Image Tamper Detection and Recovery Using Dual Watermark

Song Qiang
College of computer science
Beijing University of Technology,
Beijing, China
songqiang@emails.bjut.edu.cn

Zhang Hongbin
College of computer science
Beijing University of Technology,
Beijing, China
zhb@public.bta.net.cn

***Abstract*—A novel dual watermark scheme for image tamper detection and recovery is proposed in this paper. In the proposed watermarking algorithm, we embed the watermark information into the original image using the algorithm of the LSB (Least Significant Bit) and the DWT (Discrete Wavelet Transform). The basic principle of this scheme is to compress each block of the using SPIHT. First of all, we embed the bit stream into the watermark image using the DWT; secondly, scrambling and embedding the bit stream into LSBs of corresponding offset block. By using our algorithm, if the attackers destroy the watermark information, which is embedded the least bit of the watermarked image in case; we could extract the watermark information using DWT to tamper recovery. Experimental results demonstrate that our proposed dual watermark technique is efficient, and recover tampered block data with satisfied image visual quality.**

Keywords-dual watermark; DWT; LSB; tamper detection; image authentication

I. INTRODUCTION

In recent years, the image authentication comes to the front of the image processing and the powerful publicly available digital multimedia processing tools make digital forgeries accessible [1-3]. Multimedia data in digital format can be modified or tampered with ease using a lot of image processing tools, whether it is malicious or not. The protection of intellectual property rights is another increasingly important issue while a large number of digital images are interchanged on the Internet everyday. Therefore, multimedia authentication and integrity verification becomes a popular research area in recent years.

To address both the authentication and integrity issues, a wide variety of schemes have been proposed for different applications. An early attempt in this field was the method proposed in [4], in which the checksums of digital images were calculated and in combination with a seal to produce the watermark information that was responsible for the authentication. Fridrich and the others proposed a self-embedding watermarking algorithm based on DCT (Discrete Cosine Transform). The basic idea of this scheme was to embed a compressed version of a block into the LSBs of a different distant block [5]. Jansi and Afifah [6] first evaluate the watermarking technique proposed by Zain and Fauzi [7] and they proposed an enhancement of authentication watermarking whit tamper detection and recovery (AW-TDR) with improved image quality in Region of Interest (ROI), better recovery rate and better quality of the reconstructed image. Zhang and the others put forward a new self-embedding algorithm. A specified number of lower frequency DCT coefficients were quantized and encoded using a fixed number of bits. It improved positioning computation methods of embedding code, and enhanced the quality of the restored image and the capacity of testing and positioning [8]. CHE and the others proposed an image compression operator based on singular value decomposition, which enhanced compression ratio while improving recovery quality of tampered images [9]. Gantasala and Prasad have proposed a semi-fragile watermark technique for image authentication using discrete wavelet domain the watermark is embedded by quantizing the corresponding wavelet coefficients and they conclude that using their approach the image distortion is decreased [10]. Lee and Shinfeng proposed an effective dual watermark scheme for image tamper detection and recovery. In their algorithm, each block in the image contains watermark of other two blocks. The two copies of watermark of the whole image and provide second chance for block recovery in case one copy is destroyed, a secret key, which is transmitted along with the watermarked image, and a public chaotic mixing algorithm are used to extract the watermark for tamper recovery [1]. Based on Lee's work, Surya and Munaga proposed an effective dual watermark scheme for image tamper detection and recovery, which proposed by [1] is unable to detect the tamper in the watermarked image, if any one bit or more than one bit in 5-MSBs is changed, they demonstrated the attacks and concluded that there is a flaw in their watermarking technique and the attacker can tamper a watermarked image easily without being detected and results are compared [11].

However, the current image tamper detection and recovery algorithms have some problems. One of these problems is that the security of the algorithms is not very well.

In this paper, we present an effective dual watermark scheme for image tamper detection and recovery. Our algorithm is compressing per block of the original image

978-1-4244-3709-2/10/$25.00 ©2010 IEEE

using SPIHT to reduce the capacity, and then we embed the watermark information into the original image using the algorithm of the LSB and the DWT. To verify the effectiveness of the proposed scheme, a series of simulations and experiments are conducted. Experimental results demonstrate that our proposed dual watermark technique is efficient, and recover tampered block data with satisfied image visual quality. In addition, if the attackers destroy the watermark information, which is embedded the least bit of the watermarked image in case; we could extract the watermark using DWT to tamper recovery. Thus, this algorithm assures the security of the watermarked image.

The reminder of this paper is organized as follows: In Section 2, the proposed scheme, including the watermark generation, embedding, tamper detection and recovery is introduced. In Section 3, the experimental results are presented to show the effectiveness of this scheme. Conclusions are finally drawn in Section 4.

II. THE PROPOSED ALGORITHM

The proposed image authentication scheme is based on the self-embedding watermarking technique of image. The details are described in the following subsections.

A. Watermark Embedding

Due to the limitation of embedding capacity, it is necessary to compress the original image in a very small size. Moreover, compression of the image content should be ensured that the recovered image quality is acceptable, considering the embedding capacity of the original image. All the images used in this paper are assumed to be of size M×M pixels.

The overview of the watermark self-embedding process is illustrated in Figure.1.

The algorithm steps are listed as follows:

1) Reset the least significant bits of the original image to zero, and divide the modified image into blocks of size 32×32;

2) For each block, compress it with SPIHT encoder of rate 0.9bpp to obtain the compression watermarking information;

3) Scramble SPIHT compressed bit-stream using Arnold transformation with a secret key K to obtain the embedding watermarking information, which is converted into a binary image;

4) For the Modified image, decompose it with discrete wavelet transform (DWT), in this paper we use the 2-level DWT, the binary image embedded into the modified image using the DWT;

5) Reconstruct the processed image information using the inverse discrete wavelet transform (IDWT), in order to deal with the watermarked image;

6) Embed the watermark information into the least significant bits of an offset block which is determined by certain rules from the modified image, we could get the final watermarked image.

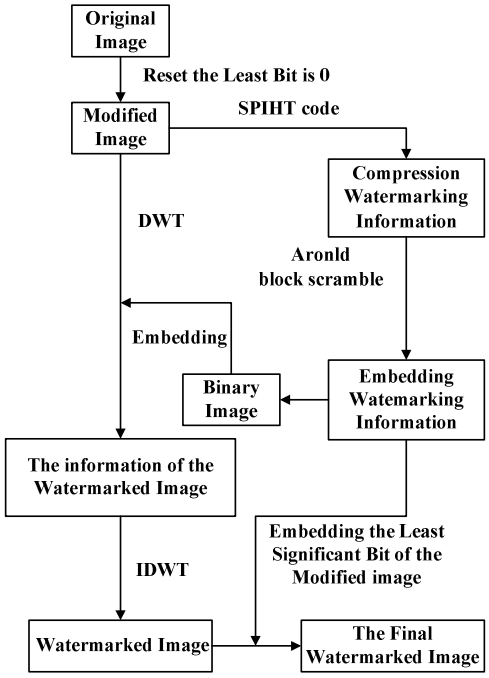


Figure 1. The overview of the watermark self-embedding process

B. Tamper Detection and Recovery

Watermark extraction is the inverse process of embedding. The crucial part of the recovery process is to locate tampered regions, and extract the embedded watermark from the remaining image to fill tampering regions.

The overview of the watermark image tamper detection and recovery process is illustrated in Figure.2.

The algorithm steps are listed as follows:

1) Extract the least significant bits per block from the watermarked image by embedding rules;

2) Get the SPIHT encode of the watermarked image;

2.1) If the SPIHT encode is incorrect, extracting the watermark information using DWT, the watermark information is binary image, which is the correct modified image information;

2.2) If the SPIHT encode is correct, we would use the watermark information to recover the tampered image;

3) Anti-scramble the watermark information using Anti-Arnold transformation with the secret key K;

4) Decompress the anti-scrambled watermark with SPIHT decoder to recover the watermarked image;

5) Compare the extracted watermarked image and the tampered image, if the two image are different;

6) Detect the tampered area by a comparison between the extracted watermark image and the watermarked image, and fill the tampered areas correspondingly with information from the recovered watermark image;

7) If the extracted watermarked image is same as the modified image, we think the image is a true image.

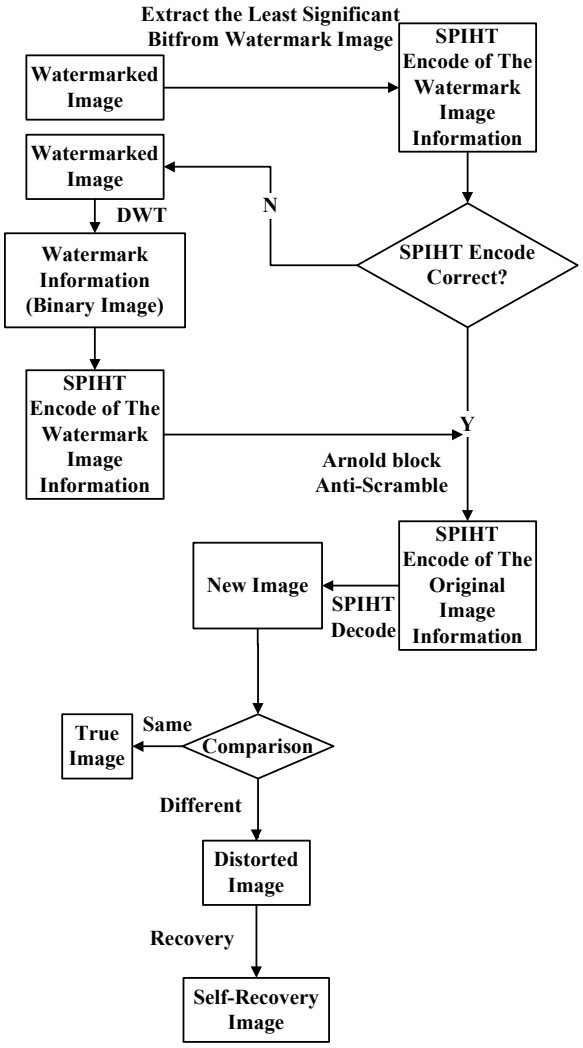


Figure 2. The overview of the watermark image tamper detection and recovery process

C. *Details of the Scheme*

According to the experimental results, we choose to divide the image into block size 32×32, because SPIHT can not achieve a good result when block size is too small. To obtain a satisfied visual quality, we set the compression ratio 0.9bpp.

In this paper, to enhance the security of watermarked image, we embed the watermark information using two methods, which are the LSB algorithm and the DWT algorithm. If an attacker deletes the information of the Least Significant Bit, we can extract the watermark information using DWT, and recover the tampered image.

III. SIMULATIONS AND RESULTS

This section presents the simulations and experiments of the proposed scheme and the results obtained.

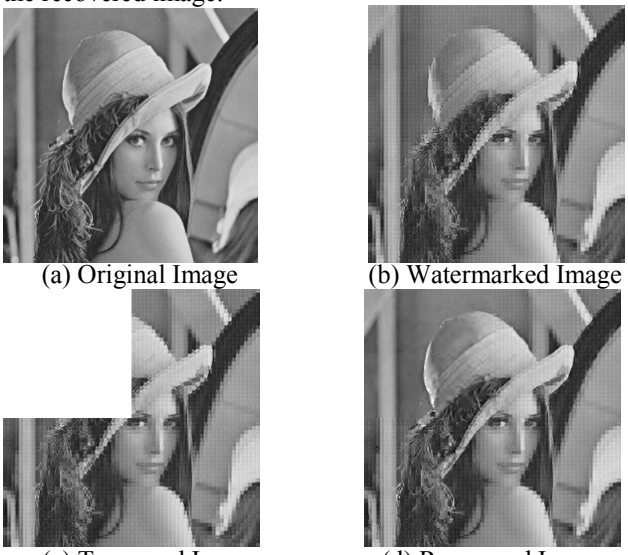
For quantitative evaluation, PSNR (Peak Signal-to-Noise Ratio) is introduced to evaluate the performance of the proposed scheme and image quality, which is defined as:

$$\boldsymbol{PSNR} = 10\log_{10}\left(\frac{255^2}{\boldsymbol{MSE}}\right)\boldsymbol{dB} \tag{4.1}$$

$$\boldsymbol{MSE} = \sum_{i=0}^{n-1}\sum_{j=0}^{m-1}\frac{(\boldsymbol{a}_{i,j} - \boldsymbol{b}_{i,j})^2}{\boldsymbol{n}\times\boldsymbol{m}} \tag{4.2}$$

where $m \times n$ is the image size, $a_{i,j}$ and $b_{i,j}$ are the corresponding pixel values of two images.

Figure.3 shows the self-embedding and tampered recovery of Lena. (a) is the original Lena image with size 256×256; (b) is the watermarked image; (c) is tampered in the top-left of (b), the tampered area is 1/4; and (d) is the recovered image.

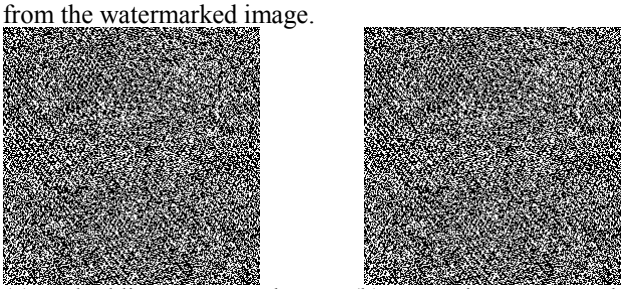


(a) Original Image (b) Watermarked Image

(c) Tampered Image (d) Recovered Image

Figure 3. Experimental result of Lena Image

Figure.4 shows the result of embedding and extracting the watermarking information, (a) is the watermark information; (b) is the extracted watermark information from the watermarked image.



(a) Embedding Watermark (b) Extracting Watermark

Figure 4. Experimental result of embedding and extracting the watermarking information

Due to the original image compressed with the SPIHT encoder, so the watermark image is a binary image.

From the experimental result, we can see the extracting watermark is the same as the embedding watermark. The value of NC is 1.0000.

The quality of recovered images highly depends on the size of tampered regions and how accurately those tampered blocks can be identified. In addition, the complex of the image content affects the quality of the recovered images.

Figure.5 shows that if an attacker deletes the LSB of watermarked image, we can extract the watermark information accurately. (a) is the original Lena image, (b) is the tampered image, which is deleted the information of the LSB. (c) is the extracted watermark information from the tampered image, (d) is the decompressed image using SPIHT decode.

(a) Original Image (b) Tampered Image

(c) Extracted Watermark (d) Decompressed Image

Figure 5. Experimental result of tampered image

To an objective description of the experimental results, TABLE.I lists the experiment results of our scheme self-embedding watermarking and recovery algorithms. TABLE.II shows the PSNR of recovered image from different tampered areas. We can see that our algorithm assures the quality of watermark image, and markedly enhances the security of watermarked image. This algorithm achieves better balance between the quality of watermark and recovery image.

IV. CONCLUSION

In this paper, a novel dual watermark scheme is presented for image tamper detection and self-recovery. We embed the watermark information into the original image using the algorithm of the LSB and the DWT. By using our algorithm, if the attackers destroy the watermark information, which is embedded the least bit of the watermarked image, we can extract the watermark using DWT to recovery. The experimental results show that the proposed scheme can effectively thwart collage attack, and tampered images can be recovered with better image visual quality and improved the security of the algorithm.

TABLE I. PSNR AND NC OF SELF-EMBEDDING AND RECOVERY

Original Image (Lena)	PSNR	NC
Watermarked Image	25.5026	0.9932
Restoration Image	30.6614	0.9939

TABLE II. PSNR OF RECOVERED IMAGES FROM DIFFERENT TAMPERED AREAS

Original Image (Lena)	PSNR
Watermarked Image	25.5026
1/8	27.1270
1/4	26.8373
1/2	26.7350

ACKNOWLEDGMENT

This work is supported in part by the National Natural Science Foundation of China (NSFC) under grant 60775011.

REFERENCES

[1] Tien-You Lee, Shinfeng D.Lin, "Dual watermark for image tamper detection and recovery", Pattern Recognition, Vol. 41, 2008, pp. 3497-3506

[2] P.L. Lin, C.-K. Hsieh, and P.-W. Huang, "A hierarchical digital watermarking method for image tamper deteciton and recovery", Pattern Recognition, Vol. 38, 2005, pp. 2519-2529

[3] Qiang Song, Hongbin Zhang, "Tamper Detection and Self-Recovery of Image Based on Self-Embedding", Proceedings - 2009 Asia-Pacific Conference on Information Processing, Vol. 2, 2009, pp. 76-79

[4] S.Walton, Image Authentication for a Slippery New Age, Dr. Dobb's Journal of Software Tools for Professional Programmers, Vol.20, Apr. 1995

[5] J.Fridrich and M.Goljan, Protection of digital images using self-embedding, Proceeding of International Conference on Information Technologies and Control, Kazakhstan, 1999, pp. 302-311

[6] Jasni Mohamad Zain, Afifah Nailah Muhamad, "Authenticaiton watermarking with tamper detection and recovery (AW-TDR)", Proceedings of the International Conference in Electical Engineering and Informatics, 2007, pp. 538-541

[7] Zain, J.M, Fanzi, A.R.M, "Medical image watermarking with tamper detecion and recovery", The 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2006, pp. 3270-3273

[8] ZHANG H B, YANG C, Tamper Detection and Self Recovery of Images Using Self-Embedding, Chinese Journal of Electronics, 2004, 32(2):196-199

[9] Sheng-Bing Che, Zu-Guo Che, Bin Ma, Qiang-Bo Huang, Image self-embedding technology research based on singular value decomposition, 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), 2008

[10] Raghu Gantasala and Munaga V.N.K, Prasad, "New quantization technique in semi-fragile digaital watermarking for image authentication", Third International Conference on Information Systems, Technology and Management, Vol. 31, 2009, pp. 244-255

[11] Chaluvadi, S.B., Prasad, M.V.N.K., Proceedings of the 2009 World Congress on Nature & Biologically Inspired Computing (NaBIC 2009), 2009, pp. 993-998