International Journal of Computer Applications Technology and Research
Volume 3– Issue 7, 479 - 483, 2014, ISSN: 2319–8656

A Survey of Image Steganography

Sandeep Kaur
Guru Nanak de Engg. Collage
Ludhiana, India

Arounjot Kaur
Guru Nanak de Engg. Collage
Ludhiana, India

Kulwinder Singh
Guru Nanak de Engg. Collage
Ludhiana, India

Abstract: This paper presents a general overview of the steganography. Steganography is the art of hiding the very presence of communication by embedding secret messages into innocuous looking cover documents, such as digital images. Detection of steganography, estimation of message length, and its extraction belong to the field of steganalysis. Steganalysis has recently received a great deal of attention both from law enforcement and the media. In this paper review the what data types are supported, what methods and information security professionals indetecting the use of steganography, after detection has occurred, can the embedded message be reliably extracted, can the embedded data be separated from the carrier revealing the original file, and finally, what are some methods to defeat the use of steganography even if it cannot be reliably detected.
Keywords: steganography, Image steganography, cryptography, stego image and stego key.

1. INTRODUCTION

Steganography comes from the Greek words Steganós (Covered) and Graptos (Writing) [1]. In the past, people used hidden tattoos or invisible ink to convey steganographic content. Today, computer and network technologies provide easy-to-use communication channels for steganography[2].

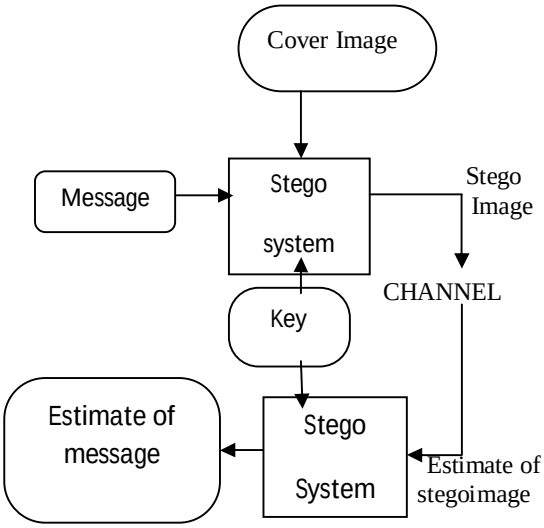

Figure 1. Overview of steganographic system

Steganography is a technique of information security that hides secret information within a normal carrier media, such as digital image, audio, video, etc. An unauthorized attempt to detect and extract the hidden secret information from stego is known as steganalysis [3]. The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message. Modern steganography goal is to keep its mere presence undetectable. classical steganographic system's security relies on the encoding system's secrecy. An example of this type of system is a Roman general who shaved a slave's head and tattooed a message on it. After the hair grew back, the slave was sent to deliver the now-hidden message.Although such a system might work for a time, once it is known, it is simple enough to shave the heads of all the people passing by to check for hidden messages—ultimately, such a steganographic system fails. Modern steganography attempts to be detectable only if secret information is known—namely, a secret keys [4]. A block diagram of a generic blind image steganographic system is depicted in Fig. 1. A message is embedded in a digital image by the stegosystem encoder, which uses a key or password. The resulting stegoimage is transmitted over a channel to the receiver, where it is processed by the stegosystem decoder using the same key[5].

2. CATEGORIES OF IMAGE STEGANOGRAPHY

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy.

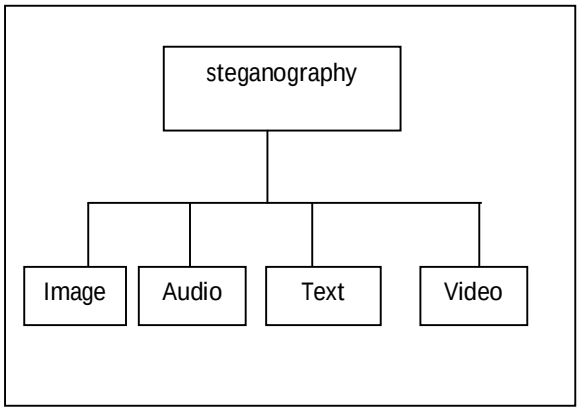

Figure 2. Categories of steganography

Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display [6].

2.1 Image steganography

To hide information, straight message insertion may encode every bit of information in the image or selectively embed the message in ―noisy‖ areas that draw less attention—those areas where there is a great deal of natural color variation [7]. The message may also be scattered randomly throughout the image. A number of ways exist to hide information in digital media. Common approaches include

2.1.1 Least significant bit insertion
2.1.2 Masking and filtering
2.1.3 Redundant Pattern Encodings
2.1.4 Encrypt and Scatter
2.1.5 Algorithms and transformations

2.2 Audio steganography

Audio Steganography is a method of hiding the message in the audio file of any formats.EAS provides an easy way of implementation of mechanisms .When compared with audio steganography. Apart from the encoding and decoding in

Audio steganography[10]. EAS contain extra layers of encryption and decryption. The four layers in EAS are:

2.2.1 Encoding
2.2.2 Decoding
2.2.3 Encryption
2.2.4 Decryption

2.3 Text steganography

Since everyone can read, encoding text in neutral sentences is doubtfully effective. But taking the first letter of each word of the previous sentence, you will see that it is possible and not very difficult. Hiding information in plain text can be done in many different ways[8][9] Many techniques involve the modification of the layout of a text, rules like using every n-th character or the altering of the amount of white space after lines or between words.

2.4 Video steganogrphy

Video files are generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too .The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds.Therefore, any small but otherwise noticeable distortions might go by unobserved by humans because of the continuous flow of information.

3. STEGANOGRAPHIC TECHNIQUES

There are quite a lot of approaches in classifying steganographic techniques. These approaches can be classified in accordance with the type of covers used with secret communications. Another possibility is done via sorting such approaches depending on the type of cover modification already applied in the process of embedding. Steganographic techniques that modify image files for hiding information include the following[11]:

- Spatial domain;
- Transform domain;
- Spread spectrum;
- Statistical methods; and
- Distortion techniques

3.1 Steganography in the spatial domain

In spatial domain methods a Steganographer modifies the secret data and the cover medium in the spatial domain, which is the encoding at the level of the LSBs. This method has the largest impact compared to the simplicity [12]. Spatial steganography mainly includes LSB (Least Significant Bit) steganography Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image . The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message.

Pixel: (10101111 11101001 10101000)

(10100111 01011000 11101001)

(11011000 10000111 01011001)

Secret message: 01000001

Result: (10101110 11101001 10101000)

(10100110 01011000 11101000)

(11011000 10000111 01011001)

3.2 Steganography in the frequency domain

New algorithms keep emerging prompted by the performance of their ancestors (Spatial domain methods), by the rapid development of information technology and by the need for an enhanced security system. The discovery of the LSB embedding mechanism is actually a big achievement. DCT is used extensively in Video and image (i.e., JPEG) lossy compression. Most of the techniques here use a JPEG image as a vehicle to embed their data.

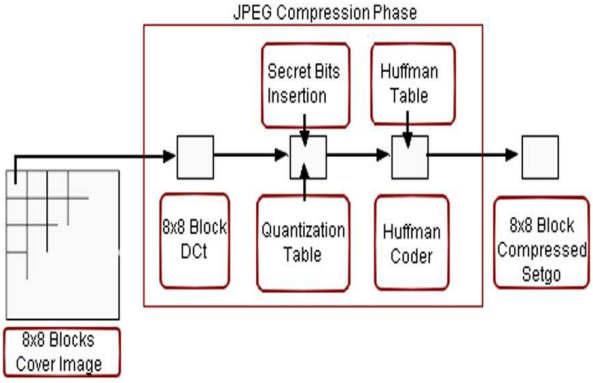

Figure 3. Data Flow Diagram showing a general process of embedding in the frequency domain.

JPEG compression uses DCT to transform successive sub-image blocks (8x8 pixels) into64 DCT coefficients.

3.3 Transform domain technique

We have seen that LSB modification techniques are easy ways to embed information but they are highly vulnerable to even small cover modifications. It has been noted early in the development of steganographic systems that embedding information in the frequency domain of a signal can be much more robust than embedding rules operating in the time domain. Transform domain methods hide messages in significant areas of the cover image which makes them more robust to attacks, such as compression, cropping, and some image processing, than the LSB approach. However, while they are more robust to various kinds of signal processing, they remain imperceptible to the human sensory system. Many transform domain variations exist. One method is to use the discrete cosine transformation (DCT) [13][14]. This method is used, but similar transforms are for example the Discrete Fourier Transform (DFT). These mathematical transforms convert the pixels in such a way as to give the effect of "spreading" the location of the pixel values over part of the image. The DCT transforms a signal from an image representation into a frequency representation, by grouping the pixels into 8 × 8 pixel blocks and transforming the pixel blocks into 64 DCT. DCT is used in steganography as- Image is broken into 8×8 blocks of pixels. Working from left to right, top to bottom, the DCT is applied to each block[15].

3.4 Spread spectrum

Spread spectrum communication describes the process of spreading the bandwidth of a narrowband signal across a wide band of frequencies. This can be accomplished by modulating the narrowband waveform with a wideband waveform, such as white noise. After spreading, the energy of the narrowband signal in any one frequency band is low and therefore difficult to detect[16].

3.5 Statistical methods

Statistical Methods also known as model-based techniques, these techniques tend to modulate or modify the statistical properties of an image in addition to preserving them in the embedding process. This modification is typically small, and it is thereby able to take advantage of the human weakness in detecting luminance variation [17]. Statistical steganographic techniques exploit the existence of a "1-bit", where nearly a bit of data is embedded in a digital carrier. This process is done by simply modifying the cover image to make a sort of significant change in the statistical characteristics if a "1" is transmitted, otherwise it is left unchanged. To send multiple bits, an image is broken into sub-images, each corresponding to a single bit of the message [18].

3.6 Distortion techniques

Distortion techniques store information by signal distortion and measure the deviation from the original cover in the decoding step[19]. In contrast to substitution systems, distortion techniques require the knowledge of the original cover in the decoding process. Alice applies a sequence of modifications to a cover in order to get a stego-object; she chooses this sequence of modifications in such a way that it corresponds to a specific secret message she wants to transmit. Bob measures the differences to the original cover in order to reconstruct the sequence of modifications applied by Alice, which corresponds to the secret message[20].

4. DIFFERENCE BETWEEN CRYPTOGRAPHY AND STEGANOGRAPHY

Basically, the purpose of cryptography and steganography is to provide secret communication. However, steganography is not the same as cryptography. Cryptography scrambles a message by using certain cryptographic algorithms for converting the secret data into unintelligible form. On the other hand, Steganography hides the message so that it cannot be seen. Cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. Cryptography can also provide authentication for verifying the identity of someone or something. In contrast, steganography does not alter the structure of the secret message, but hides it inside a cover-image so it cannot be seen. Staganography and cryptography differences are briefly summarized following in Table I.

TABLE I. DIFFERENCE BETWEEN CRYPTOGRAPHY AND STEGANOGRAPHY

CRYPTOGRAPHY	STEGANOGRAPHY
Known message passing	Unknown message passing
Common technology	Little known technology
Technology still being developed for certain Formats	Most of algorithm known by all
Cryptography alter the structure of the secret message	Steganography does not alter the structure of the secret message

5. METHODS OF STEGANALYSIS

Steganalysis is "the process of detecting steganography by looking at variances between bit patterns and unusually large file sizes". It is the art of discovering and rendering useless covert messages [21]. The goal of steganalysis is to identify suspected information streams, determine whether or not they have hidden messages encoded into them, and, if possible, recover the hidden information, unlike cryptanalysis, where it is evident that intercepted encrypted data contains a message. The process of steganalysis is depicted in Fig. 4.

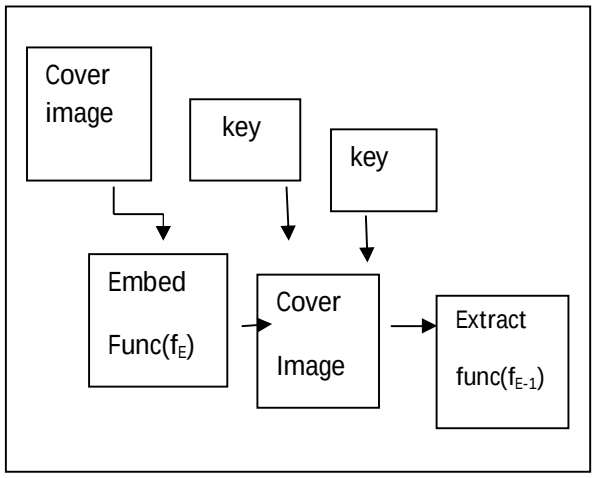

Figure 4. Process of steganalysis

It is the art of discovering and rendering useless covert messages [21]. The goal of steganalysis is to identify suspected information streams, determine whether or not they have hidden messages encoded into them, and, if possible, recover the hidden information, unlike cryptanalysis, where it is evident that intercepted encrypted data contains a message. The process of steganalysis is depicted in Fig. 4.

6. VISUAL DETECTION

Most steganographic programs embed message bits either sequentially or in some pseudo-random fashion. In most programs, the message bits are chosen non-adaptively independently of the image content. If the image contains connected areas of uniform color or areas with the color saturated at either 0 or 255, we can look for suspicious artifacts using simple visual inspection after preprocessing the stego-image. Even though the artifacts cannot be readily seen,we can plot one bit-plane (for example, the LSB plane) and inspect just the bit-plane itself [22].This attack is especially applicable to palette images for LSB embedding in indices to the palette.

7. STATISTICAL DETECTION

Statistical attack that can be applied to any steganographic technique in which a fixed set of Pairs of Values (PoVs) are flipped into each other to embed message bits[23]. These methods use first or higher order statistics of the image to reveal tiny alterations in the statistical behavior caused by steganographic embedding and hence can successfully detect even small amounts of embedding with very high accuracy.

8. CONCLUSION

The meaning of Steganography is hiding information and the related technologies.The purpose of this paper is to present a survey of various approaches for image steaganography based on their various types and techniques.

9. ACKNOWLEDGMENTS

I thanks to a great many people who helped and supported me during writing of this paper. My deepest thanks to Arunjot kaur Brar Assistant Professor of department of Information Technology Guru Nanak dev Engineering college ludhiana Punjab. Who guided and supported me in every phase of writing this paper. I am grateful to my parents who are inspirational in their understanding patience and constant encouragement.

10. REFERENCES

[1] Dr. Ekta Walia , Payal Jain , Navdeep 'An Analysis of LSB & DCT based Steganography' Vol. 10 Issue 1 (Ver 1.0), April 2010.

[2] Niels Provos and Peter Honeyman, University of Michigan, 'Hide and

[3] Seek: An Introduction to Steganography' published by the ieee computer society, 2003 IEEE.

[4] Hardik Patel*, Preeti Dave, 'Steganography Technique Based on DCT Coefficients' International Journal of Engineering Research and Applications Vol. 2, Issue 1,Jan-Feb 2012, pp.713-717

[5] Niels Provos and Peter Honeyman, University of Michigan, 'Hide and Seek: An Introduction to Steganography' published by the ieee computer society, 2003 IEEE.

[6] Lisa M. Marvel, Member, IEEE, Charles G. Boncelet, Jr., Member,

IEEE, and Charles T. Retter, Member, IEEE, ' Spread Spectrum Image Steganography',IEEE TRANSACTIONS ON IMAGE PROCESSING.

[7] T. Morkel , J.H.P. Eloff, M.S. Olivier, 'an overview of image steganography', Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa

[8] Alain C. Brainos II. — A Study Of Steganography And The Art Of Hiding Information‖, IEEE Trans. Inf. Forens. Secur. 2006

[9] Robert Krenn. — Steganography and steganalysis,‖ Computer, vol. 31, no. 2, Feb. 1998,pp. 26-34.

[10] Udit Budhiaa, Deepa Kundura. —Digital video steganalysis exploiting collusion sensitivity‖, IEEE Tans. On Image Processing,vol.15, No.8, August 2006, pp. 2441-2453.

[11] R. sridevi —Efficient Method Of Audio Steganography By Modified Lsb Algorithm And Strong Encryption Key With Enhanced Security‖ Journal of Theoretical and Applied Information Technology 2005 – 2009 JATIT.

[12] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Osamah M. Al-Qershi , 'Image Steganography Techniques: An Overview', International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3) : 2012

[13] Anu, rekha, Praveen, 'Digital Image Steganography 'International Journal of Computer Science & Informatics, Volume-I, Issue-II, 2011

[14] Cox, I., et al., "A Secure, Robust Watermark for Multimedia, " in information Hiding: First International Workshop, Proceeding ,vol. 1174 of Lecture notes in Computer Science, Springer , 1996,pp.185-206.

[15] Koch, E., and J.Zhao, "Towards Robust and Hiddden Image Copyright Labeling", in IEEE Workshop on Nonlinear Signal and Image Processing, Jun.1995.

[16] Gurmeet Kaur and Aarti Kochhar, "A Steganography Implementation based on LSB & DCT", International Journal for Science and Emerging

[17] Technologies with Latest Trends".

[18] Lisa M. Marvel, Member, IEEE, Charles G. Boncelet, Jr., Member, IEEE, and Charles T. Retter, Member, IEEE, ' Spread Spectrum Image Steganography',IEEE TRANSACTIONS ON IMAGE PROCESSING.

[19] M. Kharazi, H.T. Sencar, and N. Memon. (2004, Apr.). "Image steganography: Concepts and practice." Aug. 2011

[20] P. Kruus, C. Scace, M. Heyman, and M. Mundy. (2003), "A survey of steganography techniques for image files." Advanced Security Research Journal. Oct., 2011

[21] C.P.Sumathi, T.Santanam and G.Umamaheswari, 'A Study of Various Steganographic Techniques Used for Information Hiding' International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013.

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

[23] Jessica Fridrich*, Miroslav Goljan "Practical Steganalysis of Digital Images – State of the Art" supported by Air Force Research Laboratory, Air Force Material Command, USAF, under a research grant number F30602-00-1-0521.

[24] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, "Writing on wet paper", IEEE Trans.on Signal Processing, Special Issue on Media Security, vol. 53, Oct. 2005, pp. 3923-3935.

[25] A. Joseph Raphael, "Cryptography and Stegano-graphy – A Survey" Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630.