International Journal of Current Engineering and Technology
©2015 INPRESSCO®, All Rights Reserved

E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Review Article

A Review on different Patching Techniques

Suchi Kumari[†*] and Sanjeev Ranjan[†]

[†]Birla Institute of Technology, Ranchi, Jharkhand, India

Accepted 15 March 2015, Available online 21 March 2015, **Vol.5, No.2 (April 2015)**

Abstract

Steganography is an advanced version of cryptography basically used for coding practice and for hiding private information. While cryptography provides privacy, Steganography is intended to provide secrecy. Steganography means hiding one piece of data within another. There are different types of Steganography: Text Steganography, Image Steganography and Audio Steganography. This work will focus on comparative study on major techniques like LSB, Masking and Filtering, Transformation Domain based technique, Chaffing and Winnowing, Jsteg and F5 algorithm. It will also present the best algorithm of steganography of each type.

Keywords: *Cryptography, Jsteg, Steganography, Chaffing and Winnowing*

1. Introduction

With the ever increase in the amount of data to be stored and transmitted in various communication medium, the confidentiality and security should be maintained. Steganography is an extension of cryptography, and it is commonly used under the circumstances where encryption is not allowed.

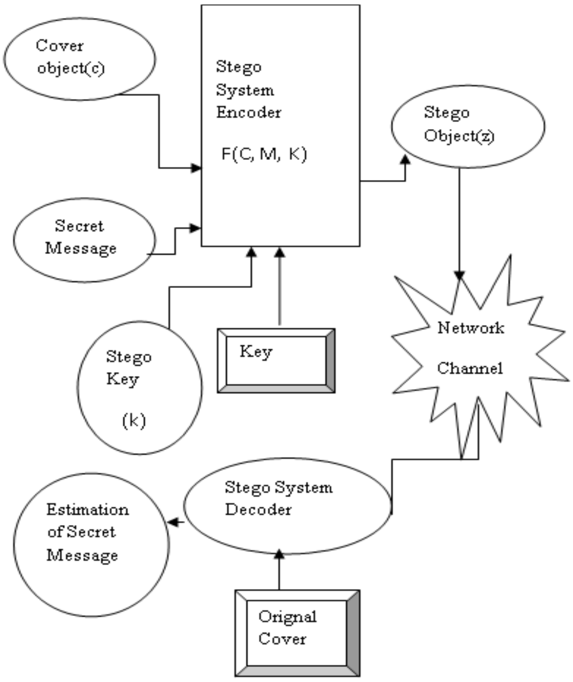


Fig.1 Basic Steganography Model

Different types of Steganography

Text Steganography uses the theme of missing letter puzzle. It is mostly applied for hiding information in plain text. Image Steganography exploits the weakness of the human visual system (HVS). It is widely used for hiding the secret message into a digital image. Audio Steganography embeds the secret message into digitized audio signal which result in slight altering of binary sequence of corresponding audio files and is basically used in WAV, AU even MP3 sound file.

2. Literature Survey

Around 500 B.C., Demaratus used the technique of Steganography. J.R.Krenn explained Steganography and its implementation techniques. Deshpande Neeta, et. al. proposed the Least Significant Bit embedding technique. K.B.Raja, et. al. proposed a challenging task of transferring the embedded information to the destination without being detected. Vijay Kumar Sharma, et. al. hadworked on a new steganography algorithm for 8bit (gray scale) or 24bit (color image) based on Logical operation to ensure the security against the steganalysis attack. Po-Yueh Chen, et.al. proposed a new Steganography technique which embeds the secret messages in frequency domain.

Beenish Mehboob, et.al. discusses the art of hiding data in a colorful image using least significant bit. Hassan Mathkour, et. al. set criterion to analyze and evaluate the strengths and weaknesses of the presented techniques.

LSB Technique

It embeds the message bit at the right most bits of pixel value so that the embedding method does not affect the

*Corresponding author **Suchi Kumari** and **Sanjeev Ranjan** are M.Tech, Computer Science and M.S, Embedded System original pixel value greatly. Traditionally, it is based on embedding each bit from the message in the least significant bit of the cover audio or video in a deterministic way.

LSB Techniques used in Still Images

Images are mainly of two types

8-bit images

The LSB or in other words 8-th bit of some or all the bytes inside an image is changed to a bit of the secret message. Let us consider a cover image contains the following bit patterns:
Byte-1 Byte-2 Byte-3 Byte-4
00101101 00011100 11011100 10100110
Byte-5 Byte-6 Byte-7 Byte-8
11000100 00001100 11010010 10101101
Suppose a number 200 is to embed in the above bit pattern. Now the binary representation of 200 is 11001000. To embed this information at least 8 bytes in cover file is needed. Hence 8 bytes in the cover file is taken. Now modify the LSB of each byte of the cover file by each of the bit of embed text 11001000.Table I: shows effect on cover file text after embedding 11001000 in the LSB of all 8 bytes.

Table 1 Illustration of LSB technique

Before Replacement	After Replacement	Bit Inserted	Remarks
00101101	00101101	1	No change in bit pattern
00011100	00011101	1	Change in bit pattern(i)
11011100	11011100	0	No change in bit pattern
10100110	10100110	0	No change in bit pattern
11000100	11000101	1	Change in bit pattern(ii)
00001100	00001100	0	No change in bit pattern
11010010	11010010	0	No change in bit pattern

24-bit images

These images have 24 bit value for each pixel in which each 8 bit value refers to the colors *red blue* and *green*. RGB 24 bit color image is achieved by applying the concept of the linked list data structures to link the secret messages in the images. The secret message bytes are embedded in the color image erratically and randomly and every message contains a link or a pointer to the address of the next message in the list. Also, a few bytes of the address of the first secret message are used as the stego-key to authenticate the message.

Masking and Filtering

It can be used on 24 bit per pixel images. The technique can be used for both colour and grey-scale images. It is similar to placing watermarks on a printed image. Masking is more robust than LSB insertion with respect to compression, cropping, and some image processing.

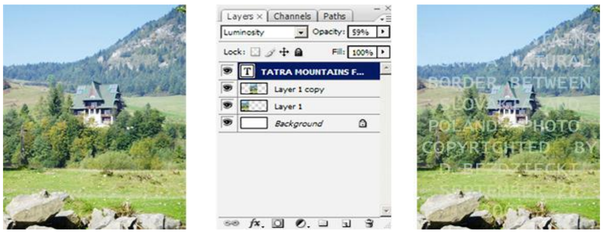


Fig.2 Masking and Filtering

Fig2 illustrate how masks and filters can be embedded into images without destroying the original quality of an image. This image cannot be illegally copied, edited or used in any application in which it was not originally intended. Changing the luminosity and opacity of the watermark layers will provide varying results. The image above has opacity of zero percent. The opacity is gradually increased until the watermark layer becomes visible.

Transformation Domain based technique

It transforms the cover image into different domain. Then the transformed coefficients are processed to hide the secret information. These changed coefficients are transformed back into spatial domain to get stego image.

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)

1. Discrete Fourier Transformation Technique (DFT)

DFT is used to transfer an image from spatial domain into frequency domain. It shares all properties of the Fourier transform.

In the following, we always assume

$$\mathcal{F}[x[m]] = X(e^{j\omega}) \quad \text{and} \quad \mathcal{F}[y[m]] = Y(e^{j\omega})$$

(a)Linearity

$$\mathcal{F}\big[ax[m] + by[m]\big] = aX(e^{j\omega}) + bY(e^{j\omega})$$

(b)Time Shifting

$$\mathcal{F}\big[x[m - m0]\big] = e^{-jm0\omega}X(e^{j\omega})$$

(c)Time Reversal

$$\mathcal{F}\big[x[-m]\big] = X(e^{-j\omega})$$

(d)Frequency Shifting

$$\mathcal{F}[x[m]e^{j\omega 0m}] = X\big(e^{j(\omega-\omega 0)}\big)$$

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

2. The Discrete Cosine Transform (DCT)

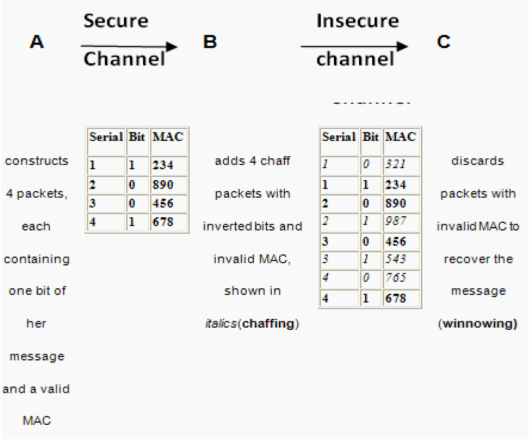
DCT uses cosine functions of different frequencies. It transforms a cover image from an image representation into a frequency representation, by dividing the image pixels into blocks of 8×8 pixels and then computes the two-dimensional DCT for each block and transforms the pixel blocks into 64 DCT coefficients each. It separates the image into parts of differing in importance. It can separate the image into high, middle and low frequency components.

3. Discrete Wavelet transformation technique (DWT)

It is used to convert a spatial domain into frequency domain. The use of wavelet in image stenographic model is to separate the high frequency and low frequency information pixel by pixel basis. 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-resolution detection of the hidden message, which is a Gaussian distributed random vector added to all the high pass bands in the Wavelet domain.

Chaffing and Winnowing

It achieves confidentiality without using encryption. It allows the sender to deny responsibility for encrypting their message. When using chaffing and winnowing, the sender transmits the message unencrypted, in clear text. Although the sender and the receiver share a secret key, they use it only for authentication. However, a third party can make their communication confidential by simultaneously sending specially crafted messages through the same channel. Chaffing and winnowing lends itself especially well to use in packet switched networks environments such as the Internet, where each message (whose payload is typically small) is sent in a separate network packet.



constructs 4 packets, each containing one bit of her message and a valid MAC

Serial	Bit	MAC
1	1	234
2	0	890
3	0	456
4	1	678

adds 4 chaff packets with inverted bits and invalid MAC, shown in *italics*(**chaffing**)

Serial	Bit	MAC
1	*0*	*321*
1	1	234
2	0	890
2	*1*	*987*
3	0	456
3	*1*	*543*
4	*0*	*765*
4	1	678

discards packets with invalid MAC to recover the message (**winnowing**)

In above example, A wishes to send the message "1001" to C. For simplicity, assume that all even MAC is valid and odd ones are invalid.

Jsteg

Jsteg is safely detected by statistical attack. This algorithm is one of the stenographic techniques for embedding data into JPEG images, which is proposed by D. Upham. It works by embedding message bits as the LSBs of the quantized DCT (Discrete Cosine Transform) coefficients. The embedding mechanism skips all coefficients with the values of '0' or '1'.There are two embedding ways according to the selection of coefficients.

One is sequential embedding; the other is random embedding whose coefficients selection is usually determined by a secret stego key shared by the communicating parties. J-Steg with sequential message embedding is detectable using the chi-square attack. JSteg algorithm replaces LSBs of quantized Discrete Courier Transform (DCT) coefficients. In this process the hiding mechanism skips all coefficients with the values of 0 or 1. This algorithm is resistant to visual attacks and offers an admirable capacity for stenographic messages. Generally, JSteg stenographic algorithm embedded the messages in lossy compressed JPEG images. It has high capacity and had a compression ratio of 12%.

F5 Algorithm

F5 is used for hiding information in JPEG images

Since the embedding is not based on bit-replacement or exchanging any fixed Pairs of Values, the F5 algorithm cannot be detected using the chi-square attack or its generalized versions. On the other hand, the F5 algorithm does modify a macroscopic quantity of the JPEG file – the histogram of DCT coefficients – in a predictable manner.

F5 implements matrix encoding to improve the efficiency of embedding. Thus it reduces the number of necessary changes. F5 employs permutative straddling to uniformly spread out the changes over the whole steno gram. As a special feature, the F5 algorithm employs matrix embedding to minimize the necessary number of changes to embed a message of certain length.

Continuous Embedding

In most of the cases, an embedded message does not require full capacity. Hence a part of the file remains unused.

Fig.3 Continuous Embedding concentrates changes(x)

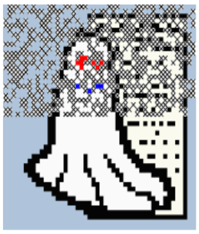


Fig.4 changes (x) concentrate on the start of the file, and unused rest resides on the end.

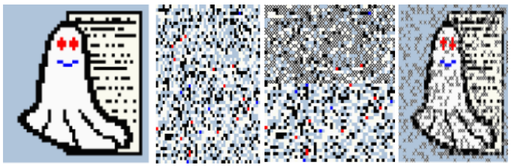


Fig.5 Permutative Straddling scatters the changes (x)

3. Performance Analysis

Table 2 List of all steganography techniques: Analysis on the basis of its advantages and disadvantages

Technique	Advantage	Disadvantage
LSB	Less chance for degradation of original image.	Less robust, the hidden data can be lost with image manipulation.
Masking and Filtering	More robust than LSB replacement with respect to compression since the information is hidden in the visible parts of the image.	Technique can be applied only to grey scale images and restricted to 24 bits.
Transformation domain based technique	These methods hide images in more significant areas of the cover-image, which makes them more robust to attack than LSB.	Methods of this type are computationally complex.
Chaffing and Winnowing	This technique is used to achieve confidentiality without using encryption when sending data over an insecure channel.	It is not based on the difficulty of breaking an encryption scheme.
Jsteg	First publicly available and simple solution.	Jsteg embedding disrupts the symmetry of histogram.
F5 Algorithm	High stenographic capacity.	The F5 algorithm cannot be detected using the chi-square attack or its generalized versions.

Conclusion

It is very difficult to conclude that a particular method is best among all. Since, each method has their own advantages, and also disadvantages in comparison with other methods of steganography. The advantage on using one technique over another one depends on the application constraints in use and its requirement for hiding capacity, embedded data security level and encountered attacks resistance.

So, comparison can be done of different aspects, which results in determining a suitable method for a specific usage.

Future Work

In the future, it is hoped that the technique of steganography will advance such that it will become much easier to encrypt secret messages in other coded forms with less complexity.

Acknowledgement

The author would like to thank Anonymous Reviewers for their valuable suggestions and Comments which helped to improve the Clarity and Presentation of the Paper.

References

Arup Kumar Bhaumik, Minkyu Choi, Rosslin J. Robles, and Maricel O. Balitanas (2009), Data Hiding in Video, *International Journal of Database Theory and Application*.

Joyshree Nath and Asoke Nath (2011), Advanced Steganography Algorithm using encrypted secret message, *International Journal of Advanced Computer Science and Application (IJACSA),*Vol.2 No.3.

Pratap Chandra Mandal (2012), Modern Stenographic technique: A survey, *International Journal of Computer Science & Engineering Technology (IJCSET).*

Pritish Bhautmage, Prof. Amutha Jeya kumar (2013), Advanced Video Steganography Algorithm, *International Journal of Engineering Research and Applications (IJERA*), Vol. 3, Issue 1.

Sushil Kumar, S.K. Muttoo (2013), A comparative study of image steganography in wavelet domain, *IJCSMC,* Vol. 2, Issue. 2.

Hemalatha, U Dinesh Acharya, Renuka (2013), comparison of secure and high Capacity color image steganography techniques in RGB and YCBR domains, *International Journal of Advanced Information Technology (IJAIT)* Vol. 3, No. 3.

Chandra Prakash Shukla, Mr. Ramneet S Chadha (2014), A Survey of Steganography Technique, Attacks and Applications, *International Journal of Advanced Research in Computer Science and Software Engineering,*Volume 4, Issue 2.