IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 4, Ver. I (Jul - Aug .2015), PP 34-38
www.iosrjournals.org

Digital Watermarking: a Technical Overview

Surajit Sur[1], Rabel Guha Roy[2], Subhro Chakraborty[3]
[1,] *(Asst. Prof.,Ece Dept.,University Of Engineering & Management,Jaipur,India)*
[2]*(Asst. Prof.,Cse Dept.,University Of Engineering & Management,Jaipur,India)*
[3]*(Asst. Prof.,Civil Dept.,University Of Engineering & Management,Jaipur,India)*

Abstract. *Digital watermarking technology has been playing an important role in protecting copyrights in images, audio and video. these can be accurately copied and arbitrarily distributed more easily. Watermarking algorithm has good robustness against the attacks like rotation, image compression, noise addition, filtering and MP4 compression etc. The most popular algorithm in spatial domain is LSB methods. In transform domain watermarking algorithms based on DCT,DWT, discrete Hadamard transform, singular value decomposition and discrete Fourier transform all are discusses this literature. Digital watermarking is the process of embedding information into a digital signal in a way that it difficult to remove.*

Keywords: *DWT,DCT,DHT, patchwork, alpha blending, invisible image watermarking, audio and video watermarking.*

I. Introduction

The growth of high speed computer networks and that of the internet has explored. Cryptography is an effective solution for distribution problem, but in most cases has to tied to specialized-and costly-hard-ware to create tamper-proof devices to avoid direct access to data in digital format. most cryptographic protocols are concerned with secured communications. Access control in set-top-boxes used for digital television demodulation and decoding succeed in avoiding unauthorized access to programs that are being broadcast in scrambled from[1]but fail to including further storage and illegal dissemination actions. Digital watermark completely characterizes by the person who applies it and, therefore, marks it as being his intellectual property.The imperceptibility and robustness are desirable characteristics of watermark.The statistical analysis should not produce any advantage from theattacking point of view. Finally, the watermark should withstand multiple watermarking to facilitate traitor tracing[2]. There are many shift in transform technique like DCT to wavelet based image compression methods, Watermarking schemes operating in wavelet transform domain[4] have become more interesting. A transparent and robust watermark should be such that the watermark is detectable in the host image. The proper selection of the frequency transform is dependent on the fact which is better in image transform approximates properties[5] of the HVS(Human Visual System) the easier is to put more energy in the embedded signal without causing perceptible distortion. DWT more effective for embedding and decoding technique. Here are so many attacks on digital watermarking like intentional and unintentional attacks against security of watermarking system. The attacks are categorized as geometrical, cryptographically and protocol attacks. However the estimation based attack on estimated data which sorts of attacks are newborn on research area

II. History Of Digital Watermarking

The secrete communication based on steganographic methods which invented by Greek philosopher Herodotus.He ia the father of steganographic history[7]. The earliest allusion to secret writing in the West appears in Homer's llaid [6]. From literature of Ovid in his "Art of love" stenography [8],[9] is an important technique to hide sympathetic links using milk to write invisibly. Chemically affected sympathetic links were developed in World Wars 1and 2.The origin of steganography is biological and physiological which use in 1500's after the appearance of Trithemius' book on the subject "steganographia".The "semagrams" and the "open code"[8],[10] are used in Linguistic steganography which is the branch of steganography which consists of linguistic or language form of hidden writing. A semagram is a secret message .watermarking technique has developed from steganography. It used in old paper manufacturing company[11].

III. Classification Of Watermarking

Digital Watermarking techniques can be classified as Text Watermarking, Image Watermarking, Audio Watermarking, and Video Watermarking. In other way, the digital watermarks can be divided into three different type's as follows visible watermark, Invisible-Robust watermark, Invisible-Fragile watermark, Dual watermark.

IV. Techniques Of Watermarking

IV. A.Frequency Domain Watermarking

In these methods selected frequencies can be altered. Because high frequencies will be lost by compression or scaling so that the watermark signal is applied to lower frequencies that containing important elements of the original picture.These techniques are like Fourier Transform,DTFT,DFT,DCT,DWT etc.

IV.B. Spread Spectrum

This technique can be used for both spatial domain and frequency domain. The spread spectrum method has the advantage that the watermark extraction is possible without using the original unmarked image

IV.C.Spatial Domain

Techniques in spatial domain class generally share the following characteristics like The watermark is applied in the pixel domain, No transforms are applied to the host signal during watermark embedding, Combination with the host signal is based on simple operations, in the pixel domain.

V. Working Methods

V.A. Image Watermarking

V.A.a Spatial Domain Analysis

Spatial domain watermarking is performed by modifying values of pixel color samples. The most common algorithm using spatial domain watermarking in LSB[12] bit for hiding image by the technique of artificial intelligence. the least-significant bit plane of a grayscale cover image and replaces it with binary watermark. Since that watermark is smaller than the cover image, we need several copies of you watermark together in order to achieve the correct size[13]. In a digital image, information can be inserted directly into every bit of image information or the more busy areas of an image can be calculated so as to hide such messages in less perceptible parts of an image [14]. Hao Luo et al [15], proposed a self-embedding watermarking scheme for digital images.They proposed algorithm used the cover image as a watermark. It generates the watermark by halftoning the host image into a halftone image. The watermark is retrieved from the LSB of the suspicious image and inverse permuted. Wen-Chao Yang et al [16] used the PKI (Public-Key Infrastructure), Public-Key Cryptography and watermark techniques to design a novel testing and verifying method of digital images and Also Hong Jie He et al [17], proposed a wavelet-based fragile watermarking scheme for secure image authentication. Sung-Cheal

Byun et al [18], proposed a fragile watermarking scheme for authentication of images. They used singular values of singular value decomposition (SVD) of images to check the integrity of images. Gil-Je Lee et al [19] presented a new LSB digital watermarking scheme by using random mapping function. Saeid Fazli et al presented imperceptibility and robustness of LSB watermarking using SSIM Quality Metrics. The new watermarking scheme[20] based on log-average luminance. It introduce a monochrome image of 1024 bytes is used as the watermark. If the byte of the watermark image represented white color (255) a value a is added to the image pixel luminance value, if it is black (0) the a is subtracted from the luminance value. To extract the watermark, the selected blocks are chosen by difference between the luminance value of the watermarked image pixel and the original image pixel is greater than 0, the watermark pixel is supposed to be white, otherwise it supposed to be black. It efficient against changing the watermarked image to grayscale. Debjyoti Basu et al proposed Bit Plane Index Modulation (BPIM) based fragile watermarking scheme for authenticating RGB color image. By embedding R, G, B component of watermarking image in the R, G, B component of original image, embedding distortion is minimized by taking least significant bit (LSB). An image watermarking method based on the human visual system. The new classes of embedding methods, termed quantization index modulation (QIM) and distortion-compensated QIM (DC-QIM).it realizations technique in the form of dither modulation. These include both additive white Gaussian noise (AWGN)[21] channels, which may be good models for hybrid transmission applications such as digital audio broadcasting, and mean-square-error-constrained attack[22] channels that model private-key watermarking applications. In invisible image watermarking median filter algorithm [23,24] is implemented for the de-noising of highly corrupted images and edge preservation. Mean, Median and improved mean filter is used for the noise detection[25].

V.A.b Frequency Domain or Transform Domain Technique

In this process firstly the gray scale host image is taken and 2D DWT (Discrete Wavelet Transform)[26]is applied to the image which decomposes image into four components low frequency approximation, high frequency diagonal, low frequency horizontal ,low frequency vertical components. In the same technique DWT is also applied to the watermark image which is to be embedded in the host image. The technique used here for inserting the watermark is alpha blending[27]. In this technique the decomposed components of the host image and the watermark which are obtained by applying DWT[28] to both the images are multiplied by a scaling

factor and are added. During the embedding process the size of the watermark should be smaller than the host image but the frame size of both the images should be made equal. Since the watermark embedded in this paper is perceptible in nature or visible, it is embedded in the low frequency approximation component of the host image and also we can used DCT domain[29] both invisible and visible watermarking technique. A digital watermarking-based image quality evaluation method[30] that can accurately estimate image quality[31,32] in terms of the classical objective metrics, such as peak signal-to-noise ratio (PSNR), weighted PSNR (wPSNR). watermark is embedded into the discrete wavelet transform (DWT) domain of the original image using a quantization method. This paper proposed a new statistical approach for watermarking mesh representations of 3-D graphical objects[33,34]. A robust digital watermarking method has to requirements of watermark invisibility, robustness, embedding capacity and key security. In this method embedding is performed by changing the normalized distribution of local geodesic distances from within each region[36]. Two different embedding methods are used by changing the mean or the variance of geodesic distance distributions and also used 3-D triangular mesh technique[35].

V.B Audio Watermarking

The audio watermark should be inaudible, statistically unnoticeable to prevent unauthorized removal. self-clocking is to detect in the presence of time scale modification attack. The audio watermarking can be classified into temporal watermarking and spectral watermarking, based on the domain where watermarks are embedded. Temporal watermarking hides watermarks directly into digital audio signals in the time domain, and spectral watermarking methods [37,38]where FFT(Fast Fourier Transform), DCT(Discrete Cosine Transform), and DWT(Discrete Wavelet Transform), etc. are commonly used. The temporal audio watermarking is relatively easy to implement and requires less computing resources, as compared with the spectral watermarking. But the temporal watermarking is weaker than the spectral watermarking against general signal processing attacks.

V.B.a Time Domain And Frequency Domain or Transform Domain Technique

Least Significant Bit substitution (LSB) and echo hiding techniques both are Time-domain analysis [39]. LSB embeds the watermark information in the least significant bits of the audio sample values by overwriting the original bits [40] to overcome the quantization error. To make echo watermarking embed information embed into the repeated version of component of original discrete audio signal with small offset value. initially amplitude and decay rate to make it imperceptible [41]. Frequency domain audio watermarking techniques apply on human perceptual properties and frequency masking characteristics of the human auditory system [42]. In these techniques, the phase and amplitude of the transform domain coefficients are modified. such as Discrete Fourier Transform (DFT), the Discrete Cosine Transform (DCT), and the Discrete Wavelets Transform (DWT). From this literature using patchwork algorithm to implement audio watermarking, artificially modifies the difference(we call this patch value) between estimated sums of samples in two randomly chosen and prescribed index subsets. Thus the modified patch value is many deviation. The artificial modification can be detected, with a high probability by comparing the observed patch value with the expected one. The new approach of watermarking algorithm based on the wavelet transform (WT) and the complex cepstrum transform (CCT) by combining with human auditory model and using the masking effect of human ears. This algorithm create binary image watermark into the audio signal and improved the imperceptibility of watermarks. The complex cepstral analysis is a homomorphic mapping and is the most effective extraction method in audio identification. the advantage of cepstral transform (CCT) is that the coefficients of the complex cepstral transform are much decorrelation. the audio watermarks embedding algorithm with the cepstral transform, a digital watermark was inserted into the cepstral components of the audio signal using a technique by spread spectrum communications to hiding a narrow band signal in a wideband channel. In this method, a pseudo-random sequence was used to watermark the audio signal. The watermark is then weighted in the cepstrum domain according to the distribution of cepstral coefficients and the frequency masking characteristics of HAS. In frequency domain C.T.Hsith and P.Y.Tsou[43] discussed the detection of audio blind watermarking in cepstrum domain using the concepts of energy characteristic radix. Audio watermarking scheme using direct sequence spread spectrum (DSSS) method enhance an audio signal imperceptibly.

V.C Video Watermarking

There are compressed and uncompressed watermarking techniques. To robust video watermarking method is presented to embeds data to the specific bands in the wavelet domain using motion estimation approach. Using random Gaussian distribution in video sequences on different types of video (compressed DVD quality movie and uncompressed digital camera movie). The proposed watermarking method in frequency domain has strong robustness against some attacks such as frame dropping, frame filtering. video watermarking techniques need to meet new difficulties such as large volume of inherently redundant data between frames, the unbalance between the motion and motionless regions, real-time requirements in the video broadcasting etc.

Watermarked video sequences are susceptible to pirate attacks such as frame averaging, frame swapping, statistical analysis, digital-analog (AD/DA) conversion, and lossy compressions, Copy control [44].Value added applications like legacy system enhancement, database linking, video tagging, digital video broadcast monitoring , Media Bridge etc. Video watermarking algorithms should directed on localized detection, real time algorithm complexity, synchronization recovery, effects of floating point representation, power dissipation etc.The main advantages of using pixel domain techniques are that they are conceptually simple to understand and the time complexity of these techniques are low which favours real time implementations. But these techniques generally lacks in providing adequate robustness and imperceptibility requirements. This paper represents a method to detect video tampering[45] and distinguish it from common video processing operations, such as recompression, noise, and brightness increase, using a practical watermarking scheme for real-time authentication of digital video[46].

VI. Conclusions

Watermarking is emerging tropic in new era of science. but not only in science it penetrate human civilization to enrich watermarking in high sky. Since 1990s it has been modified yet it not have proper modified technique. In watermarking there are so many field not to be developed in best limiting value. The fragile and semi fragile watermarking techniques have some serious disadvantages like increased use of resources, higher area requirements and high power consumption.

References

[1]. A. Herrigel et al., "Secure copyright protection techniques for digital images," in Information hiding,vol.1525 ,pp.169-190,Springer Verlag,1998.
[2]. Ravi K. Sharma, and Steve Decker, "Practical Challenges For Digital Watermarking Applications", IEEE, 2001
[3]. E. Brannocket et al., "Watermarking with Wavelets simplicity leads to Robustness", IEEE, 2008.
[4]. A.K. Goyal, N.Agrawal, S.Verma, "Robust Watermarking in Transform domain using edge detection technique", IEEE, 2007.
[5]. Yusof Yusnita and Khalifa, O. Othman"Digital Watermarking For Digital Images Using Wavelet Transform", IEEE, 2007.
[6]. Kahn. David, "Codebreakers : Story of Secret Writting", Macmillan 1967.
[7]. Homer, "The Iliad" (trans. R. Fragels), Middlesex, England: Penguin 1972.
[8]. Kahn.David, "The History of Steganography", Proc. of First Int. Workshop on Information Hiding, Cambridge, UK, May30-June1, Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.1-7,1996.
[9]. F.A.P.Petitcolas, et al.,"Information Hiding - A Survey", Proceedings of the IEEE, Vol.87, No.7, July 1999, pp.1062-1078.
[10]. B.Pfitzmann, "Information Hiding Terminology", Proc. of First Int. Workshop on Information Hiding, Cambridge, UK, May30-June1, 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.347-350.
[11]. Hal Berghel, "Watermarking Cyberspace", Communications of the ACM, Nov.1997, Vol.40, No.11, pp.19 - 24.
[12]. Kaur et al., "International Journal of Advanced Research in Computer Science and Software Engineering 3(4)",April - 2013, pp. 858-861.
[13]. C. Rey and JL. Dugelay, "A survey of watermarking algorithms for image authentication". EURASIP Journal on Applied Signal Processing, 6:613–621, 2002.
[14]. Lee, G. J., Yoon, E. J. and Yoo, K. Y., "A new LSB based Digital Watermarking Scheme with Random Mapping Function", in 2008 IEEE DOI 10.1109/UMC.2008.33.
[15]. H. Luo, S. Chu, H. and Lu, Z. M., "Self Embedding Watermarking Using Halftoning Technique, Circuits Syst Signal Process" (2008) 27: 155–170.
[16]. W. Yang, C., Wen, C. Y. and Chen, C. H., (2008), "Applying Public-Key Watermarking Techniques in Forensic Imaging to Preserve the Authenticity of the Evidence". Springer-Verlag Berlin Heidelberg 2008.
[17]. He, H. J., Zhang, J. S. and Tai, H. M., (2006), A Wavelet-Based Fragile Watermarking Scheme for Secure Image Authentication. Springer-Verlag Berlin Heidelberg 2006
[18]. Byun, S. C., et al. (2003), A SVD-Based Fragile Watermarking Scheme for Image Authentication. Springer-Verlag Berlin Heidelberg 2003
[19]. Lee, G. J., Yoon, E. J. and Yoo, K. Y. (2008), "A new LSB based Digital Watermarking Scheme with Random Mapping Function", in 2008 IEEE DOI 10.1109/UMC.2008.33
[20]. Fazli, S. and Khodaverdi, G (2009), Trade-off between Imperceptibility and Robustness of LSB Watermarking using SSIM Quality Metrics, in 2010 IEEE DOI 10.1109/ICMV.2009.68
[21]. A. Cohen and A. Lapidoth, "On the Gaussian watermarking game," in Proc. IEEE Int. Symp. Information Theory, Sorrento, Italy, June 2000, p. 48.
[22]. N. Merhav, "On random coding error exponents of watermarking systems," IEEE Trans. Inform. Theory, vol. 46, pp. 420–430, Mar. 2000.
[23]. Pei-Eng Ng and Kai-Kuang Ma, "A Switching Median Filter with BDND for Extremely Corrupted Images", IEEE Trans Image Processing, Vol. 15, No. 6, PP. 1506-1516, June 2006
[24]. Jafar Ramadhan Mohammed, "An Improved Median Filter Based on Efficient Noise Detection for High Quality Image Restoration,",IEEE Int. Conf ,PP. 327 – 331, . May 2008
[25]. Xiaoyin Xu, Eric L. Miller, Dong bin Chen and Mansoor Sarhadi, " Adaptive Two-Pass Rank Order Filter to Remove Impulse Noise in Highly Corrupted Images", IEEE Trans Image Processing,Vol.13,No.2, PP.238-247, February 2004
[26]. Zhu Xi'an, (2008), A Semi-Fragile Digital Watermarking Algorithm in Wavelet Transform Domain Based on Arnold Transform, ICSP Proceedings
[27]. Bo Shen, Iihwar K. Sethi and Vasudev Bhaskaran, (1998) DCT Domain Alpha Blending, IEEE
[28]. Y. Hu and S. Kwong, "Wavelet domain adaptive visible watermarking", Electron. Lett., vol. 37, 2001
[29]. S. P. Mohanty, J. R. Ramakrishnan, and M. S. Kankanhalli, "A DCT domain visible watermarking technique for images", ICME 2000,

[30]. T. M. Kusuma and H.-J. Zepernick "A reduced-reference perceptual quality metric for in-service image quality assessment", Proc. Joint First Workshop Mobile Future Symp. Trends Commun., pp.71 -74 2003
[31]. S. Wang , J. Zhao , W. J. Tam and F. Speranza "Image quality measurement by using digital watermarking based on discrete wavelet transform", Proc. 22nd Biennial Symp. Commun., pp.210 -212 2004
[32]. D. Zheng , J. Zhao , W. J. Tam and F. Speranza "Image quality measurement by using digital watermarking", Proc. IEEE Int. Workshop Haptic, Audio, Vis. Environ. Applicat., pp.65 -70 2003
[33]. G. Bors "Watermarking mesh-based representations of 3-D objects using local moments", IEEE Trans. Image Process., vol. 15, no. 3, pp.687 -701 2006
[34]. K. Wang , G. Lavou & eacute ; , F. Denis and A. Baskurt "A comprehensive survey on three-dimensional mesh watermarking", IEEE Trans. Multimedia, vol. 10, no. 8, pp.1513 -1527 2008
[35]. F. Cayre and B. Macq "Data hiding on 3-D triangle meshes", IEEE Trans. Signal Process., vol. 51, no. 4, pp.939 -949 2003
[36]. M. Luo and A. G. Bors "Principal component analysis of spectral coefficients for mesh watermarking", Proc. IEEE Int. Conf. Image Process., pp.441 -444 2008
[37]. D. Kirovski and H. Malvar, " Robust spread-spectrum audio watermarking", 2001 IEEE International Conference on Acoustics, Speech, and Signal Processing, Vol. 3, 2001, pp. 1345-1348.
[38]. I.-K. Yeo, and H. J. Kim,"Modified Patchwork Algorithm: a novel audio watermarking scheme", International Conference on information Technology: Coding and Computing,2001,pp.237-242.
[39]. P. Bassia and I. Pitas, "Robust Audio Watermarking in the Time Domain ," IEEE Transactions on Multimedia, vol. 3, no. 2, pp. 232-241, 2001.
[40]. N. Cvejic and T. Seppänen, "Increasing the Capacity of LSB-Based Audio Steganography," in Proceedings of the IEEE International Workshop on Multimedia Signal Processing, pp. 336-338, 2002.
[41]. H. Kim and Y. Choi, "A Novel Echo-hiding Scheme with backward and Forward Kernels," IEEE Transactions on Circuits and Systems for Video Technology; vol. 13, no. 8, pp. 885-889, 2003.
[42]. S. Katzenbeisser and F. Petitcolsd, "Information Hiding Techniques for Steganography and Digital Watermarking," Artech House, Boston, USA, 2000.
[43]. Xianghong Tang, Yamei Niu, Hengli Yue, Zhongke Yin "A Digital Audio Watermark Embedding Algorithm", International Journal of Information Technology, Vol. 11, No.12 ,2005
[44]. Sang-Kwang Lee, Yo-Sung Ho, "Digital Audio Watermarking in the Cepstrum Domain". IEEE trans. on Consumer Electronics, vol.46 (3) , pp.744-750, 2000.
[45]. S. Chen and H. Leung "Chaotic watermarking for video authentication in surveillance applications", IEEE Trans. Circuits Syst. Video Technol., vol. 18, pp.704 -709,(2008)
[46]. P.-C. Su , C.-S. Wu , I.-F. Chen , C.-Y. Wu and Y.-C. Wu "A practical design of digital video watermarking in H.264/AVC for content authentication", Signal Process, Image Commun., vol. 26, no. 8â?"9, pp.413 -426 ,2011