International Journal of Research in Computer Science
ISSN 2249-8257 Volume 1 Issue 1 (2011) pp. 55-61
© White Globe Publications
www.ijorcs.org

Digital Watermarking Trends

Sarabjeet Singh[1]

[1]*Faculty CSE, IET Bhaddal*
Email: sarabjeet_singh13@yahoo.com

Abstract

Digital Watermarking is the technique used by researchers to hide user defined information along with important information that may be visible or invisible depending upon the requirements of the user. Now Digital Watermarking is concerned with the ownership of the information. Absence of Digital Watermark in the information results in loss of revenue. The Digital Watermark packed with the information should be inseparable. This paper will present here the different tr ends that are followed in the digital watermarking.

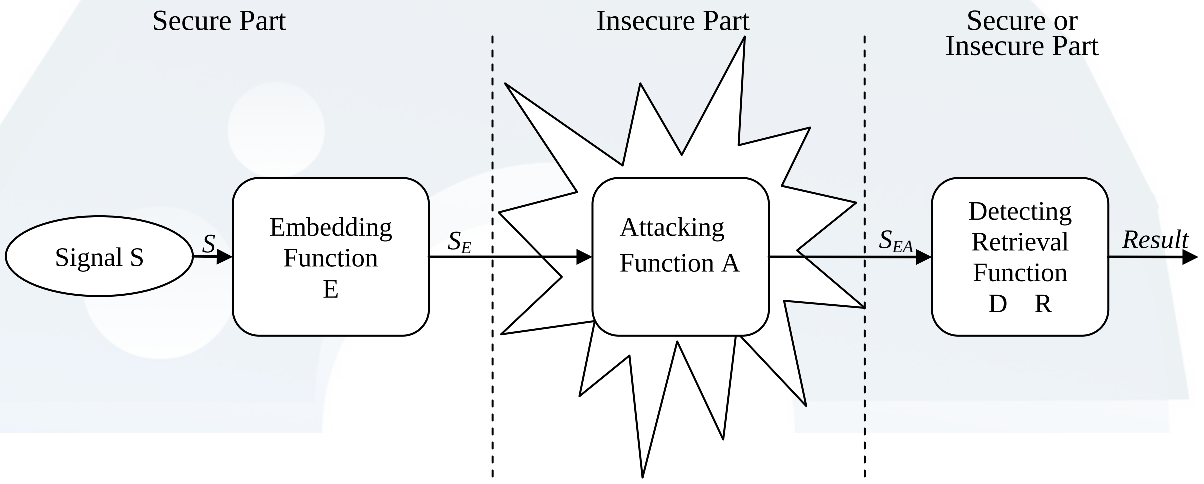
Keywords: Watermarking, DWT, spatial domain, transform domain, wavelet transform, cosine transform

I. Introduction

Digital Watermarking is to embed a hidden watermark message into a host object such that the hidden message is inseparable. Earlier watermarking was applied to text only. Now days watermarking is applied to all types of media. Digital watermarking is applied to video also to stop piracy which results in loss of revenue. There should be no perceptible difference between the watermarked and original signal, and the watermark should be difficult to remove or alter without damaging the host object.

Digital Watermarking stages:

1) Embedding a watermark
2) Attempt to remove/distort watermark
3) Detection of the watermark



Watermarking Technique requirements:

i. Robustness

Robustness refers to that the watermark embedded in data has the ability of surviving after a variety of processing operations and attacks. Then, the watermark must be robust for general signal processing operation, geometric transformation and malicious attack. The watermark for copyright protection does need strongest robustness and can resist malicious attacks, while fragile watermarking; annotation watermarking do not need resist malicious attacks.

ii. Non-perceptibility

Watermark cannot be seen by human eye or not be heard by human ear, only be detected through special processing or dedicated circuits.

iii. Verifiability

Watermark should be able to provide full and reliable evidence for the ownership of copyright-protected information products. It can be used to determine whether the object is to be protected and monitor the spread of the data being protected, identify the authenticity, and control illegal copying.

iv. Security

Watermark information owns the unique correct sign to identify, only the authorized users can legally detect, extract and even modify the watermark, and thus be able to achieve the purpose of copyright protection.

II. Techniques of Watermarking:

A. Spatial Domain

B. Transform Domain

A. **Spatial Domain: -** It is manipulating or changing an image representing an object in space which uses statistical properties of each pixel and its immediate surrounding pixels in the host image, and also the statistical properties of the host image and that of the image to be embedded (watermark), as the pixels in the host image are replaced one by one by the pixels in the watermark image. One of the Spatial domain technique is Least Significant Bit(LSB) in which message is embedded in the least significant bit.

B. **Transform Domain: -** Watermark is embedded in frequency domain of a signal such as Discrete Cosine Transform, Discrete Fourier Transform, Discrete Wavelet Transform domain coefficients. Transform domain methods hide messages in significant areas of the host image which makes them more robust to attacks.

Discrete Cosine Transform: -The DCT transforms a signal from a spatial representation into a frequency representation. Lower frequencies are more obvious in an image than higher frequency so if we transform an image into its frequency component and throw away a lot of higher frequency coefficients, we can reduce the amount of data needed to describe the image without sacrificing too much image quality.

The DWT transform:

In numerical analysis and functional analysis, a discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution. It captures both frequency and location information. The basic idea of DWT is to separate frequency detail, which is multi-resolution decomposition.

III. Document Watermarking

Much of the early work on recognizing the potential problems with intellectual property rights of digital content and addressing these issues with early watermarking techniques was in the area of document watermarking [1]-[3]. These techniques were devised for watermarking electronic versions of text documents which are in some formatted version such as postscript or PDF. Most of this work is based on hiding the watermark information into the layout and formatting of the document directly. In [1]-[3], the authors develop document watermarking schemes based on line shifts, word shifts as well as slight modifications to the characters. These techniques are focused on watermarking the binary-valued text regions of a document. Watermark detection consists of post processing steps to try to remove noise and correct for skew. These techniques are quite effective against some common attacks such as multigenerational photocopying. The authors point out that optical character recognition can remove the layout information and, for such schemes, remove the watermark information.

IV. Graphics Watermarking

There has been some work on effective watermarking of graphics, motivated in part by such standards as MPEG-4. In [4], the authors address watermarking three-dimensional polygonal models. The work in [5] addresses the watermarking of facial animation parameters as defined by the MPEG-standard. The watermark is embedded directly into the parameters and can be extracted from the watermarked parameters directly or from video sequences rendered using the parameter bit stream where the parameters are estimated using a model-based approach. One bit of watermark information is embedded in a block of facial animation parameter (FAP) data using a pseudo noise sequence that is generated from the secret key. The authors limit the amount of deviation the watermark signal has on the FAPs empirically to minimize visible distortion. For instance, global FAPs like head rotation are limited to deviate by 1% of their dynamic range while local FAPs such as lip motion is limited to 3%. Watermark detection can be done directly on the watermarked FAPs through a traditional correlation detector. The authors demonstrate that they are able to recover the watermark information without error using both the FAPs directly or by estimating them from a rendered sequence. They also show that their method is robust to moderate compression using MPEG-2.

V. Video Watermarking

The Copy Protection Technical Working Group (CPTWG), an ad hoc group consisting of the Motion Picture Association of America, the Consumer Electronics Manufacturers Association, and members of the computer industry, is examining digital video protection as it applies to digital versatile disk (DVD) technology [6], [7]. The current plan is to adopt a de facto standard for a DVD copy protection system which includes watermarking. The watermark component of the system, besides the usual requirements of robustness and transparency, must satisfy other constraints and system requirements unique to this application. In this case, the watermark is designed to support copy generation management, and the minimum information that the watermark must convey is: copy never, copy once, copy no more, and copy freely. A cost-effective solution for watermark detection is a critical requirement for DVD watermarking so that real-time decoding with no frame buffer (no reference to previous frames) is required. Low false positive rates is a critical component for the consumer driven DVD market and is much more important than the security risks associated with false negatives. Other issues that have arisen in the design of an effective copy control system for DVD includes the placement of the detector. The two remaining proposals have two different approaches for detector placement—watermark detection in the drive and watermark detection within the application (within the MPEG decoder). The drive-based solution has the advantage that as long as the watermark exists, pirated content cannot leave the drive in playback mode or recording mode. There is some added complexity with detection in the drive versus detection in the application, for example, a partial decode of the MPEG bit stream is necessary. Watermark detection in the MPEG decoder is not as secure as the drive-based solution and some added features that have been suggested for detection in the application include a protocol to recognize a compliant device, a bidirectional link with authentication, encryption and data integrity, and a protocol between source and sink which informs the drive whether to stop transmitting data. Advantages of application-based detection are the ability to provide a more complex detector and the flexibility of extending the scheme to other data types. The other unique requirement for DVD applications is copy generation management, that is, the ability to detect the *copy once* state and change it to a *copy no more* state after the recording. The two proposals have different approaches for this feature as well secondary watermarks and tickets. The secondary watermark approach adds a second watermark after the recording. The secondary watermark embedder must be computationally inexpensive, must be applicable in the baseband and compressed video domains, and should not alter the bit rate in MPEG embedding. The second approach uses a ticket which is a cryptographic counter implemented as a multibit random number. The recorder modifies the ticket by passing it through a cryptographic one-way function (hash function) where each time it goes through a player, it gets decremented by one. An excellent review article on this topic can be found in [6]. A scene-adaptive video watermarking technique is proposed in [17] where the watermarking scheme is based on temporal wavelet decomposition. The wavelet decomposition separates static areas from dynamic areas so that separate watermarking strategies can be applied to the different areas. The authors propose a constant watermark for the static area and a varying watermark for the dynamic areas to defeat watermark deletion through frame averaging. Many times, digital video will already be in a compressed format at the point where watermarking is applied, and it is desirable to be able to embed the Watermark directly into the compressed bit stream without going through a full decoding, watermarking, and reencoding step which adds considerable complexity and additional delay. Interesting work [7], [8] on watermarking of uncompressed and compressed video has been studied. One of the issues addressed in this work is the direct embedding of watermark information in a compressed video bit stream, subject to the imperceptibility constraint as well as an additional constraint that the total bit rate of the watermarked compressed bit stream cannot exceed the total bit rate of the un-watermarked bit stream. This is an important requirement because for many applications, bandwidth limitations dictate the total bit rate possible for the video stream. Current video compression standards such as MPEG or ITU H.26x standards consist of the same general framework which includes block based motion compensation which takes advantage of temporal correlation and block-based DCT coding which takes advantage of local spatial correlations. The watermarking technique does not alter the motion vector information which is used for the motion compensation and is encoded in a lossless manner or any of the critical side information. The watermark signal is only embedded into the DCT coefficients so that only partial decoding of the block DCT is necessary for watermark embedding. Only nonzero DCT coefficients are marked and if constant bit rate is required, DCT coefficients are marked only if the bit rate for the quantized representation is equal or less than the bit rate needed for the unmarked quantized coefficients. This is possible due to variable length coding. The watermark embedding process consists of inverse entropy coding and inverse quantization, embedding the watermark in the DCT coefficients and checking for bit rate compliance. Although much of the video may not be marked due to this additional constraint, it is still possible to embed a few bytes of information per second, which is useful for many applications. In other work [9], [10], two techniques are introduced for real-time watermark embedding of compressed video. One technique adds the watermark by modifying the fixed length and variable length codes in the compressed video bit stream. This allows for a computationally efficient way of real-time watermark insertion and allows for a relatively high payload. The drawback of this technique is that decoding the bit stream removes the watermark completely. A more robust technique is also proposed which adds a watermark by enforcing energy differences between various video regions. This is done by discarding high frequency components so that only partial decoding of a compressed video bit stream is necessary to apply this watermark. This technique results in a watermark that is still present after decompressing the video bit stream. In [11] a video watermarking method is proposed for broadcast monitoring where encoder and decoder complexity are critical requirements. The low complexity scheme consists of spatial domain encoding and decoding with a perceptually based scaling factor that depends on a simple measure of local activity. Other techniques proposed for video watermarking of compressed bit streams includes embedding the watermark information in the motion vectors [12], A DCT based watermarking scheme for video which is motivated by previous still image watermarking techniques is introduced in [13]. Other requirements for video watermarking may include real-time watermark detection/identification and perhaps real-time watermark embedding, robustness to NTSC/PAL conversion, MPEG compression, frame averaging attack, A/D and D/A conversion, and rate control. Other broadcast applications for hiding additional information are described in [14].

VI. Audio Watermarking

Most of the research on audio watermarking has been focused on either direct watermarking of the audio signal or bit stream embedding where the audio is represented in a compressed format. Just as in image and video watermarking, the use of perceptual models is an important component in generating an effective and acceptable watermarking scheme for audio [18], [15], [19]. Many of the requirements for audio watermarking are similar to image watermarking, such as inperceptibility (inaudibility), robustness to signal alterations such as compression, filtering, and A/D and D/A conversion. In [19], the authors propose three techniques for audio watermarking— a spread spectrum technique, echo coding, and phase coding. The approach described in [18] and [15] consists of generating a PN-sequence for the watermark and processing it with a filter that approximates the frequency masking properties of the human auditory system (HAS), followed by a time-domain weighting for temporal masking. Correlation properties of PN-sequences are desirable for detection and applying an auditory model guarantees imperceptibility, a critical feature for high quality audio clips where copyright protection may be most critical. Masking is the phenomena where the detectibility of a signal component depends on the presence or absence of other signal components in its immediate vicinity either in the frequency domain or temporal or spatial domain. Here, detectibility refers to audibility for audio or visibility for image and video signals. An overview paper on how perceptual models have been exploited for signal compression can be found in [16]. The audio watermarking technique in [18] and [15] uses the frequency masking model proposed in MPEG. More details on generating the thresholds can be found in [15]. Watermark embedding consists of adding a perceptually weighted PN-sequence to the audio file while watermark detection consists of a correlation detector to determine whether the watermark is or is not present in the received signal.

The Secure Digital Music Initiative (SDMI) that consists of companies and organizations in information technology, consumer electronics, security technology, the recording industry, and ISPs has been formed to examine technology which provides some security features for digital music and copyright protection for next-generation portable digital music devices. Phase I screening looks for a watermark in the content but allows all music that is compatible with the detection which will allow new releases to play while filtering out pirated copies of music. After extensive testing of imperceptibility and robustness, SMDI has chosen ARIS audio watermarking technology for Phase I screening technology which will be used to indicate when the software used by Phase I devices should be upgraded to incorporate Phase II technology. Some of the requirements particular to music as seen by the SDMI group include inaudibility, robustness, tamper resistance, reliability (no false positives), ease of implementation, cost, and ability to compress the content.

VII. Conclusion and Future Directions

We have reviewed the basic watermarking algorithms as they apply to different applications and media types. Although many technical problems have been addressed, there are many more yet to be solved.

VIII. References

[1] J. Brassil, S. Low, N. Maxemchuk, and L. O'Gorman, "Electronic marking and identification techniques to discourage document copying," in *Proc.Infocom' 94*,1994, pp. 1278-1287.

[2] J. Brassil, S. Low, N. Maxemchuk, and L. O'Gorman, "Electronic marking and identification techniques to discourage document copying," *IEEE J Select. Areas Commun.*, vol. 13, pp. 1495-1504, 1995. doi:10.1109/49.464718

[3] J. Brassil, S. Low, and N. Maxemchuk "Copyright protection for the electronic"

[4] R. Ohbuchi, H. Masuda, and M. Aono, “Watermarking three-dimensional polygonal models through geometric and topological modifications,” *IEEE J. Select. Areas Commun.*, vol. 16, pp. 551-560, May 1998. doi:10.1109/49.668977

[5] F. Hartung, P. Eisert, and B. Girod, “Digital watermarking of mpeg-4 facial animation parameters,” *Comput. Graph.*, vol. 22, no. 4, pp. 425-435, Aug. 1998. doi:10.1016/S0097-8493(98)00032-6

[6] J. Bloom, I. Cox, T. Kalker, J.P. Linnartz, M. Miller, and C. Traw, “Copy protection for dvd video,” *Proc. IEEE*,, no. 87, pp. 12667-1276, July, 1999. doi:10.1109/5.771077

[7] Data Hiding Subgroup; http:www.dvcc.comdhsg.

[8] F. Hartung and B. Girod, “Watermarking of uncompressed and compressed video,” *Signal Process.*, vol. 66, no. 3, pp. 283-301, May 1998. doi:10.1016/S0165-1684(98)00011-5

[9] F. Hartung, “Digital watermarking and fingerprinting of uncompressed and compressed video,” Ph.D.dissertation, Shaker Verlag, Univ. of Erlangen-Nuremberg, Aachen, Germany, Oct. 1999.

[10] C. Langelaar, R. Lagendijk, and J. Biemond, “Realtime labeling of mpeg-2 compressed video,” *J. Vis. Commun. Image Represent*., vol. 9, no. 4, pp. 256-270, Dec. 1998. doi:10.1006/jvci.1998.0397

[11] G. C. Langelaar, “Real_time watermarking techniques for compressed video cata,” Ph.D. thesis, Delft Univ. of Technology, 2000. Video watermarking system for broadcast monitoring,” in

[12] *Proc.SPIE, Security and Watermarking of Multimedia Contents*, San Jose, CA, Jan. 1999, vol. 3657, pp. 103-112.

[13] F. Jordan, M. Kutter, and T. Ebrahimi, “Proposal of a watermarking technique for hiding/retrieving data in compressed and decompressed video,” in *ISO/IEC Doc. JTC1/SC29/WG11/MPEG97/M2281*, July 1997.

[14] J. Dittmann, M. Stabenau, and R. Steinmetz, “Robust mpeg video watermarking technologies,” in *Proc. ACM Multimedia*, Sept. 1998, pp. 71-80.

[15] B. Macq and J.-J. Quisquater, “Cryptology for digital tv broadcasting,”*proc. IEEE*, vol. 83, pp. 944-957, 1995. doi:10.1109/5.387094

[16] L. Boney, A. Tewfik, and K. Hamdy, “Digital watermarks for audio signals,” in *IEEE Proc. Multimedia*, 1996, pp. 473-480. doi:10.1109/MMCS.1996.535015

[17] N.D. Jayant, J.D. Johnston, and R.J. Safranek, “Signal compression based on models of human perception,” *Proc.IEEE*, vol. 81, pp. 1385-1422, Oct. 1993. doi:10.1109/5.241504

[18] M. Swanson, B. Zhu, and A. Tewfik, “Multiresolution scene-based video watermarking using perceptual models,” *IEEE J. Select. Areas Commun.*, vol. 16, pp. 525-539, May 1998. doi:10.1109/49.668976

[19] M. Swanson, B. Zhu, A. Tewfik, and L. Boney, “Robust audio watermarking using perceptual masking,” 337-355.

[20] W. Bender, D. Gruhl, and N. Morimoto, “Techniques for data hiding,” *IBM Syst. J.*, vol. 35, nos. 3-4, pp. 313-336, 1996. doi:10.1147/sj.353.0313

How to cite

Sarabjeet Singh, "Digital Watermarking Trends". *International Journal of Research in Computer Science*, 1 (1): pp. 55-61, September 2011. doi:10.7815/ijorcs.11.2011.005