Improving the Robustness and Efficiency of Audio Steganography using Spread Spectrum Technique

Sapna Sharma
PG Student
Department of Electronics & Communication Engineering
Hasmukh Goswami College of Engineering, Vahelal, Ahmedabad

Abstract— A very efficient technique is required for audio steganography because this kind of steganography involves sound samples means the sound signal with its varying frequency signals. There are various techniques available for hiding secret information on an audio file but it is mandatory that audio host file should not be detected by any one because of its large size. So, an efficient technique is requires to design such kind of algorithm. Therefore, Spread Spectrum technique is used in this paper which will provide better results than other available methods and also provide high robustness and efficiency than other techniques. Also a comparison table will be there which will allow choosing an implementation technique on the basis of main parameters of steganography.

Key words: Steganography, cryptography, LSB technique, Spread Spectrum (SS)

I. INTRODUCTION

Audio steganography, which actually uses audio file as cover media and hides secret data behind that audible sound file. Steganography is the way of secure transmission of message by hiding the secret message inside the original message in such a way that only the intended user knows about it. The original message is also called as cover media. Cover media and secret message can be any kind of digital form like text, image, audio and video. Steganography is the art and science of invisible communication of messages (2)

Hiding text with the help of audio file is a tough task than image steganography, but provides a lot of redundant space to hide data. Therefore, steganography is an utmost challenging area in data security field.

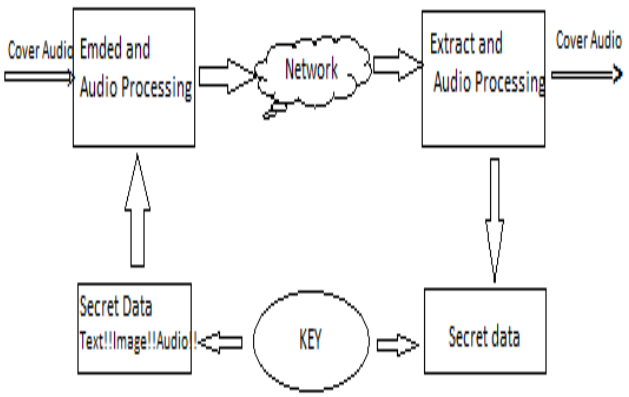

Fig. 1: Block Diagram Audio Steganography Model[4]

Here, a very basic process for audio steganography is shown, in which audio file is taken as cover media and secret message is embed into it using embedding and audio processing block, then secret message hide behind audio file is sent over network for its transmission and then on receiver side that embedded secret message and audio file is extracted. The main thing of concern is that secret message which is to be hide is kept secured using a key or a password, and it is only known by the intended sender and intended receiver, to make this process more secure and safe. (1)

II. VARIOUS TECHNIQUES OF AUDIO STEGANOGRAPHY

There are very commonly used techniques are available which hides secret message using audio file as cover media. These techniques are:

- Low bit encoding
- Parity Coding
- Phase Coding
- Echo Hiding
- Spread Spectrum

A. *Low Bit Encoding*

Low bit encoding method is also called Least Significant Bit (LSB) method. Here, the least significant bits of the original message is replaced with the bits of secret message. This method is very to implement. This method provides large space to embed secret information behind it. (8)

B. *Parity Coding*

This is one of most commonly used technique in audio steganography. In this method, a signal is divided into various individual samples and then encodes each bit from the secret message in a sample region's parity bit (3). If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region.(3)

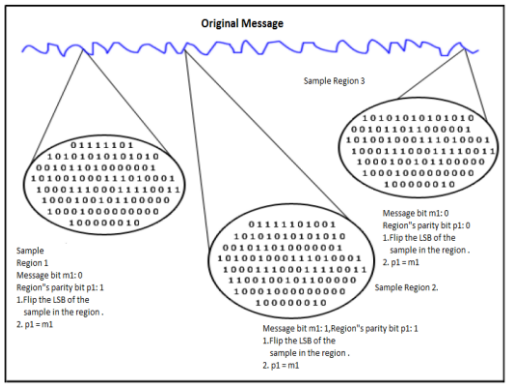

Fig. 2: Parity Coding Process [3]

C. *Phase Coding*

In Phase coding, the phase of carrier file is replaced with reference phase which represents hidden data (5) .this method works by substituting the phase of an initial audio segment with a reference phase that represents the data. The phase of subsequent segments is then adjusted in order to preserve the relative phase between segments (7). As it is

known that phase components of audio signal is not perceptible to human ears.

D. Spread Spectrum Technique

In spread spectrum method, secret information is spread over the audio signal's frequency spectrum as much as redundant space available over there (5), this method offers moderate data transmission rate and great robustness than other methods, but introduces noise to the signal.

E. Echo Hiding

An echo sound is added with the information message to the carrier file, which can be image, text, audio or video file. Echo signals represent information to be encoded (4) If only one echo produced from the original signal then only one bit of information can be encoded. Before encoding begins, the original signal is broken down into parts or blocks. When the encoding process finished, all the blocks are placed back together to create the final signal (7)

III. PROPOSED SCHEME & FLOWCHART WITH WORKING

Spread Spectrum technique is used for the designing of an efficient algorithm, which focuses mainly on robustness, confidentiality, and imperceptibility and information security.

In spread spectrum method, data is multiplied with a N-sequence code which is known only to the sender and receiver and then secret information is spread over the audio signal's frequency spectrum as much as redundant space available there (7).

Spread spectrum is actually works on radio communication, in which it spreads the secret message over the frequency spectrum. Here, the secret message is spreaded like the noise signal, which is very difficult to detect. Spread spectrum method has two types of techniques, which are:

- Direct Sequence Spread Spectrum (DSSS)
- Frequency hopping spread spectrum (FHSS)

1) Direct Sequence Spread Spectrum: The secret message to be transmitted is break down into small parts and pieces, and a frequency channel has been allocated to these parts and are spreaded over the frequency spectrum.(6)
2) Frequency hopping spread spectrum: Here, the frequency spectrum of audio file is modified constantly so that it hops between frequencies. (6)

Here, firstly read the cover file in which secret information has to be hide. There is need to pre-process the cover image in which luminance components are extracted and its DCT coefficients are being computed. DCT matrix will be reshaped in the form of DCT vectors; its watermark sequence will be generated. After this, watermark sequence is embedded into DCT vector. For the purpose of security encryption is done so that information can be made secure to reach towards its destination. This process is on the transmitter side.

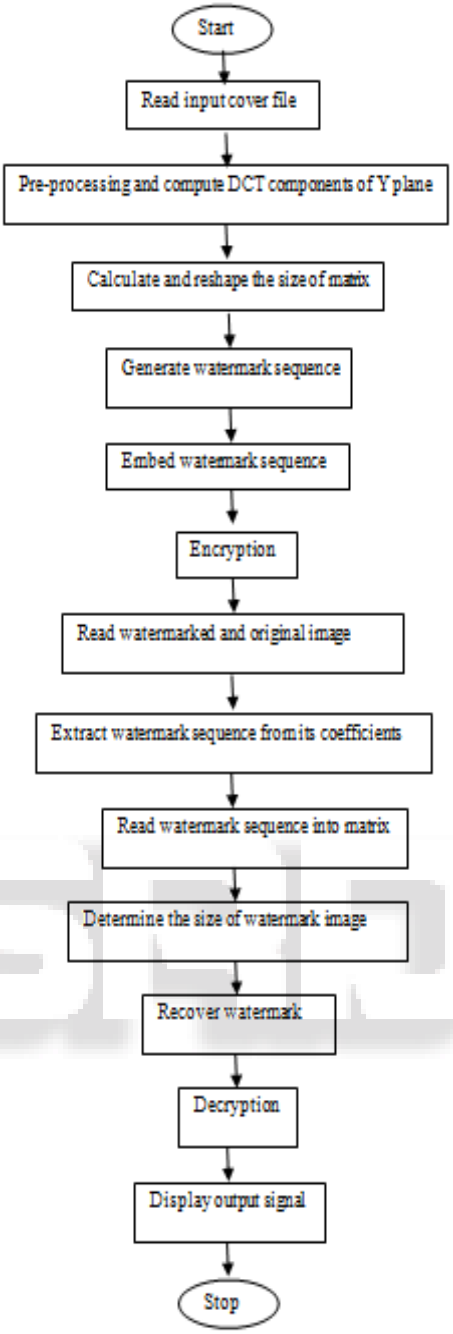

Fig. 3: Proposed Flowchart of Algorithm Using Spread Spectrum

Now at the receiver side, for the process of extraction, firstlly watermarked and original image will be read. Then the watermark sequences are extracted from its coefficients and written into a file. Then watermark sequences are converted into a matrix and are read. Also the size of watermark image is determined and watermark is recoverd and then decryption is done.

The spread spectrum technique provides added layers of security towards information protection (6) The spreaded signal is v ery difficult to detect because it is a noise like signal, which is not susceptible to anyone. This technique offers various advantages over other techniques and provides more robustness than other techniques specially LSB technique.

IV. RESULTS

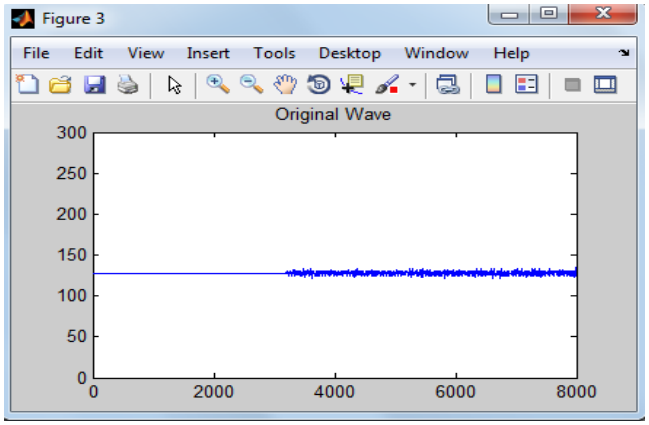

Fig. 4: Original Audio Wave Before Steganography

Fig. 5: Watermarked Image

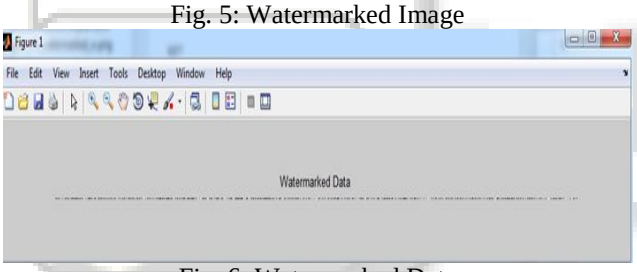

Fig. 6: Watermarked Data

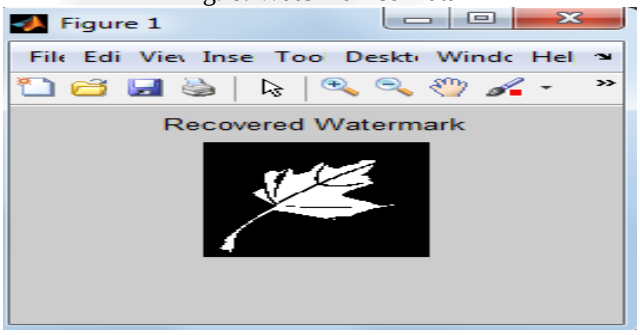

Fig. 7: Recovered Watermark Image

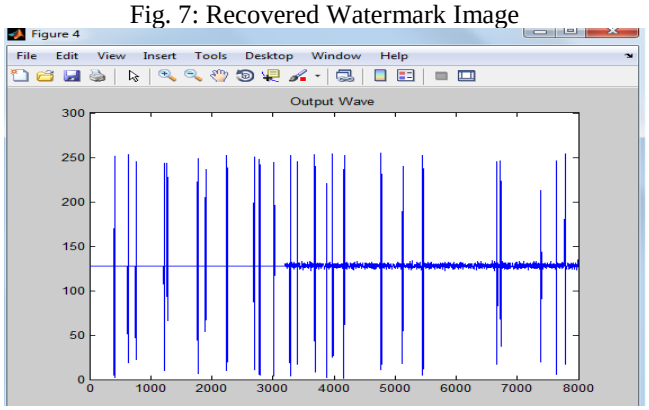

Fig. 8: Extracted Output Audio Wave

These results are simulated using Matlab R2013a simulation software, which is technical computing software and it is compared with LSB method results which are not simulated in this paper but are available from other results published in other articles and papers.

If these results are compared with the results of LSB technique as shown in (1), (9) and (10), then very main points are observed about both of these techniques.

LSB technique provides large space to hide secret information, easy to implement but at the same time this technique is very less robust as this is proposed in (7). Therefore, a new algorithm has been designed using Spread Spectrum (SS) technique.

Spread Spectrum (SS) technique focuses more on robustness, security, imperceptibility, confidentiality (9) and will hide data under audio cover media in a more secured manner

V. CONCLUSION AND COMPARISON

The proposed work shows that how an audio sound files is embedded into an audio carrier file. The proposed scheme is spread spectrum which actually spreads the secret information in noise like form over the frequency spectrum. This noise like signal makes the technique less detectable and provides no jamming and interference.

A comparison has been shown here which shows that even the most simplest and easy technique named as LSB, lacks robustness and other main attributes of a required steganography algorithm.

VI. COMPARISON TABLE FOR LSB AND PROPOSED SCHEME (SPREAD SPECTRUM)

Sr. No.	Parameters	LSB technique	Spread Spectrum technique
1.	Method of hiding	Changes secret message bits with the original cover file bits	Spreads the secret message over the frequency spectrum
2.	Imperceptibility	Very low	Very high because introduces secret message in the form of noise.
3.	Detect ability	Very high chances of detection because of huge file size	Difficult to detect that any kind of information is hidden in it.
4.	Robustness	Very low	Very high because it provides added layers of security
5.	Resistance and probability	Less resistant and low probability of receiving correct data	Provides high resistance against Noise and interference, also give high probability of receiving correct data.
6.	Implementation	Very easy to implement	Difficult to implement than LSB method.

REFERENCE

[1] Bhagyashri A. Patil1, Vrishali A. Chakkarwar, "Review of an Improved Audio Steganographic

Technique over LSB through Random Based pproach" IOSR Journal of Computer Engineering (IOSR-JCE) Volume 9, Issue 1 (Jan. - Feb. 2013

[2] Rucha Bahirat ,Amit Kolhe , "Overview of secure data transmission using Steganography" International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 3, March 2014

[3] Masoud Nosrati, Ronak Karimi, Mehdi Hariri "Audio Steganography: A Survey on Recent Approaches" World Applied Programming, Vol (2), No (3), March 2012

[4] Swati Malviya, Manish Saxena, Dr. Anubhuti hare "Audio Steganography by Different Methods" International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 7, July 2012

[5] Prof. Samir Kumar, Bandy opadhyay Barnali, Gupta Banik "LSB Modification and Phase Encoding Technique of Audio Steganography Revisited" International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 4, June 2012

[6] W. Q. Cheng, "Robust Audio Steganography using Direct-Sequence Spread Spectrum Technology", University of British Columbia, 2007

[7] Gunjan Nehru, Puja Dhar, "A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012

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

[9] Deepali Ghanwat, Prof .R .Sunder Rajan "Spread spectrum based audio steganography in transformation domain" Global Journal of Advanced Engineering Technologies, Vol2, Issue4-2013

[10] Linu Babu, Jais John S**,** Parameshachari B D,Muruganantham C, H S DivakaraMurthy, "Steganographic Method for Data Hiding in Audio Signals with LSB & DCT" International Journal of Computer Science and Mobile Computing Vol.2 Issue. 8, August- 2013

