International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 6, Issue 10 (November 2017), PP. 32-37

Steganographic Techniques

*Soumyadip Mal[1],Utsab Banerjee[2]
[1,2]*electrical engineering,netaji subhash engineering college,makaut,india*
*Corresponding Author: *Soumyadip Mal*

ABSTRACT: Steganography is the study and analysis of the art and science of concealing or protecting sensitive communication. The concealed entity might be anything from a file, message, video, image or even audio and it is embedded into other videos ,images or files, etc. In this paper we will be presenting various types of Steganography as well as the factors driving the success of a good stego system.

Keywords: Steganography, Cryptography, DNACryptography, DCT, LSB, DWT, Quantum Cryptography, Quantum Steganography, BPCS, PVD, Artificial Neural Network, QKD, QECC, Fractals.

Date of Submission: 07-09-2017 Date of acceptance: 06-10-2017

I. INTRODUCTION TO STEGANOGRAPHY

In today's technological landscape, security is of paramount importance-it always has been. However, in recent times, due to the explosion of information readily available at fingertips ,it has become all the more necessary to come up with techniques to conceal our messages from any prying third party eyes. Herein ,Steganography along with Cryptography comes into play. In this paper, we are more interested in what Steganography has to offer. The word *steganography* combines the Greek words *steganos* meaning "covered, concealed, or protected," and *graphein* meaning "writing".The first recorded use of the term was in 1499 by Johannes Trithemius in his *Steganographia*[5] , a treatise on cryptography and steganography, disguised as a book on magic. The process of information hiding involves recognising the redundant bits of information in the cover medium and then replacing them with bits from the hidden message, all this without compromising the integrity of the cover image. The goal is to do this in an undetectable way such that there is no way to know even if a concealed communication is going on or not. Whereas cryptographic techniques try to conceal the contents of a message, steganography tries to hide the fact that a communication even exists. Some forms of steganography follow the principle of security through obscurity while other are of the key-dependent types,following the Kerckhoff'sPriciple[1] or the reformulated Shannon's maxim. However,irrespective of the measures taken,stego systems do leave behind certain distortions that affect the statistical properties and the anlalysis of those is termed as the Statistical Steganalysis.

II. TYPES OF STEGANOGRAPHY

At present there are many types of steganography.The steganography can be classified according to its importance and goals.So,various types of steganography are[3][4]:

1) Linguistic Steganography: Linguistic technique is used to hide the message within the cover text in non-obvious way such that the presence of message is imperceptible to an outsider.It is divided into two types:

A) Semagrams: It uses only symbols and signs to hide the information. It is further categorized into two ways:

i) Visual Semagrams: A visual semagrams uses physical objects used every day to convey a message. For example: the positioning of items on a particular website.

ii)Text Semagrams: This type is used to hides a message by modify the appearance of the carrier text, or by changing font size and type, or by adding extra space between words and by using different flourished in letters or handwritten text.

B) Open Code: In this approach the message is embedded in legitimate paraphrases of cover text in the way such that it appears not obvious to an unsuspecting observer. It can be achieved by two ways viz., Jargon which is understood only by a group of peoples and Cipher which uses some concealed ciphers to hide a message openly in the carrier medium. A subset of jargon codes are cue codes, where certain prearranged phrases convey meaning.

2) Technical Steganography: Technical steganography uses special tools, devices or scientific methods to hide a message. In this type one can use invisible ink, microdots, computer based methods or various hiding places to keep message secret

I) Cover: The cover message is the carrier of the message such as image, video, audio, text, or some other digital media. The cover is divided into blocks and message bits which are hidden in each block. The information is encoded by changing various properties of cover image. The cover blocks remain unchanged if message block is zero.

A) Text Steganography: In this approach the cover text is produced by generating random character sequences, changing words within a text, using context-free grammers or by changing the formatting of an existing text to conceal the message. The cover text generated by this approach can qualify for linguistic steganography if text is linguisticallydriven. Although these text- based methods has its own unique characteristics for cover text but suffers from various problems from both a linguistic and security stand point.

B) Image Steganography: This Steganography technique is more popular in recent year than other steganography possibly because of the flood of electronic image information available with the advent of digital cameras and high-speed internet distribution. It can involve hiding information in the naturally occurred noise within the image. Most kinds of information contain some kind of noise. Noise refers to the imperfections inherent in the process of rendering an analog picture as a digital image. In Image steganography we can hide message in pixels of an image. An image steganographic scheme is one kind of steganographic systems, where the secret message is hidden in a digital image with some hiding method. Someone can then use a proper decoding procedure to recover the hidden message from the image. The original image is called a cover image in steganography, and the message-embedded image is called a stego image. Various methods of image steganography are:

i) Data Hiding Method: hiding the data, a username and password are required prior to use the system. Once the user has been login into the system, the user can use the information (data) together with the secret key to hide the data inside the chosen image. This method is used to hiding the
existence of a message by hiding information into various carriers. This prevents the detection of hidden information .

ii) Data Embedding Method: For retrieving the data, a secret key is required to retrieving back the data that have been embedded inside the image. Without the secret key, the data cannot be retrieved from the image. This is to ensure the integrity and confidentiality of the data. The process of embedding the message inside the image, a secret key is needed for retrieving the message back from the image, the secret message that is extracted from the system is transfer into text file and then the text file is compressed into the zip file and zip text file is converting it into the binary codes.

iii) Data Extracting Method: It is used to retrieve an original message from the image; a secret key is needed for the verification. And for extracting method, a secret key is needed to check the key is correct with the decodes from the series of binary code. If key is matched, the process continues by forming the binary code to a zipped text file, the unzip the text file and transfer the secret message from the text file to retrieve the original secret message [15].

III. FEATURES OF IMAGE STEGANOGRAPHY

The different driving forces of a good stego system are[1][2]

1) Transparency: The steganography should not affect the quality of the original image after steganography.

2) Robustness: Steganography could be removed intentionally or unintentionally by simple image processing operations like contrast or enhancement brightest gamma correction, steganography should be robust against variety of such attacks.

3) Data payload or capacity: This property describes how much data should be embedded as a steganography to successfully detect during extraction.

4) Computational Complexity: This property gives an idea about how expensive it is,computationally,to embed and extract a hidden message.

5) Temper Resistance: It should be difficult to alter the message once it has been embedded into the stego image.

6)Security: Security of a steganographic system is defined in terms of undetectability, which is assured when the statistical tests cannot distinguish between the cover and the stego-image.

7) Statistical Attacks: The process of extracting the secret information from the stego object is known as statistical attack. The algo used for steganography must be robust to statistical attacks.

8) Imperceptibility: The video with data and original data source should be perceptually identical.

9) **Accuracy**: The extraction of the hidden data from the medium should be accurate and reliable

C) 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. Audio steganography can be problematic and can be useful for transmitting covert information in an innocuous cover audio signal.

IV. TYPES OF AUDIO STEGANOGRAPHY

1) Echo Hiding: This method embeds data or text into audio signals by adding a small echo to the host signal. The Nature of the echo is a resonance added to the host audio. Then the data is invisible by varying three echo parameters: initial amplitude, decay rate, and offset. If only one echo is produced from the original signal, then only one bit of information could be encoded.

2) Phase Coding: One of the most effective coding methods in terms of the signal-to perceived noise ratio. In this phase components of sound are not as perceptible to the human ear as noise is. It can be done by substituting the phase of an initial audio segment with a reference phase that represents the data. It encodes the message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to-perceived noise ratio subsequent segments is then adjusted store the relative phase between segments. Disadvantage: It is a complex method and has low data transmission rate.

3) Parity Coding: This method breaks a signal down into different regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of selected region does not match the secret bit to be encoded, Disadvantage: This method like LSB coding is not robust in nature. Advantage: The sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive manner.

4) Spread Spectrum: This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire sound file. It is used to encode a category of information by spreading the encoded data across frequency spectrum. This allows the signal reception, even if there is interference on some frequencies. Disadvantage: It can introduce noise into a sound .

5) Tone insertion: In this inaudibility of lower power tones in the presence of significantly higher ones. Tone insertion method can resist to attacks such as low-pass filtering and bit truncation addition to low embedding capacity, embedded data could be maliciously extracted since inserted .

D) Video Steganography: The process of concealing the secret message in an Video file is known as Video steganography. Video Steganography is far more safe and efficient as compared to that of the image steganography as you can embed large amount of data in audio and frames of the video

E) Network Steganography: Network Steganography method uses modification of a single network protocol. The protocol modification may be applied to the PDU (Protocol Data Unit), time relations between exchanged PDUs, or both (hybrid methods). It is highly secure and robust.

F) Physical Steganography: Messages written in secret ink or in wax tablet were used extensively by Greeks.During World War II days,photosensitiveglass,Morse Code were in use.

G)Social Steganography: In communities with social or government taboos or censorship, people use cultural steganography—hiding messages in idiom, pop culture references, and other messages they share publicly and assume are monitored. This relies on social context to make the underlying messages visible only to certain readers.

3.Image Steganography Techniques

Image steganography techniques can be divided into following domains[6]:

A) Spatial Domain Methods: There are many versions of spatial steganography, all directlychange some bits in the image pixel values in hiding data. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. Changes in the value of the LSB are imperceptible for human eyes. Spatial domain techniques are broadly classified into:

1. Least significant bit (LSB)
2. Pixel value differencing (PVD)
3. Edges based data embedding method (EBE)
4. Random pixel embedding method (RPE)
5. Mapping pixel to hidden data method
6. Labeling or connectivity method

7. Pixel intensity based method
8. Texture based method
9. Histogram shifting methods
10. Bit-Plane Complexity Segmentation Steganography(BPCS)

General **advantages** of spatial domain LSB technique are:
1. There is less chance for degradation of the original image.
2. More information can be stored in an image.

Disadvantages of LSB technique are:
1. Less robust, the hidden data can be lost with image manipulation.
2. Hidden data can be easily destroyed by simple attacks.

B) Distortion Techniques: Distortion techniques need knowledge of the original coverimage 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.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.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. However, the need for sending the cover image limits the benefits of this technique. 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. In some cases, if the message is encoded with error correcting information, the change can even be reversed and the original message can be recovered.
C) Masking and Filtering: These techniques hide information by marking an image, in the same way as to paper watermarks. These techniques embed the information in the more significant areas than just hiding it into the noise level. The hidden message is more integral to the cover image. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image.

Advantages of Masking and filtering Techniques:
1. This method is much more robust than LSB replacement with respect to compression since the information is hidden in the visible parts of the image.

Disadvantages of Masking and filtering Techniques:
- Techniques can be applied only to gray scale images and restricted to 24 bits.

D) Transform Domain Technique: This is a more complex way of hiding information in an image. Various algorithms and transformations are used on the image to hide information in it. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested.The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Most of the strong steganographic systems today operate within the transform domain Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions. Transform domain techniques are broadly classified into:
1. Discrete Fourier transformation technique (DFT)-The Discrete Fourier Transform to get frequency component for each pixel value. The Discrete Fourier Transform (DFT) of spatial value f(x, y) for the image of size M x N is defined in equation for frequency domain transformation.
2. Discrete cosine transformation technique (DCT)-The discrete cosine transform (DCT) is a technique for converting a signal into elementary frequency components. It is widely used in image compression.
3. Discrete Wavelet transformation technique (DWT)-A discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled.

4. Lossless or reversible method (DCT)
5. Embedding in coefficient bits

V. SCOPE- WHAT LIES AHEAD

Now that we have more or less gained some idea about different steganographictechniques,which can be thought of as a more classical approach,we would like to venture into the modern advancements in the fields of cryptography and steganography.Assuch,we think that Biological computing (e.g. DNA computing) and quantum computing are two most promising technologies under development,as of now. In this process the principle is basically to encrypt and hide a message in a large number of DNA strands to prevent an adversary from reading and deciphering it. If the primer sequences are kept from an adversary, DNA steganography[5] is safer than common cryptography. However, it is not easy. If the primer sequences are all the same, the security will be weak. If the primer sequences are different every time, the management will be hard. Even worse is that it is possible for an adversary to decipher DNA steganography without the primer sequences and also the main purpose is to solve the security problem of DNA steganography.However,challenging as it may be in the present,we believe it would be an area of interest in the near future.Basically,we could use Vignere or any stream or block ciphers to encrypt the message.Then that is to be converted into ASCII code and then use DNA Steganography on it.

In this context,we would like to propose that,while keys in biological cryptosystem are biological molecules,we could use a more complex yet aesthetic approach to forming keys.We already use microdots in DNA cryptography and DNA Steganography.Wecould,in essence use **fractals** for the same. A **fractal** is an abstract object used to describe and simulate naturally occurring objects. Artificially created fractals commonly exhibit similar patterns at increasingly small scales.[1] It is also known as **expanding symmetry** or **evolving symmetry**. If the replication is exactly the same at every scale, it is called a self-similar pattern. Fractals are different from other geometric figures because of the way in which they scale. Doubling the edge lengths of a polygon multiplies its area by four, which is two (the ratio of the new to the old side length) raised to the power of two (the dimension of the space the polygon resides in). Likewise, if the radius of a sphere is doubled, its volume scales by eight, which is two (the ratio of the new to the old radius) to the power of three (the dimension that the sphere resides in). But if a fractal's one-dimensional lengths are all doubled, the spatial content of the fractal scales by a power that is not necessarily an integer.[3] This power is called the fractal dimension of the fractal, and it usually exceeds the fractal's topological dimension.As such the key developed using fractals,say a Mandelbrot Fractal would be that difficult to break too.Such an **algorithmic composition** would be hugely useful in the field of audio Steganography.

While encrypting the message,before employing Stego techniques on it,we could use ciphers that combine both **transposition and fractionation,**like the bifid cipher, the trifid cipher, the ADFGVX cipher and the VIC cipher-all those while achieving Shannon's **diffusion.**

Now,we would like to go a bit further and delve into field of **Quantum Cryptography and Quantum Steganography[9]**.Julio Gea-Banacloche introduced the idea of hiding secret messages in the form of error syndromes by deliberately applying correctable errors to a quantum state encoded in the three bit repetition quantum error-correcting code **(QECC)**. In his paper, however, he did not address the issue of an innocent-looking message—in the protocol he proposed, the messages would not resemble a plausible quantum channel. Currently used popular public-key encryption and signature schemes (e.g., RSA and ElGamal) can be broken by quantum adversaries. The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e. non-quantum) communication.Natori provides a rudimentary treatment of quantum steganography which is a modification of super-dense coding Martin introduced a notion of quantum steganographic communication in. His protocol is a variation of Bennett and Brassard's quantum-key distribution protocol (QKD), in which he hides a steganographic channel in the QKD protocol. The most well known and developed application of quantum cryptography is quantum key distribution **(QKD)**, which is the process of using quantum communication to establish a shared key between two parties (Alice and Bob, for example) without a third party (Eve) learning anything about that key, even if Eve can eavesdrop on all communication between Alice and Bob. If Eve tries to learn information about the key being established, key establishment will fail causing Alice and Bob to notice. Once the key is established, it is then typically used for encrypted communication using classical techniques. For instance, the exchanged key could be used as for symmetric cryptography.

Steganography can also be relevant within the realms of fuzzy systems and more specifically,Artificial Neural Network. Neurons may have state, generally represented by real numbers, typically between 0 and 1. Neurons and synapses may also have a weight that varies as learning proceeds, which can increase or decrease the

strength of the signal that it sends downstream.Assuch,theStego keys could be modelled on the weight itself.The trick being,the key continually changes,not being any fixed quantity.It would be more adaptive in nature.

Classical systems like Semiotics,PolybiusSquares,Acrostics,Phryctoria,tapcodes,etc can all be used in Stegosystems.Talking of file systems,the names of Ross Anderson, Roger Needham and Adi Shamir must be mentioned.They came up with the idea of steganographic file system. Their paper proposed two main methods of hiding data: in a series of fixed size files originally consisting of random bits on top of which 'vectors' could be superimposed in such a way as to allow levels of security to decrypt all lower levels but not even know of the existence of any higher levels, or an entire partition is filled with random bits and files hidden in it.

VI. CONCLUSION

There can be various innovative ways to approach to Steganography,considering it is an ever expanding field and with time,new dimensions will be appended to it.Thispaper,merely tries to bring light to the various interesting aspects of it.

ACKNOWLEDGEMENT

This Paper is completed by referring various research papers on steganography techniques and their overview and I really appreciate the hard work and dedication done by the authors of the papers.

REFERENCES

[1]. Hide and Seek: An Introduction to Steganography, NIELS PROVOS AND PETER HONEYMAN University of Michigan.

[2]. International Journal of Innovative Research in Computer and Communication Engineering (A High Impact Factor, Monthly, Peer Reviewed Journal) Vol. 4, Issue 1, January 2016 Copyright to IJIRCCE DOI: 10.15680/IJIRCCE.2016. 0401158 721-A Survey Paper on Steganography Techniques Dr. Rajkumar L Biradar , AmbikaUmashetty, Associate Professor, Dept. of Electronics and Telematics, G. Narayanamma Institute of Technology & Science, Hyderabad, India,Dept. of Computer Science & Engineering, Appa Institute of Engineering & Technology, Kalaburagi, India.

[3]. Volume 4, Issue 1, January 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com- An Overview of Different Type of Data Hiding Scheme in Image using SteganographicTechniques,Mukesh Garg A.P. GurudevJangraM.Tech. Scholar H.O.D in CSE Department Jind Institute of Engineering & Technology Jind Institute of Engineering & Technology.

[4]. Information Hiding Techniques for Steganography and Digital Watermarking Stefan Katzenbeisser Fabien A. P. Petitcolas.

[5]. International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 8 - May 2014-A Survey on various types of Steganography and Analysis of Hiding Techniques Navneet Kaur, Sunny Behal.

[6]. Security and Information Hiding based on DNA Steganography, Mrs. Aditi Sharma, IJCSMC, Vol. 5, Issue. 3, March 2016, pg.827 – 832.

[7]. Y. K. Jain and R. R. Ahirwal, "A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys", International Journal of Computer Science and Security (IJCSS), vol. 4, (2010) March 1.

[8]. C.-H. Yang, C.-Y. Weng, S.-J. Wang, Member, IEEE and H.-M. Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems", IEEE Transactions on Information Forensics and Security, vol. 3, no. (2008) September 3, pp. 488-497.

[9]. Vijay kumarsharma, Vishal Shrivastava, "A Steganography algorithm for hiding image in image by improved LSB substitution by minimize technique", Journal of Theoretical and Applied Information Technology, Vol. 36 No.1, 15th February 2012.

[10]. Quantum Cryptography Richard J. Hughes D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan and M. Schauer University of California Physics Division Los Alamos National Laboratory Los Alamos, NM 87545

*Vivien Yi-Chun Chen. "Link Block Protect Taiwan Seaports with Coastal Zones Development." International Refereed Journal of Engineering and Science (IRJES), vol. 06, no. 10, 2017, pp. 24–31.