JCSE International Journal of Computer Science and Engineering Open Access

Review Paper Volume-2, Issue-5 E-ISSN: 2347-2693

A Review of Approaches for Steganography

Komal Arora[1*] and Geetanjali Gandhi[2]

[1*,2] B.S.Anangpuria Institute of Technology and Management

www.ijcseonline.org

Received: 11/04/2014 Revised: 26 /04/2014 Accepted: 17/05/ 2014 Published: 31 /05/2014

Abstract- Steganography is the art and science of hiding communication; a steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. Many different carrier file formats are used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This paper intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganographic algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.

Keywords: Steganography, image-audio-video-text Steganography.

1. INTRODUCTION

Since the rise of the internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography.

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". In image steganography, the information is hidden exclusively in images.

Figure 1: (a) Original Image
(b) Steganographed Image with Hidden Data

In the Steganography system scenario, before the hiding process, the sender must select the appropriate message carrier (i.e. image, video, audio, text) and select the effective secret messages as well as the robust password (which suppose to be known by the receiver). The effective and appropriate Steganography algorithm must be selected that able to encode the message in more secure technique. Then the sender may send the Stego file by email or chatting, or by other modern techniques. The Stego file is the carried message with the secret information. After receiving the message by the receiver, he can decode it using the extracting algorithm and the same password is used by the sender[11][12]. The Steganography system scenario is shown in the Figure 1.

Corresponding Author: *Komal Arora*

© 2014, IJCSE All Rights Reserved

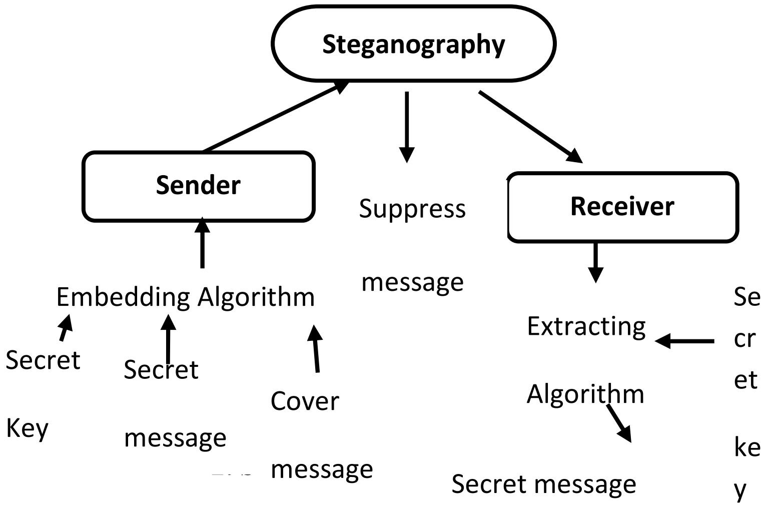


Figure 2:

The basic structure of steganography is made up of three components:

i. The carrier image,
ii. The Message
iii. The Key

The carrier refers to the object that will 'carry' the hidden message like a painting, or a digital image. A key can be anything from a password, a pattern, a back-light and used to decode/decipher the hidden message.

Accordingly, the structure of this paper as follows: Section 2 reviews the Steganographic Terms. Section 3 provides a state-of-art review and analysis of different existing methods of steganography drawn from literature survey. Section 4 presents Steganography Applications. Section 5 reviews different types of Steganography. Section 6 presents the problems with steganography. Finally, conclusion is presented in section 7.

2. STEGANOGRAPHIC TERMS

- Cover File: A File in which hidden information is stored.
- Stego Medium: Medium through which the information is hidden.
- Message: Data to be hidden or extracted.
- Steganalysis: Identify the existence of message.

3. RELATED WORK

In the related work, the most common method involve the usage of LSB developed by Chandramouli et al.[1], by applying filtering, masking and transformation on the cover media. Weiqi Luo el al.,[2] proposed LSB matching revisited image Steganography and edge adaptive scheme which can select the embedding regions according to the size of the secret message. For large embedding rates, smooth edge regions are used while for lower embedding rate, sharper regions are used. Ahn et al.,[3] propose an image steganographic method based on chaos and euler Theorem in which hidden message can be recovered using orbits which is different from embedding orbits, and the original image is not required to extract the hidden message. Hassan Mathkour et al.,[4] use a new Image Staeganography scheme based on LSB replacement technique and pixel value differencing. This scheme involve replacement of least significant bits in order to hide the colored message image with the advanced LSB methodology wherein the bit replacement takes place in accordance to range specified for the color images. Dobisicek et al.,[5] proposed an authentication model of steganography to detect any attack on the stego image by modifying two coefficients of the Discrete Wavelet Transform in each row of cover image based on a verification code. Neil Provo et al.,[6] has proposed another method to counter the statistical attack is known as Out Guess. In this method corrections are made to the coefficients to make the stego-image histogram match the cover image histogram. Pavan et al.,[7] used entrophy based technique for finding the coefficients in the image where message can be embedded with minimum distortion. Mohammad Shirali-Shahreza [8] proposed a synonym text steganographic technique in which the words in American English are substituted by the words having different terms in British English and vice-versa. Chen Ming et al.,[9] discussed different steganography tool algorithms and classified the tools into spatial domain, transform domain, document based, file structure based and other categories such as spread spectrum technique and video compressing encoding.

Markun Xu et al.,[10] proposed a Model Based steganography technique which is based on least square methods to estimate the embedding rates of secret information.

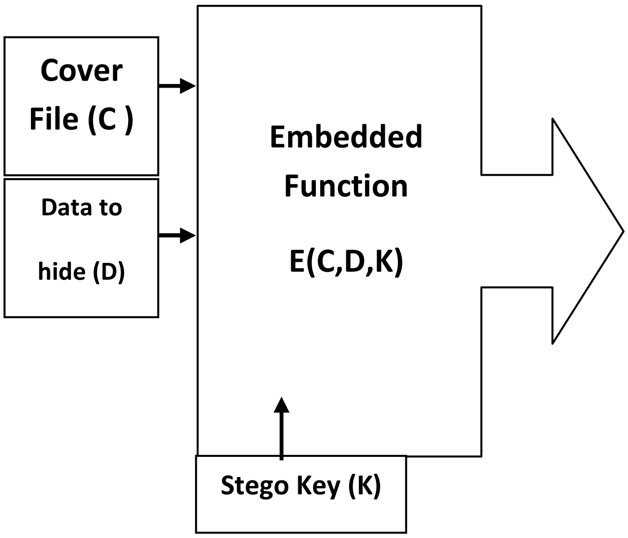


Figure 3 Steganography Diagram

4. STEGANOGRAPHY APPLICATIONS

Steganography is applicable to, but not limited to, the following areas.

- Confidential communication and secret data storing
- Protection of data alteration
- Access control system for digital content distribution
- Media Database systems

5. STEGANOGRAPHY TYPES

Steganography may be classified as pure, symmetric and asymmetric. While pure steganography does not need any exchange of information, symmetric and asymmetric need to exchange of keys prior sending the messages. Steganography is highly dependent on the type of media being used to hide the information. Medium being commonly used include text, images, audio files, and network protocols used in network transmissions.

Image Steganography is generally more preferred media because of its harmlessness and attraction. Additionally exchange of greetings through digital means is on the increase through the increased use of internet and ease of comfort and flexibility is sending them. Technology advancement in design of cameras and digital images saved in cameras and then transfer to PCs[13] has also enhanced many folds. Secondly, the text messages hidden in the images does not distort the image and there are techniques which only disturb only one bit of an image who's effects is almost negligible on its quality. The major drawbacks of Steganography are that one can hide very little information in the media selected. Some methods are following:

- Encoding secret message in text/documents
- Encoding secret message in audio
- Encoding secret message in images

5.1 Text Steganography

5.1.1 Format Based Method

This method modifies the existing text in order to hide the steganographic text. It involves the insertion of spaces, resizing the text, change the style of text to hide the secret message.

5.1.2 Random and Statistical Method

This method hides the characters that are appeared in random sequence. Statistical methods [14] determine the statistics such as means, variance and chi square test which can measure the amount of redundant information to be hide within the text.

5.1.3 Linguistic Method

It is a combination of syntax and semantics methods. Linguistic Steganography considers the linguistic properties generated and modified text, and uses linguistic structure as the space in which messages are hidden. Syntactic steganalysis is to ensure that structures are syntactically correct. Because the text is generated from the grammar, unless the grammar is syntactically flawed, the text is guaranteed to be syntactically correct. In Semantic Method, you can assign the value to synonyms and data can be encoded into actual words of text.

5.2 Audio Steganography

Embedding secret messages into digital sound is known as Audio Steganography. This can embed messages in WAV,AU and even MP3 sound files. There are three techniques that are used are :

- Low bit Encoding
- Phase Encoding
- Spread Spectrum Encoding

5.2.1 Low Bit Encoding

It is used in audio communications like mobile communications and VOIP. It performs to embed the data while pitch period prediction is conducted during low bit-rate speech encoding, thus maintaining synchronization between information hiding and speech encoding.

5.2.2 Phase Encoding

It split the original audio stream file into blocks and embeds the whole secret sequence into the phase spectrum of the first block.
Drawback: Less message Capacity

5.2.3 Spread Spectrum Encoding

It is a form of radio frequency communication. Data sent using the spread spectrum encoding is intentionally spread across as much of the frequency spectrum as possible.

5.3 Image Steganography

Images are cover object used for steganography. Image files are used for storing of digital images. An image file may store data in compressed, uncompressed format. Steganography algorithm operate on three types of images: Pallete based images(i.e. GIF images),Raw images(i.e BMP format) and JPEG images. One of the most popular format used on the internet is JPEG(Joint Photographic Expert Group)

5.3.1 Least Significant Bit Technique

Least Significant Bit (LSB) insertion is a common and simple approach to embed information in an image file. In this method, the LSB of a byte is replaced with an M's bit. For hiding information inside the images, the LSB (Least Significant Byte) method is usually used. To a computer an image file is simply a file that shows different colors and intensities of light on different areas of an image. The best type of image file to hide information inside is a 24 Bit BMP (Bitmap) image.

Algorithm

1. Select a cover image of size M*N as an input.
2. The message to be hidden is embedded in RGB component only of an image.

3. Use a pixel selection filter to obtain a better rate. The filter is applied to Least Significant Bit (LSB) of every pixel to hide information, leaving Most Significant Bit (MSB).
4. After that Message is hidden using Bit Replacement method.

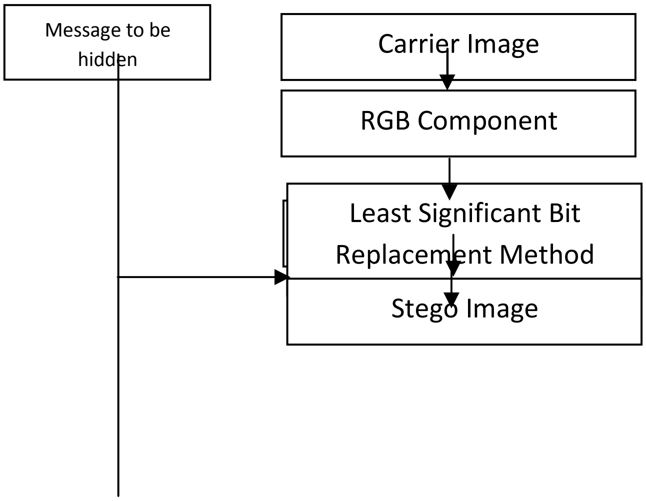
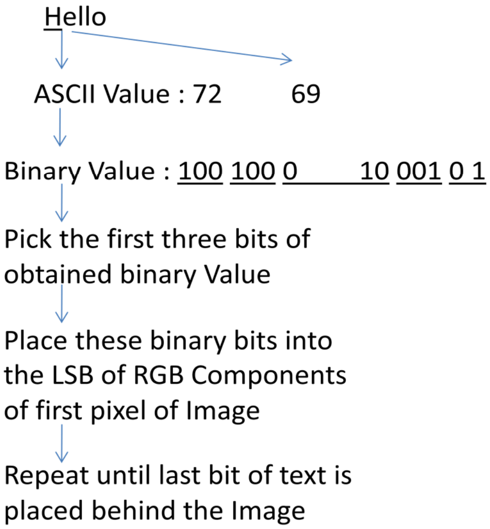


Figure 4: Flowchart For LSB

An Example


Hello
ASCII Value : 72 69
Binary Value : 100 100 0 10 001 0 1
Pick the first three bits of obtained binary Value
Place these binary bits into the LSB of RGB Components of first pixel of Image
Repeat until last bit of text is placed behind the Image

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image [13]. 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. When using a 24-bit image, a bit of each of the red, green and blue colour Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image [13]. 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.

When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data [14]. For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(0010110**1** 0001110**1** 1101110**0**)
(1010011**0** 1100010**1** 0000110**0**)
(1101001**0** 1010110**0** 01100011)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size [14]. Since there are 256 possible intensities of each primary colour, changing the LSB of a pixel results in small changes in the intensity of the colours. These changes cannot be perceived by the human eye - thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference [13].

6. PROBLEMS WITH STEGANOGRAPHY

1. Major problem is the size of the image behind which the text is to be hidden.
2. Secondly, security is the issue if the steganographed image is detected then the actual data can be easily revealed/fetched.
3. To maintain the security if the data is first encrypted using traditional encryption schemes and then steganographed, the time complexity get increased at a higher level.

7. CONCLUSION

Although only some of the main image steganographic techniques were discussed in this paper, one can see that there exists a large selection of approaches to hiding information in images. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Where one technique lacks in payload capacity, the other lacks in robustness. For example, the patchwork approach has a very high level of robustness against most type of attacks, but can hide only a very small amount of information. Least significant bit (LSB) in both BMP and GIF makes up for this, but both approaches result in suspicious files that increase the probability of detection when in the presence of a warden.

Thus, a new method has been proposed in which some sort of encryption is done firstly using K MATRIX (Mapping) that reduces the time complexity in encrypting the message and the encrypted message is then steganographed that improves the security in hiding the message.

References

[1] N.F. Johnson, S. Jajodia, Exploring steganography: seeing the unseen, IEEE Computer 31 (2) (1998) 26–34.

[2] J.C.Judge, Steganography: past, present, future. SANS Institute publication, <http://www.sans.org/ reading room/ whitepapers/ stenganography/ 552.php>, 2001

[3] F.A.P.Petitcolas, R.J.Anderson, M.G.Kuhn:"Information Hiding- A Survey", Process of IEEE, vol.87,no.7, pp.1062-1078, July, 1999.

[4] Artz D (2001). "Digital steganography: hiding data within data" Internet Computing. IEEE, 5(3): 75-80 [5] Derek Upham, Jsteg, http://zooid.org/ Paul/crypto/jsteg.

[6] Nassir Memon R. Chandramouli. Analysis of lbs. based image steganography techniques. In *Proceedings of IEEE ICIP*, 2001.

[7] R. Chandramouli, Nassir Memon, "Analysis of LSB Based Image Steganography Techniques", IEEE 2001. [8] K. Sullivan, Z. Bi, U. Madhow, S. Chandrasekaran, and B. S. Manjunath, Steganalysis of quantization index modulation data hiding, Proc. of 2004 IEEE International Conference on Image Processing, vol. 2, pp. 1165-1168, 2004.

[9]Jar no Mielikainen, "LSB Matching Revisited", Signal Processing Letters, IEEE, Publication Date: May 2006 Volume : 13, Issue : 5, pp. 285- 287

[10] K. Gopalan. Audio steganography using bit modification. In Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP '03), volume 2, pages 421–424, 6-10 April 2003.

[11] N. Johnson, Survey of Steganography Software, Technical Report, January 2002.

[12] W. Peter. Disappearing Cryptography: Information Hiding: Steganography and watermarking (second edition). San Francisco: Margan Kaufmann.

[13] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", *Computer Journal*, February 1998.

[14] Krenn, R., "Steganography and Steganalysis", http://www.krenn.nl/univ/cry/steg/article.pdf