A Review Paper of Dual Steganography Technique Using Status LSB and DWT Algorithms

Manisha[#1]
[#1]M Tech Scholar, Dept. of Computer Science & Engineering
BSAITM, M.D.U. Rohtak
Faridabad, India
[#1]mittalmanisha1301@gmail.com

Deepkiran Munjal[*2]
[*2]Assistant Professor, Dept. of Computer Science & Engineering
BSAITM, M.D.U. Rohtak
Faridabad, India
[*2] deepkiran.munjal@faculty.anangpuria.com

Abstract-**In this paper the focus is on maintaining secrecy between two communication parties using dual steganography technique. In dual steganography secret message is first embedded in to cover image by using LSB (Least Significant Bits) algorithm and then resulted embedded image will be again embedded in to another cover image by using DWT (Discrete Wavelets Transform) algorithm to form Stego-image. The DWT (Discrete Wavelets Transform) algorithm is found to be better in the terms of efficiency, robustness, highly security and embedding capacity. With rapid growth of World Wide Web and advance computer network, we need security, privacy, integrity and authentication in the data communication. A steganography is art of hiding sensitive information in another cover medium. The main objective of this paper is to achieve embedding capacity, quality and secure communication.**
Keywords-Dual Steganography ; Image Steganography; Status LSB; DWT.

I. INTRODUCTION

In today's world the data communication is the basic need of every growing area. Each and every person wants a robust, secure and high capacity steganography technique for maintaining secrecy and safety of their communicating data. The organizations such as internet banking, e-commerce, diplomacy and medicine, private communications are essential .Thus it has increased the need of storing large amounts of data and their security. In order to share the information in secret manner two techniques could be used which are cryptography and steganography. In cryptography the message is converted into encrypted form of the help of encryption key which is known to sender and receiver only. However, the transmission of encrypted message is not safe because the encrypted message may easily arouse attacker's suspicion and may be intercepted or attacked easily. In order to remove these short comings of cryptographic techniques, steganography techniques have been developed. Steganography is defined as the technique that deals with the study of secure and secret communication. "Steganography" is a Greek word which means "hiding writing". Steganography word is the combination of two parts: Steganos which means "secret" and Graphic which means "writing". Steganography is defined as the process of hiding sensitive information on any multimedia cover like image, audio, video and protocol etc in a such way that unauthorized person can't be recognized the existing of sensitive information in to the cover media. The data that to be hidden is called Stego and the cover media in which data to be hidden is called host. The main different between in cryptography and steganography is ,cryptography protect the contents of the message while steganography hides the fact that a secret message is being sent as well as to hide the contents of the message.

Dual steganography is the security mechanism in which steganography and cryptography are used together. To achieve the goal of high security use the new version of dual steganography using the two LSB (Least Significant Bits) algorithm and DWT (Discrete Wavelets Transform) algorithm together. In this new version of dual steganography uses steganography within steganography. In this secret data is embedded in cover image using the

status LSB (Least Significant Bits) embedding algorithm and generate a stego-image .Next stego-image is considered as a secret data and embedded in other cover image using the DWT (Discrete Wavelets Transforms) embedding algorithm which is created a final stego –image. A dual steganography combined with two algorithms will be a powerful and efficient tool for data security. In this paper we use discrete wavelets transforms (DWT) that identify the high and low frequency information of each pixel of the image.

Section A and B presents the data hiding and data extraction process for the proposed scheme. Block diagram for Data Embedding process and Data Extraction Process are shown in Figure1 and Figure 2.

A. Data Embedding Process:

The Block diagram for the data embedding process is shown in figure 1. In this two cover images are used i.e. cover image1 and cover image2 as shown in Figure 1. The secret data is embedded inside the cover image1 with the help of status LSB (Least Significant Bits) embedding algorithm and generated a stego image1. Next the stego image1 is considered as the secret data and embedded inside other cover image2 by using the DWT (Discrete Wavelet Transform) embedding algorithm which is generated a final stego image.

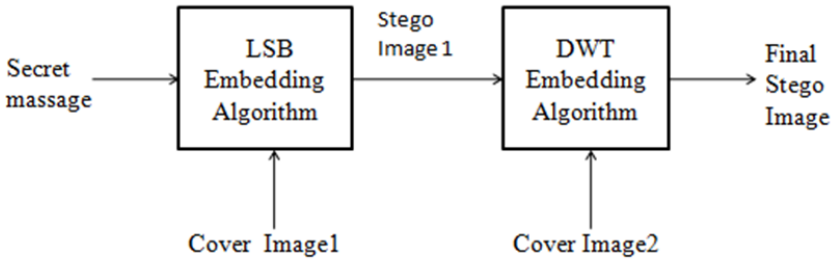

Figure 1.Data Embedding Process

B. Data Extraction Process:

The Block diagram for the data extraction process is shown in figure2. In this stego image1 is extracted from a final stego image by using the DWT (Discrete Wavelet Transform) extraction algorithm. Next, secret data is extracted from stego image1 by using LSB extraction algorithm.

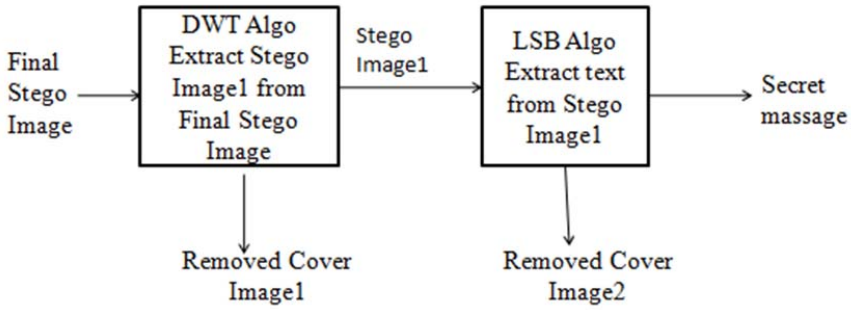

Figure 2.Data Extraction Process

A. Types of Steganography

1. *Text Steganography*: The commonest type of steganography in which a secret message is to be hidden in to a text file in such a way that secret message is hidden in every n letter of every word of the text file. This type of steganography is not widely used because text files have a very small amount of excess data.

2. *Image Steganography*: The type in which secret message is to be hidden in an image by using an embedding algorithm. Images are used as the most popular cover medium for digital steganography because of a large amount of bits is contained in a digital image.

3. *Audio Steganography*: In this type secret message is embedded with in a speech in wav, Au, MP3 format. This type of steganography is less popular than image because of large size of audio files.
.
4. *Video Steganography*: In this technique video is used as the cover medium for hiding the secret message. It hides the data in each image frame of the video in H.264, MP4, MPEG and AVI format.

5. *Protocol Steganography*: This is a technique of hiding the secret data within the network protocols such as TCP/IP, UDP, ICMP, IP etc.

B. Steganography Techniques

1. *Spatial Domain methods*: These methods directly changed some bits in the image pixel values of hiding data. There are various spatial domain methods such as (i) Least significant bits(LSB) ,(ii) Pixel values differencing (PVD),(iii) Edges based data embedding method(EBE),(iv) Pixel intensity based.LSB is the most simple and effective method that replaces a secret message bits with the LSB of each pixel values of the cover medium.

2. *Transform Domain techniques*: In this technique, the secret data is embedded in the transform or frequency domains of the cover file .In this many different algorithms and transformations are used for hiding information in an image. This technique is more robust and complex as compared to the spatial domain methods. There are some transform domain techniques such as (i) Discrete Fourier transformation technique (DFT), (ii) Discrete cosine transformation technique (DCT), (iii) Discrete wavelet transformation technique (DWT).

3. *Masking and Filtering*: The technique in which secret data is hidden in the more significant areas by marking an image. This method is more robust than LSB method. The main drawback of this technique is that this method can be applied only to gray scale images and 24 bits images.

C. Characteristics Feature of Dual steganography

1. *Payload Capacity*: It means how much information can be embedded in the cover medium. Payload capacity of secret files is depending on the number of pixels of cover image.

2. *Robustness*: It means that the secret message can't be destroyed after embedding and extraction process of an image or stego image.

3. *Imperceptibility*: After hiding the secret message in the cover medium, one should not be suspicious of the existence of the secret message within the cover medium.

4. *Accurate & Reliable*: The extraction of the secret message from the cover medium should be accurate and reliable.

5. *Peak signal to noise ratio (PSNR)*: The ratio that is used to measures the quality between the original and a compressed image. IF PSNR ratio is high then will be better quality of an image.

6. *Mean square error (MSE*): It represents the total error in the received data when it is compared to the data before and after processing. The small value of MSE will be represented more efficient image steganography technique.

II. LITERATURE SURVEY

There are lots of methods available that can be used to implement steganography using various algorithms.

S.K Muttoo et. al., [2] proposed a reversible image steganographic embedding algorithm. They used DD DT DWT in place of DWT as they provide better perceptibility and high capacity.

Souvik Bhattacharyya et.al., [6] proposed a robust image steganography using DWT difference modulation.They have embedded secret data in adjacent DWT coefficient differences. This technique can avoid various image attacks and works perfectly well for both uncompressed and compressed domains.

Barnali Gupta Banik et. al.,[8] proposed a DWT method for image steganography. This method maintains secrecy objects of steganography.

S.Jayasudha [7] proposed integer wavelet transforms based steganography method using OPA algorithm.This technique provides high hidden capacity and image quality.

Preeti chaturvedi et.al.,[10] proposed an integer wavelet transform based steganography technique. The system combines a data hiding technique and the optimum pixel adjustment algorithm to increase the hiding capacity of the system and minimize the error difference between original coefficient and modified values.

Preeti Arora et.al., [12] proposed a steganography method using integer wavelet transform and genetic algorithm. This paper proposed work is to develop RS –analysis proof design with highest imperceptibility.

Nikita Sharama et.al.,[16] proposed a novel approach to image steganography .They have used two techniques hash-LSB with RSA Algorithm and DWT technique for highly secure and robust image steganography.

Navneet choudhary et,al.,[15] proposed a approach to reduce distance error between cover and stego image. They have used frequency domains to increase the robustness.This method to improve image quality and hiding capacity with low distortion.

III. FUTURE SCOPE

In this modern eras of technology with the increase in need of secure and robust communication for military ,intelligence agencies, internet banking etc, the information technology sector looks towards the future research in the field of dual steganography. Some future researches may include:

1. Developing a system by combining the benefits of both audio and image steganography.
2. Focusing on other methods like audio, video, etc to hide the secret data.
3. Developing an environment which should be platform independent.
4. Use of best algorithms to achieve high efficiency, robustness and embedding capacity for secure.
5. Combining the concepts of hybrid cryptography and audio steganography to provide more security.

IV. CONCLUSION

This paper presents a good understanding of two popular information security techniques namely cryptography and steganography. Although both of these techniques provide security for secure information but separately one can't guarantee for absolute security of data. This paper gives a review of the research and developments in the field of steganography. Therefore in order to provide more security a novel advance technique for data security is required. In this paper dual steganography provides more security against several hacker attacks.

REFERENCES

[1] Po-Yueh Chen and Hung-Ju Lin,"*A DWT Based Approach for Image Steganography* ", International Journal of Applied Science and Engineering, (2006).

[2] S.K.Muttoo and Sushil Kumar," *A Multilayered Secure, Robust and High Capacity Image Steganographic Algorithm*", World of Computer Science and Information Technology Journal (WCSIT), Vol. 1, No. 6, (2011), Delhi, India.

[3] Jayaram, Ranganatha and Anupama," *Information Hiding Using Audio Steganography– A Survey*", The International Journal of Multimedia & Its Applications (IJMA), Vol.3, No.3, August (2011) Bangalore, INDIA.

[4] K.P.Adhiya and Swati A. Patil," *Hiding Text in Audio Using LSB Based Steganography* ", Information and Knowledge Management, Vol 2, No.3, (2012), Bambhori, India.

[5] Atallah M. Al-Shatnawi,"*A New Method in Image Steganography with Improved Image Quality*", Applied Mathematical Sciences, Vol. 6, (2012) and no. 79.

[6] Souvik Bhattacharyya, and Gautam Sanyal,"*A Robust Image Steganography using DWT Difference Modulation (DWTDM)* ", I. J. Computer Network and Information Security, (2012), West Bengal, India.

[7] S.Jayasudha," *Integer Wavelet Transform Based Steganographic Method Using Opa Algorithm*", International Journal of Engineering and Science, Vol.2, (February 2013).

[8] Barnali Gupta Banik and Samir K. Bandyopadhyay," *A DWT Method for Image Steganography* ", International Journal of Advanced Research in Computer Science and Software Engineering, Vol-3, Issue 6, June (2013).

[9] Krati vyas and B.L.Pal,"*A Proposed Method In Image Steganography To Improve Image Quality With LSB Technique*",International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 1, January (2014),Chittorgarh, India.

[10] Preeti Chaturvedi and R. K. Bairwa, "*An Integer Wavelet Transform Based Steganography Technique for Concealing Data in Colored Images*" International Journal of Recent Research and Review, Vol. VII, Issue 1, March (2014), Jaipur, India.
[11] Jasleen Kour and Deepankar Verma," *Steganography Techniques*", International Journal of Emerging Research in Management &Technology, Volume-3, Issue-5,may (2014), India.
[12] Preeti Arora, Anupam Agarwal and Jyoti," *A Steganographic Method Based on Integer Wavelet Transform & Genatic Algorithm*", Journal of Engineering Research and Applications, Vol. 4, Issue 5(Version 4), May (2014), Rajasthan, India.
[13] Ketki Thakre and Nehal Chitaliya, "*Dual Image Steganography for Communicating High Security*", Information International Journal of Soft Computing and Engineering, Vol-4, Issue-3 July (2014).
[14] R. Rejani1, D. Murugan2 and Deepu V. Krishnan3," *Pixel Pattern Based Steganography ON Image", ICTACT JOURNAL ON IMAGE AND VIDEO PROCESSING*", Feb (2015), VOLUME: 05, ISSUE: 03, India.
[15] Navneet Choudhary and RIA Gandhi, *"A Review of Different Approach to Reduce Distance Error between Cover and Stego Image*", International Journal of Emerging Research in Management &Technology, Vol-4, Issue-8, august 2015, Punjab, India.
[16] Nikita Sharma and Meha Khera," *A Novel Approach to Image Steganography Using Hash-LSB and DWT Technique*", International Journal of Advanced Research in Computer Science and Software Engineering, Vol- 5, Issue 6, June (2015), Haryana, India.