Highly Secured Dual Steganographic Technique: A Retrospective

Ms. Ketki Thakre
P.G.Student EC Dept SVIT, Vasad

Dr.Nehal Chitaliya
Asst Professor EC Dept SVIT, Vasad

Abstract

The recent growth in computational power and technology has propelled the need for highly secured data communication. One of the best techniques for secure communication is Steganography-a covert writing. It is the art of hiding very existence of communicated message. The process of using steganography in conjunction with cryptography, called as Dual Steganography, develops a sturdy model which adds a lot of challenges in identifying any hidden and encrypted data. Encrypting any secret data before hiding in the cover object will provide double protection. This paper tries to elucidate the basic concepts of steganography, its types and techniques, and dual steganography. It also briefs some of research works done in steganography field in past few years.

1. Introduction

Steganography is the science of invisible communication [1] which hides any private data within an innocent-looking cover object. It is a technique of hiding any confidential data by embedding it inside innocuous medium. The word Steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing” [5].

Steganographic techniques have been used for centuries. Steganography has widely used in historical times, even before cryptographic systems were developed. In Histories the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave’s scalp. When the slave’s hair grew back the slave was dispatched with the hidden message [18]. In the Second World War the Microdot technique was developed by the Germans. Information, especially photographs, was reduced in size until it was the size of a typed period [19]. Early in WW-II Steganographic technology consisted almost exclusively of invisible inks. Common sources for invisible inks are milk, vinegar, fruit juices and urine. All of these darken when heated [3]. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels [2].

Steganography differs from cryptography. The aim of cryptography is to secure communications by changing the data into a form that cannot be understood. Steganography techniques, on the other hand, hide the existence of the message itself, which makes it difficult for a third person to find out where the message is. Sometimes sending encrypted information may draw attention, while invisible information will not. Accordingly, cryptography is not the good solution for secure communication; it is only part of the solution. Both techniques can be used together to better protect information [4]. Digital Watermarking is an advanced technique for hiding secret data. It is the process of inserting digital signal or pattern into digital content. The signal (watermark) is used to identify owner of work, to authenticate content and to trace illegal copies of work.

Steganography can be used for wide range of applications such as defence organizations for safe circulation of private information, intelligence agencies for storing any confidential data, in smart identity cards where personal details are embedded inside the photograph for copyright purpose, medical imaging where patient's details are embedded within image for protection of information and also for reducing transmission time [2].

The paper is organized in the following sections: Section 2 describes the basic steganography model; section 3 describes types of steganography; section 4 describes techniques of steganography; section 5 describes about basic dual steganography model and related research works. Finally conclusion is presented in section 6.

2. Basic Steganography model

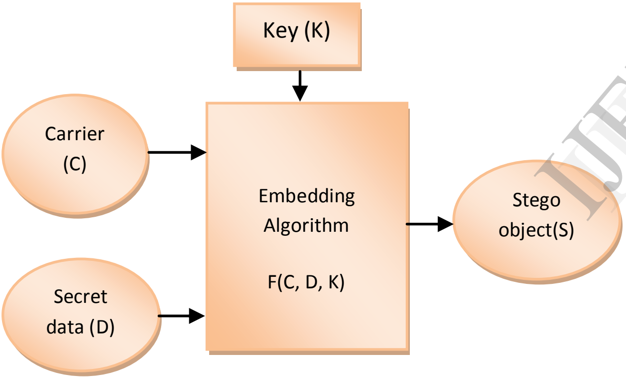

Figure 1. The Steganography Model

The model, shown in figure 1. [2], shows the basic process involved in steganography which consists of Carrier(C), Secret Data(D), Stego Key(K). Carrier is the cover object in which the message is embedded. Secret data can be any type of confidential data that can be plain text, cipher text or other image. Key mainly used to ensure that only recipient having the decoding key will be able to extract the message from a cover-object. By using the embedding algorithm, the secret data is embedded into the cover object in a way that does not change the original image in a human perceptible way. Finally, the stego object which is the output of the process is the cover-object with the secretly embedded data. Recovering secret data from a stego-object requires the cover-object itself and a corresponding decoding key if a stego-key was used during the encoding process [2].

There are four main objectives that need to be considered when designing a steganography system [20, 21]:

a) Imperceptibility: Imperceptibility prevents the naked eye to sense the existence of secret data inside the cover image.
b) Security: Security will provide protection for the confidential data from any attack in the event that the cover image suffers an attack
c) Embedding Payload: Payload means the amount of data that can be embedded within the cover image without affecting the quality of the cover.
d) Robustness against attack: Robustness against attack is the possibility of maintaining the confidential data in the event that the cover image suffers image processing operations such as filtering, compression, rotating, etc.

3. Types of Steganography

The four main categories of file formats that can be used for steganography are: Text, Images, Audio, Video, and Protocol

3.1 Text steganography

The method used to hide a secret message in every nth letter of every word of a text message [4]. It can be classified in three basic categories - format-based, random and statistical generation and linguistic method [23]. Format-based methods uses physical text formatting of text like insertion of spaces, deliberate misspellings distributed throughout the text, resizing the fonts. Random and statistical generation is generating cover text according to the statistical properties. This method is based on character sequences and words sequences [22]. Linguistic method considers the linguistic properties of generated and modified text, frequently uses linguistic structure as a place for hidden messages. Sender sends a series of integer number (Key) to the recipient with a prior agreement that the secret message is hidden within the respective position of subsequent words of the cover text. For example the series is 2, 3, 1, 5, 4, and the cover text is “Five people are still working”. So the hidden message is “ioalk”. A “0” indicate a blank space in the recovered message. If the number of characters in that word is less than the respective number in the series (Key) then it will be skipped during the recovery process [23]. Text stenography using digital files is not used very often because the text files have a very small amount of redundant data.

3.2 Image steganography

Images are used as the popular cover objects for steganography. This technique exploits the weakness of the human visual system (HVS). HVS cannot detect the variation in luminance of color vectors at collection of color pixels. A picture can be represented by a characteristics like 'brightness', 'chroma' etc. Each of these characteristics can be digitally expressed in terms of 1s and 0s [23]. For example: a 24-bit bitmap will have 8 bits, representing each of the three color values (red, green, and blue) at each pixel. If we consider just the red there will be 2 different values of red. The difference between 11111111 and 11111110 in the value for red intensity is likely to be undetectable by the human eye. Here, a message is embedded in a digital image through an embedding algorithm, using the secret key. The resulting stego image is sending to the receiver which on the other side, it is processed by the extraction algorithm using the same key. Unauthenticated persons can only notice the transmission of a stego image but can’t predict the existence of the hidden message [4].

3.3 Audio steganography [23]

Audio steganography takes advantage of the psychoacoustical masking phenomenon of the human auditory system [HAS]. Psychoacoustical or auditory masking property renders a weak tone imperceptible in the presence of a strong tone in its temporal or spectral neighborhood. This property arises because of the low differential range of the HAS even though the dynamic range covers 80 dB below ambient level. Frequency masking occurs when human ear cannot perceive frequencies at lower power level if these frequencies are present in the vicinity of tone- or noise-like frequencies at higher level. Moreover, a weak pure tone is masked by wide-band noise if the tone occurs within a critical band. This property of inaudibility of weaker sounds is used in different ways for embedding information. In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file.

3.4 Video steganography

Video files are generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. When information is hidden inside video the hiding technique will be DCT (Discrete Cosine Transform) method. DCT works by slightly changing each of the images in the video, only so much that it is unnoticeable by the human eye. Precisely, DCT alters values of certain parts of the images, it usually rounds them up. For example, if part of an image has a value of 6.667 it will round it up to 7. [6] The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds. Therefore, any small but otherwise noticeable distortions might go by unobserved by humans because of the continuous flow of information [23].

3.5 Protocol steganography

Protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission [24]. A network packet consists of packet headers, user data and packet trailers. All the packets sent across a network following OSI network model, have the same packet structure. In the layers of the OSI network model there exist covert channels where steganography can be used [25]. . Information can be hidden in the redundant parts of messages and the network control protocols can be used to transmit packets over the network An example of where information can be hidden is in the header of a TCP/IP packet in some fields that are either optional or are never used[24].

4. Techniques

There are several Steganographic techniques for image file format which are as follows: Spatial domain, Transform domain, Masking and filtering, Distortion Techniques

4.1 Spatial domain technique

It is a time domain (pixel based) and here the secret messages are embedded directly. The visibility depends on the amount of data embedded and the image content whether the area is smooth or texture [8]. The most common and simplest Steganography method is the least significant bits (LSB) insertion method.

4.1.1 Least Significant Bit. In the LSB technique, the least significant bits of the pixels are replaced by the message bits which are permuted before embedding [7]. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue color components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data [26]. For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size [26]. Since there are 256 possible intensities of each primary color, changing the LSB of a pixel results in small changes in the intensity of the colors. These changes cannot be perceived by the human eye - thus the message is successfully hidden.

Advantages of spatial domain technique are [4]:

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 [4]:

1) Less robust, the hidden data can be lost with image manipulation.
2) Hidden data can be easily destroyed by simple attacks

4.2 Transform domain

It converts image into appropriate frequency domain [8]. Hiding information in frequency domain is done by altering magnitude of all of transform coefficients of cover image [4]. It is mainly used for watermarking, fingerprinting, broadcast monitoring, and other applications that require low payload but high robustness [8].Its types are JPEG Steganography, DWT, DCT and Spread Spectrum.

4.2.1 JPEG Steganography. Originally it was thought that steganography would not be possible to use with JPEG images, since they use lossy compression which results in parts of the image data being altered. However, properties of the compression algorithm have been exploited in order to develop a steganographic algorithm for JPEGs. One of these properties of JPEG is exploited to make the changes to the image invisible to the human eye [27].

During the DCT transformation phase of the compression algorithm, rounding errors occur in the coefficient data that are not noticeable [7]. Although this property is what classifies the algorithm as being lossy, this property can also be used to hide messages. It is neither feasible nor possible to embed information in an image that uses lossy compression, since the compression would destroy all information in the process. Thus it is important to recognize that the JPEG compression algorithm is actually divided into lossy and lossless stages. The DCT and the quantization phase form part of the lossy stage, while the Huffman encoding used to further compress the data is lossless. Steganography can take place between these two stages. Using the same principles of LSB insertion the message can be embedded into the least significant bits of the coefficients before applying the Huffman encoding. By embedding the information at this stage, in the transform domain, it is extremely difficult to detect, since it is not in the visual domain [27].

4.2.2 Discrete Wavelet Transform (DWT) [13]. The wavelet transform describes a multi-resolution decomposition process in terms of expansion of an image onto a set of wavelet basis functions. Discrete Wavelet Transformation has its own excellent space frequency localization property. Applying DWT in 2D images corresponds to 2D filter image processing in each dimension.

The input image is divided into 4 non-overlapping multi-resolution sub-bands by the filters, namely (LL1), (LH1), (HL1) and (HH1). The sub-band (LL1) is processed further to obtain the next coarser scale of wavelet coefficients, until some final scale "N" is reached. When "N" is reached, we'll have 3N+1 sub-bands consisting of the multi-resolution sub-bands (LLN) and (LHX), (HLX) and (HHX) where "X" ranges from 1 until "N". Due to its frequency localization property, the exploitation of the masking effect of the human visual system such that if a DWT co-efficient is modified, modifies only the region corresponding to that coefficient. The edges and textures of the image and the human eye are not generally sensitive to changes in the high frequency sub-bands (HHX). This allows the stego-image to be embedded without being perceived by the human eye.

4.2.3 Discrete Curvelet Transform (DCT) [28]. The Curvelet transform is a higher dimensional generalization of the Wavelet transform designed to represent images at different scales and different angles. It is a new multiscale representation most suitable for objects with curves. Unlike the wavelet transform, it has directional parameters, and the curvelet pyramid contains elements with a very high degree of directional specicity. In addition, the curvelet transform is based on a certain anisotropic scaling principle which is quite different from the isotropic scaling of wavelets. The elements obey a special scaling law, where the length of the support of a frame elements and the width of the support are linked by the relation width, length.

The digital curvelet transform is implemented using the fast discrete curvelet transform. Basically, it is computed in the spectral domain to employ the advantage of FFT. Given an image, both the image and the curvelet are transformed into Fourier domain, and then the convolution of the curvelet with the image in spatial domain becomes the product in Fourier domain. Finally the curvelet coefficients are obtained by applying inverse Fourier transform on the spectral product.

4.2.4 Spread Spectrum Technique. In spread spectrum techniques, hidden data is spread throughout the cover-image, making it harder to detect [29]. Spread spectrum communication can be defined as the process of spreading the bandwidth of a narrowband signal across a wide band of frequencies [30]. This can be accomplished by adjusting the narrowband waveform with a wideband waveform, such as white noise. After spreading, the energy of the narrowband signal in any one frequency band is low and therefore difficult to detect [30]. In spread spectrum image steganography the message is embedded in noise and then combined with the cover image to produce the stego image. Since the power of the embedded signal is much lower than the power of the cover image, the embedded image is not perceptible to the human eye or by computer analysis without access to the original image [30].

Advantages of Transform Domain:

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

Disadvantages:

1) Very complex techniques
2) Too much computations required

4.3 Masking and Filtering [31]

Masking and filtering techniques hide information in a way similar to watermarks on actual paper and are sometimes used as digital watermarks. Masking images entails changing the luminance of the masked area. The smaller the luminance change, the less of a chance that it can be detected.

Masking techniques embed information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the "noise" level. This makes it more suitable than LSB with, for instance, lossy JPEG images.

Advantages of Masking and filtering Techniques:

1) Highly robust, the information is hidden in the visible parts of the image.

Disadvantages:

1) Restricted to gray scale images and 24 bits.

4.4 Distortion Techniques

Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion [9]. Using this technique, a stego object 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 [32].The message is encoded at pseudo-randomly chosen pixels. If the stego-image is different from the cover image at the given message pixel, the message bit is a “1.” otherwise, the message bit is a “0.” The encoder can modify the “1” value pixels in such a manner that the statistical properties of the image are not affected.

In any steganographic technique, the cover image should never be used more than once. If an attacker tampers with the stego-image by cropping, scaling or rotating, the receiver can easily detect it [33].

Advantages of distortion techniques:

1) Easy embedding
2) Good imperceptibility

Disadvantages:

1) Need for sending the cover image along with stego image

5. 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. The basic model of dual steganography is shown:

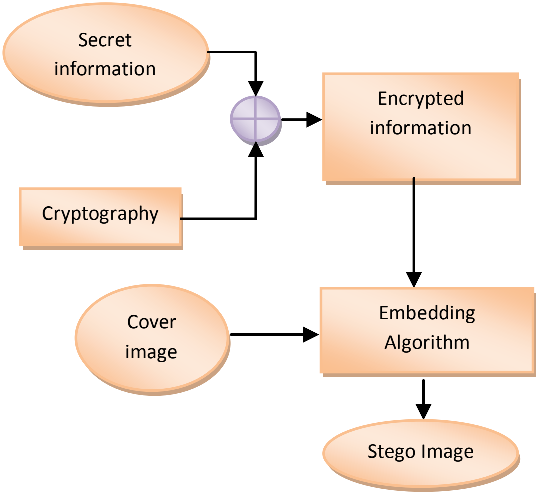

Figure 2. Dual Steganography Model

As shown in the figure2 [10], 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.

Steganalysis is the science of detecting hidden information. The main objective of steganalysis is to break steganography [9].

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.

Some of the related research works are as follows:

Shilpa Gupta, et al [11] developed an enhanced LSB algorithm which embeds the secret data only in one i.e. blue component instead of RGB component whereas in normal LSB replacement method, secret data is hidden in least significant bit of RGB component of a pixel. With this new method, the performance of LSB has been improved and leads to minimization of the distortion level which is negligent to human eye. This will increase the robustness but will decrease the payload capacity.

Shailender Gupta, et al [1] 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.

Mamta Juneja, et al [12] proposed an application of LSB based steganographic technique for 8 bit color images in which combination of image compression and steganography is been used. Compression of 24 bit image to 8 bit image is done while simultaneously encoding desired hidden information. After compression process, the message is embedded in compressed image. Algorithm used will select a palette for 8 bit image which will then be optimized to 8 bit colormap that could be applied with minimal changes to quality of original image. By this method, payload capacity and robustness will be increased but imperceptibility will be somewhat reduced.

Tanmay Bhattacharya, et al [13] proposed a DWT based Dual steganographic technique. Using DWT, a cover image is decomposed into four subbands. Two secret images are hidden within HL and HH subbands respectively by using a pseudo random sequence and a session key. After embedding the secret data, all four subbands including two modified subbands 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.

K.Sakthisudhan, et al [14] proposed a dual steganography approach in which the secret data is firstly converted to encrypted form and then steganography is used to embed it within carrier object. Here carrier object and secret data both are audio files in wav. format. In this work, a key is generated with the help of pseudo sequence and then logical operation is performed with the secret message.

This encrypted message is embedded using LSB method into carrier audio file to form stego audio file. By this technique, message is transferred with utmost security and can be retrieved without any loss of data.

Rosziati Ibrahim and Teoh Suk Kuan [15] developed a SIS (Steganography Imaging System) in which two layers of security are used for maintaining privacy, confidentiality and accuracy of data.

For using this system, firstly username and password are required and once login done, key is used to hide the secret message. Moreover the secret data to be hidden is converted from text file to zip file for masking the contents more securely. Due to this, integrity and privacy is maintained.

Weiqi Luo, Jiwu Huang, et al [16] proposed a technique in which the secret data is hidden inside the edges of the objects in image.

When embedding is done without considering the relationship between image content and size of secret message, smooth or flat regions get contaminated leading to poor visual quality. With proposed scheme, embedding regions are selected according to size of secret message and difference between two consecutive pixels in cover image. Here, LSB matching revisited is used which uses a pair of pixels as embedding unit. Sharper images are selected for hiding data so that security and visual quality is increased.

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.

6. Conclusion

Due to the exponential growth and secret communication of internet users, 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, I have reviewed the basic concepts of steganography, its methods and highly secured dual steganography. 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.

7. References

[1] Shailender Gupta, Ankur Goyal and Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography" *International Journal Modern Education and Computer Science*, June 2012

[2] Kanzariya Nitin K, Nimavat Ashish V., "Comparison of Various Images Steganography Techniques" *International Journal of Computer Science and Management Research*, Vol 2, January 2013

[3] Arvind Kumar, Km. Pooja, "Steganography- A Data Hiding Technique" *International Journal of Computer Applications*, Vol 9, November 2010

[4] Pratap Chandra Mandal, "Modern Steganographic technique: A survey", *International Journal of Computer Science & Engineering Technology*, Vol. 3, September 2012

[5] T. Sharp, "An implementation of key-based digital signal Steganography", *Proc. Information Hiding Workshop, Springer* LNCS 2137, 2001

[6] Johnson, Neil F., "Steganography", 2000 http://www.jjtc.com/stegdoc/index2.html

[7] Johnson, N.F and Jajodia, S., "Exploring Steganography: Seeing the Unseen", *Computer Journal*, February 2008

[8] H. Arafat Ali "Qualitative Spatial Image Data Hiding for Secure Data Transmission" *GVIP Journal*, Vol 7, August 2007

[9] H.S. Majunatha Reddy and K.B. Raja "High capacity and security steganography using discrete wavelet transform" *International Journal of Computer Science and Security*, 2009

[10] Mr. Vikas Tyagi, Mr. 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, March 2012

[11] Shilpa Gupta, Geeta Gujral and Neha Aggarwal, " Enhanced Least Significant Bit algorithm For Image Steganography", *International Journal of Computational Engineering & Management*, Vol. 15, July 2012

[12] Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia, "Application of LSB Based Steganographic Technique for 8-bit Color Images" *World Academy of Science, Engineering and Technology* 50, 2009

[13] Tanmay Bhattacharya, Nilanjan Dey and S. R. Bhadra Chaudhuri, "A Novel Session Based Dual Steganographic Technique Using DWT and Spread Spectrum" *International Journal of Modern Engineering Research*, Vol 1, 2012

[14] K.Sakthisudhan, P.Prabhu, "Dual Steganography Approach for Secure Data Communication" *International Conference on Modeling, Optimization and Computing, Elsevier, Procedia Engineering*, 2012

[15] Rosziati Ibrahim and Teoh Suk Kuan, "Steganography Algorithm to Hide Secret Message inside an Image", *Computer Technology and Application*, February 2011

[16] Weiqi Luo, Jiwu Huang, Fangjun Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited", *IEEE Transactions on Information Forensics and Security*, Vol 5, June 2010

[17] Mazen Abu Zaher, "Modified Least Significant Bit (MLSB)" *Computer and Information Science*, Vol 4, January 2011

[18] Silman, J., "Steganography and Steganalysis: An Overview", *SANS Institute*, 2001

[19] Jamil, T., "Steganography: The art of hiding information is plain sight", *IEEE Potentials*, 1999

[20] S. Hemalatha, Dinesh A.U., A. Renuka, and R.K. Pariya, "A secure and high capacity image steganography technique", *Signal and Image Processing: an International Journal*, Vol 4, 2013

[21] S. Kumar, and S.K. Muttoo, "A comparative study of image steganography in wavelet domain", *International Journal of Computer Science and Mobile Computing*, Vol 2, 2013

[22] Steganography, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213717,00.html

[23] Ronak Doshi, Pratik Jain, Lalit Gupta, "Steganography and Its Applications in Security" *International Journal of Modern Engineering Research*, Vol 2, November-December 2012

[24] Udit Budhiaa, Deepa Kundura. "Digital video steganalysis exploiting collusion sensitivity"

[25] Handel, T. & Sandford, M., "Hiding data in the OSI network model", *Proceedings of the 1st International Workshop on Information Hiding*, June 1996

[26] Krenn, R., "Steganography and Steganalysis", http://www.krenn.nl/univ/cry/steg/article.pdf

[27] T. morkel , J.h.p. eloff , M.s. olivier "An overview of image Steganography" *Information and computer security architecture* research group

[28] M. Prasath and D. Sharmiladevi, "Digital Image Hiding Using Transformation Techniques" *International Journal of Communications and Engineering*, Vol 5, March 2012

[29] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", *Communications of the ACM*, October 2004

[30] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", *IEEE Transactionson image processing*, 1999

[31] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das, " A Tutorial Review on Steganography" *International Conference*,2008

[32] S.C. Katzenbeisser and F. Petitcolas, "Principles of Steganography in Information Hiding Techniques for Steganography and Digital Watermarking", *Ed. London: Artech House*, 2000

[33] P. Kruus, C. Scace, M. Heyman, and M. Mundy, "A survey of steganography techniques for image files" *Advanced Security Research Journal*, 2003