Effective Audio Steganography by using Coefficient Comparison in DCT Domain

Miss Preeti Jain, Prof.Vijay Trivedi
[1] M-Tech (Computer science and engineering), LNCT, M.P. (Bhopal), India
[2] Prof. (Computer science and engineering), LNCT, M.P. (Bhopal), India

Abstract

Steganography has been proposed as a new alternative technique to enforce data security. Lately, novel and versatile audio steganographic methods have been proposed. A perfect audio Steganographic technique aim at embedding data in an imperceptible, robust and secure way and then extracting it by authorized people. We have presented a high capacity and high stego-signal quality audio steganography scheme based on Coefficient comparison in DCT 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. The entire proposed system is simulated and their corresponding waveforms prove the effectiveness of this method.

Keywords: Steganography, Audio Steganography, DCT Domain.

1. Introduction

The rapid growth in digital data usage in many real life applications has urged new and effective ways to ensure their security. Efficient secrecy can be achieved by implementing cryptography, watermarking, or steganography techniques [1]. Cryptography techniques are based on rendering the content of a message garbled to unauthorized people. In watermarking, data are hidden to convey some information about the cover medium such as ownership and copyright. Whereas Steganography is a process ofembedding secret messages in a cover signal to avoid illegaldetection [2]. Steganography differs from cryptographyinterm of message visibility. It hides secret messages totallycompared to cryptography where the secret message is stillvisible [3].

Steganography is mostly used in secretcommunication like military and governmentcommunications. Often it requires relatively high payloadswhen compared to watermarking. The major requirementsthat should be satisfied for good steganography algorithmsinclude perceptual transparency, payload or capacity androbustness [4]. High capacity is considered as an importantaspect for steganography when compared to watermarking. For watermarking, robustness should be a dominant factor. Improvement for one of the mentioned requirements willtend to degrade the other performances as they arecontradictory according to the magic triangle [5].In recently years many techniques have been developedfor information hiding [6, 7, 8], and most of thesetechniques used either image and video media but rarely useaudio signal as a cover signal especially in high rate of dataembedding, most likely due to Human Auditory System(HAS) which is more sensitive compared to the HumanVisual System (HVS) [8]. Although adopting audio signalsas a cover signals may yield inferior inaudible performance,there are still suitable features such as transitory andunpredictability that makes sound signal as a suitable securecover signal.

2. Related Work

Generally audio steganography can be classified according to the embedding domain either in time or transform domain. The simplest message hiding technique in time domain with acceptable capacity is the Least Significant Bits (LSB), but it is vulnerable due to changes in LSB that can possibly destroy the embedded message [9]. In the transform domain, there are many transform methods that can be employed in information hiding such as Fourier domain [9,10], discrete cosine domain [9, 11], and wavelet domain [8,9, 12, 13]. Each domain has its features in signal processing and information hiding.

The discrete cosine transform is a technique for converting a signal into elementary frequency components [14]. The DCT can

be employed on both one-dimensional and two dimensional signals like audio and image, respectively. The discrete cosine transform is the spectral transformation, which has the properties of Discrete Fourier Transformation [14]. DCT uses only cosine functions of various wave numbers as basic functions and operates on real valued signals and spectral coefficients. DCT of a 1-Dimensional (1-d) sequence and the reconstruction of original signal from its DCT coefficients termed as inverse discrete cosine transform (IDCT).

Some of the properties of DCT are de-correlation, energy compaction, reparability, symmetry and orthogonally [15]. DCT provides inter pixel redundancy for most of natural images and coding efficiency is maintained while encoding the uncorrelated transformation coefficients [15]. DCT packs the energy of the signal into the low frequency regions which provides an option of reducing the size of the signal without degrading the quality of the signal.

The Discrete Cosine Transform (DCT) decomposes a signal into two components, high and low frequency components. Most power of the input signal is concentrated in low frequency component called DC signal, while little power exists in the high frequency component or known as a AC signal. The reconstruction of original signal is performed by the Inverse Discrete Wavelet Transform (IDWT).The modification in the AC component little effect onthe reconstructed signal, However modification in the DC component or low frequency component may affect significantlythe reconstructed signal. Therefore using ACcomponents as acover for information embedded process enable highpayload and an acceptable quality, when it is used in thesteganography [8]. However, information embedding in ACcomponent can affect its robustness as it is possible toremove a secret message by signal processing for examplean attacker may reset the AC coefficients.

In this work we described a high capacity and high quality audio steganography algorithm. The purpose of this algorithm is to achieve a high embedding capacity and high output quality. The proposed algorithm has high embedding capacity reaches up to 4 kb/sec and high quality for output stego-signal (SNR above 50 dB). Another advantage for this 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 proposed algorithm starts by segmenting the input audio cover signal and then decomposing each segment by using DCT; one represents the DC signal that has the highest power and lowest frequency, while the others are AC signals with decreasing power, starting from the lowest to the highest frequencies details components. Subsequently after several steps, the Inverse DCT (IDCT) is used to reconstruct the output stego signal.

The proposed scheme however does not use the DC signal in embedding process to maintain the quality of output of stego-signal.

The remainder of the paper is organized as follows:

Section 3 introduces the block diagram and stepsfor 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.

3. Proposed Algorithm

3.1AtSender Side:

Input: A Cover Audio Signal ***X*** and Message ***M***

Output: A StegoSignal ***Y***.

1. 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.
2. 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.

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

3. Let the input cover signal consists of ***R*** samples, this signal is divided into two parts: Used part***A***and Unusedpart***B***. used part consists of those samples that participated in message hiding system. Rest of the samples iscalled unusedpart.Next, Used part is converted

into segments of size same as size of message bits that is ***N*** segments; each segment has length of ***Z*** samples.

[***A, B***]=*Segment*(***X***);

4. Apply DCT function on each segment of ***A*** which produces segments in frequency domain. in each segment one represents the DC signal and the others represent AC signals i.e.

```
For i=1: N
        D(i)=DCT(A(i));
end
```

5. Secret message embedding stage is based on comparison of two samples in a segment. For each segment execute the following code.

```
If(C (i)= =0)
        If(D (i,p)<D (i,q))
                Swap(D (i,p),D (i,q));
        else if(D (i,p)= =D (i,q))
                D (i,p)=D (i,p)+k/2;
                D (i,q)=D (i,q)-k/2;
        end
else if(C (i)==1)
        if(D (i,p)>D (i,q))
                swap(D (i,p),D (i,q));
        else if(D (i,p)==D (i,q))
                D (i,p)=D (i,p)-k/2;
                D (i,q)=D (i,q)+k/2;
        end
end
```

Here, the sample p and q is selected by user choice and value of k is selected as small as possible.

6. Next, all the modified segments, are converted back from frequency domain to time domain. The *IDCT* is used to reconstruct the segments of stego- signal based on modified AC samples and unmodified DC samples.

```
For i=1: N
        A(i)=IDCT(D(i));
  End
```

7. At last, the reconstructed segments will fed to segment collecting step to reconstruct the final steganography algorithm output. i.e.

Y=*Reconst (**A,B**);*

8. ***End***

3.2. At Receiver Side:

Input: A Stego Audio Signal ***Y***

Output: Message ***M***

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

2. Again the stegosignal ***Y***isdivide 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. i.e.

[***A, B***]=*Segment*(***Y***);

3. Apply DCT function on each segment of ***A*** which produces segments in frequency domain. In each segment one represents the DC signal and the others represent AC signals.

```
For i=1: N
        D(i)=DCT(A(i));
End
```

4. 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. i.e.

```
if(D(i,p)>D(i,p))
        C(i)=0;
else if(D(i,p)< =D(i,p))
        C(i)=1;
else
        error ("Stego Signal is currpted");
end
```

5. Convert the Cipher Message ***C*** into original Secret Message **M** by using secret key cryptography with key size same as size of message bit. i.e.

$$M = Decrypt\ (C, K);$$

6. END

Figure 1 presents the block diagram of proposed message hiding system .the input of this message hiding system are audio file as cover signal and text message which is to be embedded into cover signal. The output of proposed system is stego audio cover file in which message is hidden.

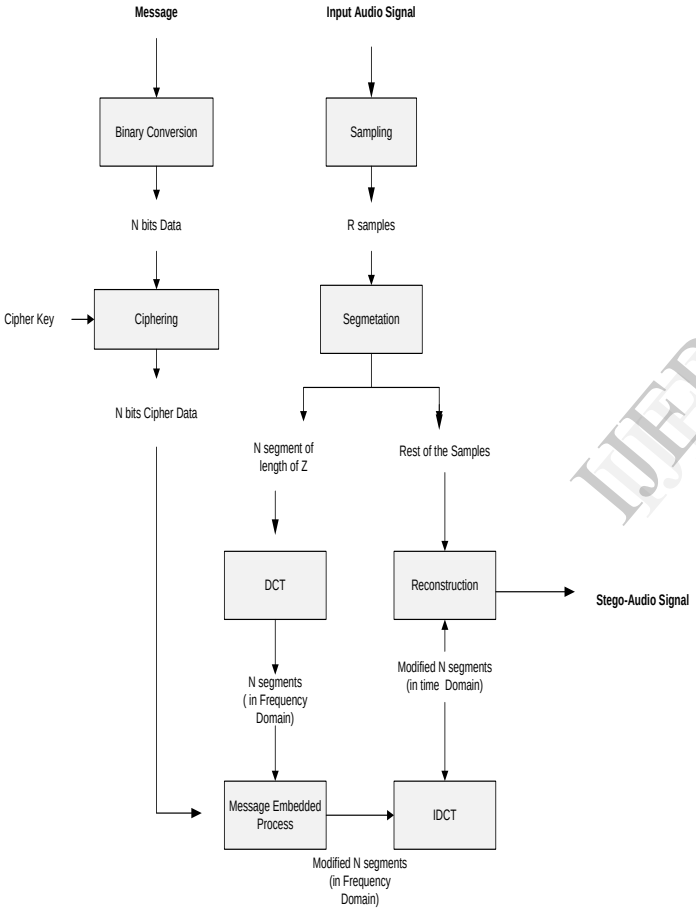

Figure 1the General Structure of the Proposed Hiding Scheme

Figure 2 presents the block diagram of proposed message Recovery system, here the input is the stego signal in which data is hidden and output is the recovered message from the input stego file.

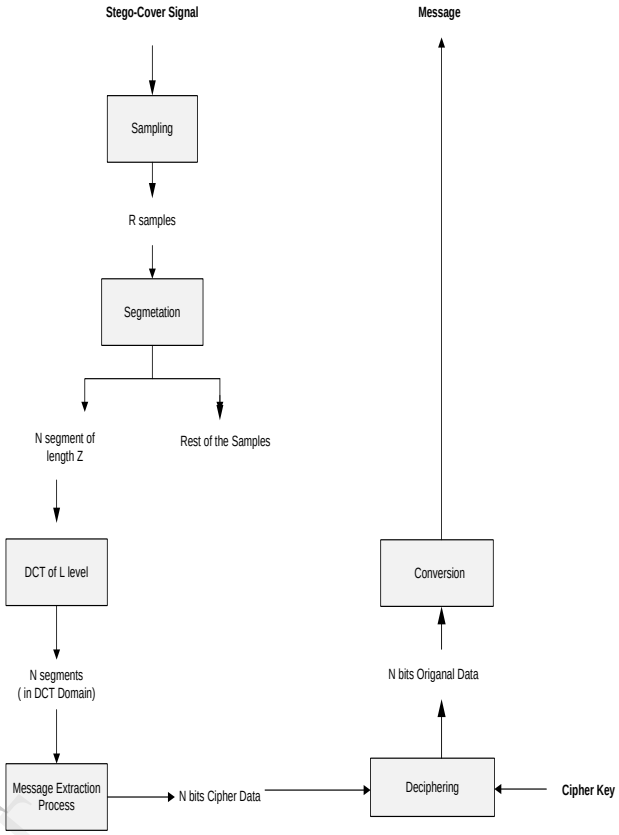

Figure 2 Block diagram of the Message Recovery Algorithm

4. Evaluation Metrics

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 Signals-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.

5. Experimental result

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

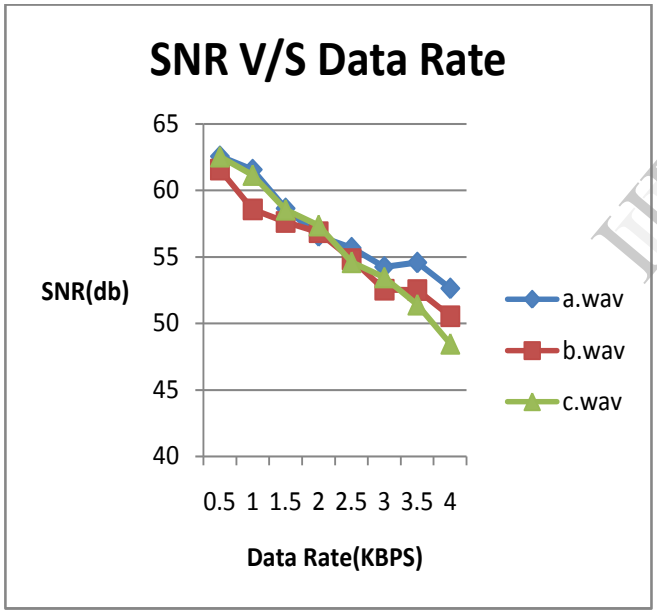

Figure 3 the Relationship between SNR and Embedding Capacity forDifferent Cover Signals and different Data Type

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 34600respectively and text file as a secret message with size of 4kb . The results in table shows that using the 4th and 5th 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 of4 kb/sec

Cover Signal	Segment	Segment	Output	Processing
a.wav	4	5	55.34	1.31
	3	6	54.65	1.24
	2	7	52.56	1.86
b.wav	4	5	58.43	1.45
	3	6	56.56	1.54
	2	7	54.42	1.22
c.wav	4	5	54.65	1.45
	3	6	53.32	1.78
	2	7	52.55	1.67

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 DWT scheme in high embedded capacity, the SNR is above 50 dB in our algorithm while it is in range of21 dB in conventional DWT scheme for different data type messages.

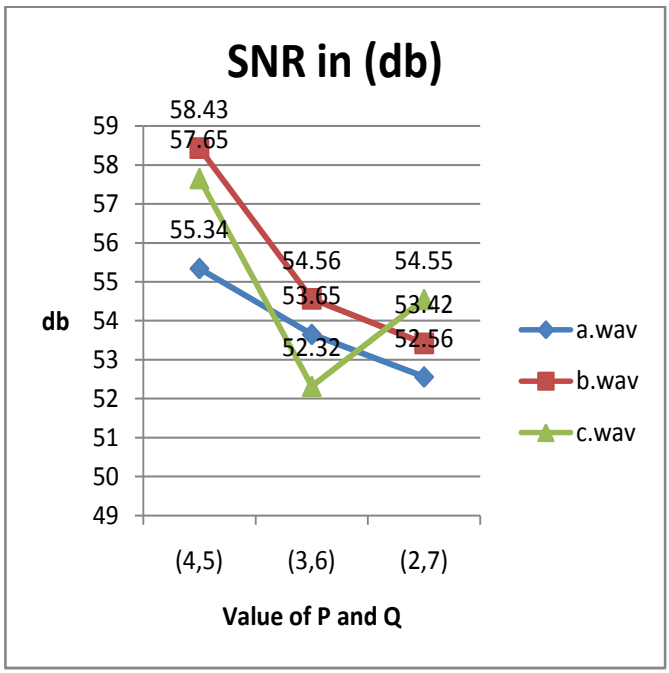

Figure 4 Comparison graph for different cover signals with respect to SNR on different P and Q value

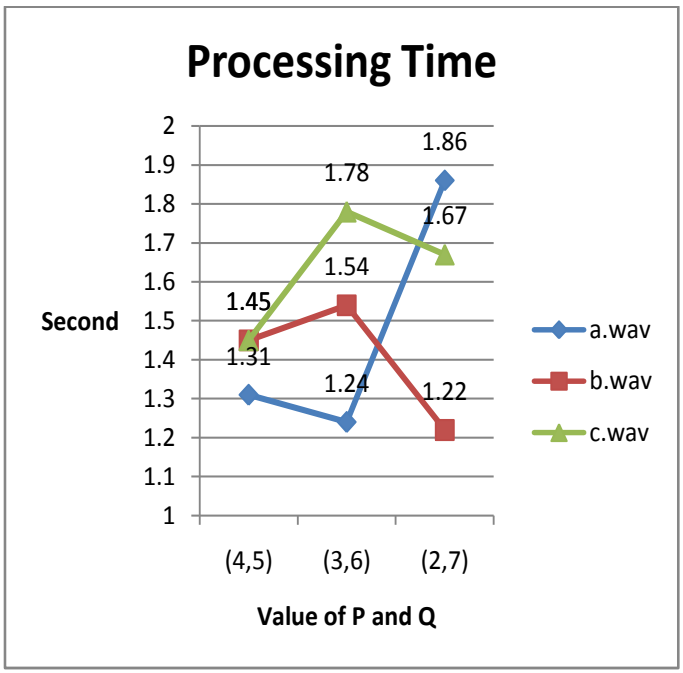

Figure 5 Comparison graph for different cover signals with respect to SNR on different P and Q value

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 DWT scheme in high embedded capacity, the SNR is above 50 dB in our algorithm while it is in range of21 dB in conventional DWT scheme for different data type messages.

6. Conclusion

We have presented a high capacity and high stego-signal quality audio steganography scheme based on samples comparison in DCT domain where two samples 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. 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 50 dB for the output signal.

The proposed algorithm was implemented by using Matlab (2009a) programming. The proposed algorithm was tested using three audio cover signals: male speaker, female speaker and music called a.wav, b.wav and c.wav respectively. Each signal has resolution of 8 bits per sample and sampling frequency 11025 samples/sec and text are used in tests as secret messages. The quality of output signal in each test was computed using SNR.In future we will modify and improve this technique so that more data can be embedded into cover signal.

Reference

[1]. Walter Bender, Daniel Gruhl, Norishige Morimoto, Anthony Lu, "Techniques for Data Hiding", *IBM Systems Journal*, vol.35, no. 3 and 4, pp. 313-336, 1996.

[2]. N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," *IEEE Security and Privacy Magazine*, Vol. 1, No. 3, June 2003, pp. 32–44.

[3]. H. Wang, and S. Wang, "Cyber warfare: Steganography vs. Steganalysis," *Communications of the ACM magazine*, Vol. 47, No.10, October 2004, pp. 76-82.

[4]. Y. Wang; P.Moulin, "Perfectly Secure Steganography: Capacity, Error Exponents, and Code Constructions," *Information Theory IEEE Transactions*, Vol. 54, No. 6, Jun 2008, pp. 2706 – 2722.

[5]. N. Cvejic,"Algorithms for Audio Watermarking and Steganography," MSc. thesis, Department of Electrical and Information Engineering, Information Processing Laboratory, University of Oulu, Finland Oulu, Finland, 2004.

[6]. K. Bailey, and K. Curran, "An Evaluation of image based Steganography methods," *Journal of multimedia Tools and Applications*, Vol. 30, No. 1, July, 2006, pp. 55-88.

[7]. N. Meghanathan, and L. Nayak. "Steganalysis algorithms for detecting the Hidden information in image, audio and Video cover media," *International Journal of Network Security &Its Application* (IJNSA), Vol.2, No.1, January 2010, pp. 43-55.

[8]. S. Shahreza and M. Shalmani, "High capacity error free wavelet Domain Speech Steganography," *IEEE International conference on acoustics, speech, and signal processing*, March 31 -April 4, 2008, pp. 1729 – 1732.

[9]. N. Cvejic,"Algorithms for Audio Watermarking and Steganography," MSc. thesis, Department of Electrical and Information Engineering, Information Processing Laboratory, University of Oulu, Finland Oulu, Finland, 2004.

[10]. A. Khashandarag, A. Oskuei, H. Mohammadi and M. Mirnia, "A Hybrid Method for Color Image Steganography in Spatial and Frequency Domain," *IJCSI International Journal of Computer Science* Issues, Vol. 8, Issue 3, No. 2, May 2011, pp. 113-120.

[11]. Z. Zhou, and L. Zhou "A Novel Algorithm for Robust Audio Watermarking Based on Quantification DCT Domain," *Third International Conference on International Information Hiding and Multimedia Signal Processing*, vol. 1, 26-28 November, 2007, pp. 441-444.

[12]. S. Wu, J. Huang, D. Huang and Y. Q. Shi, "A Self-Synchronized Audio Watermarking in DWT Domain, "Circuits, Vol. 5, 23-26 May 2004, pp. 712-715.

[13]. N. Cvejic, and T. Seppanen, A Wavelet Domain LSB Insertion Algorithm For High Capacity Audio Steganography," *Digital Signal Processing Workshop, 2002 and the 2nd Signal Processing Education Workshop.* Proceedings of 2002 IEEE 10th, 13-16 October 2002. , pp. 53-55.

[14]. A. B. Watson, "Image Compression Using the Discrete Cosine Transform,"Mathematical *Journal* , vol. 4(1), pp. 81-88, 1994.

[15]. S. Ali Khayam, "The Discrete Cosine Transform (DCT): Theory and Application," *Information Theory and Coding, Seminar 1 – The Discrete Cosine Transform: Theory and Application*, March 10, 2003.