robustness, undetectability and capacity etc. So a new method based on the combination of both cryptography and steganography known as Crypto-Steganography which overcome each other's weaknesses and make difficult for the intruders to attack or steal sensitive information is being proposed. This paper also describes the basics concepts of steganography and cryptography on the basis of previous literatures available on the topic.**

Keywords*—Steganography; Image Steganography; Cryptography; Least Significant Bit (LSB); Enhanced Least Significant Bit (ELSB); Compression; Decompression; Advanced Encryption Standard (AES); Data Encryption Standard (DES); Hashing algorithms

I. INTRODUCTION

It's a well-known fact that security of data has become a major concern nowadays. The growth of modern communication technologies imposes a special means of security mechanisms especially in case of data networks [33]. The network security is becoming more important as the volume of data being exchanged over the Internet increases day by day [29].

The two important techniques for providing security are cryptography and steganography [5]. Both are well known and widely used methods in information security.

One of the reasons why the attackers become successful in intrusion is that they have an opportunity to read and comprehend most of the information from the system [29]. Intruders may reveal the information to others, misuse or modify the information, misrepresent them to an individual/ organization or use them to plan even some more severe attacks [13]. One of the solutions to this problem is through the use of steganography and cryptography.

Steganography is the art of hiding information in digital media through the techniques of embedding hidden messages in such a way that no one except the sender and the intended receiver(s) can detect the existence of the messages [1].

Cryptography is the art of transmitting the data safely over the Internet by applying some cryptographic algorithms so that it will be difficult for an attacker to attack or steal some confidential or private information [11].

A brief description of the state of the art of steganography and cryptography is given in section II. A literature survey is described in section III. In section IV, a proposed algorithm has been described. Section V describes the comparative analysis of both the techniques. Section VI has been used for the conclusion and future direction of the research work.

II. THE STATE OF THE ART

A. Steganography

Steganography is the technique of embedding hidden messages in such a way that no one, except the sender and intended receiver(s) can detect the existence of the messages. The main goal of steganography is to hide the secret message or information in such a way that eavesdroppers are not able to detect it [1]. If they found any suspicious data, then goal is defeated. Other goal of steganography is to communicate securely in a completely undetectable manner. The various forms of data in steganography can be audio, video, text and images etc. The basic model of Steganography consists of three components [3]:

- The Carrier image: The carrier image is also called the cover object that will carry the message that is to be hidden.
- The Message: A message can be anything like data, file or image etc.
- The Key: A key is used to decode/decipher/discover the hidden message.

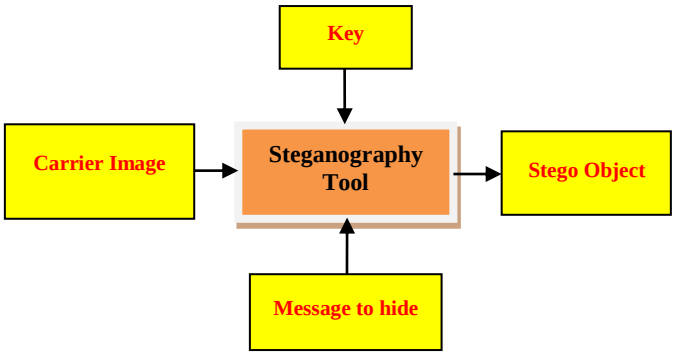

Fig. 1. Basic Model of Steganography

The encryption and decryption processes for hiding an image in steganography can be defined in a flow chart [3] as below:

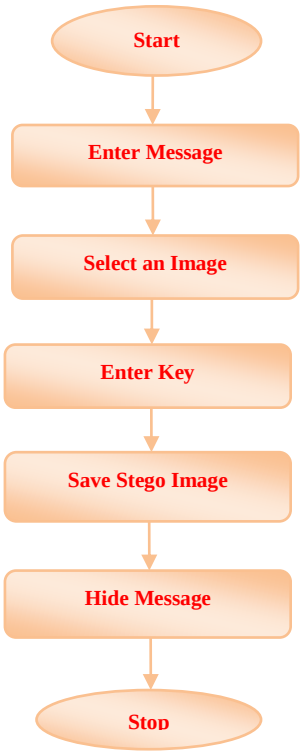

Fig. 2. Embedding Secret Message into Cover Object

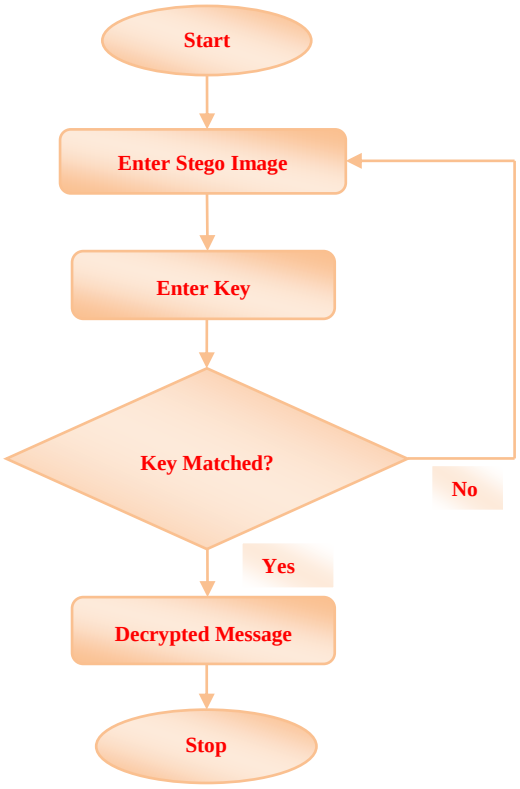

Fig. 3. Extracting Secret Message from Cover Object

1) Types of Steganography

The various types of steganography include [17]:

a) Image Steganography

The image steganography is the process in which we hide the data within an image so that there will not be any perceivable change in the original image. The conventional image steganography algorithm is LSB embedding algorithm.

b) Audio Steganography

The method of hiding secret information in an audio is known as audio steganography. There are various methods for hiding secret data in an audio such as LSB, Phase Coding etc. [17].

c) Video Steganography

The method of hiding secret information in a video is known as video steganography. Video consist of images as well as audio. Hence, both images and audio steganography can be used for video steganography [17].

d) Text files Steganography

The method of hiding secret information in a text is known as text steganography. 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 [17].

2) Techniques of Steganography

Steganography techniques are as follows:

a) Least Significant Bit (LSB)

Least Significant bit is the most common technique used for hiding the secret information in any digital media like image, text or audio/video. LSB refers to replacement of last bit of an image with the bit of secret message [23]. One can use 8 bit or 24 bit image to hide data. 24 bit images are well suited for hiding large amount of data. Although LSB is simple and useful for the user but it can be detected by an attacker during transmission of data on the network. There are many versions of LSB like Edge-LSB, Random-LSB and Enhanced LSB etc. [23].

b) Bitmap Steganography

There are two types of compressions: Lossy compression and Lossless Compression. In lossy compression, the data can be lost after applying compression while in lossless compression, the data can't be lost. For compression of images, lossy compression is generally used wherein after the compression the image can be restored but its quality can be degraded [21]. Bitmap steganography is the simple and most common approach as only BMP files gives lossless compression. BMP images are created from pixels and all pixels are comprised of three basic components i.e. Red, Green and Blue and named as RGB.

A combination of these three color components can form every color that is seen in these images. It is known that every byte in Computer Science is created from 8 bits and the first

bit is called the most significant bit (MSB) and the last bit is called the least significant bit (LSB).

Suppose that there are three adjacent pixels (9 bytes) with the RGB encoding:

10010101 00001101 11001001
10010110 00001111 11001011
10011111 00010000 11001011

The decimal number 300 can be converted into binary representation which is 100101100. This representation can be embedded into the least significant bits of the image. LSB can be represented as (where bits in different color have been changed)

10010101 00001100 11001000
10010111 00001110 11001011
10011111 00010000 11001010

Here the number 300 was embedded into the grid, only the 5 bits are needed to be changed according to the embedded message. On an average, only half of the bits in an image would be modified to hide a secret message using the maximum cover size [32].

B. Cryptography

Cryptography is the art of achieving security by encoding messages to make them non-readable [34]. Cryptography is an art of transmitting the data safely over the Internet by applying some cryptographic algorithms so that it will be difficult for an attacker to attack or steal some confidential or private information.

Two basic terms used in cryptography are encryption and decryption; encryption is the process of converting plain text into cipher text and decryption is the reverse process of encryption [34]. Plain text is the text having the actual message or data which is not encrypted and cipher text is the text after encryption of message or data which is ready to be shared [34]. A key is needed for both encryption and decryption of the message.

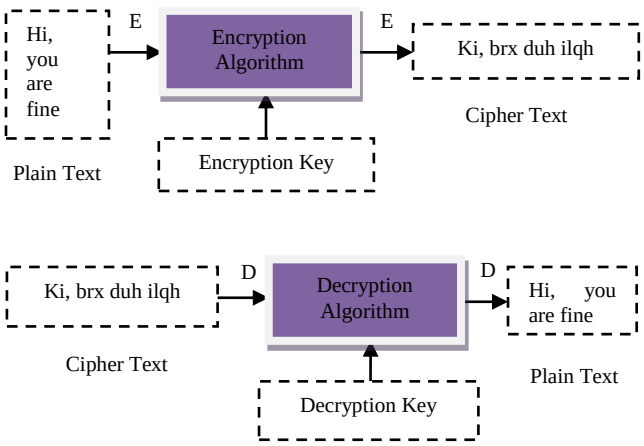

Fig. 4. Basic Model of Cryptography

C. Steganography vs Cryptography

TABLE I. DIFFERENCE BETWEEN STEGANOGRAPHY AND CRYPTOGRAPHY

Techniques	Steganography	Cryptography
Definition	Steganography means cover writing	Cryptography means secret writing
Objective	Focuses on keeping existence of a message secret	Focuses on keeping contents of a message secret
Key	Optional	Necessary
Carrier	Any digital media	Usually text based
Visibility	Never	Always
Security Services Offered	Confidentiality, authentication	Confidentiality, availability, data integrity, non-repudiation
Attacks	It is broken when attacker detects that steganography has been used known as Steganalysis	It is broken when attacker can read the secret message known as Cryptanalysis
Result	Stego file	Cipher text

III. LITERATURE SURVEY

In [1], 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.

In [2], basic cryptographic concepts and techniques are defined. 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.

In [3], Dr. R. Sridevi, Vijaya Lakshmi Paruchuri, K. S Sadasiva Rao introduced the concept of embedding the secret message into an image using LSB technique and then applied AES algorithm to provide better security.

The paper [4] proposes a reverse procedure described in paper [3] by using an alteration component method.

In [5] 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 [6] 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 [7], various technologies used in image steganography are proposed. This paper presents a review used for hiding a secret message or image in spatial and transform domain. This paper also proposed techniques for detecting the secret message or image i.e. steganalysis.

The paper at [8] 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 [9], 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.

The paper at [10] 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. Finally, a stego image has been produced but this paper lacks in integrity and this application cannot hide large data.

In [11], authors give brief review of above techniques used for ensuring security. It is proved in this paper that using these techniques, data can be made more secure and robust.

The authors in paper [12] introduced 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 [13], 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 [14], authors first encrypts the data with RC4 encryption algorithm and then embeds in BMP cover image using three different steganographic methods and then compares these three methods. This paper also results in achieving the requirements of security i.e. data confidentiality, data integrity and data authentication.

The paper at [15], 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 [16], 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 [17], authors define basic terminologies of steganography, steganography techniques, classifications and review of previous work done by researchers.

In the paper at [18], authors define a method of hiding information on the billiboard. This method can be used for announcing a secret message in public place. User first enters the normal data then hides secret data into normal data and the encrypted data is displayed on the billiboard board. This encrypted data is saved for decrypting the secret data.

In paper [19], 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. This encrypted image is embedded into video using LSB technique and forms stego video. This method provides confidentiality, authenticity, integrity and non-repudiation.

In [20], authors used a different 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 [21], 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 [22], 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 [23] is similar to paper at [10] 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. This will make difficult for an attacker to steal sensitive information. Finally, a stego image has been produced.

In [24], 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 [25], 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. The receiver should provide the same key that is hashed for encryption.

The paper [26] is similar to paper [19] but the only difference is that here user selects plain text and encrypts using BLOWFISH Algorithm. This encrypted text is embedded into image using LSB technique and forms stego image. Reverse procedure is done for decrypting the secret image.

In [27], the method is similar to that in the paper [6]; the only difference is the compressed message is not hashed. This novel approach requires less memory space, fast transmission rate, better security and no distortion in quality of image.

In the paper at [28], authors proposed two methods to ensure high security. First method includes the combination of

both steganography technique and cryptography technique and second method only includes steganography approach.

IV. The Proposed Algorithm

Based on the findings in the existing papers studied, a new algorithm is being proposed that can ensure all of the security principles i.e. robustness, confidentiality, authentication, integrity and non-repudiation and that would also satisfy the requirements of steganography i.e. capacity, undetectability and robustness [18]. The algorithm which will be implemented in a proposed system at a later stage of this research work consists of four layers. Each layer is used to achieve one security principle like layer 1 implements authorization, layer 2 implements authentication, integrity and non-repudiation, layer 3 implements confidentiality and partial security, layer 4 implements robustness and the remaining part of security. Each layer defined is unperceivable for an attacker. The flow chart below describes various steps involved in the algorithm:

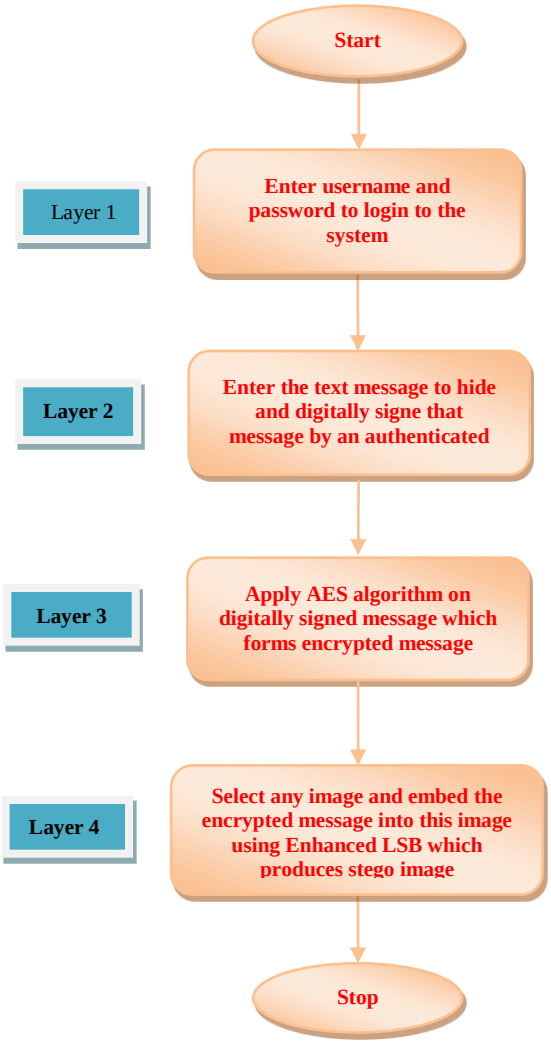

Fig. 5. Proposed Algorithm

V. Comparative Analysis

A comparative analysis is made to compare the effectiveness of the proposed method with respect to other available methods. The comparative analysis has been performed on the basis of the requirements of security i.e. confidentiality, robustness and authentication etc. From this analysis, it has been identified that all the papers discussed in literature review lack in some aspect or the other as far as the implementation of the principles of security is concerned.

The effectiveness of the proposed method can be estimated by computing some valuable statistical operations.

TABLE II. Comparative Analysis of the Literature

Literature Reference	Requirements		
	Confidentiality	***Robustness***	***Authentication***
[2]	Yes	Yes	No
[3]	Yes	No	No
[4]	Yes	No	No
[5]	No	No	Yes
[6]	Yes	No	Yes
[7]	Yes	Yes	No
[9]	Yes	Yes	Yes
[10]	No	No	Yes
[13]	Yes/No	No	No
[14]	Yes	Yes	Yes
[15]	Yes/No	No	No
[16]	Yes	Yes	No
[18]	No	No	No
[20]	Yes	Yes	No
[21]	Yes	Yes	Yes
[22]	Yes	Yes	No
[24]	Yes	Yes	No
[25]	Yes	Yes	No
[27]	No	No	No

VI. CONCLUSIONS

In this paper, a very comprehensive review of the conventional approaches and techniques used in the security of transmitted data over the data networks has been given. The survey has been carried out related to both steganography and cryptography that ensures security but lacks in some way or the other as far as their individual capabilities related to coverage of all the security principles are concerned. So, in order to overcome the lack of coverage of all the principles of security in those algorithms, a new algorithm has been proposed that would satisfy all the principles of security and also satisfy the requirements of steganography.

The proposed algorithm can be implemented in a security system as a future research work that would probably excel in comparison to the existing algorithms. The system would be tested on the basis of various test cases and the results would be compared with those of existing algorithms.

REFERENCES

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

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

[3] Dr. R. Sridevi, Vijaya Lakshmi Paruchuri, K.S. Sadasiva Rao, "Image Steganography combined with Cryptography", International Journal of Computers & Technology, ISSN: 22773061, Vol.9, July 2013, pp. 976-984.

[4] Lokesh Kumar, "Novel Security Scheme for Image Steganography using Cryptography Technique", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X Vol.2, April 2012, pp. 143-146.

[5] Mihir H Rajyaguru, "Crystography -Combination of Cryptography and Steganography with Rapidly Changing Keys", International Journal of Emerging Technology and Advanced Engineering, ISSN: 2250-2459, Vol.2, October 2012, pp. 329-332.

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

[7] 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, Dec 2012, pp. 171-177.

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

[9] A. Joseph Raphael, Dr. V.Sundaram, "Cryptography and Steganography-A Survey, International Journal of Computer and Technology Applications", ISSN: 2229-6093, Vol.2 (3), 2010, pp. 626-630.

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

[11] Vipula Madhukar Wajgade, Dr. Suresh Kumar, "Stegocrypto - A Review of Steganography Techniques using Cryptography", International Journal of Computer Science & Engineering Technology, ISSN: 2229-3345, Vol. 4, 2013, pp. 423-426.

[12] R.Nivedhitha, Dr.T.Meyyappan, "Image Security using Steganography and Cryptographic Techniques", International Journal of Engineering Trends and Technology, ISSN: 2231-5381, Vol.7, 2012, pp. 366-371.

[13] Dhawal Seth, L. Ramanathan, Abhishek Pandey, "Security Enhancement: Combining Cryptography and Steganography", International Journal of Computers Applications, ISSN: 0975-8887, Vol. 9(11), 2010, pp. 3-6.

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

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

[16] 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, June 2011, pp. 217-222.

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

[18] S. Channalli, A. Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering, ISSN: 0975-3397, Vol.1(3), 2009, pp. 137-141.

[19] Ms. Hemlata Sharma,Ms. MithleshArya, Mr. Dinesh Goyal , "Secure Image Hiding Algorithm using Cryptography and Steganography", IOSR Journal of Computer Engineering (IOSR-JCE), ISSN: 2278-8727, Vol. 13(5), August 2013, pp. 1-6.

[20] 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, 2014, pp. 136-139.

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

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

[23] M.Juneja, P.S. Sandhu, "Data Hiding with Enhanced LSB Steganography and Cryptography for RGB Color Images", International Journal of Applied Research , ISSN: 2249-555X , Vol. 3(5), May 2013, pp. 118-120.

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

[25] 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), May 2012, pp. 239-242.

[26] Ajit Singh, Swati Malik, "Securing Data by using Cryptography with Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Vol. 3(5), May 2013, pp. 404-409.

[27] 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, 2005-2009, pp. 35-39.

[28] Khalil Challita, Hikmat Farhat, "Combining Steganography and Cryptography: New Directions", International Journal on New Computer Architectures and their Applications (IJNCAA), ISSN: 2220-9085, Vol. 1(1), 2011, pp. 199-208.

[29] 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), Sep 2013, pp. 97-104.

[30] 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, ISSN: 2319-507X, Vol. 1(8), 2013, pp. 228-238.

[31] M. Pavani, S. Naganjaneyulu, C. Nagaraju, "A Survey on LSB Based Steganography Methods", International Journal of Engineering and Computer Science (IJECS), ISSN:2319-7242, Vol. 2 (8), August, 2013, pp. 2464-2467.

[32] Shilpa Gupta, Geeta Gujral, Neha Aggarwal, "Enhanced Least Significant Bit algorithm for Image Steganography", International Journal of Computational Engineering & Management (IJCEM), ISSN: 2230-7893, Vol. 15(4), July 2012, pp. 40-42.

[33] Aprajita, Ajay Rana, "Steganography-The Art of Hiding Information-Comparison from Cryptography", International Journal of Innovative Research in Science, Engineering and Technology, ISSN : 2319-8753, Vol. 1(5), May 2013, pp. 1308-1312.

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

AUTHORS' BIBLIOGRAPHY

Md. Khalid Imam Rahmani is an Associate Professor in the Department of Computer Science & Engg. of a very reputed NBA accredited Engineering College, Echelon Institute of Technology, Faridabad, India. He is having about 17 years of teaching, industry and administrative experience. He has done B.Sc. Engg. in Computer Engineering from A.M.U., Aligarh, M.Tech. in Computer Engineering from M.D.U., Rohtak and is pursuing Ph.D. in Digital Image Retrieval Algorithms. Digital Image Processing, Innovative Programming techniques, Mobile Computing, Algorithms Design and Internet & Web Technologies are his research areas.

Kamiya Arora has earned her M.Tech. degree in Computer Science & Engg. from Echelon Institute of Technology under Maharshi Dayanand University, Rohtak. Her research interests include Image Processing, Steganography, Data mining and Cryptography.

Naina Pal has earned her M.Tech. degree in Computer Science & Engg. from Echelon Institute of Technology under Maharshi Dayanand University, Rohtak. Her research interests include Image Processing, Classification of data using Clustering and Data mining.