A Review of Digital Image Steganography

Pradeep Kumar Saraswat[1,*] and Dr. R. K. Gupta[2]
[1,*]Research Scholar, IT, Singhania University, Rajasthan, India
[2]Professor, Faculty of Engg. & Tech., HR Group of Institutions, Ghaziabad, U.P., India

Steganography is defined as the science or even possibly art of hiding likely critical information within other, seemingly benign information. The point of steganography is to prevent the detection of information leakage, not encrypt data. However, there is nothing stopping a user, malicious or otherwise from first encrypting a secret message and then embedding it inside harmless information. The process only deals with embedding one bit stream (the hidden information) inside of another bit stream. Either bit stream can be of any form. However, steganography is frequently used in conjunction with cryptography. In one method, the plain-text would first be encrypted and then feed to the steganography program. This ensures that if the hidden message is retrieved, the plain-text will still be encrypted. The reverse procedure also works. Two technologies that are closely related to steganography are watermarking and fingerprinting. These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements than steganography. In watermarking all of the instances of an object are "marked" in the same way. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection. With fingerprinting on the other hand, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers. This enables the intellectual property owner to identify customers who break their licensing agreement by supplying the property to third parties.

Keywords: Steganography, Cryptography, Intellectual Property.

1. INTRODUCTION

Before the invention of digital means, traditional methods were being used for sending or receiving messages. Before phones, before mail, before horses, messages were sent on foot[1]. For the messages where privacy was of prime concern, the ways of implementing security were following:

(i) Choosing the messenger capable of delivering the message securely.
(ii) Writing the message using such notations that actual meaning of the message was concealed.
(iii) Hiding the message such that even its presence can't be predicted.

With the acceptance of digital techniques in society for sending or receiving messages in

large scale, the need of techniques to make that transmission secure also arise. One such technology is Steganography.

Steganography is the technique of hiding the message in a chosen carrier such that no one except the intended recipient is aware of its existence. Block diagram of steganography is shown in Fig. 1. Digital images, audio files, video files, text files, executable files and even voice can be used as carrier. How much data can be hidden in the carrier depends on the size of the carrier and the steganography method used to hide the message.

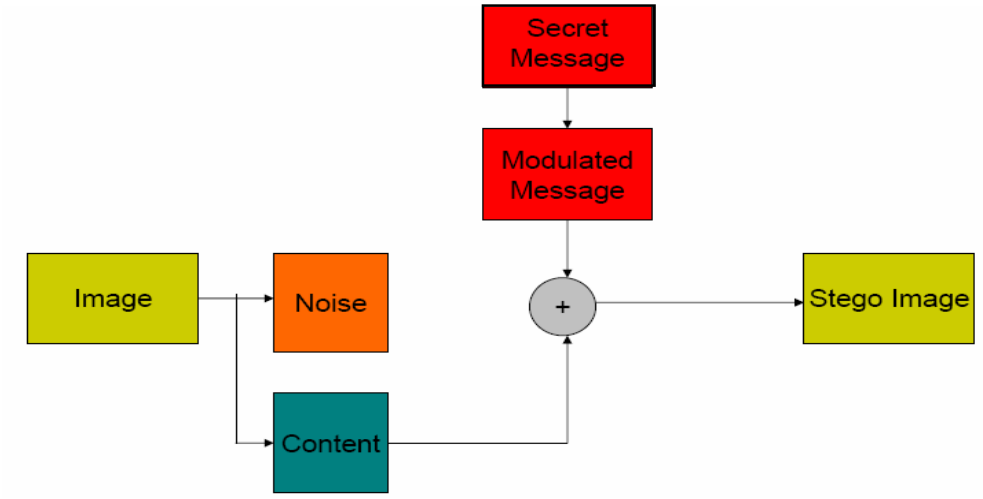

Fig. 1: Block Diagram of Steganography

Steganography is different from cryptography in the way that cryptography conceals the meaning of the message while steganoraphy conceals the existence of the message. A message in encrypted form may arise some suspicion but the risk is eliminated if the very existence of the message is hidden as done by the steganography[2]. Various research works are being done to incorporate larger size of data in same sized carrier with minimum degradation in originality of the carrier. Works are in progress to use more and more types of files as carrier.

In this paper we will introduce modern steganography with some historical background and detailed working of LSB method which is used for steganography.

2. LITERATURE SURVEY

2.1. Background of Steganography

Since man first started communicating over written messages, the need for secrecy was in high demand. In the past, messages could easily be intercepted and since there were no secrecy devices, the third party was able to read the message. This all changed during the time of the Greeks, around 500 B.C., when Demaratus first used the technique of

Steganography[3]. Steganography is the use of hiding a message so it looks like a message does not exist at all.

Throughout history, a multitude of methods and variations have been used to hide information. Bruce Norman recounts numerous tales of cryptography and steganography during times of war in Secret Warfare.

2.2. Modern Steganography

At sender site, the message to be hidden (*emb*) is hide in some cover data. The cover data may be some digital image, text file, video file, binary file, etc.. A key is associated with the hiding process. The message thus obtained is called is called stego which is transmitted to the receiver[4,5]. The same process is repeated at receiver site but in reverse order to obtain the original message as shown in Fig. 2.

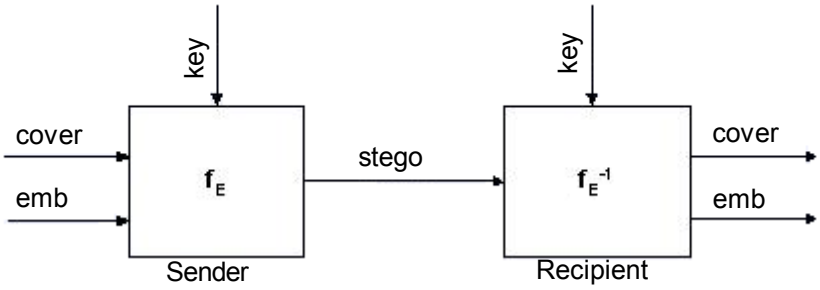

Fig. 2: Block Diagram of Steganographic Function "Embedding" and "Extracting"

where, f_E : steganographic function "embedding".
f_E^{-1} : steganographic function "extracting".
cover : cover data in which emb will be hidden.
emb : message to be hidden.
key : parameter of f_E.
stego : cover data with the hidden message[6].

There are numerous methods used to hide information inside of image. The most common methods are:

(i) LSB (Least Significant Byte).
(ii) Finger Printing & Watermarking.
(iii) Masking and Filtering.

(i) LSB Method

When files are created there are usually some bytes in the file that aren't really needed, or at least are not that important. These areas of the file can be replaced with the information that is to be hidden, without significantly altering the file or damaging it. This allows a

person to hide information in the file and make sure that no human could detect the change in the file. The LSB method works best in Picture files that have a high resolution and use many different colors, and with Image files that have many different formats and that are of resolution. The LSB method usually does not increase the file size, but depending on the size of the information that is to be hidden inside the file, the file can become noticeably distorted[7].

Usually 24-bit or 8-bit files are used to store digital images. The former one provides more space for information hiding; however, it can be quite large. The colored representations of the pixels are derived from three primary colors: red, green and blue as shown in Fig. 3. 24-bit images use 3 bytes for each pixel, where each primary color is represented by 1 byte. Using 24-bit images each pixel can represent 16,777,216 color values. We can use the lower two bits of these color channels to hide data. Then the maximum color change in a pixel could be of 64-color values, but this causes so little change that is undetectable for the human vision system. This simple method is known as Least Significant Bit insertion[6,7]. Using this method it is possible to embed a significant amount of information with no visible degradation of the cover image.

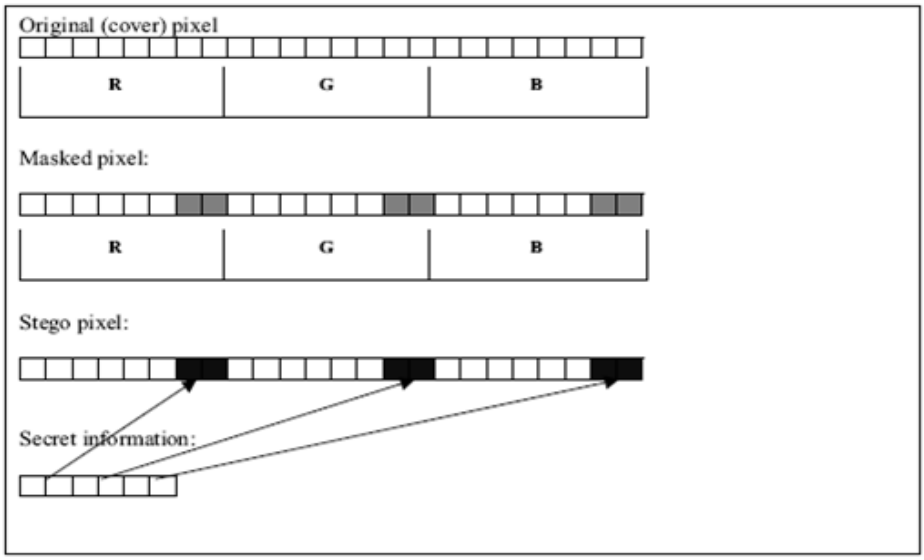

Fig. 3: Colored Representations of the Pixels

Here example of encoding of replacing LSB of the any data stream:

10010101 00001101 11001001
1010110 00001111 11001010
10011111 00010000 11001011

Now suppose we want to “hide” the following 9 bits of data (the hidden data is usually compressed prior to being hidden):

101101101.

If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following (where bits in **bold** have been changed):

10010101 00001100 11001001
10010111 00001110 11001011
10010101 00001100 11001001
10010111 00001110 11001011
10011111 00010000 11001011

(ii) Finger Printing & Watermarking Method

These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements than steganography. These requirements of a good steganographic algorithm will be discussed below. In watermarking all of the instances of an object are “marked” in the same way. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection. With fingerprinting on the other hand, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers. This enables the intellectual property owner to identify customers who break their licensing agreement by supplying the property to third parties[6,8].

In watermarking and fingerprinting the fact that information is hidden inside the files may be public knowledge but sometimes it may even be visible, while in steganography the imperceptibility of the information is crucial. A successful attack on a steganographic system consists of an adversary observing that there is information hidden inside a file, while a successful attack on a watermarking or fingerprinting system would not be to detect the mark, but to remove it.

(iii) Masking and Filtering Method

It is a steganography technique which can be used on 24 bit per pixel images. The technique can be used on both color and gray-scale images. Masking and filtering is similar to placing watermarks on a printed image. In the article "Exploring Steganography: Seeing the Unseen" by Neil F. Johnson and Sushil Jajodia from George Mason University masking is more robust than LSB insertion with respect to compression, cropping, and some image processing [9,10].

Fig. 4 illustrates how masks and filters can be embedded into images without destroying the original quality of a photographic image. The entire photograph has been watermarked. This image cannot be illegally copied, edited or used in any application in which it was not originally intended. Changing the luminosity and opacity of the watermark layers will provide varying results. The image on the left has an opacity of zero percent. the opacity is gradually increased until the watermark layer becomes visible. Using masks and filters maintains the original quality, but prohibits anyone from using the image for any purposes other than those that it was created.

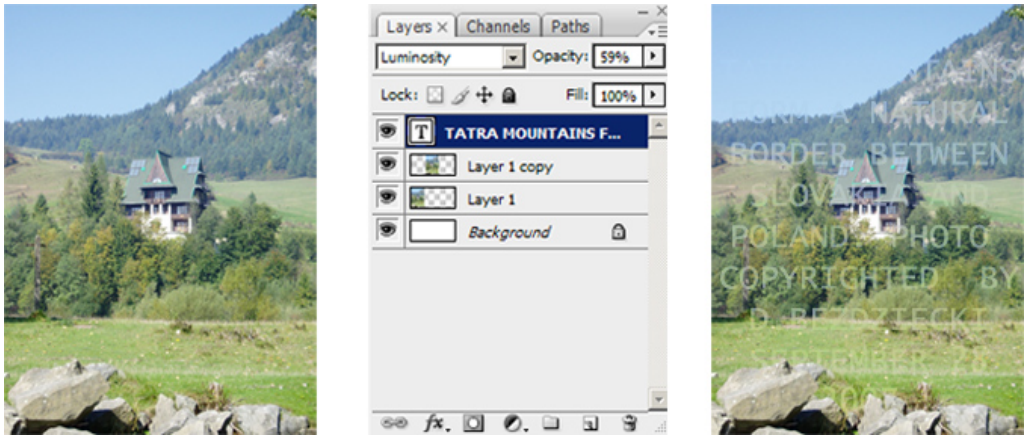

Fig. 4: Masking and Filtering Method

3. TYPES OF STEGANOGRAPHY

Steganography can be divided into categories by the kind of technique used to conceal the existence of the message[11,12]. They can be classified as shown in Fig. 5.

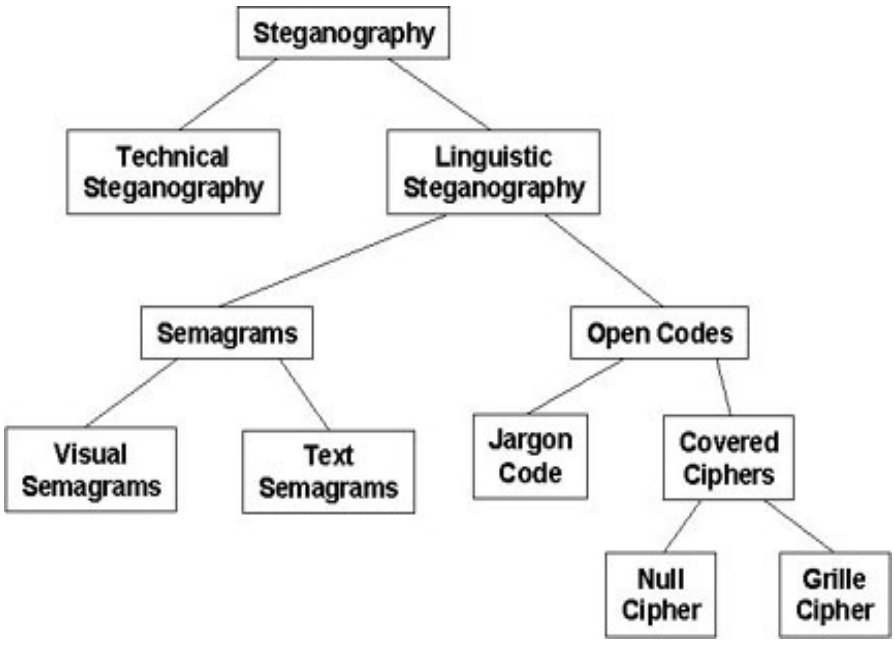

Fig. 5: Types of Steganography

These categories can be specified as:

- Technical steganography uses scientific methods to hide a message, such as the use of invisible ink or microdots and other size-reduction methods.
- Linguistic steganography hides the message in the carrier in some nonobvious ways and is further categorized as semagrams or open codes.
- Semagrams hide information by the use of symbols or signs. A visual semagram uses innocent-looking or everyday physical objects to convey a message, such as doodles or the positioning of items on a desk or Website. A text semagram hides a message by modifying the appearance of the carrier text, such as subtle changes in font size or type, adding extra spaces, or different flourishes in letters or hand written text.
- Open codes hide a message in a legitimate carrier message in ways that are not obvious to an unsuspecting observer. The carrier message is sometimes called the overt communication whereas the hidden message is the covert communication. This category is subdivided into jargon codes and covered ciphers.
- Jargon code, as the name suggests, uses language that is understood by a group of people but is meaningless to others. Jargon codes include warchalking (symbols used to indicate the presence and type of wireless network signal, underground terminology, or an innocent conversation that conveys special meaning because of facts known only to the speakers. A subset of jargon codes is cue codes, where certain prearranged phrases convey meaning.
- Covered or concealment ciphers[13] hide a message openly in the carrier medium so that it can be recovered by anyone who knows the secret for how it was concealed. A grille cipher employs a template that is used to cover the carrier message. The words that appear in the openings of the template are the hidden message. A null cipher hides the message according to some prearranged set of rules, such as "read every fifth word" or "look at the third character in every word."

4. USES OF STEGANOGRAPHY

Steganography has a wide array of uses. it can be used for digital watermarking, e-commerce, and the transport of sensitive data. Digital watermarking involves embedding hidden watermarks, or identification tokens, into an image or file to show ownership. This is useful for copyrighting digital files that can be duplicated exactly with today's technologies[3].

In current e-commerce transactions, most users are protected by a username and password, with no real method of verifying that the user is the actual card holder. Biometric finger print scanning, combined with unique session IDs embedded into the fingerprint images via steganography, allow for a very secure option to open e-commerce transaction verification[3].

Unfortunately, steganography can also be used for illegitimate reasons. For instance, if someone was trying to steal data, they could conceal it in another file or files and send it out in an innocent looking email or file transfer. As was pointed out in the concern for terroristic purposes, it can be used as a means of covert communication. Some of the tools used for Steganography are:

(i) EzStego
(ii) F5
(iii) Hide and Seek
(iv) Hide4PGP
(v) MP3Stego
(vi) OutGuess
(vii) StegHide
(viii) Stegnos
(ix) S-Tools

5. CONCLUSION

Steganography has its place in security. It is not intended to replace cryptography but supplement it. Hiding a message with steganography methods reduces the chance of a message being detected. However, if that message is also encrypted, if discovered, it must also be cracked (yet another layer of protection).

There are an infinite number of steganography applications. This paper explores a tiny fraction of the art of steganography. It goes well beyond simply embedding text in an image. Steganography does not only pertain to digital images but also to other media files such as voice, other text and binaries; other media such as communication channels, the list can go on and on[8].

REFERENCES

[1] Clair, B.; "*Steganography: How to Send a Secret Message*", 8 October 2001, http://strange horizons.com/2001/20011008/steganography.shtml .
[2] Yau, S.S.; "*Steganography*", CSE 494/598, Fall 2004, http://enpub.fulton.asu.edu/iacdev/courses/CSE465/Fall2005/files/ln_2/IA%20Steganography.pdf .
[3] Polencheck, Nathan J.; "*Steganography and the Secure Transportation of Sensitive Data*", Proceedings of the 3rd Winona Computer Science Undergraduate Research Symposium, Winona, MN, April 23-24, 2003, http://cs.winona.edu/CSConference/2003conference.pdf .
[4] Bhattacharyya, S. and Sanyal, G.; "*A Data Hiding Model with High Security Features Combining Finite State Machines and PMM method*", International Journal of Electrical and Computer Engineering, Vol. 5(2), pp. 78-85, 2010,http://www.waset.org/journals/ijece/v5/v5-2-12.pdf .
[5] Al-Khateeb, H.; "*Introduction to Modern Steganography*", 11 Jan, 2010, http://blog.creativeitp.com/posts-and-articles/cryptography/introduction-to-modern-steganography/ .
[6] Khan, M.M.; "*Steganography*", http://www.neiu.edu/~ncaftori/355/Steganography.ppt .
[7] Johnson, Neil F.; "*Information Hiding: Steganography & Digital watermarking*",1995, http://www.

jjtc.com/Steganography/ .
[8] Calpe, A.; "*Steganography in Images*", http://www.cs.ucf.edu/courses/cot4810/fall04/presentations/Steganography_in_Images.ppt#279 .
[9] Johnson, Neil F. and Jajodia, S.; "*Exploring Steganography: Seeing the Unseen*", IEEE, pp.26-34, Feb1998, http://www.jjtc.com/pub/r2026.pdf .
[10] Bezdziecki D.J.; "*Steganography-Techniques",* http://bit599.netai.net/stego_techniques.htm .
[11] Kessler, Gary C.; "*An Overview of Steganography for the Computer Forensics Examiner*", Forensic Science Communications, Vol. 6(3), July 2004, http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/july2004/research/2004_03_research01.htm/ .
[12] Jones, S.; "*Sarah Jones' Weblog*", October 17, 01:09 PM, 2009, http://www.henryfarrell.net/cybersecurity/jones/2009/10/types_of_steganography.html .
[13] Jones, S.; "*Steganography*", October 25, 01:40 PM, 2009, http://www.henryfarrell.net/cybersecurity/jones/2009/10/the_medias_take_on_steganograp.html .