International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

Comparative Studies of various Digital Image & Audio Watermarking Techniques

Ikchha Pandey
Research Scholar, Department of Electronics & Communication, Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India

Siddarth Bhalerao
Assistant Professor, Department of Electronics & Communication, Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India

Papiya Dutta
Associate Professor & H.O.D., Department of Electronics & Communication, Gyan Ganga College Of Technology, Jabalpur, Madhya Pradesh, India

ABSTRACT

In this paper a brief review of various audio and image watermarking techniques has been carried out. Properties of both image and audio are different while processing. In this work a blind frequency masking algorithm for hiding the image data into audio signal using DCT is proposed. DCT provides compression & to avoid distortions from DCT compression, additional password key would be used to encrypt data in frequency domain. The secret key or a password would be required to extract a data, also helps to make the data immune from "noise" effects represented by the addition the host signal in the embedder. In a blind watermark detector, the un-watermarked host signal is unknown, and cannot be removed before a watermark extraction. Under these conditions.

Keyword: *DCT, Watermarking, Image to Audio watermarking, Password security*

INTRODUCTION

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

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 some one 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.

Digital Watermarking 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.

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 notice 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.

Important Parameters for Audio Watermarking

As discussed earlier the main requirements of an efficient watermarking technique are the robustness and inaudibility. There is a trade-off between these two requirements; however, by testing the algorithm with the signal processing attacks the gap can be made minimal. Every application has its explicit requirements and provides an option to choose high robustness compensating with the quality of the signal and vice-versa. Without any transformations and attacks every watermarking technique performs efficiently. Many common types of processes for audio signal are used when transmitted through a medium [13]. Some of the pre-requites parameters are:

Dynamics: The amplitude variation and reduction provide the dynamics of the attacks. Limiting, extension and compressions are some sort of more complex applications which are the non-linear modifications. Some of these types of attacks are re-quantization [12].

Filtering*:* Filtering is a common practice used to amplify or attenuate some part of any signal. The basic low pass and high pass filters can be used to attain these types of attacks.

Ambience*:* In some situations the audio signal gets deferred or there are situations where in people record signal from a source and claim that the track is theirs. Those situations can be simulated in a room, which has great importance to check the performance of an audio signal.

Conversion and lossy compression*:* Audio generation is done at a particular sampling frequency and bit rate; however, the created audio track will undergo so many different types of compression and conversion techniques. Some of the most common compression techniques are audio compression techniques based on psychoacoustic effect (MPEG and Advanced Audio Codec (AAC)). In addition to that, it is common process that the original audio signal will change its sampling frequencies like from 128Kbps to 64Kpbs or 48 Kbps.

Noise*:* Whenever the signal is transmitted there is always noise is present in the signal. Hence, watermarking algorithm has to make the technique robust against the noise attacks. It is commonly used to check the algorithm for this type of noise attacks by adding the host signal by an additive white Gaussian noise (AWGN) to check its robustness. Time stretch and pitch shift: These attacks change either the length of the signal without changing its pitch and vice versa. These are some de-synchronization attacks which are quite common in the data transmission. Jittering is one type of such attack.

Overview of Digital Audio Watermarking Techniques

An audio watermarking technique can be classified into two groups based on the domain of operation. One is time domain technique and the other is transformation based method. The time domain techniques include methods where the embedding is performed without any transformation. Watermarking is employed on the original samples of the audio signal. Time domain watermarking technique is the example of least significant bit (LSB) method. In LSB method the watermark is embedded into the least significant bits of the host signal. As against these techniques, the transformation based watermarking methods perform watermarking in the transformation domain. Few transformation techniques that can be used are discrete cosine transform and discrete wavelet transform. In transformation based approaches the embedding is done on the samples of the host signal after they are transformed. Using of transformation based techniques provides additional information about the signal [11].

In all-purpose, the time domain techniques provide least robustness as a simple low pass filtering can remove the watermark [1]. Hence time domain techniques are not advisable for the applications such as copyright protection and airline traffic monitoring; however, it can be used in applications like proving ownership and medical applications. Watermarking techniques can be distinguished as visible or we can say it as non-blind watermarking

and blind watermarking. In the following, we present typical watermarking strategies such as LSB coding, spread spectrum technique, patchwork technique, and quantization index modulation (QIM).

LSB Coding

This technique is one of the common techniques in use in signal processing applications. It is based on the replacement of the LSB of the carrier signal with the bit pattern from the watermark noise [16]. The robustness depends on the number of bits that are being replaced in the host signal. This type of technique is usually used in image watermarking because each pixel is represented as an integer hence it will be easy to replace the bits. The audio signal has real values as samples, if transformed to an integer will degrade the quality of the signal to a great extent (see Fig 1).

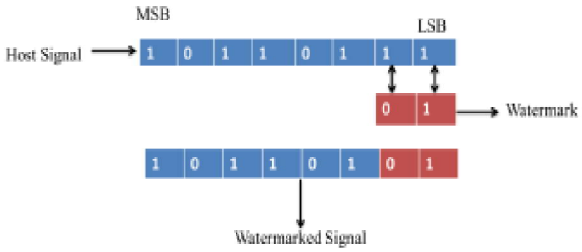

Fig 1: LSB Embedding

Spread Spectrum Technique

These techniques are derived from the concepts used in spread spectrum communication [15]. The basic approach is that a narrow band signal is transmitted over the large bandwidth signal which makes them undetectable as the energy of the signal is overlapped. In the similar way the watermark is spread over multiple frequency bins so that the energy in any one bin is very small and certainly undetectable [14]. In spread spectrum technique, the original signal is first transformed to another domain using domain transformation techniques [13]. The embedding technique can use any type of approach for example quantization. Zhou *et al.* proposed an algorithm embedding watermark in 0th DCT coefficient and 4th DCT coefficients which are obtained by applying DCT on the original signal [5]. Both embedding and extraction procedure can be interpreted using Figure 2. The original signal is transformed into frequency domain using DCT. Then watermark is embedded to the sample values in that domain. Reverse procedure is followed to obtain the watermarked signal (see Fig 2).

Embedded signal will go through some attacks, thus, noise is added to the signal. To extract the watermark the attacked signal is fed through extraction procedure. The procedure for extractions follows the same steps as that in embedding procedure as shown in Figure 2. The extraction process involves taking the attacked signal and applying DCT, framing the obtained components. And they obtained frames are used to obtain the watermark. Care is taken to replicate the procedure used for embedding process.

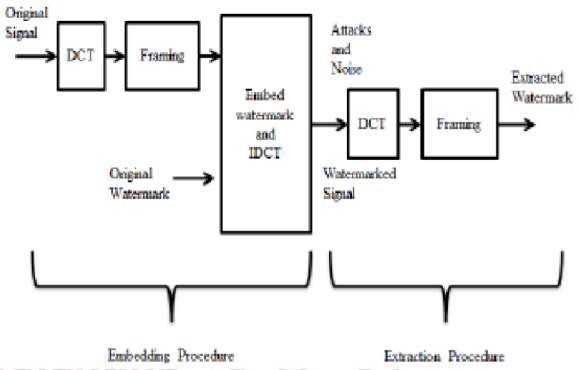

Fig 2: Example for spread spectrum technique

Patchwork Technique

The data to be watermarked is divided into two distinct subsets. One feature of the data is selected and customized in opposite directions in both subsets [13]. For an example let the original signal is divided into two parts A and B, then the part A is increased by a fraction Δ and the part B is decreased by some amount Δ. The samples separation is the secret key which is termed as watermarking key. Detection of watermark is done by following the statistical properties of the audio signal. Let NA and NB indicate the size(s) of the individual A and B parts and Δ be the total of the change made to the host signal. Suppose that $a[i]$ and $b[i]$ represent the sample values at $\mathbf{i}^{\mathbf{th}}$ position in blocks A and B. The difference of the sample values can be written as [23]:

$$S = \frac{1}{N_A}\sum_{N_A} a[i] - \frac{1}{N_B}\sum_{N_B} b[i]$$

$$= \frac{1}{N}\sum_{N}(a[i]-b[i]); \quad N_A = N_B = N.$$

The expectation of the difference is used to extract the watermark which is expressed as follows [4].

$$E\{S\} = \begin{cases} 2\Delta; \text{for watermarked data} \\ 0; \text{for unwatermarked data} \end{cases}$$

Watermarking in spectral domain

There are several transforms that brings an image into frequency domain. Among most common of those, we can mention are:

- Discrete Cosines Transform (DCT)
- Fast Fourier Transform (FFT)

Discrete Cosine Transform

The discrete cosine transform is a technique for converting a signal into elementary frequency components [17]. 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 [17]. 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) can be computed using equations [17]. In the following, fdct(x) is original sequence while Cdct(u) denotes the DCT coefficients of the sequence.

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

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

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

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:

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

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

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

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

In frequency domain, coefficients are slightly modified. This will make some unnoticeable changes in the whole image and makes it more robust to attack compared to what we have in spatial methods. One of the most popular approaches in this category is the discrete cosines transform (DCT) method.

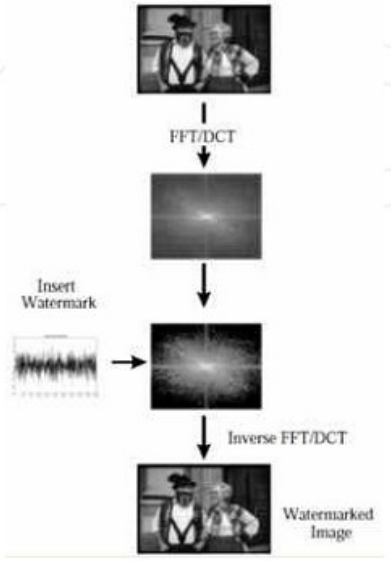

Fig 3: Watermarking in Spectral Domain

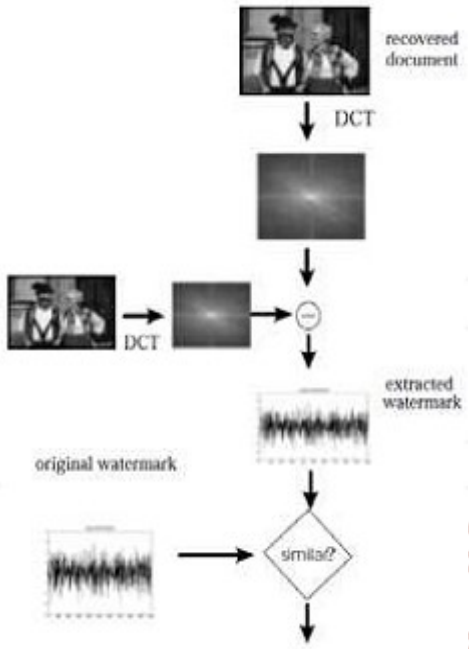

Fig 4: Watermark Extraction Process

Watermarking in hybrid domain

Watermarking in hybrid domain means modifying the image regarding both spatial and spectral specifications. One popular algorithm in this domain is performing the previous method in small blocks of the image. This could happen in 8×8 blocks which ideally match JPEG compression to provide least distort to the message facing with JPEG compression attack Fig. 4 illustrates this method. Pixels in blue represent
intensity of middle frequencies in the image and are most suitable for carrying message data. The code has not been brought here because it is simply performing spread spectrum algorithm in separate smaller blocks.

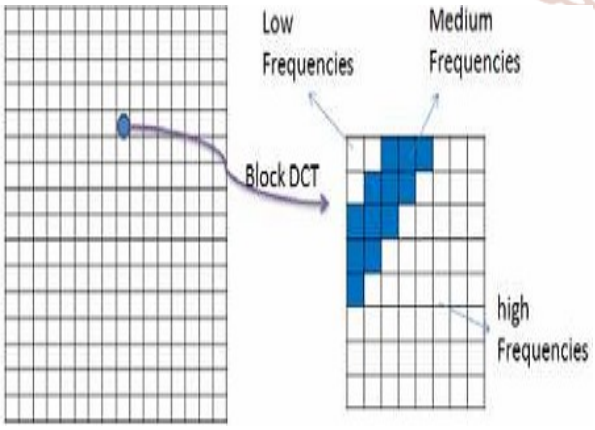

Fig 5: Block-based hybrid Watermarking method

Spread spectrum audio watermarking in time domain

One of the first audio watermarking algorithms is a time domain spread spectrum algorithm. It embeds a spread spectrum-based watermark into an uncompressed, raw audio by slightly modifying the values of samples of the host audio in time domain. The main motivation was the development of an algorithm with a low computational complexity and with an embedding and extraction of watermarks in time domain. One of the most robust methods already developed for audio watermarking was a time domain algorithm. It would definitely be hard to prove mathematically that watermarking in time domain gives smaller computational complexity in comparison with other, non-temporal algorithms because it is hard to compare complexity with each developed watermarking scheme. However, time domain algorithms have at least a lower implementation complexity and a smaller number of blocks in embedding and extraction algorithms.

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). 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*, *spread spectrum-based coding* and *echo hiding*.

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

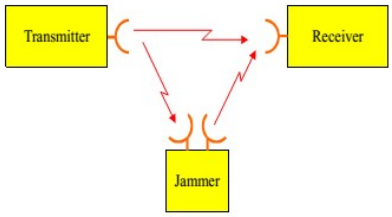

Fig 6: Basic Spread Spectrum Theory

Performance Evaluation of Watermarking Methods

Several Functions are used to qualify the watermarking algorithm, examining tests on the resulted watermarked image.

Imperceptibility: The imperceptibility of the watermark is tested through comparing the watermarked image with the original one. Several tests are usually used in this regard.

MSE: Mean Squared Error (MSE) is one of the earliest tests that were performed to test if two pictures are similar. A function could be simply written according to equation given as:

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

PSNR: Peak Signal to Noise Ratio (PSNR) is a better test since it takes the signal strength into consideration (not only the error). Given equation describes how this value is obtained:

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

Robustness: The robustness of a watermark method can be evaluated by performing attacks on the watermarked image and evaluating the similarity of the extracted message to the original one.

Compression Attack: The most used image compression is definitely JPEG. In MATLAB, for compressing an image to different quality factors, the image should be created from a matrix.

Cropping: Cropping attack is simply cutting off parts of the image. If the algorithm is non-blind, it is better to bring back those parts from the original image for a better recovery of the message.

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

Proposed method for Audio Watermarking

Audio watermarking is challenging than an image watermarking technique due to wider dynamic range of the HAS in comparison with human visual system (HVS) [1]. Human ear can perceive the power range greater than 109:1 and range frequencies of 103:1 [4]. In addition, human ear can hear the low ambient Gaussian noise in the order of 70dB [4]. However, there are many other useful features such as the louder sounds mask the corresponding slow sounds. This feature can be used to embed additional information like watermark. Further, HAS is insensitive to a constant relative phase shift in a stationary audio signal and some spectral distortions are interpreted as natural, perceptually non-annoying ones [2]. Two properties of the HAS dominantly used in watermarking algorithms are frequency (simultaneous) masking and temporal masking [3].

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 masker and maskee are close enough to each other in frequency [5]. 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.

Temporal Masking: In frequency masking, two phenomena of the HAS in the time domain also play an important role in human auditory perception. Those are pre-masking and post masking in time [5]. Temporal masking is used in those applications where the robustness is not of primary consideration.

In this work a blind frequency masking algorithm for hiding the image data into audio signal using DCT is proposed. DCT provides compression & to avoid distortions from DCT compression, additional password key would be used to encrypt data in frequency domain. The secret key or a password would be required to extract a data, also helps to make the data immune from "noise" effects represented by the addition the host signal in the embedder. In a blind watermark detector, the un-watermarked host signal is unknown, and cannot be removed before a watermark extraction. Under these conditions.

Conclusions

The above description is used for audio data signal. Some techniques use image as data and another image as carrier. Some of them uses audio as data

and another audio as cover. 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 be proposed that will take audio as a cover or carrier object and image as the data object, which has to be hidden in audio. Proposed algorithm will be based on DCT domain while considering the more active components of the signal, and audio processing can be done in better way using DCT.

References

1) Hong, Z., Wu M., Wang, Z. & Liu, K. 2003, Non linear collusion attacks on independent fingerprints for multimedia. In: Proc. IEEE Computer Society Conference on Multimedia and Expo, Baltimore, MD, p 613–616.
2) Goresky, M., Klapper, A. M., Fibonacci and Galois 2002, Representations of Feedback-With-Carry Shift Registers, IEEE Transaction on Information Theory, Vol. 48, No. 11, pp. 2826-2836.
3) Shoemaker, C. 2002, Hidden bits: A survey of techniques for digital watermarking, Independent study, EER 290, spring.
4) Bloom, J., Cox, I., Kalker, T., Linnartz, J., Miller, M., and Traw, C. 1999, Copy protection for DVD video, Proceedings of the IEEE, vo. 7, Issue 87, pp. 1267- 1276.
5) Zwicker, E., and Fast, H., Psychoacoustics 1999. Springer Verlag, Berlin, Germany.
6) Hernandez, J., Rodriguez, J. & Perez-Gonzalez, F. 2001 Improving the performance of spatial watermarking of images using channel coding. Signal Processing 80(7): p 1261–1279.
7) Polikar, R., Home page - Dr. RobiPolikar, Jan 2001. July 21, 2010.
8) Kennedy, J., IFPI Digital Music Report 2010. [Online]. Aug 8, 2010.
9) Khayam, S. A. 2003, The Discrete Cosine Transform (DCT): Theory and Application, Information Theory and Coding, Seminar 1 – The Discrete Cosine Transform: Theory and Application, March 10.
10) Salomonsen, K. 1997, Design and Implementation of an MPEG/Audio Layer III Bit stream Processor, Master´s thesis, Aalborg University, Denmark.
11) Voyatzis, G. and Pitas, I. 1996, Applications of toral automorphisms in image watermarking, Proceedings of International Conference on Image Processing, vol. 1, pp. 237– 240.
12) SDMI 2000. Call for Proposals for Phase II Screening Technology Version 1.0, July 15. 2010.
13) Wang, X. and Zhao, H. 2005, A Blind Audio Watermarking Robust Against Synchronization Attacks, CIS 2005, Part II, LNAI 3802, pp. 617-622.
14) Katzenbeisser, S. and Petitcolas, F.A.P. 2000, Information hiding techniques for steganography and digital watermarking, Artech House Publishers.
15) Arnold, M., Schmucker, M. and Wolthusen, S. D. 2003, Techniques and Applications of Digital Watermarking and Content Protection. Boston, London: Artech House, INC.
16) Kumar, M. N. 2004, Watermarking Using Decimal Sequences, M.S. thesis, Louisiana State University, Baton Rouge, LA, USA.
17) Petitcolas, F. 2000, Watermarking schemes evaluation, IEEE Signal Processing Magazine 17(5): p 58–64.
18) Steinebach, M., Petitcolas, F., Raynal, F., Dittmann, J., Fontaine, C., Seibel, S., Fates, N. & Ferri, L. 2001 Stirmark benchmark: Audio watermarking attacks, In: Proc. International Conference on Information Technology: Coding and Computing, Las Vegas, NV, p 49–54.
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.