A DCT-DWT Combined Approach for Audio Steganography

Dipali Junankar[1], Ashita Agrawal[2], Ratnashree Chavan[3], Srujana Palagiri[4]

[1]*Professor, Dept of Computer Engineering, New Horizon Institute of Technology and Management, Maharashtra, India*
[2,3,4]*New Horizon Institute of Technology and Management, Maharashtra, India*

Abstract - *Steganography is an art and a science of communicating in a way, which hides the existence of the communication. It is also called as "covered writing", because it uses a "cover" of a message for sending any important secret message. In the steganographic scenario, the secret data is first concealed within another object which is called "cover object", to form "stego-object" and then this new object can be transmitted or saved. Using different techniques, we can send secret data in the form of an image, a music file or even a video file by embedding it into the carrier, forming a stego-signal. At the receiver's end, the secret data can be recovered from the stego-signal using different algorithms. The main goal of Steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It not only prevents others from knowing the hidden information, but it also prevents others from thinking that the information even exists. Audio steganography is the scheme of hiding the existence of secret information by concealing it into audio file. This project is the software developed to embed an audio file in another audio signal. It is concerned with embedding information in an innocuous cover Speech in a secure and robust manner. This system makes the files more secure by using the concept of Steganography. The proposed steganographic method can provide a high information hiding capacity and successfully increase the security.*

Key Words: **Discrete Wavelet Transformation (DWT), Discrete Cosine Transformation (DCT), Audio Steganography, Data Hiding, Peak Signal to Noise Ratio**

1. INTRODUCTION

Steganography is an art and a science of communicating in a way, which hides the existence of the communication. It is also called as "covered writing", because it uses a "cover" of a message for sending any important secret message. Steganography serves as a means for private, secure and sometimes malicious communication. Steganography is the art to hide the very presence of communication by embedding the secret message into the innocuous looking cover media objects, such as images using the human's visual, aural redundance or media objects' statistical redundance. [1]

Steganography is a powerful tool which increases security in data transferring and archiving. In the steganographic scenario, the secret data is first concealed within another object which is called "cover object", to form "stego object" and then this new object can be transmitted or saved. Using different techniques, we can send secret data in the form of an image, a music file or even a video file by embedding it into the carrier, forming a stego-signal. At the receiver's end, the secret data can be recovered from the stego-signal using different algorithms. [1]

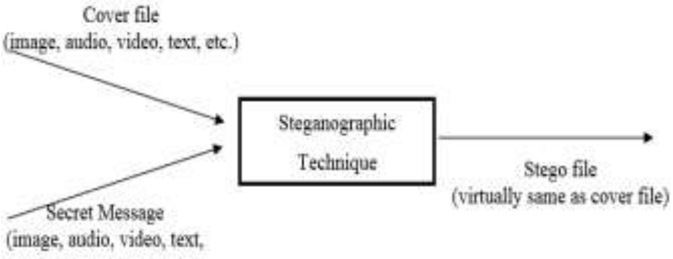

Cover file
(image, audio, video, text, etc.)
Steganographic Technique
Stego file
(virtually same as cover file)
Secret Message
(image, audio, video, text,

Fig -1: Fundamental process of Steganography

2. AUDIO STEGANOGRAPHY

The technique of steganography which embeds secret messages into digital sound is called "Audio Steganography". The process is usually more difficult than embedding messages in other media like image or video. Audio Steganography methods can embed any messages in sound files. In Audio Steganography system, secret messages are embedded into digitized audio signal which results into altering binary sequence of corresponding audio files. Audio steganography techniques are lesser prone to malicious attacks because many attacks which are malicious against image steganography algorithms like geometrical distortion, spatial scaling cannot be implemented against audio steganography schemes. Audio steganography in particular addresses key issues brought about by the P2P software, MP3 format, and the need for a secure broadcasting scheme that can maintain the secrecy of the transmitted information, even when passing through insecure channels. [2]

The information hiding process consists of following two steps.
i. Identification of redundant bits in a cover-file. Redundant bits are those bit that can be modified without corrupting the quality or destroying the integrity of the cover-file.
ii. To embed the secret information in the cover file, the redundant bits in the cover file is replaced by the bits of the secret information.

3. RELATED WORK

The biggest problem in steganography is the size of the file we embed into. For instance, if we take a message of n length then, the no of samples in the audio has to be greater than the length of the message in order to encode the bits in audio file.

The existing system of Audio Steganography poses more restrictions on the choosing of audio files. User can select only wav files to encode. Further embedding information into sound files is generally considered more difficult than images; according to the human ear is extremely sensitive to perturbations in sound and can in fact detect such turbulence as low as one part in 10 million. The four methods discussed further provide users with a large amount of choice and makes the technology more accessible to everyone.

There are various domains of information hiding i.e. spatial domain, transform domain and spread spectrum domain. In spatial domain methods a steganographer modifies the secret data and the cover medium in the spatial domain, which is the encoding at the level of the LSBs. LSB encoding, is extremely sensitive to any kind of filtering or manipulation of the stego-image. Scaling, rotation, cropping, addition of noise, or lossy compression to the stego-image is very likely to destroy the message. Furthermore an attacker can easily remove the message by removing (zeroing) the entire LSB plane with very little change in the perceptual quality of the modified stego-image. The information hiding Steganography techniques are based on following transforms such as:
1. Discrete Fourier Transform (DFT)
2. Discrete Cosine Transform (DCT).
3. Discrete Wavelet Transform (DWT)
4. Singular Value Decomposition (SVD) Transform
5. Discrete Hadamard Transform (DHT)
These techniques are independent of an image format and can hide data in more significant areas of the transformed image. [3]

4. PROPOSED WORK

The purpose of this project is to develop a hybrid system using two types of transformation techniques for hiding binary data in the audio. In the design phase of the proposed system the following two basic requirements have been taken into consideration: the first one is the perceptual transparency, and the second is the high embedding capacity. This first requirement is important to make cover object and stego cover object perceptually indiscernible, while the second is to ensure high hiding.

In this transform based hiding system both Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) have been utilized, in a hybrid way, to get better hiding rate with low perceptual changes in cover media. The above mentioned idea of using transformation in the proposed system is due to the results of previous published works which indicated that hiding in frequency domain is more effective than hiding in time domain, due to the compactness attributes of some transforms.

This proposed method provides greater security and it is an efficient method for hiding the secret information from hackers and sent to the destination in a safe and undetectable manner. This proposed system also ensures that the size of the file is not changed even after encoding and it is also suitable for any type of audio file format.

The proposed system consists of two modules: Sender module and Receiver module. The Sender module is used to hide the secret massage in cover audio file, and the Receiver module is used to retrieve the secret message from stego-cover audio file.

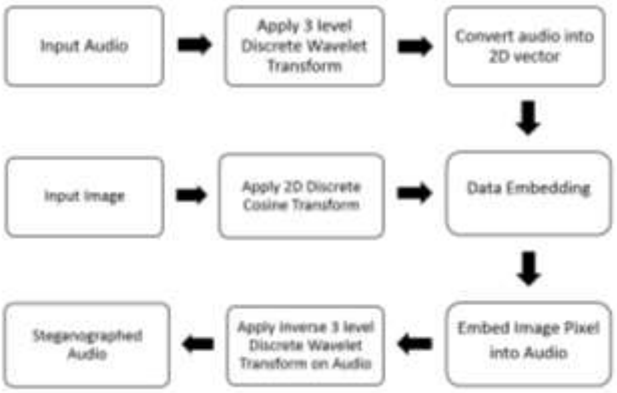

Input Audio
Apply 3 level Discrete Wavelet Transform
Convert audio into 2D vector
Input Image
Apply 2D Discrete Cosine Transform
Data Embedding
Steganographed Audio
Apply inverse 3 level Discrete Wavelet Transform on Audio
Embed Image Pixel into Audio

Fig -2: Proposed Sender Side Block Diagram

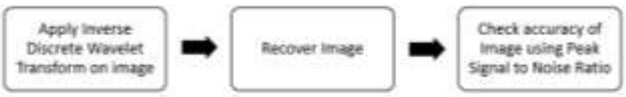

Apply inverse Discrete Wavelet Transform on image
Recover Image
Check accuracy of image using Peak Signal to Noise Ratio

Fig -3: Proposed Receiver Side Block Diagram

4.1 Discrete Cosine Transform (DCT)

The discrete cosine transform (DCT) represents an image as a sum of sinusoids of varying magnitudes and frequencies. The DCT has the property that, for a typical image, most of the visually significant information about the image is concentrated in just a few coefficients of the DCT. For this reason, the DCT is often used in image compression applications. DCT is used in the JPEG image compression algorithm. The input image is divided into 8-by-8 or 16-by-16 blocks, and the two-dimensional DCT is computed for each block. The DCT coefficients are then quantized, coded, and transmitted. The JPEG receiver (or JPEG file reader) decodes the quantized DCT coefficients, computes the inverse two-dimensional DCT of each block, and then puts the blocks back together into a single image. For typical images, many of the

DCT coefficients have values close to zero. These coefficients can be discarded without seriously affecting the quality of the reconstructed image.

The two-dimensional DCT of an M-by-N matrix A is defined as follows:

$$B_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} A_{mn} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le p \le M-1 \\ 0 \le q \le N-1 \end{matrix}$$

$$\alpha_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \quad \alpha_q = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases}$$

The values B_{pq} are called the DCT coefficients of A. The DCT is an invertible transform, and its inverse is given by:

$$A_{mn} = \sum_{p=0}^{M-1}\sum_{q=0}^{N-1} \alpha_p \alpha_q B_{pq} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N}, \quad \begin{matrix} 0 \le m \le M-1 \\ 0 \le n \le N-1 \end{matrix}$$

$$\alpha_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \quad \alpha_q = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases}$$

4.2 Discrete Wavelet Transform (DWT)

The Wavelet Transform (WT) is a technique for analyzing signals. It was developed as an alternative to the short time Fourier Transform (STFT) to overcome problems related to its frequency and time resolution properties. More specifically, unlike the STFT that provides uniform time resolution for all frequencies the DWT provides high time resolution and low frequency resolution for high frequencies and high frequency resolution and low time resolution for low frequencies. In that respect it is similar to the human ear which exhibits similar time-frequency resolution characteristics.

The Discrete Wavelet Transform (DWT) is a special case of the WT that provides a compact representation of a signal in time and frequency that can be computed efficiently.
The DWT is defined by the following equation:

$$W(j,k) = \sum_j \sum_k x(k) 2^{-j/2} \psi(2^{-j} n - k)$$

where y (t) is a time function with finite energy and fast decay called the mother wavelet. The DWT analysis can be performed using a fast, pyramidal algorithm related to multirate filterbanks.

5. REQUIREMENTS

The requirement for this project is mentioned as below;

5.1 Software Requirement

MATLAB R2015b: MATLAB is a scientific programming language and provides strong mathematical and numerical support for the implementation of advanced algorithms. It is for this reason that MATLAB is widely used by the image processing and computer vision community. New algorithms are very likely to be implemented first in MATLAB, indeed they may only be available in MATLAB.

5.2 Hardware Requirement

- Windows 7 or latest version
- 4/8 GB RAM
- Pentium 4 + Processor
- 100 GB free Hard Disk

6. PERFORMANCE ANALYSIS

The performance of the proposed technique is analyzed based on peak signal to noise ratio.

6.1 Peak Signal to Noise Ratio (PSNR)

Peak Signal to Noise Ratio (PSNR) represents peak error, the lower the MSE and higher the PSNR values indicates that the stego image quality is better than original. Image quality is observed using PSNR. Generally higher value of PSNR indicates that reconstructed image is of high quality. The PSNR between two images having 8 bits per pixel or sample in terms of decibels (dBs) is given by:

$$\text{PSNR} = 10 \log_{10} [\text{Max}^2/\text{MSE}]$$

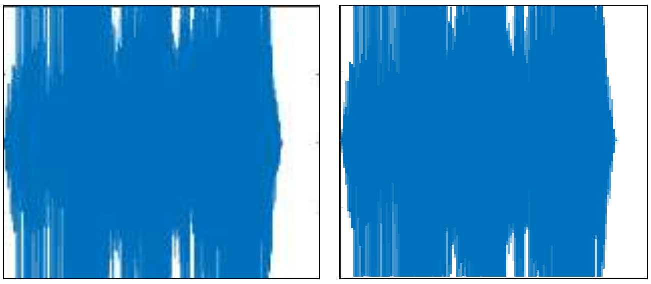
Where,
MAX^2 = Max value of pixels in Original image
MSE = Mean Square Error

7. RESULT

Below are the results obtained after the implementation in MATLAB.

7.1 Original Audio and Encrypted Audio

Original audio is cover audio before encryption and encrypted audio is cover audio with secret data hidden. The difference between these audio wave files cannot be identified with naked eyes or by human ear.



Original Audio Encrypted Audio

Fig -4: Original Audio and Encrypted Audio

7.2 Original Image and Received Image

Original image is image before encryption and received image is image after extraction. The PSNR ratio received was high and the accuracy was achieved.

Original Image Received Image

Fig -5: Original Image and Received Image

8. APPLICATIONS

Some common applications of steganography are mentioned below:

- Secret communication: Some people may use information hiding in order to hide data and be in confidential communication.
- Secure storage: Many types of sensitive information such as medical records of patients or prescription drug information need security during transmission because in case those are accessible for unauthorized person could lead to illegal activities as identity theft as well as insurance fraud. It can be embedded in audio files
- Copy right protection: While a considerable portion of economic resources is dedicated to the creation of intellectual property, particularly in industrial societies, the cost of reproducing such intellectual creations typically constitutes only a small fraction of the creation. In the copy right protection, a watermark which contains the information of the owner is embedded into the host media. The watermark is supposed to be robust and enables the owner to prove his ownership in case is needed.

9. CONCLUSIONS

Steganography is not intended to replace cryptography but rather to supplement it. If a message is encrypted and hidden with a steganographic method it provides an additional layer of protection and reduces the chance of the hidden message being detected. Steganography is still a fairly new concept to the general public although this is likely not true in the world of secrecy and espionage.

Many currently used technologies are not strong enough to prevent the embedded data detection and removal. The use of benchmarking techniques become more common, the need for a more robust standard definition, in order to help overcome this. While studying audio Steganography it was found that lot of work already done on this technique. Text, video, Image, audio can hide inside the audio and one can use audio as a cover file and also as a secret message but did not get anything done on encrypted images.

Here we have tried to perform audio steganography using encrypted image (encrypted using DCT). The results prove that most of the images are having PSNR more than 40 which shows that the loss in the image data is quite low.

REFERENCES

[1] Audio Steganography Using Discrete Wavelet Transformation (DWT) & Discrete Cosine Transformation (DCT), IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. V (Mar – Apr. 2015), PP 32-44 www.iosrjournals.org

[2] A Comparative Study of Audio Steganography Techniques, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 p-ISSN: 2395-0072, Volume: 03, Issue: 04, Apr-2016, PP 580 -585 www.irjet.net

[3] A Discrete Wavelet Transform: A Steganographic Method for Transmitting Images, International Journal of Computer Applications (0975 – 8887), Volume 129 – No.5, November 2015 .

[4] An Improved DCT based Steganography Technique, International Journal of Computer Applications (0975 – 8887), Volume 102– No.14, September 2014