



A Study and Survey on Digital Image Watermarking

KEYWORDS

Watermarking, Advance Techniques, Application of watermarking, Features of digital watermarking, DFRFT.

Grishma H. Goswami

PG Scholar, SPBPEC, SIT, Linch, Mehsana-Gujarat

Mr.Krunal R. patel

Asst Professor, IT Department SPBPEC, SIT, Linch, Mehsana-Gujarat

ABSTRACT This paper surveys in recent advances in watermarking techniques in digital images. Digital watermarking is to include subliminal information about multimedia information to provide a security service or simply a labeling application. It's possible to recover the embedded message, if the information is some non-destructive attacks, it's malicious or not. It's commercial application range from copyright protection to digital right management. This paper include Watermarking introduction, features of digital watermarking, types of watermarking, application of digital watermarking, watermarking techniques. In my major work describes a watermark embedding technique for images using discrete fractional Fourier transform.

I. INTRODUCTION

watermarking is the process of embedding secret information (i.e. watermark) into digital multimedia data such as texts, audio, images, and video by taking into account the limitations of human perception system such as Human Auditory System(HAS) and Human Visual System(HVS). These techniques can be used on any type of digital data including still images, movies, and music [1]. Methods are based on change of least significant bits (LSBs) of the pixel values of an image.

A digital watermarking is a signal permanently embedded into digital multimedia data i.e., host signal (audio, video, images and text) that can be detected or extracted. That means of computing operations in order to make assertions about the multimedia data [3-5].

Watermarks and attacks on watermarks are sides of the same coin. The goal of both is to preserve the value of the digital multimedia data. However, the goal of a watermark is to be robust enough to resist attacks but not at the expense of altering the value of the multimedia data being protected [3].

This paper is organized as follows: Section II describes important features of digital watermarking.

II. FEATURES OF DIGITAL WATERMARKING

Important features of digital watermarking are imperceptibility, robustness and embedding capacity.

a) Imperceptibility: The embedded watermarks should be imperceptible both perceptually as well as statistically and do not change the aesthetics of the multimedia content after watermarking. The watermarks do not create visible artifacts in still images, alter the bit rate of video or introduce audible artifacts in audio signals.

b) Robustness: Depending on the application, the digital watermarking technique can support different levels of robustness against changes made to the watermarked content. If digital watermarking is used for copyright owner identification.

c) Embedding Capacity: The watermarking algorithm should embed predefined number of bits to be hidden in the host signal. This number will depend on the field of digital

watermarking that the above three requirements compete with each other.

III. TYPES OF WATERMARKING

Each of the different types of watermarking techniques mentioned below has different applications.

1) Robust and Fragile Watermarking: Robust watermarking is a technique in which modification to the watermarked signal will not affect the watermark. As opposed to this, fragile watermarking is a technique in which watermark gets destroyed when watermarked signal is modified or tampered with.

2)Visible and Transparent Watermarking: Visible watermarks are ones which are embedded in visual content in such a way that they are visible when the content is viewed. Transparent watermarks are imperceptible and they cannot be detected by just viewing the digital content.

3)Public and Private Watermarking: In public watermarking, users of the content are authorized to detect the watermark while in private watermarking the users are not authorized to detect the watermark.

4)Asymmetric and Symmetric Watermarking: Asymmetric watermarking is a technique where different keys are used for embedding and detecting the watermark. In symmetric watermarking, the same keys are used for embedding and detecting the watermarks.

5)Blind and Non-blind Watermarking: Watermarking in which original host signals is not required for watermark detection/extraction is known as blind watermarking. If original host signal is required in watermark detection/extraction then this watermarking is said non-blind (informed) type.

IV. APPLICATION OF WATERMARKING

Digital watermarking techniques have wide ranging application. Some of the applications are enlisted below:

1) Copyright protection: Digital watermarking can be used to identify and protect copyright ownership. Digital content can be embedded with watermarks depicting metadata identifying the copyright owners.

2)Copy protection: Digital content can be watermarked to indicate that the digital content can be illegally replicated.

Devices capable of replication can then detect such watermarks and prevent unauthorized replication of the content.

3) Tamper Proofing: Digital watermarks, which are fragile in nature, can be used for tamper proofing. Digital content can be embedded with fragile watermarks that get destroyed whenever any sort of changes is made to the content. Such watermarks can be used to authentication the content.

4) Broadcast Monitoring: Digital watermarks can be used to monitor broadcasted content like television and broadcast radio signals.

V. DIGITAL WATERMARKING TECHNIQUES

In this section, some important digital watermarking techniques for multimedia data such as audio, images and video will be discussed in brief. Recently use of watermarking techniques can be grouped into three different classes. The first include the time-domain/spatial-domain watermarking techniques. In these techniques, the watermark signal is embedded by directly modified the sample values/pixel values of the original audio signal/image. A part from this, considerations similar to those drawn for still images are also, in general, valid for video.

1) SPATIAL-DOMAIN WATERMARKING TECHNIQUES

The most straightforward way to hide a watermark signal within a host signal is to directly embed a watermark in the original host signal. For audio signal, this direct watermarking technique is called time-domain watermarking, whereas for still images this corresponds to spatial-domain watermarking.

Several audio watermarking algorithms in time-domain have been proposed. The first and the most common one is to embed the watermark in time domain. One of the simplest techniques under this category is Least Significant Bit (LSB) alteration. In this technique, LSB of each sample value of the host audio signal is made 0 or 1 depending upon the watermark bit to be embedded [6]. A large amount of data can be embedded into an audio signal using this method. Echo hiding is another audio watermarking technique in time domain which embeds the watermark by introducing an echo [7]-[9]. In the most basic echo watermarking scheme, the watermark information is encoded in the signal by modifying the delay between the host signal and echo signal obtained from host signal. This means that two different values of delay (offset values) i.e.

Dt_1 and Dt_2 are used in order to encode either a 0 or 1. Both offset values have to be carefully chosen in a way that makes the watermark both inaudible and extractable or recoverable [7]. If only one echo was produced from the original audio signal, only one bit of information could be encoded. Therefore, the original audio signal is broken down into blocks before the encoding process begins. Another category of watermarking techniques in time-domain is Quantization Index Modulation (QIM) watermarking methods [10]-[11].

QIM methods have shown a very good rate-distortion-robustness trade-offs and are provably better than additive spread spectrum and generalized LSB methods, against bounded perturbations. QIM refers to modulating an index or sequence of indices with the watermark information and quantizing the host signal with the associated quantizer or sequence of quantizers [11]-[12]. Due to its advantages of low computational complexity, large capacity, great robustness and blind extraction, it is widely used in recently

developed digital audio watermarking schemes [13].

The basic idea of spread spectrum is to encode audio signal by spreading the watermark information [14] across as much of the audible spectrum as possible. In this technique, the masking regions are first computed and the watermarks is then embedded into these areas [15].

Several spatial-domain watermarking techniques for images are proposed in [15] one technique consists of embedding a texture-based watermark into a section of the image with identical texture.

Assuming for average, without the watermark, this value is zero for image data. A difference of this approach is described in [18], where more information can be inserted in the multimedia data. Another spatial domain technique is proposed in [23].

2) TRANSFORM-DOMAIN WATERMARKING TECHNIQUES

In transform-domain watermarking techniques, the watermark is inserted into the coefficients of digital transform of the host asset or host signal. Most commonly used transforms preferred for watermark embedding in the frequency domain are DFT, DCT, DWT, DFRFT etc. Usually, transform-domain watermarking techniques exhibit a higher robustness to attacks. In particular, by spreading the watermark over the whole asset, they are intrinsically more resistant to cropping than asset domain techniques.

Perceptual constraints aiming at ensuring invisibility can also be readily incorporated into frequency domain representations, e.g. by avoiding the modification of low spatial frequencies where alterations may produce very visible distortions.

For transform-domain audio watermarking, the one-dimensional (1D) versions of various transforms that were used for 2D still images are the most suitable.

Various transform-domain audio watermarking techniques [24]-[31] were proposed. The transform can be DFT [24]-[26], DCT [27].

A common transform framework for images is the block-based on DCT is a fundamental building block of current image coding standards and video coding standards are respectively such as JPEG and MPEG coders. The watermark embedding algorithm could be described as $x = s(1 + aw)$, where s is the original host signal, w is the watermark consisting of a random, Gaussian distributed sequence, a is a watermark scaling factor and x is the watermarked signal. Parameter a is used to provide a good trade-off between imperceptibility and robustness.

The watermark was embedded in wavelet domain and detected in the Fractional Fourier Transform (FRFT) domain. This method does not need the original image for watermarking algorithm using FRFT was presented. In this technique, multiple chirps were used as watermark which was embedded in the spatial domain directly and watermark was detected in FRFT domain. This algorithm has good security, imperceptibility and excellent resistant against the attacks of JPEG compression, noise, cropping and filtering.

VI. CONCLUSION

In this paper we have surveyed of current advances in digital images watermarking. Also, study the watermarking properties, applications and techniques. These techniques are classified into several categories depending upon the

domain in which the hidden data is inserted, the size of hidden data and the requirement of which is the hidden data is to be extracted. A few techniques of these are used for audio and video watermarking.

REFERENCE

- [1] C. S. Lu, "Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property", Idea Group Publishing 2005. [2] R.G. Schyndel, A. Tirkel, and C.F. Osborne, "A Digital Watermarking" Proceedings of IEEE International Conference on Image Processing, ICIP-1994, pp. 86-90, 1994. [3] M. Potdar, S. Han, and E. Chang, "A Survey of Digital Image Watermarking Techniques", IEEE International Conference on Industrial Informatics, pp. 709-716, 2005. [4] M. Barni and F. Bartolini, "Watermarking Systems Engineering Enabling Digital Assets Security and Other Applications", Marcel Dekker, 2004. [5] N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Steganography", IEEE Security and Privacy, pp. 32-44, 2003. [6] Y. Xiong and Z. X. Ming, "Covert Communication Audio Watermarking Algorithm Based on LSB", International Conference on Communication Technology, ICCT-2006, pp. 1-4, 2006. [7] N. F. Johnson, and S. C. Katzenbeisser, A Survey of Steganographic Techniques, First Edition, Artech House Boston, M.A., pp. 43-78, 2000. [8] B. S. Ko, R. Nishimura, and Y. Suzuki, "Time-Spread Echo Method for Digital Audio Watermarking", IEEE Transactions on Multimedia, Vol. 7, No. 2, pp. 212-221, April 2005. [9] H.O. Oh, J.W. Seok, J.W. Hong, and D.H. Youn, "New Echo Embedding Technique for Robust and Imperceptible Audio Watermarking", Proceedings of ICASSP 2001, pp. 1341-1344, 2001. [10] Y.W. Liu, and J.O. Smith, "Watermarking Sinusoidal Audio Representations by Quantization Index Modulation in Multiple Frequencies", Proceedings of ICASSP 2004, Vol. 5, pp. 373-376, 2004. [11] B. Chen and G.W. Wornell, "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding", IEEE Transactions on Information Theory, Vol. 47, No. 4, pp. 1423-1443, 2001. [12] B. Chen and G.W. Wornell, "Digital Watermarking and Information Embedding using Dither Modulation", Proceedings of IEEE Second Workshop on Multimedia Signal Processing, M.I.T., U.S.A., pp. 273-278, 1998. [13] S. Yang, W. Tan, Y. Chen, and W. Ma, "Quantization-Based Digital Audio Watermarking in Discrete Fourier Transform Domain", Journal of Multimedia, Vol. 5, No. 2, pp. 151-158, April 2010. [14] J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for multimedia", IEEE Transactions on Image Processing Vol. 6, pp. 1673-1687, Dec. 1997. [15] W. Bender, D. Gruhl, N. Morimoto, and A. Lu Techniques for Data Hiding, IBM Systems Journal, Vol. 35, Nos. 3 & 4, pp. 313-226, 1996. [16] G. Caronni, Assuring Ownership Rights for Digital Images, Proceedings of Reliable IT Systems, VIS-1995, pp. 251-263, 1995. [17] K. Tanaka, Y. Nakamura, and K. Matsui, Embedding Secret Information a Dithered Multi-Level Image, Proceedings of Conference on Military Communications, pp. 216-220, 1990. [18] I. Pitas, A Method of Signature Casting on Digital Images, Proceedings of IEEE International Conference on Image Processing, ICIP-1996, Vol. 3, pp. 215-218, 1996. [19] R. B. Wolfgang and E. J. Delp, A Watermark for Digital Images, Proceedings of IEEE International Conference on Image Processing, ICIP-1996, Vol. 3, pp. 219-222, 1996. [20] R. G. Schyndel, and C. Osborne, A Two-Dimensional Watermark Proceedings of DICTA-1993, pp. 378-383. [21] R. B. Wolfgang and E. J. Delp, Fragile Watermarking using the vwd2 Watermark, Proceedings of SPIE Conference on Security and Watermarking of Multimedia Contents, San Jose, Vol. 3657, pp. 204-213, 1999. [22] S. Walton, Information Authentication for a Shppery New Age, Dr. Dobbs Journal, Vol. 20, No. 4, pp. 18-26, April 1995. [23] M. Kutter, F. Jorden, and F. Bossen, Digital Watermarking of Color Images using Amplitude Modulation, Journal of Electronic Images, Vol. 7, No. 2, pp. 326-332, April 1998. [24] S. Yang, W. Tan, Y. Chen, and W. Ma, "Quantization-Based Digital Audio Watermarking in Discrete Fourier Transform Domain", Journal of Multimedia, Vol. 5, No. 2, pp. 151-158, April 2010. [25] L. Xie, J. Zhang and H. He, "Robust Audio Watermarking Scheme Based on Non-uniform Discrete Fourier Transform", Proceedings of IEEE International Conference on Engineering of Intelligent Systems, pp. 1-5, 2006. [26] J. Singh, P. Garg, and A. N. de, "Audio Watermarking using Spectral Modifications", International Journal of Signal Processing, Vol. 5, pp. 297-301, 2009. [27] X. Y. Wang and H. Zhao, "A Novel Synchronization Invariant Audio Watermarking Scheme Based on DWT and DCT", IEEE Transactions on Signal processing, Vol. 54, No. 12, pp. 4835-4840, 2006. [28] M. Ketcham, and S. Vongpradhip, "Intelligent Audio Watermarking using Genetic Algorithm in DWT Domain", International Journal of Intelligent Technology, Vol. 2, No. 2, pp. 135-140, 2007. [29] Y. Wu and S. Shimamoto, "A Survey on DWT-Based Digital Audio Watermarking for Mobile Ad Hoc Network", Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, Vol. 2, pp. 247-251, 2006.