A New Approach to Audio Wave Watermarking

Namrata G. Murumbekar
M. B. E. Society's College of Engineering, Ambajogai. Maharashtra

B. M. Patil
M. B. E. Society's College of Engineering, Ambajogai. Maharashtra

Vijay Chandode
M. B. E. Society's College of Engineering, Ambajogai. Maharashtra

ABSTRACT

There are different watermark embedding methods invented for digital media which contains lot of watermarking algorithms for text, image, audio, and video. In this paper focus is on audio watermarking part of digital media. Here we are describing a technique for embedding digital watermarks into digital audio signals. On audio wave signal apply quantization, LSB destruction, DCT and inverse of it. The key concept for proposed work is using the watermark from the original audio sample itself. The advantage of doing this is to avoid the excess raw data. The result of proposed work is compared with Noriega method, shows better performance for proposed work.

Keywords

Audio, Watermark, Wave.

1. INTRODUCTION

The distribution of digital media is becoming faster, easier and requiring less efforts to make exact replica of data, so there is need to find the solution for copyright issues like exact replica or duplication of data, plasticity of digital media [1]. A watermarking is a technique used to label digital media by hiding the copyright or other information in the underlying data. The watermark must be imperceptible. It should be robust to attacks and other types of distortions. In addition to this watermark should be unique, undetectable to users, and must satisfy the signal processing properties, security properties along with general properties of particular algorithm used in that technique. In considering the face of challenges derived from the characteristics of digital media and advanced internet facilities, digital watermarking has been proposed as a guideline to claim the ownership of source and owner. Audio watermarking algorithms are not easy to develop as human ears are the most sensitive organ to detect even a small amount of embedded noise, particularly when signal is low. Audio watermarking algorithms are comparatively few in number [2], [3], [4], [5], [6], [7], [8].

There are two groups of algorithms on the basis of embedding domain: one which embeds data by directly modifying pixel values of original image and other which embeds data by modulating the transform domain coefficients called as transform domain method. By altering values of certain frequencies from their original form and embedding the watermarks into transformed image is the basic concept of frequency-domain watermarking. Frequency domain watermarking is more robust than the spatial domain technique. DFT (Discrete Fourier Transform), DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet Transform) [9] are the common transforms used in frequency domain for watermarking purpose.

Patchwork watermarking algorithm for image [3], was not successful in audio watermarking applications. In succession, Arnold et al. [2], tried to improve the performance of Patchwork algorithm for audio in frequency domain. Arnold's algorithm also not very encouraging and needs to be refined further. Won and Kim came with modified patchwork algorithm (MPA) [8]. In [10], Watermark is generated by filtering a PN-sequence with a filter that approximates the frequency masking characteristics of the HAS (Human Auditory System).

In the proposed scenario we are randomly selecting some sample points from the original source audio and then applying techniques like quantization, DCT and LSB for generating watermarks which is to be embedded in that original source audio. Other methods use source sample, watermark and secret key independently, Instead of that, in this method all these contents are made in use only from source sample. Proposed method helps in avoiding algorithm complications, excess memory space and chance of identifying secret key information. This paper is organized as follows; A brief background about digital watermarking particularly audio watermarking described in section 2. The proposed technique for audio source watermarking is described in section 3. Section 4 shows the result analysis. Finally section 5 concludes the paper.

2. LITERATURE REVIEW

2.1 Digital Watermarking

Digital watermarking is a technique to hide secret information into the signals. It discourages unauthorized copying of data or attests the origin of media. Generally, a link between raw data and its corresponding information is established by watermark. On the basis of this the watermarks can be categorized in two different kinds; public and secret watermarks.

2.1.1 Secret watermark:

These watermarks are secured link, which works like authentication mechanism. The authorized person having knowledge about the secret can only be able to read the content. Invisible watermarking like simple text embedded into image or audio is a good example of this type. Our proposed method is a good example of secret watermarks.

2.1.2 Public watermarks:

These watermarks are easily readable by everybody. They act as an information carrier. It is mainly used to distinguish between original and duplicate data.

The watermark should be:

- Inaudible: Watermarked data must not be audible to sensitive human ears.
- Imperceptible: It should not affect the viewing experience of audio quality of original signal.
- Robust to deliberate attacks by pirates: To prevent unauthorized detection and removal by pirates it

should be difficult or even impossible to detect and remove watermarking signal belonging to same author.

- Robust to Lossy Data Compression: The watermark must have similar compression characteristics as the original signal. Compression/decompression technique is used for transmission and storage.
- Robust to Signal Manipulation and Processing Operations on the original data: We must able to retrieve the digital watermark even if, signal enhancement, noise, filtering, compression and cropping like signal processing operations are applied on it.
- Unambiguous: The procedure of watermark extraction should be known to owner only. The accuracy of identification of watermark should degrade gracefully in case of attack.
- Watermark should be directly embedded in the data, not in header.
- It should support multiple watermarking techniques.

The watermarking algorithm must have to satisfy at least two constraints which seem to be contradictory in nature i.e. Inaudibility and Robustness.

To retrieve the watermarks there are three different schemes; Non blind scheme requires watermarked audio signal, original audio and watermark key. For Semi blind scheme original audio signal and watermark key are required. There is no need of original audio signal in Blind scheme.

In our proposed method we are trying to implement non-blind watermarking scheme in order to do that we are producing the watermark from the original watermark audio signal itself.

2.2 The Watermarking Techniques

There are several watermarking techniques for text, image, audio and video data. Several digital watermarking techniques have been investigated for the study [10], [11], [8], [12].

2.2.1 The Watermarking Techniques for Text

Texts in the electronic version have both original and duplicate copies which are identical in nature. For embedding information inside a document simply one has to alter some of characteristics. This can be done either by text formatting or altering the characteristics of the characters. Problem in this is altering the characteristics will become visible to all including attackers. To solve this problem, alter the document in such a way that it is not visible to human eye and still can be possible to decode by computer. Encoder and decoder are the two components used for embedding and extracting the text respectively. A codebook having set of rules that tells the encoder which parts of the documents it need to change is one of the factor required for text watermarking. It also finds whether the marked documents are same or different. For applying text watermarks there are three proposed methods [13].

Line Shift Coding: As per this coding method, just shift the various lines inside the document up or down by small fraction as per rules present in the codebook. In this case change can be detectable when computer measures distance between each line but undetectable by human eye.

Word Shift Coding: Word shift coding also known as document justification. It operates on the same principle that of line shift coding only change is to shift the words from left to right or right to left. Codebook provides the guidelines to encoder about which of the words are to be shifted and where. During decoding, spaces between each word are measured by computer.

Feature Coding: In this coding technique document is passed through a parser. Parser is a program which examines the document and automatically builds a codebook for that document. The characteristics like height of characters, dots above i and j, and the horizontal line length of letters such as f and t are used to select which information is to hide. To hide information, features are separated and marked into the document. This technique can also be used with line and word shifting technique to increase the amount of data that can be hidden.

2.2.2 The Watermarking Technique for Image

Image watermarking can be applied in the transform domain [14] where values of selected frequencies can be altered, as in spatial domain watermarking. There is a greater tradeoff between invisibility and robustness. There are many algorithms on image watermarking in spatial domain [15]. One drawback of using spatial domain watermarks is the watermark can be eliminated by performing operation like cropping on picture [16].

Simple Watermarking: This technique involves addition of pattern like an image or logo on the top of an existing image; resulting an image containing both original image and logo, one on background and other on front respectively. Using the image editor it is possible to merge both images. This results into watermarked image with visible changes. Also the retrieval of pattern from the watermarked image is possible [13].

Least Significant Bit (LSB) Hiding: This is the easiest and surprisingly effective watermarking method for images. This method hides the MSB of one image using LSB of each pixel in another image. For better performance of LSB hiding technique the more bits used in the host image, the more it deteriorates. With the increase in number of bits used trough out this process, increases the clarity of secret image. It works well when both host and secret images are given equal priority. We have to compromise the quality of watermarked image if one image has significantly more space than other. In [17], hiding the watermark into cover signal by XOR operation and ITSAS (Integer Transform based Secure Audio Steganography) which uses LSB coding technique are implemented. In the proposed method we have embedded the watermark into first LSB. In future it can be further expanded to 2 LSBs, 3 LSBs up to 16 LSBs. To increase the robustness that is to decrease the embedding distortions generally we embed the watermark into higher LSBs.

Discrete cosine transform (DCT): DCT is one of the widely used linear transformations in digital signal processing. In this method, an image can be broken up into different frequency bands which make it easier to embed watermarking information into the middle frequency bands of an image. Choosing the middle frequency band in DCT is due to the fact that, much of the signal energy lies at low frequency band consisting the most important visual parts of image. “Figure 1” shows process of embedding the watermark invisibly, which can survive lossy data compressions. There is a reasonable tradeoff to embed the watermark into the middle frequency range of the image [18]. In DCT technique the middle frequency bands are selected in such a way that, they have minimized the chance of avoiding the most visual important parts of the image (low frequency) without over exposing themselves to removal through compression and noise attacks. DCT watermarking technique has resistance against the attacks such as noising, compression and filtering.

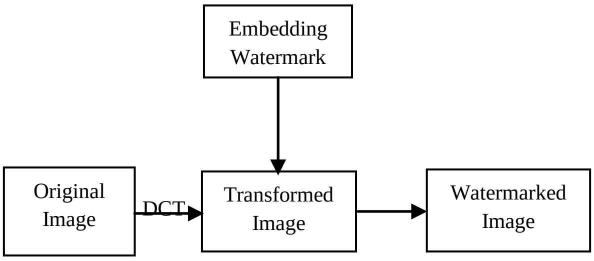

Fig 1: Watermark embedding in DCT

DCT works as: First the image is split up into 8×8 squares, and then each square is transformed via DCT. Next the quantizer rounds each of those coefficients, which essentially is compression stage as this is the stage where data is lost. Here small unimportant coefficients are rounded to zero while larger ones lose some of their precision. At this stage we got an array of streamlined coefficients, which are further compressed. Inverse DCT is used to decompress watermarking using DCT implies that if anyone sees the value of image pixels then also he/she is unaware about any watermark is embedded in it because the hidden data can be distributed more evenly over the whole image resulting good robustness. We may also hide the data in the quantizer stage. For that if we wish to encode the bit value 0 in specific 8×8 square of pixels then by tweaking the coefficient vales make sure that all coefficients are even. Similarly for inserting value 1 condition is coefficients must be odd. Advantages of this method are, it works well in keeping down distortions and also it is vulnerable to noise.

Discrete Wavelet Transform (DWT): Most promising factors in DWT are its hierarchical representation and multi resolution characteristics. They can be applied recursively on the low pass series until the desired numbers of iterations are reached. DWT for a one dimensional signal works as: The signal is splits into high frequencies and low frequencies part. As edge components of the signal are largely to the high frequency part, low frequency part is again splits into two parts of high and low frequencies. As per required application, above process is continued an arbitrary number of times. “Figure 2” shows decomposing an image in wavelet transform into four parts as: HH(High frequency coefficient diagonally), HL(High frequency coefficient vertically), LH(High frequency coefficient horizontally) and LL(Low frequency coefficient). Watermark should be embedded in low frequency coefficient at each level of decomposition.

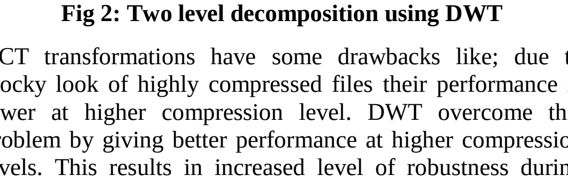

Fig 2: Two level decomposition using DWT

DCT transformations have some drawbacks like; due to blocky look of highly compressed files their performance is lower at higher compression level. DWT overcome this problem by giving better performance at higher compression levels. This results in increased level of robustness during information hiding. The compression of image at higher level can be done by segregating the high frequency detail from low frequency parts. After that compression of low frequency areas are carried out. For further compression quantization can then be took place. According to the need whole process can start again. In case of DWT the coefficients of wavelet are altered with the noise within tolerable level, while in DCT coefficient with pseudo noise are altered. Embedding information into wavelet is an ongoing research topic.

The comparative study of DCT and DWT is analyzed in [19]. In case of structural attacks DWT is effective than DCT. Also DWT has significant advantages over attacks such as compression, scaling & cropping. DWT is more robust to cropping as compared to DCT. DCT technique does not work with scaling attacks on the other hand DWT shows acceptable performance.

2.2.3 The Watermarking Technique for Audio

Audio clips which currently present and distributed over the cell phone and internet are mainly modified by compression. Compression is one of the most effective and easiest way to overcome digital watermark without significantly deteriorating or distributing the quality of audio [13].

Spread Spectrum: In Spread spectrum system, at the encoder side binary sequence of data is used which sounds like noise, while at the receiver side secret key is required to recognize the hidden data. This technique uses the comparison between the narrow bandwidth of embedded data and the large bandwidth of medium. This technique is particularly used in military as the signals are hard to jam and also they lost in the background noise.

MIDI: It refers to Musical Instrument Digital Interface. It provides good places to hide information. MIDI files consists of number of different messages out of which some control the notes at the time of hearing, while others are silent and make up the file header or change the notes being played. Program Change (PC) is the most important message from MIDI. Program change works for changing the type of instrument being played on a certain channel. If there are multiple PC messages in succession, then the instrument played will be the very end of message chain. As these messages occur so frequently, there are no noticeable side effects to the sound. Every PC message has numbering as from 0 to 127 which corresponds to the number of different instruments. For embedding of hidden data the necessary number of PC messages is just need to string together. The performance degrades for this method if huge amount of data is to be stored and also the hidden data can be easily seen.

MP3: For music files MP3 is the common compression format which is used currently. As in MP3Stego program, technique used for this is similar to frequency transformation. During the compression stage itself, MP3 file is created which contains data to be hidden. All the sound file compression takes place during layer 3 encoding process. So the data is selectively lost depending on bitrate, specified by user. At the time of encoding, the watermark can be encoded in the parity bit of this information. MP3 file is divided into number of pieces with own parity bit for each frame, so the reasonable amount of information can be stored. For retrieving the data, un-compress the MP3 file and read the parity bits. This technique is effective as it detects even a little distortion in the music file.

2.2.4 The Watermarking Technique for Video

As video is the combination of sound and image, it has separate inner files for sequence of images and sound. Video files are large in size, so having large scope for information hiding which minimizes the chances of hidden data being detected. As per [11], MPEG bit streams are used to embed watermarks into intra-frame and non-intra-frame with different residual masks. The Moving Picture Expert Group [20] video compression standard is in hybrid DCT block based scheme. There are three types of picture frames like Intra-frame (I-frame), forward-predicted frame (P-frame), and Bi-directional predicted frame (B-frame).

2.3 Distortions and Attacks

Watermarking system should be strong enough to detect and extract the watermark, alteration of watermarked objects done either on purpose or accidentally. Distortions are limited to those that do not produce excessive degradation and so that objects may be used further. These types of distortions may degrade the performance of the system. Every technique has its own limitations. There is only variation in robustness criteria for different watermarking techniques. Attacks have following categories as: basic, robustness, presentation, interpretation and implementation attacks. Attacks may be either intentional or unintentional depending on application.

Additive Noise: These attacks may seem in application where A/D and D/A converter are used. For that, perceptually shaped noise with maximum unnoticeable power is introduced by attacker.

Filtering: It does not introduce considerable degradation in watermarked data, but dramatically affects the performance.

Cropping: It is the attack in which attacker has interest in small portion of watermarked objects. To avoid this we need to spread the watermark over dimensions where this attack takes place.

Compression: Mainly internet data is in compressed form. This attack is mainly for multimedia applications. For the better resistance of watermark, insert the watermark in the same domain where compression takes place.

Rotation and Scaling: The embedded watermark and locally generated watermark do not share same spatial pattern so correlation based detection and extraction fails when rotation and scaling are performed on watermarked data. In audio watermarking, it is easy to perform a non-linear transformation of time axis that considerably difficult the watermark detection.

Multiple Watermarking: Already watermarked object may again be watermarked by attacker and can claims for ownership. For this problem, one should timestamp the hidden information by a certification authority.

3. AUDIO WAVE WATERMARKING

3.1 Audio Watermarking Algorithm

This paper presents a model that allows information hiding in audio wave format. “Figure 3” shows the proposed model architecture. We are using the following scheme for embedding the watermark in audio wave;

Step 1: Read the .wav file.

Step 2: Divide the audio source into pieces, for 256 points per
piece and also find the total piece count.

Step 3: Do the quantization as follows

```
        For:  total points (j)
        If (total points(j) is positive)
        Quantized music sample = music sample *2^15;
        Else
        Quantized music sample = music sample *2^15 *(-1);
```

Step 4: Clear LSB bits since it contains the least information.

Step 5: Apply DCT transform to the output of step 4.

Step 6: Produce the watermark from source audio file by
sorting lowest DCT components that can be easily
mixed into cover file by sorting components of step 5.

Step 7: Embed the produced watermark in the cover file by
XORing LSBs.

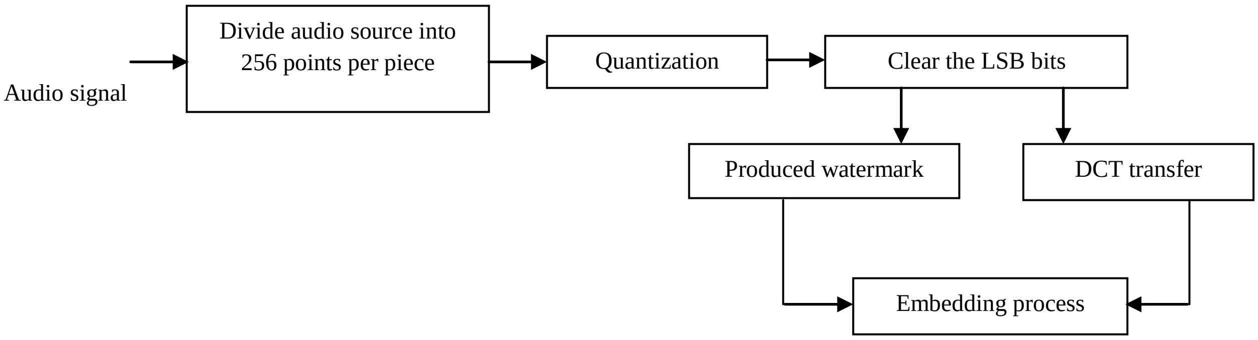

Fig 3: Proposed model architecture

Below “Figure 4” shows the original audio wave sample.

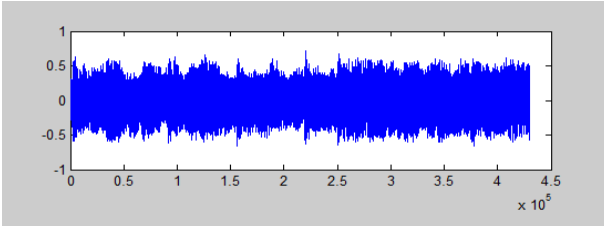

Fig 4: Music sample

We have plotted the results in “Figure 5” into four parts. First part shows the music quantized piece’s LSB zero as an output, while in the second part DCT is applied to the output of above step. In third part the music piece watermark is plotted and last part is of inverse DCT of music piece watermark.

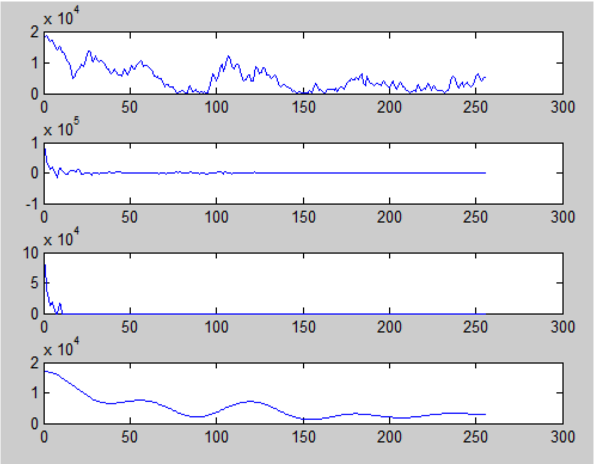

Fig 5: Results for intermediate steps of watermarking

In the last section for displaying output we have plotted the extracted watermark in "Figure 6".

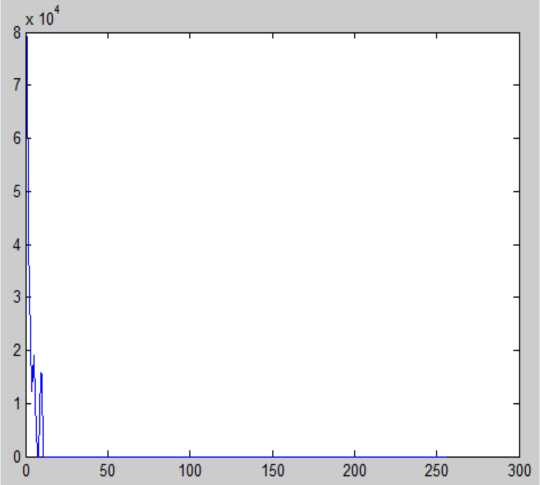

Fig 6: Extracted watermark

3.2 Result Analysis

For evaluating and analyzing the result of this model with Noriega et al. method [12] on the criteria of different types of attacks we mentioned the results in "Table 1".

Table 1. Attack types with results

Serial no.	Attacks	R. M. Noriega method	Proposed method
1	No attack	1	1
2	Compression 128 kbps	0.96	0.991
3	Add white noise	0.7023	0.876
4	Add FFT noise	0.8756	0.93
5	Resampling	0.6569	0.8345
6	Low pass filter	0.9426	0.9657

4. CONCLUSION

This paper presents a model for new approach to audio watermarking using the concept of generating the watermark from original sample audio. Experimental results are presented to claim the invisibility and robustness of the proposed audio watermarking process. The watermarking techniques were evaluated in terms of quality, security and higher degree for robustness. The security is guaranteed by the huge number of watermarks and the vanishing probability of faking a watermark. Possible enhancements were discussed and are subject of current research. Future work includes integrating the human audio system characteristics into this approach, also the algorithm can be extended to video. Further research is needed to make it work if the insertion/extraction is to be performed in real time. In future the algorithm can be extended in compressed domain watermarking where watermark is embedded in compressed audio itself and also extracted from compressed domain provided at no point of time we will decompress the audio.

5. REFERENCES

[1] P. Samuelson, "Digital Media and the Law," Communications of ACM, vol. 34, no. 10, pp.23- 28, Oct. 1991.

[2] M. Arnold, "Audio watermarking: Features, Applications and Algorithms," in IEEE Int. Conf. Multimedia and Expo 2000, vol. 2, 2000, pp. 1013–1016.

[3] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for Data Hiding," IBM Syst. J., vol. 35, no. 3/4, pp. 313–336, 1996.

[4] L. Boney, A. H. Tewfik, and K. N. Hamdy, "Digital Watermarking for Audio Signals," in Proc. 3rd Int. Conf. Multimedia Computing and Systems, 1996, pp. 473–480.

[5] J. Dittmann, M. Steinebach, and R. Steinmetz, "Digital Watermarking for MPEG Audio Layer 2," in Proc. ACM Multimedia, 1999, pp. 117–122.

[6] J. W. Seok and J. W. Hong, "Audio Watermarking for Copyright Protection of Digital Audio Data," Electron. Lett., vol. 37, no. 1, pp. 60–61, 2001.

[7] M. D. Swanson, B. Zhu, A. H. Tewfik, and L. Boney, "Robust Audio Watermarking using Perceptual Coding," Signal Process., vol. 66, no. 3, pp. 337–356, 1998.

[8] I. K. Yeo and H. J. Kim, "Modified Patchwork Algorithm: The novel audio watermarking scheme," in Proc. IEEE Int. Conf. Information Technology: Coding and Computing, Las Vegas, NV, April 2–4, 2001, pp. 237–242.

[9] M. Chandra, S. Pandel, Rama Chaudhary " Digital Watermarking Technique for Protecting Digital Images"226-233, IEEE 2010.

[10] L. Boney, A. H. Tewfik, and K. N. Hamdy, "Digital Watermarking for Audio Signals," in Proc. 3rd Int. Conf. Multimedia Computing and Systems, 1996, pp. 473–480.

[11] C. T. Hsu and J. L. Wu, "DCT-based Watermarking for Video," IEEE Transaction on Consumer Electronics, Vol. 44, No. 1, FEBRUVARY 1998.

[12] R. M. Noriega, H. Kang, B. Kurkoski, K.Yamaguchai and M.N.Miyatake, "Audio Watermarking Based on Wavelet Transform and Quantization Index Modulation".

[13] J. Cummins, P. Diskin, S. Lau and R. Parlett, “Steganography and Digital Watermarking,” School of Computer Science, University of Birmingham, http://www.gnu.org/copyleft/fdl.html.

[14] J. Cox, J. Kilian, T. Leighton and T. Shamoon, “Secure Spread Spectrum Watermarking for Multimedia,” Tech. Rep. 95-1 0, NEC Research Institute, 1995.

[15] O. Bruyndonckx, J. J. Quisquater and B. Macq, “Spatial Method for Copyright Labeling of Digital Images,” Proc. IEEE Nonlinear Signal and Image Processing, pp. 456-459, June 1995.

[16] H. Berghel and L. O‘Gorman, “Protecting Ownership Rights through Digital Watermarking,” ComputerMagazine, pp. 101-103, July 1996.

[17] S. Agaian, D. Akopian, S. A. D’Souza1, “Two Algorithms in Digital Audio Steganography using Quantized Frequency Domain Embedding and Reversible Integer Transforms,” USA.

[18] Mei Jiansheng1, Li Sukang1 and Tan Xiaomei” A Digital Watermarking Algorithm Based on DCT and DWT”,104-107, International Symposium on Web Information Systems and Applications (WISA’09) 2009.

[19] R. V. Totla and K. S. Bapat, “Comparative Analysis of Watermarking in Digital Images Using DCT and DWT,” International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013, ISSN 2250-3153.

[20] ISO/IEC 1 1 172-2, “Coding of Moving Pictures and Associated Audio - for Digital Storage Media at up to About 1.5 Mbits/s - Part 2 Video.”