Digital Watermarking in Discrete Wavelet Transformation - Survey

Rama Seshagiri Rao C.[1], Sampath Kumar M.[2] and Prakasam T.[3]

[1] Professor, CSE Department, Geethanjali College of Engineering and Technology, Cheeryal(V), Keesra(M), R.R.Dist., A.P. - 501301, INDIA

[2] Assoc. Professor, CSE Department, Geethanjali College of Engineering and Technology, Cheeryal(V), Keesra(M), R.R.Dist., A.P. - 501301, INDIA

[3] Professor, IT Department, Geethanjali College of Engineering and Technology, Cheeryal(V), Keesra(M), R.R.Dist., A.P. - 501301, INDIA

Abstract

In the early days, encryption and control access techniques were used to protect the ownership of media. Recently, the watermark techniques are utilized to keep the copyright of media. Digital watermarking, a concept of embedding a special pattern, uses an algorithm of inserting a watermark to protect the copyright of media. It has recently become important in various application areas. The various of watermark techniques have been proposed by many authors in the last several years. However, there are not enough analysis and comparison on the previous researches. In this paper, for the understanding of the previous works and for the future related research, we try to classify and analyze the conventional watermark techniques from the various points of view. Currently watermark techniques based on the transfer domain, are more popular than those of the spatial domain. DCT-based methods have been most widely used among the transform based methods. However, recently wavelet based watermark techniques are becoming main research topic. With wide use of internet, effective audio and video watermarking researches are also required.

Keywords: *Digital Watermarking, encryption techniques, wavelet transformation, Image Processing.*

1. Introduction

Data is getting distributed rapidly in the world via the internet. It is very much required to authenticate the data to whom it belongs to. This has increased the requirement of the reliable and secure copy right protection technique invention.

Digital watermarking and fingerprinting are the techniques in the field of Digital Rights Management (DRM). The companies working on tools for digital watermarking and fingerprinting are expecting the market growth to reach more than US$500 million worldwide by 2012, according to a new Multimedia Intelligence report[1]. Companies, such as Cinea, Philips and Verimatrix, are positioning transactional digital watermarking for integration into set-top boxes, to increase content traceability and security. Fox Company has already announced that for early-release of high definition content, watermarking shall be made a compulsory component.

Digital watermarking is a technique to embed copy right protection signature within multimedia contents. Watermark is nothing but an embedded signature, which can be an image or any type of media. A robust watermarking method provides a mark that cannot be removed from the watermarked content. For a watermarking technique to be robust, the watermark should be embedded in the perceptually significant portion of the data. Some typical distortions or attacks that digital watermarking schemes are expected to survive, include re-sampling, rescaling, compression, linear and nonlinear filtering, additive noise, A/D and D/A conversion, and transcoding.

2. Classification of Digital Watermarking Techniques

There are many watermark techniques in terms of their application areas and purposes. And they have different insertion and extraction methods. The following table demonstrates the watermarking classification.

Table 1. Classification of watermarking according to several view points

Classification	Contents
Inserted Media Category	Text, image, audio, video
Perceptivity of watermark	visible, invisible
Robustness of watermark	robust, semi-fragile, fragile
Inserting watermark type	Noise, image format
Processing method in Spatial Domain	LSB, patch work, random function
Transform Domain	Look-up table, spread spectrum
Necessary Data for extraction	Private, semi- private, public watermarking

3. Background on wavelets

Wavelets are functions that satisfy certain mathematical requirements and are used in representing data or other functions. Approximation using superposition of functions has existed since early 1800's , when Joseph Fourier discovered that he could superpose sine and cosines to represent other functions. Wavelet algorithms process data at different scales and resolutions i.e. the resultant activity depends on the perception of the requirement. There are various wavelets: Haar, Coiflet, Daubechie, etc. Whereas the basis function of the Fourier transform is a sinusoid, the dyadic wavelet basis is a set of function which are defined by a recursive difference equation

$$\Phi(X) = \sum_{K=0}^{M-1} CK \quad \Phi(2x-k)$$

where M is the number of nonzero coefficients. The value of coefficients is determined by constraints of orthogonality and normalization.

Wavelet transform uses wavelets as basis and is a tool that cuts up data or functions or operation into different frequency components, and then studies each component with a resolution matched to its scale.

3.1 Wavelet based Watermarking

Watermarking in the Discrete Wavelet Transform (DWT) domain consists of encoding and decoding parts. In the encoding part, we first decompose an image into wavelet frequency domain to obtain decomposed image. Image permuted watermark we add to obtained image decomposition. The watermark permutation is reversible and it is the key for correct watermark extraction. For each coefficient within the wavelet domain, the key has a corresponding value of one or zero (if watermark is a binary image) to indicate if the coefficient is to modify or not. Note that watermarks are not inserted into the LH1, HL1 and HH1 bands (where L denotes the low pass band and H denotes the high pass band), because the energies in these bands are relatively small. In decoding part, we then take the two-dimensional (2D) inverse DWT (IDWT), obtaining the watermarked image I'.

4.0 Watermarking Algorithms in DWT Domain:

Zhu and Tewfik [2] proposed two techniques, which uses a mask in the spatial or frequency domain. Generally, the effects of space or frequency masking are often used to form sequences of pseudo noise in order to maximize the energy of a watermark while maintaining the watermark itself invisible. The authors used the masking values obtained by the model with visual threshold from their work on image binary rate low coding.

Inoue [3] invented a method that applies a DWT to the image, inserts the watermark in low frequency Sub bands and carries out an inverse DWT to obtain the watermarked image. This method allows the embedding of the watermark bits in the same block from which they were extracted, which help enabling good detection and localization of corrupted regions. The obtained watermark is then compared with the bits extracted for each block. If the number of different bits exceeds a predefined threshold, the corresponding block is considered altered. Otherwise the block is authentic.

Paquet and Ward proposed a method based on the DWT [4]. This method was also simulated by Kundur and Hatzinakos with some modifications[5]. The proposed algorithm can detect and localize any tampering with acceptable precision. It is robust against JPEG2000 compression that is based on DWT. Moreover, its security is based on the key security that must be transmitted separately through a secure channel.

In [6], S.C.Chu, H.C. Huang, Y.Shi, S.Y.Wu,C.S.Shieh have used genetic algorithm to select appropriate zero trees in the wavelet transform to pursue both the watermarked image quality and the robustness of the extracted watermark under planned attacks.

In [7], Angela D Angelo, Mauro Barni and Neri Merhav have tested the perceptual intrusiveness and desynchronization efficacy through generating more powerful classes of geometric attacks on images.

In [8], X.B.Wen, H.Zhang, X.Q.Xu,J.J.Quan, the algorithm takes the host image and divides the image into small blocks and then by verifying whether the block can be used for embedding the watermark or not, a decision is taken for embedding watermark. This is mainly to avoid the perceptual degradation of the image. And trained probabilistic Neural networks is applied to recover the watermark.

In[9], A.E.Hassanien, A.Abraham and C.Grosan , have used pulse coupled Neural Networks to enhance the contrast of the human iris image and adjust the intensity with the median filter. They then used PCNN segmentation algorithm to identifying

boundaries of the iris image and then used texture segmentation algorithm to isolate the iris from human eye. They then extracted texture feature from quad tree wavelet and then Fuzzy C-Means algorithm is applied to the quad tree for further processing of boundaries. And then iris codes are extracted that characterizes human iris by using wavelet theory. These codes are embedded in to host images to identify the owner. In the authentication process, hamming distance metric that measure the recorded iris code and the extracted code from watermarked image is used to test whether the image is modified or not.

Lin and Delp proposed a method [10], to generate a smooth watermark that resists to damages caused by JPEG compression. Gaussian distributions of pseudo-random numbers, with a zero average and unit variance, are used to generate the watermark. In consequence, each block contains a different watermark, but the distribution of the watermark in all blocks is similar. Detecting the presence of the watermark is based on the difference between adjacent pixels in the spatial domain. Block's authenticity is decided by comparing the difference with a predefined threshold. The detection and localization capabilities of this algorithm are very acceptable, but its performance could be affected by the block size.

5.0 Conclusion

Many watermarking techniques have been proposed by various authors in the last several years. In this paper, we tried to classify and analyze many previous watermarking methods for understanding them and a help for new researchers in related areas. We classified the previous works from the various points of view: the inserted media category, the perceptivity, the robustness, the inserting watermark type, the processing method and the necessary data for the watermark extraction. Most of researches handled the watermark techniques on image media. Invisible watermarking, robust watermarking and noise style embedding have been main issues in the previous researches. In terms of processing domain, transform domain has been used rather than the spatial domain. Especially DCT-based approach has been widely used among the transform domain approaches, however, currently wavelet-based approach which has the multi-resolution characteristic, is getting its popularity day by day. With the broad spreading of internet, audio and video based services such as MP3 and VOD are also being widely used. Therefore, proper audio and video watermarking techniques are also required to study intensively.

Acknowledgments

We would like to convey our regards to Dr. M.V.N.K.Prasad for guiding us in pursuing our PhD programs. We also convey our regards to the Chairman and Principal, Geethanjali College of Engineering and Technology, for supporting by all means.

References

[1] Securitypark.net
[2]. Zhu B, Swanson MD, Tewfik AH (1996)." Transparent robust authentication and distortion measurement technique for images ". *IEEE digital signal processing workshop (DSP 96)"*
[3]. Inoue H, Miyazaki A, Katsura T (2000) "A digital watermark for images using the wavelet transform." *Integr Comput Aided Eng 7(2):105–115*
[4]. Paquet AH, Ward RK (2002) Wavelet-based digital watermarking for image authentication. *In:Proceedings of the IEEE Canadian conference on electrical and computer engineering, vol I. Winnipeg, Manitoba, Canada, pp 879–884*
[5]. Kundur D, Hatzinakos D (1999) Digital watermarking for telltale tamper proofing and authentication." *Proc IEEE 87(7):1167–1180"*
[6]. S.C.Chu, H.C. Huang, Y.Shi, S.Y.Wu,C.S.Shieh: Genetic watermarking for Zerotree based applications: *Circuits Syst Signal Process(2008) 27:17-182*
[7]. Angela D Angelo, Mauro Barni and Neri Merhav: Stochastic Image Warping for improved watermark desyncronization: *EUROSIP Journal on Information Security:Vol.2008 Art.ID.345184*
[8]. X.B.Wen, H.Zhang, X.Q.Xu,J.J.Quan: A new watermarking approach based on probabilistic neural network in wavelet domain *@ Springer -Verlog 2008*
[9]. A.E.Hassanien, A.Abraham and C.Grosan: Spiking neural networks and wavelets for hiding iris data in digital images, *Published online: 7 June 2008,© Springer-Verlag 2008*
[10]. Lin ET, Christine I, Podilchuk B, Delp EJ (2000) Detection of image alterations using semi-fragile watermarks. *In: Proceedings of the SPIE international conference on security and watermarking of multimedia contents II, vol 3971, San Jose, CA, USA*
[11]. Adil Haouzia & Rita Noumeir : Methods for image authentication: a survey; Published online: *1 August 2007 © Springer Science + Business Media, LLC 2007*

C.Rama Seshagiri Rao B.E.(1991), M.I.T.(1998), M.Tech(2008), pursuing PhD at JNTU Hyderabad. He is presently working as a Professor in Geethanjali College of Engineering and Technology. He is a Life member of CSI and ISTE chapters. He has published many papers in International Journals. He is currently pursuing his PhD in Digital Watermarking under the guidance of Dr.M.V.N.K.Prasad.

M.Sampath Kumar B.E.(1998), M.Tech(2000). He is presently working as a Associate Professor in Geethanjali College of Engineering and Technology. He is a Life member of ISTE chapter. He has published many papers in International Journals. His research interest includes Image Processing, Remote Sensing and GIS applications.

T. Prakasam B.Tech.(1991), M.Tech(1999). He is presently working as a Professor in Geethanjali College of Engineering and Technology. He is a Life member of ISTE chapter. He has published many papers in International Journals. His research interest includes Image Processing, Software Engineering and Data Base Management Systems.