SURVEY AND ANALYSIS OF VARIOUS STEGANOGRAPHIC TECHNIQUES

Ramanpreet Kaur[1], Prof.Baljit Singh[2]

[1] *Student of Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib.* ***er.raman12@yahoo.com***
[2]*Assist.prof.of Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib.*

Abstract

Steganography is a method of secret communication that hides the existence of hidden message. The hidden message can be text, image, audio, video, etc. The innocent files can be a cover image after inserting the message into the cover image using stego-key, it is reffered to as stego-image. Steganography becomes more important due to the exponential growth and secret communication of potential computer users on the internet. Steganography is different from cryptography in the way that cryptography hides the contents of secret message where as steganography is about hiding the message. In this paper various steganographic techniques have been analyzed. This paper also gives an overview of steganography, its applications, how it is different from cryptography and different methods of steganography.

Index Terms: *Cryptography, Filtering and Masking, Spatial domain, Steganography, Transform domain.*

---------- *** ----------

1. INTRODUCTION

Steganography is the art of hiding data in a cover. The cover can be text, audio, image, video, etc.The goal of steganography is to hide the existence of a message. The word steganography comes from the Greek Steganos, which mean covered or secret and graphy mean writing or drawing, that combined means, "Covered Writing". The original files can be a cover text, cover image, or cover audio, after inserting the secret message using stego-key which is used for hiding the message, it is referred to as stego-image, stego-text etc. For hiding the data, the image quality means the quality of the stego-images.

The cracking or extraction of steganographic messages is called steganalysis, and it is of two main types. The first type which is easiest type of extraction makes the hidden message unreadable by modifying the carrier. The goal of steganalysis is to identify the information and determining that whether or not they have hidden messages encoded into them and if possible, extract the hidden information [6].

2. STEGANOGRAPHY VS. CRYPTOGRAPHY

Basically, purpose of cryptography and steganography is to provide secret communication. However, steganography and cryptography are different. Cryptography hides the contents of message from intruders, whereas steganography even conceals the existence of that message[4].Cryptography is about protecting the content of messages (their meaning) from the third party, where as steganography is about hiding the existence of message so that intermediate persons cannot see the message.

In cryptography, the structure of a message is scrambled so that it can't be understood and it is undetectable until the decryption key is not known. It doesn't hide the encoded message. Basically, cryptography transmits the information between two or more persons in a way that the third party is not able to read it. Advantage of cryptography is that it provide authentication for verifying the identity of someone or something [4].

In steganography, it does not alter the structure of the secret message, but hides the message into a cover-image so that nobody can see it. In other words, steganography prevents an unintended recipient from suspecting that the data exists [4].

The main advantage of steganography over other methods such as cryptography is that, a third party can't even guess if message falls in their hand. Unlike cryptographic messages, stegnographic messages will not attract the attention of a third party that there exists a message. Thus stegnography has benefit over cryptography as it involves both encryption and security.

3. APPLICATIONS OF STEGANOGRAPHY:

The interest is increasing day by day in the digital steganography. Image trafficking applications due to the internet is more popular. Stegnography becomes more important due to the exponential growth and secret communication of potential computer users on the internet. Intruders can acquire the information from a system and they can reveal the information to others or can read or modify the information that needs to be secure, so for this type of security stegnography is useful. . Intruders can use information to launch an attack One solution to this problem is, through the use of steganography.

Steganography can be used for wide range of applications such as:

1. Steganography is mainly used for securing the confidential information or data during transmission and storage. For example, one can hide a secret message in an audio file and transfer to another party through email instead of sending the message in the textual format.
2. In defence organisations, for the safety of secret data.
3. In smart identity cards where personal details are inserted in the photograph itself for copyright control of materials [8].
4. In medical imaging, for embedding patient's details within image provides protection of information and reduce the transmission time and cost [8].
5. In online voting system for securing the online election.
6. In Military communications systems, for increasing use of traffic security technique, instead of concealing the contents of a message using encryption, conceal its sender or its receiver or its very existence [4].

4. DIFFERENT KINDS OF STEGANOGRAPHY

The four main categories of file formats that can be used for steganography are:

i. Text
ii. Images
iii. Audio
iv. Protocol

4.1. Text steganography: Hiding information in text is historically the most important method of steganography. A simple method was to hide a secret message in every nth letter of every word of a text message. Due to the beginning of the Internet and due to the different type of digital file formats it has decreased in importance. Text stegnography using digital files is not used very often because the text files have a very small amount of redundant data [9].

4.2. Image steganography: Images are the most popular cover objects for steganography [9]. A message is embedded in a digital image (cover image) through an embedding algorithm, by using the secret key. The resulting stego image is transmitted to the receiver. On the other hand, it is processed by the extraction algorithm using the same key. During the transmission of stego image, it can be monitored by some unauthenticated persons who will only notice the transmission of an image but can't guess the existence of the hidden message.

4.3. Audio steganography: Audio stegnography is masking, which exploits the properties of the human ear to hide information unnoticeably. An audible, sound becomes inaudible in the presence of another louder audible sound .This property allows to select the channel in which to hide information.Although it is similar to images in steganographic potential, the larger size of meaningful audio files makes them less popular to use than images[9].

4.4. Protocol steganography: The term protocol steganography refers to embedding information within network protocols such as TCP/IP. An example of it is hiding information in the header of a TCP/IP packet in some fields that can be either optional or are never used.

5. STEGANOGRAPHIC TECHNIQUES

As we have discussed above that images are the most popular cover objects for steganography, so this paper introduced various stegnography techniques for hiding data in images. The images are represented with numerical values of each pixel where the value represents the color and intensity of the pixel.
Images are mainly of two types:
24-bit images
8-bit images

24-bit images: These images have 24 bit value for each pixel in which each 8 bit value refers to three colors red, blue and green.
8-bit images: In 8-bit images maximum number of colors that can be present are only 256 colors.

Steganographic techniques for image file format are classified as:

i. Spatial domain technique
i. Masking and filtering
ii. Transform techniques

5.1 Spatial Domain Technique

In spatial domain methods a steganographer modifies the secret information and the cover medium in the spatial domain, which involves the LSBs.

LSB Technique: The simplest of the LSB steganography techniques is LSB replacement. In LSB replacement steganography the data or message which is to be hidden is inserted into the least significant bits of the pixel information.
24-bit images*:* We can store 3 bits of information in each pixel, one in each LSB position of the three 8 bit values in 24 bit value.

For example suppose 3 pixels of a 24-bit image can be as follows:
(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

The Secret number is 200(11001000)

The result is as follows:
(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the image, only the 3 bits needed to be changed according to the embedded message. On average, LSB requires that only half the bits in an image be changed to hide a secret message. 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. Still, human eye would not be able to discover these changes thus we can say that the message is successfully hidden.

8-bit images: In these images 1 bit of information can be hidden in each pixel. The color variation may occur and therefore, care should be taken in selecting the cover image. For example, a simple four-color palette of white, blue, green and red has corresponding palette position of 00, 01, 10 and 11 respectively. The raster values of four adjacent pixels of white, white, blue, and blue are 00, 00, 10, and 10.

The secret number is 01 (0001)

It will change the raster data to 00,00,10,11, which is white, white, and green, red. These changes in the color of image are visible and clearly highlight the weakness of using 8-bit images.

Advantages of spatial domain LSB technique are:

1. There is less chance for degradation of the original image.
2. Hiding capacity is more i.e. more information can be stored in an image.
3.

Disadvantages of LSB technique are:

1. Less robust, the hidden data can be lost with image manipulation.
2. Hidden data can be easily destroyed by simple attacks.

5.2 Masking and Filtering

These techniques, usually restricted to 24 bits and gray scale images, hide information by marking an image, in the same way as to paper watermarks. These techniques embed the information in the more significant areas than just hiding it into the noise level, so that the hidden message is more integral to the cover image. Watermarking techniques may be applied without the fear of image destruction due to lossy compression as they are more integrated into the image.

Advantages of Masking and filtering Techniques:

This method is much more robust than LSB replacement with respect to compression since the information is hidden in the visible parts of the image.

Disadvantages:

These techniques can be applied only to gray scale images and restricted to 24 bits.

5.3 Transform Domain Technique

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.

Transform domain techniques are broadly classified into three categories:

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).

5.3.1. Discrete Fourier Transformation Technique (DFT):

DFT is used to transfer an image from spatial domain into frequency domain.
DFT is defined by the following equation:

$$F(u,v)=\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)e^{-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)}$$

$$u=0,1,2,\ldots,M-1 \text{ and } v=0,1,2,\ldots,N-1$$

M and N are the size of image.
Inverse Discrete Fourier Transform (IDFT).

$$f(x,y)=\frac{1}{MN}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}F(u,v)e^{j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)}$$

$$x=0,1,2,\ldots,M-1 \text{ and } y=0,1,2,\ldots,N-1$$

Fourier Transform (FT) methods introduce round off errors, thus it is not suitable for hidden communication.

The difference between a Discrete Fourier Transform and a Discrete Cosine Transform is that the DCT uses only real numbers, while a Fourier transform can use complex numbers.

5.3.2. The Discrete Cosine Transform (DCT):

DCT is a popular signal transformation method, which is making use of cosine functions of different frequencies. There are several variants of DCT with few modifications in definitions and properties, like DCT I, II, III, IV, V-VIII with the corresponding inverse formulas. Among these types the DCT II, is usually used in image processing and compression (JPEG, MPEG), because it has strong energy compaction, meaning that a few coefficients enclose the most of the signal in process.

The DCT transforms a cover image from an image representation into a frequency representation, by dividing the image pixels into blocks of 8×8 pixels and then compute the two-dimensional DCT for each block and transforms the pixel blocks into 64 DCT coefficients each. A modification of a single DCT coefficient will affect all 64 image pixels in that block. The DCT coefficients of the transformed cover image will be quantized, and then coded according to the secret data. The secret data is embedded in the carrier image for DCT coefficients lower than the threshold value. To avoid visual distortion, insertion of secret information is avoided for DCT coefficient value 0. Insertion and extraction of secret image is an important part for any steganographic technique. It separates the image into parts of differing in importance. It can separate the image into high, middle and low frequency components.

The mathematical definition of DCT is:
The general equation for a 1D (N data items) DCT is defined by the following equation:

$$F(u)=\left(\frac{2}{N}\right)^{\frac{1}{2}}\sum_{i=0}^{N-1}\Lambda(i).cos\left[\frac{\pi.u}{2.N}(2i+1)\right]f(i)$$

where

$$\Lambda(i)=\begin{cases}\frac{1}{\sqrt{2}} & \text{for}\xi=0\\ 1 & \text{otherwise}\end{cases}$$

and the corresponding inverse 1D DCT transform is simple $F^{-1}(u)$.

The general equation for a 2D (N by M image) DCT is defined by the following equation:

$$F(u,v)=\left(\frac{2}{N}\right)^{\frac{1}{2}}\left(\frac{2}{M}\right)^{\frac{1}{2}}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}\Lambda(i).\Lambda(j).cos\left[\frac{\pi.u}{2.N}(2i+1)\right]cos\left[\frac{\pi.v}{2.M}(2j+1)\right].f(i,j)$$

High energy compactness and thus the resulted DCT coefficients fully describe the signal in process is the advantage of DCT.

5.3.3. Discrete Wavelet Transform (DWT):

A Wavelet is simply, a small wave which has its energy concentrated in time to give a tool for the analysis of transient, non-stationary or time-varying phenomena. A signal can be better expressed as a linear decomposition of sums of products of coefficient and functions. A system with two-parameters is constructed, with one having a double sum and coefficient with two indices. The set of coefficients are called the DWT of a signal.

Wavelet transform is used to convert a spatial domain into frequency domain. The use of wavelet in image stenographic model is that the wavelet transform separates the high frequency and low frequency information on a pixel by pixel basis. Discrete Wavelet Transform (DWT) is always preferred over Discrete Cosine Transforms (DCT) because at various levels image in low frequency can offer corresponding resolution needed.
The use of DWT transforms mainly address the capacity of the Information-Hiding system features and robustness. The hierarchical nature of the Wavelet representation allows multi-resolutional detection of the hidden message, which is a Gaussian distributed random vector added to all the high pass bands in the Wavelet domain.

The Forward DWT Eq. is:-

$$W\varphi(J_O, K) = \frac{1}{\sqrt{M}} \sum_n f(n) \varphi j_{\,o,k}(n)$$

$$W_\Psi(j, k) = \frac{1}{\sqrt{M}} \sum_n f(n) \Psi_{J,K}(n) \quad \text{for } j \geq j_0$$

The complementary inverse DWT Eq. is:-

$$f(n) = \frac{1}{\sqrt{M}} \Sigma\, W\varphi(J_O, K)\, \varphi j_{o,k}(n) + \frac{1}{\sqrt{M}} \Sigma\, \Sigma\, W_\Psi(j,k)\, \Psi_{J,K}(n)$$

Advantages of Transform Domain Technique:

1. These methods hide messages in more significant areas of the cover-image, which make them more robust to attack than LSB.
2. Transformations can be applied to the entire image, to block throughout the image, or other variants.

Disadvantages:

Methods of this type are computationally complex.

6. CONCLUSION

This paper introduced stegnography and analyzed various techniques of stegnography. Steganography hides the message so that intermediate persons cannot see the message. Different stenography techniques have their own strong and weak points. So, it depends upon the size of image (8bit or 24bit) and type of image (jpeg, png, gif etc.) that which technique is to be preferred. The LSB technique has more hiding capacity but is less robust than other techniques like filtering and transform. On the other hand filtering and masking techniques is restricted to 24 bit and transform techniques are complex and slower.

ACKNOWLEDGEMENT

I am thankful of my Professor, Prof. Baljit Singh who has supported and encouraged me to do this work.

REFERENCES

[1]. Vijay Kumar Sharma and Vishal Shrivastava, "A Stegnography Algorithm for hiding image in image by improved LSB substitution by minimize detection", Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1.

[2].Lina Saeed Jajo and Susan.S.Ghazoul, "Improving Hiding Information Process based on GA Technique with Secure Extraction Process", ijccoe, vol10, n0.1, 2010.

[3]. Ünal Tatar and Tolga Mataracioglu, Tubitak Uekae, "Analysis and Implementation of Distinct Steganographic Methods", Department of Information Systems Security 06700, Kavaklıdere, Ankara/Turkey.

[4]. Muhalim Mohamed Amin, Subariah Ibrahim ,Mazleena Salleh and Mohd Rozi Katmin, "Information Hiding using Stegnography", of Computer System & Communication Faculty of Computer Science and Information system Universiti Teknologi Malaysia 2003.

[5]. Ghasemi Elham, Shanbehzadeh Jamshid and ZahirAzami Bahram, "A Steganographic method based on Integer Wavelet Transform and Genetic Algorithm", 978-1-4244-9799-7/111$26.00 ©20 11 IEEE.

[6].Kumar Arvind and Km. Pooja, "Steganography- A Data Hiding Technique" International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.

[7]. Goudar R.M. ,Prashant N. Patil, Aniket G. Meshram*, Sanyog M. Yewale, Abhay V. Fegade, "Secure Data Transmission by using Steganography" , Information and Knowledge Management ISSN 2224-5758 (Paper) ISSN 2224-896X (Online) Vol 2, No.1, 2012.

[8].Babloo Saha and Shuchi Sharma, "Steganographic Techniques of Data Hiding using Digital Images", Defence Science Journal, Vol. 62, No. 1, January 2012.

[9]. T. Morkel, J.H.P. Eloff, M.S. Olivier, "An Overview Of Image Stegnography", Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.

[10].Kaveh Ahmadi, "A New Method for Image Security and Data Hiding in Image", American Journal of Scientific Research ISSN 1450-223X Issue 38(2011), pp. 41-49© EuroJournals Publishing, Inc. 2011.

BIOGRAPHIES

Ramanpreet Kaur doing Master of Technology in Computer Science with specialization in E-Security at BBSBEC, Fathehgarh Sahib and completed B.Tech in Information Technology from the same college. After completion of Masters willing to work in challenging environment to enhance the knowledge.