Optics and Photonics Journal, **2013, 3, 103-107**
doi:10.4236/opj.2013.32B026 Published Online June 2013 (http://www.scirp.org/journal/opj)

Scientific Research

A Simple Image Tamper Detection and Recovery Based on Fragile Watermark with One Parity Section and Two Restoration Sections*

Chao-Ming Wu, Yan-Shuo Shih
Graduate Institute of Aeronautical and Electronic Engineering, National Formosa University
Email: cmwu@nfu.edu.tw

Received 2013

ABSTRACT

A fragile self-recovery watermarking scheme with simple and effective tamper detection capability is proposed in this paper. In conventional fragile watermark for tamper detection and recovery, the parity section of the watermark is used for tamper detection and the restoration section of the watermark is used for image recovery, separately. In addition, to provide second chance for block recovery in case one copy is destroyed, Lee and Lin proposed dual watermarking scheme in which two copies of restoration watermark are embedded. In the proposed new scheme, fragile watermark with one parity section and two restoration sections are embedded, too. In addition to the second chance for image restoration, the two restoration sections as well as the parity section are all used for tamper detection. Experimental results show that the tamper detection capability is superior to other techniques.

Keywords: Tamper Detection; Recovery; Fragile Watermark; Dual Watermark; Collage Attack

1. Introduction

In recent years, the image authentication is an interesting research topic since 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 integrity and authenticity of digital images can be guaranteed by using digital fragile watermarking which is a technique to embed a digital signature into an image [1, 5, 7]. To reconstruct tampered regions, several self-recovery watermarking schemes have been proposed [2-4, 6]. These schemes embed image block features as a watermark payload of a different image block (or blocks).

Lin *et al.* [4] proposed that the validity of an image block was determined by additional authentication data in a block. Specifically, the payload of watermark consists of authentication data as well as recovery data. The authentication data for a block is embedded in the block itself, whereas the recovery data is embedded in a different block.

If large portions of an image are tampered, then the quality of the recovered image is generally poor. To improve the recovery quality, Lee and Lin [3] proposed a dual-watermarking method. This scheme maintains two watermark copies of the whole image and provides a second chance for block recovery in case one copy is destroyed.

He *et al.* [2] presented the performance analysis of a self-recovery fragile watermarking scheme employing an optimized neighborhood characterization method to detect the tampering.

In this paper, we propose an improved watermark embedding and tamper recovery scheme which is superior to other techniques. The fragile watermark consists of one parity section and two copies of restoration section. In tamper detection phase, the detection algorithm utilizes all of the three watermark sections such that the false detection probability can be reduced. In recovery phase, two copies of restoration section provide dual chance for block recovery. As the same as the dual watermarking scheme proposed by Lee and Lin [3], it will result in better performance especially when the tampered area is really large.

The remainder of this paper is organized as follows. In Section 2, the watermark generation and embedding of the proposed algorithm is described. Section 3 and 4 presents the tamper detection strategies and image recovery process. Experimental results are shown in Section 5 and conclusions are given in Section 6.

2. Block-Based Watermark Embedding

The flowchart of watermark embedding procedure is

*This work was supported by the National Science Council of the Republic of China under grant NSC 101-2221-E-150-006-MY2.

shown in **Figure 1**. To localize tampering, the original image is partitioned into blocks of size 3×3. The two LSBs of every pixel are replaced for watermark embedding. So, the amount of watermark capacity in an image block is 18 bits. For each image block, the 2 LSBs of each pixel are reset to 0 firstly. Then, the 6-bit parity section W_d of the watermark is generated by applying the XOR operation on the 54 MSBs and an 9×6 encrypt table that is randomly generated by secret key1. The block diagram is shown in **Figure 2**. The restoration watermark section W_r is the average intensity of pixels in an image block. The 6-bit parity watermark section of image block *i* is embedded as a payload of block *i*. To embed the two copies of 6-bit restoration watermark section, two random block mapping functions, σ_1 and σ_2, are required. The two copies of 6-bit restoration watermark section of block *i* are embedded into block $\sigma_1(i)$ and $\sigma_2(i)$. The relationship between image blocks is shown in **Figure 3.**

3. Tamper Detection Strategies

The tamper detection procedure is divided into the following five steps.

Setp 1. Intra-block parity check: Recompute block-parity bits W_d^1 from MSBs of each block. Then, extract the embedded block-parity bits W_d^2 from LSBs of each block. If $W_d^1=W_d^2$, the block is valid and set $m_1=0$; otherwise, $m_1=1$. m_1 is the tamper detection index in step 1.

Setp 2. Improvement based on block-neighborhood tampering characteristics. The detection index in step 2 is assign as:

$$m_2=\begin{cases}1, & if\ m_1=0\ and\ N_{m_1=1}\geq 4\\ m_1, & others\end{cases} \quad (1)$$

where $N_{m_1=1}$ is the number of the eight neighboring blocks with $m_1=1$.

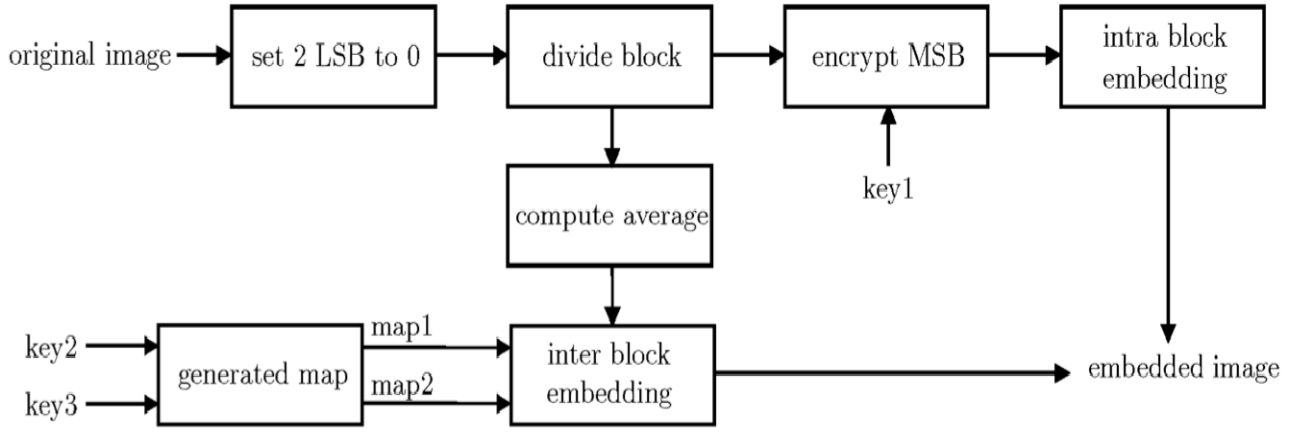

Figure 1. Flowchart of watermark embedding.

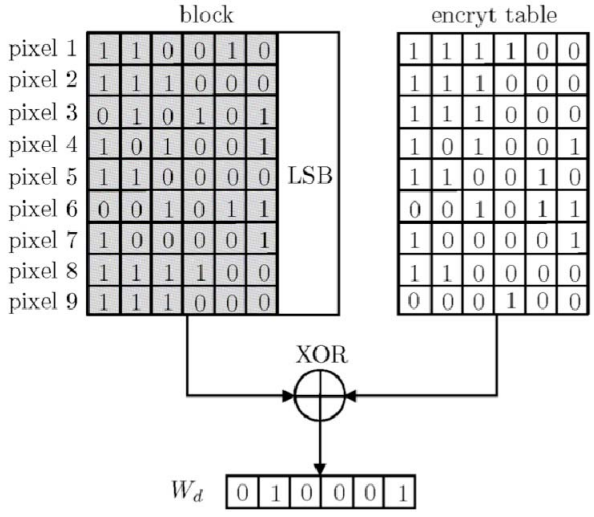

Figure 2. Generation of 6-bit parity watermark.

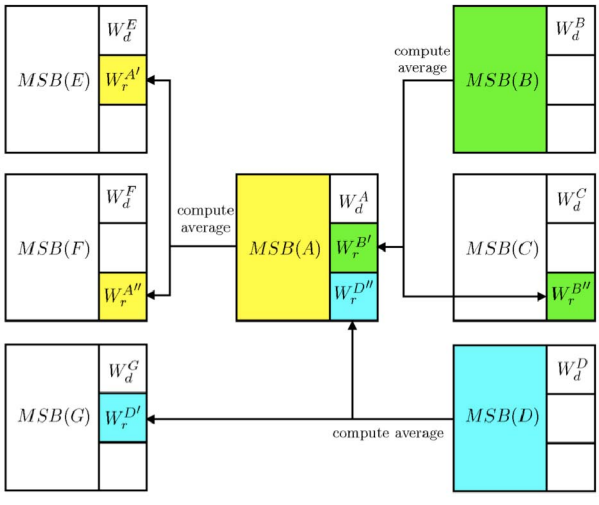

Figure 3. Relationship between image blocks.

The above two detection steps can achieve good performance for most types of tampering. But, for collage attack, additional detection steps below are required.

Setp 3. Inter-block restoration watermark section comparison: As demonstrated in **Figure 3**, there are at most six valid pairs of inter-block comparison. Assume N denotes the number of valid inter-block comparison pairs. The detection index in step 3 is:

$$m_3 = \begin{cases} 1, & \text{if } m_2 = 0 \text{ and the number of} \\ & \text{inconsistent pairs is more than } N/2 \\ m_2, & \text{others} \end{cases} \quad (2)$$

Setp 4. Improvement based on block-neighborhood tampering characteristics: In tampered region, the probability of false accept is high for large tamper ratio, especially. To reduce this undesired property, the tamper detection index needs to be corrected by:

$$m_4 = \begin{cases} 1, & \text{if } m_3 = 0 \text{ and } N_{m_3=1} \geq \lambda_1 = 3 \\ m_3, & \text{others} \end{cases} \quad (3)$$

Setp 5. Improvement based on block-neighborhood tampering characteristics: In addition to the detection index correction for tampered region in step 4, the probability of false reject in the non-tampered region can also be reduced according to block-neighborhood tampering characteristics. The modification of tamper detection index is:

$$m_5 = \begin{cases} 0, & \text{if } m_4 = 1 \text{ and } m_2 \neq 1 \text{ and} \\ & N_{m_4=1} \geq \lambda_2 = 3 \\ m_4, & \text{others} \end{cases} \quad (4)$$

Note, λ_1 and λ_2 are determined by simulation such that the probability of false detection is minimized.

4. Image Recovery

All blocks in the test image are marked as either valid or invalid after tamper detection. The invalid block needs to be recovered using the restorstion watermark section that is embedded in the other block. In the proposed scheme, since two copies of restorstion watermark section are embedded, the invalid block can be recovered if any one of the two blocks that the restorstion watermark section embedded into is valid. In this case, by padding the extracted 6-bit restoration watermark section with two 0s to the end, the image recovery process is just replacing the intensity of each pixel within the invalid block with this new 8-bit intensity. To further improve the recovered image quality, the invalid blocks without valid restorstion watermark section can be recovered by the average intensity of the neighboring valid pixels.

5. Experimental Results

Numerous experiments are conducted to demonstrate the effectiveness of the proposed self-recovery fragile watermarking scheme. The 8-bit gray-scale image Lena is used as the host image. **Figure 4** shows the original and the watermarked images. Since only 2 LSBs are changed, the PSNR of the watermarked image is 44.33 dB. The probability of false rejection (PFR), probability of false acceptance (PFA), and probability of false detection (PFD) are used as the quantitative performance measures [2]. Types of tampering including the crop tampering, the content-only tampering, the constant-average attack, and the collage attack are considered. For cropping attack, the PFA, PFR, and PFD are all zero for different tamper ratio from 0 to 80%. Under both the content-only tampering and constant-average attack, the PFA, PFR, and PFD are less than 10^{-3} for tamper ratio in the range of [0, 80%]. Consider the effect of collage attack, both images "Lena" and "Barbara" were watermarked using the same key. The collaged image was constructed by copying certain regions of Barbara and pasting it onto the Lena image, and their relative spatial locations in the image were preserved. **Figure 5** is the collage attacked image with tamper ratio 25% and the recovered image.The tamper detection performance under collage tampering is shown in **Figure 6**. It's apparent that PFA, PFR, and PFD are all less than 0.1 if the tamper ratio is less than 40%.

(a)

(b)

Figure 4. (a)Original image (b)Watermarked image.

(a)

(b)

Figure 5. (a)Collage attacked image (b)Recovered image.

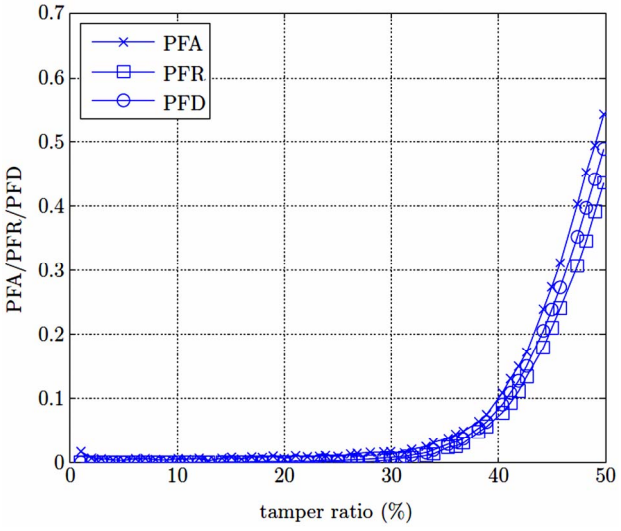

Figure 6. Tamper detection performance under collage tampering.

Figure 7 shows the PFD by the proposed scheme, Lee's scheme [3], and He's scheme [2] under the collage attack. As shown in **Figure 7**, the PFD of Lee's scheme increases linearly with the increase of the tamper ratio. For tamper ratio less than 30%, the proposed scheme and He's scheme have similar performance. But, for tamper ratio larger than 30%, our new scheme is superior to He's method.

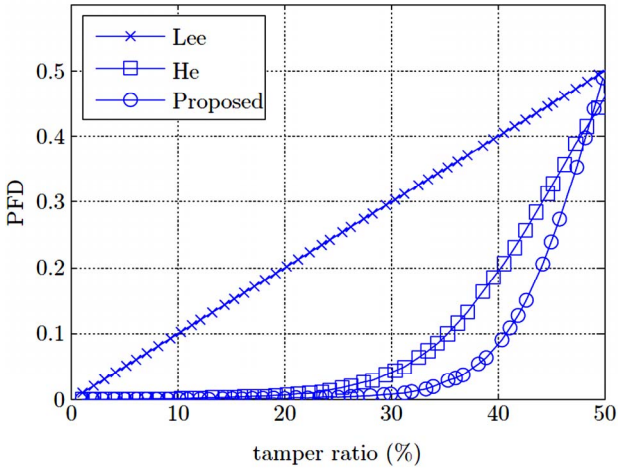

Figure 7. Performance comparison under the collage attack.

6. Conclusions

A simple self-recovery fragile watermarking scheme is proposed in this paper. To localize tampering, the original image is partitioned into blocks of size 3×3. In this new scheme, the watermark payload is composed of parity watermark section and two copies of restoration watermark section. All of the watermark sections are used for tamper detection. Thus, with the same size of watermark payload, the tamper detection performance of the proposed scheme is better. Since only the two LSBs of each pixel are used for watermark embedding, the PSNR of the watermarked image is about 44 dB. Under general tampering, content-only tampering and constant-average attack, the PFA, PFR, and PFD all approach zero for different tamper ratio from 0 to 80%. For the collage attack, the proposed new scheme is superior to both Lee's scheme and He's method.

REFERENCES

[1] J. Fridrich, "Security of Fragile Authentication Water-Marks with Localization," *Proceedings of SPIE 4675, Security and Watermarking of Multimedia Contents IV*, Vol. 691, 2002, pp. 691-700. doi:10.1117/12.465330

[2] H. J. He, F. Chen, H.-M. Tai, T. Kalker and Jiashu Zhang, "Performance Analysis of A Block-Neighborhood-Based Self-Recovery Fragile Watermarking Scheme," *IEEE Transactions on Information Forensics and Security*, Vol.7, No.1, 2012, pp.185-196. doi:10.1109/TIFS.2011.2162950

[3] T.-Y. Lee, S. F. Lin and D. Dual, "Watermark for Image Tamper Detection and Recovery," *Pattern Recognition*, Vol.41, No.11, 2008, pp. 3497-3506. doi:10.1016/j.patcog.2008.05.003

[4] P. L. Lin, C.-K. Hsieh and P.-W. Huang, "A Hierarchical

Digital Watermarking Method for Image Tamper Detection and Recovery," *Pattern Recognition*, Vol.38, No.12, 2005, pp. 2519-2529. doi:10.1016/j.patcog.2005.02.007

[5] M. Utku Celik, G. Sharma, E. Saber and A. Murat Tekalp, "Hierarchical Watermarking for Secure Image Authentication with Localization," *IEEE Transactions on Image Processing*, Vol. 11, No.6, 2002, pp. 585-595. doi:10.1109/TIP.2002.1014990

[6] X. P. Zhang and S. Z. Wang, "Fragile Watermarking with Error-Free Restoration Capability," *IEEE Transactions on Multimedia*, Vol.10, No.8, pp. 1490-1499, 2008. doi:10.1109/TMM.2008.2007334

[7] X. P. Zhang and S. Z. Wang, "Statistical Fragile Watermarking Capable of Locating Individual Tampered Pixels," *IEEE Signal Processing Letters*, Vol.14, No.10, 2007, pp. 727-730.doi:10.1109/LSP.2007.896436

