A Study on Features, Types, Applications and Techniques of Digital Image Watermarking

G S Pradeep Ghantasala
Dept. of Computer Science Engineering
Brilliant Institute of Engineering and Technology
Hyderabad, India
ggspradeep@gmail.com

Abstract - This paper surveys in recent advances in watermarking techniques in digital images. Digital watermarking is toinclude subliminal information about multimedia information to provide a security service or simply a labelingapplication. It's possible to recover the embedded message, if the information is some non-destructive attacks, it's malicious ornot. 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, watermarkingtechniques. In my major work describes a watermark embedding technique for images using discrete fractional Fourier transform.

Keywords: Watermarking, HAS, HVS, QIM,FRFT

I. INTRODUCTION

Watermarking is the process of embedding secret information(i.e. watermark) into digital multimedia data such astexts, audio, images, and video by taking into account thelimitations of human perception system such as HumanAuditory System(HAS) and Human Visual System(HVS).These techniques can be used on any type of digital dataincluding still images, movies, and music. Methods arebased on change of least significant bits (LSBs) of the pixelvalues 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. Thatmeans of computing operations in order to make assertions about the multimedia data.

Watermarks and attacks on watermarks are sides of the samecoin. The goal of both is to preserve the value of the digitalmultimedia data. However, the goal of a watermark is to berobust enough to resist attacks but not at the expense ofaltering the value of the multimedia data being protected.

II. FEATURES OF DIGITAL WATERMARKING

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

a) Imperceptibility: The embedded watermarks should beimperceptible both perceptually as well as statistically anddo not change the aesthetics of the multimedia content afterwatermarking. The watermarks do not create visible artifactsin still images, alter the bit rate of video or introduce audibleartifacts in audio signals.

b) Robustness: Depending on the application, the digitalwatermarking technique can support different levels ofrobustness against changes made to the watermarkedcontent. 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 thehost signal. This number will depend on the field of digital watermarking that the above threerequirements competewith each other.

III. TYPES OF WATERMARKING

Each of the different types of watermarking techniquesmentioned below has different applications.

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

2) Visible and Transparent Watermarking: Visiblewatermarks are ones which are embedded in visual contentin such a way that they are visible when the content is viewed.Transparent watermarks are imperceptible and they cannotbe detected by just viewing the digital content.

3) Public and Private Watermarking: In publicwatermarking, users of the content are authorized to detectthe watermark while in private watermarking the users arenot authorized to detect the watermark.

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

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

IV. APPLICAION OF WATERMARKING

Digital watermarking techniques have wide rangingapplication. Some of the applications are enlistedbelow:

1) Copyright protection: Digital watermarking can be usedto identify and protect copyright ownership. Digital contentcan be embedded with watermarks depicting metadataidentifying the copyright owners.

2) Copy protection: Digital content can bewatermarked toindicate that the digital content can be illegally replicated.Devices capable of replication can then detect suchwatermarks and prevent unauthorized replication of thecontent.

3) Tamper Proofing: Digital watermarks, which are fragile innature, can be used for tamper proofing. Digital content canbe embedded with gracklewatermarks that get destroyedwhenever any sort of changes is made to the content. Suchwatermarks can be used to authentication the content.

4) Broadcast Monitoring: Digital watermarks can be used tomonitor broadcasted content like television and broadcastradio signals.

V. DIGITAL WATERMARKING TECHNIQUES

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

1) SPATIAL-DOMAIN WATERMARKING TECHNIQUES

The most straightforward way to hide a watermark signalwithin a host signal is to directly embed awatermark in theoriginal host signal. For audio signal, this direct watermarking technique is called time – domainwatermarking, whereas for still images this corresponds tospatial-domain watermarking.

Several audio watermarking algorithms in time-domain have been proposed. The first and the most common one is toembed the watermark in time domain. One of the simplesttechniques under this category is Least Significant Bit (LSB)alteration. In this technique, LSB of each sample value of thehost audio signal is made 0 or 1 depending upon the watermark bit to be embedded. A large amount of datacan be embedded into an audio signal using this method.Echo hiding is another audio watermarking technique intime domain which embeds thewatermark by introducing an echo. In the most basic echo watermarking scheme,the watermark information is encoded in the signal bymodifying the delay between the host signal and echo signalobtained from host signal. This means that two differentvalues of delay (offset values) i.e.

Dt1 and Dt2 are used in order to encode either a 0 or 1. Bothoffset values have to be carefully chosen in a way that makesthe watermark both inaudible and extractable or recoverable. If only one echo wasproduced from the originalaudio signal, only one bit of information could be encoded.Therefore, theoriginal audio signal is broken down intoblocksbefore the encoding process begins. Anothercategory of watermarking techniques in time-domain isQuantization Index Modulation (QIM) watermarking

methods.

QIM methods have shown a very good rate-distortion robustnesstrade-offs and are probably better then additivespread spectrum and generalized LSB methods, againstbounded perturbations. QIM refers to moduling an index orsequence of indices with the watermark information andquantizing the host signal with the associated quantizer or sequence of quantizers. Due to its advantages oflowcomputational complexity, large capacity, greatrobustness and blind extraction, it is widely used in recently developed digital audio watermarking schemes.

The basic idea of spread spectrum is to encode audio signalby spreading the watermark information across as muchof the audible spectrum as possible. In this technique, the masking regions are first computed and the watermarks arethen embedded into these areas.

Several spatial-domain watermarking techniques for imagesare proposed in one technique consists of embeddinga texture-based watermark into a section of the imagewith identical texture.

Assuming for average, without the watermark, this value iszero for image data, where more information can be inserted inthe multimedia data.

2) TRANSFORM-DOMAIN WATERMARKING TECHNIQUES

In transform-domain watermarking techniques, theWatermark is inserted into the coefficients of digitalTransform of the host asset or host signal. Most commonlyused transformspreferred for watermark embedding in thefrequency domain are DFT, DCT, DWT, DFRFT etc. Usually,transform-domain watermarking techniques exhibit a higherrobustness to attacks. In particular, byspreading thewatermark over the whole asset, they are intrinsically moreresistant to cropping then asset domain techniques.

Perceptual constraints aiming at ensuring invisibility can alsobe readily incorporated into frequency domain representations, e.g. by avoiding the modification of low spatialfrequencies where alterations may produce very visibledistortions.

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

A common transform framework for images is the block basedon DCT is a fundamental building block of currentimage coding standards and video coding standards arerespectively such as JPEG and MPEG coders. The watermarkembedding algorithm could be described as x=s(1+aw),where s is the original host signal, w is the watermarkconsisting of a random, Gaussian distributed sequence, a is awatermark scaling factor and x is the watermarked signal.Parameter a is used to provide a good trade-off betweenimperceptibility and robustness.

The watermark was embedded in wavelet domain anddetected in the Fractional Fourier Transform(FRFT) domain.This method does not need the original image forwatermarking algorithm using FRFT was presented. In thistechnique, multiple chirps were used as watermark whichwas embedded in the spatial domain directly andwatermarkwas detected in FRFT domain. This algorithm has goodsecurity, imperceptibility and excellent resistant against theattacks of JPEG compression, noise, cropping and filtering.

VI. CONCLUSION

In this paper we have surveyed of current advances in digitalimages watermarking. Also, study the watermarkingproperties, applications and techniques. These techniques are classified intoseveral categories depending upon the domain inwhich the hidden data is inserted, the size ofhidden data and the requirement of which is the hidden datais to be extracted. A few techniques of these are used foraudio and video watermarking.

VII.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 IEEEInternational Conference on ImageProcessing, ICIP-1994, pp. 86-90, 1994.

[3] M. Potdar, S. Han, and E. Chang, “A Survey of Digital Image Watermarking Techniques”, IEEE International Conference onIndurstial 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 Bosten, M. A. , pp. 43-78, 2000.

[8] B. S. Ko, R. Nishimura, and Y.Suzuki, “Time-Spread Echo Method for Digital AudioWatermarking”, 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 Frequenceies”, 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 InformationEmbedding”, IEEE Transactions on Information Theory, Vol. 47, No. 4, pp. 1423-1443, 2001.

[12] B. Chen and G.W. Wornell, “DigitalWatermarking and InformationEmbedding 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 formultimedia”, IEEE Transactions on ImageProcessing Vol. 6, pp. 1673-1687,
Dec. 1997.

[15] W. Bender, D. Gruhl, N. Morimoto, and A. Lu Techniques for Data Hiding □, IBM SystemsJournal, 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, EmbeddingSecret Information a Dithered Multi-Level Image, Proceedings of Conference on Military Communications, pp. 216-220, 1990.

[18] I. Pitas, A Method of Signature Castingon 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, AWatermark 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.Osbome, A Two-Dimensional Watermark Proceedings of DICTA-1993, pp. 378-383.
R. B. Wolfgang and E. J. Delp, Fragile Watermarking using the vw2d Watermark,

[21] Proceedings of SPIE Conference on Security and Watermarking of Multimedia Contents, San Jose, Vol. 3657, pp. 204-213, 1999.

[22] S. Walton, InformationAuthentication 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 ColorImages 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-BasedDigital 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, “RobustAudio Watermarking Scheme Based on Non-uniform Discrete Fourier Transform”, Proceedings of IEEE International Conference on Engineering ofIntelligent Systems, pp. 1-5, 2006.

[26] J. Singh, P. Garg, and A. N. de, “AudioWatermarking using Spectral Modifications”, International Journal of Signal Processing, Vol. 5, pp. 297-301, 2009.

[27] X. Y. Wangand H. Zhao, “A NovelSynchronization Invariant Audio Watermarking Scheme Based on DWT and DCT”, IEEETransactions 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 ofIntelligent 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 HocNetwork”, Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, Vol. 2, pp. 247-251, 2006.