Audio Stegnography with Data Encryption and Decryption using Discrete Wavelets Transformation

[1]B.Koteswarao, [2]B.Vishnu Vardhan

[1]PG Scholar, [2]Assistant Professor
Department of CSE,
[1]Prasad V Potluri Siddartha Institute of Technology, Vijayawada, AP, India

ABSTRACT: **A Previously traditional methods were sufficient to protect the information, since it is simplicity in the past does not need complicated methods but with the progress of information technology, it become easy to attack systems, and detection of encryption methods became necessary to find ways parallel with the differing methods used by hackers, so the embedding methods could be under surveillance from system managers in an organization that requires the high level of security. This fact requires researches on new hiding methods and cover objects which hidden information is embedded in. It is the result from the researches to embed information in executable files, but when will use the executable file for cover they have many challenges must be taken into consideration which is any changes made to the file will be firstly detected by untie viruses , secondly the functionality of the file is not still functioning. In this paper, a new information hiding system is presented. The aim of the proposed system is to hide information (data or text) by using Wavelets Transformation. First we encrypt the data in a wave format and we can decrypt the data from the wave signal.**

KEYWORDS: **information Hiding, Wavelets, Steganography**

I. INTRODUCTION

The recent development of digital media has increased. The nasty users can copy and store the digital media like audio, video, image without any loss of conformity. This has to be protected from the malicious use. The people using the internet download the audio files from various websites and they modify the work as their own copyright. This has become an large issue today in the internet world. The protection is being vanished and the immoral use is done.

To protect this Digital Audio Watermarking is used. This technique protects from nasty users and provides copyright, robustness, security to digital contents. The audio watermarking is technique of embedding and extraction procedures. In embedding process the content like audio, video or image is embedded into a original file which is to be secured. The extraction procedure allows us to extract the content but the file is being still protected.

There are about some properties that satisfy the need for effective watermarking applications. These are

Inaudible- The digital watermark is embedded into audio data as it should not be audible to human ear.

Security- A system is believed to be protected if the cracker cannot take away the watermark applied without having the knowledge of embedded algorithm, detector and composition of watermark. Only the authorized users can access it.

Verifiability- It can be used to check the object is protected i.e. copyright-protected and identify the authenticity and control of illegal copying

Robustness- It is the capability to deal with the copyright information of digital works, the embedded watermark can refuse to accept the common editing process, processing the image and lossy compression. Also after attacks the watermark cannot be damaged and can be still detected to offer certification. For example filtering, noise, compression, cropping, A/D-D/A conversions, geometrical or non-geometrical attacks etc.

Fragile- Fragile watermarking is used for mainly integrity protection which is very sensitive to the changes of the signal. We can determine tampered data in accordance with the state of fragile watermarking.

Semi fragile- Itis proficient in managing changes made to watermarked image such as addition of lossy compression (i.e. noise).

Constant Bit-rate- The amount of watermark data may be securely embedded within the host signal per unit space or time.

For solving the data security the watermarking techniques are introduced to provide security of information. In recent years the watermarking techniques have been introduced to focus on images and video clips but audio watermarking is more complicated that video and image watermarking.

Here are two key reasons so as audio watermarking has become complicated.

First, the **Human Auditory System** (HAS) has larger sensitivity than the Human Visual System (HVS) since human ear is capable of detecting the amplitude and frequency changes of the signal.

Second, the duration and size of the audio signal are very shorter than a video clips and image files and this information reduces the audio signal quality.

Least Significant Bit

Least Significant Bit embedding is simple strategy of watermarking. It embeds the data into the cover message so that it cannot be detected by visual eyes. This method works by replacing bits with secret message. It is possible by changing some bits with

secret message. It is embeds data into image on any bit-plane. This reduces the variations in colors that embedding creates. For example embedding into the first bit plane change the value by 1. Similarly for second bit plane it changes the value by 2. This process is followed for all the bits.

Motivation and Objective of the Project

The discrete wavelet transform (DWT) is a well-known and powerful methodology that expresses a signal at different scales in time and frequency. Taking into account the non-stationary characteristic of real signals, the DWT provides good time and frequency resolution. The discrete wavelet packet transform (DWPT) is a variant of the DWT technique. DWPT permits to tile the frequency space in a discrete number of intervals. For music analysis, this possibility has an enormous advantage: it allows us to define a grid of Heisenberg boxes matching musical octaves and musical notes. Considering just the frequencies corresponding to the musical notes, the spectrum characterization becomes a relatively easy task. DWPT is achieved by recursively convolving the input signal with a pair of quadrature mirror filters g (low pass) and h (high pass). Unlike the DWT that recursively decomposes only the low-pass sub-band, the DWPT decomposes both sub-bands at each level. It is possible to construct a tree (a wavelet packet tree) containing the signal approximated at different resolutions.

II. LITERATURE SURVEY

A Survey of Water marking

Watermarking is the process that embeds data called a watermark, tag or label into a multimedia object such that watermark can be detected or extracted to make an assertion about the object may an image or video or audio may also be text only. A watermark can be perceived as an attribute of the carrier (cover). It may contain information such as copyright, license, tracking and authorship etc. Digital watermarking differs from digital fingerprinting.

Nowadays cases involving fake currency are increasing rapidly, so no one needs to be reminded of the importance of watermarking. A watermark is a form, image or text that is impressed onto paper, which provides evidence of its authenticity. Digital watermarking is an extension of this concept in the digital world. In recent years, the rapid growth of the Internet has highlighted the need for mechanisms to protect ownership of digital media. Exactly identical copies of digital information, be it images, text or audio, can be produced and distributed easily. In such a scenario, how can we identify that who is the actual owner? It was impossible to tell until now, but now it's possible only because of Digital Watermarking.

A study on Audio Stegnography

The word steganography means "covered or hidden writing" The object of steganography is to send a message through some innocuous carrier (to a receiver while preventing anyone else from knowing that a message is being sent at all). Computer based stenography allows changes to be made to what are known as digital carriers such as images or sounds. The changes represent the hidden message, but result if successful in no discernible change to the carrier. The information may be nothing to do with the carrier sound or image or it might be information about the carrier such as the author or a digital watermark or fingerprint Steganography (which is somewhat different from watermarking) deals with techniques for hiding information, the goal of steganalysis is to detect and/or estimate potentially hidden information from observed data with little or no knowledge about the steganography algorithm and/or its parameters. It is fair to say that steganalysis is both an art and a science. The art of steganalysis plays a major role in the selection of features or characteristics a typical stego message might exhibit while the science helps in reliably testing the selected features for the presence of hidden information. While it is possible to design a reasonably good steganalysis technique for a specific steganography algorithm, the long term goal must be to develop a steganalysis framework that can work effectively at least for a class of steganography methods if not for all.Cryptography andsteganography are different. Cryptographic techniques can be used to scramble a message so that if it is discovered it cannot be read. If a cryptographic message is discovered it is generally known to be a piece of hidden information (anyone intercepting it will be suspicious) but it is scrambled so that it is difficult or impossible to understand and de-code. Steganography hides the very existence of a message so that if successful it generally attracts no suspicion at all. Using steganography, information can be hidden in carriers such as images, audio files, text files, videos and data transmissions.

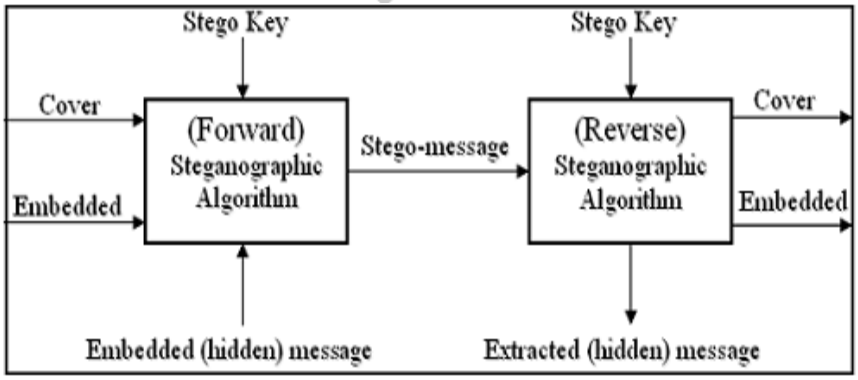

Fig 2.1: Stegnography technique

The above figure 2.1. shows the stegnography technique that is used for hiding the data.

LEAST SIGNIFICANT BIT (LSB) TECHNIQUE

The most straightforward method of watermark embedding would be to embed the watermark into the least significant bits of the cover object. Given the extraordinarily high channel capacity of using the entire cover for transmission in this method, a smaller object may be embedded multiple times. Even if most of these are lost due to attacks, a single surviving watermark would be considered a success. The following fig shows an example of modifying LSB.

Despite its simplicity, LSB technique brings a host of drawbacks. Although it may survive transformations such as cropping, any addition of noise or lossy compression is likely to defeat the watermark. An even better attack would be to simply set the LSB bits of each pixel to one, fully defeating the watermark with negligible impact on the cover object. Furthermore, once the algorithm is discovered, the embedded watermark could be easily modified by an intermediate party.

A Study on "Wavelet Theory

The vast amount of music available electronically presents considerable challenges for information retrieval. There is a need to annotate music items with descriptors in order to facilitate retrieval. In this paper we present a process for determining the music genre of an item using a new set of descriptors. A Wavelet Packet Transform is applied to obtain the signal representation at different levels. Time and frequency features are extracted from these levels taking into account the nature of music. Using *round-robin* and one-against-allensembles of simple classifiers, together with feature selection methods, we evaluate the best signal representation for music genre classification. Ensembles based on different feature sub-spaces are explored as well in order to overcome over-fitting issues. Our evaluation shows that Wavelet Packet analysis together with ensemble methods achieves very good classification accuracy.

III.MEHODOLOGY

BLOCK DIAGRAM

The below diagram 3.1.shows the architecture of the project. First we select a media from the file then we will select the signal to decompose then by applying LSB technique we will trace the position the bit that is extracted from the position is converted to binary and ascii conversations and the data is stegnographed by using Wavelets transformation. In the first phase we Encrypt the data or text in the .WAV format and the text is hidden in a audio file. If we want to decrypt the data then we will select the media file and Bits is Extracted by using LSB technique then the text is extracted from the position and converted to Binary and Ascii Conversations Finally the desired Text is Extracted and decrypted from the audio file.

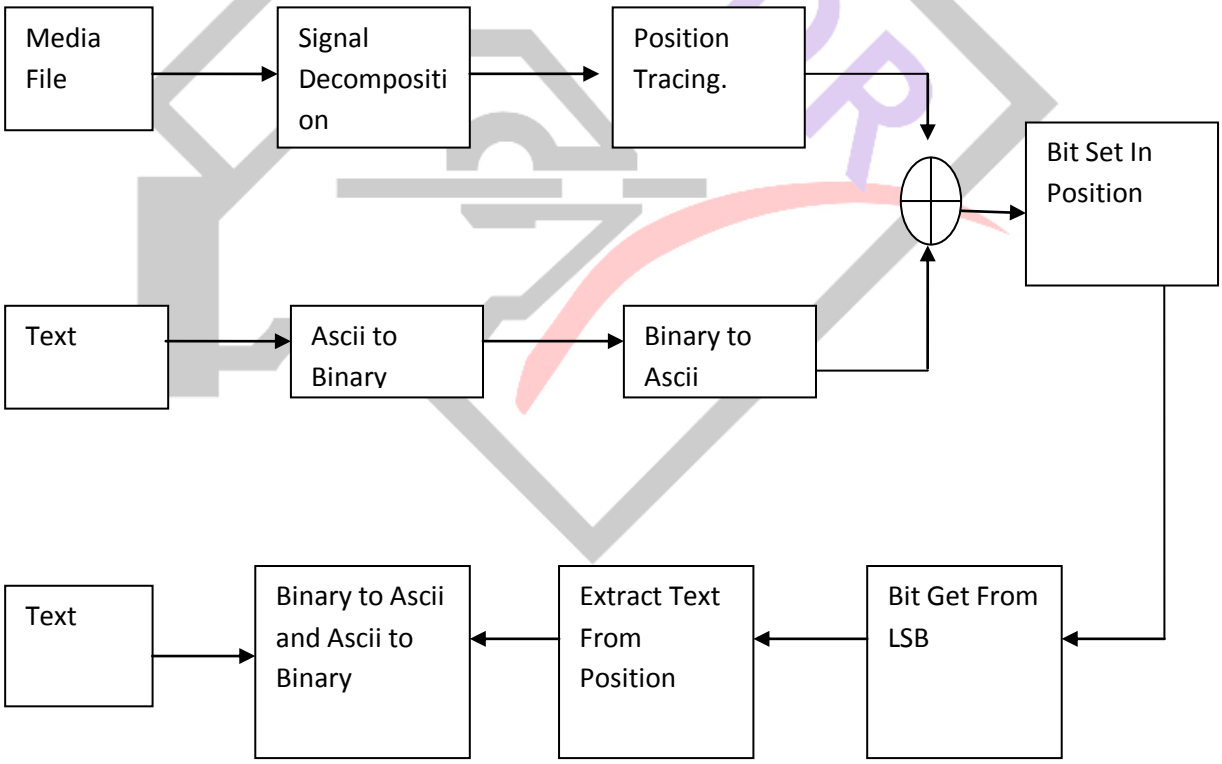

Fig 3.1. Block diagram showing the process of execution

Algorithm & Training:

Step 1: select desired(.WAV), read the designed wavelet and play select desired speech signal
Step 2: select the embedded speech signal(.WAV), read and play selected embedded signal
Step3: select the desired speech signal(.WAV), read and play selected embedded signal
Step 4: The above signals applied Discreate Wavelets Transformation with the name of wavelet "haar".
Step 5: Extract Positions in signal.
Step 6: Enter the string, Encode the string.

Step 7: From LSB position insert the data into signal.
Step 8: Reconstruct the signal by using IDWT.
Step 9: Read the reconstructed stegno-signal
Step 10: Apply DWT using "haar", Extract Positions and Extract data from positions.
Step 11: Decode data which was stegnified.

Finally our goal is to execution while applying DCT is high Compared with DWT and the result of accuracy is also high in DWT while reconstructing the data that is hidden.

Embedding phase

The embedding phase contains, loading the wav file, transform the audio file into the frequency domain using Wavelet transform, and ciphering text message by using DES.

Load Wave file

Firstly, the wave file content is loaded; it consists of header and data section. Header contains information about the audio file attributes (like, sample rate, no. of channels, bits per channel ...etc), while the data section holds the values of audio samples within the wave. In this paper the number of samples are 11024 sample/sec, the number of channel is one (mono), and the number of bits in each sample is 8 bits.

Wavelet Transform

Wavelet transform was used as a cover to hide secret text message in frequency domain. The use of frequency domain instead of spatial domain, adds more robustness to the hiding process. Haar filter is selected for wavelet transform. The Haar Wavelet is a simplest and the fast wavelet transformation, which operates on data by calculating the sums and the differences of the adjacent elements. Only one wavelet pass is applied; which leads to two sub bands (i.e., low and high). High frequency coefficients are treated as the host for the secret bit, while the low coefficients are kept unchanged.

Encryption text Message

The encrypted text message will be hidden in Audio, encrypt by Data Encryption Standard (DES) method. At beginning converting the message into ASCII code, making the 64 bits blocks of the message, generating an encryption key, and performing permutations and logical operations to bit pattern the following steps shows the process of DES algorithm. After encryption the text message using DES method, the message convert it into ASCII code, and transform the audio file form time domain to frequency domain by Haar wavelet transform. We take the high frequency coefficient for hiding the secret message by using the LSB (Least Significant Bit) algorithm. And after bits embedding, the audio file transformed back to spatial domain using inverse Wavelet transform.

Extraction Phase

The Extraction Phase contains, decrypt the hidden message, and take the inverse of wavelet transform.

Decrypt the Message

Decryption is simply the inverse of encryption, following the same steps as mentioned in, but reversing the order in which the sub keys are applied.

IV. CONCLUSION

The main aim is to come up with a technique to hide the data in audio file in such a way there are no perceivable changes in the audio file after the message insertion. Also, if the message that is to hidden was also encrypted then the level of security would be further raised to a more satisfactory level. The person who got the message would only have the encrypted form of the message with no way of decrypting it so the hidden messages were to be discovered. Proposed scheme has been discussed in this paper for embedding text in cover audio file. Emphasis is on proposed scheme from simple LSB based data hiding in audio, and their robustness in term of steganolys is. Proposed method is better by using the concept of DWT (Discrete Wavelet Transform) and LSB technique.

REFERENCES

1. New Design for Information Hiding with in Steganography Using Distortion Techniques. Hamid.A.Jalab, A.A.Zaidan, B.B.Zaidan ,IACSIT International Journal of Engineering and Technology Vol. 2, No.1, February, 2010.
2. Bidyut S; Kunal K. and Arun, 2013. Digital Image Encryption using ECC and DES with Chaotic Key Generator, IJERT, 2 (11):1-10
3.Steinbuch, M. Van de Molengraft and M.J.G, 2005. Wavelet Theory and Applications, a Literature Study, Eindhoven University of Technology, 53(7):53.
4.Steganography in Audio Using Wavelet and DES Rasha H. Ali*Vol.12(2)2015
5. Humanth Kumar, M.Shareef, R. P. Kumar, "Securing Information Using Steganography", IEEE Xplore International Conference on Circuits, Pwer and Computing Technologies, March 2013, pp. 1197- 1200.
6.Audio Steganography in Discrete Wavelet Transform Domain International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 16 (2015)

7. Doshi, R., Jain, P., and Gupta, L., 2012, "Steganography and its Applications in Security", International Journal of Modern Engineering Research (IJMER), 2(6).
8. Weeks, M., "Digital Signal Processing Using MATLAB and Wavelets", Pearson publications, ISBN – 81-297-0272-X.
9. Verma, S. S., Gupta, R., and Shrivastava, G., 2014, "A Novel Technique for Data Hiding in Audio Carrier by Using Sample Comparison in DWT Domain", IEEE conference, pp 639-643.
10. Dieu, H. B. andHuy, N. X., 2014, "An Improved Technique for Hiding Data in Audio", IEEE conference, pp 149-153.
11. Elshazly, A. R., M. M. Fouad, and M. E. Nasr. "Secure and robust high quality DWT domain audio watermarking algorithm with binary image." Computer Engineering & Systems (ICCES), 2012 Seventh International Conference on.IEEE, 2012.