International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-6, Issue-4)

Research Article | **April 2017**

A Study of Steganography Based Data Hiding Techniques

Vijay Kumar Sharma*, Dr. Devesh Kr Srivastava, Dr. Pratistha Mathur
Department of CSE, Manipal University, Jaipur,
Rajasthan, India

Abstract—

Today the exponential growth in internet users demand secure data communication, for that it is required to send the data in the form of encrypted or hidden form. Many information system security techniques are available. They are classified into three classes as cryptography, steganography and watermarking. This paper presents a review on steganography techniques and their uses and attacks on these. The steganography is commonly known as covert writing and mainly used in hidden communication. A reliable internet communication is free from the attacks on it.

Keywords— Information system security, cryptography, steganography, watermarking.

I. INTRODUCTION

The word steganography came from the combinations of two Greek words, first word is stegos which means covert and second is graphica which means writing. The combination of these two words is commonly known as covert writing or steganography. It is used for secret communication. Embedder selects any cover media (i.e. image, audio file, video file etc.) that results stego file or the file which contain the hidden information inside it. Security is the main concern in today's digital communication when the information is being transferred or in other world we can say that confidential information demands the steganography technique that more resists against the steganographic attack. Here secure communication demands for development of steganography techniques[1] Figure 1 infers the enclosed lizard, somewhat is concealed within this enclosed lizard but inside portion or information is not visible by the outsider.

Figure 1 Stegosaurus: a covered lizard

Information System Security (Cryptography, Watermarking and Steganography) is a discipline that protects the Confidentiality, Integrity and Availability of information and information services. Steganalysis is a type of attack, that always tries to break the security. Steganography's ultimate objectives and the main factors separate it from the related techniques such as cryptography and watermarking. Steganography trends to hide the existence of the message itself, which makes it difficult for an observer to figure out where the message is[2] Sometimes, sending encrypted information may draw the attention of an observer, while invisible information will not. Watermarking is similar, but has a completely different purpose. Watermarking is the process of embedding information on the multimedia. Placing a watermark in media file serves to identify the artist or author of the work i.e. it is used for copyright protection [3] [4].

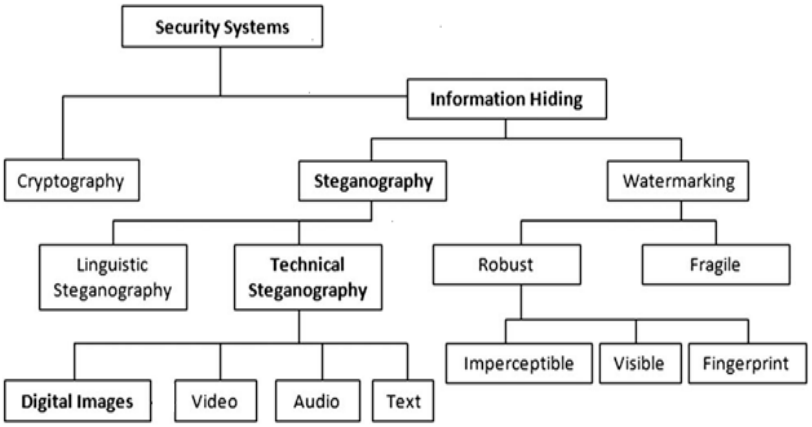

Figure 2. Classification of different security system, for information hiding

A watermark can be either visible or invisible. The broad application area of information hiding, security, encryption and watermarking can be categorized as shown in figure2.

A relation between various data hiding techniques and related parameters is illustrated below in table 1.

Table 1 Comparison of Steganography, Watermarking and Cryptography

Method→ Parameter ↓	**Steganography**	**Watermarking**	**Cryptography**
Carrier	Any digital media	Mostly image/audio files	Usually text based, with some extensions to image files
Secret data	Payload	Watermark	Plain text
Input files	At least two	N/A	One
Detection	Blind	Usually informative	Blind
Result	Stego-file	Watermarked-file	Cipher-text

II. SCOPE OF STEGANOGRAPHY

With the boost in computer power, the internet each and everything has gone in ‘‘digital’’. The Steganography has been created an atmosphere of community vigilance that can spawn in the various appealing applications, so its enduring development is guaranteed. One of the earliest methods to discuss digital steganography is credited to Marvel [5] who proposed a method which resembles embedding into the 4 LSBs (least significant bits). They examined image downgrading and contamination which is known now as image-based steganography. Cyber-crime is believed to benefit from this digital revolution. Hence it is required to find out the all possible attacks on steganography algorithm to hold over steganalysis, and simultaneously, strength in existing steganography techniques against popular attacks.

III. APPLICATIONS OF STEGANOGRAPHY

1. Steganography can be a solution which makes it possible to send news and information without being censored and without the fear of the messages being intercepted and traced back to us.
2. steganography can use to store the information in hidden form, it is depends on the are or security level as in bank.
3. The transportation of sensitive data is another key use of steganography.

IV. HISTORICAL OVERVIEW OF STEGANOGRAPHY

Steganography dates back to ancient Greece when etching messages or images in wooden tablets and casing them with polish, and tattooing on a lacking hair herald head and wait until hair raise back, and then shave the head again to find the message, were general practices.

Early in WWII (world war second) steganographic technology consisted almost exclusively of invisible inks. Resource for imperceptible inks includes milk, vinegar, juice of fruit that darken when heated. A steganographic message generally appears to be something else, like an article or a picture, or some other "cover" message. Drawings have often been used to cover up secure information as it is easy to encode a message by colors in pictures.

(a) Past

Steganography is an ancient art of hiding information. The word steganography is of Greek origin and means “concealed writing” from the Greek words steganos sense "enclosed”, and graphei meaning "script”. Herodotus was the first Greek scientist. His grand work, The name Histories, is the narrative of the conflict between the vast Persian territory and the much smaller city of Greek. Herodotus narrates the story of Histaiaeus, who encouraged Aristagoras of Miletus to revolt against the Persian king. In order to securely convey his plan, Histaiaeus shaved the head of his messenger, tattoo a message on the messenger’s head and waited for the hairs to grow back. The messenger could travel freely as no one can detect the presence of the hidden message on his head. He shaved his head after arriving at the destination and showed the message to the recipient.

Another method used to convey a secret message by ancient Greeks was to write text on wax-covered tablets. In Histories, Herodotus narrated that Demaratus sent a warning about the forthcoming attack to Greece by scrape polish off a pill, write a message on the original wood and again wrap the pill with polish to make it appear clean and vacant. In this way, no one apart from the intended recipient was able to detect the presence of the message.

During World War II, invisible inks came into use for invisible writing. The French Resistance sent some messages written on the backs of couriers using invisible ink. Also hidden messages were written on paper with invisible ink under other messages or on the blank parts of the other messages.

During and after World War II, the Germans developed microdot technology. Microdots are photographs of approximately less than the size of a period produced by a typewriter, having the clarity of standard-sized type-written pages, which allows the transmission of large amounts of data, including drawings and photographs. Microdots needed to be embedded in the paper and sheltered with an glue, such as involvement. This was reflective and thus detectable by viewing against glancing light.

(b) Present

With every discovery of the ancient message hiding techniques, a new steganographic application was being devised. Old methods are given new twists. Computer technology has sparked a revolution in this field of steganography. Modern steganography came into existence in 1985 with the beginning of personal computer being applied to classical steganographic problems. At that time the developments were slow but since then advances are taking place at a rapid rate. The majority of today's steganographic systems uses multimedia stuff , as cover media because persons often convey digital pictures over email and other Internet communication. In modern technique, depending on the temperament of cover object, on the basis of multimedia steganography may be divided into following types:

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography
- Protocol Steganography

In the current time so many steganographic techniques have developed which works with the above multimedia objects. Day by day the security is going in advance; so now and again come on certain cases in which a mixture of Cryptography and Steganography are used to achieve more data isolation in secrecy. a variety of S/w kits are also available in this regard [6],[7].

(c) Future

In today's world, we often listen a popular term "Hacking". Hacking is nothing but an illegal access of data which can be composed at the time of data broadcast. With respect to steganography this problem is often taken as Steganalysis. Steganalysis is a method in which a steganlysis brock the cover media to get the concealed information. So, no matter what be the approach will be developed in upcoming time, level of security related with that has to be kept back in mind. It is hoped that Dual Steganography, Steganography with Cryptography may be the future answer for this above trouble.

V. STEGANOGRAPHY TECHNIQUES

Many steganography and watermarking techniques are developing today for providing confidential and intellectual property copyright against unauthorized access and use in digital materials such as music, film, book and software through the use of digital watermarks.

There are many ways to hide information in digital images. The most of them are the following:

1. least significant bit insertion
2. masking and filtering
3. algorithms and transformations

1. Least significant bit insertion

Many stego tools make use of least significant bit (LSB). For example, 11111111 is an 8-bit binary number. The rightmost bit is called the LSB because changing it has the least effect on the value of the number. The idea is that the LSB of every byte can be replaced with little change to the overall file. The binary data of the secret message is broken up and then inserted into the LSB of each pixel in the image file.

Hiding the data is implemented using the Red, Green, Blue (RGB) model; a stego tool, and making copy of an image palette, say, an 8-bit image. The copy is rearranged so that colors near each other in the RGB model are near each other in the palette. The LSB of each pixels 8-bit binary number is replaced with one bit from the hidden message. A new RGB color in the copied palette is found. A new 8-bit binary number of the new RGB color in the original palette is found. The pixel is changed to the 8-bit binary number of the new RGB color.

Recovering the data is done using the stego tool which finds the 8-bit binary number of each pixels RGB color. The LSB of each pixel's 8-bit binary number is one bit of the hidden data file. Each LSB is then written to an output file.
A simplified example with an 8-bit image
1 pixel:
(00 01 10 11)
white red green blue
Insert 0011:
(00 00 11 11)
white white blue blue
As can be seen from the example, with an 8-bit image, the cover image must be carefully selected since LSB manipulation is not as forgiving because of the color limitations. To hide information in the LSBs of each byte of a 24-bit image, it is possible to store 3 bits in each pixel.

2. Masking and filtering

Masking techniques hide information in such a way that the hidden message is more integral to the cover image than simply hiding data in the "noise" level. Masking adds redundancy to the hidden information. This makes the masking technique more suitable than LSB with lossy JPEG images. It may also help protect against some image processing such as cropping and rotating.

3. Algorithms and transformations

Another steganography technique is to hide data in mathematical functions used in compression algorithms. The idea is to hide the data bits in the least significant coefficients. A key advantage of JPEG images over other formats is its lossy compression methods [8]. It enables high quality images to be stored in relatively small files. The compressed data is stored as integers but the calculations for the quantization process require floating point calculations which are rounded. Errors introduced by rounding define the lossy characteristic of the JPEG compression method. JPEG images use the discrete cosine transform (DCT) technique to achieve image compression. The DCT is "a technique for expressing a waveform as a weighted sum of cosines" [9]. In a JPEG file, the image is made up of DCT coefficient. When a file is steganographically embedded into a JPEG image, the relation of these coefficients is altered. Instead of actual bits in the image being changed as in LSB steganography, it is the relation of the coefficients to one another that is altered.

In addition to DCT, images can be processed with fast Fourier transform (FFT). FFT is "an algorithm for computing the Fourier transform of a set of discrete data values" [10]. The FFT expresses a finite set of data points in terms of its component frequencies. It also solves the identical inverse problem of reconstructing a signal from the frequency data.

The wavelet transform is a transformation to basic functions that are localized in frequency. The wavelet compression methods are better at representing transients, such as an image of stars on a night sky. This means that "elements of some data signal that are transient can be represented by a smaller amount of information than would be the case if some other transform, such as the more widespread discrete cosine transform, had been used" [11]. Wavelet compressions are good for transient signal characteristics but not for smooth, periodic signals. Many transform domain methods are not dependent on the image format so that the hidden message is retained after conversion between lossless and lossly formats.

The steps for hiding the data are to take the DCT or wavelet transform of the cover image and find the coefficients below a specific threshold. Replace these bits with bits to be hidden (for example, use LSB insertion) and then take the inverse transform and store it as a regular image.

To extract the hidden data take the transform of the modified image and find the coefficients below a specific threshold. Extract bits of data from these coefficients and combine the bits into an actual message. Other techniques of steganography include spread spectrum steganography, statistical steganography, distortion, and cover generation steganography.

VI. STEGANALYSIS NOMENCLATURE

The art of detecting Steganography is referred to as Steganalysis. To put it simply Steganalysis involves detecting the use of Steganography inside of a file. It does not attempt to decrypt the hidden information. There are many methods that can be used to detect Steganography such as:

1. Viewing the file and comparing it to another copy of the file if available.

For example, by comparing the suspected file with any other copy of the file, if available, it is found that one is larger in memory size than the other, it is most probable to suspect file has hidden information inside of it.

2. Listening to the file.

This is similar to the above method for detecting Steganography in picture files. To detect hidden information inside a MP3 audio file one needs to find an audio file to compare it to that uses the same compression (MP3).

The desired outcome of steganalysis depends on what the steganalyst wants to achieve. For example, one steganalyst may want to know whether Alice and Bob are communicating, another steganalyst may want to know how Alice and Bob are communicating so that he can impersonate Alice and send Bob false messages. In fact, the role of the steganalyst can be defined in three categories - passive, active, and malicious.

Passive steganalysts intercept a work as it is passed through the communications channel, and then tests it to identify whether it contains a secret message or not. If no secret message is detected, the work will be allowed to continue through the communications channel. However, if a secret message is detected, the steganalyst will block the transmission and Bob will not receive the secret message.

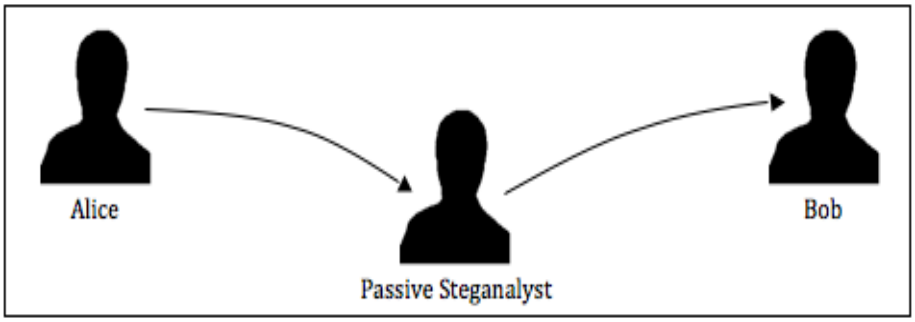

Fig.ure 3 The Passive Steganalyst

However, in actuality that Bob did not get the information or message as bob was waiting from a time, this lead him to suspect that a attacker or steganalyst has been broken down the communication, therefore they will repeatedly modify the algorithm and resend the message again.

An active steganalyst differs from a passive steganalyst because if the existence of a secret message is found, the active warden would modify the work such that the integrity of the message is broken. This modification may be achieved by compressing the image in the hope that some important pixel values alter the secret message data. Most steganographic techniques assume a passive steganalyst, and therefore the stegogramme is not designed to survive modifications such as these. With this method, Bob will still receive the work, but when he extracts the message he will find that it does not make sense.

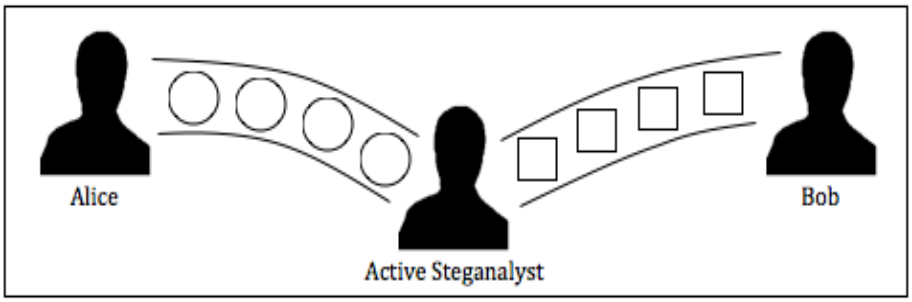

Figure 4 The Active Steganalyst

A mailicious steganalyst will analyse the work sent between Alice and Bob to determine if it contains a hidden message. If it does, they will then try and work out how the message was embedded such that they can then impersonate Alice and send their own messages to Bob.

However, this method is about much more than just detecting whether or not a secret message is embedded within a work. For this reason, it is very rare for a steganalyst to carry these traits.

VII. TYPES OF ATTACKS

Attacks and analysis on hidden information may take several forms: detecting, extracting, and disabling, destroying or modifying hidden information. An attack approach is dependent on what information is available to the steganalyst. The possible attacks on a stego media can be one of the following:

1. Known-carrier attack: The carrier, ie: the original cover, and steganography media are both available for analysis.
2. Known-message attack: The hidden message is known.
3. selected-steganography attack: this type of attack is possible when both the steganography media and the tool or algorithm are known..
4. Chosen-message attack: A known message and steganography tool (or algorithm) are used to create steganography media for future analysis and comparison..
5. Known-steganography attack: The carrier and steganography medium, as well as the steganography tool or algorithm, are known.

One can hide information almost anywhere on the Internet. For example, there are several places on a webpage to hide information:

1. Text

Text information can be hidden by making it the same color as the background. Small shift in word and line spacing may be difficult to visually detect. One way to find any invisible text on a page is to do a Control-A on the page. This will select all the text on the page.

Non-text elements

Any graphic or media clip can contain hidden links or messages.

2. Links

Links can be created without it being underlined, or change of color when the mouse cursor moves over them. The easiest way to find links on a page is to view the source and search for HREF=. Optionally the searcher can use the key which is known as tab key to emphasize all the clickable matter on a page.

3. Comments

The contents of a comment is viewable only in the source code of a page.

4. Structure

Most browsers ignore information provided in the source code that is not interpretable. For example, unusual options in markup tags can possibly hide clues.

5. Frames

View the source code of each frame on a web page. Sometimes a site disables the right-click or use of the menu function to find the source code. In such cases, try using the command view-source:http://(site url) in the address line of the browser.

VIII. STEGANALYSIS TECHNIQUES

Hiding information within electronic medium cause alterations of the medium properties that can result in some form of degradation or unusual characteristics. The visual detection of stego media demands good visibility so that steganalysis can not identify the visual difference in between original file and stgo file.

IX. CONCLUSION

Today the digital communication demands to adopts secure communication that need to study and developments in secure data communication techniques. steganography is the better choice of someone who wants to secret communication because feature is not visible in it. Better steganography techniques is free or have the grate resistant against the power full steganography attacks. Here are demands to develop good steganography technique because of the advancement of the attackers.

REFERENCES

[1] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt "Digital image steganography: survey and analysis of current methods**"** Signal processing, Volume 90, Issue 3, March 2010, pp. 727-752.

[2] Harvinder Singh, Anuj kumar and Prateek Bansal, "Analysis and Implementation of Algorithm to Hide Secret Message" International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 2, February - 2013, pp. 327-333.

[3] Abbas Cheddad , Joan Condell, Kevin Curran, Paul Mc Kevitt "Digital image steganography: Survey and analysis of current methods", Elsevier Signal Processing volume 90, January 2010, Pages. 727-752.

[4] Farooq Husain, "A Survey of Digital Watermarking Techniques for Multimedia Data", MIT International Journal of Electronics and Communication Engineering Vol. 2, No. 1, Jan 2012 pp. 37-43.

[5] Marvel, L.M., Boncelet, C.G. and Retter, C.T., "Spread spectrum image steganography", IEEE Trans. Image Process., vol. 8, no. 8, pp. 1075–1083,1999.

[6] Moerland T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/tmoerl/privtech.pdf.

[7] Ahsan K. & Kundur D., "Practical Data hiding in TCP/IP", Proceedings of the Workshop on Multimedia Security at ACM Multimedia, 2002.

[8] Bharat Sinha, " Comparison of PNG & JPEG Format for LSB Steganography", International Journal of Science and Research, Volume 4 Issue 4**,** 2015, pp.198-201.

[9] Yash Kumar Singh, Sudhanshu Sharma, "Image steganography on gray and color image using DCT enhancement and RSA with LSB method" Inventive Computation Technologies (ICICT), International Conference, 2016.

[10] Ashish Soni, Jitendra Jain, Rakesh Roshan, "Image Steganography using Discrete Fractional Fourier Transform", International Conference on Intelligent Systems and Signal Processing, 2013, pp. 97-100.

[11] Mohammed Abo-Zahhad, Sabah M. Ahmed & Ahmed Zakaria "ECG Signal Compression Technique Based on Discrete Wavelet Transform and QRS-Complex Estimation" Signal Processing – An International Journal (SPIJ), Volume (4) : Issue (2), 2010, pp.138-160.

