ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 10, January 2016

REVIEW OF CLASSICAL STEGANOGRAPHY TECHNIQUES

Suchitra Sinha[#], Prof. Prateek Gupta[*]
[#]Departmanet of Computer Sc & Engg,
SRIST, RGPV University, Jabalpur,MP,India
suchitrasinha884@gmail.com
[*]Head of Department, Computer Sc. & Engineering Department,
SRIST, RGPV University, Jabalpur, MP, India.
pguptace@yahoo.com

Abstract— Steganography is the art and science of hidden communication. There are two important aspects of the steganography system: capacity and security. Steganography and cryptography share the objective of protecting secret information. Cryptography encrypts the secret information prior to communication, whereas steganography hides the existence of the secret information. Steganography leaves behind detectable traces in the stego object and modifies the statistical properties. Detecting the presence of distorted statistical properties is called statistical steganalysis. This paper gives the review of various techniques used in steganography and tries to identify the requirements of an efficient steganography algorithm.

Keywords— Steganography, Cryptography, Steganalysis. Image Processing, Data Hiding.

I. INTRODUCTION

Steganography is an art of sending a secrete message under the camouflage of a carrier content. The goal of steganography is to mask the very presence of communication, making the true message not discernible to the observer. It aims to embed secret data into a digital cover media, such as digital audio, image, video, etc., without being suspicious.

The term steganography literally means ―covered writing‖.
The objective of steganography is to communicate information in an undetectable manner such that when the messages are observed by unintended recipient there will not be enough evidence that the messages conceal additional secret data [4].

The protection of sensitive information against unauthorized access or fraudulent changes has been of prime concern throughout the centuries. Modern communication techniques, using computers connected through networks, make all data even more vulnerable for these threats. Also, new issues have come up that were not relevant before, e.g. how to add a (digital) signature to an electronic document in such a way that the signer cannot deny later on that the document was signed by him.

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 10, January 2016

Cryptology addresses the above issues. It is at the foundation of all information security. The techniques employed to this end have become increasingly mathematical of nature. Figure-1.1 shows the major branches of cryptology.

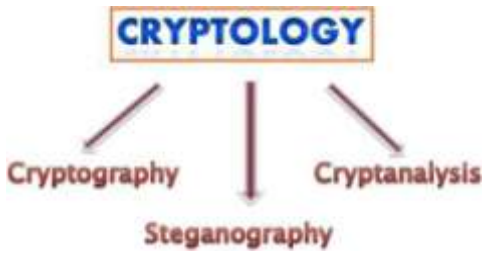

Figure 1.1: Branches of Cryptology

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription.

Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses .

With Secret key cryptography, a single key is used for both encryption and decryption. The sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key (or ruleset) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.

Public-key cryptography has been said to be the most significant new development in cryptography in the last 300-400 years. Modern public-key cryptography was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Their paper described a two-key crypto system in which two parties could engage in a secure communication over a non-secure
communications channel without having to share a secret key. Public-key cryptography depends upon the existence of so-called one-way functions, or mathematical functions that are easy to compute whereas their inverse function is relatively difficult to compute [5].

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 10, January 2016

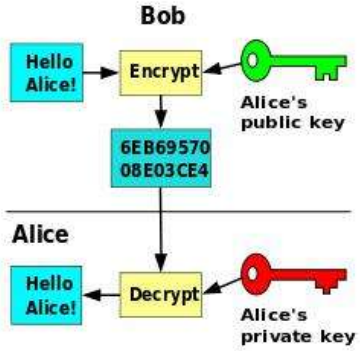

Figure 1.2: A view of Cryptography

One more cryptography technique is Hash functions. Hash functions, also called message digests and one-way encryption, are algorithms that, in some sense, use no key. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file.

II. CLASSIFICATION OF STEGANOGRAPH

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. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object‟s use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding. There are four main categories of file formats that can be used for steganography as shown in Figure 1.3 [1].

Following section gives a brief description of these categories of steganography.

IMAGE STEGANOGRAPHY: JPEG compression is a commonly used method for reducing the size of an image, without reducing the aesthetic qualities enough to become noticeable by the naked eye. Broadly speaking, it extracts all the information from an image that the human eye is not perceptible to and would therefore not miss should it not be there [2]. Since, images are quite popular cover or carrier objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithms exist. Here, in this paper, we will discuss about the image domain steganography methods. In Image Domain methods secret messages are embedded using the intensity of the pixels

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 10, January 2016

values directly. The image domain methods are relatively simple compared to the other methods and are sometimes characterized as the ―simple systems‖. However, they are generally more sensitive to small changes on the image such as filtering, resizing and squeezing.

AUDIO STEGANOGRAPHY: Audio Steganography is the technology of embedding information in an audio channel. It is used for digital copyright protection. Watermarking is the technique which hides one piece of information [message] in another piece of information [carrier]. It is widely used for applications such as audio clip etc [2].

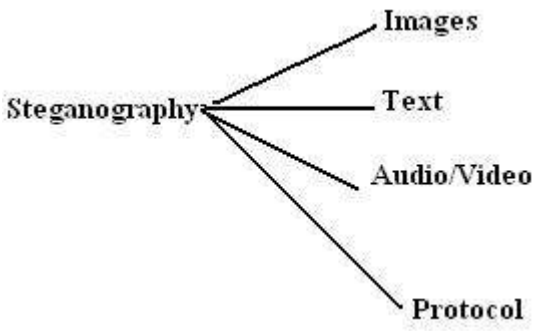

Figure 1.3: Categories of Steganography

VIDEO STEGANOGRAPHY: 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 & sounds. Therefore, any small out otherwise noticeable distortions might go by unobserved by humans because of the continuous flow of information [2].

PROTOCOL STEGANOGRAPHY: The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission. In the layers of the OSI network model there exist covert channels where steganography can be used. An example of where information can be hidden is in the header of a TCP/IP packet in some fields that are either optional or are never used.

TEXT STEGANOGRAPHY: One major category, perhaps the most difficult kind of Steganography is text Steganography or linguistic Steganography because due to the lack of redundant information in a text compared to an image or audio. The text Steganography is a method of using written natural language
to conceal a secret message. The advantage to prefer text Steganography over other media is its smaller memory occupation and simpler communication [2].

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 10, January 2016

III. DIFFERENT STEGANOGRAPHY TECHNIQUES

The steganography techniques broadly classified three categories: Spatial domain steganography, Transform domain steganography and Adaptive steganography [3].
Following section gives a brief description of these techniques of steganography.

SPATIAL DOMAIN METHOD

In spatial domain scheme, the secret messages are embedded directly. Here, the most common and simplest steganography method is the least significant bits (LSB) insertion method. In the LSB technique, the least significant bits of the pixels are replaced by the message bits which are permuted before embedding. Most steganography software hide information by replacing only the least-significant bits (LSB) of an image with bits from the file that is to be hidden. This technique is generally called LSB encoding. One of the most common techniques used in steganography [1].

The following example shows how the letter A can be hidden in the first eight bytes of three pixels in a 24-bit image [1].

Pixels:

(10101111 11101001 10101000)
(10100111 01011000 11101001)
(11011000 10000111 01011001) Secret message:
01000001

Result:

(10101110 11101001 10101000)
(10100110 01011000 11101000)
(11011000 10000111 01011001)

The three bold bits are the only three bits that were actually altered. Since the 8-bit letter A only requires eight bytes to hide it in, the ninth byte of the three pixels can be used to begin hiding the next character of the hidden message. A slight variation of this technique allows for embedding the message in two or more of the least significant bits per byte. This increases the hidden information capacity of the cover-object, but the cover-object is degraded more, and therefore it is more detectable [1].

Sharp.T in 2001 proposed simple Least Significant Bit (LSB) steganography, long-known to steganographers, in which the hidden message is converted to a stream of bits which replace the LSBs of pixel values in the cover image. (Sharp, 2001)

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 10, January 2016

NEIL F. Johnson and Sushil Jajodia, 2000. Discuss three popular methods for message concealment in digital images. These methods are LSB insertion, masking and filtering and algorithmic transformations (Johnson, Duric and Jajodia, 2000).

(Chang et al., 2002) (Thien et al., 2003) had insinuate, LSB substitution is basically a method to directly switching the LSBs of pixel in the cover image with secret bits to get the stego-image. This method replaces the LSB of each pixel with the encrypted message bit stream to hide message in a host image. Authorized receivers can extract the message by decoding the host image with the help of a pre-shared key. Capacity of algorithm is 1 bit per pixel. (Chang, Lin and Hu, 2002; Chang, Hsiao and Chan, 2003; Thien and Lin, 2003)

(Wang et al., 2000 and 2001) examined on to improve the quality of stego-image and employed a genetic algorithm to generate a substitution table. The substitution table consists the value of the secret data to be embedded into each host pixel is transformed to another value in advance which is closer to the original value of the host pixel. But substitution table may not be the optimal solution. (Wang, Lin and Lin, 2001)

To find out the optimal solution (Chang et al., 2003 and 2006) proposed dynamic programming (Chang, Hsiao and Chan, 2003; Chang, Chan and Fan, 2006) strategy. But the optimal substitution process may require huge computational cost because of using genetic algorithm and dynamic programming strategy. Rather to use genetic algorithm, an Optimal Pixel Adjustment Process (OPAP) is used to enhance the visual quality of the stego-image by LSB substitution [3].
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 coefficients each. A modification of a single DCT coefficient will affect all 64 image pixels in that block [6].

The next step is the quantization phase of the compression. Here another biological property of the human eye is exploited: The human eye is fairly good at spotting small differences in brightness over a relatively large area, but not so good as to distinguish between different strengths in high frequency brightness. This means that the strength of higher frequencies can be diminished, without changing the appearance of the image. JPEG does this by dividing all the values in a block by a quantization coefficient. The results are rounded to integer values and the coefficients are encoded using Huffman coding to further reduce the size [7].

ADAPTIVE STEGANOGRAPHY

Adaptive steganography is a special case of the two former methods. It is also known as ―Statistics-aware embedding, masking or Model-Based. This method takes statistical global features of the image before attempting to interact with its LSB/DCT coefficients. The statistics will dictate where to make the changes (Kharrazi, *et al.*,; Tzschoppe, Baum, Huber and Kaup, 2003).

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 10, January 2016

Wayner (2002) dedicated a complete chapter in a book to what he called ―*life in noise*‖, pointing to the usefulness of data embedding in noise. It is proven to be robust with respect to compression, cropping and image processing.

The model-based method (MB1), described in, generates a stego-image based on a given distribution model, using a generalized Cauchy distribution, that results in the minimum distortion (Sallee, 2003).

Chin-Chen *et al*. (2004), propose an adaptive technique applied to the LSB substitution method. Their idea is to exploit the correlation between neighboring pixels to estimate the degree of smoothness. They discuss the choices of having 2, 3 and 4 sided matches. The payload (embedding capacity) was high.

Embedding is performed by replacing selected suitable pixel data of noisy blocks in an image with another noisy block obtained by converting data to be embedded.

Kong *et al.*, (2009) proposed a content-based image embedding based on segmenting

homogenous gray scale Areas using a watershed method coupled with Fuzzy C-Means

TRANSFORM DOMAIN

To understand the steganography algorithms that can be used when embedding data in the transform domain, one must first explain the type of file format connected with this domain. The JPEG file format is the most popular image file format on the Internet, because of the small size of the images.

To compress an image into JPEG format, the RGB colour representation is first converted to a YUV representation. In this representation the Y component corresponds to the luminance (or brightness) and the U and V components stand for chrominance (or colour) [5].

According to research the human eye is more sensitive to changes in the brightness (luminance) of a pixel than to changes in its colour. This fact is exploited by the JPEG compression by downsampling the colour data to reduce the size of the file. The colour components (U and V) are halved in horizontal and vertical directions, thus decreasing the file size by a factor of 2.

The next step is the actual transformation of the image. For JPEG, the Discrete Cosine Transform (DCT) is used, but
(FCM). Entropy was then calculated for each region. Entropy values dictated the embedding strength where four LSBs of each of the cover's RGB primaries were used if it exceeded a specific threshold otherwise only two LSBs for each were used.

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 10, January 2016

Chao *et al*. presented a 3D steganography scheme. The embedding scheme hides secret messages in the vertices of 3D polygon models.

Bogomjakov *et al*., hide a message in the indexed representation of a mesh by permuting the order in which faces and vertices are stored. Although, such methods claim higher embedding capacity, however time complexity to generate the mesh and then rendering can be an issue. Moreover 3D graphics are not that portable compared to digital images [3].

IV. ADVANTAGES & LIMITATIONS OF STEGANOGRAPHY

Following section enlist the advantages and disadvantages of steganography [2].

ADVANTAGES

- The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.
- This method featured security, capacity, and robustness, the three needed aspects of steganography that makes it useful in hidden exchange of information through text documents and establishing secret communication.
- Important files carrying confidential information can be in the server in and encrypted form No intruder can get any useful information from the original file during transmit.
- With the use of Steganography Corporation government and law enforcement agencies can communicate secretly [2].

LIMITATIONS

- Huge number of data, huge files size, so someone can suspect about it.
- If these techniques are gone in the wrong hands like hackers, terrorist, criminals then this can be very much dangerous.

V. CONCLUSIONS

Information hiding techniques received very much less attention from the research community and from industry than cryptography. Steganography has its place in security. It is not intended to replace cryptography but supplement it. Here in this paper we have tried to present a brief description of various techniques of Steganography so that one can able to select a particular algorithm based on his application (i.e. requirement).

REFERENCES

[1] Shikha Mohan and Satnam Singh, Image Steganography: Classification, Application and Algorithms, International Journal Of Core Engineering & Management (IJCEM), Volume 1, Issue 10, January 2015.

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 10, January 2016

[2] Sagar S.Pawar, Prof. Vinit Kakde, Review On Steganography For Hiding Data, International Journal of Computer Science and Mobile Computing, ISSN 2320–088X, IJCSMC, Vol. 3, Issue. 4, pg.225 – 229, April 2014.

[3] Tanmoy Halder, Sunil Karforma**,** and Rupali Mandal**,** E-govornence Data Security using Steganography, Concepts, Algorithms and Analysis, International Journal of Applied Sciences & Engineering (IJASE) 2(1) : April 2014, 41-54.

[4] Jessica Fridrich and Miroslav Goljan, Practical Steganalysis of Digital Images – State of the Art, Department of Electrical Engineering, Binghamton, NY 13902-6000, 2003.

[5] Satenik Bagyan, Thomas Mair, Yuri Suchorski, Marcus J. B. Hauser and Ronny Straube, Spatial desynchronization of glycolytic waves as revealed by Karhunen–Loeve analysis, September, 2008.

[6] Arijit Sur, Devadeep Shyam, Piyush Goel, and Jayanta Mukherjee, An image steganographic algorithm based on spatial desynchronization, Multimedia Tools Appl, Springer Science & Business Media New York, Nov 2012.

[7] Sur A., Goel P., and Mukhopadhyay J., Spatial Desynchronization: A Possible Way to Resist Calibration Attack, Dept. of Comput. Sci. & Eng., Indian Inst. of Technology, Guwahati, India, 2009.