Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.904 – 909

SURVEY ARTICLE

Literature Survey on DWT Based Image Steganography

[1]Mrs. Suvarna Patil, [2]Mr. Gajendra Singh Chandel

[1,2]IT Department & RGPV University

[1] patilsuvarna555@gmail.com, [2] hodcsit.sssist@yahoo.com

Abstract- Steganography is the science of secure communication which has received much attention from the scientific community recently. The four main objectives of steganography are: Indefectibility, Security, embedding payload, and Robustness. However, steganography can protect data by hiding it in a cover object but using it alone may not guarantee total security. Thus, the use of encryption in steganography can lead to 'security in depth'. It is the science of embedding information into the cover image viz., text, video, and image (payload) without causing statistically significant changes to the cover image. The advanced secure image steganography presents a challenging task of transferring the embedded information to the destination without being detected .This paper provides a state-of-the-art review and analysis of the different existing methods of steganography along with some common standards and guidelines drawn from the literature.

Introduction

Steganography is the art of hiding and sending data through apparently innocuous carriers in an effort to conceal the existence of the information, the word Steganography literally means covered or hiding writing as derived from Greek language. Steganography has its place in security and privacy. It is not intended to replace cryptography but enhance it. Hiding a message with Steganography methods decreases the chance of a message being detected. If the

message is encrypted then it provides another layer of protection .Therefore, some Steganography methods combine traditional Cryptography with Steganography; the sender encrypts the secret message prior to the overall communication process, as it is very difficult for an attacker to detect embedded cipher text in a cover .In the field of Steganography, some terminology has developed. The adjectives 'cover', 'embedded', and 'stego' were defined at the information hiding workshop held in Cambridge, England. The term "cover" refers to description of the original massage, data, audio, video, and so on. Steganography isn't a new science; it dates back to past times. It has been used through the ages by ordinary people, spies, rulers, government, and armies. Hidden information in the cover data is known as the "embedded" data and information hiding is a general term encompassing many sub disciplines, is a term around a wide range of difficulties beyond that of embedding message in content. The word hiding here can refer to either making the data not detectable or keeping the existence of the information secret. Data hiding is a technique of hiding secret using cover data such as images, audios, movies, documents, etc. This technique has currently become important in a number of application areas. For example, video, audio, and images are embedded with indefectible marks, which may contain hidden signatures or watermarks that help to prevent not authorized copy. It's a performance that inserts secret messages into a cover file, so that the presence of the messages is unapparent. Research in information hiding has tremendous enhanced during the past decade with commercial interests driving the field.

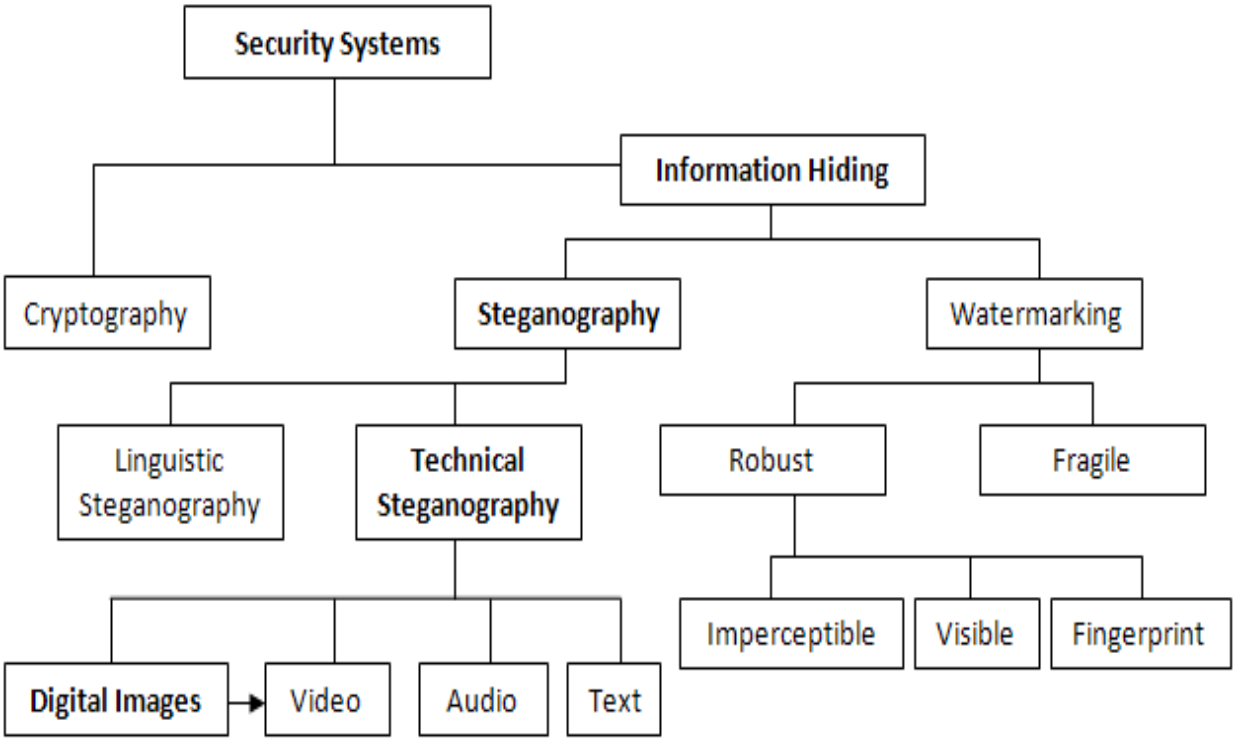

Fig. 1.The different embodiment disciplines of information hiding. The arrow indicates an extension and bold face indicates the focus of this study

Table 1. Comparison of steganography, watermarking and encryption.

Criterion/Method	Steganography	Watermarking	Encryption
Carrier	any digital media	mostly image/audio files	usually text based, with some extensions to image files
Secret data	payload	watermark	plain text
Key	optional		necessary
Input files	at least two unless in self-embedding		one
Detection	blind	usually informative (i.e., original cover or watermark is needed for recovery)	blind
Authentication	full retrieval of data	usually achieved by cross correlation	full retrieval of data
Objective	secrete communication	copyright preserving	data protection
Result	stego-file	watermarked-file	cipher-text
Concern	delectability/ capacity	robustness	robustness
Type of attacks	steganalysis	image processing	cryptanalysis
Visibility	never	sometimes (see Fig. 2)	always
Fails when	it is detected	it is removed/replaced	de-ciphered
Relation to cover	not necessarily related to the cover. The message is more important than the cover.	usually becomes an attribute of the cover image. The cover is more important than the message.	N/A
Flexibility	free to choose any suitable cover	cover choice is restricted	N/A
History	very ancient except its digital version	modern era	modern era

DWT Based Steganography

This is another frequency domain in which steganography can be implemented. CT is calculated on blocks of independent pixels, a coding error causes discontinuity between blocks resulting in annoying blocking artifact. This drawback of DCT is removed using DWT. DWT applies on entire image. DWT offers better energy compaction than DCT without any blocking artifact. DWT divide component into numerous frequency bands called sub bands known as

LL – Horizontally and vertically low pass
LH – Horizontally low pass and vertically highpass
HL - Horizontally high pass and vertically lowpass
HH - Horizontally and vertically high pass

Since Human eyes are more sensitive to the low frequency part (LL sub band) we can hide secret message in other 3 parts without making any alteration in LL sub band. As other three sub-bands are high frequency sub-band they contain insignificant information. Hiding secret data in these sub-bands does not degrade image quality that much. DWT used in this work is Haar-DWT, the simplest type of DWT.

Algorithm to DWT retrieve secrete data:-Step 1: Scan the cover image and secret data which is to be hidden in the cover image. Step 2: translate the secret data into binary. Apply 2D-Haar transform on the cover image. Step 3: Access the horizontal and vertical filtering coefficients of the cover image. Cover image is inserted with data bits for DWT coefficients. Step 4: Obtain stego image. Step 5: Compute the Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego image.

Algorithm of DWT to retrieve secret data:-Step 1: Scan the stego image. Step 2: Achieve the horizontal and vertical filtering coefficients of the cover image. Extraction of the secret data bit by bit and recomposing the cover image. Step 4: Translate the data into message vector and compare it with original data.

Literature Survey

Most of the published articles are concerned with the description of some software tools designed and built to perform Steganography on some text, image, and audio cover media. The publication about the scheme of the stego system is more primitive, and mostly does not offer a key solution for some weak aspects which may face the discussed system. Among the large number of published articles, this section shows the current researches being done, in comparison with this research:

LIU Tong and QIU Zheng-ding [1] and Vladimir Banoci*et al*. proposed a DWT based color image steganography method. In the former method the secret information is hidden into a publicly accessed color image by a quantization-based strategy. Whereas, the latter case method processes grey scale images as cover object for creating subliminal channel and it utilizes transform coefficients of 2-Dimensional Discrete transform for embedding process. Johri and Asthana [2] proposed steganography and its implementation techniques. Deshpande Neeta,[3] et. al. proposed the Least Significant Bit embedding technique suggests that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. Ali Al-Ataby, [4] proposed a modified high-capacity image steganography technique that depends on wavelet transform with acceptable levels of imperceptibility and distortion in the cover image and high level of overall security. T. Narasimmalou[5] Proposed a new image data hiding technique based on discrete wavelet transform . The stego-image is looking perfectly intact and has high peak signal to noise ratio value. Hence, an unintended observer will not be aware of the very existence of the secret-image. The extracted secret image is perceptually similar to the original secret image. In this paper two different techniques namely 1. using three level discrete wavelet transform and 2. using single level discrete wavelet transform for hiding images has been proposed and implemented.. The relative analysis between the proposed technique and the other existing techniques has shown the pre-eminence of the proposed technique. H.J .Patel and Dave [6] have proposed a new variant of LSB based image steganography. In this, both the parties will have to agree upon a set of carrier images and certain required parameters. Then the sender will select an image, from the set of carrier images which requires least number of bit manipulations on LSB substitution of secret data, and produce stegoimage. Then the receiver on receiving stegoimage will extract LSBs along with the help of the received parameters. The probability of guessing parameters is very less. So extraction without those parameters is very difficult. Here since both the parties agree upon a set of carrier images the visual difference between stegoimage and original image can be reduced. T. Narasimmalou[7], .Proposed an optimal discrete wavelet transform (DWT) based steganography. Experiments represent that the peak signal noise ratio (PSNR) generated by the proposed method is better. Ashok Kumar [8] proposed biometric steganography that uses skin region of images in DWT domain for embedding secret data. By embedding data in only specific region (here skin region) and not in whole image security is enhanced. Also image cropping concept introduced which maintains security at respectable level since no one can extract message without having value of cropped region. Features

obtained from DWT coefficients are utilized for secret data embedding. This also increases the quality of stego because secret messages are embedded in high frequency sub-bands which human eyes are less sensitive to. Swati and Mahajan [9] proposed a secure image steganographic model using RSA algorithm and LSB insertion. In this method, the secret data is first encrypted using recipient's RSA public key. Then each bit of the encrypted message is inserted to the LSBs of image in different images so as to find the best cover image. Best cover image is the one which requires minimum number of LSB extract the message in the encrypted form and will decrypt it using private key. Stuti Goel[10] proposed the performance and comparison of three techniques DCT,LSB &DWT is evaluated on the basis of the parameters MSE, PSNR, Capacity & Robustness. From the results, it is clear that PSNR of DCT is high as compared to the other two techniques. This implies that DCT provides best quality of the image. DWT is a highly robust method in which the image is not destroyed on extracting the message hidden in it and provides maximum security.

Conclusion

This paper has surveyed various different schemes that are used for collective behavior prediction. Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and recipient, suspects the existence of the message. DWT is a highly robust method in which the image is not destroyed on extracting the message hidden in it and provides maximum security. In this paper, the more importance is given on the secrecy as well as the privacy of all information. The embedding process is hidden under the transformation (DWT and IDWT) of cover image. These operations provide sufficient secrecy. After comparison it is found that in our paper PSNR is higher than the mentioned paper. Data embedding using a DWT to improve data hiding capacity & retain good stego image quality.

References

[1] T. Liu and Z. Qiu, "A DWT-Based Color Image Steganography Scheme," in *Proc. IEEE, 6th International Conference on Signal Processing*, 2002, vol. 2, pp. 1568-1571.

[2] J.R. Krenn, "Steganography and Steganalysis", January 2004.

[3] Deshpande Neeta, KamalapurSnehal, Daisy Jacobs, "Implementation of LSB Steganography and Its Evaluation for Various Bits", 2004.

[4] Ali Al-Ataby and Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform". The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.

[5] T. Narasimmalou, Allen Joseph .R, "Optimized Discrete Wavelet Transform based Steganography" , IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT),2012.

[6] H. J. Patel and P. K. Dave, "Least Significant Bits Based Steganography Technique," in *Proc. IJECCE 2012*, vol. 3, pp. 97-103.

[7] T. Narasimmalou, Allen Joseph .R " Discrete Wavelet Transform Based Steganography for Transmitting Images". IEEE-International Conference On Advances In Engineering, Science And Management (lCAESM -2012) March 30, 31, 2012 370.

[8] BY ASHOK KUMAR BALIJEPALLI & L.SRINIVAS, NIET,KANTEPUDI. "steganography based secrete communication using dwt **"** International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 5, July - 2012
ISSN: 2278-0181.

[9]S. Tiwari, R. P. Mahajan, and N. Shrivastava, "Steganography-an Approach for Data Hiding Based on Encryption and Lsb Insertion,"
IJECCE, vol. 3, pp. 76-83, 2012.

[10] Stuti Goel,2Arun Rana,3Manpreet Kaur," A Review of Comparison Techniques of Image Steganography". IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 6, Issue 1 (May. - Jun. 2013), PP 41-48.

