International Journal of Electrical and Computer Engineering (IJECE)
Vol.3, No.1, February 2013, pp. 1~6
ISSN: 2088-8708

Digital Image Watermarking in Wavelet Domain

H. E. Suryavanshi, Amit Mishra, Shiv Kumar
Department of Information Technology, Technocrats Institute of Technology, Bhopal

Article Info

Article history:

Received Nov 2, 2012
Revised Dec 20, 2012
Accepted Jan 6, 2013

Keyword:

Watermarking
Wavelet
DWT

ABSTRACT

Internet allows individuals to share the information. The shared information is like text, image, audio and video files. This information sharing results in some problems such as copyright violation, unauthorized use of documents. Such problems can be solved by using a technique called as digital watermarking. This paper presents different aspects of watermarking and how it is useful for intellectual property protection on internet.

Corresponding Author:

H. E. Suryavanshi,
Departement of Information Technology,
Technocrats Institute of Technology, Bhopal
India
Email: hitendra.suryavanshi@gmail.com

1. INTRODUCTION

The process of embedding information in digital media such that it is imperceptible for human but can be detected by computer algorithm is known as digital watermarking. Figure 1 shows the general process of watermarking. Digital watermarks can be inserted into image, audio and video files using various approaches, schemes and algorithms. [2] The watermark (W) is inserted into the image (I) which results in watermarked data (I').

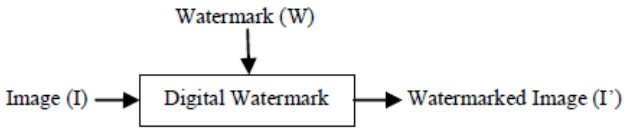

Figure 1. General concept of Watermarking

1.1 Watermark Insertion

The watermark insertion process is shown in figure 2. Encoder (E) takes original image (I) and watermark (W) as input and generates watermarked image (I').

$$E(I, W) = I'$$

1.2 Watermark Extraction

The watermark extraction process is shown in figure 3. Depending on the type of algorithm; the watermark extraction process takes original image (I) and watermarked image (I') for extracting the watermark.

$$D(I', I) = W$$

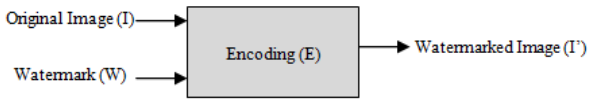

Figure 2. Watermark Insertion

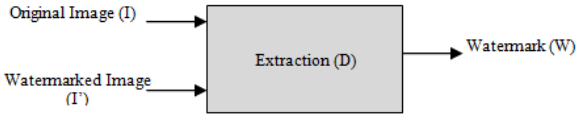

Figure 3. Watermark Extraction

2. PROPERTIES

Watermarking system has number of properties and the importance of each property depends upon the type of applications and role that watermark plays. The important properties of watermarking are given as follows [1]:

2.1 Effectiveness

Probability of embedding watermark into the original contents effectively is nothing but effectiveness. 100% effectiveness is always desired in watermarking but this goal comes with very high cost.

2.2 Fidelity

Fidelity defined as perceptual similarity between un-watermarked and watermarked contents at the particular point of time.

2.3 Data Payload

Data Payload refers to the amount of data that can be embedded into the original content. The payload is different for different types of contents. Example, for image, payload can be a number of bits embedded.

2.4 Robustness

The ability to detect the watermark after performing common operations, such as compression, printing, geometric distortion on watermarked contents, is called robustness.

2.5 Security

Security of watermarking refers to the protection of watermark against various attacks that aimed to thwart the purpose of watermark. Attacks can be passive or active aimed to eliminate watermark.

2.6 Blind or Informed Detection

In some applications, decoder requires original contents during watermark extraction while some not. The decoder which refers to un-watermarked content is known as informed decoder and one that doesn't, known as Blind.

2.7 False Positive Rate

A false positive refers to the detection of watermark in content which is not watermarked. A false positive rate defined as number of false positive which are expected to occur in number of runs of detector.

3. PROPERTIES

Watermarking can be classified into number of types given below [3, 4, and 5]:

3.1 Visible Watermarking

The idea of visible watermark is very simple. The logos used in today's world everywhere is an example of visible watermark. They are especially used for conveying the immediate claim of ownership.

3.2 Invisible Watermarking

In this type of watermarking, rather than displaying logo, the information is concealed into the content itself.

3.3 Fragile Watermarking

Fragile watermarks have limited robustness. They are used to check whether any modification had taken place into the watermarked data.

3.4 Public Watermarking

These types of watermark are not secure because they can read or viewed by anyone using specific algorithms.

3.5 Private Watermarking

Private watermarks are more secure as they need secrete key to be used for retrieving it.

4. WATERMARKING TECHNIQUES

Based on domain used for watermark embedding process, the watermarking techniques can be classified into the following types [4]:

4.1 Spatial Domain

Spatial watermarking can also be applied using color separation such that the watermark appears in only one of the color bands. However, the watermark appears immediately when the colors are separated for printing. Spatial domain technique involves addition of fixed amplitude pseudo-noise into the image. These approaches modify the least significant bits of original contents. The watermark can be hidden into the data by assuming that the LSB data are visually insignificant.

4.2 Transformation Domain

There are many techniques proposed based on transformation domain. Watermarking can be applied in the transform domain; including such transforms are Fast Fourier, discrete cosine, and wavelet. In this first the original data is transformed and then modifications are applied to transformed coefficients.

4.3 Feature Based

Conventional watermarking techniques (first generation watermarking) based on applying watermarking on entire host data. To increase the robustness and invisibility, second generation watermarking was developed. This approach takes into account region, boundary, and object characteristics and so it is robust against the geometric attacks.

5. ATTACKS ON WATERMARKING

Based on how watermark extraction process impaired, the attacks can be classified into four categories given below:

5.1 Removal Attack

Removal attacks main aim is to remove the traces of watermark so that extraction is not be possible.

A) Blind Attack

Noise Addition: Random noise added to garble the watermark.
Filtering: A simple filtering operation can be performed to remove watermark.

B) Estimation Attack

Attacker has certain assumption about the watermark. Then using certain criteria, the embedding distortion is estimated.
Denoising Attack: The cover signal is estimated and then watermark signal replaced by obtained estimate.
Remodulation Attack: The modulation of cover signal is done after estimating embedding distortion.

5.2 Desynchronization Attack

In this case, attacker tries to remove the synchronization between the encoder and decoder instead of removing watermark.

A) Geometric Attack
In this attack, common image processing operations are performed such as filtering, jittering, cropping, change of aspect ratio etc

B) Mosaic Attack
This attack applied on web based applications, where attacker displays stego signal as a tile of many pieces so that decoder will not be able to extract watermark.

5.3 Cryptographic or Security Attack

The main aim of this attach is not to destroy watermark but try to find out secrete of method used for watermark embedding.

5.4 Protocol Attack

The protocol attack aimed at shedding doubt on the reliability of the information system.

6. APPLICATIONS OF WATERMARKING

6.1 Broadcast Monitoring

With the watermark added at the time of creation of contents, easily allows the owner to identify when and where content is broadcast, who is broadcasting and how long.

6.2 Contents Identification

A unique identifier added to the content using watermarking which persist with content whenever it travels.

6.3 Ownership Proof

In case of any dispute, the watermark can be used as proof of ownership.

6.4 Transaction Tracking

This application used to track the record of any transaction made in the history of original content.

6.5 Contents Authentication

Digital work can be easily tampered using various approaches. To identify any changes done in original contents, watermarking can be used.

6.6 Copy Control

This application is used to prevent unauthorized person from making illegal copies of copyrighted material.

7. DISCRETE WAVELET TRANSFORMATION

Fourier Transformations are effectively utilized for representing and analyzing the stationary signals where frequency components do not change over period of time. However, sometimes it is required to determine the existence of frequency components along with their position in case of non-stationary signals. Images are usually non-stationary two-dimensional signals and wavelet transform is effective in such case [13].

The Discrete Wavelet Transform (DWT) generates a matrix which is used for image processing since it captures both frequency and location information. Discrete wavelet transformation (DWT) when applied on image, it decompose image into four frequency sub-bands (LL, HL, LH, HH) where LL refers to low pass band and other three sub-bands corresponds to horizontal (HL), vertical (LH) and diagonal (HH) high pass bands[14]. Figure 4 shows two-level DWT decomposition of image. In general, the watermark can be inserted into low frequency sub-bands (LL) because it increases the robustness of watermark but at the

same time it may degrade the image significantly. High frequency bands (HH) contains edges and textures and changes that are caused due to watermark data inserted in such band cannot be noticed by human eye [9].

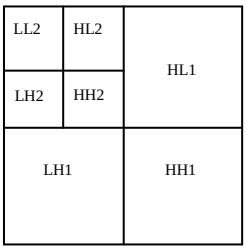

Figure 4 Two-level DWT Decomposition

8. RESEARCH IN WAVELET DOMAIN

A watermarking scheme based on Distributed Discrete Wavelet Transform (DDWT) for image was proposed in [7]. This involves transferring original data from spatial domain to frequency domain using DDWT technique and then embed watermark in the four sub-bands in frequency domain. The watermark information is distributed into the spatial coefficients and thus prevents cropping attack. It also greatly improve performance so that the scheme is robust against geometric attacks such as rotation or scaling and non-geometric attacks such as Gaussian noise, sharpening, and contrast adjustment, too.

An effective image watermarking algorithm based on wavelet transform and edge detection is presented in [8]. The watermark is embedded into the sub-bands coefficients that lie on the edge. Also, the watermark is embedded to selected coefficients around edges, using a different scale factor for watermark strength, that are captured by a morphological dilation operation.

Ali Al-Haj proposed a new image watermarking concept for image that utilizes the best features of Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) [9].Watermarking was done by embedding the watermark in the first and second level DWT sub-bands of the host image, followed by the application of DCT on the selected DWT sub-bands. The combination of the two transforms improved the watermarking performance considerably when compared to the DWT-Only watermarking approach.

In [10] a robust digital watermarking algorithm using wavelet transform was proposed. In this approach coefficients of all sub-bands were utilized to embed the watermark into whole image. Level-adaptive thresholding scheme used to select coefficients. The watermark is embedded to the selected coefficients, using different scale factors depending on the level of decomposition.

A wavelet tree based blind watermarking algorithm for image watermarking using contrast level transformation presented in [11]. The wavelet coefficients of the host image are grouped into trees. The robust watermark and the semi-fragile watermark are embedded by quantizing one tree and resetting the other. Both of the watermarks can be independently extracted without the original image.

A new method for non-blind image watermarking presented in [12] is robust against affine transformation and ordinary image manipulation. The proposed method presents a watermarking scheme based on redundant discrete wavelet transform (RDWT) and Singular Value Decomposition (SVD). After applying RDWT to cover image, SVD applied to each sub-band. Then singular values of the cover image modified using singular values of the visual watermark.

9. CONCLUSION

This paper summarizes different aspects of digital watermarking technique. Digital watermarking provides a potential to protect intellectual property rights. Watermarks can be embedded in a file using various methods but most suitable one is wavelet based as it improves robustness and also watermark remains imperceptible.

ACKNOWLEDGEMENTS

The authors wish to thanks his guides who give a valuable support during the entire work.

REFERENCES

[1] Ingemar J. Cox, *et al*., "Digital Watermarking and Steganography", Second Edition, Morgan Kaufmann Publishers.
[2] Husrev T. Sencar, *et al.*, "Data Hiding Fundamentals and Applications", *Elsevier Academic Press*,Copyright © 2004, Elsevier Inc.
[3] Keshav S Rawat, "Digital Watermarking Scheme for Authorizationagainst Copying or Piracy of Color Images", *Indian Journal of Computer Science and Engineering*,vol. 1 No. 4 295-300, ISSN: 0976-5166
[4] Mohamed Abdulla Suhail, University of Bradford, UK, "Digital Watermarking for Protection of Intellectual Property", Copyright © 2005, Idea Group Inc.
[5] Stefan Katzenbeisser, Fabien A. P. Petitcolas,"Information Hiding Techniques for Steganography and Digital Watermarking",©2000, ARTECH HOUSE, INC.
[6] Vaishali S. Jabadeand and Dr. Sachin R. Gengaje, "Literature Review of Wavelet Based Digital Image Watermarking Techniques", *International Journal of Computer Applications*, vol. 31–No.1, October 2011.
[7] Jung-Chun Liu, Chu-Hsing Lin, and Li-ChingKuo, "A Robust Full-band Image Watermarking Scheme", 1-4244-0411-8/06© 2006 IEEE.
[8] John N. Ellinas, "A Robust Wavelet-Based Watermarking Algorithm Using Edge Detection", *World Academy of Science, Engineering and Technology*, vol. 34, 2007
[9] Ali Al-Haj,"Combined DWT-DCT Digital Image Watermarking", *Journal of Computer Science* vol. 3 No.9 pp 740-746, 2007
[10] Jong Ryul Kim and Young ShikMoon, "A Robust Wavelet-Based Digital Watermarking Using Level-Adaptive Thresholding",0-7803-5467-2/99 ©1999 IEEE.
[11] Min-Jen Tsai *et al.*, "Multipurpose Image Watermarking Based on the Wavelet Tree Contrast Level Transformation" 978-1-4244-3435-0/09, IEEE ICC 2009 proceedings.
[12] Samira Lagzian *et al.*, "Robust watermarking scheme based on RDWT-SVD: Embedding Data in All subbands", 978-1-4244-9834-5/11 ©2011 IEEE.
[13] B. Chanda and D. DuttaMajumder, "Digital Image Processing and Analysis", Second Edition, PHI Publication.
[14] Peining Tao and Ahmet M. Eskicioglue, "A robust multiple watermarking scheme in the Discrete Wavelet Transformation Domain"

BIOGRAPHIES OF AUTHORS

H E Suryavanshi was born in Jaynagar, Maharashtra, India on October 15, 1987. He obtained his B. E. degree in Information Technology from North Maharashtra University in 2009. Currently he is pursuing M. Tech. in Information Technology. His area of interest is in the field of watermarking, steganography. He is a life time member of International Association of Engineers (IAENG).

Amit Mishra received the B.Tech. Degree in Information Technology from M.G.C.G.V, in 2006, the M.Tech. Degree in Computer Science & Engineering from the M.V.J.C.E, Bangalore in 2009, Currently, He is an assistant Professor of Information Technology at TIT, Bhopal. His teaching and research areas include Image processing, Data Mining and watermarking. Mr. Amit Mishra may be reached at amitmishra.mtech@gmail.com.

Shiv Kumar received Diploma (Leather Technology Branch) from Govt. Leather Institute, Agra (U.P.)/ Board of Technical Education, Lucknow (U.P.)-India in year 2000. He worked as a Tanner in Ajaction Lather Punjab Ltd. (Punjab)-India during 2000 to 2001. After that he completed B. Tech. (Information Technology Branch) from Bhagwant Institute of Technology, Muzaffarnagar (U.P.)/ Uttar Pradesh Technical University-Lucknow (U.P.)-India in year 2004, and M. Tech. (Honors, Information Technology Branch) from Technocrat Institute of Technology (TIT), Bhopal (M.P.)/ Rajeev Gandhi Technical University, Bhopal (M.P.)-India in year 2010. He completed Ph.D. (Computer Science & Engineering Branch) from Banasthali University, Tonk (Rajasthan) in year 2012.