ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

Secured and Robust Dual Image Steganography: A Survey

Hemang A. Prajapati[1], Dr. Nehal G. Chitaliya[2]

PG Student, Dept of E&C, SVIT, Vasad, Anand, India[1]

Assoc. Professor, Dept of E&C, SVIT, Vasad, Anand, India[2]

ABSTRACT: In the last few years communication technology has been improved, which increase the need of secure data communication. For this, many researchers have exerted much of their time and efforts in an attempt to find suitable ways for data hiding. There is a technique used for hiding the important information imperceptibly, which is Steganography. Steganography is the art of hiding information in such a way that prevents the detection of hidden messages. The process of using steganography in conjunction with cryptography, called as Dual Steganography. This paper tries to elucidate the basic concepts of steganography, its various types and techniques, and dual steganography. There is also some of research works done in steganography field in past few years.

KEYWORDS: Cryptography, Dual Steganography, Steganalysis, Steganography, LSB technique, DWT technique.

I. INTRODUCTION

Steganography is a data hiding technique which conceals the existence of data in the medium. It provides secrecy of text or images to prevent them from attackers. It provides secret communication so that intended hacker or attacker unable to sense the presence of information. Steganography, derived from Greek, literally means "covered writing" [1].

This paper is organized as follows. Section II discusses the comparison between cryptography and steganography. Section III discusses the basics of steganography. Section IV discusses the different types of steganography. Section V briefly discusses the various types of image steganography techniques. Next section VI gives basic idea about steganalysis. Section VII provides the applications of steganography. Section VIII discusses briefly about dual image steganography and literature survey of various combinations in section IX. Finally section X gives conclusion.

II. COMPARISON OF STEGANOGRAPHY AND CRYPTOGRAPHY

Steganography and cryptography are closely related. Cryptography scrambles plain text into cipher text so it can't be understood. While Steganography hide the message so there is no knowledge of the existence of the message. The final result in cryptography is the cipher text, while the final result in steganography is the stego-media [1].
Steganography and cryptography are both ways to protect data from unwanted parties but neither technology alone is perfect. Once the presence of the hidden information is revealed or even suspected, the purpose of the Steganography is partly defeated. The strength of Steganography can be amplified by combining it with cryptography [18].

III. STEGANOGRAPHY MODEL

Generally a steganographic system has a cover file that is used to cover the original message and the steganography algorithm to carry out the required object as shown in Fig. 1. The result is a file called stego-file which has the message inside it, hidden. This stego file is then sent to the receiver where the receiver retrieves the message by applying the de-steganography. The goal of modern steganography is to keep the message undetectable [2].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

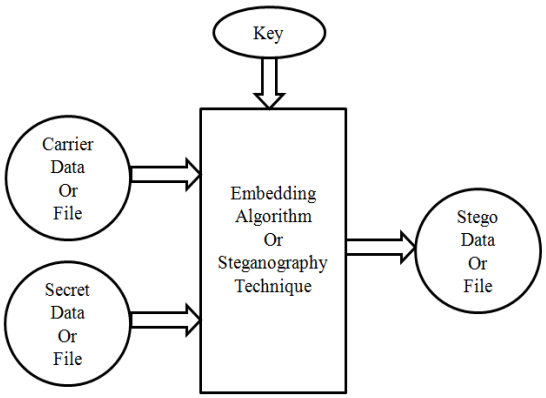

Fig.1: Basic Steganography Model [18]

IV. STEGANOGRAPHY TYPES

There are five main categories of file formats that can be used for steganography based on these, the types are:

A. *Text Steganography*

Hiding information in text is the most important and basic method of steganography. It can be classified in three categories: format based, random & statistical generation and linguistic method [30].

B. *Image Steganography*

Images are used as the popular cover files for steganography. This technique exploits the weakness of the human visual system (HVS). HVS can't detect the variation in luminance of color vectors expressed in terms of 1s and 0s [30, 31].

C. *Audio Steganography*

It takes advantage of the psycho acoustical masking phenomenon of the human auditory system [HAS]. Psycho acoustical or auditory masking property renders a weak tone imperceptible in the presence of a strong tone in its temporal or spectral neighbourhood. In audio steganography, secret file is embedded into digitized audio signal which result slight altering of binary sequence of the cover audio file.

D. *Video Steganography*

Video files are generally a collection of image and audio, so most of the presented techniques on images and audio can be applied to video files too [16]. The advantages of video are the large amount of data that can be hidden inside and noticeable distortions might go unobserved by humans because of the continuous flow of information.

E. *Protocol Steganography*

In this technique, the information is embedded within messages and network control protocols used in network transmission. A network packet consists of packet headers, user data and packet trailers. So during some of the layers of the network model, steganography can be used [32].

V. IMAGE STEGANOGRAPHY TECHNIQUES

Different types of Image Steganography Techniques are: Spatial domain, Transform domain, Spread spectrum, Masking & filtering and Distortion Techniques.

A. *Spatial Domain Technique*

In this technique, the secret file is embedded directly in the image [16]. Following are some techniques used in spatial domain [8]:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

1) LSB Substitution Method

The most well known and simplex steganographic technique in the data hiding is least-significant-bits (LSB) substitution. In this, the least significant bits of the pixels are replaced by the message bits. This technique is simple, but causes noticeable distortion when the number of embedded bits exceeds three for each pixel.

2) Optimum Pixel Adjustment Procedure

The Optimal Pixel adjustment Procedure (OPAP) reduces the distortion caused by the LSB substitution method by adjusting pixel value after the hiding of the secret.

3) Inverted Pattern Approach

This inverted pattern (IP) LSB substitution approach uses the idea of processing secret messages prior to embedding. In this method each part of secret images is determined to be inverted or not inverted before it is embedded so stego image has less distortion [26].

4) Pixel Value Differencing

Pixel Value Differencing (PVD) is able to provide a high quality stego image in spite of the high capacity of the concealed information. In this message is embedded within edge area because human perception is less sensitive to subtle changes in edge areas, it is more sensitive to changes in the smooth areas.

Advantages of Spatial Domain Technique [3]:

1. There is less chance for degradation of the original image.
2. Hiding capacity is more i.e. more information can be stored in an image.

Disadvantages:

1. Large payload but often offset the statistical properties of the image
2. Not robust against lossy compression and image filters
3. Not robust against rotation, cropping and translation
4. Not robust against noise
5. Many work only on the BMP format

B. *Transform Domain Technique*

This is more complex way of hiding information in an image where various algorithms and transformations are used on the image to hide information in cover image. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Today most of the strong steganographic systems operate in the transform domain [15]. Its types are JPEG Steganography and Discrete Wavelet Transformation (DWT).

1) JPEG Steganography:

Originally thought was steganography would not be possible to use with JPEG images, as they use lossy compression which results in parts of the image data being altered. During the DCT transformation, rounding of coefficients are not noticeable by human eye [16]. This same property is also used to hide messages. The DCT and the quantization phase form part of the lossy stage and the Huffman encoding used to further compress the data is lossless stage. Steganography take place between these two stages [27]. By same principles of LSB insertion the message can be embedded into the LSB of the coefficients before applying the Huffman encoding. So it is extremely difficult to detect, as it is not in the visual domain [29].

2) Discrete Wavelet Transformation

The wavelet transformation describes a multi-resolution decomposition process in terms of expansion of an image onto a set of wavelet basis function. DWT has its own excellent space frequency localization properly [7]. By applying 2D DWT on the image, the four subbands are generated which are LL, LH, HL and HH. So by modifying these co-efficient the stego image is generated [14, 28]. The Haar wavelet is also possible wavelet transform technique [6].

Advantages of Transform Domain Technique:

1. Highly robust, the hidden data cannot be lost with image manipulation
2. Higher imperceptibility

Disadvantages:

1. Very complex techniques

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

2. Too much computations required

C. *Spread Spectrum Technique*
In this technique, hidden data is spread throughout the cover image making it harder to detect. Marvel et al, proposed a system that combines spread spectrum communication, error control coding and image processing to hide information in images [12]. Here the message is embedded in noise and then combined with the cover image to generate the stego image. Because of the power of the embedded image is much lower than the power of the cover image, the embedded image is not perceptible by human eye or computer without access to the original cover image [11].

D. *Masking and Filtering Technique*
These techniques hide information by marking an image, in a way similar to watermarks on actual paper and are sometimes used as digital watermarks. These techniques embed the information in the more significant areas such that the hidden message is more integral to the cover image. Masking images entails changing the luminance of the masked area. The smaller the luminance change, the lesser chance of detection [16]. This makes it more suitable than LSB with, for instance, lossy JPEG images [13]. Weiqi Luo [23] proposed a method that finds the edges of cover image and within this mask area the secret data is embedded. Here the change in edge is less visual compared with change in smooth region.

Advantages of Masking and filtering Technique:
This method is much more robust than LSB substitution method with respect to compression since the information is hidden in the visible parts of the image.
Disadvantages:
Techniques can be applied only to gray scale images and restricted to 24 bits.

E. *Distortion Technique*
In this technique, a stego image is created by applying a sequence of modifications to the cover image. This sequence of modifications is use to match the secret message required to transmit which is encoded at pseudo randomly chosen pixels [20]. In this cover image is also transmitted so comparing with it, the secret message is extracted. Here the cover image should never be used more than one time. If an attacker tampers with stego image by cropping, scaling or rotating, the receiver will easily detect it [21].

Advantages of Distortion Technique:
1. Easy embedding
2. Good imperceptibility
Disadvantages:
Need for sending the cover image along with stego image

VI. STEGANALYSIS

Steganalysis is the science of detecting hidden information. The objective of steganalysis is to break steganography and the detection of stego image is the goal of steganalysis. Most of steganalysis algorithms rely on steganographic algorithms introducing statistical differences between the cover image and stego image. It deals with three important categories: Visual attacks, Statistical attacks and Structural attacks [30, 31].

VII. APPLICATION

Few applications of the steganography are [30]:
- Defense Organizations: Security from enemies
- Intelligence Agencies: Security of person's private information
- Government Agencies: Store critical data like criminal record
- Smart Identity Cards: Personal information is embedded into photo
- Medical: Patient's details are embedded within image
-

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

VIII. DUAL STEGANOGRAPHY

As we know steganography and cryptography, both are data hiding techniques used for secure communications over insecure channel. But for obtaining much higher security, the combination of two is used. Inside the steganography process, cryptography is used, so it's called as Dual Steganography [25].
The basic model of dual steganography is shown Fig 2. Here, the secret data is firstly converted into encrypted form and then using this encrypted information as secret data, is hidden inside the cover image with the help of embedding algorithm and finally the stego image is formed which is same as cover image in human perceptible way. The cryptography algorithms used are RSA (Rivest Shamir Adelman), DES (Data Encryption Standard), AES (Advanced Encryption Standard), Diffie Hellman or different algorithms can also be created. Sometimes a stego key is also used to make the communication more secured. This key can directly be given by the sender and used during the embedding algorithm. The stego key must be known at both transmitter and receiver side. Thus using cryptography along with steganography, secret information can be easily communicated with high security. This is more secured way of using steganography [19].

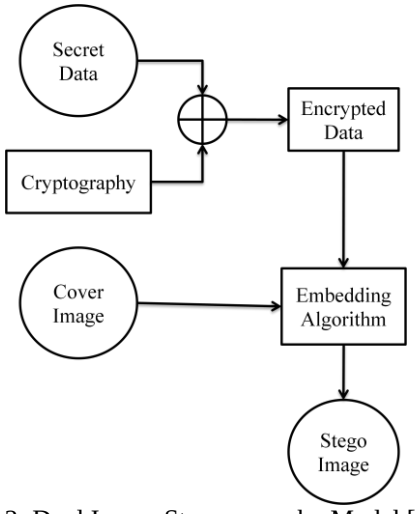

Fig. 2: Dual Image Steganography Model [10]

If steganalysis occur during the transmission of stego image generated using dual steganography then even if the hidden information is detected then it's in the scrambled form which cannot be understood by the eavesdropper. So by using dual steganography, highly secured communication can occur.

IX. LITERATURE SURVEY

In this review paper, depending on the combination of steganography and cryptography various papers are referred which are explained in following parts:

1) LSB and Encryption Combination
In this, first the secret file is encrypted with cryptography technique then this encrypted data is embedded within cover image by LSB substitution technique. Some of the related research works are as follows:
Shailender Gupta, et al [4] developed a technique for hiding information using LSB steganography and cryptography where the secret information is encrypted first using RSA or Diffie Hellman algorithm and then the encrypted ASCII value is converted to binary form. Here even the cover image is converted from pixels to binary form and then the secret message is embedded in the cover image using LSB technique and the stego image is formed. With the proposed method, time complexity is increased but high security is achieved at that cost.

Md. Rashedul Islam, et al [5] proposed a method that has two parts; one is changing the secret message to cipher text by AES Cryptography and other is hiding the cipher into image Steganographic technique. But here the LSB substitution is performed based on the cover image, depending on the darker and lighter area steganography is performed.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

Mazen Abu Zaher [17] developed a modified LSB method in which text message to be hidden is treated as 8 bit ASCII codes. Using encryption algorithm these codes are then converted into 5 bit codes and then hidden in cover image using LSB. As encryption algorithm used, if anyone extract bits from image, he won't understand until he decrypt it. So with this technique, more information can be hidden with a level of protection.

Mamta Juneja, et al [24] proposed a method that first encrypts the secret data by RSA algorithm. By using this encrypted data method finds the best match for cover image so that after LSB substitution the generated stego image has fewer chances of visual attack. So this method has better statistical and visual attack protection.

S. M. Masud Karim, et al [25] proposed an efficient LSB based steganographic method that utilizes the secret key to hide the information into an input pixel of cover image without producing perceptible distortions. Here a bit of hidden information is placed in either LSB of Green or Blue matrix of a specific pixel which is decided by the secret key. So anyone cannot exactly make a decision that the bit of hidden information is placed in either LSB of Green or Blue matrix. As a result, the security level of image steganography IS attained.

2) DWT and Encryption Combination

In this, the secret file is encrypted with any cryptography technique then this encrypted data is embedded within cover image by DWT technique. Some of the related research works are as follows:

Tanmay Bhattacharya, et al [15] proposed a DWT based Dual steganographic technique. Using DWT, a cover image is decomposed into four sub bands. Two secret images are hidden within HL and HH sub bands respectively by using a pseudo random sequence and a session key. After embedding the secret data, all four sub bands including two modified sub bands are combined to produce the stego image using IDWT. By this method large amount of information is transferred in a more secured way and also have an acceptable level of imperceptibility.

Amritha G. [22], et al proposed method steganography is object oriented as it is based on one of the feature of image. Here the feature used is skin region of image. Instead of using full cover image, embedding data only within the skin regions provide an excellent secure location for data hiding. Encrypt secret image using RC4 algorithm before embedding enhances the security level. In this cover image is converted to HSV form to detect the skin color. After that skin segment is detected and cropped. That region is transformed into DWT form and secret image encrypted with RC4 cryptography algorithm. This encrypted data embedded within high frequency sub band of cover image and IDWT is performed. At last by merging this segment stego image is generated.

Ketan Shah [33], el at proposed a method which combines the DWT steganography and DES cryptography technique. In DWT, haar transform is used in two stages and the secret image is encrypted by DES algorithm. This algorithm has 64 bits secret key, 16 rounds of encryption, 64 bits pain text input and 64 bits cipher text output. This output is embedded into HH sub band. Then IDWT is performed to generate stego image.

Archana S. Vaidya [34], el at developed method that uses Blowfish algorithm for encryption. It has scalable secret key from 32 to 256 bits. It is a block cipher which uses 64 bits message block to encrypt it. Then encrypted data is embedded within cover image and by IDWT stego image is generated.

X. CONCLUSION

For the secret communication of internet users, as well as for others, information security has become one of the most significant problems. Unauthorized access to secret data can have serious repercussions like financial loss etc. Steganography is one of the solutions whose goal is to hide the existence of communicated message. By using dual steganography in which steganography and cryptography are woven together, attempts to make steganalysis difficult. In this paper, the basic concepts of steganography, its methods and highly secured dual steganography methods has been reviewed. The battle between steganography and steganalysis will continually give rise to new techniques by countering each other. In near future, the most important use of steganographic techniques will probably lie in the field of digital watermarking.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

REFERENCES

1. Ross J. Anderson, Fabien A. P. Petitcolas, "On the Limits of Steganography", IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, pp. 474-481, May 1998.
2. M. Hossain, S.A. Haque, F. Sharmin, "Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Iriformation", 12th International Conference on Computer and Information Technology (ICCIT 2009) 21-23 December 2009.
3. Abbas Cheddad, Joan Condell, Kevin Curran, Paul McKevitt, "Digital image steganography: Survey and analysis of current methods", Elsevier, Signal Processing, Vol. 90, pp. 727-752, 18 August 2009.
4. Shailender Gupta, Ankur Goyal, Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography", International Journal Modern Education and Computer Science, Vol. 6, pp. 27-34, June 2012.
5. Md. Rashedul Islam, Ayasha Siddiqa, Md. Palash Uddin, Ashis Kumar Mandal, Md. Delowar Hossain, "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography", 3rd International Conference on Informatics, Electronics & Vision 2014.
6. K. Sakthisudhan, P. Prabhu, "Dual Steganography Approach for Secure Data Communication", International Conference on Modeling, Optimization and Computing, Elsevier, Procedia Engineering, Vol. 38, pp. 412-417, 2012.
7. Ali Al-Ataby, Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform", The International Arab Journal of Information Technology, Vol.7, October 2010
8. R.Amirtharaja, R.Akila, "A Comparative Analysis of Image Steganography", International Journal of Computer Applications, Vol.2, pp. 41- 47, May 2010.
9. V. Nagaraj, Dr. V. Vijayalakshmi, Dr. G. Zayaraz, "Modulo based Image Steganography Technique against Statistical and Histogram Analysis", IJCA Special Issue on "Network Security and Cryptography" NSC, Vol. 4, pp. 34-39, 2011.
10. Vikas Tyagi, Atul kumar, Roshan Patel, Sachin Tyagi, Saurabh Singh Gangwar, "Image Steganography Using Least Significant Bit With Cryptography", Journal of Global Research in Computer Science, Vol. 3, pp. 53-55, March 2012.
11. Lisa M. Marvel, L.M., Boncelet Jr., C.G., Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, Vol. 8, pp. 1075-1083, August 1999.
12. Wang H., Wang S., "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, Vol. 47, pp. 76-82, October 2004.
13. Samir K. Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee, Poulami Das, "A Tutorial Review on Steganography", International Conference, Vol. 3, pp. 105-114, 2008.
14. Amitava Nag, Sushanta Biswas, Debasree Sarkar ,Partha Pratim Sarkar, "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding", International Journal of Computer Science and Security (IJCSS), Vol.4, Issue -6, 2011.
15. Tanmay Bhattacharya, Nilanjan Dey, S. R. Bhadra Chaudhuri, "A Novel Session Based Dual Steganographic Technique Using DWT and Spread Spectrum" International Journal of Modern Engineering Research, Vol.1, pp. 157- 161, 2012.
16. Neil F. Johnson, Sushil Jajodia, "Exploring steganography: Seeing the unseen", IEEE Computer Journal, Vol. 31, pp. 26–34, 1998.
17. Mazen Abu Zaher, "Modified Least Significant Bit (MLSB)", Computer and Information Science, Vol.4, pp. 60-67, January 2011.
18. Kanzariya Nitin K., Nimavat Ashish V., "Comparison of Various Images Steganography Techniques", International Journal of Computer Science & Management Research, Vol. 2, Issue 1, pp. 1213-1217, January 2013.
19. H.S. Majunatha Reddy, K.B. Raja, "High capacity and security steganography using discrete wavelet transform", International Journal of Computer Science and Security, Vol. 3, pp. 462-472, 2009.
20. S.C. Katzenbeisser, F. Petitcolas, "Principles of Steganography in Information Hiding Techniques for Steganography and Digital Watermarking", Ed. London: Artech House, 2000.
21. P. Kruus, C. Scace, M. Heyman, M. Mundy, "A survey of steganography techniques for image files", Advanced Security Research Journal, Vol. 5, pp. 41- 52, 2003.
22. Amritha G., Meethu Varkey, "Biometric Steganographic Technique Using DWT and Encryption", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue 3, pp. 566-572, March 2013.
23. Weiqi Luo, Jiwu Huang, Fangjun Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions on Information Forensics and Security, Vol.5, pp. 201-214, June 2010.
24. Mamta Juneja, Parvinder Singh Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", IEEE International Conference on Advances in Recent Technologies in Communication and Computing, pp. 302-305, 2012.
25. S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, "A New Approach for LSB Based Image Steganography using Secret Key", IEEE 14th International Conference on Computer and Information Technology, December 2011.
26. Nadeem Akhtar, Shahbaaz Khan, Pragati Johri, "An Improved Inverted LSB Image Steganography", IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques, 2014.
27. Neda Raftari, Amir Masoud Eftekhari Moghadam, "Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT", IEEE Fourth International Conference on Computational Intelligence, Comm. Systems and Networks, 2012.
28. Parul, Manju, Dr. Harish Rohil, "Optimized Image Steganography using Discrete Wavelet Transform (DWT)", International Journal of Recent Development in Engineering and Technology, Vol. 2, Issue 2, pp. 75-81, February 2014.
29. M. Iwata, K. Miyake, A. Shiozaki, "Digital Steganogaphy utilizing features of JPEG images", IEICE Transactions on Fundamentals, 2004.
30. Ronak Dhoshi, Pratik Jain, Lalit Gupta, "Steganography and Its Applications in Security", International Journal of Modern Engineering Research (IJMER), Vol.2, pp. 4634- 4638, November 2012.
31. Pratap Chandra Mandal, "Modern Steganographic technique: A survey", International Journal of Computer Science & Engineering Technology, Vol.3, pp. 444-448, September 2012.
32. Handel T., Sandford M., "Hiding data in the OSI network model", Proceedings of the 1st International Workshop on Information Hiding, Vol. 1174, pp. 23-28, June 1996.
33. Ketan Shah, Swati Kaul, Manoj S.Dhande, "Image Steganography using DWT and Data Encryption Standard", International Journal of Science and Research (IJSR), Vol. 3, Issue 5, pp. 372-376, May 2014.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

34. Mrs.Archana S. Vaidya, Pooja N. More, Rita K. Fegade, Madhuri A. Bhavsar, Pooja V. Raut, "Image Steganography using DWT and Blowfish Algorithms", IOSR Journal of Computer Engineering (IOSR-JCE), Vol.8, Issue 6, pp. 15-19, January 2013.

BIOGRAPHY

Mr. Hemang A. Prajapati received the Diploma degree in Electronics and Communication from Sigma Institute of Technology and Engineering, Vadodara, Gujarat, India in 2010. He has received the Bachelor degree in Electronics and Communication from Sardar Vallabhbhai Patel Institute of Technology, Vasad, Gujarat, India in 2013. He is currently pursuing the Master degree in Electronics and Communication Engineering from Sardar Vallabhbhai Patel Institute of Technology, Vasad, India. His research interests include Digital Image Processing.

Dr. Nehal G. Chitaliya received B.E Electrical (1996) and M.E Electrical (2000) and Ph.D. Electrical (2013) from the Electrical Engineering department, Faculty of Technology and Engineering, The M.S. University of Baroda, Vadodara, Gujarat, India. She is Associate Professor of Electronics and Communication Engineering Department, SVIT, Vasad, Gujarat, India. Her research interests are in the field of Digital Image Processing, Signal Processing and Motion Analysis. She is a member of professional bodies like Indian society for Technical Education (ISTE) and International Association of Computer Science and Information Technology (IACSIT).