INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A SURVEY OF SEMI-FRAGILE IMAGE WATERMARKING ALGORITHM AUTHENTICATION TECHNIQUE

[1] Mangesh Dattatray Sanap, [2]Dr. Vivek Shrivastava

[1]M.tech, Information Technology, ITM Bhilwara, Rajasthan.
[2]H.O.D., Information Technology, ITM Bhilwara, Rajasthan.

Abstract: A semi-fragile image watermarking algorithm based on contour is proposed in this paper. The Y subdivision of original image is subdivided to 4x4 blocks and executed 2-levelDWT transform first, then filtered contour image derived from canny edge detector is used as image feature to generate a watermark. Arnold transform is performed on watermark image to destroy space relativity. Watermark embedding is realized through changing the relationship of selected central DWT coefficients according corresponding watermark bit.
The subtraction result of calculated contour image and extracted watermark image is used to authenticate the content of the image. There is no perceptible degradation to original image. Experiments show that the scheme is useful to meet the requirements of image content authentication and no acceptable PEG compression is rejected. a watermark is embedded in data but to save watermark from counterfeiters we need to find locations which are invariant to all kind of attacks

Keywords- semi-fragile watermark, wavelet transform, contour, content authentication. Discrete Wavelet Transform.

I. INTRODUCTION

Digital watermarking has been developed to protect the copyright and integrity of multimedia content. Digital watermarking is technique about how to hide a special mark into digital multimedia data to protect copyright or verify the integrity and/or the authenticity of the original data [1-2]. Usually, robust watermarking is used to protect the copyright while a fragile or semi-fragile watermarking is used to verify the authenticity [3-4]. Authentication of image data is a challenging task. Content modification or tampering is defined as an object appearance or disappearance, modification to an object position, or changes to texture, color or edges. Image watermarking algorithm used to detect tampering has several essential properties.
First is transparency. The embedding processing should not degrade the quality of the original digital media and should be perceptually invisible to maintain its protective secrecy.
Second is sensitivity. The embedded watermark is robust to resist normal image processing (such as JPEG compression) while it is fragile to malicious tampering to image content.

Third is security. The watermark is embedded in a secure way and it cannot be removed illegally [5-10].Computer and networking facilities are becoming very less expensive and more widespread along with rapid growth of the handling, manipulation and transmission of digital multimedia data, and this gives rise to a wide range of application in entertainment, media technology, agriculture, Medicine, historical research, academics, military and among other fields. Also digital multimedia data have properties like easy processing, compact storage and distortion free transmission [1]. But, under all of these advantages of digital multimedia, there are many undesired issues, like unauthorized replication, manipulation of digital content, pirates of digital works, illegal distribution, copy and modification to digital works which leads to insecurity of IP (Intellectual Property) [3]. By encrypting the multimedia data we can make sure that only the authorized user receives it. But there is no guarantee that this authorized user will not pass it on to others after decryption.

This possibility could be avoided if we trace the undesired operations like copying and distribution of owner's data. In a given Image Watermarking Algorithm, we first convert the color image into gray scale image.

The gray scale image is then subdivided to 2x2, 4x4 and 8x8blocks and executed 2-level DWT transform, then filtered contour image derived from canny edge detector is used as image feature to generate a watermark. Arnold transform is performed on watermark image to destroy space relativity. Watermark embedding is realized through changing the relationship of selected middle DWT coefficients according corresponding watermark bit.

II. CONCEPT OF DIGITAL WATERMARK

Digital watermarking is the state-of-the art in technical multimedia content protection. Stemming from the legal need to protect the intellectual property of the owner from the unauthorized usage, digital watermarking technology attempts to reinforce the copyright by embedding a digital message, called watermark, which can identify the creator or the intended recipients. Digital watermarking process is used for copyright protection, authentication, broadcast monitoring for video, copy control and fingerprinting [1].The digital watermarking scheme consists of different parts such as watermark, encoder, decoder and comparator for extraction of watermark which is may be blind or non-blind extraction [2][8]. The watermark is usually an image in case of a visible watermarking. In case of invisible watermarking, it can be a binary image, random or pseudo-random number.

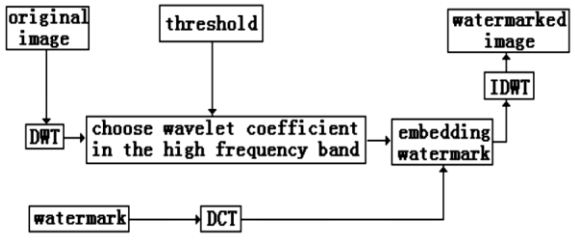

Figure 1.Sketch Map of Watermark Embedding

Step A: For improving the robustness of the watermark algorithm and the secrecy of watermarking image, transform the watermark, that is to make the image DCT transformed and a disordered image will be obtained.

Step B: DWT transform: Decompose the host image X by L-levels using two-dimensional DWT. Then a Approaching sub-image (low frequency band information) and 3L detail sub-images (high-frequency band information) are obtained. How to choose the DWT levels L is depended on the sizes of the original image and the watermarking signal. The higher DWT level is, the better the concealing effect of embedding watermarks.

Step C: Choose the streak blocks: The high frequency

Band information of DWT image is plotted into *2 ⋆2*

Image sub-blocks *Bk*. Then calculate entropy and square values of each image sub-block *Bk*. The image sub-block with small value of entropy should be smooth block, which with big value should be streak block or edge block. And the square value of streak block is small; the one of edge block is bigger. By choosing the right threshold of entropy and the square, the streak blocks wanted

Uk (*k* = *1*, *2*, ⋯, *P*×*Q*) will be obtained.

Step D: Embedding the watermark: Amend the wavelet coefficient values *Ck* of the chosen streak blocks *Bk* to complete the watermark embedding. And the embedding formula is as follow:

$Ck' = Ck + a \times vk, \quad k = 1, 2, \cdots, P \times Q$ (3)

Where, *Ck* represents the former wavelet coefficient Value of streak sub-block *Uk*, *Vk* represents the No. *K componential* weight of one-dimensional digital Watermarking sequence *V*, *′Ck* represents the new Wavelet coefficient value of streak sub-block *k U*, *a*
Represents the embedding depth for digital watermarking.
Figure 1. Sketch Map of Image DWT Decomposed
Figure 2. Sketch Map of Watermark Embedding106

Step E: Inversing transform: After embedding the watermarking signal, unite the information of the lowest frequency band and the mended high frequency band. Then the wavelet transform of the image is inversed byte L-level, and the watermarked image is obtained.

A. Watermark Distilling:

The way of watermark distilling is shown in Fig.3. It
Contains some steps as follow:

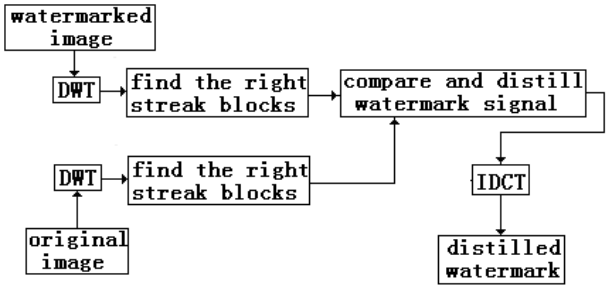

Figure 2. Sketch Map of Watermark Distilling

Step A: DWT transform: Transform the original age
And the watermarked image by L-levels using DWT. And the information of the lowest frequency band and the high frequency band are obtained.

Step B: Make sure the streak blocks: The high Frequency band information, both of DWT image of the original and the watermarked one is plotted into *2 ⋆2*image sub-blocks. The streak block *U* , which is obtained from the high frequency band of original image after being DWT transformed.

(i) Encoder

Encoder takes an image (I) and signature (W) as a watermark and generate new image called watermark image (I'). The encoder function is represented as in eq. (2.1) where the embedding function which is is depends on the watermarking algorithm. The encoding block is represented as shown in Figure 3

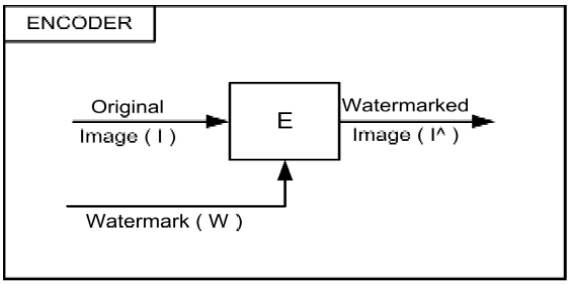

Fig. 3 Encoding block

(ii) Decoder and Comparator

Extracting of watermark is necessary for resolving the ownership or authentication this is done with the help of decoder. Decoding process is distinct approach and it depends on the watermark insertion process and watermarking algorithm. Figure 4: Watermark encoder [2]

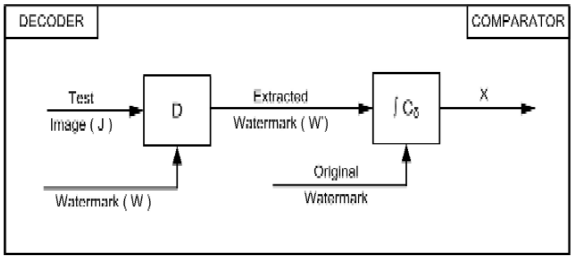

Fig. 4 Watermark Decoder and Comparator

A decoder function D takes an image J (which is watermarked image or no watermarked image or corrupted image) whose ownership is to be determined and recovered the watermark W'[2]. The decoding function is represented as eq. (2.2).

And block diagram representation is

The extracted watermark W' is compared with original Watermark W with the help of Comparator

Figure 2.2: Watermark Decoder and Comparator [2]

Block which is shown in Figure 2.2 and binary output decision is generated. It is '1' if match otherwise '0' which can represent as semi blind algorithm as watermark is used during extraction process. When the original watermark is not used for the extraction of the watermark, called blind algorithm for watermarking, extraction is done with correlation. Where C is the correlation between the two signatures and T is some threshold. Thus the watermarking scheme can be treated as triplet

III. Classification of watermarking techniques

General classification of watermarking techniques is shown in Figure 5 [1].According to embedding domain watermarking is classified into three categories. In spatial domain [1], directly apply the changes to values of pixels. For example, pseudo-random watermark (WM) works by a simple addition of a small amplitude pseudo-noise signal to the original media data

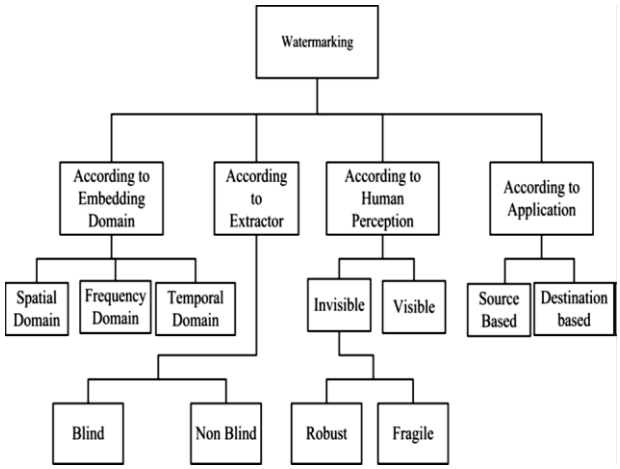

Fig. 5 General classification of watermarking techniques

IV. CONCLUSION

This paper introduces a discrete wavelet transform (DWT) digital watermark algorithm based on human vision characters. By using the block technology, Watermarking signal is embedded into the high frequency band of wavelet transformation domain. And before embedding this watermark image has been discrete cosine transformed in order to improve its robustness. The simulation results suggest that this watermarking system not only can keep the image quality well, but also can be robust against many common image processing operations of filer, sharp enhancing, adding salt noise, image compression, image cutting and so on. This algorithm has strong capability of embedding signal and anti-attack.

V. EXPERIMENT RESULTS

The experiments in this paper are tested with MATLAB 7.0.The original image used to test is a 512×512 image.

A. JPEG 90% Compression

Lossy compression, such as JPEG, is a widely used operation of image, so authentication algorithm should be compatible with image compression operation to distinct it from malicious tamper. Fig. 5 is the experimental results of PEG compression test. The watermarked Lena image's PSNR is 36.41; after 90% JPEG compression, the PSNR descend to 32.87.

REFERENCES

[1] I. J. Cox, M. L. Miller and J. A. Bloom, Digital Watermarking, New York: Academic Press, 2012.
[2] I. Cox, J. Kilian, F. T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing, vol. 6, pp. 1673-1687, December 2013
[3] S. Walton, "Authentication for a slippery new age," Dr. Dobb's Journal, vol. 20, no. 4, pp. 18-26, April 2010.
[4] C. Lu and H. Liao, "Multipurpose watermarking for image authentication and protection," IEEE Transactions on Image Processing, vol. 10, no. 10, pp. 1579- 1592, October 2013
[5] C. Y. Lin and S. F. Chang. "Semi-fragile watermarking for authenticating JPEG visual content," Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents II, San Jose, USA, vol.3971, pp.140-151, 2012.
[6] S. Yang, Z. Lu and F. Zou."A Novel Semi-fragile Watermarking Technique for Image Authentication," ICSP Proceedings, pp. 2282–2285, 2005.
[7] J. Huang, Y. Shi and W. Cheng, "Image watermarking in DCT: An embedding strategy and algorithm," Acta Electronica Sinic, vol.28, no.4, pp.57-60, 2011. (in Chinese)

[8] X. Li, "Blocked DCT and quantization based blind image watermark algorithm," Computer Engineering, vol.32, no.21, pp.139-144, 2013. (in Chinese)
[9] J. Zhang and C. Zhang, "Semi-fragile watermarking for JPEG2000image authentication," ACTA Electronic Sinica, vol.32, no.1, pp.157-160, 2004. (in Chinese)
[10] X. Wang, L. Meng and H. Yang, "Geometrically invariant color image watermarking scheme using feature points," Sci China Ser F-InfSci,vol.52, no.9, pp.1605-1616, September 2009.
[11] M. Yu, H. He and J. Zhang, "A digital authentication watermarking scheme for JPEG images with superior localization and security, "Science in China Series F: Information Sciences, vol.50, no.3,pp.491-509, June 2007.
[12] P. Bao and X. Ma, "Image adaptive watermarking using wavelet domain singular value decomposition," IEEE Trans CircSyst Video Technol, vol. 15, no. 1, pp.96–102, January 2005.
[13] T. Uehara, R. Safavi-Naini, P. Ogunbona, "A secure and flexible authentication system for digital images," Multimedia Systems, vol. 9, no.5, pp.441–456 , March 2004.
[14] J. Wu and F. Lin, "Image authentication based on digital watermarking," Chinese Journal of Computers, vol. 27, no. 9, September 2004. (in Chinese)
[15] D. Zhang, Z. Pan and H. Li, "A novel watermarking algorithm in DCTdomain to authenticate image content," Proceedings of 2009 IEEE International Conference on Intelligent Computing and Intelligent System (ICIS2009), vol. 3, pp.608-611, November 2009.
[16] M. P. Queluz, "Content-based integrity protection of digital images," inSPIE Conf. Security and Watermarking of Multimedia Contents, vol. 3657, pp. 85–93, January. 1999.
[17] C. Lin and S. Chang, "A robust image authentication method distinguishing JPEG compression from malicious manipulation," IEEE Transactions on Circuits and System of Video Technology, vol. 11, no.2,February2001,231