J Inf Process Syst, Vol.14, No.3, pp.666~679, June 2018
https://doi.org/10.3745/JIPS.03.0096

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

LBP and DWT Based Fragile Watermarking for Image Authentication

Chengyou Wang*, Heng Zhang*, and Xiao Zhou*

Abstract

The discrete wavelet transform (DWT) has good multi-resolution decomposition characteristic and its low frequency component contains the basic information of an image. Based on this, a fragile watermarking using the local binary pattern (LBP) and DWT is proposed for image authentication. In this method, the LBP pattern of low frequency wavelet coefficients is adopted as a feature watermark, and it is inserted into the least significant bit (LSB) of the maximum pixel value in each block of host image. To guarantee the safety of the proposed algorithm, the logistic map is applied to encrypt the watermark. In addition, the locations of the maximum pixel values are stored in advance, which will be used to extract watermark on the receiving side. Due to the use of DWT, the watermarked image generated by the proposed scheme has high visual quality. Compared with other state-of-the-art watermarking methods, experimental results manifest that the proposed algorithm not only has lower watermark payloads, but also achieves good performance in tamper identification and localization for various attacks.

Keywords

Discrete Wavelet Transform (DWT), Fragile Watermarking, Image Authentication, Local Binary Pattern (LBP), Semi-blind Detection

1. Introduction

The development of multimedia and Internet technologies makes it more convenient for us to transmit and store digital images. At the same time, due to the massive emergence of image-editing software, digital images can be easily manipulated according to our own minds. Therefore, the integrity and authenticity of images have been seriously challenged. To solve this problem, a new technology called digital watermarking arises at the historic moment. Its main idea is to insert the secret information associated with host image into the image itself. According to the embedding domain, digital watermarking algorithms can be classified into two categories, namely spatial domain watermarking and frequency domain watermarking [1,2]. In spatial domain, the watermarking message is inserted by modifying pixel values directly. In frequency domain, the transform coefficients are modulated by the watermarking message. Many watermarking algorithms have been presented in the last few years. In terms of different functions, these watermarking algorithms can be further split into

Manuscript received February 14, 2017; first revised April 2, 2017; accepted May 30, 2017; onlinefirst May 14, 2018.
Corresponding Author: Xiao Zhou (zhouxiao@sdu.edu.cn)
* School of Mechanical, Electrical and Information Engineering, Shandong University, Weihai, China (wangchengyou@sdu.edu.cn, sdwhzh @mail.sdu.edu.cn, zhouxiao@sdu.edu.cn)

robust watermarking algorithm and fragile watermarking algorithm [3,4]. Generally, the robust watermark can resist common attacks, which is usually utilized for copyright authentication. The fragile watermark is sensitive to modifications, and it is usually applied in image content authentication.

In this paper, we focus on the fragile watermarking algorithm used for tamper identification and localization. Many researchers have made great efforts in this field. The most typical fragile watermarking method is the watermarking algorithm based on the least significant bit (LSB), which was proposed by Walton [5]. In his method, the check-sum of the seven most significant bits is embedded into the LSB of each pixel. Though it is simple, this scheme is less secure and provides very limited ability in tamper detection. To overcome this defect, a lot of improved methods have been presented. Liu et al. [6] introduced a fragile watermarking algorithm based on chaotic system and pixel-pairs. The watermark is obtained by mapping the difference image between the original image and chaotic image into a binary image. Then the watermark is inserted into the LSBs of original image. Rawat and Raman [7] suggested a chaotic pattern based fragile watermarking method in which a scrambled watermark is generated by applying exclusive-or operation between a binary watermark image and a chaotic image produced by logistic map. These two methods achieve good performance under some common attacks, but they cannot resist the content-only attack. To address this issue, Teng et al. [8] presented an improved fragile watermarking algorithm on the basis of [7]. Compared with the method in [7], the image content is taken into account during the watermark embedding process [8]. Recently, the local binary pattern (LBP) operator was introduced into watermarking field [9,10]. A semi-fragile watermarking based on LBP operators in spatial domain was proposed by Zhang and Shih [9]. A binary watermark is inserted into the host image by adjusting the neighborhood pixel values in each block using its LBP pattern. Experimental results prove that this algorithm is robust against general image processing operations to a certain extent, such as contrast adjustment and JPEG compression. However, the main drawback of these watermarking schemes mentioned above is that they are not blind in tamper detection. The original watermark or image is still needed when the detection process is applied on the receiving side. This is not practicable because the original watermark or image is not always available. So the semi-blind and blind watermarking scheme with high detection accuracy becomes a research focus. Benrhouma et al. [11] suggested a fragile watermarking algorithm for blind tamper detection in which the watermark is constructed by the local pixel contrast between the neighborhood pixel values and average pixel value of each block. However, a false alarm exists in the detection result. Preda [12] proposed a semi-fragile watermarking in wavelet domain. In his method, the wavelet coefficients are firstly permuted by using a secret key, and then they are divided into different groups. A binary random sequence formed by the secret key is adopted as the watermark. By means of quantization, a watermarking bit is inserted into a group of coefficients. This scheme achieves better image quality with low watermark payloads. However, in tamper detection, many noise dots are spread all over the image which reduces the detection precision. To clean the noise dots, the filtering and mathematical morphology operations are adopted in [12]. However, the intensity of post-processing operations should be different for different tampered images, which is hard to achieve.

This paper presents a fragile watermarking algorithm based on LBP and discrete wavelet transform (DWT) for image tamper detection. The LBP pattern of low frequency wavelet coefficients is served as authentication watermark and inserted into the LSB of the maximum pixel value in each image block. To ensure the security of the proposed algorithm, the watermark is permuted by a logistic map before it is embedded into the host image. In addition, the embedding positions are stored beforehand and

served as a key matrix to extract the watermark in detection process. In other words, the proposed watermarking method is semi-blind. Compared with other fragile watermarking methods, the proposed scheme not only has much lower watermark payloads, but also can detect and locate the tampered regions accurately.

The remainder of this paper is organized as follows. Section 2 makes a brief explanation for LBP operator and logistic map. In Section 3, the proposed algorithm is described which includes watermark embedding process and tamper detection process. Experimental results and analysis are illustrated in Section 4. Section 5 concludes the paper.

2. LBP Operator and Logistic Map

2.1 LBP Operator

The LBP operator was first proposed by Ojala et al. [13] and conventionally used as a kind of texture descriptor. It describes the spatial relationship between a central pixel value and its neighborhood pixel values, and this relationship is represented by a set of binary numbers. In terms of this good property, the LBP operator has been widely applied in texture analysis [14] and face recognition [15]. The LBP operator is defined as a circular symmetric model with radius r, and the total numbers of involved neighborhood pixels are denoted as p. The relation between r and p can be expressed as:

$$p = (2r+1)^2 - 1 . \tag{1}$$

The neighborhood pixels are firstly labeled by the local contrast between the central pixel value and neighborhood pixel values. If the value of neighborhood pixel is larger than that of the pixel in the center, the corresponding position is assigned to 1. Otherwise, it will be assigned to 0. Then we get a binary pattern of the image block. After binary-to-decimal conversion, the LBP value of the central pixel is obtained, which is utilized to reflect the texture information of local region. Considering a circular symmetric neighborhood (p, r), this process can be defined as:

$$LBP_{(p,r)} = \sum_{i=1}^{i=p} 2^i \times S(g_i - g_c), \tag{2}$$

$$S(g_i - g_c) = \begin{cases} 1, & g_i - g_c \geq 0 \\ 0, & \text{otherwise} \end{cases}, \tag{3}$$

where g_i $(i = 1,2,\cdots,p)$ is the gray value of neighborhood pixel, g_c is the gray value of central pixel, and $S(\cdot)$ is a threshold function.

The LBP pattern can represent the local texture information of an image effectively. Therefore, it has been widely concerned in digital watermarking for image tamper detection in recent years [9,10]. In this article, we use LBP operator to generate the feature information for image authentication.

2.2 Logistic Map

The logistic map is a typical chaotic map which is often utilized in information hiding. The general logistic map can be expressed as:

$$x_{n+1} = \mu(1 - x_n)x_n, \tag{4}$$

where μ is a positive constant called control parameter, and x_{n+1} is the next state of x_n ranging from 0 to 1. Here, $n \in \boldsymbol{N}$ is a nonnegative integer. The logistic map could reach to a chaotic pattern under the condition that $3.5699456 < \mu < 4$. Besides, the initial condition plays a significant role in logistic map. For different parameter μ and initial value x_0, the logistic map is statistically unrelated. Therefore, the initial condition (μ, x_0) is usually adopted as the secret key in watermarking scheme to increase the safety of watermark.

3. The Proposed Watermarking Scheme

In this section, we describe the proposed watermarking algorithm based on LBP and DWT, which includes two main stages: watermark embedding and tamper detection. The concrete steps are presented as follows.

3.1 Watermark Embedding

Fig. 1 illustrates the block diagram of watermark embedding, which includes the following steps:

Step 1. Since the authentication information is inserted into the LSBs of original image, the LSBs of host image are firstly set to 0.

Step 2. The processed image is then decomposed by Haar wavelet transform and the approximation coefficients LL_1 are used to generate the original authentication watermark $\boldsymbol{W}_0$.

Step 3. A series of non-overlapping sub-blocks with size of 3×3 are obtained by partitioning the approximation wavelet coefficients. Then the LBP operator is performed on each block to form a binary LBP pattern.

Due to the good multi-resolution characteristic of wavelet transform, the LBP pattern of LL_1 can reflect the texture feature of original image effectively with less data volume. Fig. 2 illustrates the process of watermark generation, where g_i $(i = 1, 2, \cdots, 8)$ denotes the gray value of neighborhood pixel, g_c is the central pixel value, w_i $(i = 1, 2, \cdots, 8)$ denotes the binary pattern obtained by LBP operator, and w_c is calculated by the exclusive-or operation among w_i. After Step 3, the approximation wavelet coefficients are all assigned to 0 or 1, which will be served as the original watermark.

Step 4. To encrypt the watermark, a pseudo-random sequence is produced by the logistic map with secret keys μ and x_0. Then the values in this sequence are rounded to the nearest integers and reshaped into a chaotic image. By using exclusive-or operation ($\oplus$ in Fig. 1) between the original watermark and chaotic image, an encrypted watermark $\boldsymbol{W}_e$ is formed, whose size is one-quarter of the original image.

Step 5. To select watermark embedding positions, the host image is firstly partitioned into non-overlapping blocks with size of 2×2. The LSB of the maximum pixel value in each block is selected to insert the watermark. If there is more than one pixel with the maximum value, we choose the first one as the embedding position. In other words, only one bit is embedded in each 2×2 image block. In addition, the coordinates of the maximum value in each block are stored in a key matrix $\boldsymbol{K}$, which will be utilized to extract the watermark on the receiving side.

Step 6. After the image reconstruction, the watermark embedding process is finished and the watermarked image is obtained in the end.

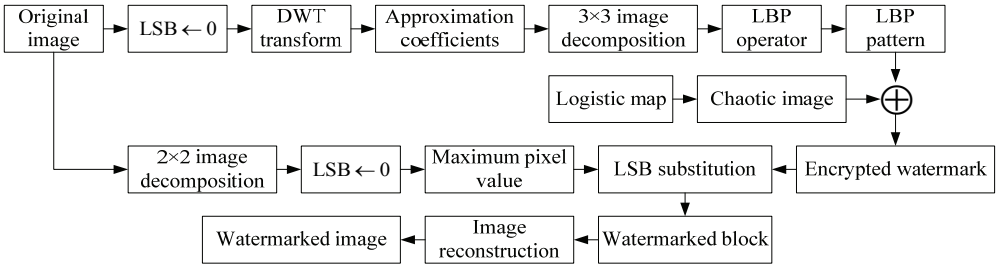


Fig. 1. Block diagram of watermark embedding.

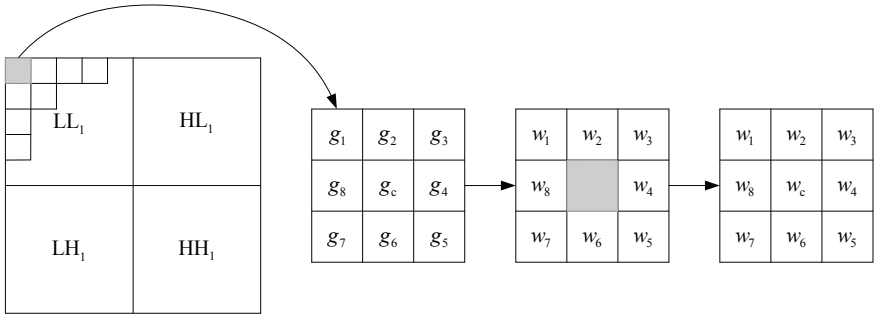


Fig. 2. Watermark generation.

3.2 Tamper Detection

The tamper detection process involves three main procedures including watermark extraction, watermark reconstruction, and tamper localization. The block diagram of tamper detection is illustrated in Fig. 3. The specific steps are as follows:

Step 1. The watermarked image or suspicious image is firstly partitioned into 2×2 non-overlapping sub-blocks. With the help of key matrix $\boldsymbol{K}$, the location of maximum pixel value in each block is determined and the watermarking bit is extracted from its LSB. Therefore, the watermark extraction process is semi-blind. We get the extracted encrypted watermark $\boldsymbol{W}_e'$, whose size is one-fourth of the image.

Step 2. To obtain the original feature watermark $\boldsymbol{W}_0'$, a chaotic image is produced by the logistic map with correct keys. Then the original watermark is recovered by the exclusive-or operation between the extracted encrypted watermark and chaotic image. We denote this process as inverse scrambling.

Step 3. By applying the first three steps in watermark embedding process, a new watermark is reconstructed which we denote as $\boldsymbol{W}_1$. As mentioned in Section 2.1, the new generated watermark is closely related to the texture of suspicious image.

Step 4. The tampered area $\boldsymbol{S}$ is determined by taking the exclusive-or operation between the extracted decrypted watermark $\boldsymbol{W}_0'$ and reconstructed watermark $\boldsymbol{W}_1$. This process can be expressed as:

$$\boldsymbol{S} = \boldsymbol{W}_0' \oplus \boldsymbol{W}_1 . \tag{5}$$

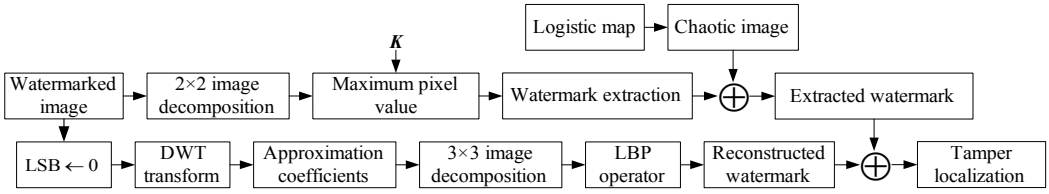


Fig. 3. Block diagram of tamper detection.

4. Experimental Results and Analysis

We test the performance of the presented watermarking scheme in terms of watermark invisibility and tamper localization ability for various attacks. In the experiment, the control parameter μ and initial state value x_0 for logistic map are set as 3.99 and 0.7654, respectively.

4.1 Watermark Invisibility

Watermark invisibility is an important assessment index in watermarking schemes, which is usually measured by the quality of watermarked image. Generally, the better the quality of watermarked image is, the better the watermark invisibility of watermarking scheme will be. Several standard test images with size of 256×256 shown in Fig. 4 are used as host images to investigate the performance of the presented algorithm in image quality.

Fig. 4. Test images: (a) Lena, (b) Clock, (c) Barbara, (d) Boat, (e) Cameraman, and (f) Airplane.

To objectively assess the image quality, the peak signal-to-noise ratio (PSNR) and structural similarity (SSIM) index [16] are adopted in this article. Generally, the larger PSNR value corresponds to the better image quality. The SSIM index is frequently adopted to assess the similarity between two images. The value of SSIM ranges from 0 to 1, where 0 means that there is no connection between two images while 1 indicates that the two images are almost the same.

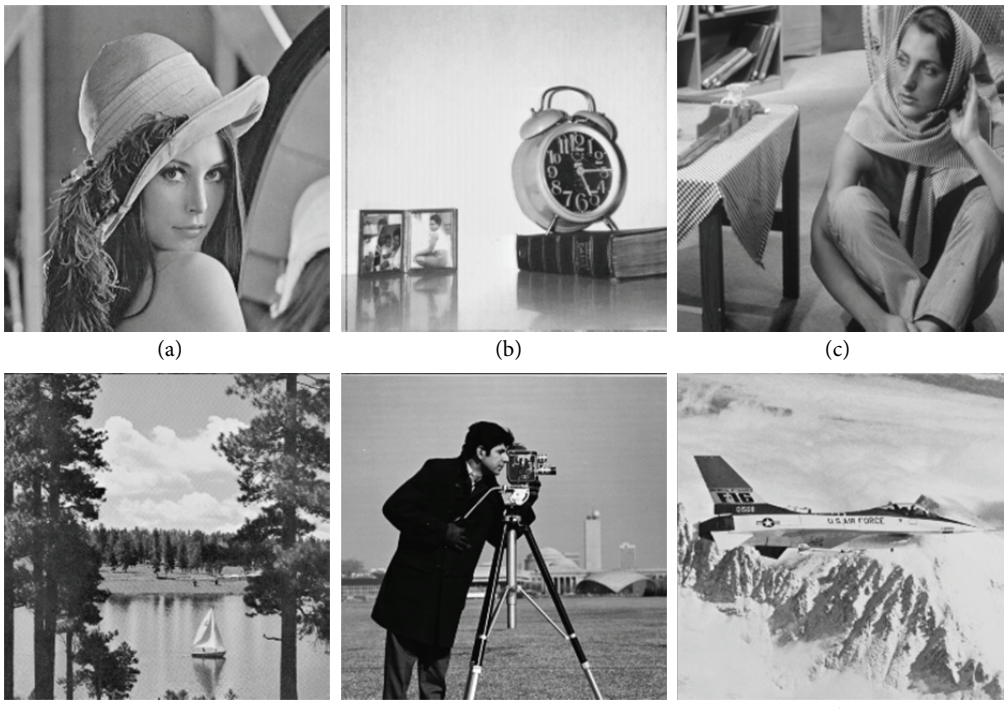
To further evaluate the effect of watermark embedding on image pixels, the percentage of distorted pixels caused by watermark embedding is revealed by a ratio called pixel error rate (PER). Its definition can be expressed as:

$$\mathrm{PER} = \frac{N_{\mathrm{error}}}{N_{\mathrm{total}}}, \tag{6}$$

where N_{error} is the number of pixels that are different from original image and N_{total} is the number of total pixels.

Fig. 5 shows the watermarked versions of test images in Fig. 4. From Fig. 5, we can see that the watermarked images have almost the same subjective quality as the host images. We cannot tell the difference between the original images and the watermarked images by our naked eyes. Table 1 lists the PSNR, SSIM, and PER values of watermarked images mentioned above. From Table 1, it is observed that the average PSNR and SSIM values of these watermarked images can reach to 57.31 dB and 0.9992, respectively, which indicates that the images after embedding is almost the same as host images. The average value of PER is 0.1207, which further suggests that the watermark makes little effect on host images. These objective evaluations prove that the proposed scheme can preserve good image quality. This good performance is closely related to the watermark embedding rule that only one LSB in each image block might be changed by plus or minus 1. Besides, only the maximum pixel value is selected to embed the watermarking bits. Generally, the image pixel with maximum value in image block represents the texture pixel, and the larger the pixel value is, the smaller the impact of watermark on host image will be. In conclusion, the proposed watermarking scheme achieves good performance in image quality with lower watermark embedding payloads.

As we know, DWT has good multi-resolution decomposition characteristic. It is identical to a hierarchical sub-band system that the approximation wavelet coefficients LL_1 can be further decomposed by DWT [17]. Therefore, we can take advantage of this property to generate fewer authentication bits and improve the PSNR of watermarked images further. This is feasible in theory because the low frequency wavelet coefficients of the next layer still contain enough information of the image. It could reconstruct the original image with much fewer amounts of data and its LBP pattern can still reflect image's texture information effectively. Taking two-level DWT for example, the watermark embedding steps are similar to those in Section 3.1. The host image is first transformed twice by DWT, and we get the second-level approximation coefficients LL_2 whose size is one-sixteenth of the host image. Then a binary authentication watermark with the same size can be obtained using LBP operator. After permutation by logistic map, the encrypted binary watermark is inserted into the LSB of the maximum pixel value in each 4×4 image block. In tamper detection, the tampered region can be determined by Eq. (5). In Table 2, different approximation coefficients obtained from different level wavelet decompositions of image Lena with size of 512×512 are adopted to generate the watermarks. From Table 2, we can see that the higher the level of DWT decomposition is, the larger the PSNR and block size will be. Besides, the PSNR and SSIM values can reach to 69.35 dB and 1, respectively. By multi-level DWT decomposition, the watermark payloads are greatly reduced and the quality of watermarked image is thus improved.



(a) (b) (c)

(d) (e) (f)

Fig. 5. Watermarked images: (a) Lena, (b) Clock, (c) Barbara, (d) Boat, (e) Cameraman, and (f) Airplane.

Table 1. PSNR, SSIM, and PER values of watermarked images

Image	PSNR (dB)	SSIM	PER
Lena	57.31	0.9993	0.1208
Clock	57.32	0.9988	0.1204
Barbara	57.31	0.9994	0.1209
Boat	57.32	0.9995	0.1205
Cameraman	57.33	0.9990	0.1202
Airplane	57.28	0.9991	0.1216
Average	57.31	0.9992	0.1207

Table 2. Quality of watermarked images generated by DWT approximation coefficients at different levels

Level	Block Size	PSNR (dB)	SSIM	PER
1	2×2	57.31	0.9998	0.1208
2	4×4	63.24	0.9999	0.0308
3	8×8	69.35	1.0000	0.0076

4.2 Performance under Various Attacks

In this subsection, several experiments are performed to test the tamper localization ability of the presented algorithm for various attacks. We select the first-level approximation coefficients LL_1 of host image with size of 256×256 to generate the watermark. The attacks used in this paper are all completed by Adobe Photoshop CS3. To diminish the effect of noise, the median filter with window size of 2×2 is

performed on detection map. The performance of the presented algorithm against different attacks is as follows.

4.2.1 Performance under copy and paste operation

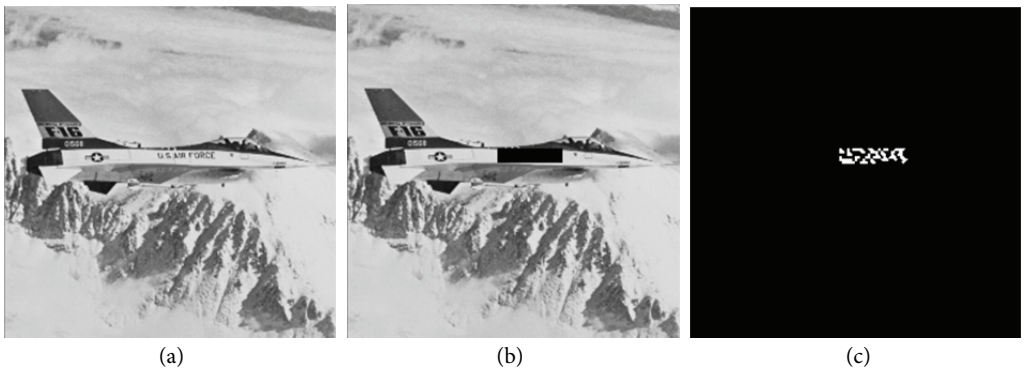
Fig. 6 shows the performance of the proposed algorithm under copy and paste operation. The boat in watermarked image Boat is copied and inserted into the same image, and the forged image is obtained which is shown in Fig. 6(b). Fig. 6(c) shows the tamper detection result. As we can see from Fig. 6(c), the tampered region could be revealed accurately in tamper localization map.

(a) (b) (c)

Fig. 6. Performance under copy and paste operation: (a) watermarked image Boat, (b) tampered image, and (c) tamper localization.

4.2.2 Performance under remove operation

In this attack, part of watermarked image is removed from the image which includes two categories given in Figs. 7 and 8, respectively. The first remove operation is shown in Fig. 7(b), in which the logo of airplane is cropped from the image directly. But it might leave some modification traces on the image. The second kind of remove operation is shown in Fig. 8(a). The logo of airplane is erased without leaving any trace. The tamper localization results of these two remove operations are illustrated in Fig. 7(c) and Fig. 8(b), respectively. From the tamper localization maps, we can see that the detection results can identify the tampered areas accurately.



(a) (b) (c)

Fig. 7. Performance under the first remove operation: (a) watermarked image Airplane, (b) tampered image, and (c) tamper localization.

(a) (b)

Fig. 8. Performance under the second remove operation: (a) tampered image and (b) tamper localization.

4.2.3 Performance under content-only attack

Fig. 9 shows the content-only attack and the corresponding tamper detection result. In content-only attack, a certain area in watermarked image is manipulated intentionally without affecting the watermarking bits in LSBs. Since the watermark in the proposed scheme is generated by the LBP pattern of LL_1, it is closely related to the content of host image. Therefore, the presented method can resist the content-only attack effectively, which can be shown in Fig. 9(c).

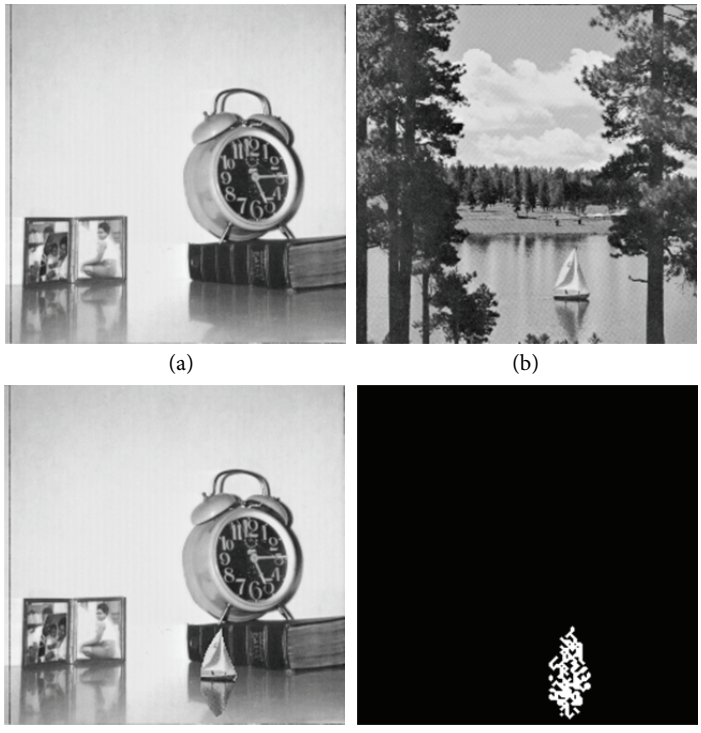
(a) (b) (c)

Fig. 9. Performance under content-only attack: (a) watermarked image Cameraman, (b) tampered image, and (c) tamper localization.

4.2.4 Performance under collage attack

Fig. 10 shows the experimental results for collage attack in which the tampered image is composed by two watermarked images. The sailboat in image Boat is copied and inserted into another watermarked image Clock. Due to the fact that collage attack could lead to sharp edges, the local frequency distribution and LBP pattern of host image will be changed. Therefore, the proposed method has good ability in resisting collage attack, which is shown in Fig. 10(d).

From the above experiments, we can get the conclusion that the presented method not only can preserve good image quality, but also can detect and locate the tampered region effectively.



(a) (b)

(c) (d)

Fig. 10. Performance under collage attack: (a) watermarked image Clock, (b) watermarked image Boat, (c) tampered image, and (d) tamper localization.

4.3 Performance Comparisons

In this subsection, we compare the proposed method with other related watermarking schemes in references [7] and [11]. Table 3 illustrates the comparisons among these three methods, where the values in the first three rows are the average PSNR, SSIM, and PER values of watermarked images in Fig. 5, respectively. By using DWT, the average PSNR value of watermarked images obtained by the proposed method has at least 6 dB improvements in comparison with the other two methods. The average values of SSIM and PER of the presented algorithm are also much better. Compared with the methods introduced by Rawat and Raman [7], only a key matrix $\boldsymbol{K}$ and two secret keys (μ and x_0) are needed in tamper detection process of the proposed scheme. In other words, the proposed scheme achieves semi-blind detection. In addition, the proposed algorithm can resist the content-only attack effectively.

Table 3. Comparisons among different watermarking methods for image authentication

Item	Rawat and Raman [7]	Benrhouma et al. [11]	The Proposed Algorithm
PSNR (dB)	51.14	51.16	57.31
SSIM	0.9967	0.9967	0.9992
PER	0.5005	0.4982	0.1207
Content-only attack	No	Yes	Yes
Collage attack	No	Yes	Yes
Tamper detection	Non-blind	Blind	Semi-blind

To further evaluate the tamper detection ability of the presented algorithm, the false positive rate (FPR) and false negative rate (FNR) [18] are applied in this paper. The FPR reflects the ratio of authentic pixels that are determined as tampered pixels improperly, while the FNR denotes the ratio of tampered pixels that are falsely determined as authentic pixels. In general, an image authentication algorithm with lower FPR and FNR values has better tamper detection accuracy. Since the watermarking method in [7] is not blind in tamper detection, the original watermark is needed on the receiving side, which is not practical in some cases. Therefore, we only compare the proposed algorithm with Benrhouma et al.'s method [11] in FPR and FNR. Table 4 lists the FPR and FNR values of the above two methods under different cropping sizes. From Table 4, we can see that the proposed method has lower FPR and FNR values than the method in [11]. In conclusion, compared with other algorithms, the proposed scheme achieves greater success in tamper detection by using much lower watermark payloads.

Table 4. FPR and FNR comparisons under different cropping sizes

Algorithm	Index	32×32	64×64	96×96	128×128	160×160
Benrhouma et al. [11]	FPR	0	0.0044	0.0409	0.1015	0.1801
	FNR	0.4189	0.3899	0.3943	0.3757	0.3657
The proposed algorithm	FPR	0	0	0	0	0.0053
	FNR	0.3555	0.3535	0.3568	0.3574	0.3689

5. Conclusion

A fragile watermarking method based on LBP and DWT is presented in this paper. The binary watermark is obtained by applying LBP operator to the wavelet approximation coefficients. To ensure the security of the proposed algorithm, the logistic map is utilized to encrypt the watermark. Then the encrypted watermark is inserted into the LSB of the maximum pixel value in each image block. In addition, the locations of the maximum pixel values are stored in a key matrix and used to extract watermark on the receiving side. Therefore, the proposed watermarking algorithm achieves semi-blind detection. The tampered region is determined by comparing the extracted watermark with the reconstructed watermark. From experimental results, we can see that the watermarked images obtained by the presented algorithm have higher image quality than other methods. Since the LBP pattern can well represent the local texture information, the proposed method achieves good tamper detection results. It can resist various attacks and locate the tampered regions accurately with lower watermark payloads. We also study the quality of different watermarked images where the watermarks are generated by approximation coefficients at different levels.

Due to the limitation of conventional LBP operator, the proposed algorithm cannot detect tampered regions at image edges. In the future work, we will address this problem and further improve the tamper localization ability for small regions. In addition, we will research the watermarking scheme with recovery ability.

Acknowledgement

This work was supported by the National Natural Science Foundation of China (No. 61702303, No.

61201371); the Natural Science Foundation of Shandong Province, China (No. ZR2017MF020, No. ZR2015PF004); and the Research Award Fund for Outstanding Young and Middle-Aged Scientists of Shandong Province, China (No. BS2013DX022).

References

[1] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data: A state-of-the-art overview," *IEEE Signal Processing Magazine*, vol. 17, no. 5, pp. 20-46, 2000.

[2] H. Nyeem, W. Boles, and C. Boyd, "Digital image watermarking: Its formal model, fundamental properties and possible attacks," *EURASIP Journal on Advances in Signal Processing*, vol. 2014, no. 1, pp. 1-22, 2014.

[3] T. Hai, C. M. Li, J. M. Zain, and A. N. Abdalla, "Robust image watermarking theories and techniques: A review," *Journal of Applied Research and Technology*, vol. 12, no. 1, pp. 122-138, 2014.

[4] K. Sreenivas and V. K. Prasad, "Fragile watermarking schemes for image authentication: A survey," *International Journal of Machine Learning and Cybernetics*, pp. 1-26, 2017. https://doi.org/10.1007/s13042-017-0641-4

[5] S. Walton, "Information authentication for a slippery new age," *Dr. Dobb's Journal*, vol. 20, no. 4, pp. 18-26, 1995.

[6] S. H. Liu, H. X, Yao, W. Gao, and Y. L. Liu, "An image fragile watermark scheme based on chaotic image pattern and pixel-pairs," *Applied Mathematics and Computation*, vol. 185, no. 2, pp. 869-882, 2007.

[7] S. Rawat and B. Raman, "A chaotic system based fragile watermarking scheme for image tamper detection," *AEU - International Journal of Electronics and Communications*, vol. 65, no. 10, pp. 840-847, 2011.

[8] L. Teng, X. Y. Wang, and X. K. Wang, "Cryptanalysis and improvement of a chaotic system based fragile watermarking scheme," *AEU - International Journal of Electronics and Communications*, vol. 67, no. 6, pp. 540-547, 2013.

[9] W. Y. Zhang and F. Y. Shih, "Semi-fragile spatial watermarking based on local binary pattern operators," *Optics Communications*, vol. 284, no. 16-17, pp. 3904-3912, 2011.

[10] J. D. Chang, B. H. Chen, and C. S. Tsai, "LBP-based fragile watermarking scheme for image tamper detection and recovery," in *Proceedings of the IEEE International Symposium on Next-Generation Electronics*, Kaohsiung, Taiwan, 2013, pp. 173-176.

[11] O. Benrhouma, H. Hermassi, A. A. A. El-Latif, and S. Belghith, "Chaotic watermark for blind forgery detection in images," *Multimedia Tools and Applications*, vol. 75, no. 14, pp. 8695-8718, 2016.

[12] R. O. Preda, "Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain," *Measurement*, vol. 46, no. 1, pp. 367-373, 2013.

[13] T. Ojala, M. Pietikainen, and D. Harwood, "A comparative study of texture measures with classification based on feature distributions," *Pattern Recognition*, vol. 29, no. 1, pp. 51-59, 1996.

[14] Z. P. Dan, Y. F. Chen, Z. Yang, and G. Wu, "An improved local binary pattern for texture classification," *Optik*, vol. 125, no. 20, pp. 6320-6324, 2014.

[15] B. Yang and S. C. Chen, "A comparative study on local binary pattern (LBP) based face recognition: LBP histogram versus LBP image," *Neurocomputing*, vol. 120, pp. 365-379, 2013.

[16] H. Shi, X. H. Wang, M. C. Li, J. Bai, and B. Feng, "Secure variable-capacity self-recovery watermarking scheme," *Multimedia Tools and Applications*, vol. 76, no. 5, pp. 6941-6972, 2017.

[17] G. Bhatnagar and B. Raman, "A new robust reference watermarking scheme based on DWT-SVD," *Computer Standards and Interfaces*, vol. 31, no. 5, pp. 1002-1013, 2009.

[18] H. Zhang, C. Y. Wang, and X. Zhou, "Fragile watermarking for image authentication using the characteristic of SVD," *Algorithms*, vol. 10, no. 1, article no. 27, 2017.

Chengyou Wang https://orcid.org/0000-0002-0901-2492

He received his M.E. and Ph.D. degrees in signal and information processing from Tianjin University, China, in 2007 and 2010, respectively. He is currently an associate professor and supervisor of postgraduate students at Shandong University, Weihai, China. His current research interests include image/video coding, digital watermarking, and tamper detection.

Heng Zhang https://orcid.org/0000-0003-1864-5432

He received his B.E. degree in communication engineering from Shandong University of Technology, China, in 2015. He is currently pursuing his M.E. degree in electronics and communication engineering at Shandong University, China. His current research interests include watermarking-based image authentication and tamper detection, and computer vision.

Xiao Zhou https://orcid.org/0000-0002-1331-7379

She received her M.E. degree in information and communication engineering from Inha University, Korea, in 2005; and her Ph.D. degree in information and communication engineering from Tsinghua University, China, in 2013. She is currently a lecturer and supervisor of postgraduate students at Shandong University, Weihai, China. Her current research interests include channel estimation, image communication, and image watermarking.