IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SURVEY ON DIFFERENT STEGANOGRAPHY TECHNIQUES

Tandel Bhavisha [*], Mr.Divyesh Joshi
Master of computer engineering, Parul Institute of Engineering and Technology, India

ABSTRACT

The paper describes short survey on different steganography techniques for an image in spatial and transform domains and steganalysis techniques for hide the secret message. The strong and weak points of these techniques are mentioned briefly so that researchers who work in steganography and steganalysis gain prior knowledge in designing these techniques and their variants. One can develop a better steganography technique by analyzing the contemporary steganalysis techniques.

KEYWORDS: Discrete wavelet transform (DWT), Discrete cosine transform(DCT), Integer wavelet transform(IWT), Least significant bits(LSB),Pixel value differencing(PVD),Gray level modification(GLM).

INTRODUCTION

Steganography is a process that hide the secret information or message into a cover media.Cover media can be a image or a audio or video file. There are two main steganography techniques: Spatial Domain and Transform Domain. Spatial – domain techniques embed messages in the intensity of the pixels directly, while for transform – also known as frequency – domain, images are first transformed and then the message is embedded in the image. Image domain techniques encompass bit-wise methods that apply bit insertion and noise manipulation and are sometimes characterized as “simple systems”.

The image formats that are most suitable for image domain steganography are lossless and the techniques are typically dependent on the image format. Steganography in the transform domain involves the manipulation of algorithms and image transforms. These methods hide messages in more significant areas of the cover image, making it more robust. Many transform domain methods are independent of the image format and the embedded message may survive conversion between lossy and lossless compression. In the next sections steganographic algorithms will be explained in categories according to image file formats and the domain in which they are performed.

STEGANOGRAPHY TECHNIQUES

Spatial Domain Steganographic Method

a) LSB Technique[3]

Steganography software hide information by replacing only the least significant bits (LSB) of an image with bits from the file that is to be hidden. One of the most common techniques used in steganography. The following example shows how the letter A can be hidden in the first eight bytes of three pixels in a 24-bit image.

Example of Lsb:

Pixels: (1010111**1** 11101001 10101000)

(1010011**1** 01011000 1110100**1**)

(11011000 10000111 01011001)

Secret message: 01000001

Result: (1010111**0** 11101001 10101000)

(1010011**0** 01011000 1110100**0**)

(11011000 10000111 01011001)

The three bold bits are the only three bits that were actually altered. Since the 8-bit letter A only requires eight bytes to hide it in, the ninth byte of the three pixels can be used to begin hiding the next character of the hidden message. A slight variation of this technique allows for embedding the message in two or more of the least significant bits per byte. This increases the hidden information capacity of the cover-object, but the cover-object is degraded more, and therefore it is more detectable.

B) **Gray level modification method**:[8]

- Gray level modification Steganography is a technique to map data (not embed or hide it) by modifying the gray level values of the image pixels. GLM Steganography uses the concept of odd and even numbers to map data within an image.
- A set of pixels are selected based on a mathematical function from a given pixel. The gray level values of those pixels are examined and compared with the bit stream that is to be mapped in the image.

C) **Data Hiding by PVD:[8]**

- The pixel-value differencing (PVD) method segments the cover image into non overlapping blocks containing two connecting pixels and modifies the pixel difference in each block (pair) for data embedding.
- This Steganography method is based on image layers. This method divides the host image into each block and embeds the corresponding secret message bits into each block using the layers which are made by binary representation of pixel values. It then performs a search on the rows and columns of the layers for finding the most similar row and columns of the layers for finding the most similar row or column. The location of row/column and its differences from secret message is then marked by modifying the minimum number of bits in the least significant bits of the blocks.[8]

TRANSFORM DOMAIN STEGANOGRAPHIC METHOD

A) DCT based Data Hiding[10]

- DCT coefficients are used for JPEG compression. It separates the image into parts of differing importance It can separate the image into high, middle and low frequency components.
- In low frequency sub-band, much of the signal energy lies at low frequency which contains most important visual parts of the image while in high frequency sub-band, high frequency components of the image are usually removed through compression and noise attacks .

B) Discrete Wavelet Transform Technique (DWT)[5]

- Scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighbouring pixels. Store the sum on the left and the difference on the right. Repeat this operation until all the rows are processed.
- The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image. Secondly, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighbouring pixels and then store the sum on the top and the difference on the bottom .
- Repeat this operation until all the columns are processed. Finally we will obtain4 sub-bands denoted as LL, HL, LH, and HH respectively.
- Integer wavelet transform has been derived from using lifting scheme. IWT results the coefficients in terms of integers. Therefore this transform is used for LSB based embedding.
- In general, Low Frequency (LF) and High Frequency (HF) components are generated by averaging and differencing methods respectively.

C) IWT (Integer wavelet transform):[1]

- Integer wavelet transform has been derived from using lifting scheme. IWT results the coefficients in terms of integers. Therefore this transform is used for LSB based embedding.
- In general, Low Frequency (LF) and High Frequency (HF) components are generated by averaging and differencing methods respectively.
- Haar wavelet transform is a basic wavelet transform among wavelet family. Integer wavelet transform has been derived using lifting scheme. IWT results the coefficients in terms of integers.
- Therefore this transform is used for LSB based embedding. In general, Low Frequency (LF) and High Frequency (HF) components are generated by averaging and differencing methods respectively. First level decomposition of an image gives Approximation (LL), Horizontal (LH), Vertical (HL) and Diagonal (HH) coefficients. LL coefficients are more sensitive than the remaining coefficients, so the embedding is done in all the sub bands except LL subband. Since LH, HL and HH coefficients contain edge information more information can be embedded in these coefficients.

CONCLUSION

The paper describes a short survey on different types of steganography techniques for image in spatial and transform domains and steganalysis techniques for the detection of secret message in the image in spatial domain. The strong and weak points of these techniques are mentioned briefly so that researches who work in steganography and steganalysis 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 the majority of contemporary staganlysis techniques fail to detect the presence of secret messages.

REFERENCES

1. Thanikaiselvan V, Arulmozhivarman P," High Security Image Steganography Using IWT and Graph Theory" IEEE International Conference on Signal and Image Processing Applications (lCSIPA),2013.
2. S. Saejang, A. Boondee, J.Preechasuk, C.Chantrapornchai," On The comparison of digital image steganography algorithm based on DCT and Wavelet" IEEE International Computer Science and Engineering Conference (ICSEC),2013
3. Rajib Biswas, Sayantan Mukherjee, Samir Kumar Bandyopadhyay, "DCT Domain Encryption in LSB Steganography" IEEE 5th International Conference on Computational Intelligence and Communication Networks,2013.
4. Hemalatha S, U. Dinesh Acharya, Renuka A, Priya R Kamath," A Secure Image Steganography Technique Using Integer Wavelet Transform" IEEE 2012. 5.
5. Anjali A. Shejul, Prof. U.L Kulkarni, "A DWT based Approach for Steganography Using Biometrics" IEEE International Conference on Data Storage and Data Engineering,2010.
6. Hui-Yu Huang, Shih-Hsu Chang, "A 9/7 wavelet-based lossless data hiding" IEEE Department of Computer Science and Information Science,2011.
7. K B Shiva Kumar, Khasim T, K B Raja, Sabyasachi Pattnaik, R K Chhotaray," Dual Transform Technique for Robust Steganography" IEEE International Conference on Computational Intelligence and Communication Systems,2011.
8. Yam bern Jina Chanu, ThemrichonTuithung, Kh. Manglem Singh" A Short Survey on Image Steganography and Steganalysis Techniques" IEEE 2012.
9. Prabakaran. G, Bhavani.R" A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform" IEEE International Conference on Computing, Electronics and Electrical Technologies [ICCEET],2012.
10. K.B.Shiva Kumar, K.B.Raja, R.K.Chhotaray, Sabyasachi Pattnaik," Coherent Steganography using Segmentation and DCT" IEEE 2010.
11. Neda Raftari and Amir Masoud Eftekhari Moghadam, "digital image Steganography based on Assignment Algorithm and Combination of DCT-IWT" IEEE Fourth International Conference on Computational Intelligence, Communication Systems and Networks,2012.
12. Xianhua Song ,Shen Wang, Xiamu Niu" An Integer DCT and Affine Transformation Based Image Steganography Method" IEEE Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing,2012.
13. A K Singh, M Dave, Anand Mohan" Performance Comparison of Wavelet Filters against Signal Processing Attacks" IEEE Second International Conference on Image Information Processing (ICIIP-2013)
14. Prahalad Saha y Ghasal, Prakriti Trivedi, Anjali Chandwani,Madan Lal Tetrawal,Abhinash Jha,Ayush Kumar," Payload Minion Stenographic Technique for Color Images" IEEE 2014 International Conference on Reliability, Optimization and Information Technology -ICROIT 2014, India, Feb 6-8 2014.
15. Neha Gupta, Ms. Nidhi Sharma" Dwt and Lsb Based Audio Steganography" IEEE International Conference on Reliability, Optimization and Information Technology -ICROIT 2014, India, Feb 6-8 2014.
16. Satish Singh Verma, Ravindra Gupta, Gaurav Shrivastava" A Novel Technique for Data Hiding in Audio Carrierby Using Sample Comparison in DWT Domain"

IEEE Fourth International Conference on Communication Systems and Network Technologies,2014.

17. Prabakaran G, Dr. Bhavani R, Sankaran S, “Dual Wavelet Transform in Color Image Steganography Method” IEEE International Conference on Electronics and Communication System,2014.