Review Paper On Image Based Steganography

By Indu Nehra, Rakesh Sharma

Abstract: Steganography is one of the methods used to hide information for the purpose of exchanging information and it can be defined as the study of communication that usually deals with ways of hiding the message with other medium like image, audio etc. In this way, if message is hidden properly,then message is not easy to be extracted by from eavesdroppers and attackers. Using steganography, information can be hidden in different embedding mediums, known as carriers. These carriers can be images, audio files, video files, and text files. This is a review paper for various studies done on steganography. Also paper provides various ways for betterment of LSB method of staganography.

1. Introduction

In the current trends of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the world. There are many possible ways to transmit data using the internet: via e-mails, chats, etc. The data transition is made very simple, fast and accurate using the internet. However, one of the main problems with sending data over the internet is the „security threat‟ it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most essential factors that need attention during the process of data transferring.

Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data modification. This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet. In order to improve the security features in data transfers over the internet, many techniques have been developed like: Cryptography, Steganography and digital watermarking. While Cryptography is a method to conceal information by encrypting it to „cipher texts‟ and transmitting it to the intended receiver using an unknown key, Steganography provides further security by hiding the cipher text into a seemingly invisible image or other formats.

Cryptography and steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence. These techniques have many applications in computer science and other related fields: they are used to protect e-mail messages, credit card information, corporate data, etc. communication. A steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. As an example, it is possible to embed a text inside an image or an audio file. On the other hand, cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

Cryptography protects information by transforming it into an unreadable format. It is useful to achieve confidential transmission over a public network. The original text, or plaintext, is converted into a coded equivalent called ciphertext via an encryption algorithm. Only those who possess a secret key can decipher (decrypt) the ciphertext into plaintext. Cryptography systems can be broadly classified into symmetric-key systems that use a single key (i.e., a password) that both the sender and the receiver 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.

It is a high security technique for long data transmission. There are various methods of steganography:

1 .Least significant bit (LSB) method
2. Transform domain techniques
3. Statistical methods
4. Distortion techniques

2. Details of each method

Least significant bit (LSB) method

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. This technique works good for image, audio and video steganography. To the human eye, the resulting image will look identical to the cover object. For example, if we consider image steganography then the letter A can be hidden in three pixels (assuming no compression). The original raster data for 3 pixels (9 bytes) may be

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

The binary value for A is 10000001. Inserting the binary value for A in the three pixels would result in

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

The underlined bits are the only three actually changed in the 8 bytes used. On average, LSB requires that only half the bits in an image be changed. You can hide data in the least and second least significant bits and still the human eye would not be able to discern it.

Transform domain techniques

This is a more complex way of hiding information in an image. Various algorithms and transformations are applied on the image to hide information in it.

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.

Distortion techniques

Distortion techniques require knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder, on the other hand, adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion.

3. Literature review

The word cryptography is derived from two Greek words which mean "secret writing". Cryptography is the process of scrambling the original text by rearranging and substituting the original text, arranging it in a seemingly unreadable format for others. Cryptography is an effective way to protect the information that is transmitting through the network communication paths (**Bishop, 2005).**

Steganography in Greek means "covered writing". Steganography is the process of hiding the one information into other sources of information like text, image or audio file, so that it is not visible to the natural view. There are varieties of steganographic techniques available to hide the data depending upon the carriers we use. Steganography and cryptography both are used for the purpose of sending the data securely.

In steganography the message is kept secret without any changes but in cryptography the original content of the message is differed in different stages like encryption and decryption. Steganography supports different types of digital formats that are used for hiding the data. These files are known as carriers. Depending upon the redundancy of the object the suitable formats are used. Redundancy is the process of providing better accuracy for the object that is used for display by the bits of object. The main file formats that are used for steganography are Text, images, audio, video, protocol **(Morkel, 2005).**

Cryptology is the science that deals about cryptography and cryptanalysis. Cryptography is the approach of sending the messages secretly and securely to the destination. Cryptanalysis is the method of obtaining the embedded messages into original texts**(Whitman, 2007).**

C.P.Sumathi et. al (2013) describes, While steganography can be achieved using any cover media, we are concerned with hiding data in digital images. The features expected of a stego-medium are imperceptibility and robustness, so that the secret message is known only to the intended receiver and also the stego-medium being able to withstand attacks from intruders. The amount of secret message embedded should be such that it doesn't reduce the quality of the stego image. The goal of steganography is to embed secret data into a cover in such a way that no one apart from the sender and intended recipients even realizes there is secret data. A few key properties that must be considered when creating a digital data hiding system are

- Imperceptibility: Imperceptibility is the property in which a person should be unable to distinguish the original and the stego-image.
- Embedding Capacity: Refers to the amount of secret information that can be embedded without degradation of the quality of the image.

- Robustness: Refers to the degree of difficulty required to destroy embedded information without destroying the cover image.

Mamta Juneja, and Dr. Parvinder S. Sandhu(2013), proposed an improved LSB(least Significant bit) based Steganography technique for images imparting better information security . They presents an embedding algorithm for hiding encrypted messages in nonadjacent and random pixel locations in edges and smooth areas of images. It first encrypts the secret message, and detects edges in the cover-image using improved edge detection filter. Message bits are then, embedded in the least significant byte of randomly selected edge area pixels and 1-3-4 LSBs of red, green, blue components respectively across randomly selected pixels across smooth area of image.

M.Rajkamal And B.S.E.Zoraida(2014), developed a new technique of image steganography inside the embedding the encrypted Data file or message using Hash-LSB with RSA algorithm for providing more security to data as well as our data hiding method. The developed technique uses a hash function to generate a pattern for hiding data bits into LSB of RGB pixel values of the carry image. This technique makes sure that the data has been encrypted before embedding it intoa carry image. Embedded-text in images usually carries important messages about the content.

Efficiency considerations

Which working with the concept, we studied the concept of LSB. We found three main issues which needs to be cover for efficiency and security of message which is hidden in the image.

- **Storing length of message:** As per most of the references, the length is stored in first 31 pixels and data is stored in next each pixel. This is the general idea. So a malicious user can retrieve the first step of message by first 31 pixels. We thought to store this length somewhere else.

- **Storing message:** After the length, the data is being stored in each pixel which can be easily retrieved by any malicious user. We had idea of hide the dmessage not in continous pixel, this might be stored in even pixels or odd pixels or any arbitrary order like every 5th pixel. Its dependent on the size of message to be hidden behind the image.

- **Encoding messages:** The first concen of study was to make message more and more secure. Any malicious user can retrieve the data easily if the structure of storage of message is known. So one more thought was to given on security of data/message. We found that data should be stored in LSB after encryption so that this will be next layer of security.

4. References

[1] Ali-al, H. Mohammad, A. 2010. Digital Audio Watermarking Based on the Discrete Wavelets Transform and Singular Value Decomposition, European Journal Of Scientific Research, vol 39(1), pp 231-239.

[2] Amirthanjan, R. Akila,R & Deepika chowdavarapu, P., 2010. A Comparative Analysis of Image Steganography, International Journal of Computer Application, 2(3), pp.2-10.

[3] Arnold, M. 2000. Audio watermarking: Features, applications and algorithms,
Proceeding of the IEEE International Conference on Multimedia and Expo,
pp 1013-1016.

[4] Bandyopadhyay, S.K., 2010. An Alternative Approach of Steganography Using Reference Image. International Journal of Advancements in technology , 1(1), pp.05-11.

[5] Siridevi,R. Damodaram, A. & Narasingham, S.,2009. Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security. Journal of theoretical and applied information technology, 5(2), pp.25-31.

[6] Zaidoon Kh, A. Zaidan,A.A. Zaidan,B.B & Alanazi.H.O., 2010. Overview: main fundamentals for steganography. Journal of Computing, 2(3), pp.40-43.

[7] C.P.Sumathi et al(2013) A Study of Various Steganographic Techniques
Used for Information Hiding, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6.

[8] Mamta Juneja (2013), An Improved LSB based Steganography Technique for RGB Color Images, 2nd International Conference on Latest Computational Technologies (ICLCT'2013) June 17-18.

[9] Masoud Nosrati(2013), An introduction to steganography methods, World Applied Programming, Vol (1), No (3) pp 191-195.