International Journal of Advanced Science and Technology
Vol.60, (2013), pp.45-58
http://dx.doi.org/10.14257/ijast.2013.60.05

Overview of Digital Steganography Methods and Its Applications

V. Nagaraj[1], Dr. V. Vijayalakshmi[2], and Dr. G. Zayaraz[3]
[1]*Research scholar,* [2]*Assistant Professor,*[3]*Professor,*
[1,2]*Department of Electronics and Communication Engineering,*
[3] *Department of Computer Science and Engineering,*
[1.2.3]*Pondicherry Engineering College,*
Puducherry-605014, India
[1]*nagu.n84@gmail.com*

Abstract

Steganography is the skill of communicating secret data by embedding it into multimedia carriers like image, audio, videos. The ultimate goal here is to mask the very existence of the embedded data. Even though the term Steganography has been known for thousands of years, its digital form came about only lately and research was make stronger after the depressing event on 11th Sep 2001(Twin towers). In contrast to Steganography, Steganalysis is the official counter attack science used for detects and or estimate the hidden information with little knowledge of Steganography algorithms. Steganography's ultimate intentions are robustness, undetectability, and size of the hidden data. This paper provides a survey review and analysis of the different existing methods of steganography along with some common standards and guidelines drawn from the literature. This paper completes with some recommendations and advantages of Steganography techniques and current research scopes.

Keywords: *Steganography, Steganalysis, discrete cosines transform, least significant bit, adaptive algorithm, spatial domain, frequency domain, security, embedding payload*

1. Introduction

Steganography word is of Greek origin and essentially means covered writing. Greek words "stegos" meaning "cover" and "grafia" meaning "writing" so it define as covered writing. Steganography is defined by Markus Kahn as follows; Steganography is the art and science of communicating in a way which hides the existence of the communication. Steganography differs from cryptography in the sense that where cryptography focuses on secure communication, steganography focuses on secure and secret communication. In Cryptography, where the enemy is allowed to identify, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the aim of Steganography is to hide messages inside other harmless carrier in a way that does not allow any enemy to even detect that there is a second message present.

In a digital world, Steganography and Cryptography are both intended to protect information from unwanted users. Both Steganography and Cryptography are excellent means by which to accomplish this but neither technology alone is perfect and both can be broken. It is for this intention that most experts would suggest using both to add multiple layers of security. The watermarking and fingerprinting are other technologies that are closely related to steganography.

Steganography can be used in a large amount of data formats in the digital world of today. The most common data formats used are .txt, .doc, .bmp, .gif, .jpeg, .mp3, .avi and .wav.

ISSN: 2005-4238 IJAST

Mainly because of their popularity on the Internet and the ease of use of the steganography tools that use these data formats. These formats are also famous because of the relative ease by which redundant or noisy data can be removed from them and replaced with a hidden message. Steganography technologies are very important face of the future of Internet security and privacy on open systems such as the Internet. Many governments have created laws that either limit the strength of cryptosystems or prohibit them completely. This has been done mainly for fear by law enforcement not to be able to gain intelligence by wiretaps, *etc*., This unfortunately leaves the popular of the Internet community either with relatively weak and a lot of the times breakable encryption algorithms or none at all. [1] Civil liberties advocates fight this with the argument that “these limitations are an assault on privacy”. This is where Steganography comes in. Steganography can be used to hide significant data inside another file so that only the parties intended to get the message even knows a secret message present. To add multiple layers of security and to help sub side the "crypto versus law" problems previously mentioned, it is a good exercise to use Cryptography and Steganography together. As mentioned prior, neither Cryptography nor Steganography are considered "turnkey solutions" to open systems privacy, but spending both technologies together can offer a very acceptable amount of privacy for anyone connecting to and communicating over these systems.

2. The Classic Steganography and its Limitation

The earliest recordings of Steganography were by the Greek historian Herodotus in his chronicles known as "Histories" and date back to nearby 440 BC. Herodotus documented two stories of Steganography techniques during his time in Greece. The first stated that King Darius of Susa shaved the head of one of his prisoners and wrote a secret message on his scalp. When the prisoner’s hair grew back, he was sent to the Kings son in law Aristogoras in Miletus undetected. The second story also came from Herodotus, which statements that a soldier named Demeratus needed to send a message to Sparta that Xerxes intended to invade Greece. Back then, the writing medium was text written on wax covered table. Demeratus removed the wax from the table, wrote the secret message on the underlying wood, recovered the table with wax to make it appear as a blank table and finally sent the document without being noticed. Romans used invisible inks, which were based on natural elements such as fruit juices and milk. This was succeeding by heating the hidden text, thus revealing its contents. Invisible inks have become much more advanced and are still in limited use today.

One of the earliest known forms of image steganography was done in the early twentieth century. During the Boer War in South Africa, the British were using Lord Robert Baden Powell as a scout. He was scouting the Boer artillery bases mapping their positions. He took his maps and converted them into pictures of butterflies with certain markings on the wings that were actually the enemies’ positions.

During the times of WWI (World War I) and WWII (World War II), significant advances in Steganography took place. Ideas such as null ciphers (taking the 3rd letter from each word in a harmless message to create a hidden message, *etc*.), image substitution and microdot (taking data such as pictures and reducing it to the size of a large period on a piece of paper) were introduced and embraced as great steganography techniques.

In the digital world of today, Steganography is being used all over the world on computer society. Many tools and technologies have been generated that take advantage of old steganography techniques such as null ciphers, coding in images, audio and video. With the research this topic is now receiving a lot of great applications for Steganography in the near future.

3. Security Issues in Steganography

It is not enough if a Steganography is imperceptible. The prime concern is about undetectability. Only a naive steganography hides messages "invisibly". A good steganography is undetectable or at least very hard to detect by any means provided the original cover is not known. It is also not enough for a steganography system to be just secure; it also needs to have high capacity. For example a method that may hide very few bits of data in a cover image securely is not very viable. Perfect means that the mutual information between the presence of a stego message and the observed content is null. It means that there is no information leakage about the presence of stego content. Steganography usually entails one person communicating with one other. In practice, this means the message need only survive during transmission over a known channel, such as e-mailing an image. However, if the message refers to the cover work, it can assume that it's relevant as long as the cover work is recognizable, and it wants to be robust to all processing that doesn't destroy the work. This leads to the emphasis on robustness in steganography literature. The central issue in steganography is not the issue of perceptibility, but rather the issue of suspiciousness. That is, the work in which the message is hidden must be unsuspicious. Suspiciousness is very different from perceptibility.

4. Applications of Steganography

The main applications of the steganography are used for secret invisible communication between the two persons in the open communication system.

- To be necessary for secure and secret communications where strong cryptography is impossible.
- In some cases, for example in military uses, even the knowledge that two parties communicate can be of large importance.
- The medical image and Electronic Identification Card systems may very much benefit from information hiding techniques.

Online Voting systems and Online Banking operation are current applications of Steganography.

5. Literature Survey

In recent years steganography techniques received much attention from the research world, many researchers have spent considerable effort in designing several steganography algorithms.

F. Petioles *et al.*, [2] explained the information hiding techniques and also briefed the future directions in hidden communication system. An obvious method was to hide a secret message in every n^{th} letter of every word of a text message. Text steganography using digital files is not used very often since text files have a very small amount of redundant data.

W. Bender *et al.*, proposed a technique for data hiding techniques for addressing the data hiding process and evaluate these techniques in light of three applications: tamper proofing, copyright protection and augmentation data embedding [3]. H. Farid in his work [4] paper presents improved methods for information hiding. J. Fridrich *et al.*, in her work [5] Detecting LSB Steganography in Color and Gray Scale Images. This work describes liable and accurate method for detecting least significant bit (LSB) non sequential embedding in digital images.

Practical Steganalysis of Digital Images has explained [6] the problems encountered in deploying jpeg images and the universal blind detection schemes and special cases such as

JPEG compatibility Steganalysis. A Double Layered "Plus-Minus One" Data Embedding Scheme has been developed by W. Zhang *et al.*, [7]. This work can hide a longer message than simple LSB embedding. Attacks on Steganography Systems were analyzed [8] by A. Westfeld and A. Pfitzmann.

X. Zhang and S. Wang in their paper [9] efficient steganography embedding by exploiting modification direction deals with the steganography embedding process especially on the Internet and given the large amount of redundant bits present in the digital representation of an image.

H. Zhang and H. Tang proposed in their paper [10] a novel image steganography algorithm against statistical analysis. This is an easiest method for embedding messages in an image with high capacity. It is not detectable by statistical analysis such as RS and Chi-square analysis.

J. Kang *et al.*, in their paper [11] Steganography using block based adaptive threshold method used encoder and decoder design for image steganography. Attack against Statistical Steganalysis and given the proliferation of digital images on the Internet, and given the large amount of redundant bits exist in the digital representation [12] of an image was dealt in depth by N. Provos.

J. Fridrich and P. Lison in their paper efficient steganography embedding by Grid coloring [13] in image steganography discuss a different technique unique to audio steganography is concealing, which exploits the properties of the human ear to hide information unnoticeably. A weak, but audible, sound becomes inaudible [14] in the presence of another louder audible sound.

Shivendra Katiyar *et al.*, are explained new Steganography application in Online Voting System. The basic idea of that system is to merge the secret key with the cover image on the basis of key image. The result of that process produces a stego image which looks quite similar to the cover image but not noticeable by human eye. The system targets the validation requirement of a voting system.

6. Information Hiding

The General Classifications of Information Hiding is shown in the Figure 1. Depending on the meaning and goal of the embedded metadata, several information hiding fields can be defined, even though in literature this term is often used as a synonym for steganography. In a broad sense, 'information hiding' could be classified into two, steganography and watermarking.

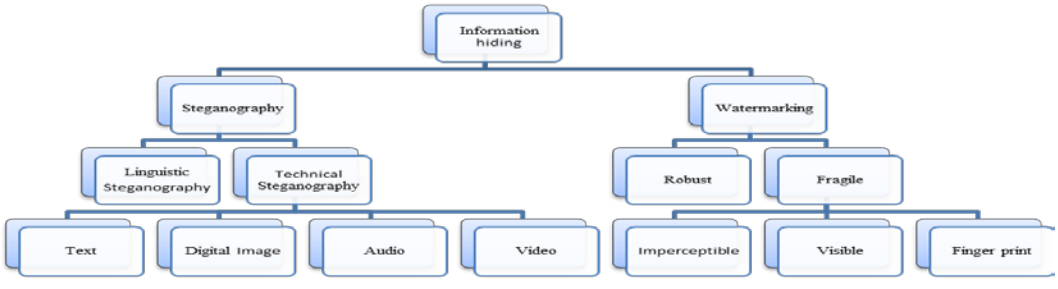

Figure 1. General Classifications of Information Hiding

7. Steganography vs. Digital Watermarking

Digital Information Hiding is the protection or concealing of digital information. Steganography and Digital Watermarking are both sub disciplines of information hiding. Steganography is a way of hiding pertinent information. An example of Steganography is sending a message containing invisible ink. The message appears to be saying one thing but the invisible ink contains the true message. This concept can also be applied to audio by hiding echoes that are not easily detected within other audio context. Watermarking unlike Steganography focuses on the robustness of the information being hidden or protected. The goal of Watermarking is for the watermarked information to be irremovable. In fact, although primary focus is on invisible watermarks, this is not a requirement. Watermarking focuses on protecting digital content and therefore the watermarked information is always related to the digital content it is applied to. Steganography does not follow this criterion while it is possible that the information being hidden is related to the digital content itself, in many cases the digital content is simply a decoy to hide the pertinent hidden information.

Steganography is usually applied to a one-to-one relationship and it is a two-way communication. Data is hidden by one individual for another individual to decode. Watermarking is usually applied to a one-to-many relationship and the communication is one-way. Data is watermarked by one to prevent the theft by many.

Table 1. Comparison of Steganography and Watermarking

Watermarking	***Steganography***
Main goals are copyright protection and information authentication.	Main goal is covert communication.
Inserts information related either to the host signal or its owner.	Inserts any kind of information.
Is either visible or imperceptible.	Must not only be imperceptible but also statistically undetectable.
Is for communications point-to-multiple points.	Is for communications point-to-point.
Capacity is not an important issue.	Capacity is an important issue.
Robustness is an important issue.	May be robust (not necessary).

8. Steganography Techniques

8.1. Image Steganography

8.1.1. LSB (Least Significant Bit)

A simple way of steganography is based on modifying the least significant bit layer of images, known as the LSB technique. In the LSB technique, the least significant bits of the pixels is replaced by the message which bits are permuted before embedding. In some cases (Fridrich *et al.*, [4]) LSB of pixels visited in random or in certain areas of image and sometimes increment or decrement the pixel value.

Still image steganography

The most widely used technique today is hiding of secret data into a digital image. This steganography technique exploits the faintness of the human visual system (HVS). HVS cannot notice the variation in luminance of color vectors at higher frequency side of the visual band. A picture can be represented by a collection of pixels. The individual pixels can be represented by their optical characteristics like 'brightness', 'chroma' *etc*. The characteristics

of images can be digitally expressed in terms of 1s and 0s. For example: a 24-bit bitmap image will have 24 bits, representing 8 bit for each of the three color values (red, green, and blue) at each pixel. Consisting blue there will be 28 different values of blue. The change between 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye. Hence, if the terminal recipient of the data is nothing but HVS then the Least Significant Bit (LSB) can be used for something else other than color information. This technique can be applied on digital image in bitmap format as well as for the compressed image format like JPEG. In compressed image format, each pixel of the image is digitally coded using discrete cosine transformation (DCT). The LSB of encoded DCT components can be used as the carriers of the hidden data. The details of above techniques are explained below:

Modification of cover image in 'bitmap' format using LSB
In this method binary equivalent of the message (to be hidden) is distributed among the LSBs of each pixel [14]. For example: the character 'A' as to hide inside an 8-bit image. Eight consecutive pixels from top left corner of the image are taken.
The equivalent binary bit pattern of those eight pixels is given:
00100111 11101001 11001000 00100111 11001000 11101001 11001000 00100111
Then binary equivalence of letter 'A' **01100101** is embedded serially (from the left hand side) to the LSB's of equivalent binary pattern of pixels, results of the bit pattern will become like this: -
00100110 11101001 11001001 00100110 11001000 11101001 11001000 00100111
Attacks like image compression and formatting having a problem on this technique.

8.1.2 DCT (Discrete Cosines Transform)
DCT is used in JPEG compression. Embedding in DCT domain is simply done by altering the DCT coefficients[16]. One of the limitation in DCT domain happened when 64 coefficients are equal to zero. Values will have an importance on the compression rate. So the number of bit one could embed in DCT domain is less that the number of bits one could embed by the LSB method. Also embedding capacity becomes dependent on the image type used in the case of DCT embedding.

Modification of a cover image in 'bitmap' format using DCT
The following steps are followed in DCT: -
1. The Image is broken into data units each of them consists of 8 x 8 block of pixels.
2. Working from top-left to bottom-right of the cover image, DCT is applied to each pixel blocks.
3. After applying DCT, one DCT Coefficient is generated for each pixel in data unit.
4. Each DCT coefficient is then quantized against a reference quantization table.
5. The LSB of binary equivalent the quantized DCT coefficient can be replaced by a bit from secret message.
6. Encoding is then applied to each modified quantized DCT coefficient to produce compressed Stego Image.

(a) Cover image (b) Stego image

Figure 2. Example of Image Steganography

Figure 2 shows the Left hand side image is the original cover image, whereas right hand side is the stego image which is secret text embedded into the cover image.

8.2. Audio and Video Steganography

In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the cover audio file. There are various approaches are available for audio steganography. Some of the approaches are as follows: -

- *LSB Coding*: Sampling method followed by Quantization converts analog audio signal tosequence.

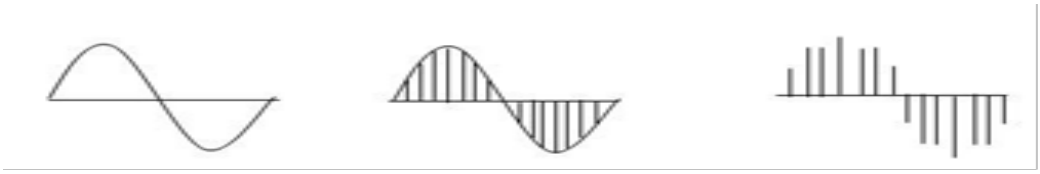

Figure 3. Sampling of the Sine Wave followed by Quantization Process

In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message. For example: the letter 'A' (binary equivalent 01100101) is embedded in to digitized audio file where each sample is represented with 16 bits, then LSB of 8 consecutive samples (each of 16 bit size) is replaced with each bit of binary equivalent of the letter 'A'.

Sampled Audio Stream (16 bit)	'A' in binary	Audio Stream with Encoded Message
1011 1000 0011 1100	0	1011 1000 0011 110**0**
1111 1011 0011 1000	1	1111 1011 0011 100**1**
1010 1100 1011 1101	1	1010 1100 1011 110**1**
1001 1111 0011 1100	0	1001 1111 0011 110**0**
1010 1010 0111 1111	0	1010 1010 0111 111**0**
1011 1010 0011 1100	1	1011 1010 0011 110**1**
1100 1100 0111 1000	0	1100 1100 0111 100**0**
1010 1000 0001 1111	1	1010 1000 0001 111**1**

- *Phase Coding:* Human Auditory System (HAS) can't recognize the phase change in audio signal as easy it can recognize noise in the signal [17, 18, and 19]. The phase coding technique exploits this fact. This technique encodes the secret message bits as phase shifts in the phase spectrum of a digital signal, attaining an inaudible encoding in terms of signal-to- noise ratio.
- *Spread Spectrum:* There are two approaches are used in this technique: the direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS). Direct sequence spread spectrum (DSSS) is a modulation technique used in telecommunication [20]. As with other spread spectrum technologies, the transmitted signal takes up more spectrum bandwidth than the information signal that is being modulated. DSSS transmissions multiply the data being transmitted by a noise signal. This noise signal is a pseudorandom sequence of 1 and −1 values, at a frequency higher than that of the original signal, thereby spreading the energy of the original signal into a much wider band. The resulting signal looks like white noise. This noise like signal can be used to exactly reconstruct the original data at the receiving end by multiplying it, by the same pseudorandom sequence. This process is known as *de-spreading*, mathematically establishes a correlation of the transmitted Pseudo random Noise (PN) sequence with the receiver's expected sequence. For de-spreading to work properly, transmit and receive sequences must be synchronized. This requires the receiver to synchronize its sequence with the transmitter's sequence via some sort of timing search process.

In contrast, FHSS pseudo randomly retunes the carrier, instead of adding pseudo random noise to the data, which results in a uniform frequency distribution whose width is determined by the output range of the pseudo random number generator.

- *Echo Hiding*: In this method the secret message is embedded into cover audio signal as an echo. Parameters of the echo of the cover signal namely amplitude, decay rate and offset from original signal are varied to represent encoded secret binary data. These data are set below to the threshold of Human Auditory System (HAS) so that echo can't be easily resolved.

Video files are generally consists of images and sounds, so most of the applicable techniques for hiding data into images and audio are also usable to video steganography. In the video steganography sender sends the secret message to the recipient using a video sequence as cover media. Secret key 'K' can be used in embedding of the secret message to the cover media to produce *stego-video*. After that the *stego-video* is transferred over public channel to the receiver. At the receiving end, user uses the secret key along with the extracting algorithm to extract the secret message from the *stego video*. The original cover video consists of frames represented by C_k (*m,n*) where 1 < k < N. 'N' is the total number of frame and *m,n* are the row and column indices of the pixels.

The binary secret message denoted by M_k (*m, n*) is embedded into the cover video by modulating it into a signal. M_k (*m, n*) is defined over the similar area as the host C_k (*m, n).*The *stego video* signal is represented by the equation

$$S_k(m, n) = C_k(m, n) + a_k(m, n) M_k(m, n), k = 1, 2, 3 \ldots N$$

Where a_k (m, n) is a scaling factor. For simplicity a_k (m, n) can be considered to be constant over all the pixels and frames. Therefore the equation becomes:

$$S_k(m, n) = C_k(m, n) + a(m, n) M_k(m, n), k = 1, 2, 3 \ldots N.$$

8. 3. Steganalysis Techniques

Steganalysis is used to sense and, or estimate the hidden data from observed data with little or no knowledge about the steganography algorithm. Steganalysis can be normally classified into two types: signature Steganalysis and Statistical Steganalysis. As more and more techniques of hiding data are developed and improved, the methods of detecting the use of steganography also advance. Most Steganography techniques involve changing properties of the cover source and there are several ways of detecting these changes. Now discuss the detection procedures separately depending on the type of the cover media.

Detection technique in Text Steganography

While information can be hidden inside texts in such a way that the presence of the message can only be detected with knowledge of the secret key, for example when using the earlier mentioned method using a publicly available book and a combination of character positions to hide the message, most of the techniques involve alterations to the cover source[15]. These modifications can be detected by looking for patterns in texts or disturbing thereof, odd use of language and unusual amounts of white space.

Detection technique in Image Steganography

Even though stego images can rarely be spotted by the naked eye, they usually leave behind some type of statistical hint that they have been modified. It is those discrepancies which an analysis tool may be able to detect. Since certain techniques and their effects are commonly known, a statistical analysis of an image can be achieved to check for a hidden message(s) in it. A commonly used technique for image scanning involves statistical analysis. Most steganography algorithms that work on images take to that the LSB method. The LSB might not seem to be of much importance, applying a filter which only shows the LSB bits, will still produce a detectable image. Since this is the case, it can be established that the LSB are not random at all, but actually holding information about the whole image. When inserting a hidden data into an image, this particularly property changes with encrypted data, which has very high entropy, the LSB of the cover image will no longer contain information about the original, but as a result of the modifications they will now be more or less random [1, 15]. With a statistical analysis on the LSB bits, the changes between random values and real image values can easily be identified. Using this technique, it is also possible to detect data hidden inside JPEG files with the DCT method, since this also includes LSB modifications, even though these take place in the frequency domain [21].

Detection technique in Audio and Video Steganography

The statistical analysis method can be used against audio files too, since the LSB modification technique can be used on sounds too. Apart from this, there are numerous other things that can be detected. High, inaudible frequencies can be scanned for information and odd distortions or patterns in the sounds might point out the existence of a secret data. Also, changes in pitch echo or background noise may raise doubt. Implementing Steganography using video files as cover sources, the methods of detecting hidden information[22] are also a combination of methods used for images and audio files. However, a different steganography method can be used that is especially effective when used in video films.

9. Evaluation

In this section, Evaluation of different steganography techniques that are discussed already depending on certain criteria, then any kind of approach to obtain data security, it always keep focusing on the degree of security. The progresses are described below.

For Text Steganography

The first letter algorithm used in general is not very secure, as facts of the system that is used, spontaneously gives the secret message. This is a common problem in hiding secrets inside plain text.

For Image Steganography

All the above mentioned algorithms for image steganography have different plus and minus points. It is important to ensure that one uses the most suitable algorithm for an application. All steganography algorithms have to fulfill with a few basic necessities. The most important necessity is that a steganography algorithm has to be imperceptible.

These requirements are as follows: *Invisibility* – The invisibility of a Steganography algorithm is the first and main requirement, since the strong point of steganography lies in its ability to be unnoticed by the human eye. The instant that one can see that an image has been tampered with, the algorithm is compromised. *Payload size* – Steganography requires necessary embedding capacity whereas watermarking wants to embed only a small amount of copyright information. *Robustness* – Statistical Steganalysis is the practice of detecting hidden information through applying statistical tests on image data. Many algorithms leave a signature when embedding information that can be easily detected through statistical analysis. An efficient Steganography algorithm must not leave any signature in the image as be statistically significant. *Robust against image operation* – In the communication of a stego image by trusted systems, the image may suffer changes by an active warden in an attempt to remove hidden data. Image operation, such as cropping or rotating can be done on the image before it touches its endpoint.

These operations like cropping or rotating may abolish the hidden data. It is preferable for steganography algorithms to be robust against unintentional changes to the image. The most powerful steganography algorithms thus possess the ability to embed information in any type of image file. *Unsuspicious files* – This requirement includes all characteristics of a steganography algorithm that may result in images that are not used normally and may cause doubtful.

The levels at which the algorithms fulfill the requirements are separated as high, medium and low. A high level algorithm are completely satisfies the requirements, while a low level point out that the algorithm has a weakness in this requirement. A medium level point out that the requirement depends on outside effects, for example: The GIF type cover images are used in LSB methods because of the potential of hiding a large message size. The perfect steganography algorithm would have a high level in every requirement. Unfortunately there is no only one algorithm that fulfills all of the requirements.

For Audio steganography

Audio steganography is potentially powerful. The audio provide users with a large amount of choice and makes the technology more reachable to everyone. A user can wishes to communicate can rank the significance of factors such as data transmission rate, bandwidth, robustness, and noise audibility and then select the method that best fits their conditions. For example, two persons who just want to send the rare secret message back and forth might use the LSB coding method that is easily realized. On the other hand, a large concern wishing to

protect its intellectual property from "digital pirates" may consider a more sophisticated technique such as phase coding or echo hiding.

For Video Steganography

Video file is a combination of both image and audio. So, video Steganography is nothing but a combination of image and audio steganography [23]. So, the combined evaluations *i.e.*, the evaluations for image and audio steganography can be taken together for the evaluation of video steganography. While doing video steganography, the effect on video has to be kept in mind to achieve a secure communicating media.

10. Recommendation

Steganography is used to ensure a level of privacy while doing data communication with others. Level of security along with the privacy has to be incorporated. Steganography, especially joined with cryptography is a powerful tool which allows people to communicate without possible eavesdroppers even knowing there is a form of communication in the leading place. The methods used in the steganography have innovative a lot over the past centuries, especially with the growth of the computer era. Even if the techniques are still not used very often, the opportunities are endless.

The basic concept of a modulus operation in steganography is providing greater security [24]. In the modulus function improves capacity by overcoming the falling-off-boundary problem and provides good image quality by minimizing the changes in pixel values. The implementing of modulo function and an optimal approach to alter the remainder so as to greatly reduce the image distortion caused by the hiding of the secret data[25]. It can also solve the falling-off-boundary problem by readjusting the remainder of the two pixels, staying secure against the RS detection attack. The simple modulus function in steganography techniques, higher embedding capacity can be obtained for a larger divisor, while also obtaining a higher visual quality of a stego image using a smaller divisor. [26]This scheme additionally yields lower computational costs and memory needs in its embedding and extracting procedures.

The PVD method is data hiding scheme based on pixel difference in cover image. [27], in which cover image area are classified into two types one is smoother region and other one is hard regions. In the smoother region pixel are having small differences with their neighbor pixels. These smoother pixels are not suitable for data embedding. So the pixels with large differences with their neighbor pixels are used for data embedding. This method provides good embedding capacity but stego images are statically detectible one.

Modified version of PVD method is Tri-way pixel value differencing (TPVD) method [28], In the TPVD method three direction pixel selections is made for increasing the payload by embedding secret bits in three different directions on cover image. PVD method only uses one direction for data embedding. Whereas TPVD use horizontal, vertical and diagonal edges of image for embeds secret data. Preprocessing phase of cover image into 2x2 pixel blocks is required in TPVD method.

Another modified version of PVD is Adaptive pixel value differencing (APVD) method. APVD method is only applied for gray scale images. In gray scale digital image having pixel value ranges from 0 to 255. The stego image of exceeding the range of gray scale will be problem [29]. So the APVD method will solve these problems with modulus function and some conditions. So the pixel values of stego image will not exceed the gray scale range. The hidden capacity of the APVD method will be equal to Wu-Tsai's PVD method with satisfactory stego image quality.

The Five pixel pair PVD algorithm is a latest version of PVD series. In this algorithm cover image is divides into 2x3 blocks [30]. So more number of pixel pairs is formed, which provides more space for data hiding. The secret data hidden in the stego image can be extracted correctly without the participation of original cover image.

So the concept of modulus operation based steganography techniques and PVD methods are providing greater security and high embedding capacity on the cover images. Therefore developing new modulo based PVD steganography algorithms against steganalysis seems to have much meaning.

For the expansion in the capacity, splitting cover image by Red, Green and Blue planes then secret bits are encoded into RGB planes by three times of modulus functions. More exactly, to alleviate further color alteration and obtain a higher hidden capacity, the R, G and B section is encoded by Mod u, Mod v and Mod w function respectively. This technique will show the improved data hiding capacity in the cover image. It can be obtained without any compromise in histogram and statistical analysis. It also provides good perceptual quality in stego image and greater security.

11. Conclusion

In this paper, different techniques are discussed for embedding data in text, image, audio and video files as cover media. Undetectability, capacity, and robustness are three main design factor of steganography. All steganography methods are trying to satisfy these three factors. But unfortunately all the existing steganography methods have some advantages, and also disadvantages in comparison with other methods of steganography. So it is not conceivable to give or take that a specified method is the best and best off all. But developing combination of PVD methods with genetic algorithms using modulus function seems to have much meaning.

The stego multimedia produced by mentioned methods for multimedia steganography are more or less vulnerable to attack like media formatting, compression etc. Steganalysis is the technique to detect steganography or defeat steganography. In this respect, the research to device strong Steganography and Steganalysis technique is a continuous process.

Steganography might also become limited under laws in the meantime governments already claimed that criminals use these procedures to communicate. More restrictions on the use of privacy safeguarding technologies are not very unlikely, particularly in this period of time with great anxiety of terrorist and other attacks.

References

[1] B. Dunbar, “Steganographic Techniques and their use in an Open-Systems Environment”, Information Security Reading Room, SANS Institute, **(2002)**.
[2] F. Petioles, J. Anderson and G. Kuhn, “Information hiding-A survey”, Proceeding of IEEE, vol. 87, no. 7, **(2000)** June, pp. 1062-1078.
[3] W. Bender, D. Gruel, N. Morimoto and A. Lu, “Techniques for data hiding”, IBM Systems Journal, vol. 35, no. 3-4, **(2006)** December, pp. 313-336.
[4] H. Farid, “Detecting hidden messages using higher-order statistical models”, Proceeding of IEEE, vol. 15, no. 6, **(2002)** October, pp. 68-72.
[5] J. Fridrich, M. Goljan and R. Du, “Detecting LSB Steganography in Color and Gray-Scale Images”, Magazine of IEEE Multimedia Special Issue on Security, **(2001)** November, pp. 22-28.
[6] J. Fridrich and M. Goljan, “Practical Steganalysis of Digital Images – State of the Art”, Proceeding of SPIE, Photonics West, Electronic Imaging 2002, Security and Watermarking of Multimedia Contents, San Jose, California, vol. 4675, **(2002)** January, pp. 1-13.
[7] W. Zhang, X. Zhang and S. Wang, “A Double Layered “Plus-Minus One” Data Embedding Scheme”, IEEE signal processing letters, vol. 14, no. 11, **(2007)** November.

[8] A. Westfeld and A. Pfitzmann, "Attacks on Steganographic Systems", Proceedings of the third international workshop on Information Hiding, Springer Verlag, **(2005)** September.
[9] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction", IEEE Communication Lett., vol. 10, no. 11, **(2006)** November, pp. 781-783.
[10] H. Zhang and H. Tang, "A Novel image steganography algorithm against statistical analysis", Proceeding of the IEEE, vol. 19, no. 22, **(2007)**, pp. 3884-3888.
[11] J. Kang, Y. You and M. Young Sung, "Steganography using Block-based Adaptive Threshold", Proceeding of the IEEE, vol. 11, **(2007)** November, pp. 234-241.
[12] N. Provos, "Defending against Statistical Steganalysis", 10th USENIX Security Symposium, Washington, **(2005)** August.
[13] J. Fridrich and P. Lison, "Grid coloring in steganography", IEEE Transaction on Information theory, vol. 53, no. 4, **(2007)** April, pp. 1547-1549.
[14] J. Mielikainen, "LSB matching revisited", IEEE Signal Processing lecture notes, vol. 13, no. 5, **(2006)** May, pp. 285-287.
[15] R. Krenn, "Steganography and Steganalysis", Internet Publication, http://www.krenn.nl/univ/cry/steg/article.pdf, **(2004)** March.
[16] K. Cabeen and P. Gent, "Image Compression and Discrete Cosine Transform", Math 45 College of the Redwoods, http://online.redwoods.cc.ca.us/instruct/darnold/LAPROJ/Fall98/PKen/dct.pdf, **(1998)**.
[17] MP3Stego: Hiding Text in MP3 Files, The Information Security Reading Room, SANS Institute **(2001)**, http://www.sans.org/reading_room/whitepapers/stenganography/550.
[18] Digital video steganalysis exploiting collusion sensitivity- Udit Budhiaa and Deepa Kundur Sensors, Command Control, Communications and intelligence (C3I) Technologies for Homeland Security and Homeland Defense, Edward M. Carapezza, ed., Proc. SPIE, Orlando, Florida, http://www.ece.tamu.edu/~deepa/pdf/BudKun04.pdf, vol. 5403, April **(2004)**.
[19] Methods of Audio Steganography, Internet Publication on http://www.snotmonkey.com/work/school/405/methods.html.
[20] Direct-sequence spread spectrum (DSSS), Frequency-hopping spread spectrum (FHSS) Wikipedia, the free encyclopedia, GNU Free Documentation license. http://en.wikipedia.org/wiki/Direct-sequence_spread_spectrum, http://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum.
[21] M. Kharrazi Husrev, T. Sencar and N. Memon, "Performance study of common image steganography and steganalysis techniques", SPIE Proceedings, vol. 5681.
[22] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for data hiding", IBM Systems Journal, vol. 35, **(1996)**.
[23] N. F. Johnson and S. Jajodia, "Steganalysis of Images Created Using Current Steganography Software", Proceedings of the 2nd Information Hiding Workshop, **(1998)** April.
[24] J. C. Joo, H. Y. Lee, C. N. Bui, W. Y. Yoo and H. K. Lee, "Steganalytic measures for the steganography using pixel-value differencing and modulus function", Proceedings of the 9th Pacific Rim Conference on Multimedia, Lecture Notes in Computer Science, vol. 5353, **(2008)**, pp. 476-485.
[25] C. F. Lee and H. L. Chen, "A novel data hiding scheme based on modulus function", Journal of Systems and Software, vol. 83, no. 1, **(2009)** December, pp. 832-843.
[26] J. C. Joo, H. Y. Lee and H. Y. Lee, "Improved Steganographic Method Preserving Pixel-Value Differencing Histogram with Modulus Function", EURASIP Journal on Advances in Signal Processing, vol. **(2010)**.
[27] C. M. Wang, N. I. Wu, C. S. Tsai and M. S. Hwang, "A high quality steganography method with pixel-value differencing and modulus function", Journal of System Software, vol. 81, no. 1, **(2008)**, pp. 150-158.
[28] K. C. Chang, C. P Chang, P. S. Huang and T. M. Tu, "A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing", Journal of Multimedia, vol. 3, no. 2, **(2008)**, pp. 37-44.
[29] J. K. Mandal and D. Das "Steganography Using Adaptive Pixel Value Differencing (APVD) for Gray Images through Exclusion of Underflow/Overflow", Computer Science & Information Series, ISBN: 978-1-921987-03-8, **(2012)**, pp. 93-102.
[30] K. Gulve Avinash and M. S. Joshi, "A Image Steganography Method with Five Pixel Pair Differencing and Modulus Function", International Journal of Computer Applications (0975 – 8887) ,vol. 68, no. 1, **(2013)** April.

Authors

V. Nagaraj received B. E degree in Electronics and Communication Engineering from IFET College of Engineering, Anna University in 2007. In 2009 received M.Tech degree with specialization in Wireless Communication from Pondicherry Engineering College, Pondicherry University, Puducherry and Presently Pursuing Research from same university since 2011. His Research interest includes in Steganography, Cryptography, Image Processing, Intellectual Property Rights, and Pattern Recognition.

V. Vijayalakshmi is currently working as Assistant Professor in Electronics & Communication Engineering Department at Pondicherry Engineering College, Puducherry, India. She completed her B.Tech, M.Tech and PhD in Pondicherry Engineering College which is affiliated to Pondicherry University. She has 20 years of teaching experience. To her credit, she has published more than 25 research papers relating to Network Security and VLSI in several National / International Journals and Conferences. She can be reached by email at vijizai@pec.edu.

G. Zayaraz is currently working as Professor in Computer Science & Engineering Department at Pondicherry Engineering College, Puducherry, India. He received his Bachelors, Masters and Doctorate degrees in Computer Science & Engineering from Pondicherry University. He has published more than Forty five research papers in reputed International Journals and Conferences. His areas of specialization include Software Architecture and Information Security. He is a reviewer for several reputed International Journals and Conferences. He can be reached by email at gzayaraz@pec.edu.