ISSN:0975-9646

Literature Survey on Digital Watermarking

Manoranjan Kr Sinha , Dr. Rajesh Rai, Prof. G. Kumar

Dept.of E.C.E. NIRT-
Bhopal, India

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.

Keywords: Watermarking, Data Security

1. INTRODUCTION

Nowadays, watermarking of images is becoming increasingly of interest in tasks such as copyright control, image identification, verification, and data hiding. Advances in computer networking and high speed computer processors have made duplication and distribution of multimedia data easy and virtually costless, and have also made copyright protection of digital media an ever urgent challenge. As an effective way for copyright protection, digital watermarking, a process which embeds (hides) a watermark signal in the host signal to be protected. Watermarking techniques can be divided into four categories based on the type of document to be watermarked which is Text Watermarking, Image Watermarking, Audio Watermarking and Video Watermarking. In case of images, watermarking techniques are classified based on two working domains:
Spatial Domain in which pixels of one or two randomly selected subsets of an image are modified based on perceptual analysis of the original image and Frequency Domain in which values of certain frequencies change. In this thesis, we have a brief review of audio, image and video watermarking schemes.

Image Watermarking

Initially, watermarking method obtains a checksum of the image data and then embeds the checksum into the LSB of randomly chosen pixels. Others add a modified maximal length linear shift register sequence to the pixel data which can identify the watermark by using spatial cross correlation function of the modified sequence and part of the watermarked image. Watermarks can modify the images spectral by modulating DCT, DFT or DWT coefficients according to a sequence known only to the owner. As a result, the security level of the watermark in the image increases while maintaining the imperceptibility of the mark.

2. LITERATURE SURVEY

In case of images, watermarking techniques are classified based on two working domains. Spatial Domain in which pixels of one or two randomly selected subsets of an image are modified based on perceptual analysis of the original image and Frequency Domain in which values of certain frequencies change.

2.1 Spatial domain:

A watermarking method based on the spatial domain scatters information to be embedded to make the information more secure so that it is very difficult to detect. It uses minor change of the value of pixels. This approach has an advantage which is it is strong for cropping and translation.
Various approaches for spatial domain techniques have been proposed so far which are checksum techniques, two-dimensional spatial watermark, spread spectrum approach are some of them.

2.1.1 Checksum Technique

In this approach [1], a watermark is formed from the checksum value of the seven most significant bits of all pixels. A checksum is the modulo-2 addition of a sequence of fixed-length binary words which is a type of hash function. This technique randomly chooses the locations of the pixels that are to contain one bit of the checksum. The pixel locations of the checksum together with the checksum value form the watermark which must be kept secret. To verify the watermark, the checksum of a test image is obtained and compared to the watermark.
The advantages of this technique are mentioned below:

- Embedding watermark only changes half of the pixels that covered by it, as a result it not only reduces visual distortion but also increases security.
- An image may hold many watermark as long as they do not overlap.

The drawback of this technique is that it is fragile, therefore any change to either the image data or the embedded checksum can cause the verification procedure to fail.

2.1.2 Basic M-sequence approach

In this approach, the watermark is formed based on using a modified m-sequence. A linear feedback shift register with n stages can form pseudo-random binary sequences with maximum period of 2n-1 [2]. Two types of sequences may be formed from an m-sequence: unipolar and bipolar.
The advantages of this technique are that
The watermark is robust to small amounts of noise, in the image. Successive watermarks treat the previously watermarked image as a new. An attacker can deduce watermark if 2n consecutive bits in it are known.

The drawback of this method is that it does not protect the DC value of the pixels covered by an individual block.

2.1.3 Secure Spread Spectrum Watermarking for Multimedia:

This approach inserts a watermark into the spectral components of the data using the techniques which are analogous to spread spectrum communication, therefore hiding a narrow band signal in a wideband channel

The advantages of this approach are as

- The watermark is difficult to remove for an attacker even when several individuals combine together with independently watermarked copies of the data.
- It is robust to common signal and geometric distortions such as digital-to-analog and analog-to-digital conversion, re-sampling, and re-quantization, including dithering and recompression and rotation, translation, cropping and scaling.

2.2 Frequency domain

In frequency domain, DCT, FFT and DWT [3],[4] methods are used for data transformation. Wavelet transform decompose an image into a set of band limited components that can be reassembled to reconstruct the original image without error. Linear programming optimized the Wavelet domain watermarking method. In Object based image watermarking technique, a watermark that embeds in distributed of an original data is very difficult to delete.

2.2.1 A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Image

This approach first inserts the watermark into the middle-frequency range. Filter banks can be saved for the watermark embedding and the middle-frequency band to insert the watermark is chosen the coefficient in that band of the image is replace by the watermark.

The advantages of this approach:

- This technique achieves both spatial and frequency localization.
- It is both perceptual invisibility and robustness to compression.
- It is robustness to noise, image processing techniques, median filter, geometric transform.

2.2.2 Hierarchical Watermarking Depending on Local Constraints

In this approach, the watermark is embedded according to two keys [5]. The first key is used to embed a code bit in a block of pixels. The second bit is used to generate the whole sequence of code bits. The watermark is embedded in spatial domain by adding or subtracting a random digital pattern to the given image signal depends on the local energy distribution. The embedding depth level depends on the spectral density distribution of DCT coefficients and on the JPEG quantization table and inserts the watermark in the low frequency component. The depth label consists of a set of bits that are embedded locally in a rectangular set of blocks and it is repeated over the entire image. After detecting individual bits, the retrieve label is verified by performing a XOR operation to the watermark code.

2.3 Hybrid Watermarking

In this method, watermark can be embedded into both spatial and frequency domain.

A Hybrid Watermark for Tamper Detection in Digital Image – A hybrid image authentication watermark can be obtained as a combination of fragile and a robust watermark. The fragile watermark has the advantages that it has good localization and security properties. The hybrid watermark can be used to precisely identify changes as well as distinguish malicious tamper from simple operations. The authentication can be done without accessing any information about the original image.

Effective Hybrid Digital Watermarking Scheme Using Direct Sequence-Spread Spectrum Method – in this scheme, a watermark image is produced using the personal ID of copyrighter which is inserted into the original images and the watermark image is detected. It is an extension of the spread-spectrum watermarking scheme which combine key with logo method. Binary image is used as watermark image, and the degradation of image quality between original image and watermarked image is applied to confirm required invisibility in watermark system and watermark robustness is applied to protect a attack from the outside are analyzed using the values of PSNR of the watermark image.

Discrete Cosine Transform

The DCT [3] transforms a signal from a spatial representation into a frequency representation. Lower frequency 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 discrete cosine transform (DCT) is closely related to the discrete Fourier transform. It is a separable linear transformation; that is, the two-dimensional transform is equivalent to a one dimensional DCT performed along a single dimension followed by a one-dimensional DCT in the other dimension.

Audio Watermarking

Comparing with the development of digital video and image watermarking, digital audio watermarking provides a special challenging issue because

Data hiding is not audible otherwise it will mask the original audio signal that can be easily tampered with and removed,

The human auditory system (HAS) operates over a wide dynamic range between 20 Hz to 20 kHz, therefore it is difficult to embed outside this rage,

There is a limited area of embedding the data.

Audio watermarking techniques [6] mainly focus on four characteristics, which are (1) low bit coding, (2) phase coding, (3) spread spectrum-based coding and (4) echo hiding.

Low-Bit Coding

In the low-bit coding technique, the watermark in an audio signal is embedded by replacing the least significant bit of each sampling point by a coded binary string corresponding to the watermark.

Phase Coding

Phase coding is one of the most efficient coding schemes in term of the signal-to-noise ratio because in this approach, it cannot be found any difference caused by a smooth phase shift, even though the signal patterns may change dramatically.

Spread Spectrum

The spread spectrum technique is intended to encrypt a stream of information by spreading the encrypted data across as much of the frequency spectrum as possible.

Echo Hiding

Echo hiding is a method for embedding information into an audio signal in such a way that the original signal is not degraded perceivably. This approach embeds data by introducing an echo. The value of a hidden datum corresponds to the time delay of the echo and its amplitude. The echo delays are selected to be less than the detectable hearing limited.

Affine Resistant Digital Audio Watermarking Using Template Matching

This approach is used for embedding a digital watermark inaudibly into an audio clip according to the difference between two half blocks of each block. This scheme [7],[2] does not require any host-related information for watermark extraction. The embedded watermark is robust to common audio signal manipulations, such as MP3 compression, time shifting, cropping, time scaling, D/A A/D conversion, insertion, deletion, re-sampling, re-quantization and filtering. Two kinds of information are hidden in the audio: the owner's information and a synchronization template. The owner's information is a binary image provided by the copyright owner, which can be words, numbers, a signature, a personal seal or an organization's logo. The synchronization template is generated by a random number generator controlled by a secret key and is used for synchronizing the signal caused by time shifting, cropping and time scaling attacks. This information are combined together and isolated by another secret key before embedding. This technique can be applied to automatically search for a protected audio from an audio database by first matching the synchronization template and then show the owner's information if it is claimed to have been watermarked.

Digital Audio Watermarking Based-on Multiple-Bit Hopping and Human Auditory System

To optimally balance the audibility and robustness when embedding and extracting watermarks, the embedding scheme is high related to audio content by making use of the properties of human auditory system and multiple-bit hopping technique. The watermark embedding design is based on audio content and HAS [8]. With content-adaptive embedding scheme, the embedding parameter for setting up the embedding process will vary with the content of the audio signal. Therefore, this technique involves segmenting an audio signal into frames in time domain, classifying the frames as belongs to one of several known classes and then encoding each frame with an appropriate embedding scheme. To enhance the robustness and resistance of the embedded watermark, a multiple-bit hopping technique is employed. In this method, instead of embedding one bit into an audio frame, multiple bits with different time delay can be embedded into each audio sub-frame.

Muteness-Based Audio Watermarking Technique

In this audio watermarking approach, the audio counterparts of text spaces are periods of silence. In audio signal, a mute period offers the following advantages:

A mute period is an integral part of any audio signal which cannot be omitted since it represents an integral part of the studio signal.

It occurs randomly in audio signal which is generated by the music process.

A mute period represents a real time interval that will not be decreased when compressed.

In this approach, the audio watermarking technique is a muteness-based which offers the following features:

a) It extends the mute periods in an audio signal without any perceptual difference to the average human auditory system.

b) The extension of mute periods carries the same amplitude such that it will blend with the original and will not attract any attention.

c) It does not require the original signal to extract the watermark.

Image Watermarking based on DWT

Recent researchers on secure digital watermarking techniques have revealed the fact that the content of the images could be used to improve the invisibility and robustness of a watermarking scheme. In this approach, watermark is created from the content of the host image and discrete wavelet transform (DWT) is used for embedding watermarks, since it is an excellent time-frequency analysis method which can be adapted well for extracting the information content of the image [9].

Wang et al. [10] adopt a key dependent wavelet transform. To take the advantage of localization and multi-resolution property of the wavelet transform, **Wang and Lin** [11] proposed wavelet tree based watermarking algorithm. In this approach, the host image is transformed into wavelet coefficients using a discrete-time wavelet transform (DTWT). The watermark is embedded in the wavelet coefficients which are grouped into super trees. Each watermark bit is embedded using two super trees. Depending on the value of the watermark bit, one of the super trees is quantized with respect to a quantization index in such a way that the two super trees exhibit a large enough statistical difference, which can be extracted for obtaining decision. As each watermark bit is embedded in various frequency bands and the information of the watermark bit is spread throughout large spatial regions, therefore the watermarking technique is robust to attacks in both frequency and time domains. This technique is useful for removal of high-pass details in JPEG compression and robust to time domain attacks such as pixel shifting and rotation. In addition to copyright protection, the proposed watermarking scheme can also be applied to data hiding or image authentication.

Tao et al. [12] proposes a discrete-wavelet transform based multiple watermarking algorithms. In this approach, two important tools encryption and watermarking can be used to prevent unauthorized consumption and duplication. The

watermark is embedded into LL and HH subbands to improve the robustness. This approach is useful in such a way that embedding the watermark in lower frequencies is robust to a group of attacks such as JPEG compression, blurring, adding Gaussian noise, rescaling, rotation, cropping, pixilation, sharpening and embedding the watermark in higher frequencies is robust to another set of attacks such as histogram equalization, intensity adjustment, gamma correction.

Luo et al. [13] introduced an integer wavelet based watermarking techniques to protect the copyright technique to enhance the security. This technique is useful for digital watermarking in DEM (digital elevation mode) data, which effectively protects the copyright of DEM data and avoids the unauthorized user. As lifting based scheme is added to construct the compactly supported wavelets whose coefficients are composed of a free variable therefore, it uses only integral addition and shift which is fast and easily realized via hardware. As wavelet coefficient set is embed watermark information, therefore the bit is inserted in the high activity texture regions with the maximum strength of Just Noticeable Distortion (JND) tolerance of Human Visual System (HVS) that makes the digital watermark robust.

Yuan et al. [6] proposed an integer wavelet based multiple logo watermarking scheme. The watermark is permutated using Arnold transform and is embedded by modifying the coefficients of the HH and LL subbands. In this approach, an integer wavelet based multiple logo-watermarking schemes for copyright protection of digital image is presented. A visual meaningful binary logo is used as watermark. The process of watermark embedding is carried out by transforming the host image in the integer wavelet domain. To construct a blind watermarking scheme, wavelet coefficients of HH and LL bands are modified depending on the watermark bits. To add the security, permutation is used to preprocess the watermark.

Lin et al. [14] put forward a DWT based blind watermarking scheme by scrambling the watermark using chaos sequence.

In addition, watermarking in DWT domain has drawn extensive attention for its good time-frequency features and its accurate matching of the human visual system (HVS).

Chen et al. [15] proposed two DWT-based audio watermarking algorithms that one of them is based on optimization scheme using group-amplitude quantization and the other embeds information by energy-proportion scheme. Therefore, normalized energy is used instead of probability which rewrites the entropy in information theory as energy proportion function.

Preda et al. [16] proposed three DWT-based video watermarking approaches in which the watermarks used are binary images. Although, in one of them a spread-spectrum technique is used to spread the power spectrum of the watermark data, in the two others, watermarking methods are based on a combination of spread spectrum and quantization.

Deng and Jiang [17] proposed a DWT-based image watermarking algorithm in which the code-division multiple access (CDMA) encoded binary watermark, adaptively is embedded into the third level detail sub-band of DWT domain.

It can be inferred from the literature survey that many of the algorithms proposed met the imperceptibility requirement quite easily but robustness to different image processing are mainly applied to content authentication attacks is the key challenge and the algorithms in literature addressed only a subset of attacks.

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.

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.

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.

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 [18][19]. 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.

3. RESEARCH FINDINGS

The existing approach applies correlation based image watermarking algorithms with respect to changes in watermarking anticipating properties such as imperceptibility and robustness against different attacks.

For security, the binary watermark image scrambled which is reshaped to a sequence and then a random binary sequence is adopted to encrypt the watermark. This process uses a pseudo-random number generator to determine the pixel to be used on a given key.

The RGB channels of the host image are converted to the intended channels and then the first channel is pre-filtered to enhance embedding process.

Low frequency sub-band of wavelet decomposition of its first channel is quantized and divided to different sub-blocks with the certain sub-block size to embed the encrypted watermark.

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. Digital audio and video watermarking techniques rely on the perceptual properties of a human auditory system (HAS) and human visual system (HVS) respectively. The HVS is less sensitive as compared to the HAS.

REFERENCES

[1] Xia, C. Boncelet, and G. Arce, "A Multiresolution Watermark for Digital Images," Proc. IEEE Int. Conf. on Image Processing, Oct. 1997, vol. I, pp. 548-551.

[2] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[3] M. Shensa, "The discrete wavelet transform: Wedding the a trous and mallat algorithms," IEEE Transactions on Signal Processing, vol. 40, no. 10, pp. 2464–2482, 1992.

[4] Mitchell D. Swanson, Mei Kobayashi, Ahmed H. Tewfik, "Multimedia Data Embedding and Watermarking Technologies", Proceedings of the IEEE, 86(6):10641087, June 1998

[5] F. Bartolini, M. Barni, V. Cappellini, and A. Piva, "Mask Building for Perceptually Hiding Frequency Embedded Watermarks," Proc. Int. Conf. on Image Processing, Oct. 1998, vol. I, pp. 450-454.

[6] Yuan Y., Huang D., Liu D., "An Integer Wavelet Based Multiple Logo- watermarking Scheme", In IEEE, Vol-2, pp. 175-179, 2006.

[7] N. Ahmed, T. Natarajan, and K. Rao, "Discrete cosine transform," IEEE Transactions on Computers, vol. 100, no. 1, pp. 90–93, 1974.

[8] P. Bas, J. Chassery, and F. Davoine, "Using the Fractal Code to Watermark Images," Proc. IEEE Int. Conf. on Image Processing, vol. I, Oct. 1998, pp. 469-473.

[9] Reddy R., et al, "Robust Digital Watermarking of Color Images under Noise Attacks", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.

[10] Wang Y., Doherty J.F., Dyck V.R.E., "A wavelet-based watermarking algorithm for ownership verification of digital images", IEEE Transactions, Image Processing, 11 pp. 77-88, 2002.

[11] Wang S.H., LinY.P., "Wavelet Tree quantization for copyright protection for watermarking", IEEE Transactions, Image Processing, pp. 154-165, 2002.

[12] Tao P., Eskicioglu A.M., "A robust multiple watermarking scheme in the discrete wavelet transform domain", Proceedings of the SPIE, Vol. 5601, pp. 133-144, 2004.

[13] Luo Y., et al. "Study on digital elevation mode data watermark via integer wavelets", Journal of software, 16(6), pp. 1096-1103, 2005.

[14] Lin Q., Lin Z., Feng G., "DWT based on watermarking algorithm and its implementing with DSP", IEEE Xplore, pp. 131-134, 2009.

[15] Chen, S.T., Huang, H.N., Chen, C.J., Wu, G.D., 'Energy-proportion based scheme for audio watermarking', IET Signal Process., 2010, 4,(5), pp. 576–587.

[16] Preda, R.O., Vizireanu, D.N., 'A robust digital watermarking scheme for video copyright protection in the wavelet domain', Measurement, 2010, 43, (10), pp. 720– 1726.

[17] Deng, N., Jiang, C.S., 'CDMA watermarking algorithm based on wavelet basis'. Proc. 9th Int. Con. Fuzzy Systems and Knowledge Discovery, May 2012, pp. 2148– 2152.

[18] 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.

[19] 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.