ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 4, Issue 6, June 2015

Image with Secret Message Embedded in Audio File by DWT: Compressed, Transmitted and Recovered

Anjali K B, Vishnu Prabha N Kaimal

***Abstract*— the best known method for securing data, which is a major challenge in today's rapidly changing technological world, is Steganography. Steganography, being a branch of Security System, is a method of embedding the data to be hidden in digital mediums. Transparency, Capacity and Robustness are the three major parameters that distinguish the steganographic algorithms. Samples comparison in DWT domain base audio steganographic algorithm that offers a very good capacity and quality for stego signal is being laid out. Here the secret message converted to image is embedded in the audio file and resultant audio stego file is compressed and transmitted. The image is then recovered from the received stego file. The strength of the algorithm, which depends on segment size, helps to attain considerable SNR and high capacity in embedding.**

***Index Terms*—Embedding, DWT, Security System, Steganography, Stego Signal.**

I. INTRODUCTION

Interception is the major threat faced by long distance communication. Security system in communication should thus be designed in a way to safeguard privacy and data integrity. Traditional or classic cryptography that hides the meaning of the message does not come handy in many situations and the very occurrence of communication must be made hidden. These requirements along with other reasons lead to the extensive development in the field of information hiding. The process of concealing details of an object or function is called information hiding. It is a branch of security system in communication and the latter can be classified as provided in Figure 1.

Often, there is a misconception that steganography and watermarking are same. We should understand that they are different methods though there seems to be a slight similarity in overall concept. When undetectability to human senses becomes the major concern in steganographic algorithms, watermarking mainly focuses on maintaining robustness.

Manuscript received Jun 02, 2015.
***Anjali K B**, Department of ECE, Nehru College of Engineering and Research center, Thrissur, India.*
***Vishnu Prabha N Kaimal**, Department of ECE, Nehru College of Engineering and Research center, Thrissur, India.*

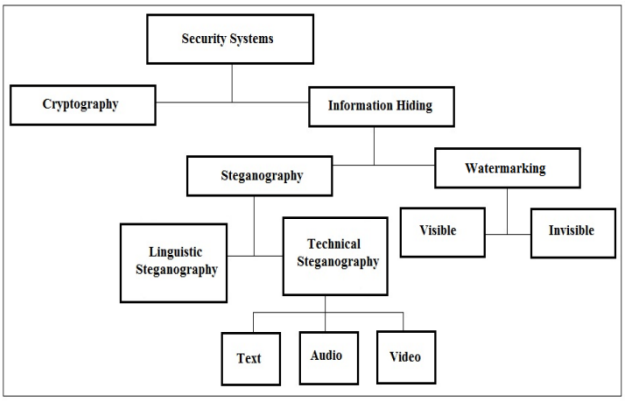

Figure 1: Classification of Security System

Table I: Comparison- Steganography and Watermarking

Criterion / Method	Steganography	Watermarking
Carrier	Any digital data	Mostly image / audio files
Secret Data	Payload	Watermark
Detection	Blind	Usually informative
Objective	Secret communication	Copyright preserving
Result	Stego file	Watermarked file
Concern	Detectability and Capacity	Robustness
Types of Attacks	Steganalysis	Image processing
Visibility	Never	Sometimes
Relation to Cover	Message is important Not necessarily related to cover.	Cover is more important. Usually attribute of cover.
Flexibility	Free to choose cover	Choice is restricted
History	Ancient except digital version	Modern era

Steganography is best interpreted as the art of 'concealed

communication', i.e. existence of secret message is made undetectable by hiding and sending the same using apparently innocuous and consistent carriers or cover. The Greek words 'steganos' means 'covered' and 'graphei' means 'writing' which when combined forms 'steganography' that indicates 'covered writing'. Steganography and watermarking are the classification or branches of the field of information hiding. When undetectability to human senses becomes the major concern in steganographic algorithms, watermarking mainly focuses on maintaining robustness. Quality of the steganographic algorithm can be traced by analyzing the three parameters, namely, Payload Capacity, Transparency and Robustness. A number of techniques have been established so far in order to successfully hide the secret information, namely, LSB Encoding, Phase Coding, Parity Coding, Echo Hiding and Spread Spectrum Techniques.

The 'cover signal' in steganographic process refers to the digital signal or medium where the secret information is hidden. The method of steganography can thus be classified according to the digital signal or medium used in the form of cover signal. It includes Image, Audio and Video steganography. Among them, audio steganography possess number of merits such as audio file makes a harmless file of exchange and the payload capacity is very high so that more secret data can be embedded in to the audio cover file. Here the secret message converted to image is embedded in the audio file and resultant file is called 'stego file' which is compressed and transmitted. The image is then recovered from the received stego file.

II. DWT & IDWT

Processing techniques in audio signal processing is customized by the usage of different transformation domains. Wavelet Transformation is one such domain in which different resolutions are used to analyse the signal with distinct frequencies i.e. in contrast to Short Time Fourier Transform (STFT), WT behaves differently with distinct frequencies. WT propose a technique that includes low time resolution and high frequency resolution for low frequencies and vice versa for high frequencies. Equation (1) and (2) can be used to determine the coefficients of WT.

$$W_\psi(a, b) = \int_{-\infty}^{\infty} f(t)\, \psi^*_{a,b}(t)\, dt \quad \text{----- (1)}$$

$$\psi_{a,b}(t) = a^{-1/2}\, \psi(t-b/a) \quad \text{----- (2)}$$

Where 'a' is the scale or dilation parameter and 'b' is the shift or translation parameter. WT can be classified in to three types, namely, Continuous WT (CWT), Semi-discrete WT and Discrete WT (DWT). The vital and worthwhile WT when dealing with audio signals is DWT since we can recover the audio signal from the discrete coefficients or values. In case of DWT, there is no need to have all the values of the function on the time axis for calculating the WT of the function at some point in time scale plane. We need to have only those values of function where the wavelet is nonzero. Therefore, computation of WT can be done on real time basis.

The notable feature of DWT is its time variant property. This means that the original function's DWT and the DWT of its time shifted version are quite different from each other. Equation (3) provides DWT of a function with dilation parameter, 'a = 2^{-k}' and the translation parameter, 'b = $j2^{-k}$'. DWT when applied to an audio signal provides two sets of coefficients, namely, the low frequency coefficients or approximate coefficients and high frequency coefficients or detailed coefficients.

$$W\psi(2^{-k}, j2^{-k}) = 2^{k/2} \Sigma_n f(n)\, \psi(2^k n - j) \quad \text{----- (3)}$$

While analysis of the audio signal, according to the application, the approximate coefficients or the low frequency part may be decomposed further in to another set of low and high frequencies. The embedding process can be done by carefully choosing one of detail coefficient from obtained set of coefficients. Also, the Inverse Discrete Wavelet Transform (IDWT) can be used to reconstruct the original audio signal from the decomposed coefficients. Equation (4) is used to carry out IDWT.

$$f(n) = \Sigma_k \Sigma_l W\psi(2^{-k}, j2^{-k})\, 2^{-k/2}\, \psi(2^{-k} n - j) \quad \text{----- (4)}$$

Here, in the DWT process, we use the wavelet named 'Haar Wavelet'. The major advantage while using Haar wavelet in audio signal is that it is the simplest possible wavelet. It has a technical disadvantage of not being continuous and thus not differentiable, which become an advantage while analyzing the signals with sudden transitions like audio signal. Equation (5) shows the Haar wavelet.

$$\psi(t) = \begin{cases} 1; & 0 \le t \le \tfrac{1}{2} \\ -1; & \tfrac{1}{2} \le t \le 1 \\ 0; & \text{otherwise} \end{cases} \quad \text{----- (5)}$$

Haar wavelet has the following major properties:

1) No multiplication operation is required.
2) The computation time is very short since addition is the only operation to be carried out on Haar matrix, which consists of many zero valued elements. In other words, it is faster than any other wavelet.
3) Input and output lengths are the same.
4) Localized characteristics of a signal can be analysed.
5) Orthogonal property of Haar wavelet makes way for frequency component analysis of a signal.

III. AUDIO STEGANOGRAPHY

The audio steganographic method focuses to hide the secret information or secret message bit inside a safe cover audio file or signal securely and strongly. Security and robustness in communication are essential for transmitting secret and important information to authorized recipients, while denying access to unauthorized entities. When we embed secret message using an audio signal as the cover file, the very presence of secret message is hidden away in communication. This is a major requirement in real time applications like communication in battlefield and banking transactions. In digital audio steganographic system, the secret information or

message bits are embedded in digital sound. The process of embedding secret message is done by changing the binary sequence of a acoustic file. So far, the audio steganographic algorithms can embed messages in audio file with WAV, AU and MP3 formats.

The basic audio steganographic system includes Carrier (Audio file), Message and Password. Carrier which is also known as a cover-file hides the secret message. Message represents the data or information that needs to be made confidential. The different forms of message include plain text, image, audio or any type of data. Password represents the stego-key, and it ensures that only intended recipient who knows the corresponding stego-key will be able to extract original information from audio cover file. The output which is the cover-file along with the secret message is called stego-file.

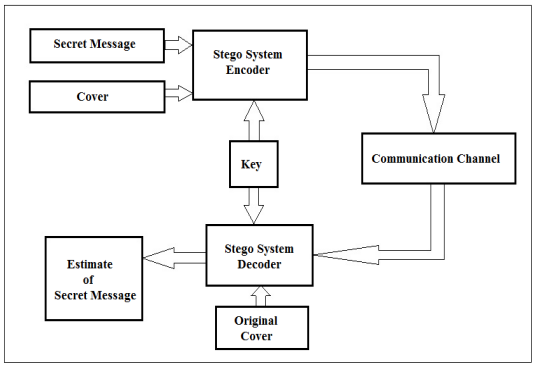

Figure 2: Basic Steganographic System

The most difficult task while carrying out steganography is encoding secret messages in audio. The major and only weakness in Human Auditory System (HAS) is in differentiating sounds and this weakness of HAS is to be exploited in order to encode secret messages in audio file and make it undetectable. The information hiding process in audio steganography makes use of the steps provided below:

1) Identifying redundant bits from cover-file. The redundant bits are the ones that when modified will not corrupt the quality or destroy integrity of cover-file.
2) Embedding secret message within cover file, by replacing redundant bits in cover file with secret message bits.

IV. HIDING ALGORITHM

The algorithm for the process of message hiding is as depicted in block diagram of Figure 3.

A. Selecting Secret Message and Cover File

The secret information or message in text form is being converted in to an image file. The cover signal is an audio file and then input the cover signal in which data is to be embedded. The size of the cover signal must be large enough to conceal the secret message. Next, after selecting the input secret message and cover signal, the length or size of the audio cover file as well secret image file has to be checked and compared.

B. Encryption of Secret Image File

The secret message or information in the form of image must be converted in to some other form before it in to cover signal so as to make it undetectable by unauthorized entities. In order to carry out this, first, we have to convert the secret image file to binary form or bits. Let the length of converted secret message bits be N bits. Next, a random number is used to generate private key of length N since size of encrypted message has to be equal to original secret message. Finally, an X-OR operation is carried out to generate the cipher message of length N bits.

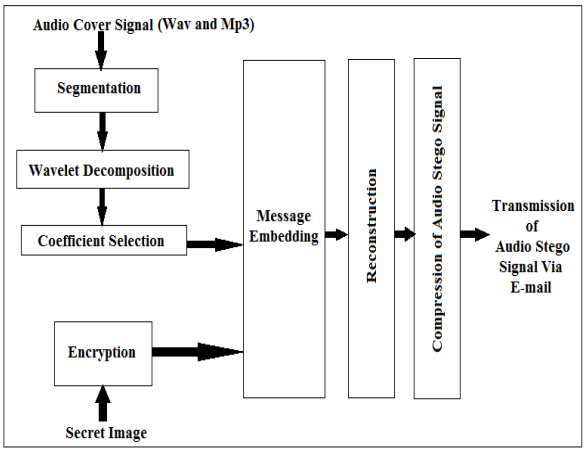

Figure 3: Block Diagram of Image Hiding Algorithm

C. Segmentation of Cover Signal

Consider that the input cover audio signal includes R samples and is segmented into two groups, namely, processed samples and unprocessed samples. Size of processed samples is depends on message bits size i.e. for message bit of size N has N*2^L processed samples where L is decomposition level. The remaining are unprocessed samples. The processed part is then partitioned to segments of size N and each of these segments has length of Z samples.

D. Decomposing Segment and Selecting Coefficient

Each segment of the input audio cover signal is decomposed using L level of Haar DWT transformation to obtain 2^L signals, each one of the produced signal has length of Z/2^L samples. One represents the Approximated signal and the others represent detailed signals. From the detailed signal we select one of the detail signals for embedding process.

E. Embedding the Secret Image

Message embedding process is carried out by comparing with the value of a chosen threshold. There are two steps in the comparison process as provided below:

1) If secret message or image in bit format is found to be 0, then compare selected coefficient with threshold T and if selected coefficient is greater than T, then modify the coefficient so that it will be less than T otherwise no change is required.
2) If secret message or image in bit format to be embedded is 1 and if the selected coefficient is less than threshold value T, then modify the coefficient to become greater

than or equal to T. Otherwise no modification is required.

F. Reconstruction of Audio Stego Signal

When reconstructing the stego signal, every altered segment is converted back to time domain from frequency domain. Reconstruction of the segments based on modified detailed coefficient and unmodified approximate coefficient is done by IDWT process. The segments thus obtained or reconstructed will be fed to segment collecting step to obtain audio stego file.

G. Compression and Transmission

The audio stego signal is then compressed using widely used multimedia compression technique (DCT or DWT). The compressed audio stego file is then transmitted via e-mail.

V. RECOVERY ALGORITHM

The process of extraction of secret message from the stego-file is illustrated by the block diagram in Figure 4.

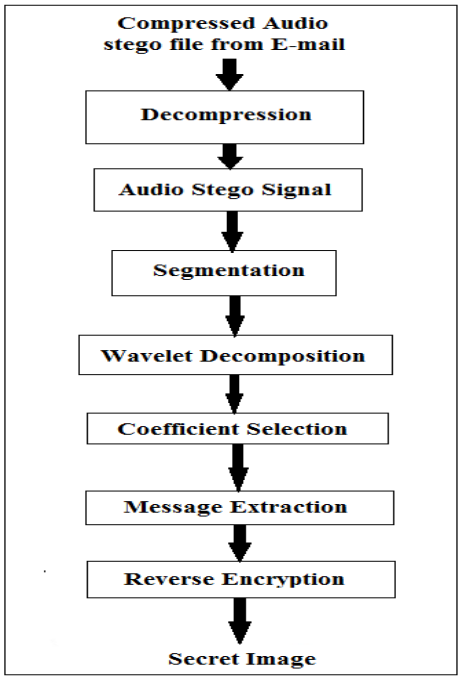

Figure 4: Block Diagram of Image Recovery Algorithm

A. Receiving and Decompression

The compressed audio stego-file received via e-mail is decompressed using a multimedia decompression algorithm. The output of this block provides the audio stego signal.

B. Audio Stego Signal Input

In the algorithm for recovering the image, audio stego signal selection is carried out first, from which the data is to be extracted. This audio stego signal has to be the same as the one used during message hiding process.

C. Segmentation of the Stego Signal

Here, the stego signal is getting segmented to two groups, namely, processed and unprocessed samples. The processed sample size is calculated by multiplying the N with 2^L, where L is the wavelet decomposition level. Then the Processed part is segmented to N segments with each having size of Z samples.

D. Decomposing Stego Signal and Selection of Coefficient

Each segment of the audio stego signal is being decomposed using L level of Haar DWT in order to obtain the 2^L number of samples, and each of these will have a length of Z/2^L. The process of Haar DWT generates Approximate and detailed coefficients and from the latter we select that particular detail signal used during embedding process.

E. Recovering Secret Image in Bit format

The process of recovery of secret image stage is very simple and is based on comparing the selected detail coefficient with threshold value T. If the detail coefficient is greater than or equal to pre set threshold T then message bit is 1 otherwise 0.

F. Reverse Encryption and Conversion

The secret message has to be converted back to the original form i.e. the image file. In order to achieve this, first, we use the same random number and generate private key of size N, then X-OR operation is applied to obtain the original message in bits of size N. Finally, we convert these bits in to image file and deliver to receiver.

VI. PARAMETERS AND OUTPUT

The major parameters used for analysis here are payload capacity and SNR. The measure of these parameters determines the transparency and payload that can be embedded and in turn describes the efficiency of the steganographic algorithm. The definition and detailed explanation about the parameters are as provided below.

A. Payload Capacity

Payload capacity or simply capacity is defined as the amount or size of secret message that can be embedded within the cover file without making distortions or changes in the cover audio file. The unit of payload capacity is bits/second.

B. SNR

Signal-to-Noise Ratio (SNR) is a parameter that is very sensitive to the alignment in time domain of the original as well as the distorted audio signal. The SNR is described for the steganographic algorithm by the equation (6). Here, x(i) is the original audio signal which is used as the cover file, y(i) is the distorted audio signal or the audio stego signal and N represents the number of samples in both signals.

$$SNR = 10 \log_{10} {}_{i=1}\sum^{N} x^2(i) / {}_{i=1}\sum^{N} ((x(i) - y(i))^2) \quad \text{----- (6)}$$

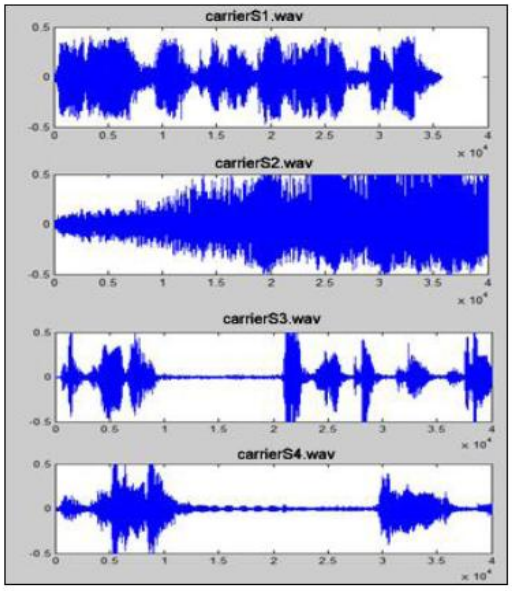

Figure 5: An Example Time Domain Response of Original Audio File

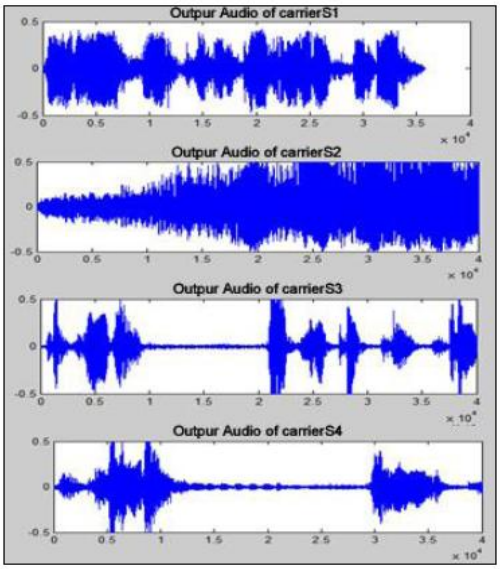

Figure 6: An Example Time Domain Response of Audio Stego File

The possible time domain response of the audio cover file and the output embedded stego file is as provided in the Figure 5 and 6. From the response it is evident that the difference between the embedded stego audio file and original audio cover file is negligible and is very difficult to detect during unauthorized access.

VII. CONCLUSION

A high capacity and high stego-signal quality audio steganographic algorithm based on sample comparison in DWT domain where the selected coefficients of a segment of the audio cover file are compared with pre determined threshold value T and based on comparison, the secret Image bits, which is an image file, are hidden or embedded has been presented. The strength of the algorithm depends on the segment size enables the algorithm to achieve very high embedding capacity. An SNR of more than 25 dB can be achieved using the algorithm. The algorithm can also be extended further using MP3 audio file as cover and audio and video files as secret messages.

ACKNOWLEDGMENT

My endeavour stands incomplete without dedicating my gratitude to everyone who has contributed a lot towards the successful completion of the project work. First of all, I offer my thanks to my parents for their blessings. I am indebted to God Almighty for blessing me with His grace and taking my endeavour to a successful culmination. I am very much grateful and thankful to our Principal Prof. Dr. A. S. Varadarajan for his guidance and support. I express my gratitude and heartfelt thanks to the Dean of Department of Electronics & Communication Engineering, Prof. H. S. Divakara Murthy, for giving directions and providing me with an opportunity to undertake this project. I would like to place on record my deep sense of gratitude to our Project coordinator Mr. Murughanadham C, Assistant Professor of Electronics & Communication Engineering Department for his valuable support and guidance throughout the course of the project. I would also like to extend my sincere gratitude and heartfelt thanks to my Internal Project Guide Mr. Vishnu Prabha N Kaimal, Assistant Professor of Department of Electronics & Communication Engineering, for his support and guidance. I would like to thank all the faculties of NCERC for the help they have extended. Last, but not the least I thank my friends and all my well-wishers who supported me directly and indirectly, encouraged me and gave me the motivation to complete the project work.

REFERENCES

[1] Satish Singh Verma, Mr. Ravindra Gupta, and Mr. Gaurav Shrivastava, "A Survey on Recent Steganography Technique Using Audio Carrier," International Journal Of Advanced Research In Computer Science And Software Engineering, vol. 3, Issue. 11, pp. 731- 738, November 2013.

[2] Neil Jenkins and Jean Everson Martina, "Steganography in Audio", Computer Laboratory, University of Cambridge, 15 JJ Thomson Avenue, Cambridge - UK, CAPES Foundation/Brazil on grant #4226-05-4, 269- 278, January 2009.

[3] Jisna Antony, Sobin c. c and Sherly A. P, "Audio Steganography in Wavelet Domain – A Survey", MES College of Engineering, Kuttippuram, India, "International Journal of Computer Applications", vol. 52– No.13, pp. 0975 – 8887, August 2012.

[4] Sheetal A. Kulkarni, Dr. Shubhangi B. Patil, and Prof B.S.Patil, "A Optimized and Secure Audio Steganography for Hiding Secret Information – Review", Pune University, India, "Journal of Electronics and Communication Engineering", vol. 4, pp. 12-16, Nov- Dec 2012.

[5] Satish S. V, Ravindra Gupta and Gaurav Shrivastava, "A Novel Technique for Data Hiding in Audio Carrier by Using Sample Comparison in DWT Domain", "IEEE Computer Society", ISBN 978-1-4799-3070-8/14, April 2014.

[6] Stephen G. Mallat, "A wavelet tour of signal processing", AcademicPress.

Anjali K B pursuing M. Tech in Applied Electronics and Communication Systems at Nehru College of Engineering and Research Center, Thrissur, Kerala, India under University of Calicut. Participated and presented in National and International Conferences.

Vishnu Prabha N Kaimal, M. Tech graduate specialized in Optoelectronics and Optical Communication. Now, the Assistant Professor at Nehru College of Engineering and Research Center, Thrissur, Kerala, India.