International Journal of Innovative Research in Advanced Engineering (IJIRAE) **ISSN: 2349-2163**
Volume 1 Issue 8 (September 2014) **www.ijirae.com**

Steganography- A Sin qua non for Disguised Communication

Rashmi A. Gandhi
MCA Department
Shri Sunshine College, Rajkot,Gujarat

Atul M. Gosai
Department of Computer Science
Saurashtra University, Rajkot,Gujarat

Abstract -- Steganography is the science of hiding the fact that communication is taking place, by hiding secure information in other information whereas steganalysis is the art of detecting the presence of steganography. Many different carrier formats can be used like image, audio, video or text files but digital images are the most popular due to their ease of availability. The purpose of steganography is defeated if the presence of hidden information is revealed or even suspected. For hiding secret information in images, a large variety of steganographic techniques are available with their respective advantages and disadvantages. Besides, based on the requirement of application different techniques can be employed. Some applications require total invisibility of the secret data while others may require high payload. This paper provides a comprehensive introduction about some of the existing image steganography techniques.

Keywords: Steganography, Cryptography, Data Hiding, Payload, Imperceptibility, LSB, Image Encryption Techniques, computational intelligence, genetic algorithms.

Introduction

"Computer and Communication are having a race and whichever wins, will dominate the other." **Tanenbaum**

Ultimately communication won the race and we know its significance. Importance of networks, their effect and their presence can't be ignored. The widespread use of digital data in real life applications and their importance have craved the need of new and effective ways to ensure their security. The quick development in computer technologies and internet had made the security of information as most important factor in information technology and communication.

Information security is the techniques, policies and strategies used to protect and secure computer systems and important information. The main concern in information security is the concept of information hiding. It is the process of embedding information into digital content without causing perceptual degradation. [9]

There are two main purposes in information hiding: (1) to protect against the detection of secret messages by a passive adversary, and (2) to hide data so that even an active adversary will not be able to isolate the secret message from the cover data.

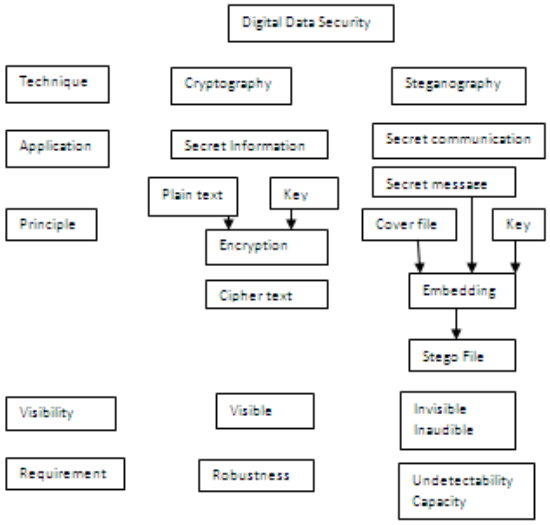
Secret information can be hidden in two ways, like ***Cryptography*** and ***Steganography***. Cryptography makes the data incomprehensible to outsiders by various transformations, whereas the methods of steganography conceal the existence of messages.

The word **Steganography** is derived from the Greek words ***"stegos"*** meaning "cover" and ***"grafia"*** meaning "writing" defining it as **"covered writing"**. **Steganography** is the art and science of secret communication, aiming to conceal the existence of a communication which has been used by revolutionaries, spies, the military, and perhaps terrorists.

In Cryptography, the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem. The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present.

The crucial requirement for steganography is perceptual and algorithmic undetectability. ***If the presence of hidden information is revealed or even suspected the purpose of steganography is defeated*** even if the message content is not extracted or deciphered.

In the present day digital world, where information security is of prime importance Steganography and Cryptography are both excellent tools to protect information from unwanted parties. Both the techniques are competent enough to accomplish this but neither technology alone is perfect and both can be cracked. The strength of Steganography can be improved by combining it with Cryptography.



This paper is intended to provide an overview of the different algorithms used for image Steganography. It demonstrates the suitability of various techniques for different applications. Structure of the paper is as follows: Section 2 gives the reader an overview of Steganography, its origin, and different kinds of Steganography. In section 3, property of image and the most popular algorithms for image Steganography are discussed. Section 4 provides performance evaluation of different techniques. In Section 5 limitations of existing techniques and future improvements are suggested. In section 6 a conclusion is reached.

2: Overview of Steganography

To get in depth knowledge about Steganography, the terms related to Steganography need to be discussed first.

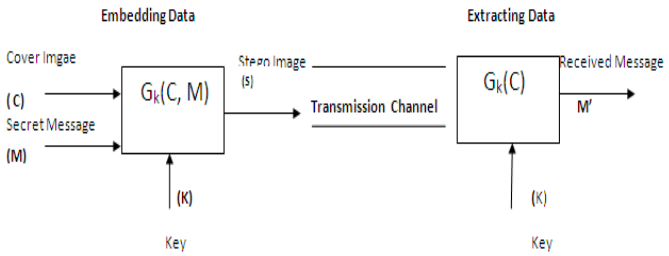
2.1: Basics of Steganography

STEGANOGRAPHY is the study of techniques for hiding the existence of a secondary message in the presence of a primary message. [5] The primary message is referred to as the **carrier signal** or **carrier message**; the secondary message is referred to as the **payload signal** or **payload message or secret message**. Steganography itself offers mechanisms for providing confidentiality and deniability.
The Steganography process can be represented diagrammatically as follows:

The description of the diagram given below is as follows:

- The cover image(C) that will hold the hidden data
- The secret message (M), may be plain text, or cipher text
- An optional stego key (K) if the secret message is a cipher text.
- The stego function G_k.
    - At the sender's end it take the cover image and secret message as input and produces the stego image as output.
    - At receiver end this function works on the stego image and produces the secret message as output.

The output of the Stego function is the Stego image(S).



2.2 History

Steganography ancient origins can be traced back to 440 BC, from the Histories of Herodotus. Histiacus shaved the head of his most trusted slave and tattooed a message on it. After his hair had grown the message was hidden. The purpose was to instigate a revolt against the Persians. Demeratus sent a warning about a forthcoming attack to Greece by writing it on a wooden panel and covering it in wax.
During the 15th and 16th centuries, many writers including Johannes Trithemius (author of Steganographia) and Gaspari Schotti (author or Steganographica) wrote on Steganographic techniques such as coding techniques for text, invisible inks, and incorporating hidden messages in music.
During the times of WWI and WWII, significant advances in Steganography took place like Microdots, and have reused invisible ink and null ciphers (unencrypted messages). It is the technique of taking the 3rd letter from each word in a harmless message to create a hidden message, etc. An example of null ciphers that was sent by a Nazi spy is read as follows:

"A**p**parently neutral's p**r**otest i**s** t**h**oroughly d**i**scounted a**n**d i**g**nored. I**s**man h**a**rd h**i**t. B**l**ockade i**s**sue a**f**fects p**r**etext f**o**r e**m**bargo o**n** b**y** p**r**oducts, e**j**ecting s**u**ets a**n**d v**e**getable o**i**ls."

Sent by a German Spy in WWII, by taking the second letter in each word the following message emerges:

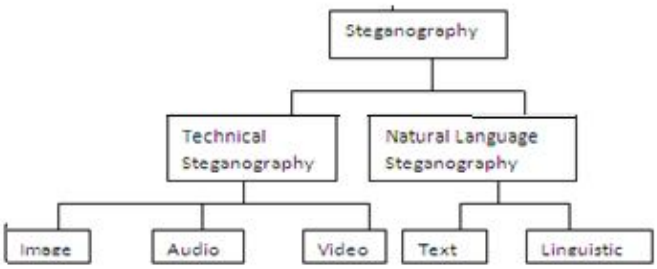
Pershing sails from NY June 1.

Microdot Technology

Shrinking messages down to the size of a dot became a popular method. Since the **microdot** could be placed at the end of a sentence or above a j or an i.

In the digital world of today, namely 1992 to present, Steganography is being used worldwide. Many tools and technologies have been developed taking the help of old steganographic techniques such as null ciphers, coding in images, audio, video and microdot. The continuous demand for information security and wide application area opens a bright future for Steganography in the near future.

2.3: Different kinds of Steganography



Steganography can be divided into two broad categories namely technical steganography and natural language steganography [9]. Technical Steganography is a technique of hiding information inside a medium such as image, audio, and video. Natural language Steganography is the art of using natural language to conceal secret message. It focuses on hiding information in text by using steganography and linguistic steganography.
Johnshon and Katzenbeisser group steganographic techniques into six categories: Substitution system, Transform domain technique, Spread spectrum technique, Statistical methods, Distortion techniques, Cover generation methods.

2.3.1: Image Steganography

The most common cover objects used for steganography are images. The scope of image steganography is large because of the various image formats available such as BMP,JPEG, PNG, GIF etc. The user can use any of the formats as per their convenience. Any simple looking original image is used as the cover-image to conceal the secret data. The secret data are embedded into the cover-image by modifying the cover-image to form a stego-image.

2.3.2: Audio Steganography

Audio steganography, the hiding of messages in audio "noise" (and in frequencies which humans can't hear), is another area of information hiding that relies on using an existing source as a space in which to hide information.[12] The idea of hiding data in audio files originates from the prevailing presence of audio signals as information vectors in our human society.

The most important requirement for steganography demands that the cover utilized to hide messages should not raise any suspicion to opponents.The wide availability and use of audio files make them eligible to carry hidden information. At present the maximum steganalysis efforts are paying attention to digital images leaving the audio steganalysis relatively poor. Data hiding in audio files is especially challenging because of the sensitivity of the HAS (Human Auditory System). However, HAS still tolerates common alterations in small differential ranges. For example, loud sounds tend to mask out quiet sounds. Additionally, there are some common environmental distortions, to the point that they would be ignored by listeners in most cases. These properties have led researchers to explore the utilization of audio signals as carriers to hide data[8].

2.3.3 Text Steganography

Linguistic Steganography

Text steganography is the method of hiding information within text (i.e. character-based) messages. The huge availability of electronic textual information and the difficulty of serious linguistic analysis make this an interesting medium for steganographic information hiding. Text is also one of the oldest media used in steganography. Before the electronic age, letters, books, and telegrams hide secret messages within their texts. There are three basic categories of text steganography: format-based methods, random and statistical generation, and linguistic methods. ***Text steganography*** involves changing the formatting of an existing text, changing words within a text, or generating random character sequences or using context-free grammars to generate readable texts. Whatever be the method, the common denominator is that hidden messages are embedded in character-based text. The differentiating feature of each method is whether or not the text is preexisting or is completely generated by the steganographic tool, and whether or not the resulting text is a result of random generation/modification, "statistical" generation, or linguistically-driven generation/modification. Only linguistically-driven generation and modification of cover texts qualifies as ***linguistic steganography***

3: Image Steganography

As discussed earlier the most common type of steganography is image steganography. Different steganographic techniques have been developed on the basis of the different image formats available.. Each image hiding system consists of an embedding process and an extraction process.

3.1 Image Introduction

A digital image is an arrangement of small dots known as pixels, each having different light intensity [18]. The bit depth is the number of bits in a pixel. The smallest bit depth for color images is 8 (upto 24), which means 8 bits are used to describe the color of each pixel. Thus, 8-bit depth color and grayscale images can display 256 (i.e. 2^8) different colors or shades of grey respectively. A 24-bit color image can display upto 16,777,216 (2^{24}) discrete combinations of Red, Green and Blue values. These images use RGB color model commonly known as true color model. Here, every 8-bits of 24 bits represent one of the three color components i.e. red, green and blue.

3.2 Image Compression

The larger images of greater bit depth take more time to transmit over a standard Internet connection. To display an image in a reasonable amount of time image's file size need to be reduced. Compression is the technique that makes use of mathematical formulas to analyze and condense image data, resulting in smaller file sizes. In images there are two types of compression: lossy and lossless [2]. In both methods storage space is saved but their implementation procedure is different.

Lossy compression creates smaller files by discarding excess image data that are too small for the human eye to differentiate from the original image. The image format that uses this compression technique is JPEG.

Lossless compression never removes any information from the original image, but instead represents data in mathematical formulas. The original image's integrity is maintained and the decompressed image output is bit-by-bit identical to the original image input. The most popular image formats that use lossless compression is GIF and 8-bit BMP.

Compression plays a very important role in choosing which steganographic algorithm to use. Lossy compression techniques result in smaller image file sizes, but the possibility that the embedded message may be partly lost. Lossless compression, on the other hand keeps the original digital image intact without the chance of lost, although file size is not that small.

3.3 Digital Image Formats

A) GIF (Graphics Interchange Format)

The GIF format supports up to 8-bits per pixel, thus allowing a single image to reference a palette of up to 256 distinct colors. GIF format is suitable for storing graphics with relatively few colors such as simple diagrams, shapes, logos and cartoon style images. The GIF format supports animation and is still widely used to provide image animation effects. It also uses a lossless compression.

B) BMP: Bitmap Image File
This image format is common for MS Windows. The BMP images are large in size and their quality varies from medium to high. BMP files are uncompressed; hence they are large in size.
C) JPEG (Joint Photographic Experts Group)
JPEG is a commonly used file format of lossy compression for digital image. This is the most widely used image format for photographic images. JPEG images are of high quality and small in size.
D) PNG (Portable Network Graphics)
This file format was created as the free, open-source successor to GIF. The PNG file format supports 8 bit paletted images and 24 bit truecolor (16 million colors) or 48 bit truecolor with and without alpha channel - while GIF supports only 256 colors and a single transparent color. Compared to JPEG, PNG excels when the image has large, uniformly colored areas.

3.4: Classification of Image Steganography Techniques

Image steganography based on substitution approach can be divided into three groups [10]:
Spatial Domain Technique group: It embeds information in the intensity of the pixels directly. Advantages are high embedding capacity, ease of implementation and imperceptibility of hidden data. The major drawback is its vulnerability to various simple statistical analysis methods.
Transform Domain Technique group: This technique, first transforms the cover-image into its frequency domain, secret data is then embedded in frequency coefficients. Advantages include higher level of
robustness against simple statistical analysis. Unfortunately, it lacks high payload.
Compression Domain Technique Group: Secret data is embedded into compression codes of the cover-image which is then sent to the receiver. It is of great importance where bandwidth requirement is a major concern.

3.5 Naïve implementation of Steganographic technique

The simplest way of accomplishing Steganography is by feeding into a Windows operating systems command prompt the following code:
C :\> Copy cover.jpg /b + Msg.txt /b Steg.jpg The above code appends the secret message found in the text file 'Msg.txt' into the JPEG image file 'Cover.jpg' and gives the output stego-image 'Steg.jpg'. Here the message is packed and inserted after the EOF tag. When 'Steg.jpg' is viewed using any photo editing application, it will just display the picture ignoring anything coming after the EOF tag. This simple technique does not resist any steganalysis attack.

3.6 Spatial Domain Technique group

Pixel's color is represented by giving an ordered triplet of numbers: red (R), green (G), and blue (B) that comprises particular color. The other way is to use a table known as palette to store the triplet, and put a reference into the table for each pixel. The spatial domain-based steganographic techniques use LSB algorithm for embedding/extraction of data.

3.6.1 EzStego Data Hiding

EzStego data hiding scheme [10] was given by Machado. In this method palette is first sorted by luminance to minimize the perceptual distance between consecutive colors. EzStego then embeds the secret data into the lSB of the indices pointing to the palette colors. This approach works quite well in gray scale images and may work well in images with related colors. The major drawback is, since luminance is a linear combination of colors R, G, and B (Luminance = 0.299 R + 0.587 G + 0.144 B), occasionally colors with similar luminance values may be relatively far from each other. Other drawbacks are the ease of extraction of hidden data, dependency of stego-image quality on number of palette colors, and ease of detection of presence of data using simple statistical histogram analysis.
Fridrich proposed a palette modification scheme for hiding data. In this method, both the cost of removing an entry color in a palette and the benefit of generating a new one to replace it are calculated. If the maximal benefit exceeds the minimal cost, entry color is replaced. This method remarkably reduces the distortion of the carrier images, but suffers with the low embedding capacity as EzStego does**. *Cheng***
proposed high embedding capacity technique that can hide 1 bit to 8 bits per pixel, and has no distortion in contrast to EzStego. High capacity data hiding algorithm based on relevance of adjacent pixels difference was given by Ren. Ren's method guarantees the better quality of image after hiding mass information.

3.6.2 S-Tools, Hide & Seek, StegoDos, White Noise Storm and other techniques

S-Tools by Andy Brown [10] reduces the number of colors from 256 to 32 while maintaining the image quality. S-Tools manipulate the palette to produce colors that have a difference of one bit. Non-linear insertions in S-Tools method make the presence and extraction of secret data more difficult and achieve better results in terms of visual perceptibility.

Hide & Seek given by Maroney uses lsb of each pixel to encode characters of secret data and has embedding capacity which is restricted to 1/8th of the size of the cover-image. **StegoDos** [10] works only with 320 X 200 pixels image and involves much effort in encoding and decoding of the secret message. **White Noise** Storm includes encryption to randomize the bits within an image and suffers with the problem of using large cover file. Younes [10] proposed a method in which data is inserted into lsb of each byte within the cover-image in encrypted form.

3.6.3 Bit Plane Complexity Segmentation Steganography

Bit plane complexity segmentation steganography (BPCS) was introduced by Kawaguchi [10]. It is based on the idea that the higher bit planes can also be used for embedding information. In BPCS, each block is decomposed into bit-plane. The lSB plane would be a binary image consisting of the lSB of each pixel in the image. In each segmented bit-plane its complexity is analyzed and based on a threshold value block is divided into 'informative region' and 'noise-like region' and the secret data is hidden in noise regions without degrading image quality. BPCS provides high embedding capacity and least degradation of the cover-image as compared to traditional lSB manipulation techniques.

3.6.4 Dynamic Programming-based Steganographic Technique

Mielikainen [10] proposed lSB matching revised technique to achieve data hiding. Advantage is that for hiding two secret bits in a pair of cover pixels, only one cover pixel is need to be modified. To illustrate Mielikainen's method, consider two cover pixels (y1, y2) and two secret bits (s1, s2). Mielikainen's method defines a formula called as binary function as F (y1, y2) = LSB (y1/2 + y2). The function LSB(x) stands for the value of the lSB of the pixel x. More precisely, the more frequently the Case 1 occurs, the better the results Mielikainen's method
can obtain.

3.6.5 Data Hiding using Information Secret Sharing Method

Threshold secret sharing (k, n) method was proposed by Shamir, where a secret d in the form of an integer is to be shared, n is the number of participants in the secret sharing activity, and k is a threshold specifying the minimum number of shares which should be collected to recover the secret. D.lee used Shamir's sharing method and proposed information-sharing-based data hiding method. Secret data string is transformed next into shares using the coefficients of

3.7 DATA HIDING TECHNIQUES IN FREQUENCY DOMAIN

Frequency domain methods hide messages in significant areas of the cover-image which makes them more robust to attacks such as compression, cropping or image processing methods than lSB approach and moreover they remain imperceptible to the human sensory system as well. Many transform domain variations exist, one of which is discrete cosine transform (DCT).

3.7.1 JSteg, JPHide, and OutGuess

JSteg developed by Derek Upham [18] sequentially replaces the LSB of the DCT coefficients with the message's data. After quantization, this algorithm skips all coefficients of value 0 or 1 and replaces the LSB's of the rest of the frequency coefficients by the secret message [12]. This technique does not require a shared secret, hence can be easily caught by any steganalysis system **JPHide** steganographic system was given by Allan Latham[18]. Two versions 0.3 and 0.5 are available. Version 0.5 supports additional compression of the secret message. As the DCT coefficients are not selected sequentially from the beginning of the image Provos proposed **OutGuess** was as a response to the statistical tests given by Andreas Westfeld. It improves embedding by selecting DCT coefficients randomly.

3.7.2 F3, F4 and F5

F3

Contrary to Jsteg, F3 makes use of coefficients having value 1. It decrements the coefficient's absolute values if their LSB does not match—except coefficients having value 0, because the absolute value can't be decremented in this case. That's why zero coefficients are not used steganographically. Main flaw in F3 technique is that several embedded bits become victim to shrinkage which occurs when F3 decrements the absolute values of 1 and −1 resulting in a 0.

F4

F4 algorithm eliminates the shortcomings of F3 by
mapping negative coefficients to the inverted steganographic values i.e. even negative coefficients represent a one (steganographically produced), odd negative a zero, even positive represent a zero (same as with Jsteg and F3), and odd positive a one.

F5

F5 algorithm selects DCT coefficients randomly to
embed secret data bits. Thereafter, it applies matrix embedding, due to which the changes needed on the cover image to embed secret bits get reduced.

4 Performance Evaluation of Different Steganographic techniques

The steganographic algorithms that we considered above, algorithms which are not discussed or the future emerging algorithms all need to fulfill a set of criteria.

Invisibility – The invisibility of a secret message is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye.
Payload capacity – It is the amount of secret data that can be hidden in the cover object. Steganographic algorithms demands sufficient embedding capacity.
Robustness against statistical attacks[3] – Statistical steganalysis is the practice of detecting hidden information through applying statistical tests on image data. Many steganographic algorithms leave a 'signature' when embedding information that can be easily detected through statistical analysis. To be able to pass by a warden without being detected, a steganographic algorithm must not leave such a mark in the image as be statistically significant.

Robustness against image manipulation
Image manipulation, such as cropping or rotating, can be performed on the image during its transition from source to intended destination. Depending on the manner in which the message is embedded, these manipulations may destroy the hidden message. It is preferable for steganographic algorithms to be robust against either malicious or unintentional changes to the image.
Independent of file format
The Steganographic algorithms must possess the ability to embed information in any type of file. This also solves the problem of not always being able to find a suitable image at the right moment, in the right format to use as a cover image.
Unsuspicious files – This requirement includes all characteristics of a steganographic algorithm that may result in images that are not used normally and may cause suspicion. Abnormal file size, for example, is one property of an image that can result in further investigation of the image by a warden.

5 Limitations and Future Improvements

Existing steganographic algorithms are providing a trade-off between imperceptibility and payload. Lot many techniques are developed and further work is going on to find new dimensions. Research work is going on to take the help of artificial intelligence approach to improve the steganographic methods.

6. Conclusion

Being a researcher for research on Audio Encryption technique for secure communication, we started to explore different steganographic technique and its use in my research work. I have examined all possible techniques and read all algorithms to find whether any algorithm can be applicable or I can take some ideas in my work. So during this process I have summarized few of the studied steganographic techniques. The present paper gives an idea about the recent work in field of steganography. Here the discussion was focused on image steganography. The spatial, transform, and compression domain techniques are discussed. Transform domain techniques make changes in the frequency coefficients instead of manipulating the image pixels directly, thus distortion is kept at minimum level and that's why they are preferred over spatial domain techniques.

Spatial domain techniques give better results in terms of embedding capacity. However, there exists a trade-off between the image quality and the embedding capacity. Hiding more data results directly into more distortion of the image. A particular steganography technique is dependent on the type of application requirement.Recent research work is focusing on applying new emerging techniques like adaptive technology, computational intelligence, and genetic algorithms to improve the capability of steganography. Steganography can be misused by anti-social elements. However if used properly it will remain the point of attraction for researchers.

References:

[1] Amanpreet Kaur, Renu Dhir, and Geeta Sikka *"A New Image Steganography Based On First Component Alteration Technique,"(IJCSIS) International Journal of Computer Science and Information Security,Vol. 6, No. 3, 2009.*
[2] T. Morkel, J.H.P. Eloff, M.S. Olivier**,"**AN OVERVIEW OF IMAGE STEGANOGRAPHY**,"** *Information and Computer Security Architecture (ICSA) Research Group*
[3] Swati Tiwari, R. P. Mahajan and Neeraj Shrivastava**, "**Steganography- An Approach for Data Hiding Based on Encryption and LSB Insertion" *Proceedings of the 5th National Conference; INDIACom-2011.*
[4] Jyoti, Md. Sabir, "Genetic Algorithm Based Image Steganography for Enhancement of Concealing Capacity and Security," *I.J. Image, Graphics and Signal Processing,* 2013, 7, 18-25
Published Online June 2013 in MECS (http://www.mecs-press.org/).
[5] Mazdak Zamani, Azizah A. Manaf,, Rabiah B. Ahmad, Akram M. Zeki, and Shahidan Abdullah, "A Genetic-Algorithm-Based Approach Audio Steganography," *World Academy of Science, Engineering and Technology.*
[6] Hengfu YANG, Xingming SUN, Guang SUN, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution," RADIOENGINEERING, *VOL. 18, NO. 4, DECEMBER 2009*
[7] Manish Mahajan, Dr. Navdeep Kaur, "Adaptive Steganography: A survey of Recent Statistical Aware Steganography Techniques," *I. J. Computer Network and Information Security,* 2012, *Published Online September 2012 in MECS.*
[8] Fatiha Djebbar, Beghdad Ayad, Karim Abed Meraim and Habib Hamam, "Comparative study of digital audio steganography techniques", *Djebbar et al. EURASIP Journal on Audio, Speech, and Music Processing 2012.*
[9] Roshidi Din and Azman Samsudin, "Digital Steganalysis: Computational Intelligence Approach", *INTERNATIONALJOURNAL OF COMPUTERS Issue 1, Volume 3, 2009.*
[10] Babloo Saha and Shuchi Sharma, "Steganographic Techniques of Data Hiding using Digital Images", Defence Science Journal, Vol. 62, No. 1, January 2012.
[11] Chiang-Lung Liu, Shiang-Rong Liao, "High-performance JPEG steganography using complementary embedding Strategy".
[12] Krista Bennett, "LINGUISTIC STEGANOGRAPHY: SURVEY, ANALYSIS, AND ROBUSTNESS CONCERNS FOR HIDING INFORMATION IN TEXT"**,** *CERIAS Tech Report 2004-13*
[13] Ching-Yun Chang, Stephen Clark, "Linguistic Steganography Using Automatically Generated Paraphrases".
[14] Kaustubh Choudhary, "Mathematical Modeling of Image Steganographic System", *OSRJournal of Computer Engineering (IOSRJCE), Volume 2, Issue 5 (July-Aug. 2012)*
[15] Andrew D. Ker, Patrick Bas, Rainer Böhme, "Moving Steganography and Steganalysis from the Laboratory into the Real World".
[16] Neil F. Johnson, Sushil Jajodia," Exploring Steganography: Seeing the Unseen"
[17] Bin Li, Junhui He, "A Survey on Image Steganography and Steganalysis," Journal of Information Hiding and Multimedia Signal Processing 2011, Ubiquitous International Volume 2, Number 2.
[18] Awdhesh Kumar Shukla, Vishu, "Steganography for Invisible Communication: A Review", International Journal of Advanced Research in Computer Science

