International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
www.ijset.com, Volume No.1, Issue No.4, pp : 08-11 01 Oct. 2012

A Literature Review on Water Marking Techniques

Charu Kavadia, Vishal Shrivastava
Department of Computer Science & Engineering, Arya college of engineering & I.T. Jaipur
charukavadia@gmail.com,Vishal500371@yahoo.co.in

Abstract: this paper presents a review on different digital watermarking techniques and their properties. The main reason for development of digital watermarking research is to protect intellectual properties of the digital world. Since the recent technology makes it easy copying the digital contents without any restrictions and editing without any prohibitive professional efforts. In the absence of protecting techniques, it difficult to rely on digital storage & communication systems for secure medical, business, and military applications. Watermarking is one of the most common solutions to make the data transferring secure from the illegal interference.

Keywords: Watermarking, Data Security.

1. Introduction

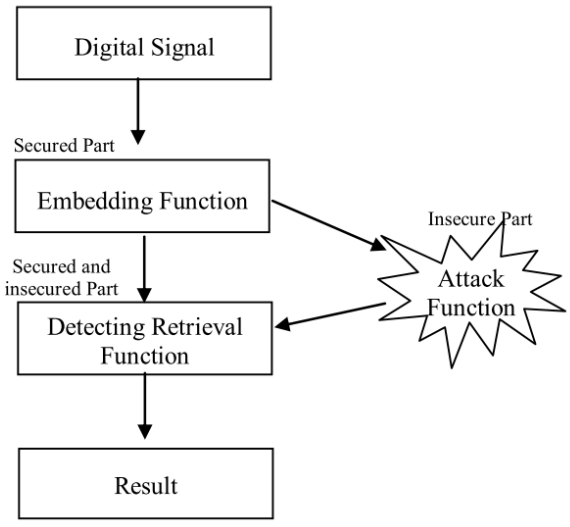
Digital watermarking is the process of computer-aided information hiding in a carrier signal; the hidden information should,[1] but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication. Like traditional watermarks, digital watermarks are only perceptible under certain conditions, i.e. after using some algorithm, and imperceptible anytime else [2] If a digital watermark distorts the carrier signal in a way that it gets perceivable, it is of no use.[2] Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal.

The needed properties of a digital watermark depend on the use case in which it is applied. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied.Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. But whereas steganography aims for imperceptibility to human senses, digital watermarking tries to control the robustness as top priority.Since a digital copy of data is the same as the original, digital watermarking is a passive protection tool. It just marks data, but does not degrade it nor controls access to the data.

One application of digital watermarking is source tracking. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies.

2. Generic Watermarking System

Digital watermarking algorithms are composed of three parts, namely, watermark embedding algorithm, watermark extraction algorithm and watermark detection algorithm [3][4]. A general watermark system phases is shown in Figure



1.

Figure 1: Watermark Lifecycle Phases [4].

During embedding process, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored. If a person makes a modification, then the digital content is said to be attacked. A watermark attack is an attack on digital data where the presence of a specially crafted piece of data can be detected by an attacker without knowing the encryption key [4].

3. Classification of Watermarking Schemes

Digital watermarking schemes can be broadly classified into four categories, namely, Robust, Fragile, Semi-fragile and Reversible. While, as mentioned previously, imperceptibility, low embedding distortion and security are the common requirements of all classes, each different category of scheme has different characteristics and, thus, is suitable for different applications. For example, while robustness is an essential requirement for copyright applications, it has no role in most authentication applications. This section provides a brief explanation of each of these schemes along with application areas where they can be applied [4].

3.1. Robust Watermarking Schemes

A robust watermarking system is resilient against wide range of intentional and unintentional image processing operations such as image enhancement, altering, noise addition, JPEG compression and geometrical transformations, collusion and forgery attacks.

3.2 Robust Watermarking Methods

(a) Spread Spectrum based Robust Watermarking

The spread spectrum communications embed information using small amount of energy with large spectrum. In each band, the corresponding information or energy becomes very small and undetectable. Thus, it is difficult to remove the signal (watermark) from the host signal (cover content) if spread spectrum communication is applied. This approach uses spread spectrum communication techniques embed a single bit in the image. spread spectrum communication can be defined as : "Spread spectrum is a means of transmission in which the signal occupies a band width in excess of minimum necessary to send the information, the band spread is accompanied by a code which is independent of the data, and a synchronized reception with the code at the receiver is used for dispreading and subsequent data recovery".

(b) JND Model based Robust Watermarking

In this method to embed the amount of modification on image which will not be aware by human perception as JND (Just Noticeable distortion). This model is tested in both DCT and DWT domains and the result indicated that the manipulation is not noticed by human eyes. JND model or HVS (Human Visual System) are subjective measure of transparency. The masking effect is the minimum level below which a signal cannot be aware, in DCT domain. Using the masking effect, the watermark can be embedded into an image in a manner such that human eyes cannot perceive.

(c) Spatial Domain based Robust Watermarking

In this technique modification of random selected pixels is performed and hypothesis testing is used to detect the watermark. This approach is robust to JPEG compression and low passes filtering.

(d) Channel State Estimation based Robust Watermarking

This method proposes the scenario of optimal watermark embedding and extraction. The watermark problem is treated as communication with side information. The side information includes secret key and channel state information such as cover image and attack channel. According to the combination of whether the side information is available on watermark embedding and watermark extraction. It can be concluded that the optimal watermarking system should take into consideration all available side information at both watermark embedding and watermark extraction.

3.3 Fragile Watermarking

A fragile watermark can be destroyed easily. This property is useful to identify whether a multimedia is modified or not. By modulating fragile watermark into multimedia, the authenticity of multimedia can be authenticated. Any modification on the multimedia will make the corresponding embedded fragile watermark destroyed. By examining a fragile watermark, the position where the modification occurred can be identified easily.

3.4 Fragile Watermarking Methods

(a) Quantization-based Fragile Watermark

In this technique by examining the destroyed fragile watermark, the position where malicious modification occurred could be identified. This technique identifies the type of incidental distortion as JPEG compression, if the ratio of the number of destroyed watermark over the number of all watermark decrease from high resolution to low resolution in wavelet transform. However, this approach cannot identify the type of modification if both an instance of malicious tampering and an incidental distortion are simultaneously applied.

(b) Block Hashing

In the first variance of the approach, hash function is applied on blocks of image. Any modification on this protected image will vary the value of the hash function. Thus, the area which is tampered with can be identified. In second approach, they examined the Variable-Watermark Two-Dimensional Algorithm (VW2D). The VW2D technique use the stored values obtained watermark and the watermarked image to perform image authentication on a block-by-block basis. Both of these two examined methods need store values for further processing. There is an extra need of management of these stored data.

3.5. Semi-Fragile Watermarking Schemes

To facilitate the authentication and content-integrity verification for multimedia applications where content-preserving operations are a common practice, semi-fragile watermarking scheme have been proposed in the last few years [7], [8]. This class of watermarks is intended to be fragile only when the manipulations on the watermarked media are deemed malicious by the schemes. Usually, to achieve semi-fragility, the schemes exploit properties of, or relationships among, transformed coefficients of the media. Such properties and relationships are invariant to content-preserving operations while variant to malicious manipulations. The watermark is embedded by quantizing or adjusting the coefficients according to the watermark. The defined quantization step governs the fragility or sensitivity to manipulations and the degree of distortion. However, an immediate result of coefficient quantization is that a unique watermark may be extracted from many different media, which might have been subjected to some forms of content-preserving operations or malicious manipulations. Such a one-to-many correspondence can be problematic in terms false positives (i.e. a watermark, that was never embedded, is detected by the detector) and false negatives (i.e. the detector fails to detect an embedded watermark). Unfortunately, no optimal criteria for maintaining low false positive and false negative rates are currently in existence. Another challenge semi-fragile schemes faces is how to distinguish content-preserving operations from malicious attacks. For example, transcoding may be deemed acceptable for one application while it may be seen as malicious for another. Therefore, with these two issues, semi-fragile watermarking is usually not suitable for applications concerning legal and national security issues.

4. Conclusion

The literature review presents the fact that there are large numbers of innovative and inventive watermarking approaches are available. Now research should be directed towards multi-objective watermarking schemes. Most of the proposed watermarking schemes are based on Human Visual System (HVS) using Just Noticeable Distortion (JND) for the selection of watermark positions. Further, the review reveals the fact that even though abundant information on watermarking schemes are published, a performance evaluation of various schemes is absent. Future work is also planned to perform a comparative performance evaluation of existing watermarking schemes.

References

[1] Ingemar J. Cox: Digital watermarking and steganography. Morgan Kaufmann, Burlington, MA, USA, 2008.

[2] Frank Y. Shih: Digital watermarking and steganography: fundamentals and techniques. Taylor & Francis, Boca Raton, FL, USA, 2008.

[3] Zhang, X. and Wang, S. “Fragile watermarking scheme using a hierarchical mechanism”, Signal Processing Vol. 89, Issue 4, Pp. 675-679. 2009.

[4] S. Radharani, M.L. Valarmathi, “A Study on Watermarking Schemes for Image Authentication” International Journal of Computer Applications (0975 – 8887) Volume 2 – No.4, June 2010.

[5] Sviatoslav Voloshynovskiy, F. Deguillaume, Shelby Pereira and Thierry Pun "Optimal adaptive diversity watermarking with channel state estimation" University of Geneva - CUI, 24 rue du General Dufour, CH 1211, Geneva 4, Switzerland.

[6] Lahouari Ghouti and Ahmed Bouridane "A JUST-NOTICEABLE DISTORTION (JND) PROFILE FOR BALANCED MULTIWAVELETS" Computer Standards & Interfaces 28 (2006) 356–367.

[7] Wu, X., Hu, J., Gu, Z. and Huang, J "A secure semi fragile watermarking for image authentication based on integer wavelet transform with parameters" Conferences in Research and Practice in Information Technology Series; Vol. 108, 2005.

[8] Ho, C.K. and Li, C.T. Semifragile watermarking scheme for authentication of JPEG images. Proceeding of the IEEE international Conference on Information Technology: Coding and Computing, I, Pp. 7 – 11 2004.

[9] Parthasarathy, A.K. and Kak. S.,"An Improved Method of Content Based Image Watermarking", IEEE Transactions On Broadcasting, Vol. 53, No. 2, Pp.468-479. (2007).