INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

EMBEDDING & EXTRACTION OF POWER DATA INTO A AUDIO FILE USING MODIFIED DIRECT SEQUENCE SPREAD SPECTRUM TECHNIQUE

Vijeta Pandey[1], Vikas Verma[2], Gourav Sharma[3]

[1],M.Tech Student, Electrical Engineering Deptt.,
[2,3]Associate Prof, Electrical Engineering Deptt.,
MMU Mullana, Ambala, Haryana, India
[1]vijeta0037@gmail.com, [2]vikasverma@mmumullana.org,[3] gorutyagi11@gmail.com

Abstract: *With the development of computer and expanding its use in different areas of life and work, the issue of information security has become increasingly important. One of the grounds discussed in information security is the exchange of information through the cover media. To this end, different methods such as cryptography, steganography, coding, etc have been used. The method of steganography is among the methods that have received attention in recent years. The main goal of steganography is to hide information in the other cover media so that other person will not notice the presence of the information. This is a major distinction between this method and the other methods of covert exchange of information because, for example, in cryptography, the individuals notice the information by seeing the coded information but they will not be able to comprehend the information. However, in steganography, the existence of the information in the sources will not be noticed at all. Spread spectrum techniques were invented in the 1950s as a means of improving the security and reality of digital communications systems, and they are regularly employed in wireless systems today. A narrowband data signal, such as a frequency shift keying (FSK) signal for example, is converted into a spread signal by modulating it with a wideband spreading signal that is independent of the data signal. Two commonly spread spectrum techniques are used direct sequence spread spectrum (DSSS) and frequency hopped spread spectrum (FHSS). Implementation of steganography in audio data using Direct Sequence Spread Spectrum method has been presented in this thesis. The Spread Spectrum method used in this thesis is Direct Sequence Spread Spectrum. A key is needed to embed messages into noise, this key is used to generate pseudo-random key sequence. The information to be embedded must first modulated using the pseudo- random key sequence. Also, Random location selection to embed the data within the cover image pixels is also proposed in the work. These modifications give a more secure stegano-graphic system, making guesses about the bit-rate or message length less feasible. The proposed stego and extraction system uses DSSS technique. These are used to increase the security and robustness of the system. Improvement has been achieved in robustness on the expense of reducing the capacity of hiding. The imperceptibility of the stego audio and extracted image is assessed by using peak signal-to-noise ratio (PSNR), MSE and normalized correlation measure. MATLAB R2013a has been used as an implementation platform.*

Keywords: *stego-system, steganography, cryptography, watermarking, embedding, extraction etc.*

1. INTRODUCTION

Before the discovery of steganography and cryptography, it was challenging to transfer secure information and, thus, to achieve protected communication environment [1]. The development of technology has increased the scope of steganography and at the same time decreased its efficiency since the medium is relatively insecure. This lead to the development of the new but related technology called „Watermarking". Some of the applications of watermarking include ownership protection, proof for authentication, air traffic monitoring, medical applications etc. [1] [2] [4]. Watermarking for audio signal has greater importance because the music industry is one of the leading businesses in the world [7].

Steganography and Watermarking

The steganography technique needs a **cover object** and **message** that is to be transported. It also requires a **stego key** to recover the embedded message. Users having the stego key can only access the secret message. Another important requirement for efficient steganographic techniques is that, the cover object is modified in a way that the quality is not lost after embedding the message.

Watermarking

Watermarking is a technique in the course of which the secure information is carried without degrading the quality of the original signal. The technique consists of two blocks:

i) Embedding block
ii) Extraction block

The system has an **embedded key** as in case of a steganography. The key is used to increase security, which does not allow any unauthorized users to manipulate or extract data. The embedded object is known as **watermark**, the watermark embedding medium is termed as the **original signal** or **cover object** and the modified object is termed as **embedded signal or watermarked data** [3].

2. PROPOSED METHODOLOGY

Spread Spectrum Technique

These techniques are derived from the concepts used in spread spectrum communication [4]. The basic approach is that a narrow band signal is transmitted over the large bandwidth

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

signal which makes them undetectable as the energy of the signal is overlapped. In the similar way the watermark is spread over multiple frequency bins so that the energy in any one bin is very small and certainly undetectable [5].

In spread spectrum technique, the original signal is first transformed to another domain using domain transformation techniques [4]. The embedding technique can use any type of approach for example quantization. Zhou *et al.* proposed an algorithm embedding watermark in 0th DCT coefficient and 4th DCT coefficients which are obtained by applying DCT on the original signal [6]. Both embedding and extraction procedure can be interpreted using Figure 1. The original signal is transformed into frequency domain using DCT. Then watermark is embedded to the sample values in that domain. Reverse procedure is followed to obtain the watermarked signal. This process of generating embedded signal is shown as embedding procedure in Figure 1.

Embedded signal will undergo some attacks, thus, noise is added to the signal. To extract the watermark the attacked signal is fed through extraction procedure. The procedure for extractions follows the same steps as that in embedding procedure as shown in Figure 1. The extraction process involves taking the attacked signal and applying DCT, framing the obtained components. And they obtained frames are used to obtain the watermark. Care is taken to replicate the procedure used for embedding process.

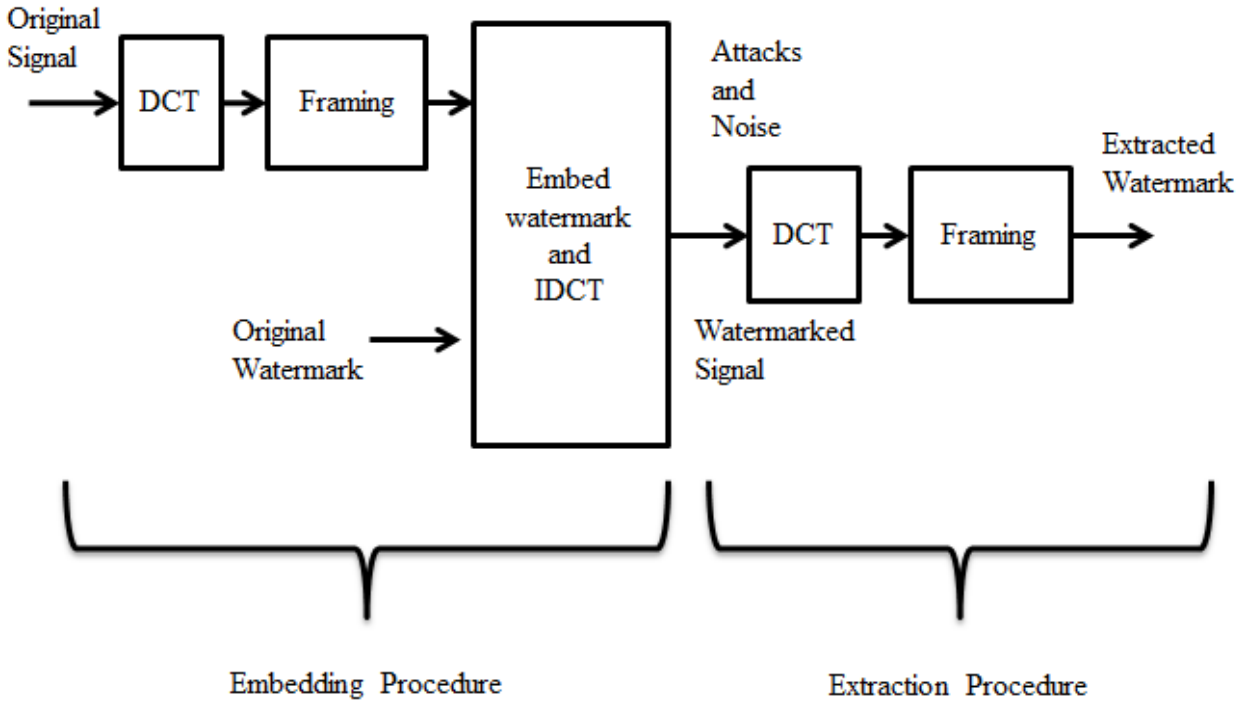

Figure 1: Example for spread spectrum technique

In the context of audio steganography, the basic spread spectrum (SS) method attempts to spread secret information across the audio signal's frequency spectrum as much as possible. This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire sound file. However, unlike LSB coding, the SS method spreads the secret message over the sound file's frequency spectrum, using a code that is independent of the actual signal. As a result, the final signal occupies a bandwidth in excess of what is actually required for transmission.

Two versions of SS can be used in audio steganography: the direct-sequence and frequency-hopping schemes. In direct-sequence SS, the secret message is spread out by a constant called the chip rate and then modulated with a pseudorandom signal. It is then interleaved with the cover-signal. In frequency-hopping SS, the audio file's frequency spectrum is altered so that it hops rapidly between frequencies.

The math theory behind SS is quite complicated and goes beyond the scope of this project. However, Katzenbeisser and Petitcolas write about a generic steganography system that uses direct-sequence SS in *Information Hiding Techniques for Steganography and Digital Watermarking*. The following procedural diagram illustrates the design of that system when applied to our specific topic of audio steganography.

The SS method has the potential to perform better in some areas than LSB coding, parity coding, and phase coding techniques in that it offers a moderate data transmission rate while also maintaining a high level of robustness against removal techniques. However, the SS method shares a disadvantage with LSB and parity coding in that it can introduce noise into a sound file.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Here are the steps for proposed method:

EMBEDDING OF WATERMARK

- First of all read cover audio signal and get equivalent 2D matrix & calculate size of matrix i.e. rows and column. Read watermark image and get equivalent 2D matrix & calculate size of matrix i.e. rows and column. Convert watermark matrix into binary matrix & reshape binary matrix into row matrix. Get spreading size by multiplying spreading factor i.e. 2 with total number of elements of binary watermark matrix and generate a random binary key sequence according to spreading size, so as to provide security.
- Encode watermark matrix by Binary XOR-ing of row vector watermark matrix with key sequence. Now, encoded watermark matrix has a double size as compared to that of original. If cover image is too big then divide cover image matrix into two parts. Select a block size, which must be suitable to the size of first part of cover image matrix & divide cover image matrix into first and second part. Segmentation of first part matrix into an array of sub-matrix is given below.
- Each sub-matrix has a specific number of elements which depends upon block size. Application of Discrete Cosine Transform (DCT) on each element of all the sub-matrices.
- Embedding of watermark by multiplication of encoded watermark matrix with cosine transform matrix
- Reconstruction of matrix by application of inverse discrete cosine transform on resultant matrix
- Join reconstructed matrix with second part of cover image matrix and getting of embedded image and resize embedded image according to original audio cover signal. Plot frequency coefficients of both audio cover signals, so as to make comparison.

EXTRACTION OF WATERMARK

- Read audio cover signal and audio watermarked signal & calculate size of cover audio signal. Read watermark image and calculate size of watermark image. Also calculate number of elements in watermark image. Select block size of 10 so as to increase the spreading and divide both images i.e. cover and marked audio into two parts. Declare empty cell having array of empty matrices so as to fill these with first part of both matrices. Also declare threshold value so as to fill the empty cell up to a certain limit.
- Application of discrete cosine transform on both cell.
- Division of 3rd element of each matrix of watermarked signal by that of original audio cover signal.
- Decoding of watermark components or removal of key sequence.
- Reconstruction of extracted watermark according to size of original watermark image
- Plotting of both watermark images i.e. original and extracted.

3. EXPERIMENTAL RESULTS

A method for audio steganography using modified Direct Sequence Spread spectrum has been proposed in this work. Firstly, embedding of a secret watermark image has been hide behind a audio with encryption of watermark image. Then, extraction of same watermark has been done in an efficient way, so that the extracted watermark is almost same as compared to that of original watermark. The proof of above statements is the value of PSNR, MSE and Cross-correlation (between original and extracted watermark & between original and embedded watermark). Above mentioned has been calculated at the last of embedding and extraction process, so as to evaluate the performance of proposed method. Simulations work has been performed in MATLAB R2013a using image processing tool box and generalized MATLAB toolbox. There are 6 figures below. Figure 2 is the snapshot of graph of original audio. Figure 3 is the snapshot of embedded audio containing information of watermark also. It can be easily seen that both have almost characteristic and almost similar, which can be proved by Normalized correlation value i.e. 0.9972, shown in figure 4. Figure 4 is the snapshot of command window, shows the value of other two mentioned parameters. The PSNR and MSE value of embedded audio signal is 96.0729 dB and 0.00016172 respectively. Next 3 figures have been driven from the extraction simulation of watermark. Figure 5 is the snapshot of original Secret watermark image. Figure 6 is the snapshot of extracted watermark image. The similarity between both images can be described by Normalized correlation value i.e. 0.9749, shown in figure 7. Figure 7 is the snapshot of command window, shows the value of other two mentioned parameters. The PSNR and MSE value of extracted watermark is 69.0460 dB and 0.0081 respectively. If we compare both the watermark analytically both have no difference, which is a good sign for proposed method in terms of correlation.

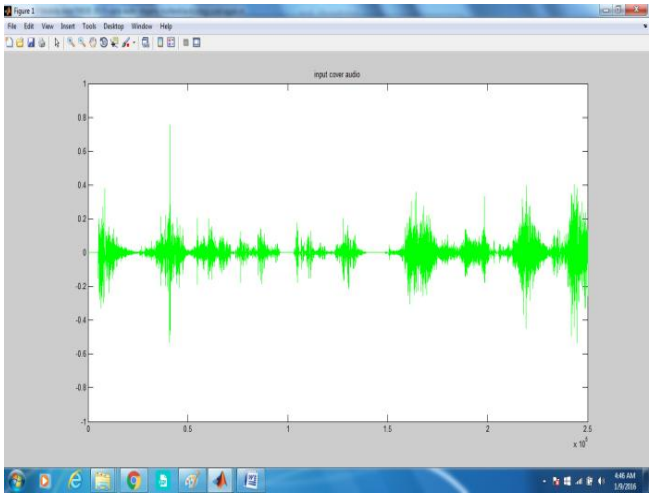

Figure 2: snapshot of graph of original audio

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

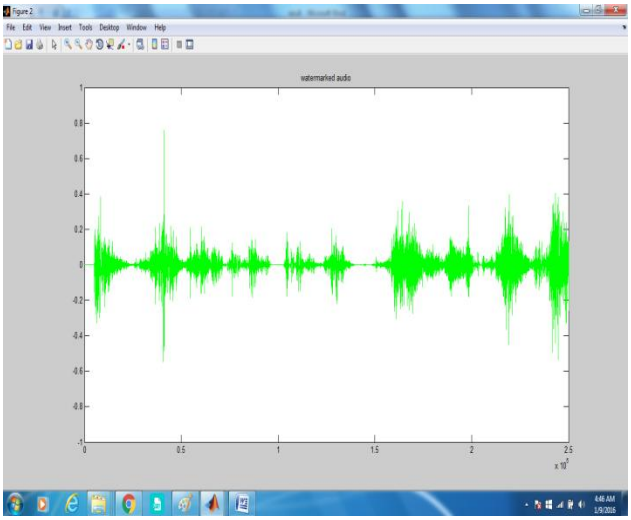

Figure 3: snapshot of embedded audio containing information of watermark also

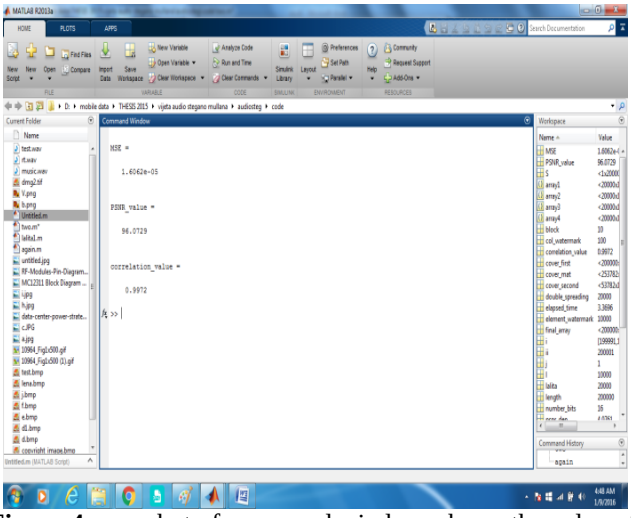

Figure 4: snapshot of command window, shows the value of other two mentioned parameters

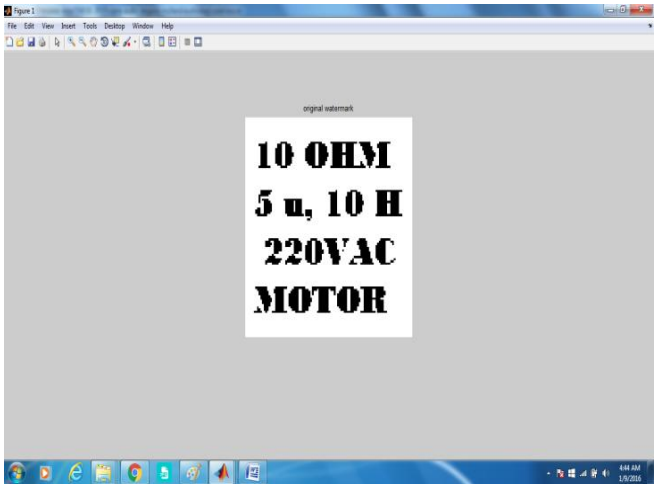

Figure 5: snapshot of original Secret watermark image

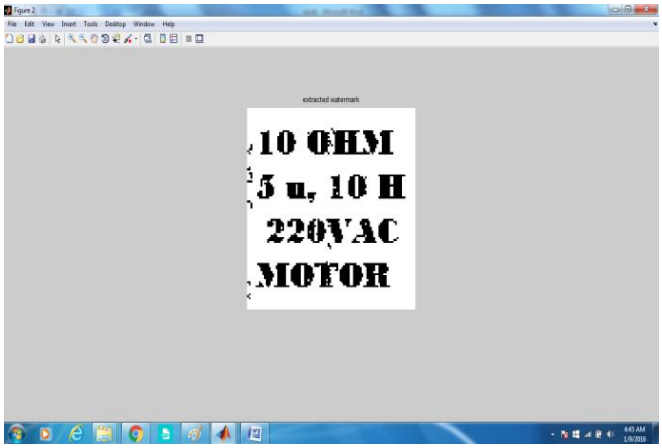

Figure 6: snapshot of extracted watermark image

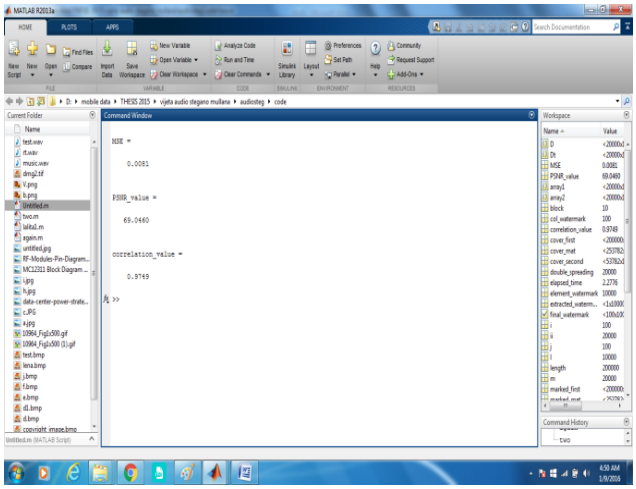

Figure 7: snapshot of command window, shows the value of other two mentioned parameters

4. CONCLUSION &FUTURE SCOPE

The steganography have received much more attention in recent years. The main goal of steganography is to hide information in the other cover media so that other person will not notice the presence of the information. From all the results derived in the present thesis, it can be concluded that proposed methodology is much efficient in terms of PSNR, correlation with original watermark, complexity and invisibility as compared to existing other methods for the same. Proposed method is more barely visible and a robust combined algorithm of digital watermarking, which is based on advanced spread spectrum methodology, PSNR (i.e. 96.0729 dB and 69.0460 dB) and normalized correlation (i.e. 0.9972 and 0.9749) values are very high whereas, Mean Square Error (i.e. 0.00016172 and 0.0081) is very low. Performance evaluation results shows that advancement of spread spectrum methodology improved the performance of the already existed watermarking algorithms that are based exclusively on the normal spread spectrum methodology. The simulation result shows that this algorithm is much better for invisible watermarking and has good robustness for some common

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

signal processing operations. This work can be extended in future by improving the performance of current methodology by making it more vigorous and less complex for low frequency audio signal. Also, the time consumption for embedding as well as for the extraction of watermark can be reduced.

REFERENCES

[1] R. S. Youail, V. W. Samawi and A. K. A. R. Kadhim, "Combining a spread spectrum technique with error-correction code to design an immune stegosystem," *Anti-counterfeiting, Security and Identification, 2008. ASID 2008. 2nd International Conference on*, Guiyang, 2008, pp. 245-248.

[2] Marcus Nutzinger, Christian Fabian, Marion Marschalek "Secure Hybrid Spread Spectrum System for Steganography in Auditive Media" Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing 2010. Pp. 78-81.

[3] Bo Liu, Erci Xu, Jin Wang, Ziling Wei, Liyang Xu, Baokang Zhao*, Jinshu Su "Thwarting Audio Steganography Attacks in Cloud Storage Systems" International Conference on Cloud and Service Computing 2011. Pp. 259-265.

[4] Parul Shah, Pranali Choudhari and Suresh Sivaraman "Adaptive Wavelet Packet Based Audio Steganography using Data History" 2008 IEEE Region 10 Colloquium and the Third ICIIS, Kharagpur, INDIA December 8-10.. pp. 286-291.

[5] Gao, S., et al. "A detection algorithm of audio spread spectrum data hiding. "Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on. IEEE, 2008.

[6] S. Hernández-Garay, R. Vázquez-Medina, L. Niño de Rivera and V. Ponomaryov "Steganographic Communication Channel Using Audio Signals" 12th International Conference on Mathematical Methods in Electromagnetic Theory June 29 – July 02, 2008, Odesa, Ukraine. Pp. 427-429.

[7] XUE-MIN RU, HONG-JUAN ZHANG , XIAO HUANG " STEGANALYSIS OF AUDIO: Attacking the Steghide "Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, 18-21 August 2005 ". Pp. 3937-3943.