Digital Audio Watermarking using Frequency Masking Technique

Ankita Tiwari
Reasearch Scholar M.Tech
Digital Communication
NRI Institute of Information Science & Technology
Bhopal

Lalit Jain
Professor
EC Department
NRI Institute of Information Science & Technology
Bhopal

ABSTRACT

There is a need of an effective watermarking technique for copyright protection and authentication of intellectual Property [12]. In this work we propose a digital watermarking technique which makes use of simultaneous frequency masking to hide the watermark information into host. The algorithm is based on Psychoacoustic Auditory Model and Spread Spectrum theory [2]. It generates a watermark signal using spread spectrum theory and embeds it into the signal by measuring the masking threshold using Modified Psychoacoustic Auditory model and using dct transform. Since the watermark is shaped to lie below the masking threshold, the difference between the original and the watermarked copy is imperceptible. Recovery of the watermark is performed without the knowledge of the original signal. The software system is implemented using MATLAB and the characteristics studied.

General Terms

Digital Watermarking, Audio Watermarking, Masking.

Keywords

Frequency Masking, Watermarking, Embed, MATLAB.

1. INTRODUCTION

In modern world each and every form of information, like text, images, audio or video, has been digitized [14]. Widespread networks and internet has made it easier and far more convenient to store and access this data over large distances. Although advantageous, this property threatens the copyright protection purpose [13].

Media and information in digital form is easier to copy and modify, and distribute with the aid of widespread internet. Every year thousands of sound tracks are released and within a few days are readily available on the internet for download. Without any information on the track itself, it's easy for someone to make profit out of them by modifying the original and selling under a different name. As a measure against such practices and other intellectual property rights, digital watermarking techniques can be used as a proof of the authenticity of the data.

1.1 Digital Watermarking

It is the process of embedding or inserting a digital signal or pattern in the original data, which can be later used to identify the author's work, to authenticate the content and to trace illegal copies of the work [12].

1.2 Requirements

Some of the requirements of the digital watermarking are:

* The original media should not be severely degraded and the embedded data should be minimally perceptible. *The words hidden, inaudible, imperceptible, and invisible mean that nobody notices the presence of the hidden data.

* The hidden data should be directly embedded into the carrier, rather than into the header of it.

* The watermark should be robust, also it should immune to all types of modifications including channel noise, filtering, re-sampling, cropping, encoding, lossy compressing, digital-to-analog (D/A) conversion, and analog-to-digital (A/D) conversion, etc.

* It should be easy for the owner or a proper authority to embed and detect the watermark.

* It should not be necessary to refer to the original signal when extracting a watermark.

1.3 Important Parameters for Audio Watermarking

As discussed earlier the main requirements of an efficient watermarking technique are the robustness and inaudibility. Some of the prerequisite parameters are:

- Dynamics
- Filtering
- Ambience
- Conversion and lossy, compression
- Noise

2. OVERVIEW OF DIGITAL AUDIO WATERMARKING TECHNIQUES

2.1 Digital watermarking [1] has been found to be effective for integrity examination. The goal of watermarking is to embed a piece of secret information (the watermark) into the original data so that any change or tampering with the data would alter the watermark. This type of watermarking is called fragile watermarking. Another type of watermarking, termed robust watermarking [3]–[5], can also be applied for copyright protection.

2.2 One way to implement the fragile watermarking is to hide watermark in the least significant bits (LSBs) of a host image in the spatial domain [6], [7]. Although high perceptual transparency can be achieved by the technique, tampering in the other bit planes of the host image cannot be detected. Another approach for fragile watermarking is to embed watermark in the transform domain. Many transform domain algorithms care based on image coding standards such as JPEG [8]. In addition to the distortion produced by the lossy

JPEG quantization, some watermarking operations may introduce further perceptual degradation. Algorithms employ invertible data hiding techniques for JPEG so that additional perceptual degradation due to watermarking can be avoided [10]. However, the quantization distortion produced by JPEG still cannot be recovered. In many applications (such as medical or military ones), because of the requirements for legal considerations or high precision nature, it is desired that no distortion is introduced in the host images even with the employment of watermarking. Therefore the watermarking algorithms may not be well-suited for these applications.

2.3 A number of reversible watermarking techniques have been proposed for full host image recovery [16]. The work in compresses LSBs of a host image loss less in the spatial domain to leave space for hiding watermark. Studies in are based on histograms of a host image in the spatial domain. The watermark is hidden in a set of pixels selected from the host image using the histograms [14]. To further extend the capacity for data hiding, algorithms in embed watermark using the histogram of pixel differences. Hiding techniques in are based on the histograms of interpolation errors [15]. A common drawback of these techniques is that the capacity for data hiding may vary for different images. The capacity will be large for host images exhibiting a high degree of concentration in histograms. For noise-like images such as holograms, the distribution in histograms is likely to be uniform. Amount of data allowed to be hidden by the algorithms may then be low. Another drawback is that only the pixels or bit planes embedded by watermark are protected. Direct applications of these algorithms for full coverage protection and detection may then be difficult.

2.4 To enhance the vigilance of fragile watermarking for holograms, the work in embeds watermark in the transform domain [21]. The marked holograms are then transformed back to spatial domain for storage and transmission. A single change in spatial domain may alter the values of all coefficients in the transform domain. A full coverage protection is then possible [17].

2.5 However, discrete cosine transform (DCT) computations are required for both watermark embedding and extraction. The algorithm therefore has high computational complexities. Moreover, although the algorithm is able to achieve high perceptual transparency, it is not reversible. For high fidelity 3D reconstruction and rendering applications, reversible watermarking is desired [1]

2.6 Discrete Cosine Transform

In the following, fdct(x) is original sequence while Cdct(u) denotes the DCT coefficients of the sequence.

$$C_{dct}(u) = \alpha(u)\sum_{x=1}^{N_{1t}-1} f_{dct}(x)\cos\left[\frac{\pi(2x+1)u}{2N_{1t}}\right], \mathit{for}\, u = 0,1,2,...,N_{1t}-1$$

$$f_{dct}(x,y) = \sum_{u=1}^{N_{1t-1}} \alpha(u)C_{dct}(u)\cos\left[\frac{\pi(2x+1)u}{2N_{1t}}\right], \mathit{for}\ x = 0,1,2,...,N_{1t}-1$$

$$\mathit{where}\ \alpha(u) = \begin{cases} \sqrt{\frac{1}{N_{1t}}} & \text{for}\, u = 0 \\ \sqrt{\frac{2}{N_{1t}}} & \text{for}\, u \neq 0 \end{cases}$$

From the equation for Cdct(u) it can be inferred that for u = 0, the component is the average of the signal also termed as dc coefficient in literature [38]. And all the other transformation coefficients are called as ac coefficients. Some of the important applications of DCT are image compression and signal compression.

The most useful applications of two-dimensional (2-d) DCT are the image compression and encryption [17]. The 1-d DCT equations, discussed above, can be used to find the 2-d DCT by considering every row as an individual 1 -d signal. Thus, DCT coefficients of an M×N two dimensional signals Cdct2(u, v) and their reconstruction fdct2(x, y)can be calculated by the equations below:

$$C_{dct2}(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{M_{2t-1}}\sum_{y=0}^{N_{2t-1}} f_{dct2}(x,y)\cos\left[\frac{\pi(2x+1)u}{2M_{2t}}\right]\cos\left[\frac{\pi(2y+1)v}{2N_{2t}}\right]$$

$$f_{dct2}(x,y) = \sum_{x=0}^{M_{2t-1}}\sum_{y=0}^{N_{2t-1}} \alpha(u)\alpha(v)C_{dct2}(u,v)\cos\left[\frac{\pi(2x+1)u}{2M_{2t}}\right]\cos\left[\frac{\pi(2y+1)v}{2N_{2t}}\right]$$

$$\mathit{where}\ u\,\&\,x = 0,1,2,...,M_{2t-1} \quad \mathit{and} \quad \mathit{where}\ v\,\&\,y = 0,1,2,...,N_{2t-1}$$

$$\alpha(u) = \begin{cases} \sqrt{\frac{1}{N_{2t}}} & \text{for}\, u = 0 \\ \sqrt{\frac{2}{N_{2t}}} & \text{for}\, u \neq 0 \end{cases} \quad \& \quad \alpha(v) = \begin{cases} \sqrt{\frac{1}{N_{2t}}} & \text{for}\, v = 0 \\ \sqrt{\frac{2}{N_{2t}}} & \text{for}\, v \neq 0 \end{cases}$$

Discrete cosines transform (DCT) method can be explained as:

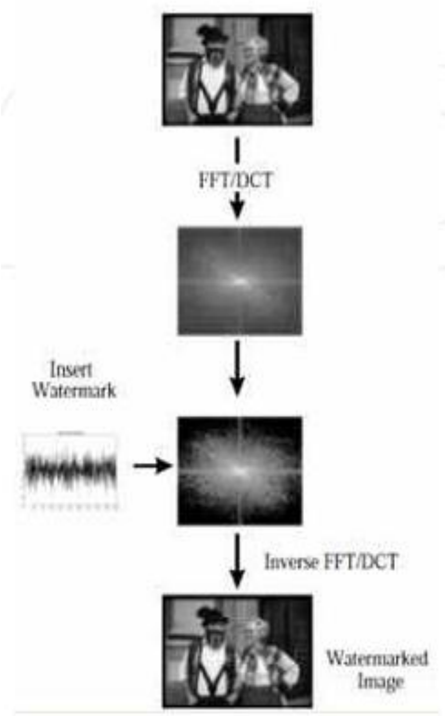


Fig 1: Watermarking in Spectral Domain

Compared with the image and video watermarking, digital audio watermarking is especially challenging, because the human auditory system (HAS) is extremely more sensitive than Human Visual System (HVS) [20]. There are many methods we can use to embed audio watermarks. Currently, audio watermarking techniques mainly focus on four aspects: low bit coding, phase coding, and spread spectrum-based compared and echo hiding [4].

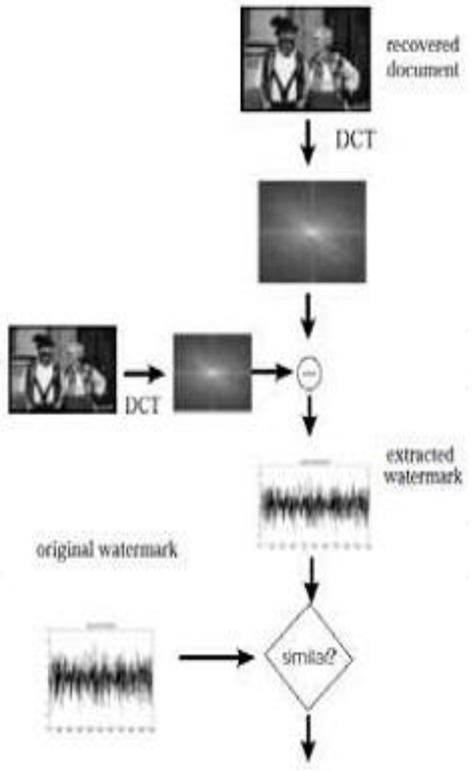


Fig 2: Watermark Extraction Process

In this work we used principles of Spread Spectrum Theory and Psychoacoustic Auditory Model to embed the watermark. The watermarking system uses an algorithm that relies on the above principles, to generate a digital watermark. (bit-stream, character string, etc.), and embed it into the original audio file (which is in .wav format) by spectrally shaping the watermark signal [8].

The second difference involves destruction. While robustness is merely desired in steganography, it is required for copyright marking [10]. For example, cropping a picture or changing an image format should not destroy copyright information.

In this work, simultaneous frequency masking is closely studied to be used for watermark shaping purposes [14]. The auditory model made here is used the audio information to produce information about the final masking threshold. The final masking threshold information is used to shape the generated audio watermark [13]. This shaped watermark is ideally imperceptible for the average listener. To overcome the potential problem of the audio signal being too long to be processed all at the same time, and also extract quasi-periodic sections of the waveform, the signal is segmented in short overlapping segments, processed and added back together. Each one of these segments is called a “frame.” The steps involved in creating a Modified Psychoacoustic Auditory Model include, Discrete Cosine Transform / Fast Fourier Transform

- Amplitude Spectra
- Separation of non-integer components
- Spread masking
- Masking threshold Estimation

3. PERFORMANCE EVALUATION OF WATERMARKING METHODS

Several Functions are used for quality assessment of the digital watermarking algorithms, examining tests on the resulted watermarked image.

3.1 MSE

Mean Squared Error (MSE) function is defined as:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}\left(X_i - X_i^*\right)^2$$

3.2 PSNR

Peek Signal to Noise Ratio (PSNR) is defined as for SNR of an image:

$$PSNR = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

3.3 SSIM

The Structural Similarity (SSIM) is a function defined as equation given below:

$$SSIM = \frac{\left(2\mu_x\mu_y + c_1\right)\left(2\sigma_{xy} + c_2\right)}{\left(\mu_x^2 + \mu_y^2 + c_1\right)\left(\sigma_x^2 + \sigma_y^2 + c_2\right)}$$

Where: “μ”, “σ”, & “σxy” are mean, variance, and covariance of the images, and “c1, c2” are the stabilizing constants.

3.4 Robustness

Basically this term is related to the security and immunity to the attacks.

3.5 Noise

Gaussian, Poisson, Salt &Pepper, and Speckle etc. Also in extraction process the image from host has loss of some components which appears as noise.

4. PROPOSED METHODOLOGY

In our proposed work we have used Transformation (DCT) technique for watermarking of image (Original Signal) into Audio (Carrier). Audio watermarking is challenging than an image watermarking technique due to wider dynamic range of the HAS in comparison with human visual system (HVS) [11]. By using Frequency masking and temporal masking the original signal is hidden in the carrier. For security purpose 10 bit Password (Owner’s Key) is also required at the time of Embedding and for detection.

4.1 Frequency Masking

Frequency (simultaneous) masking is a frequency domain observable fact where low levels signal (the maskee) can be made inaudible (masked) by a simultaneously appearing stronger signal (the masker), if the watermarked and host are close enough to each other in frequency [15]. A masking threshold can be found and is the level below which the audio signal is not audible. Thus, frequency domain is a good region to check for the possible areas that have imperceptibility.

4.2 Temporal Masking

In frequency masking, two basic phenomenon of the HAS in the time domain play major role in human auditory perception. Those are pre-masking and post masking in time [14]. Temporal masking is used in those applications where the robustness is not of primary consideration.

In this proposed blind frequency masking algorithm entire embedder [18]. In a watermark detector, the un-watermarked host signal is known, and cannot be removed before a watermark extraction. Under these conditions, the analogy with Figure 3 can be made, where the added watermark is corrupted by the combination of impacts of the cover work and the noise signal. The received watermarked signal c_{wn}, is now viewed as a corrupted version of the added pattern w_a and the entire watermarked detector is viewed as the channel decoder.

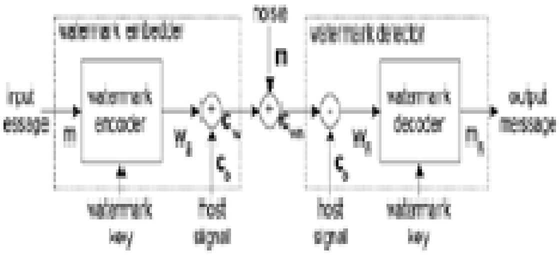


Fig 3: Proposed Frequency Masking Watermarking system with blind detection

4.3 Proposed Embedding Algorithm

1. First take image i.e. information signal.
2. Convert it in to frequency domain by taking its transform using discrete cosine transform.
3. Result in transformed image.
4. Similarly find transformed audio signal i.e. carrier signal.
5. Form embedded signal by adding transformed information and carrier signal i.e. watermarked sub – band.
6. The take inverse transform i.e. convert it into time domain.
7. Obtain watermarked audio.

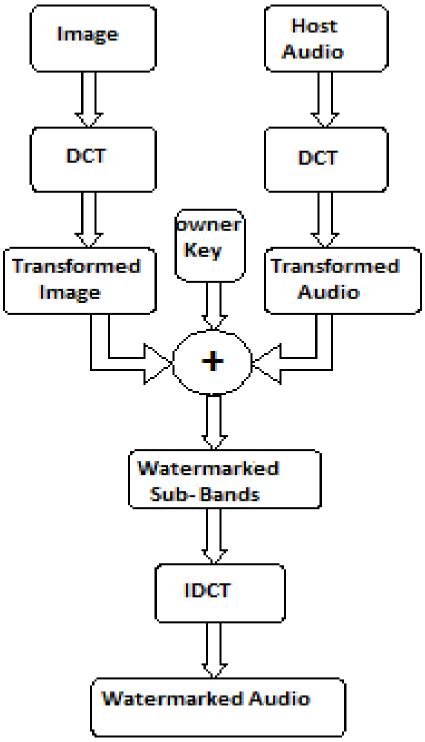


Fig 4: Proposed Watermark Embedding Algorithm

4.4 Proposed Extraction Algorithm

1. First take watermarked audio.
2. (2) Convert it in to frequency domain by taking its transform using discrete cosine transform.
3. (3) Result in transformed watermarked audio signal.
4. Take transformed host audio carrier signal using discrete cosine transform.
5. Extract image by subtracting watermarked audio and audio signal.
6. The take inverse transforms (inverse discrete cosine transform) i.e. convert it into time domain.
7. Obtain original image i.e. information signal this is called extracted watermarked image.

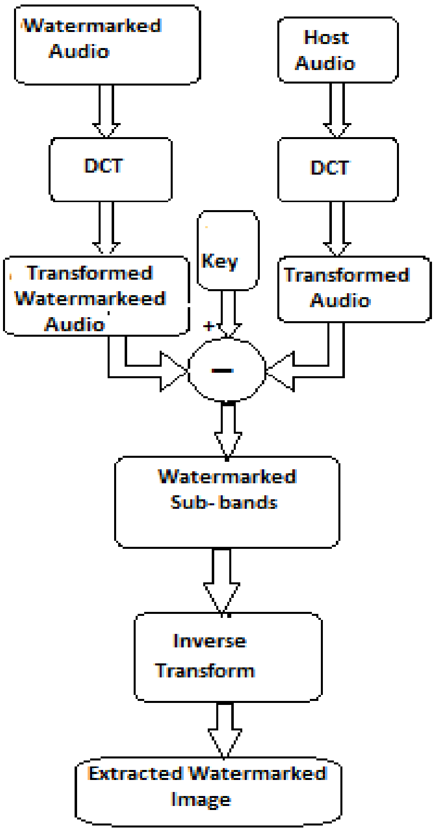
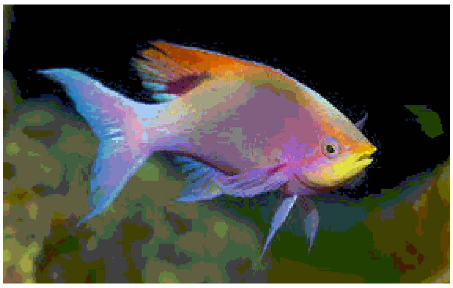


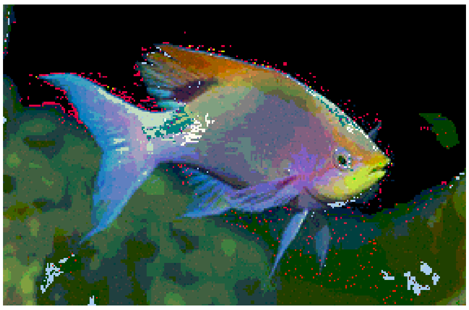
Fig 5: Proposed Watermark Extraction Algorithm

5. SIMULATION RESULTS & DISCUSSIONS

5.1 Original Image (To be hidden in audio)

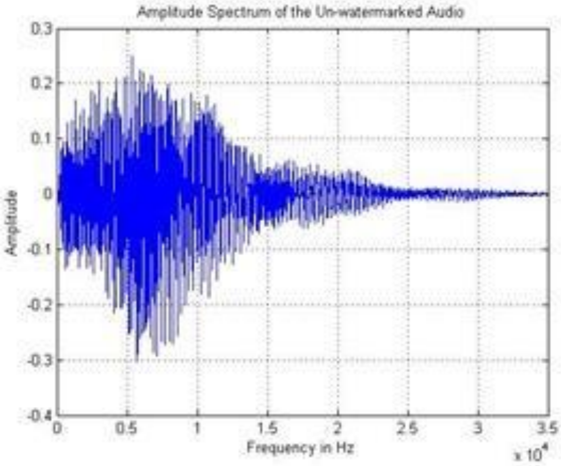


5.2 Detected / Extracted Image from audio

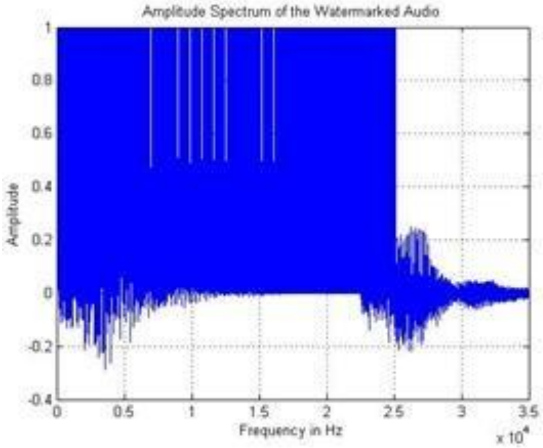


5.3 Component Spectrum Comparison of Audio

5.3.1 Amplitude Spectrum of the Un-Watermarked Audio



5.3.2 Amplitude Spectrum of the Watermarked Audio



5.4 RESULT COMPARISON

Images	PSNR			MSE		
	LSB	*DCT*	*DWT*	*LSB*	*DCT*	*DWT*
Jet [1]	46.9015	47.9532	46.7309	0.5325	0.3320	1.3912
Baboon[1]	47.3214	48.2092	46.8262	0.4834	0.3130	1.3610
Fish	---------	49.4257214	---------	---------	0.75	---------

6. CONCLUSIONS

The level of watermarking increases robustness of the secret information. The watermarks are embedded into non overlapping DCT coefficients of the audio signal which are randomly selected and very hard to detect even with the blind detection. The audio watermarking is relatively new and has wide scope for research. For future, a new algorithm will proposed that taking features of Human Auditory System and the signal processing theories. Proposed algorithm is based on DCT domain while considering the more active components of the signal. We use this Proposed algorithm which is based on DCT domain in video watermarking to hide image and also hide audio in video.

7. REFERENCES

[1] Saravanan Chandran , Koushik Bhattacharya "Performance Analysis of LSB, DCT and DWT for Digital watermarking Application using Steganography" 978-14799-7678-2/15/31.00 ©2015IEEE.

[2] Ms. Komal V. Goenka et-al, "Overview of Audio Watermarking Techniques", IJETAE, Volume 2, Issue 2, February 2012.

[3] Shweta Sharma et-al, "Survey on Different Level of Audio Watermarking Techniques", International Journal of Computer Applications (IJCA), Volume 49– No.10, July 2012.

[4] K.B.Raja, C.R.Chowdary, Venugopal K R, L.M.Patnaik, "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images", IEEE-0-7803-9588-3/05/$20.00.

[5] NageswaraRaoThota, Srinivasa Kumar Devireddy, "Image Compression Using Discrete Cosine Transform", Georgian Electronic Scientific Journal: Computer Science and Telecommunications, No.3 (17), 2008.

[6] Dhananjay Yadav et-al, "Reversible Data Hiding Techniques", International Journal of Electronics and Computer Science Engineering (IJECSE), Volume 1, Number 2, 2013.

[7] Ali Al-Haj et-al, "DWT–Based Audio Watermarking", The International Arab Journal of Information Technology, Vol. 8, No. 3, July 2011.

[8] N.F. Johnson, S. Jajodia, and Z. Duric, Information hiding: Steganography and watermarking attacks and countermeasures, Kluwer academic Publishers, 2000. 2. M. Goresky, A. M. Klapper.

[9] Fibonacci, and Galois, "Representations of Feedback-WithCarry Shift Registers," IEEE Transaction on Information Theory, Vol. 48, No. 11, pp. 2826-2836. 2002.

[10] C. Shoemaker, "Hidden bits: A survey of techniques for digital watermarking," Independent study, EER 290, spring 2002.

[11] B. Dumitrescu, and A. B. Rad, "A Method for Designing the Double-Density Dual-Tree Discrete Wavelet Transform," Proc. Int. TICSP Workshop on Local and Non-Local Approximation in Image Processing, Lausanne, Switzerland, Aug. 2008.

[12] S. Katzenbeisser, and F.A.P. Petitcolas, Information hiding techniques for steganography and digital watermarking, Artech House Publishers, 2000

[13] G. Voyatzis, and I. Pitas, "Applications of toralautomorphisms in image watermarking," Proceedings of International Conference on Image Processing, vol. 1, pp. 237– 240, 1996.

[14] S.A. Craver, B. Liu, and M. Wu, "What can we reasonably expect from watermarks? Applications of Signal Processing to Audio and Acoustics." IEEE Workshop on 10/21/2001 -10/24/2001, pp. 223-226, 2001. Proceedings of the IEEE, vo. 7, Issue 87, pp. 1267-1276, 1999.

[15] J. Bloom, I. Cox, T. Kalker, J. Linnartz, M. Miller, and C. Traw. "Copy protection for DVD video," Proceedings of the IEEE, vo. 7, Issue 87, pp. 1267- 1276, 1999

[16] F.A.P Petitcolas. "Watermarking schemes evaluation," IEEE Signal Processing Magazine, Volume 17, Issue 5, pp.58-64, 2000.

[17] M. Steinebach, F. Petitcolas, F. Raynal, J. Dittmann, C. Fontaine, S. Seibel, et al., "Stirmark benchmark: Audio watermarking attacks," Proceedings of the International Conference on Information Technology: Coding and Computing, pp. 49-54, 2001, Las Vegas, Nevada.

[18] X. Wang, and H. Zhao, "A Blind Audio Watermarking Robust Against Synchronization Attacks," CIS 2005, Part II, LNAI 3802, pp. 617-622, 2005.

[19] Voloshynovski, S., Pereira, S., Iquise, V. & Pun, T. 2001, Attack modelling: towards a secondgeneration watermarking benchmark, Signal Processing 81(6): p 1177–1214.

[20] Miller, M, Dorr, G. & Cox, I. 2002, Dirty-paper trellis codes for watermarking, In: Proc. IEEE International Conference on Image Processing, Rochester, NY, p 129–132.

[21] Petitcolas, F.A.P. 2000, Watermarking schemes evaluation, IEEE Signal Processing Magazine [Online], Volume 17, Issue 5, pp.58-64.