Digital Watermarking: Applications, Techniques and Attacks

Smitha Rao M.S
Department of Master of Computer Applications
Reva Institute of Technology and Management
Bengaluru, India

Jyothsna A.N
Department of Master of Computer Applications
Reva Institute of Technology and Management
Bengaluru, India

Pinaka Pani.R
Department of Master of Computer Applications
Reva Institute of Technology and Management
Bengaluru, India

ABSTRACT

As information transmission technology progresses, the technology to protect data from unauthorized users also needs to be enhanced. Data can be plagiarized, modified, deleted etc without proper authentication and authorization. Various security mechanisms have evolved that enhances the security of digital media. Each technology to be applied successfully should ensure a balance between the three pillars of security; confidentiality, integrity and availability. Digital watermarking is one such technique. It is a mechanism to monitor the digital media with the help of information residing within the content itself. To put it simply, digital watermarking is embedding of information into source content that can be detected and extracted. Digital watermarking can be applied to media like text, audio, image, video etc. This paper provides a comprehensive idea behind this technology and its usage.

General Terms

Digital Watermarking, Watermarking Attacks, Watermarking Applications.

Keywords

Steganography, Fingerprinting, Phase Encoding, Spread Spectrum Watermarking, Echo Watermarking, Dual Watermark, Class A attacks, Class B attacks.

1. INTRODUCTION

Growth of computer technology and internet has led to tremendous opportunities for creation and distribution of digital media content. Real time audio and video delivery, electronic advertising, digital repositories etc are some of the digital media applications. One of the major impediments to this growth is the lack of effective intellectual property protection of digital media to discourage unauthorized copying and distribution. Conventionally, in analog world, a painting is signed by the artist to attest the copyright and paper money is identified by embossed portrait. These types of signatures and seals have been used since ancient times to identify the creator of the content. However, in the digital world, technologies for manipulating images have made it difficult to distinguish the visual truth. Besides, the characteristics of digitization bring significant changes in copyright issues, which create an urgent need to intellectual property protection on the digitally recorded information. The copyright laws that exist today are inadequate to deal with digital media. This led to the emergence of new technologies to deter unauthorized copying and distribution of digital content. One of such technologies is Digital watermarking, which is today synonymous to digital content protection. Digital watermarking is the process of embedding information into the source content that can be detected and extracted. Watermark is integrated into the content of host signal itself and requires no additional file header or conversion of data format. Unlike cryptographic technologies, digital watermarking does not restrict access to the source content but protects ownership of the content.

Digital watermarking, steganography are techniques under the banner of information hiding. Steganography is used for coveted communication, wherein secret information is concealed behind media content so as to hide its very existence. The basic difference between steganography and digital watermarking is that in the case of former the secret message is more important than the source in which it is embedded but in the later the source content is of primary importance and the information embedded is used to protect the source content.

Current study focuses on investigating various techniques used in digital watermarking for numerous applications, primarily in the context of text, audio, image and video media. The characteristics of a watermark are based on the application and the need for watermarking. The characteristics of the watermark in turn decide the technique to be used for watermarking.

Organization of the paper is as follows. Digital watermarking applications are presented in Section II. Requirements, classification and techniques in watermarking are presented in Section III, section IV deals with various kinds of attacks on watermarks. Finally, conclusions are drawn in Section V.

2. DIGITAL WATERMARKING APPLICATIONS

Digital watermarking is used for numerous applications which include:

2.1 Copyright Protection

Watermarking can be used for copyright protection in text, image, video and audio media and is the most important watermarking application [1][2]. The owner of the digital media can protect his content from being used commercially. This form of copyright protection requires high level of robustness so that the embedded watermark cannot be removed without data distortion. To combat online music piracy, a digital watermark could be added to all recording prior to its release which signifies not only the author of the work, but the user who has purchased a legitimate copy. Newer operating systems equipped with Digital Rights Management (DRM) software will extract the watermark from audio files prior to playing them on the system. The DRM software will ensure that the user has paid for the audio by comparing the watermark to the existing purchased licenses on the system.

2.2 Fingerprinting

A key issue in real time application is illegal distribution of copy righted digital content like movies, which can be avoided by watermarking the video using a technique called fingerprinting. Fingerprinting is used to trace the origin of illegal copies. In this technique, the content owner embeds a different secret code or serial number specific to a customer to the digital data before distributing it, which is used to trace the illegal copies.

2.3 Tamper proofing

Digital photography authentication has become a great concern as they can be easily tampered. Such problems have hindered the application of digital images for courtroom evidence, insurance claims, copyright claims and journalistic photography. The indication of content manipulation (tamper-proofing) from the authorized state could be detected by the usage of a public or fragile watermark.

2.4 Medical Image Watermarking

The evolution of medical information systems, supported by advances in information technology, enables information to be shared between distant health professionals. However, this could pose a threat to privacy of information if security measures are not considered. Medical images can be watermarked with patient identification, prescription information etc.

2.5 Broadcast Monitoring

Watermark can be embedded in commercial advertisements. A computer-based monitoring system could then detect the embedded watermark, to ensure that they receive all of the airtime they purchased from the broadcasters.

2.6 Indexing

Comments, markers or key information related to the data can be inserted as watermarks for the purpose of indexing. This watermarked information is used by a search engine for retrieving the required data quickly and without any ambiguity.

2.7 Bank Monitoring System

Bank monitoring system is another important real time application which could benefit by using video watermarking. Such a system comprises of surveillance video cameras with watermarking facility, such that the video cameras will watermark each frame of the video footage with the bank logo or any secret identification, and then encrypt the video taken using a key. Such material provides good legal evidence in the court of law, and makes sure that video has not been altered after the occurrence of any incident.

Other uses for watermarking technology include embedding auxiliary information which is related to a particular song, like lyrics, album information etc. Watermarking could be used in voice conferencing systems to indicate to others which party is currently speaking. A video application of this technology would consist of embedding subtitles or captioning information as a watermark. Digital watermark has great potential to be used as part of an overall system for managing IP rights, and can be used not only to identify the author of a particular file, but also trace and catalog the path a particular file takes if it is distributed in an unauthorized manner.

Watermarks are designed to permanently reside in the host data. When the ownership of the data is in question, the embedded information can be extracted to completely identify the owner. Applications of digital watermarking are not restricted to the area of copyright management, but can be extended to inclusion of augmentation data [3]. Most of the applications require the watermarking system to be robust against various types of attacks and transformations.

3. DIGITAL WATERMARKING REQUIREMENTS CLASSIFICATION AND TECHNIQUES

To achieve maximum protection of intellectual property with watermarked media, digital watermarks and the watermarking system must satisfy several requirements which include:

- *Perceptual transparency*: The inserted watermark should not affect the quality of the cover media. In case of invisible watermarking, the watermark should go unnoticed as long as the data is not compared with original data.

- *Robustness:* Robustness is a measure of the ability of the embedding algorithm to introduce the watermark in such a way that it is retained in the source content despite several stages of processing. A special class of watermarks called fragile watermarks are intentionally made non-robust intended only for authentication rather than tracing back the source after being processed. Semi fragile watermarks are able to survive standard unintentional processing such as compression for storage.

- *Security:* Security of a watermarking technique can be judged the same way as with an encryption technique. The watermarking algorithm is truly secure, if knowing the exact algorithm to embed and extract data does not help an unauthorized party in actually recovering the original content from the watermarked data.

  Pay load of watermark: The amount of bits that the watermark signal carries depends on the application, for example, for copy protection purpose; a payload of one bit is sufficient.

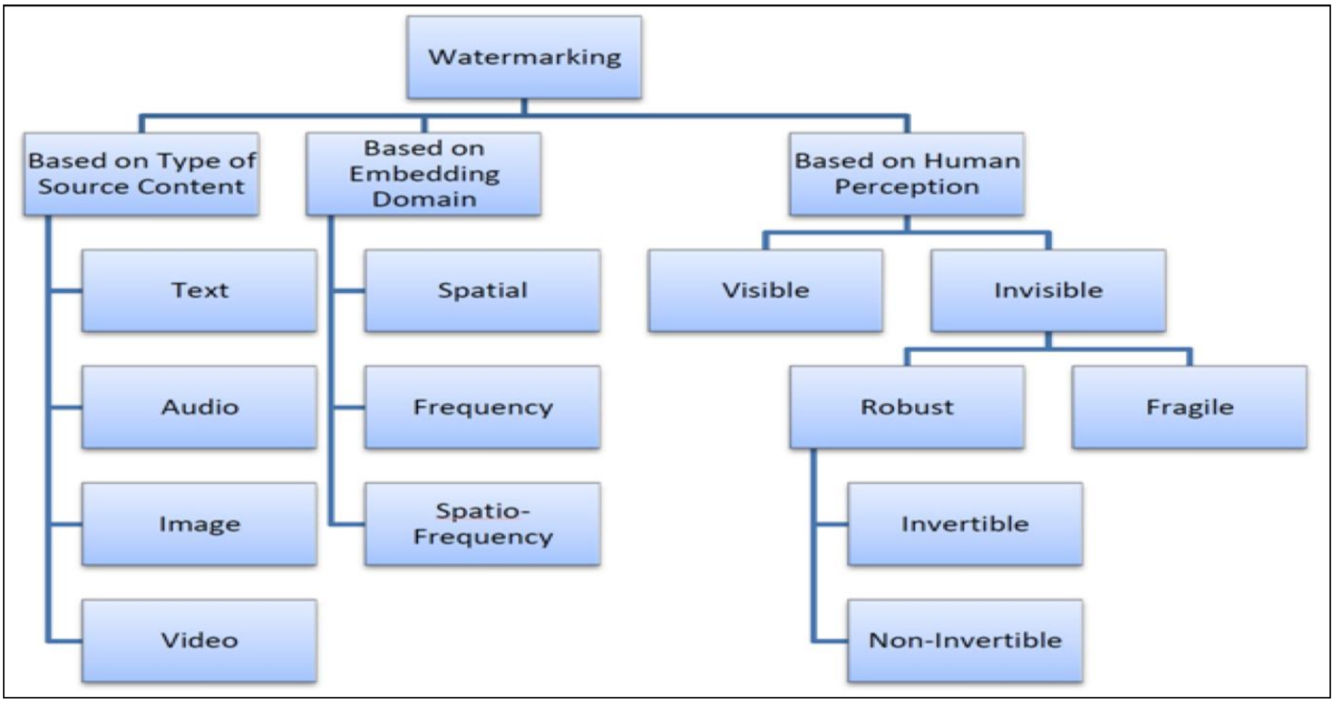

Figure 1: Watermarking Classification

Watermarking granularity is a term used to refer to the number of bits that are actually needed to represent the entire watermark in the source content.

- *Oblivious versus non-oblivious (blind or non-blind):* In applications such as copyright protection and data monitoring, the watermark extraction algorithm can use the original un-watermarked data to find the watermark, this is called non-oblivious watermarking (non-blind watermarking). In other applications such as copy protection and indexing the watermark extraction algorithm does not have access to the un-watermarked data. This significantly raises the difficulty of extraction; such methods are called oblivious watermarking algorithms.

Based on the above requirements, Figure 1 provides a comprehensive classification diagram of different types of digital watermarking.

A variety of signal processing algorithms have been used for digital watermarking. Some of the properties for Watermarking algorithms are: the algorithm should support real-time processing [4], they must be adjustable to different degrees of robustness, quality and different amount of data and also the algorithms should be tunable to different media [5]. The watermarking procedure should rely on a key to ensure security, not on the algorithm’s secrecy. Not all the properties and characteristics of digital watermarks can be achieved using a single technique or algorithm. Multimedia represents amalgamation of several media such as text, image, video, audio etc. each of them exhibiting different characteristics. Digital watermarking algorithms should exploit the statistics and characteristics of the source media [6]. To simplify, we have categorized the various techniques based on the type of source content.

3.1 Text Watermarking

Digital watermarking techniques for text are limited owing to the binary nature of the data and the lack of rich gray scale information. The three main types of text watermarking methods are line-shift coding that vertically shifts the locations of text lines to encode the document; word-shift coding that horizontally shifts the locations of words within text lines to encode the document and feature coding which chooses certain text features and alters those features [7]. The basic features of textual content include word/line and block patterns, background and foreground areas, pattern of inter word spacing etc. These features need to be exploited for a good and robust text watermarking. Text image watermarking algorithms proposed by researchers chiefly rely on patterning inter-word spaces and word classification [8], line-shifting and word-shifting techniques especially on imperceptible modification of spacing of words, spacing of letters, shifting of baselines, modifying the serifs, kerns etc. like the line shift and word shift algorithms proposed by Brassil et al[9].

3.2 Audio Watermarking

Audio watermarking based on domains can be classified as time-domain and frequency-transform domain techniques [10, 11]. Thus the performance of the techniques may vary not only with respect to the robustness and imperceptibility (inaudibility) requirements of audio watermarking but also with respect to the characteristics of the domains. Popular audio watermarking techniques include: Phase Encoding, Spread Spectrum Watermarking, Echo Watermarking etc. Phase encoding watermarking technique exploits the human auditory system’s lack of sensitivity to absolute phase changes and thus encoding the watermark in an artificial phase signal. Spread Spectrum Watermarking technique relies on Direct Sequence Spread Spectrum (DSSS) to spread the watermarked signal over the audible frequency spectrum such that it approximates white noise at a power level as to be inaudible. Echo Watermarking relies on distorting an audio signal in a way which is perceptually dismissed by the human auditory system as environmental distortion. Some of the other audio watermarking techniques are based on Amplitude Modulation [12], Wavelets Transform (DWT), Singular Value Decomposition (SVD) [13] etc. Time Domain Techniques, such as Least Significant Bit (LSB) substitution methods, and Echo Hiding methods, embed the water mark directly in the time domain. Frequency domain audio watermarking uses DFT(Discrete Fourier Transform), DCT (Discrete Cosine Transform) or DWT (Discrete Wavelet Transform) to transform the audio signal to locate appropriate embedding location. Real time audio watermarking techniques are based on Pulse Code Modulation (PCM) in digital instrument [14]. Audio watermarking based on Quantizing Coefficients, quantizes the lowest frequency coefficients of DWT of the audio signals and can be detected in an oblivious way [15]. Audio watermarking using psychoacoustic watermark filtering [16, 17] is another popular audio watermarking. Various blind and non-blind watermarking techniques for digital audio signals using compression expansion of signals are also discussed in [18, 19].

3.3 Image Watermarking

Dorairangaswamy et al proposed an invisible and blind watermarking scheme for copyright protection of digital images [20]. A dual watermarking technique was suggested by S.P. Mohanty et al. [21]. Combination of visible and an invisible watermark is known as dual watermark. In dual watermarking scheme the invisible watermarking is used for the protection or the backup of the invisible watermark. For images that have predominantly texture areas, Bender et al [22] described a texture block method. An invisible watermark was proposed by I.J.Cox et al. [23]. Various kinds of watermarking methods were identified for medical images in [24]. These techniques embed the watermark within region of non-interest (RONI). The main characteristic of these methods is reversibility i.e. once the embedded content is read the watermark can be removed from the image allowing retrieval of the original image losslessly. The concept of a reversible watermark was first introduced by Mintzer et al [25]. In recent times reversible watermarking using wavelet transforms have gained a lot of popularity. Tian applied an integer Haar wavelet transform to an image and embedded the watermark into high-frequency coefficients by difference expansion [26]. Tanaka et al proposed watermarking method for color images and video using Discrete Cosine Transforms [27].

3.4 Video Watermarking

Video watermarking involves embedding information into the frames of the video. The watermark is part of the video itself rather than part of the file format or DRM (Digital Rights Management) system, this technology works independently of the video file format or codec. Video watermarking is an extension of image watermarking and hence the techniques used for image watermarking can be applied to watermark video content as well. Video watermarking can be done on spatial domain, frequency domain or spatio-frequency domain. Spatial domain video watermarking is much simpler than frequency domain video watermarking; however frequency domain watermarking is comparatively more robust and can withstand most of the unintentional attacks. Widely used frequency transforms are DFT (Discrete Fourier Transform) [28], FFT (Fast Fourier Transform) [29], DCT (Discrete Cosine Transform) [30] and DWT (Discrete Wavelet Transform). Wavelet transforms is a new time-frequency analyzing method to localize spatial and frequency domain. Many watermark algorithms are implemented using discrete wavelet transform [31]. It is proved practically that discrete wavelet transform based watermarking is robust due to its filtering characteristics and can withstand most of the attacks. Video watermarking is not just an extension of image watermarking as by exploiting the temporal properties of video higher degree of robustness can be achieved [32].

Every watermarking system consists of a watermark embedder and watermark detector. The most critical part of a successful watermarking system is the selection of the embedding algorithm which is based on the type of the embedding media and the requirements of the watermark. Certain watermarking applications requires watermark to be invisible. Invisible watermarking mandates an addition requirement that the difference between the watermarked content and original content to be imperceptible to the human eye. This can be achieved quantitatively by calculating PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error). The higher the PSNR, the closer the watermarked image is to the original. Additional to invisibility requirement, certain applications could also require the watermark to be reversible and the watermarking system to be blind. All these requirements increase the complexity of the watermarking embedding and detection algorithms. Apart from the quantitative and qualitative measures the watermarking system should also withstand various kinds of attacks discussed in the next section.

4. WATERMARKING ATTACKS

Watermarking systems are susceptible to various types of attacks. Lack of standard benchmarking tools creates problems for content providers. The existing benchmarking tools like Strimark, Unzign etc. could combat a few of the attacks that aim at removal of the watermark from a watermarked content. Main goals of attacks on watermarks and the watermarking systems are to preserve the quality of the source content and/or render the watermark undetectable or un-decodable. These attacks could be either intentional or unintentional. In intentional attacks, the attacker tries to extract the watermark from the embedded media to claim ownership of the content. In unintentional attacks, the watermark is rendered un-decodable by the decoder due to common signal processing applications like cropping, clipping, transformations, compression etc. Attacks on watermarks are categorized as Class A and Class B attacks. Class A attacks deals with removal attacks, synchronization attacks etc. These attacks are carried out through brute-force, statistical averaging, lossy compression, collusion, scrambling etc. In Class B category the attacker attacks the watermarking system rather than the watermarked data. This can be achieved through hacking, cracking, hardware tampering etc. to combat these attacks, watermarks should primarily consist of two components namely dynamic and static components. The dynamic component varies for each user and might average to zero as the result of an attack. The static component, however will not average to zero and therefore will remain present in the attacked content. To withstand most of the attacks, the watermarking technique should take into account the statistics of both, the source content and the watermark i.e. the watermark should be content dependent. Also there is a need for building strongly tamper resistant "unrestricted-key" watermarking schemes in which the attacker knows how to detect a watermark, but despite this knowledge he cannot remove or alter the watermark [33].

5. CONCLUSIONS

This paper provides an overview of the concept of digital watermarking focusing on its various applications. Each application of watermarking dictates the characteristics required by the watermark and the watermarking system. These characteristics should be considered during selection of an appropriate technique to embed the watermark. Apart from using modern approaches of signal processing to provide better and robust watermarks, the features and statistics of the source media as well as the watermark should also play a major role in deciding the technique. Exploiting these features increases the resistance of the embedded watermark to various types of attacks. Digital watermarking is still in its infancy and the complete potential of this concept has not yet been completely utilized. Web based watermarking system using a distributed approach could be one of the future applications of this technology.

6. REFERENCES

[1] Joo Lee and Sung-Hwan Jung: "A survey of watermarking techniques applied to multimedia," Proceedings 2001 IEEE International Symposium on Industrial Electronics (ISIE2001), Volume. 1, pp: 272 -277,[2001].

[2] Jiang Xuehua;, "Digital Watermarking and its Application in Image Copyright Protection," Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on , vol.2, no., pp.114-117, 11-12 [May 2010].

[3] D. Gruhl, A. Lu, and W. Bender. "Echo hiding". In Proceedings of the First Internationational Workshop on information hiding LNCS 1174, pages 295-315, 1996

[4] Christoph Busch, Wolfgang Funk, and Stephen Wolthusen, "Digital watermarking: From concepts to real-time video applications", IEEE Computer Graphics and Applications 19 (1999), no. 1, pp 25–35.

[5] Ingemar J. Cox, Joe Kilian, Tom Leighton, and Talal hamoon, "Secure spread spectrum watermarking for multimedia", Technical Report 95-10, NEC Research Institute, 1995.

[6] F. Hartung and M. Kutter, "Multimedia watermarking techniques," In Proceedings of the IEEE, Vol.87, No.7, pp.1079-1107, July 1999.

[7] Ding Huang; Hong Yan; , "Interword distance changes represented by sine waves for watermarking text images," Circuits and Systems for Video Technology, IEEE Transactions on , vol.11, no.12, pp.1237-1245, Dec 2001

[8] Young-Won Kim; Kyung-Ae Moon; Il-Seok Oh; , "A text watermarking algorithm based on word classification and inter-word space statistics," Document Analysis and Recognition, 2003. Proceedings. Seventh International Conference on, vol., no., pp. 775- 779, 3-6 Aug. 2003.

[9] J.T. Brassil, S. Low, and N.F. Maxemchuk, "Copyright protection for the electronic distribution of text documents," Proceedings of IEEE, Vol.87, No.7, pp.1181- 1196, July 1999.

[10] Acevedo A., "Digital Watermarking for Audio Data in Techniques and Applications of Digital Watermarking and Content Protection", Artech House, USA, 2003.

[11] Arnold M., "Audio Watermarking: Features, Applications and algorithms". In Processings of the IEEE International Conference on Multimedia and Expo, pp. 1013-1016, 2000.

[12] Akira Nishimura, "Presentation of Information Synchronized with the Audio Signal reproduced by Loudspeakers using an AM based Watermark".

[13] Ali Al-Haj (2010), "Digital Watermarking based on the Diescrete Wavelets Transforms and Singular Value Decomposition" proceedings of the European journal of Scientific Research ISSN 1450-216 abd Vol.39 No. 1 pp 6-21.

[14] Kotaro Yamamoto and Munetoshi Iwasiri, (2010), "Real-Time Audio Watermarking Based on Charecteristics of PCM in Digital Instrument", Journal of Information Hiding and Multimedia Signal Processing, (2010), ISSN 2073-4212 and Vol.1, No.2 April 2010.

[15] Zhao Xu, Ke Wang and Xiao-hua Qiao, "Digital Audio Watermarking algorithm Based on Quantizing Coefficients" , proceedings of the 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing(IIH-MSP'06.

[16] Nedeljko Cvejic, Tapio Seppanen, " Improving Audio Watermarking Scheme Using Psychoacoustic Watermark Filtering".

[17] W.N. Lie and L.C. Chang, "Robust and High-Quality Time-Domain Audio Watermarking Subject to Psychoacoustic Masking ", proceedings of IEEE International symposium on circuits and system, 2001, 2 , pp. 45-48.

[18] Hyoung Joong Kim, "Audio Watermarking Techniques".

[19] Say Wei Foo; "Non-blind audio-watermarking using compression-expansion of signals," Circuits and Systems, 2008. APCCAS 2008. IEEE Asia Pacific Conference on, vol., no., pp.1288-1291, Nov. 30 2008-Dec. 3 2008.

[20] M.A. Dorairangaswamy, B.Padmavathi, "An Effective Blind Watermarking Scheme for Protecting Rightful Ownership of Digital Images", IEEE international conference TENCON 2009.

[21] S.P.Mohanty, et al., "A Dual Watermarking Technique for Images", Proc. 7th ACM International Multimedia Conference, ACM-MM'99, Part 2, pp. 49-51, Orlando, USA, Oct. 1999.

[22] Bender W., Gruhl D., Morimoto N. and Lu A. 1996, "Techniques for Data Hiding", IBM Systems Journal, Vol. 35, No. 3 & 4, pp. 313-335.

[23] I.J.Cox et. al., "Secure Spread Spectrum Watermarking of Images, Audio and Video", Proc

IEEE International Conf on Image Processing, ICIP-96, Vol.3, pp 243-246.

[24] G.Coatrieux H. Maitre, B.Sankur, Y. Rolland, R. Collorec, "Relevance of Watermarking in Medical Imaging," in Proc. IEEE Int. Conf. ITAB, USA, 2000, pp. 250-255.

[25] F. Mintzer, J. Lotspiech, and N. Morimoto, "Safeguarding digital library contents and users: Digital watermarking," D-Lib Mag., Dec.1997.

[26] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896,Aug.2003.

[27] K. Tanaka, Y. Nakamura, and K. Masui, "Embedding secret information into a dithered multilevel image," In Proceedings of the 1990 IEEE Military Communications Conference, pp. 216-220, September 1990.

[28] C.-M. Pun, " A Novel DFT-based Digital Watermarking System for Images," Proceedings of the 8th International Conference on Signal Processing, Volume II of IV, pp. 1245-1248, IEEE Press, Guilin, China, November 2006.

[29] Lu Ye; "FFT Based Blind Watermarking Algorithm for Three Dimensional Motion Picture", Internet Technology and Applications, 2010 International Conference on , vol., no., pp.1-4, 20-22 Aug. 2010 doi: 10.1109/ITAPP.2010.5566494

[30] Yang, M. Schmucker, W. Funk, C. Busch, and S. Sun, "Integer DCT-based reversible watermarking for images using companding technique," in Proc. SPIE, Security, Steganography, andWatermarking of Multimedia Contents, San Jose, CA, Jan. 2004, pp. 405–415.

[31] Sunil Lee, Chang D. Yoo and Ton Kalker, "Reversible Image Watermarking Based on Integer to Integer wavelet Transform", IEEE Transactions on Information Forensics and Security, Vol. 2 No. 3, September 2007

[32] M.D. Swanson, B. Zhu and A.H. Tewfik,"Multiresolution scene-based video watermarking using perceptual models", IEEE Journal on selected Areas in communications, vol. 16, no. 4, pp. 540-550, May 1998.

I. Cox, J. Linnartz, "Some General Methods for Tampering with Watermarks", IEEE Journal on sel. areas, in Comm., vol. 16, no. 4, May 1998.