ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

Survey on Different Methods of Image Steganography

Palak R Patel, Yask Patel

Department of Computer Engineering, Parul Institute of Engineering & Technology (PIET), Limda, India

Assistant Professor, Dept. of I.T, Parul Institute of Engineering & Technology (PIET), Limda, India

ABSTRACT: With the rapid advance in digital network, digital libraries, and particularly WWW (World Wide Web) services, we can retrieve many kinds of images on personal and mobile computer anytime and anywhere. At the same time, secure image archiving is becoming a major research area because the serious concern is raised about copyright protection and authority identification in digital media. A more sophisticated technique is required for future multimedia copyright protection. Steganography is the idea of hiding private or sensitive data or information within something that appears to be nothing out of the normal. Steganography and cryptology are similar in the way that they both are used to protect important information. Nowadays the term "Information Hiding" relates to both watermarking and steganography. This paper intends to give an overview of image steganography and various techniques like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Least Significant Bit (LSB), Hash LSB and Spread Spectrum.

KEYWORDS: DCT(Discrete Cosine Transform), DWT(Discrete Wavelet Transform), LSB(Least Significant Bits), Hash LSB, Spread Spectrum

I. INTRODUCTION

With advancements in digital communication technology and the growth of computer power and storage, the difficulties in ensuring individuals privacy become increasingly challenging. The degrees to which individuals appreciate privacy differ from one person to another. Various methods have been investigated and developed to protect personal privacy. Encryption is probably the most obvious one, and then comes steganography [2]. Encryption lends itself to noise and is generally observed while steganography is not observable. The term steganography refers to the art of covert communications [1]. Steganography's aim is to make the secret communication undetectable, that is, to hide the presence of the secret message. It modifies the carrier in an imperceptible way only so that it reveals nothing neither the embedding of a message nor the embedded message itself. The recent development of the Internet has brought new attention to steganography. The interest in steganography has been enhanced recently by the emergence of commercial espionage and the growing concerns about homeland security due to terrorism.

Image steganography is the art of information hidden into cover image, Is the process of hiding secret message within another message. The word steganography in Greek means "Covered Writing". The information hiding process in a steganography with different techniques includes identifying cover mediums redundant bits. The embedding process creates a stego medium by replacing the redundant bits with data from the hidden message. During the process of hiding the information three factors must be considered that are ***capacity*** it includes amount of information that can be hidden in the cover medium. ***Security*** implies to detect hidden information and ***Robustness*** to the amount of modification the stego medium can withstand before an adversary can destroy hidden information [6].

Main objective of steganography is to communicate securely in such a way that the true message is not visible to the observer. Today steganography is mostly used on computer with digital data being the carriers and networks being the high speed delivery channel [5]. Using steganography a secret message is embedded inside a piece of unsuspicious information and sent without anyone knowing the existence of the secret message. Secrets can be hidden inside all sorts of cover information that is text, image, audio, video, etc. Most steganographic utilities hide information inside image,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

as it is relatively easy to implement images are mostly used in the process or of steganography because it is hard to break. [3]

This paper is organized as follow. In section II, we describe survey of different Steganography methods. In section III, we describe scope of research. In section IV, represents comparative analysis. In section V, represents conclusion and future work.

II. SURVEY OF DIFFERENT METHODS

A. Least Significant Bit Substitution Technique[9]

In LSB steganography, the least significant bits of the cover media's digital data are used to conceal the message. The simplest of the LSB steganography techniques is LSB replacement. LSB replacement steganography flips the last bit of each of the data values to reflect the message that needs to be hidden.

Consider an 8-bitgrayscale bitmap image where each pixel is stored as a byte representing a gray scale value. Suppose the first eight pixels of the original image have the following gray scale values [4]:
11010010
01001010
10010111
10001100
00010101
01010111
00100110
01000011
To hide the letter C whose binary value is 10000011, we would replace the LSBs of these pixels to have the following new grayscale values:
11010011
01001010
10010110
10001100
00010100
01010110
00100111
01000011

Note that, on average, only half the LSBs need to change. The difference between the cover (i.e. original) image and the stego image will be hardly noticeable to the human eye. However, one of its major limitations is small size of data which can be embedded in such type of images using only LSB. LSB is extremely vulnerable to attacks. LSB techniques implemented to 24 bit formats are difficult to detect contrary to 8 bit format [8].

B. Discrete Cosine Transform(DCT) [10]

DCT domain embedding techniques is the most popular one, mostly because of the fact that DCT based image format are widely available in public domain as well as the common output format of digital camera. JPEG image format for color components a discrete cosine transform (DCT) to transform successive 8 * 8 pixel block of the image into 64 DCT coefficients each. *The DCT coefficients F(u,v)* of an 8*8 block of pixel *f(x,y*) are given by

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

$$F(u,v) = \frac{1}{4}C(u)C(v)\left[\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y) * \cos\frac{(2x+1)u\pi}{16}\cos\frac{(2y+1)v\pi}{16}\right],$$

Where u= horizontal spatial frequency, v=vertical spatial frequency.
C(x)=1/√2 when x=0 and C (x)=1 otherwise.
Embedding in DCT domain is simply done by altering the DCT coefficients. For example by changing the least significant of each coefficient. The modification of a single DCT coefficient affects all image pixels.

C. Discrete Wavelet Transform (DWT) [11]

Discrete wavelet transform (DWT) is used to transform the image from its spatial domain into its frequency domain. We use DWT in the process of steganography so that we can clearly identify the high frequency and law frequency information of each pixel of the image.

To obtain the DWT of the cover image, a filter pair called the Analysis Filter pair is used. First, the low pass filter is applied to each row of data in order to get the low frequency components of the row. Since the LPF is a half band filter, the Output data needs to be sub-sampled by two, so that the output Data now contains only half the original number of samples. Next, the high pass filter is applied for the same row of data, and similarly the high pass components are separated, and placed by the side of the low pass components. This procedure is done for all rows. Again filtering is done for each column of the intermediate data. The resulting two-dimensional array of coefficients contains four bands of data, each labelled as LL (Low-Low), HL (High-Low), LH (Low High) and HH (High-High). The LL band can be decomposed once again in the same manner, thereby producing even more sub-bands.

D. Spread Spectrum [7]

In spread spectrum techniques, The message is spread over a wide frequency bandwidth than the minimum required bandwidth to send the information. This can be accomplished by adjusting the narrowband waveform with a wideband waveform, such as white noise. After spreading, the energy of the narrowband signal in any one frequency band is low and therefore difficult to detect [7]. In spread spectrum image steganography the message is embedded in noise and then combined with the cover image to produce the stego image. Since the power of the embedded signal is much lower than the power of the cover image, the embedded image is not perceptible to the human eye or by computer analysis without access to the original image [7].

E. Hash-Least significant Bits (Hash-LSB) [12]

The Hash based Least Significant Bit (H-LSB) technique for steganography in which position of LSB for hiding the secret data is determined using hash function. Hash function finds the positions of least significant bit of each RGB pixel's and then message bits are embedded into these RGB pixel's independently. Then hash function returns hash values according to the least significant bits present in RGB pixel values. The cover image will be broken down or fragmented into RGB format. Then the Hash LSB technique will uses the values given by hash function to embed or conceal the data. In this technique the secret message is converted into binary form as binary bits; each 8 bits at a time are embedded in least significant bits of RGB pixel values of cover image in the order of 3, 3, and 2 respectively. According to this method 3 bits are embedded in red pixel LSB, 3 bits are embedded in green pixel LSB and 2 bits are embedded in blue pixel LSB. These 8 bits are inserted in this order because the chromatic influence of blue color to the human eye is more than red and green colors. Therefore the distribution pattern chooses the 2 bits to be hidden in blue pixel. Thus the quality of the image will be not sacrificed.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

III. SCOPE OF DISSERTATION WORK

The scope of the study encompasses:

- The scope of the project is to limit unauthorized access and provide better security during message transmission**.**
- The proposed system for security of image for transmission would be very helpful in internet where large user sends images via mail, social networking sites.
- It has a vital role in defense as well as civil applications.
- This would also be beneficial in space technology where satellite sends images of planets preventing it from going in wrong hands.
- This would be beneficial to nation for over all security.

IV. COMPARATIVE ANALYSIS

TABLE 1 COMPARISION OF DIFFERENT METHODS

Method	Description	Advantage	Limitation
Least Significant Bit (LSB) substitution	Data hides in least significant bit of the pixel..	1.High Capacity 2.simple to Implement	It has low robustness and pros to some attacks like low-pass filtering and compression.
Discrete cosine transform	Data is embedded by changing the coefficient of transform of image.	1. Compression is used to reduce bandwidth hence it is achieved by using quantization techniques. 2. High security and PSNR.	Large amount of Data cannot be hiding means smaller embedding capacity.
Discrete wavelet transform	Discrete wavelet transforms (DWT), which transforms a discrete time signal to a discrete wavelet representation.	1.High capacity 2.high security and Robustness	1. The cost of computing DWT may be higher. 2. Low PSNR.
Spread Spectrum	In spread Spectrum techniques, hidden data is spread throughout the cover-image making it harder to detect	In channels with narrowband noise, increasing the transmitted signal bandwidth results in an increased probability that the information received will be correct.	1. Improving the embedded signal estimation process in order to lower the signal estimation BER. 2. Medium Robustness and PSNR.
Hash-LSB	Hash function is used to find position of LSB.	Very good MSE and PSNR.	1.low robustness

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

V. CONCLUSION AND FUTURE WORK

In this paper, we have carried out different methods of Steganography. And we have also done comparative analysis of different methods. From this analytical survey we have conclude that all method have advantages and limitations. The strong and weak points of these techniques are mentioned briefly so that researches who work in steganography gain prior knowledge in designing these techniques and their variants. The next plan is to develop a steganography technique that is robust to different types of attacks. and also work can be enhanced for other data file like audio, video and text. By this method we can achieve best completeness, correctness, quality, accuracy.

ACKNOWLEDGMENT

Thanking to Prof. G. B. Jethva, Head of Department in Master's In Information Technology Department, for his valuable knowledge and support and guiding us to the right path.

REFERENCES

[1] I. Cox, M. Miller, J. Bloom, J.Fridrich, and T. Keller. "Digital Watermarking and Steganography (Second Edition)", Morgan aufmann Publishers, ISBN: 978-0-12- 372585-1, 2007.
[2] Yambern Jina Chanu, ThemrichonTuithung, Kh. Manglem Singh "A Short Survey on Image Steganography and Steganalysis Techniques" IEEE-2012.
[3]Ge Huayong ,Huang ,"Steganography and Steganalysis Based on Digital Image", International conference & signal Processing-2011 IEEE.
[4] Vijay KumarSharma, Vishalshrivastava, "A Steganography Algorithm for Hiding Images by improved LSB substitution by minizedetection."journal of Theoretical and Applied Information Technology, Vol. 36 No.1, ISSN: 1992-8645, 15th February 2012.
[5] Amitava Nag, Sushanta Biswas,"A Novel Techniques for image steganography based on DWT and Huffman Encoading", IJCSS, Vol(4): issue(6).
[6] Hniels Provos & Peter Honeyman,"Hide & Seek : An Introduction to Steganography" IEEE Computer Society Pub-2003.
[7]Marvel, L.M., Boncelet Jr., C.G. & Retter, C.,"Spread SpectrumSteganography",IEEE Transactions on image processing, 8:08, 1999
[8]BeenishMehboob and Rashid Aziz Faruqui, "A Steganography Implementation", IEEE -4244-2427-6/08/$20.00 ©2008.
[9] Stuti Goel, Arun Rana, Manpreet Kaur," A Review of Comparison Techniques of Image Steganography",IOSR-JEEE vol(6):issue(1),may-june-2013.
[10]Prof.S.V.Kamble, ,Prof. B.G.Warvante, " A Review on Novel Image Steganography Techniques",IOSR-JCE-2004.
[11]Nadiya, P.V.; Imran, B.M., "Image steganography in DWT domain using double-stegging with RSA encryption," Signal Processing Image Processing & Pattern Recognition (ICSIPR), 2013 International Conference on , vol.7, no. 8, pp.283,287, Feb. 2013.
[12] Anil Kumar , Rohini Sharma," A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", International Journal of Advanced Research in Computer Science and Software Engineering on Vol.3 ,no.7, July 2013.

BIOGRAPHY

Palak R Patel is a student in the Computer Engineering Department, College of Parul Institute of Engineering and Technology, Limada,India. Research interests are Image processing, computer network, Wireless etc.