Segments Samples Comparison Based Audio Steganography Technique in DWT Domain

Surbhi Thigale[1], Priyanka Saxena[2]

[1]M-tech Research Scholar, [2]Research Guide

Dept. of Computer Science & Engg.

Abstract - Providing confidential information and establishing concealed association has been a great interest since long time ago. So, there are a lot of methods which are widely used. Steganography is one of them it is the art and science of hiding a secret message in a cover media such as image, text, audio or video in such a way that no one, except the intended recipient knows the existence of the data. This paper provides a high capacity and high stego-signal quality audio steganography scheme based on Coefficient comparison in DWT domain where two Coefficients of a segment are compared and based on comparison bits are embedded. The proposed scheme was tested for different hiding capacity and the results showed that it has excellent output quality.

Keywords - Data Hiding, Stegnography, Stego image, DWT, IDWT.

1. INTRODUCTION

Steganography is an art and science of hiding information in some cover media. The term originated from Greek roots literally mean “covered writing”. The main purpose of steganography is to hide the fact of communication. The sender embeds a secret message into digital media (e.g. im-age) where only receiver can extract this message [1].

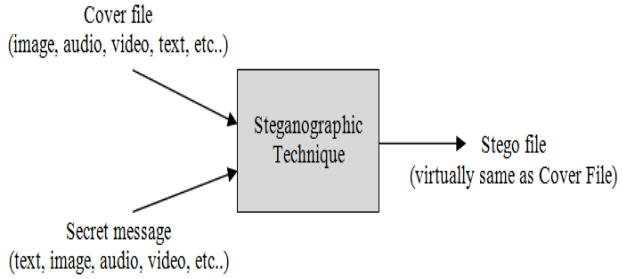

Figure 1: Fundamental process of steganography

The ability of science of hiding the information is known as Steganography. Steganography is of Greek origin and means “concealed writing” where from the Greek word steganos meaning “covered” and the Greek word graphie meaning “writing. Steganography is the process of hiding of a secret message in such a way that no one can able to read the message only the sender and receiver can read.

Secure image transmission is considered to be one of the most important area concerns for security. In this world; whether the image having some text or some scenario information. It is a matrix computation scheme which uses a concept of secret sharing and key safeguarding. Random images are used as shares with the secret image to form a key by using deformation algorithm and to regenerate the secret image back reformation algorithm is used on the random images and key image. The regenerated secret colour image is same as the original image and there is no information lost while recovering the image. This deformation and reformation algorithm reduces the drawbacks of key safe and secret sharing scheme and having its advantages.

Image stenography for hiding a secret image in the cover image. This approach aims at improving the visual quality of the stego image along with the security of the secret image. This approach still provides high embedded capacity. As it is popular that, Steganography is a technique that allows the one to hide the data within an image while adding some notable changes. In this approach we have explored various steganography methods like image steganography, audio steganography, video steganography and text steganography. All these stenography techniques are used to embed the information in digital carriers. The two most important aspects that should be considered for the image based steganography system are as follows: the quality of stego image and the capacity of the cover image [2].

2. SYSTEM MODEL

Audio Data Hiding Techniques:

There are many steganographic techniques for hiding secret data or messages in audio in a way that the modifications made to the audio file are perceptually unclear. Several recent methods require previous familiarity with signal processing techniques, Fourier transform, and other high level mathematics areas.

Some existing techniques of audio data hiding namely Least Significant Bit Encoding, Phase Coding, Echo Hiding and Spread Spectrum techniques. There are two main areas of modification in an audio for data embedding. First, the storage environment, or digital representation of

the signal that will be used, and second the transmission pathway the signal might travel.

Many software implementations of these methods are available on the Web. Some of the latter methods require previous knowledge of signal processing techniques, Fourier analysis, and other areas of high level mathematics. Figures and pseudo code are used in place of exact mathematical formulas in attempts to make the theory more accessible to readers possessing just a basic knowledge of steganography [3,4].

3. PREVIOUS WORK

In the year 2009, [5] Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security R.Sridevi, Dr.A.Damodaram, Dr. Svl.Narasimham, proposed Enhanced Audio Steganography (EAS) which is based on audio Steganography and cryptography that ensures secure data transfer between the source and destination. EAS uses most powerful encryption algorithm in the first level of security, which is very complex to break. In the second level it uses a more powerful modified LSB (Least Significant Bit) Algorithm to encode the message into audio. It performs bit level manipulation to encode the message.

The basic idea behind this paper is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safer manner. Though it is well modulated software it has been limited to certain restrictions. The quality of sound depends on the size of the audio which the user selects and length of the message. Though it shows bit level deviations in the frequency chart, as a whole the change in the audio cannot be determined.

In [6] Information Hiding Using Audio Steganography, Jayaram P, Ranganatha H R, Anupama H S., describe Today's large demand of internet applications requires data to be transmitted in a secure manner. Data transmission in public communication system is not secure because of interception and improper manipulation by eavesdropper. So the attractive solution for this problem is Steganography, which is the art and science of writing hidden messages in such a way that no one, apart from the sender and intend recipient, suspects the existence of the message, a form of security through obscurity. Audio steganographyis the scheme of hiding the existence of secret information by concealing it into another medium such as audio file . In this paper they mainly discuss different types of audio steganographic methods, advantages and disadvantages.

In [7] An Approach to Improve the Robustness of Substitution Techniques of Audio Steganography. Bairagi, A.K, Mondal, S., propose a novel approach of substitution technique of audio steganography. Using genetic algorithm, message bits are embedded into multiple, vague and higher LSB layers, resulting in increased robustness. The robustness specially would be increased against those intentional attacks which try to reveal the hidden message and also some unintentional attacks like noise addition as well.

In this work we proposed a high quality audio steganography algorithm. The aim of proposed algorithm is to gain a high embedding capacity with high quality of output stego file. The proposed algorithm can achieves high embedding and high quality for output stego-signal . Another advantage for proposed algorithm over most algorithms is hardly to detect the positions of embedded secret message especially in low and medium capacity .Furthermore the secret message recovery algorithm does not need the original audio cover signal.

The remainder of the paper is organized as follows: Section 3 introduces the block diagram and steps for encoding and decoding process of the proposed algorithm. In Section 4 the Basic Evaluation parameter for audio steganography is given Section 5 deals with the simulation results and section 6 provides the conclusion.

4. PROPOSED METHODOLOGY

At Sender Side:
In the proposed method the carrier file is taken as audio format and the secret message may be a text or audio format files. Our system provides a very friendly User Interface where the user had to specify just the required inputs (audio, text).

Input: A Cover Audio Signal X and Message M

Output: A Stego Signal Y.

- Input a Cover Audio Signal X of sample rate r samples per second and n bit per sample. Also input the Secret Text Message M of Size N bits .
- Convert the Secret Message M into Cipher Message C by using secret key cryptography with key size same as size of message bit. i.e.

$$C = Encrypt(M, K);$$

- Let the input cover signal consist of R samples, this signal is segmented into two categories: Used segment A and Unused segment B.

- Apply DWT function on each segment of *A* which produces segments in frequency domain.

- Secret message embedding stage is based on comparison of two samples in a segment. Here, the sample p and q is selected by user choice and value of k is selected as small as possible.

- Next, all the modified segments, are converted back from frequency domain to time domain. The IDWT is used to reconstruct the segments of stego-signal.

- At last, The reconstructed segments will fed to segment collecting step to reconstruct the final steganography algorithm output.

At Receiver Side:

Input: A Stego Audio Signal Y

Output: Message M

- Input a Stego Audio Signal Y of sample rate r sample per second and n bit per sample.

- Again the stego signal Y is divide into two parts: Used segment A and unused segment B. The size of Used segment is known to receiver with the help of size of message bit .so the used part is partitioned again into segments of size same as size of message bits that is N segments; each segment has length of Z samples.

- Apply DWT function on each segment of A which produces segments in frequency domain. In each segment one represents the approximate signal and the others represent detailed signals.

- Secret message recovery stage is very simple and based on comparison of two samples in a segment. If the pth sample is greater than Qth sample it means that data is 0 otherwise the Message bit is 1

- Convert the Cipher Message C into original Secret Message M by using secret key cryptography with key size same as size of message bit

Flow Chart of Proposed Method:

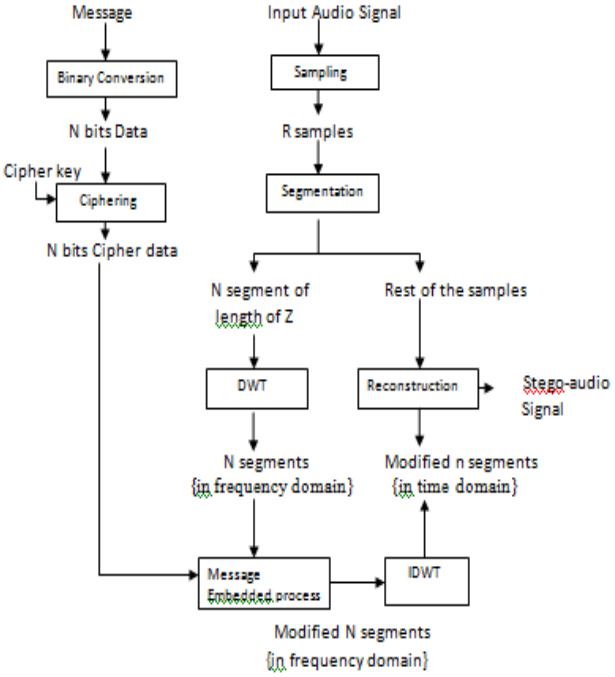

Figure 2: Flow Chart of Message Extraction Algorithm

5. EXPERIMENTAL RESULTS

In this section we give brief descriptions of the quality measures used. The original signal (the cover document) is denoted $x(i), i = 1,..N$ while the distorted signal (the stego-document) as $y(i), i = 1,..N$.

4.1 Signal-to-Noise Ratio (SNR):

The SNR is very sensitive to the time alignment of the original and distorted audio signal. The SNR is measured as

$$SNR = 10\log_{10}\frac{\sum_{i=1}^{N} x^2(i)}{\sum_{i=1}^{N}\left(x(i)-y(i)\right)^2}$$

Where x(i) is the original audio signal, y (i) is the distorted audio signalHere N represents the number of samples in both signals.

Figure 3 shows the relationship between SNR and embedding capacity for fixed message type and four different cover signals.

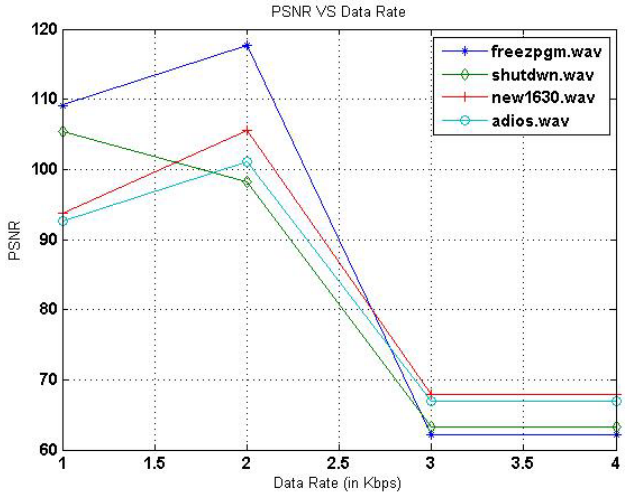

Figure 3 the Relationship between SNR and Embedding Capacity for Different Cover Signals and different Data Type

Table 1 shows a comparison of different cover signal with respect to SNR on different values of P and Q and processing time for fixed capacity (about 200 word/sec) and Z = 8 samples. In these tests we use male speaker female speaker and music as a cover signal with length of 35900 samples 54600 and 34600 respectively and text file as a secret message with size of 4kb . The results in table shows that using the pth and qth sample for comparison will increase the SNR The arbitrary result of bits block matching make the distribution of secret message blocks over the cover signals arbitrary and that increase the security of secret message.

Table 1 SNR and Processing Time for Different P and Q with capacity of 4 kb/sec

Cover Signal	Segment (Pth Sample)	Segment (Qth smaple)	Output SNR (dB)	Processing Time (sec)
freezpgm.wav	2	3	93.66	2.15
	2	4	88.22	2.13
	3	4	92.64	2.15
shutdwn.wav	2	3	101.8	2.25
	2	4	97.24	2.13
	3	4	101.04	2.12
new1630.wav	2	3	67.18	2.18
	2	4	95.85	2.16
	3	4	66.95	2.13
adios.wav	2	3	67.19	2.18
	2	4	95.85	2.12
	3	4	66.95	2.12

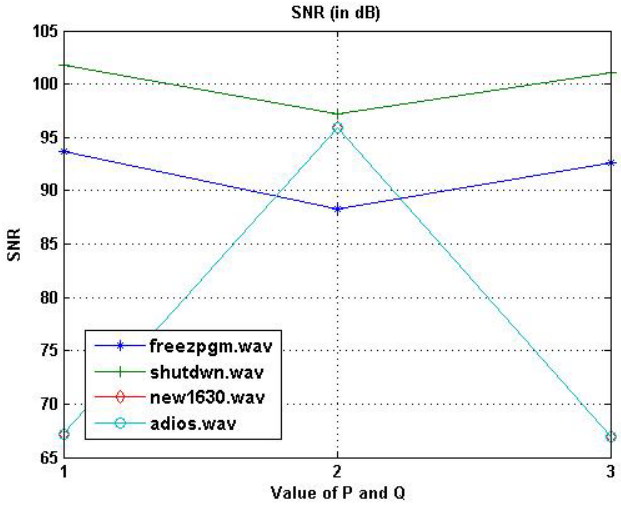

Figure 4 Comparison graph for different cover signals with respect to SNR on different P and Q value

Figure 4 shows a comparison graph of different cover signal with respect to SNR on different values of P and Q and processing time for fixed capacity (about 200 word/sec) and Z = 8 samples. The comparison showed the clearly superiority of the proposed scheme over the conventional DCT scheme in high embedded capacity, the SNR is above 65 dB in our algorithm while it is in range of 21 dB in conventional DCT scheme for different data type messages.

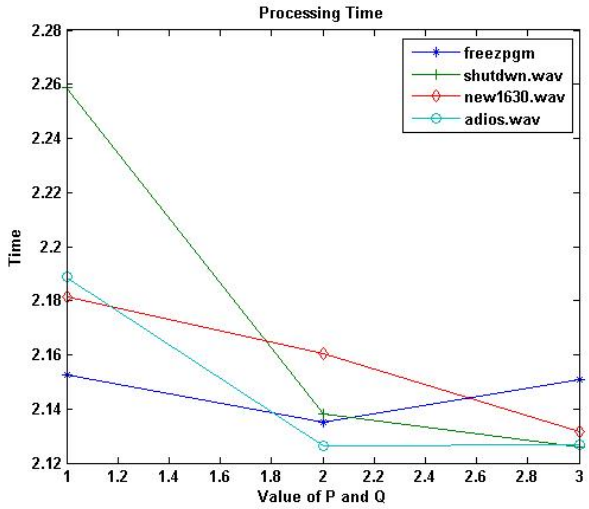

Figure 5 Comparison graph for different cover signals with respect to SNR on different P and Q value

Figure 5 shows a comparison graph of different cover signal with respect to Processing Time on different values of P and Q for fixed capacity (about 200 word/sec) and Z = 8 samples. The comparison showed the clearly superiority of the proposed scheme over the conventional DCT scheme in high Performance Rate. The Processing Time is approx 2 sec in our algorithm while it is in range

of21 dB in conventional DWT scheme for different data type messages.

6. CONCLUSION

Steganography is an information hiding technique where secret message is embedded into unsuspicious cover signal. An effective audio steganographic scheme should possess the following three characteristics: Perceptual Transparency, Capacity and Robustness. We have presented a high capacity and high stego-signal quality audio steganography scheme based on samples comparison in DWT domain where two samples of a segment are compared and based on comparison bits are embedded. The strength of our algorithm is depend on the segment size and their strength are enabled the algorithm to achieve very high embedding capacity. The proposed scheme was tested for different hiding capacity and the results showed that it has excellent output quality. From the tests we find the proposed algorithm support high capacity rate reach up to 4 kb/sec and that is form above 25% from the size of the input audio cover file at SNR above 65 dB for the output signal.

REFERENCES

[1] Rajkumar Yadav," Study of Information Hiding Techniques and their Counterattacks", *International Journal of Computer Science & Communication Networks*, Vol 1(2), 142-164 Oct-Nov 2011.

[2] A.A.J Altaay, S.Sahib, M Zamani, "An Introduction to Image Steganography Techniques", International *Conference on Techniques Adavance Computer Science Applications and Technologies (ACSAT)*, pp. 122 – 126, 2012.

[3] Neil Jenkins, Jean Everson Martina ," Steganography in Audio" *Anais do IX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais* page: 269-278,2007

[4] Swati malviya,manish Saxena, Dr. Anubhuti Khare,"Audio Steganography by Different Methods", *Internation Journal of Energing Technology and Advanced Engineering*, Volume 2, Issue &, July 2012.

[5] Sridevi, R. Damodaram, A. Narasimham, S, "Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security", *Journal of Theoretical and Applied Information Technology*, vol. 5, no. 6, pp. 768 – 771, June 2009.

[6] Jayaram P, Ranganatha H R, Anupama H S," Information Hiding Using Audio Steganography".

[7] Bairagi, A.K, Mondal, S," An Approach to Improve the Robustness of Substitution Techniques of Audio Steganography", *International Conference on Informatics, Electronics & Vision (ICIEV)*, 2012 May 2012.