J Inf Process Syst, Vol.13, No.2, pp.385~399, April 2017
https://doi.org/10.3745/JIPS.03.0070

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

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Fragile Watermarking Based on LBP for Blind Tamper Detection in Images

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

Abstract

Nowadays, with the development of signal processing technique, the protection to the integrity and authenticity of images has become a topic of great concern. A blind image authentication technology with high tamper detection accuracy for different common attacks is urgently needed. In this paper, an improved fragile watermarking method based on local binary pattern (LBP) is presented for blind tamper location in images. In this method, a binary watermark is generated by LBP operator which is often utilized in face identification and texture analysis. In order to guarantee the safety of the proposed algorithm, Arnold transform and logistic map are used to scramble the authentication watermark. Then, the least significant bits (LSBs) of original pixels are substituted by the encrypted watermark. Since the authentication data is constructed from the image itself, no original image is needed in tamper detection. The LBP map of watermarked image is compared to the extracted authentication data to determine whether it is tampered or not. In comparison with other state-of-the-art schemes, various experiments prove that the proposed algorithm achieves better performance in forgery detection and location for baleful attacks.

Keywords

Fragile Watermarking, Local Binary Pattern (LBP), Least Significant Bit (LSB), Tamper Detection and Localization

1. Introduction

In today's digital era, digital images have been broadly applied in our production and lives. Images are more persuasive than words. However, due to the usage of image editing software, anyone can modify and edit digital images according to their wishes. The integrity and authenticity of digital images cannot be guaranteed. To resolve this issue, many schemes have been proposed including digital signature [1] and digital watermarking [2,3]. The authentication algorithm based on digital signature attaches a signature to the data, which is usually a hash code about the image or its characteristics. On the receiving side, the protected data is verified by comparing original signature to the extracted signature. Although, the digital signature can determine whether an image is falsified or not, it cannot locate the altered areas. In some cases, especially in court, tamper localization is needed to find where it is tampered. To overcome this problem, many authentication schemes based on digital watermark have been presented in last decades.

Manuscript received January 26, 2017; first revision February 10, 2017; accepted March 4, 2017.
Corresponding Author: Chengyou Wang (wangchengyou@sdu.edu.cn)
* School of Mechanical, Electrical and Information Engineering, Shandong University, Weihai, China (sdwhzh@mail.sdu.edu.cn, {wangchengyou, zhouxiao}@sdu.edu.cn)

According to its characteristics, digital watermarking scheme is divided into three types [4]: robust watermarking, fragile watermarking, and semi-fragile watermarking. The watermarking algorithm based on robust watermark can resist almost all the attacks, which is generally applied in copyright authentication. On the contrary, the fragile watermark is very susceptive to any modification, so it is widely utilized in image forgery detection and location. The semi-fragile watermark can survive in general image processing operations and it is also susceptive to malicious attacks. Due to this good property, the semi-fragile watermarking has attracted great attention in image authentication and recovery [5,6].

A lot of fragile watermarking algorithms for image tamper localization have been put forward recently. The most typical one for image authentication is the watermarking algorithm based on the least significant bit (LSB). The main idea of LSB-based watermarking algorithm is that the authentication information is inserted into host image by replacing one or few LSBs of original pixels [7]. Since the LSB makes little difference on original image, it has been applied broadly in watermarking for tamper localization. However, the original LSB-based embedding algorithm is not robust enough. It is vulnerable to many common image processing operations. To increase its security, a number of improved schemes based on LSB were proposed. Wong [8] presented a public-key based watermarking algorithm for image authentication. In his method, a key is applied to generate a signature. The signature contains the feature information of an original binary watermark and seven most significant bits (MSBs) of host image. Then the signature is inserted into LSBs of the corresponding sub-blocks. Chang et al. [9] presented a block-wise fragile watermarking algorithm. The authentication data of each block is acquired by applying a cryptographic hash function, and it is inserted into adaptive LSBs of the embedded pixels. To break block-wise dependency, Chen and Wang [10] proposed fuzzy c-means clustering-based algorithm to achieve image authentication. In their scheme, the image blocks are firstly clustered via fuzzy c-means clustering. Two LSBs of each pixel are used to insert authentication data. In [11], the authors presented a chaotic scrambling based fragile watermarking algorithm. A binary scrambled watermark is formed through exclusive-or operation between an original binary image such as a logo and a chaotic image produced by logistic map. In tamper detection, the tampered region is determined by absolute difference of the extracted authentication data and the initial binary image. Since it does not consider the image content during watermark embedding, this scheme cannot resist the content-based attack mentioned in [12] and [13]. To overcome this weakness, Teng et al. [13] suggested an improved fragile watermarking algorithm on the basis of a chaos system. A binary watermark is obtained by exclusive-or operation among original watermark, a chaotic map, and two MSBs planes. Unlike the method proposed by Rawat and Raman [11], the watermark is inserted into one of the lower three LSBs in terms of the chaos system, which improves the security of the algorithm further. However, as we know, the higher bit plane has greater effect on image quality. Three lower LSBs are randomly used to embed the watermark in Teng et al.'s method [13], which makes it a lower peak signal-to-noise ratio (PSNR) than the algorithm in [11]. In addition, the authentication algorithms in [11] and [13] have to send the original watermark along with the watermarked image, which exposes a serious threat to the security of watermark. To achieve blind tamper detection, Benrhouma et al. [14] presented a chaos watermark for blind falsified detection of digital images. The carrier image is first partitioned into lots of non-overlapping sub-blocks. Then a binary watermark is produced by the comparison between pixel values and its average pixel value in each block. The biggest defect of this method is that a false alarm appears all over the image blocks in tamper detection result, and the

detection accuracy needs further improvement. Zhang and Shih [15] presented a semi-fragile watermarking method based on local binary pattern (LBP). The local pixel contrast is used to complete watermark insertion and extraction. Though it achieves good performance in tamper detection, a binary watermark is necessary to determine the tampered areas.

In this article, we present an improved fragile watermarking method based on [14] for blind falsified detection in images. The most advantage of this method is that the authentication watermark of host image is built by LBP operator from image itself. It needs no original image or watermark in tamper detection. Besides, it achieves superior performance in tamper detection and location under diversified attacks such as text addition, collage attack, and content-based attack. Especially, we evaluate the performance of the presented scheme for constant average attack which is not implemented in the above schemes. Before watermark embedding, Arnold transform and logistic map are employed to fortify the security of the presented method.

The rest of this paper is organized as follows. In Section 2, mathematical preparations are given for complete and profound study of LBP, Arnold transform, and logistic map. Section 3 explains the proposed algorithm including watermark embedding, watermark extraction, and tamper detection. Experimental results and analysis are presented in Section 4. Conclusions and the future work are illustrated finally in Section 5.

2. Mathematical Preparations

2.1 Local Binary Pattern

LBP was firstly developed by Ojala et al. [16,17], which was traditionally used to describe local textural feature of an image. Although it is simple, the LBP operator is a very efficient texture feature descriptor. Due to this good property, it has been successfully used in texture analysis [18] and image forgery detection [19]. Recently, the LBP operator has got great development in digital watermarking field for image authentication [15]. The main process of generalized LBP is shown in Fig. 1. The image is firstly partitioned into lots of $m \times m$ sub-blocks, for example $m = 3$ shown in Fig. 1(a). Then the central pixel value of the sub-block is used as a threshold to label the neighbor pixels. If the neighbor pixel value is smaller than the threshold, it is set to 0. If the neighbor pixel value is greater than the threshold, it will be set to 1. Then, we get 8-bit binary numbers in clockwise direction as 10001011. By binary-decimal conversion, the decimal form of LBP is obtained which is shown in Fig. 1(b). The definition of generalized LBP can be formulated as:

$$\mathrm{LBP}(x_c, y_c) = \sum_{i=0}^{i=7} S(p_i - p_c) 2^i, \tag{1}$$

where p_c is the value in central pixel (x_c, y_c) and p_i $(i = 0,1,\cdots,7)$ refers to the value of corresponding neighbor pixel. $S(x)$ is a sign function which is defined as:

$$S(x) = \begin{cases} 1, & x \geq 0, \\ 0, & \text{otherwise}. \end{cases} \tag{2}$$

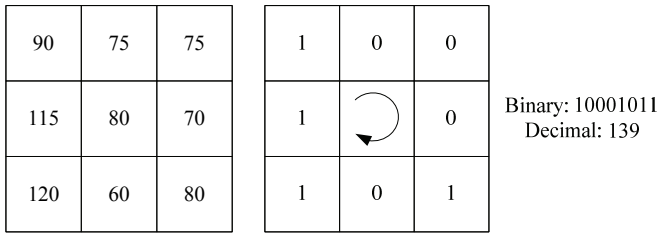


Fig. 1. Generalized LBP operator for 3×3 block: (a) original image block and (b) local binary pattern.

Since LBP is closely linked to image texture characteristic, any tampering with the image will lead to changes in LBP. Therefore, the LBP operator can be applied as an efficient tool for image tamper detection and location. In the proposed algorithm, the LBP operator is used to generate the authentication watermark from host image itself, which will help to achieve blind tamper detection.

2.2 Arnold Transform

In the proposed scheme, Arnold transform is adopted to guarantee the security of the algorithm. The generalized Arnold transform is defined as follows:

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod N, \tag{3}$$

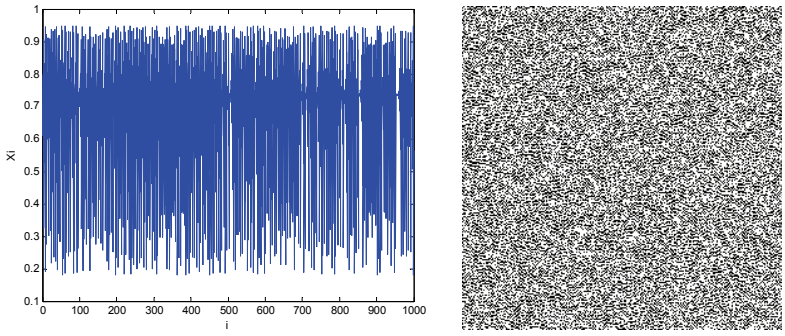
where (x_i, y_i) refers to the original position of image pixel, and (x_{i+1}, y_{i+1}) denotes the corresponding position after permutation. a and b are two control parameters, and N is the size of image. For different parameters and image sizes, Arnold transform has different period T. In other word, after a certain times scrambling, it will turn back to the original image again. By applying Arnold transform, not only the image content is encrypted, the permuted times can also be utilized as the encryption key k to enhance the security of the algorithm [20].

2.3 Logistic Map

Logistic map is another chaotic map adopted in the scheme and it is used to produce a series of random numbers. Its definition can be expressed as:

$$x_{i+1} = \mu x_i (1 - x_i), \tag{4}$$

where $0 < \mu \le 4$ is a control parameter; x_i is original value; and x_{i+1} is the corresponding value after scrambling. When the control parameter $\mu \in (3.5699456,\ 4]$, the logistic map reaches a chaotic pattern where the sequence obtained is extremely susceptive to its initial state. In other words, different initial conditions will lead to uncorrelated logistic sequences. Since all the values in the sequence belong to $[0,\ 1]$, a binary chaotic image is obtained by rounding operation and re-arranging, which will be applied in watermark encryption process. Fig. 2 shows the chaotic pattern and the binary chaotic image with size of 256×256.



(a) (b)

Fig. 2. Logistic map: (a) chaos pattern and (b) binary chaotic image.

3. The Proposed Method

We introduce an improved fragile watermarking method for blind tamper detection in this section. The processes of watermark embedding, watermark extraction, and tamper detection are described as follows.

3.1 Watermark Embedding

The block diagram of watermark embedding is illustrated in Fig. 3. A watermark $\boldsymbol{W}$ is formed by LBP operator and inserted into the carrier image $\boldsymbol{I}$ with size of $M \times M$. The detailed steps of watermark insertion are indicated below.

Step 1. To get LBP of the host image $\boldsymbol{I}$, image boundary extension is performed on $\boldsymbol{I}$. In this paper, we adopt symmetric boundary extension and denote the image after boundary extension as $\boldsymbol{I}_b$.

Step 2. Since the LSB embedding rule is applied in the proposed algorithm, the LSBs of $\boldsymbol{I}_b$ are firstly initialized to zeros. Then $\boldsymbol{I}_b$ is partitioned into a lot of non-overlapping blocks with size of $m \times m$, in this paper $m = 3$.

Step 3. For each 3×3 block, LBP operator is used to generate 8-bit binary numbers for neighbor pixels, which are served as the authentication data of the block. We denote these numbers as w_i ($i = 0, 1, \cdots, 7$), and then w_c in the location of center pixel is obtained using exclusive-or operation between w_i, which can be described as:

$$w_c = w_0 \oplus w_1 \oplus \cdots \oplus w_7. \tag{5}$$

Step 4. After all the sub-blocks are set to 1 or 0 by LBP operator, we get the authentication information of the whole image, which is a binary image. To ensure the security of authentication data, Arnold transform with an encryption key k is utilized to permute the authentication data. Then we get a scrambled binary image $\boldsymbol{B}$ which contains image texture information.

Step 5. By using the logistic map shown in Section 2.3, a binary chaotic image $\boldsymbol{C}$ with size of $M \times M$ is generated.

Step 6. To further improve the security of the proposed method, a binary chaotic watermark $\boldsymbol{W}$ is obtained via the exclusive-or operation between authentication data $\boldsymbol{B}$ and chaotic image $\boldsymbol{C}$.

Step 7. The watermark embedding process is finished by replacing the LSB plane of carrier image using $\boldsymbol{W}$. We get the watermarked image $\boldsymbol{I}_w$.

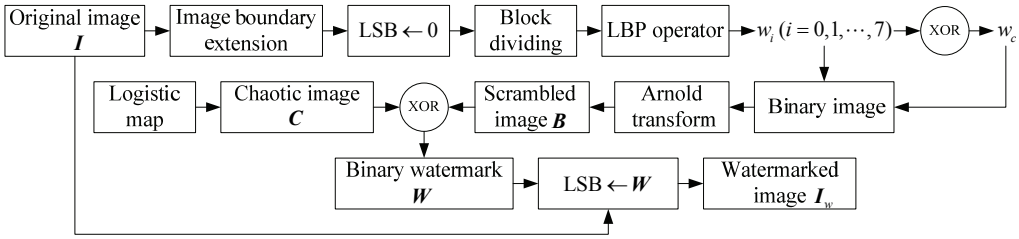


Fig. 3. Block diagram of watermark embedding.

3.2 Watermark Extraction and Tamper Detection

In the proposed algorithm, the procedure of watermark extraction is the inverse process of watermark insertion, which is illustrated in Fig. 4. Because the authentication data is constructed by LBP operator from the image itself, it achieves blindness in tamper detection. The concrete steps of watermark extraction and tamper detection are given as follows.

Step 1. Apply the first three steps in watermark embedding process to regenerate the authentication data of watermarked image. We denote the reconstructed binary image as $\boldsymbol{B}'$.

Step 2. Extract the binary chaotic watermark from the LSB plane of watermarked image, which is represented as $\boldsymbol{W}'$.

Step 3. By using the initial condition of logistic map, a binary chaotic image $\boldsymbol{C}$ used in watermark embedding process is obtained.

Step 4. By exclusive-or operation between the chaotic map $\boldsymbol{C}$ and the extracted watermark $\boldsymbol{W}'$, another binary image is produced. After inverse Arnold transform with decryption key $T-k$, the image $\boldsymbol{B}''$ is constructed, which should be the same as image $\boldsymbol{B}'$ normally.

Step 5. In order to locate the tampered region, the absolute difference between $\boldsymbol{B}'$ and $\boldsymbol{B}''$ is calculated. Then the tamper detection result $\boldsymbol{R}$ is obtained, which can be expressed as:

$$\boldsymbol{R}=\left|\boldsymbol{B}'-\boldsymbol{B}''\right|. \tag{6}$$

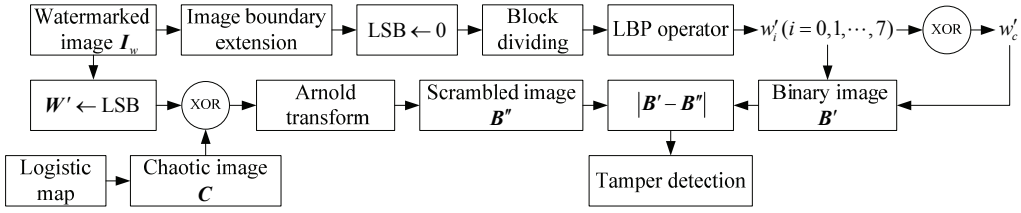


Fig. 4. Block diagram of watermark extraction and tamper detection.

4. Experimental Results and Analysis

Some experiments are conducted to assess the performance of the proposed algorithm. Many different images with size of 256×256 are adopted in this paper. The parameters of Arnold transform are $a=1$, $b=1$, and $k=75$. The control parameter of logistic map is set as $\mu=3.854$ and initial value is set as $x_0=0.654$.

4.1 Imperceptibility Evaluation

PSNR and structural similarity (SSIM) [21] are two evaluation indexes adopted in the experiment to assess the visual effect of the image after watermark embedding. Given an image with size of $M \times M$, the PSNR value is given by:

$$\mathrm{PSNR} = 10\log_{10}\frac{M \times M \times \max\left[\boldsymbol{I}(i,j)^2\right]}{\sum_{i=1}^{M}\sum_{j=1}^{M}\left[\boldsymbol{I}(i,j) - \boldsymbol{I}_w(i,j)\right]^2}(\mathrm{dB}), \tag{7}$$

where $\boldsymbol{I}(i,j)$ and $\boldsymbol{I}_w(i,j)$ are the gray values at the position (i,j) of the original image $\boldsymbol{I}$ and its watermarked version $\boldsymbol{I}_w$, respectively. Generally, a watermarked image whose PSNR is larger than 28 dB is regarded as the image in good quality. The SSIM defined by Eq. (8) is utilized to measure the comparability between the original image and its embedded version by considering the human visual system (HVS).

$$\mathrm{SSIM} = \frac{2\mu_I\mu_{I_w} + C_1}{\mu_I{}^2 + \mu_{I_w}{}^2 + C_1}\frac{2\sigma_I\sigma_{I_w} + C_2}{\sigma_I{}^2 + \sigma_{I_w}{}^2 + C_2}\frac{\sigma_{II_w} + C_3}{\sigma_I\sigma_{I_w} + C_3}, \tag{8}$$

where μ_I and μ_{I_w} are the mean values of $\boldsymbol{I}$ and $\boldsymbol{I}_w$, respectively; σ_I and σ_{I_w} are their standard deviations correspondingly; and σ_{II_w} is the covariance between these two images. C_1, C_2, and C_3 are positive parameters. The range of SSIM is between 0 and 1. Generally, the closer SSIM is to 1, the more similar two images are to each other. When SSIM is equal to 1, it means that $\boldsymbol{I}$ and $\boldsymbol{I}_w$ are exactly the same.

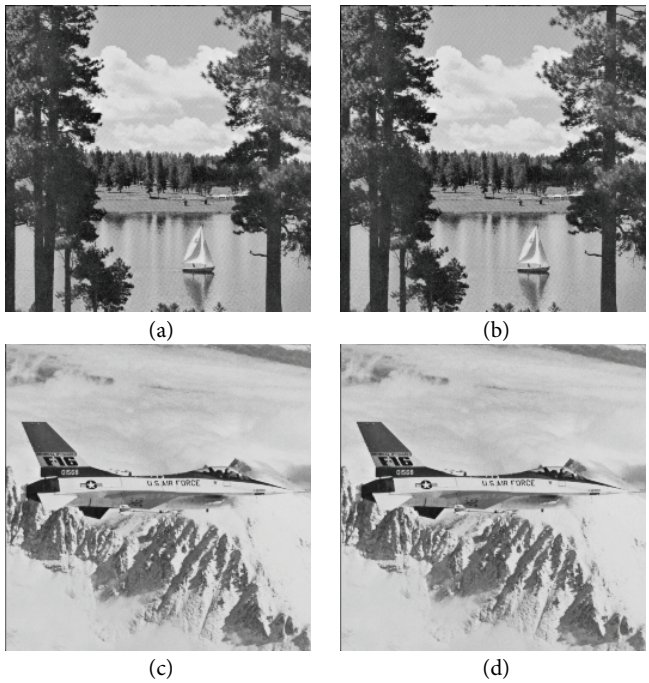


Fig. 5. Original images and its watermarked versions: (a) original image Boat, (b) watermarked image Boat, (c) original image Airplane, and (d) watermarked image Airplane.

Image Boat and image Airplane as well as their watermarked versions are given in Fig. 5, from which we can see there is no distinction between the host image and the watermarked image. It proves that the proposed watermarking algorithm has perfect invisibility. For a watermarked image with the same size, Table 1 illustrates the comparisons between the proposed algorithm and references [11,14] in terms of PSNR and SSIM. From Table 1, it proves that for the same image, the proposed method has approximate and even better PSNR and SSIM values than the method in [11]. Though the PSNR is little lower than that of Benrhouma et al.'s scheme [14], the proposed scheme has better tamper detection result, which will be illustrated in the next subsection.

Table 1. Comparisons of PSNR and SSIM among different methods

Image	Rawat and Raman [11]		Benrhouma et al. [14]		The proposed	
	PSNR (dB)	SSIM	PSNR (dB)	SSIM	PSNR (dB)	SSIM
Lena	51.1497	0.9972	51.1516	0.9971	51.1418	0.9972
Boat	51.1416	0.9978	51.1804	0.9979	51.1716	0.9979
Cameraman	51.1468	0.9959	51.1614	0.9959	51.1211	0.9959
Airplane	51.1448	0.9964	51.1355	0.9964	51.1625	0.9964
Clock	51.0986	0.9950	51.1459	0.9951	51.1320	0.9951
Average	51.1363	0.9965	51.1550	0.9965	51.1458	0.9965

4.2 Performance against Tampering

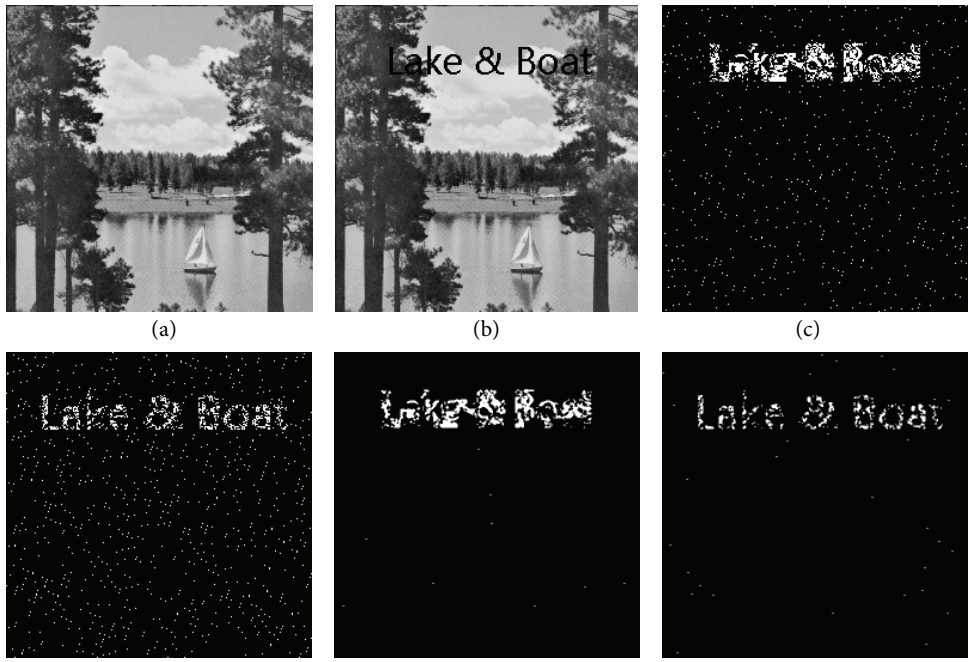
To test the tamper detection and location ability of the proposed algorithm under various attacks, some experiments are presented. The attacks used in this paper include text addition attack, copy-paste attack, object deletion attack, collage attack, content-based attack, and constant average attack.

4.2.1 Text addition attack

In text addition, the watermarked image is falsified by writing texts on it. Fig. 6 shows the tampered image and its tamper detection maps. The watermarked image Boat is manipulated with the text "Lake & Boat" on it. Fig. 6(c) and Fig. 6(d) are the location maps of Benrhouma et al.'s scheme [14] and the proposed method, respectively. Although there are some white spots both in Fig. 6(c) and Fig. 6(d), the proposed algorithm can identify and locate the added text more precisely than the method in [14]. To make better comparison, a cleaning step used in [14] is also applied in the experiments which are illustrated in Fig. 6(e) and Fig. 6(f), respectively. By the comparison of these two figures, it can be proved that the detection result of the proposed algorithm has better visual effect than that of the method in [14].

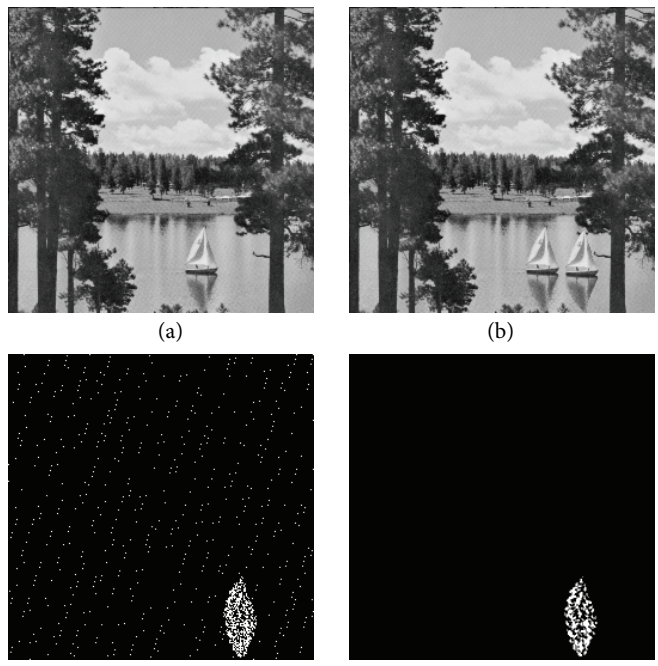
4.2.2 Copy-paste attack

In copy-paste operation, parts of an image are copied and inserted back to the watermarked image. Fig. 7 shows the watermarked image Boat, tampered image, and its tamper detection maps. The modification is so natural that it is hard to determine which image is the real image by human eyes. The tamper detection result with cleaning operation is given in Fig. 7(d). From the detection map, we can learn that the presented algorithm achieves better performance under copy-paste operation.



(a) (b) (c) (d) (e) (f)

Fig. 6. Text addition: (a) watermarked image Boat, (b) tampered image, (c) detection result in [14], (d) detection map of the proposed algorithm, (e) detection result in [14] with cleaning step, and (f) detection map of the proposed algorithm with cleaning step.

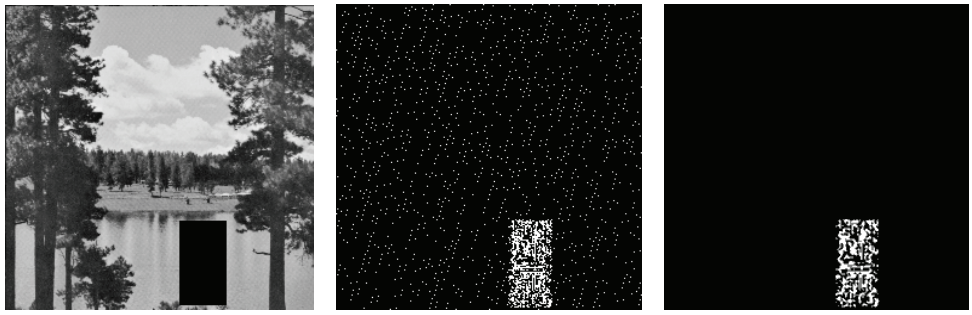


(a) (b) (c) (d)

Fig. 7. Copy-paste operation: (a) watermarked image Boat, (b) tampered image, (c) detection map, and (d) detection map with cleaning step.

4.2.3 Object deletion attack

Object deletion attack is one of the most common attacks, which can be classified into two categories. One is that a portion of the watermarked image is cropped directly; the other is that some contents of the watermarked image are deleted without impact the image visual effect. The latter attack makes it more difficult to find the suspicious region than the first one. In the experiment, the boat in watermarked image Boat is deleted by these two deletion attacks. Fig. 8 shows the first object deletion attack and its detection result. The experimental result of the second deletion attack is given in Fig. 9. From the authentication results, it is suggested that the presented algorithm can effectively resist these two kinds of object deletion attacks.



(a) (b) (c)

Fig. 8. The first kind of delete operation: (a) tampered image, (b) detection map, and (c) detection map with cleaning step.

(a) (b)

Fig. 9. The second kind of delete operation: (a) tampered image and (b) detection map with cleaning step.

4.2.4 Collage attack

Collage attack proposed by Fridrich et al. [22] forges an image by inserting parts of other watermarked images and keeps their relative spatial positions unchanged. Besides, all watermarked images used in collage attack are formed by the same watermark embedding algorithm. Fig. 10 gives an example of collage attack. In Fig. 10, the airplane is copied from watermarked image Airplane given in Fig. 10(b) and spliced into watermarked image Boat shown in Fig. 10(a). The tamper detection maps of

Benrhouma et al.'s approach [14] and the proposed algorithm are presented in Fig. 10(d) and Fig. 10(e), respectively. By comparing with these two figures, it is indicated that the presented algorithm can point out the airplane outline more precisely and effectively than Benrhouma et al.'s approach.

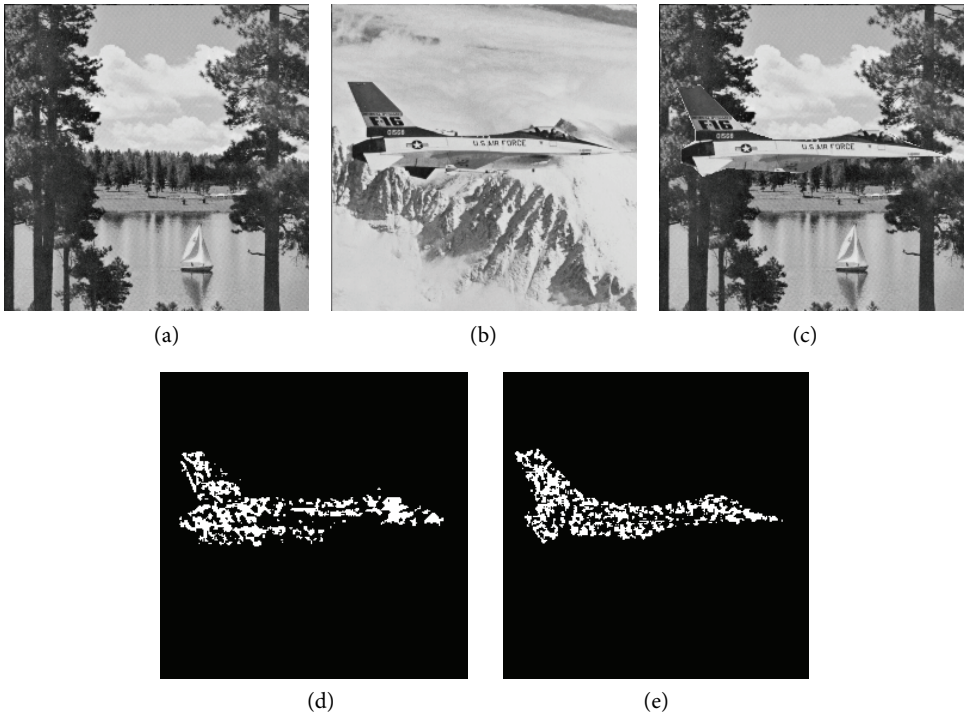


Fig. 10. Collage attack: (a) watermarked image Boat, (b) watermarked image Airplane, (c) splicing image, (d) detection result in [14], and (e) detection map of the proposed algorithm.

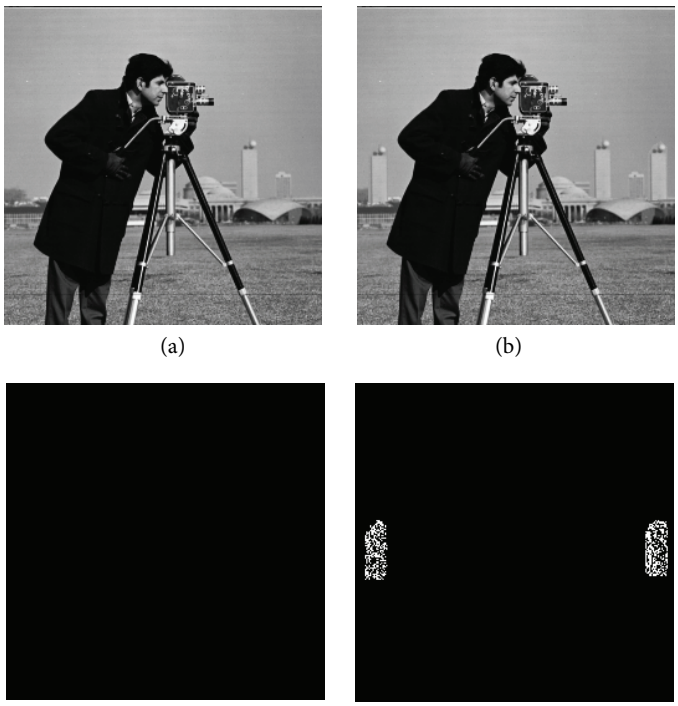
4.2.5 Content-based attack

Content-based attack is a manipulation on watermarking algorithms using LSB embedding rule. It manipulates the image content while preserving the watermark bits. For some LSB-based watermarking schemes without considering the image content during watermark embedding [11], the content-based attack is a big threat to the authenticity of watermarked image. To assess the detection ability of the proposed algorithm for content-based attack, the LSB plane of watermarked image is extracted first. Then, the rest is manipulated optionally. At last, the authentication bits are inserted back to the LSBs of tampered image. The tampered image and its detection result are presented in Fig. 11. From Fig. 11(c) and Fig. 11(d), we can get the conclusion that the watermarking scheme in [11] cannot resist the content-based attack while the proposed method avoids this limitation and achieves great success in tamper detection.

4.2.6 Constant average attack

Constant average attack proposed in [23] is a common attack against the block-based watermarking schemes [6]. In block-wise independent watermarking technique, the watermark is usually formed by average pixel values of image blocks. The main drawback of this technique is that an attacker can forge

each block with the same average intensity of that block and keep their watermarking information untouched. Since the watermark is constructed by LBP operator from the image, this problem is well solved in our method. Fig. 12 gives the authentication results of the presented algorithm and the method in [11]. In Fig. 12(a), the logo "U.S. AIR FORCE" on the watermarked image Airplane is removed via constant average attack. From the tamper detection maps given in Fig. 12(b) and Fig. 12(c), we can get that compared with [11], the proposed scheme can resist constant average attack and locate the tampered region effectively.



(a) (b)

(c) (d)

Fig. 11. Content-based attack: (a) watermarked image, (b) tampered image, (c) detection result in [11], and (d) detection map of the proposed algorithm.

(a) (b) (c)

Fig. 12. Constant average attack: (a) tampered image, (b) detection result in [11], and (c) detection map of the proposed algorithm.

From the above simulation results, we can draw the conclusion that the presented watermarking algorithm has good invisibility. Besides, it can detect various hostile attacks and locate the tampered region accurately.

5. Conclusions

In this article, an improved fragile watermarking algorithm based on LBP is proposed for blind tamper detection in images. Compared with the method proposed by Rawat and Raman [11], the watermark in our scheme is constructed by LBP operator from the host image itself. In other words, no original image is required in tamper localization. In addition, the proposed algorithm overcomes the defects existing in [11] that it cannot resist the content-based forgery and constant average attack. Since the LBP pattern of an image is closely associated with the texture information, any modification to the image will lead to changes in LBP. Therefore, the proposed scheme can identify and locate the falsified area more effectively and precisely for different common attacks than Benrhouma et al.'s approach [14] especially in text addition and collage attack. In the future research, we will further increase the accuracy of tamper detection by using improved LBP operator and research the watermarking approach for tamper detection and self-recovery.

Acknowledgement

This work was supported by the National Natural Science Foundation of China (No. 61201371), the Natural Science Foundation of Shandong Province, China (No. ZR2015PF004), and the Research Award Fund for Outstanding Young and Middle-Aged Scientists of Shandong Province, China (No. BS2013DX022).

References

[1] C. S. Lu and H. Y. M. Liao, "Structural digital signature for image authentication: an incidental distortion resistant scheme," *IEEE Transactions on Multimedia*, vol. 5, no. 2, pp. 161-173, 2003.

[2] Y. S. Singh, B. P. Devi, and K. M. Singh, "A review of different techniques on digital image watermarking scheme," *International Journal of Engineering Research*, vol. 2, no. 3, pp. 193-199, 2013.

[3] S. M. Mousavi, A. Naghsh, and S. A. R. Abu-Bakar, "Watermarking techniques used in medical images: a survey," *Journal of Digital Imaging*, vol. 27, no. 6, pp. 714-729, 2014.

[4] O. Benrhouma, H. Hermassi, and S. Belghith, "Tamper detection and self-recovery scheme by DWT watermarking," *Nonlinear Dynamics*, vol. 79, no. 3, pp. 1817-1833, 2015.

[5] H. M. Al-Otum, "Semi-fragile watermarking for grayscale image authentication and tamper detection based on an adjusted expanded-bit multiscale quantization-based technique," *Journal of Visual Communication and Image Representation*, vol. 25, no. 5, pp. 1064-1081, 2014.

[6] C. L. Li, A. H. Zhang, Z. F. Liu, L. Liao, and D. Huang, "Semi-fragile self-recoverable watermarking algorithm based on wavelet group quantization and double authentication," *Multimedia Tools and Applications*, vol. 74, no. 23, pp. 10581-10604, 2015.

[7] S. Walton, "Information authentication for a slippery new age," *Dr. Dobb's Journal*, vol. 20, no. 4, pp. 18-26, 1995.
[8] P. W. Wong, "A public key watermark for image verification and authentication," in *Proceedings of IEEE International Conference on Image Processing*, Chicago, IL, USA, 1998, pp. 455-459.
[9] C. C. Chang, Y. S. Hu, and T. C. Lu, "A watermarking-based image ownership and tampering authentication scheme," *Pattern Recognition Letters*, vol. 27, no. 5, pp. 439-446, 2006.
[10] W. C. Chen and M. S. Wang, "A fuzzy c-means clustering-based fragile watermarking scheme for image authentication," *Expert Systems with Applications*, vol. 36, no. 2, pp. 1300-1307, 2009.
[11] 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.
[12] M. Botta, D. Cavagnino, and V. Pomponiu, "A successful attack and revision of a chaotic system based fragile watermarking scheme for image tamper detection," *AEU - International Journal of Electronics and Communications*, vol. 69, no. 1, pp. 242-245, 2015.
[13] 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.
[14] 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.
[15] 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.
[16] T. Ojala, M. Pietikainen, and D. Harwood, "Performance evaluation of texture measures with classification based on Kullback discrimination of distributions," in *Proceedings of the 12th IAPR International Conference on Pattern Recognition*, Jerusalem, Israel, 1994, pp. 582-585.
[17] 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.
[18] T. Ojala, M. Pietikainen, and T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 7, pp. 971-987, 2002.
[19] Y. J. Zhang, C. L. Zhao, Y. M. Pi, S. H. Li, and S. L. Wang, "Image-splicing forgery detection based on local binary patterns of DCT coefficients," *Security and Communication Networks*, vol. 8, no. 14, pp. 2386-2395, 2015.
[20] F. F. Yang, C. Y. Wang, W. Huang, and X. Zhou, "Embedding binary image watermark in DC components of all phase discrete cosine biorthogonal transform," *International Journal of Security and Its Applications*, vol. 9, no. 10, pp. 125-136, 2015.
[21] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600-612, 2004.
[22] J. Fridrich, M. Goljan, and N. Memon, "Cryptanalysis of the Yeung-Mintzer fragile watermarking technique," *Journal of Electronic Imaging*, vol. 11, no. 2, pp. 262-274, 2002.
[23] C. C. Chang, Y. H. Fan, and W. L. Tai, "Four-scanning attack on hierarchical digital watermarking method for image tamper detection and recovery," *Pattern Recognition*, vol. 41, no. 2, pp. 654-661, 2008.

Heng Zhang http://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.

Chengyou Wang http://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 with Shandong University, Weihai, China. His current research interests include image/video coding, digital watermarking, and tamper detection.

Xiao Zhou http://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 with Shandong University, Weihai, China. Her current research interests include channel estimation, image communication, and image watermarking.