J Inf Process Syst, Vol.13, No.5, pp.1382~1396, October 2017
https://doi.org/10.3745/JIPS.02.0063

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

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

An Improved Secure Semi-fragile Watermarking Based on LBP and Arnold Transform

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

Abstract

In this paper, we analyze a recently proposed semi-fragile watermarking scheme based on local binary pattern (LBP) operators, and note that it has a fundamental flaw in the design. In this work, a binary watermark is embedded into image blocks by modifying the neighborhood pixels according to the LBP pattern. However, different image blocks might have the same LBP pattern, which can lead to false detection in watermark extraction process. In other words, one can modify the host image intentionally without affecting its watermark message. In addition, there is no encryption process before watermark embedding, which brings another potential security problem. To illustrate its weakness, two special copy-paste attacks are proposed in this paper, and several experiments are conducted to prove the effectiveness of these attacks. To solve these problems, an improved semi-fragile watermarking based on LBP operators is presented. In watermark embedding process, the central pixel value of each block is taken into account and Arnold transform is adopted to guarantee the security of watermark. Experimental results show that the improved watermarking scheme can overcome the above defects and locate the tampered region effectively.

Keywords

Digital Image Watermarking, Semi-fragile Watermarking, False Detection, Local Binary Pattern (LBP), Arnold Transform

1. Introduction

With the widespread utilization of digital technology, digital media (particularly digital images) has come to play a significant role in daily lives. However, the increasing use of image and video editing tools brings about a serious threat. Copyrights and the content of digital media are being severely destroyed. As an effective way of addressing this problem, digital watermarking scheme has emerged at a historic moment. Generally, digital watermarks can be classified into three categories including robust watermarks, fragile watermarks, and semi-fragile watermarks [1]. As the name implies, robust watermarks are robust against general image processing operations and malicious attacks. Due to this property, robust watermarks are widely used in copyright protection [2]. On the contrary, fragile watermarks are susceptible to any modification, which are typically applied in image content authentication [3]. Semi-fragile watermarks exploit the advantages of the above two watermarks. It is immune to general image processing operations and sensitive to malicious attacks. Therefore, semi-fragile watermarks have

Manuscript received October 24, 2016; revised December 29, 2016; accepted January 28, 2017; onlinefirst July 20, 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)

received more attention from researchers.

Moreover, spatial domain and frequency domain are two embedding domains used in watermarking scheme. In spatial-domain watermarking, watermark message is inserted into image by altering the pixel values directly [4,5]. In frequency-domain watermarking, watermark message is embedded by modulating the transformation coefficients. The commonly used transforms include discrete cosine transform (DCT) [6,7], discrete Fourier transform (DFT) [8], and singular value decomposition (SVD) [9,10]. Compared to the latter, the spatial-domain watermarking is more susceptible to image modifications, which is generally applied in fragile watermarking and semi-fragile watermarking.

In the last few years, a large number of semi-fragile watermarking schemes have been presented for image authentication [11]. In [12], Zhang and Shih proposed a novel semi-fragile watermarking scheme based on the local binary pattern (LBP). To the best of our knowledge, this is the first time that the LBP operator has been introduced into the watermarking scheme. According to the exclusive-or (XOR) value of LBP in each block, a binary watermark is embedded into the host image by adjusting pixel values in the neighborhood. Although this scheme is computationally straightforward and can locate the tampered region to a certain extent, it suffers from a major flaw that different image blocks might have the same LBP pattern, which will result in detection errors during watermark extraction. In this paper, two kinds of malicious attacks are presented to demonstrate that this watermarking scheme is less secure and cannot be used for ownership protection and tamper detection. To address this problem, a secure semi-fragile watermarking algorithm is presented. A new reference value is calculated by combining the LBP sequence and central pixel value in each block. Besides, an encryption method called Arnold transform is utilized to improve the watermark's security.

The organization of this paper is as follows. In Section 2, the main procedures of LBP-based semi-fragile watermarking are briefly described. In Section 3, we analyze the weakness of this semi-fragile watermarking scheme. The proposed secure LBP-based watermarking is presented in Section 4. Experimental results and analysis are documented in Section 5. The conclusions are given finally in Section 6.

2. Semi-fragile Watermarking Based on LBP Operators

2.1 LBP Operator

The LBP operator is a simple texture descriptor that was first proposed by Ojala et al. in [13]. It reflects the local contrast between central pixel value and its neighborhood pixel values, and this spatial relationship is finally described in a binary pattern. With continuous improvements to the LBP algorithm, many improved LBP operators have been proposed, such as uniform LBP and rotation invariant LBP. The definition of LBP operator is based on a circularly symmetric model. Given a radius *r*, a circularly symmetric neighborhood *p* can be determined by:

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

For a local region $(p,\ r)$, the LBP pattern of central pixel is defined as:

$$LBP(x_c,\ y_c) = \sum_{i=0}^{p-1} 2^i \times S(g_i - g_c) , \tag{2}$$

where g_c is the pixel value in central pixel (x_c, y_c) and g_i $(i = 0,1,\cdots,p-1)$ refers to the pixel value in the neighborhood. $S(x)$ is a sign function given as:

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

Due to its property of texture description, the LBP pattern has been extensively used in face recognition [14] and tamper detection [15]. In [12], the authors introduced LBP operator into watermarking scheme. Since then, many LBP-based digital watermarking algorithms have been put forward [16,17]. To better understand the LBP pattern and reveal the errors in [12], Fig. 1 shows the original LBP operator used in [12], where $r = 1$ and $p = 8$.

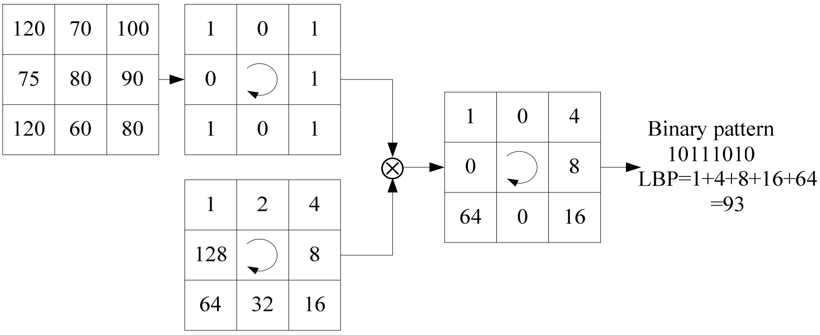


Fig. 1. Original LBP operator used in semi-fragile watermarking [12].

2.2 LBP-Based Semi-fragile Watermarking

In this subsection, we briefly summarize the main process of the semi-fragile watermarking proposed in [12]. The concrete steps are as follows.

Step 1. According to the given r, the host image is first segmented into many (p, r) local region blocks.

Step 2. Calculate the difference between the central pixel value g_c and neighborhood pixel values g_i $(i = 0,1,\cdots,p-1)$ in the (p, r) local region, and denote them as $\boldsymbol{m}_p = \{m_0, m_1, \cdots, m_{p-1}\}$. Perform LBP operator on each block, and then a binary sequence $\boldsymbol{s}_p = \{s_0, s_1, \cdots, s_{p-1}\}$ is generated.

Step 3. Compute the value $f_{\oplus}(\boldsymbol{s}_p)$ by XOR operation, which can be expressed as:

$$f_{\oplus}(\boldsymbol{s}_p) = s_0 \oplus s_1 \oplus \cdots \oplus s_{p-1}, \tag{4}$$

where $\oplus$ is the XOR operation.

Step 4. For each image block, if the value of $f_{\oplus}(\boldsymbol{s}_p)$ is equal to watermark bit w, the neighborhood pixel values remain unchanged; if the value of $f_{\oplus}(\boldsymbol{s}_p)$ is different from watermark bit w, one of the neighborhood pixel values is modified to make $f_{\oplus}(\boldsymbol{s}_p)$ consistent with w. This process can be derived as:

$$\begin{aligned}
&\text{if } (w=1 \text{ and } f_{\oplus}(\boldsymbol{s}_p)=0) \text{ or } (w=0 \text{ and } f_{\oplus}(\boldsymbol{s}_p)=1)\\
&\text{then } \{\text{select } m_i=\min(\boldsymbol{m}_p);\\
&\text{if } (s_i=1) \text{ then } g_i=(g_i-m_i)\times(1-\beta);\\
&\qquad\qquad \text{else } g_i=(g_i+m_i)\times(1+\beta)\},
\end{aligned} \tag{5}$$

where β represents the watermarking intensity factor. A larger value of β indicates better robustness and worse image quality at the same time.

On the receiving end, the watermark is extracted from watermarked image by judging the value of $f_{\oplus}(\boldsymbol{s}_p)$, which can be defined as:

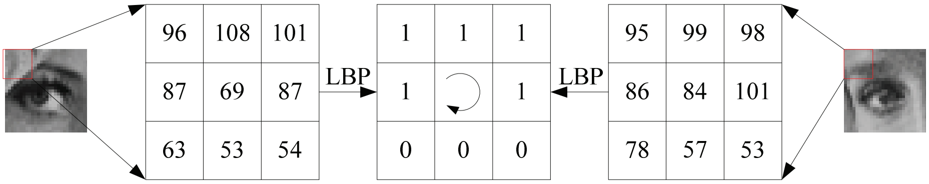
$$\text{if } f_{\oplus}(\boldsymbol{s}_p)=1 \text{ then } w=1; \text{ else } w=0\ . \tag{6}$$

3. False Detection in LBP-Based Watermarking

In this section, the limitation of LBP operator is firstly analyzed. Then we propose two successful copy-paste attacks to tamper the watermarked images, which will not be detected by the LBP-based semi-fragile watermarking in [12]. The original watermark can still be extracted integrally, which proves that this scheme has a fundamental flaw in watermark extraction process.

3.1 The Defect of LBP Operator

Although the LBP operator has got broad application, there is nevertheless a major defect that different image blocks might have the identical LBP pattern. Fig. 2 gives an example where the same LBP pattern could be generated for two completely different image blocks. This occurs because LBP pattern is obtained by the local contrast between two pixels. If the relative size between the central pixel value and neighborhood pixel values is invariant, the LBP pattern will not be changed regardless of how the image block is modified.



96	108	101
87	69	87
63	53	54

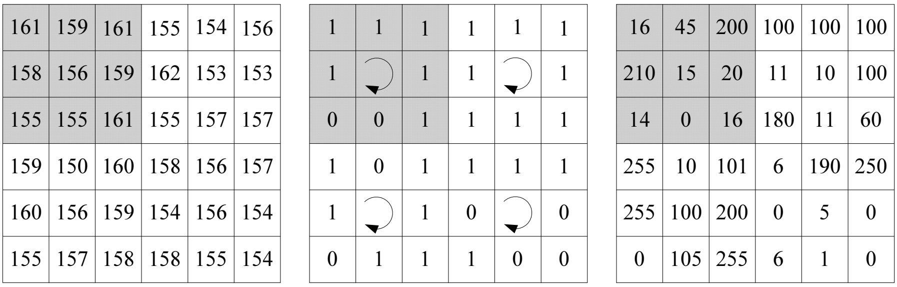
1	1	1
1		1
0	0	0

95	99	98
86	84	101
78	57	53

Fig. 2. Same LBP pattern for completely different image blocks.

3.2 Analysis of LBP-Based Semi-fragile Watermarking

In Zhang and Shih's method [12], the value after XOR operation, $f_{\oplus}(\boldsymbol{s}_p)$, plays an important role in watermark embedding and extraction processes. According to the above analysis, it is possible to acquire two identical $f_{\oplus}(\boldsymbol{s}_p)$ from different image blocks. Therefore, if we use an arbitrary matrix with the same LBP pattern to replace the objective block, the watermark bit can still be extracted according to Eq. (6), which leads to a detection error. Taking a 6×6 sub-image for example, Fig. 3 illustrates the process of manipulation, in which the original watermarked image blocks are replaced by some arbitrary matrices. From Fig. 3, we can observe that the arbitrary image forgery could be achieved as long as the LBP pattern is kept unchanged.



161	159	161	155	154	156
158	156	159	162	153	153
155	155	161	155	157	157
159	150	160	158	156	157
160	156	159	154	156	154
155	157	158	158	155	154

(a)

1	1	1	1	1	1
1	↻	1	1	↻	1
0	0	1	1	1	1
1	0	1	1	1	1
1	↻	1	0	↻	0
0	1	1	1	0	0

(b)

16	45	200	100	100	100
210	15	20	11	10	100
14	0	16	180	11	60
255	10	101	6	190	250
255	100	200	0	5	0
0	105	255	6	1	0

(c)

Fig. 3. Image forgery by arbitrary matrices: (a) original watermarked image blocks, (b) binary pattern obtained by LBP operator, and (c) tampered blocks according to (b).

In fact, only the value of $f_{\oplus}(\boldsymbol{s}_p)$ is used in watermark extraction. Therefore, it is unnecessary to make all the LBP values the same as those of original watermarked image blocks. We simply need to ensure that the replacement blocks have the same value of $f_{\oplus}(\boldsymbol{s}_p)$ as the objective image blocks. From this perspective, this attack can be regarded as a special copy-paste attack. It is generally known that there are two kinds of copy-paste attacks. In the first type, the tampered image blocks are copied from the host image itself. In the second type, the tampered image blocks are from other images.

Fig. 4 depicts the block diagram of the first copy-paste attack, which is finished in the same watermarked image. The detailed process can be described as follows.

Step 1. Divide the watermarked image into many $(p,\ r)$ local region blocks and determine the blocks that we want to tamper.

Step 2. Generate the binary sequence based on LBP operator, and calculate $f_{\oplus}(\boldsymbol{s}_p)$ according to Eq. (4).

Step 3. Select an initial image block randomly from the remaining image blocks, and compute $f_{\oplus}{}'(\boldsymbol{s}'_p)$. If the value of $f_{\oplus}{}'(\boldsymbol{s}'_p)$ is equal to $f_{\oplus}(\boldsymbol{s}_p)$, we use this block to replace the original image block determined previously. Otherwise, we keep searching until all the blocks in the tampered region are substituted by other blocks in the image.

The second type of copy-paste attack is shown in Fig. 5, in which the star logo on the image Airplane is replaced by the flower on the head of image Lena. Like the first copy-paste attack, $f_{\oplus}(\boldsymbol{s}_p)$ and $f_{\oplus}{}'(\boldsymbol{s}'_p)$ are first calculated and judged. If the value of $f_{\oplus}(\boldsymbol{s}_p)$ is identical with $f_{\oplus}{}'(\boldsymbol{s}'_p)$, the original image block will be replaced directly by the tampered block. Otherwise, minor adjustment is needed for the tampered block before it is pasted on the host image. Since the value of $f_{\oplus}(\boldsymbol{s}_p)$ is either 1 or 0, this adjustment is completed by modifying only one of the neighborhood pixels in tampered image block. Generally, modification to one pixel will not affect the image block too much. To maintain the visual quality of tampered image, the pixel which has the minimum difference with central pixel is adjusted to make $f_{\oplus}'(\boldsymbol{s}_p')$ equal to $f_{\oplus}(\boldsymbol{s}_p)$.

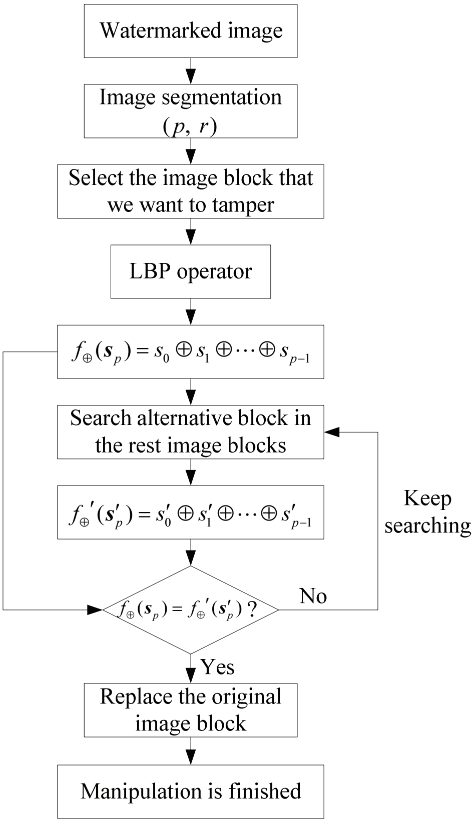

Watermarked image
Image segmentation (p, r)
Select the image block that we want to tamper
LBP operator
$f_{\oplus}(\boldsymbol{s}_p) = s_0 \oplus s_1 \oplus \cdots \oplus s_{p-1}$
Search alternative block in the rest image blocks
$f_{\oplus}'(\boldsymbol{s}_p') = s_0' \oplus s_1' \oplus \cdots \oplus s_{p-1}'$
Keep searching
$f_{\oplus}(\boldsymbol{s}_p) = f_{\oplus}'(\boldsymbol{s}_p')$?
No
Yes
Replace the original image block
Manipulation is finished

Fig. 4. The first type of copy-paste attack.

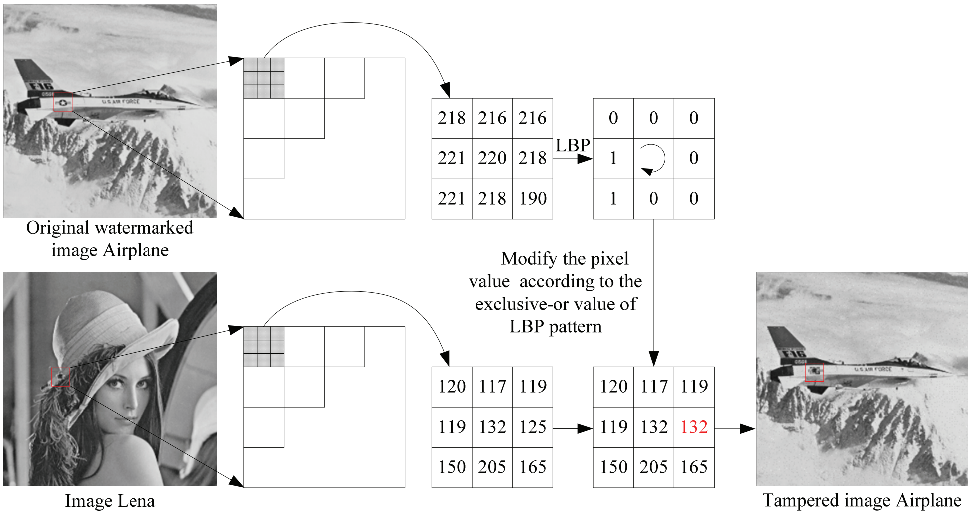
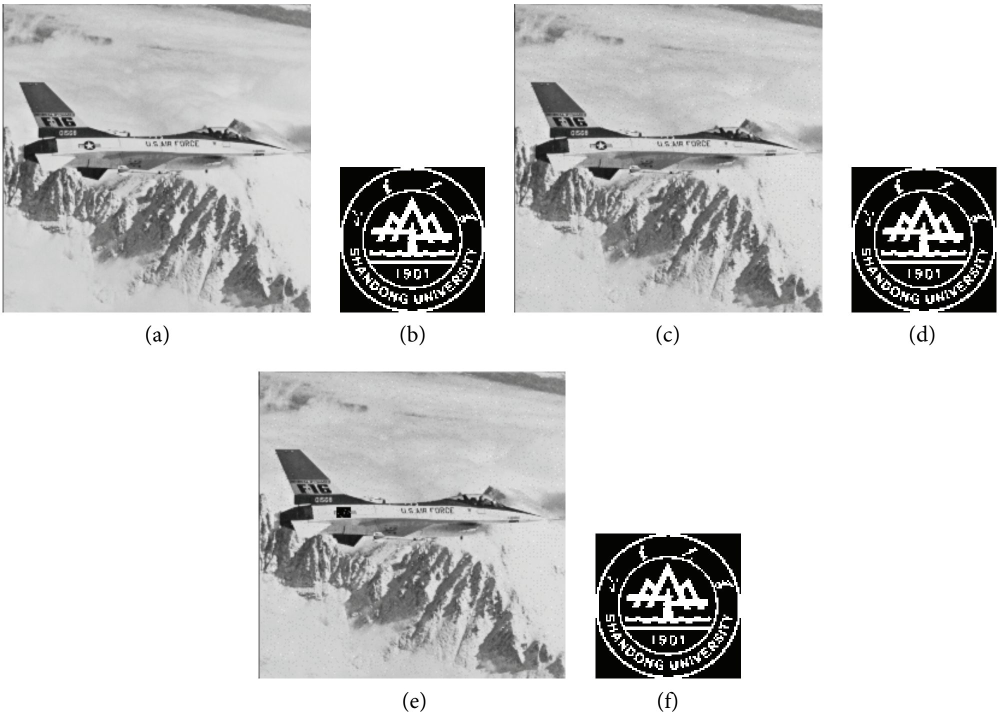


Fig. 5. The second type of copy-paste attack.

To investigate the effectiveness of the proposed attacks, several experiments are carried out. Image Airplane with size of 256×256 is adopted as host image, and the logo of Shandong University is served as binary watermark. The general LBP operator described in Section 2 is used to generate the LBP binary sequence. Fig. 6 shows the experimental results, where the star logo on the airplane is deleted by using arbitrary matrices. The normalized correlation (NC) given in Eq. (7) is used to objectively evaluate the similarity between the original watermark and extracted watermark. If the NC value is equal to 1, it manifests that these two watermarks are exactly the same.

$$\mathrm{NC}=\frac{\sum_{i=1}^{M}\sum_{j=1}^{M}[\boldsymbol{W}(i,j)\boldsymbol{W}^{*}(i,j)]}{\sum_{i=1}^{M}\sum_{j=1}^{M}[\boldsymbol{W}(i,j)]^{2}}, \tag{7}$$

where $\boldsymbol{W}$ and $\boldsymbol{W}^{*}$ are the original watermark and extracted watermark, respectively. M is the length and width of the watermark. From Fig. 6(d) and Fig. 6(f), we can see that the watermark can be extracted without any distortion. Furthermore, the NC value is equal to 1, which also indicates that the extracted watermark is the same as original watermark objectively. Therefore, the watermarking scheme proposed by Zhang and Shih [12] loses its effectiveness in detecting this attack.



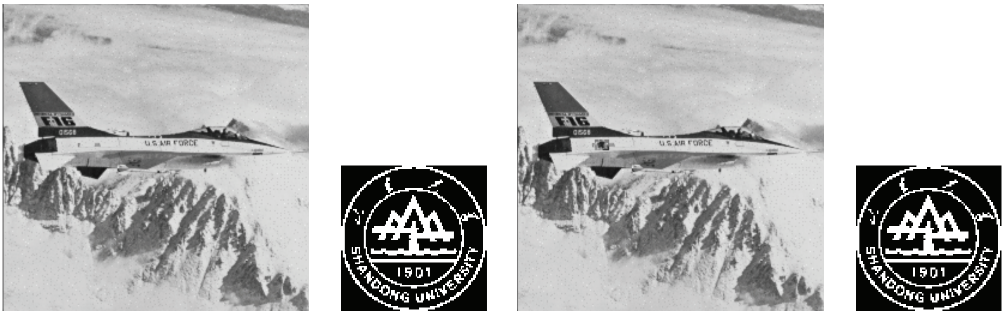
(a) (b) (c) (d)

(e) (f)

Fig. 6. Image forgery using arbitrary matrices: (a) original image Airplane, (b) original watermark, (c) watermarked image Airplane generated by LBP-based semi-fragile watermarking, (d) extracted watermark without attacks, (e) watermarked image forged by arbitrary matrices, and (f) extracted watermark from (e).

Fig. 7 reveals the watermark false detection problem under the two special copy-paste attacks mentioned above. In Fig. 7(a), the star logo is erased without leaving any trace. Fig. 7(c) shows the second type of copy-paste attack obtained by Fig. 5. Based on the extracted watermarks shown in Fig. 7(b) and Fig. 7(d), it is suggested that both these two attacks can survive the tamper detection introduced in [12].

From the above analysis, we can learn that the LBP-based semi-fragile watermarking presented by Zhang and Shih [12] has a flaw in tamper detection. Besides, there is no encryption during the whole watermarking scheme. Anyone who is familiar with the extraction rule could extract the right watermark, which will result in serious security breach. Therefore, a simple and effective encryption algorithm is indispensable. We would like to note that similar problems also exist in other recently proposed watermarking schemes based on LBP [16,17].



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

Fig. 7. Watermark false detection under the two special copy-paste attacks: (a) tampered image by the first copy-paste attack, (b) extracted watermark, (c) tampered image by the second copy-paste attack, and (d) extracted watermark.

4. The Proposed Secure Watermarking Based on LBP and Arnold Transform

An improved secure LBP-based semi-fragile watermarking is presented in this section to solve the problems mentioned above and ensure the security of the watermarking scheme. The LBP pattern only considers the size relationship between the central pixel value and neighborhood pixel values. The central pixel value plays an important role as a threshold. Therefore, if we take the information of central pixel value into account, it can reduce the false detection problem to a certain extent. Inspired by this, we define a new reference value $f_{\oplus}(\boldsymbol{b})$ calculated by:

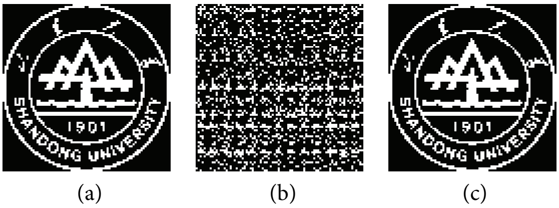
$$f_{\oplus}(\boldsymbol{b}) = b_0 \oplus b_1 \oplus \cdots \oplus b_7 , \tag{8}$$

where b_i $(i=0,1,\cdots,7)$ is the binary representation of central pixel value. Then we get the final reference value $f_{\text{final}} = f_{\oplus}(\boldsymbol{s}_p) \oplus f_{\oplus}(\boldsymbol{b})$. The watermark embedding is completed by modifying the neighborhood pixel values according to the value of f_{final} and Eq. (5). In this way, the central pixel is connected with the watermark bit *w*. Similarly, in watermark extraction, the above two values $f_{\oplus}(\boldsymbol{b})$ and $f_{\oplus}(\boldsymbol{s}_p)$ are first computed, and f_{final} is adopted to extract the watermark. If f_{final} is equal to 1, watermark bit *w* is 1. Otherwise, watermark bit *w* is 0.

To protect the watermark information, a suitable encryption method is necessary. Arnold transform has been widely used in information hiding due to its simplicity and good periodicity [18]. Arnold transform can be defined as:

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod N, \tag{9}$$

where (x_i, y_i) is the original coordinate of image pixel, (x_{i+1}, y_{i+1}) is the corresponding coordinate after permutation, and *N* is the width of image. After a certain times permutations, the transformed image can turn back to the original image again. So the transform time *k* can be taken as a secret key to encrypt the binary watermark image. Fig. 8 shows the original watermark and permuted watermarks, whose size is 84×84. In the improved LBP-based watermarking method, we take advantage of this property and perform Arnold transform on watermark image. After inverse transform, the watermark will be recovered from encrypted watermark. What's more, it is difficult for attackers to obtain the right watermark without correct key, even though they have learned the extraction rules.



(a) (b) (c)

Fig. 8. Arnold transform: (a) original watermark, (b) transformed image when $k=12$, and (c) transformed image when $k=24$.

To better illustrate this scheme, Fig. 9 gives the block diagram of the improved watermarking scheme based on LBP and Arnold transform. In addition to watermark extraction, the tamper location is realized by the difference-image between two scrambled watermarks obtained in watermark embedding and watermark extraction. Since there is only one bit watermark in each 3×3 image block, the tamper location is then obtained by mapping the difference-image to host image.

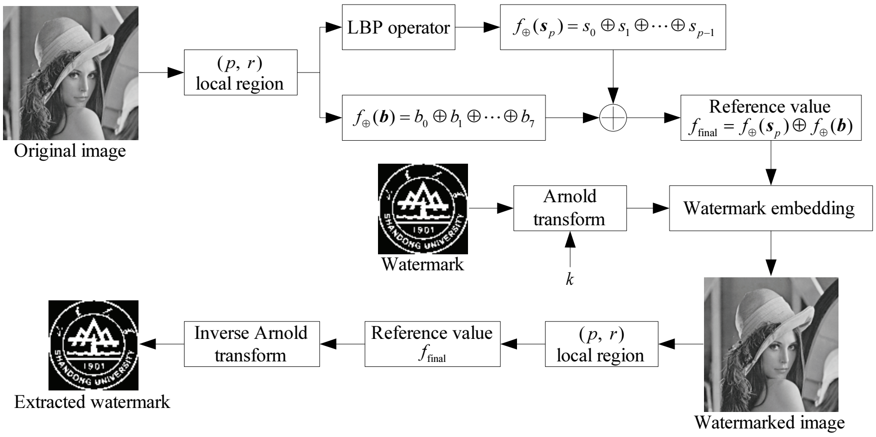

Original image
(p, r) local region
LBP operator
$f_{\oplus}(\boldsymbol{s}_p) = s_0 \oplus s_1 \oplus \cdots \oplus s_{p-1}$
$f_{\oplus}(\boldsymbol{b}) = b_0 \oplus b_1 \oplus \cdots \oplus b_7$
Reference value $f_{\text{final}} = f_{\oplus}(\boldsymbol{s}_p) \oplus f_{\oplus}(\boldsymbol{b})$
Watermark
Arnold transform
k
Watermark embedding
Watermarked image
(p, r) local region
Reference value f_{final}
Inverse Arnold transform
Extracted watermark

Fig. 9. Block diagram of the improved secure LBP-based watermarking scheme.

5. Experimental Results and Analysis

In this section, several experiments are conducted to prove the validity of the suggested watermarking scheme under general attacks and the proposed attacks. The local region blocks are determined by $r = 1$, and the secret key k in Arnold transform is set as 12. The peak signal-to-noise ratio (PSNR) and NC value are two evaluation indexes used in the experiments.

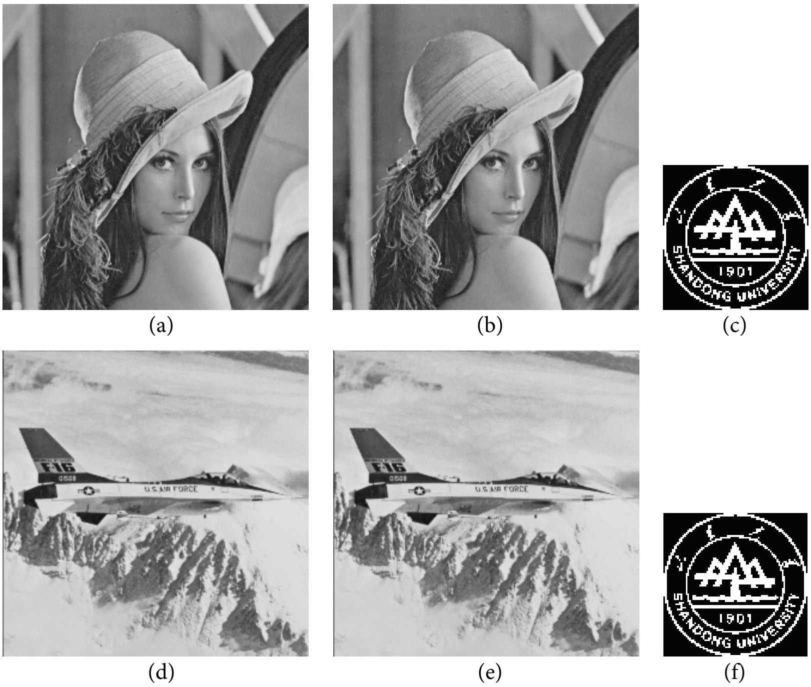
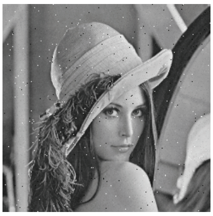
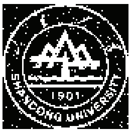
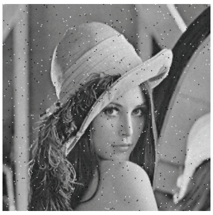
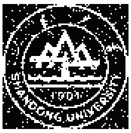
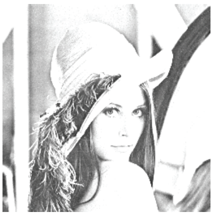
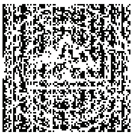
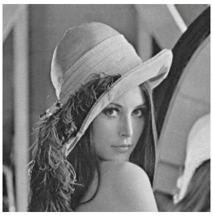
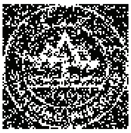
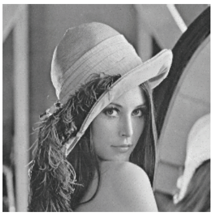
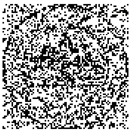

(a) (b) (c)
(d) (e) (f)

Fig. 10. Watermarked images and extracted watermarks without attacks: (a) original image Lena, (b) watermarked image Lena (PSNR=38.38 dB), (c) watermark extracted from image Lena (NC=1), (d) original image Airplane, (e) watermarked image Airplane (PSNR=35.33 dB), and (f) watermark extracted from image Airplane (NC=1).

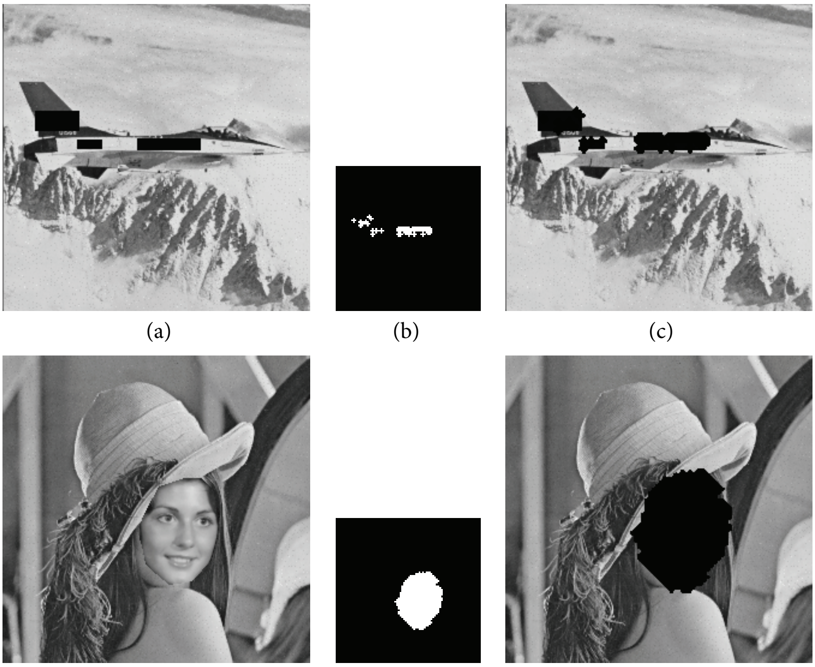
Table 1. Distorted watermarked images, extracted watermarks, and NC values under different general attacks

Attack	Watermarked image	Extracted watermark	NC
Salt & Pepper noise (0.005)			0.9829
Salt & Pepper noise (0.01)			0.9687
Contrast adjustment (×2)			0.9197
JPEG (*Q*=99)			0.8002
Brightness adjustment (+8)			0.3068

5.1 Performance under General Attacks

Fig. 10 presents the watermarked images and their corresponding extracted watermarks without attacks. It can be observed that the watermarked images have good visual quality and the PSNR is more than 35 dB, which implies that the watermark has good imperceptibility. However, during the process of image transmission and storage, the watermarked images always suffer from many innocent attacks, such as noise, JPEG compression, etc. To evaluate the performance of the improved watermarking scheme under these attacks, Table 1 lists the distorted watermarked images and extracted watermarks as well as the NC values under different general attacks. From Table 1, we can learn that the improved LBP-based semi-fragile watermarking shows certain robustness against general attacks, especially for Salt & Pepper noise. However, since the watermark embedding process is completed in spatial domain, this watermarking scheme is not robust enough for JPEG compression and other attacks, which needs to be addressed in the next research.

Except for general image processing operations, the semi-fragile watermark should be sensitive to malicious attacks. Object removal and copy-paste operation are two common attacks usually used by attackers. Fig. 11 depicts the tamper detection results for these two attacks, where the logos on the airplane are deleted and the face of image Lena is replaced. To highlight the tampered regions, the tamper location maps are dilated by using mathematical morphology operations. The detection results indicate that the proposed scheme performs well under baleful attacks.

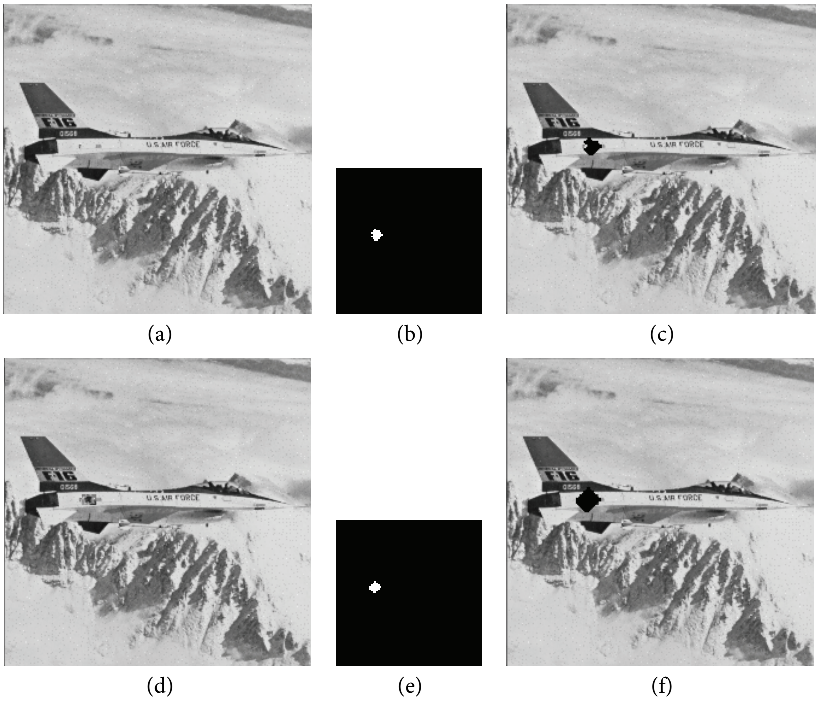

(a) (b) (c)

(d) (e) (f)

Fig. 11. Performance under baleful attacks: (a) tampered image Airplane, (b) tamper detection, (c) tamper location in host image, (d) tampered image Lena, (e) tamper detection, and (f) tamper location in host image.

5.2 Performance under the Proposed Attacks

To test the performance of the improved watermarking scheme under the proposed attacks, Fig. 12 shows the tamper location maps of the two special copy-paste attacks mentioned above. From Fig. 12, it is suggested that the improved scheme can avoid the limitation in LBP-based semi-fragile watermarking scheme [12] and locate the tampered regions effectively.



(a) (b) (c)

(d) (e) (f)

Fig. 12. Performance under the proposed attacks: (a) the first copy-paste attack, (b) tamper detection, (c) tamper location in host image, (d) the second copy-paste attack, (e) tamper detection, and (f) tamper location in host image.

6. Conclusions

In this paper, we analyze the defect of LBP operator, and note that different image blocks might have the same LBP pattern. Inspired by this, two special copy-paste attacks are proposed to prove the weakness of a semi-fragile watermarking based on LBP operators. By using the proposed attacks, same watermark bits can be obtained regardless of whether the image block is embedded by watermark. Therefore, this semi-fragile watermarking cannot be used for ownership protection and tamper location. To address this tough question, an improved watermarking based on LBP and Arnold transform has been presented. To avoid the flaw of LBP operator, the central pixel value is taken into account in watermarking embedding process. In addition, Arnold transform is employed in watermark embedding and extraction to ensure the security of the improved method. Experimental results show that this improved watermarking scheme achieves good effect in tamper detection and localization. However, due to the disadvantage of spatial-domain watermarking, the proposed scheme is not robust enough for some general attacks like JPEG compression. In the future work, we will introduce this method to frequency domain and improve the detection accuracy further.

Acknowledgement

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

References

[1] V. Verma and M. J. Singh, "Digital image watermarking techniques: A comparative study," *International Journal of Advances in Electrical and Electronics Engineering*, vol. 2, no. 1, pp. 173-184, 2013.

[2] 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.

[3] 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.

[4] T. Y. Lee and S. D. Lin, "Dual watermark for image tamper detection and recovery," *Pattern Recognition*, vol. 41, no. 11, pp. 3497-3506, 2008.

[5] 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.

[6] S. D. Lin, S. C. Shie, and J. Y. Guo, "Improving the robustness of DCT-based image watermarking against JPEG compression," *Computer Standards & Interfaces*, vol. 32, no. 1-2, pp. 54-60, 2010.

[7] Y. F. Zhu and L. Lin, "Digital image watermarking algorithm based on dual transform domain and self-recovery," *International Journal on Smart Sensing and Intelligent Systems*, vol. 8, no. 1, pp. 199-219, 2015.

[8] V. Solachidis and I. Pitas, "Circularly symmetric watermark embedding in 2-D DFT domain," *IEEE Transactions on Image Processing*, vol. 10, no. 11, pp. 1741-1753, 2001.

[9] J. M. Guo and H. Prasetyo, "Security analyses of the watermarking scheme based on redundant discrete wavelet transform and singular value decomposition," *AEU - International Journal of Electronics and Communications*, vol. 68, no. 9, pp. 816-834, 2014.

[10] S. Dadkhah, A. A. Manaf, Y. Hori, A. E. Hassanien, and S. Sadeghi, "An effective SVD-based image tampering detection and self-recovery using active watermarking," *Signal Processing: Image Communication*, vol. 29, no. 10, pp. 1197-1210, 2014.

[11] A. Tiwari and M. Sharma, "Comparative evaluation of semifragile watermarking algorithms for image authentication," *Journal of Information Security*, vol. 3, no. 3, pp. 189-195, 2012.

[12] 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.

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

[14] 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.

[15] A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, G. Bebis, and H. Mathkour, "Passive detection of image forgery using DCT and local binary pattern," *Signal, Image and Video Processing*, vol. 11, no. 1, pp. 81-88, 2017.

[16] 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.

[17] S. R. Chalamala and K. R. Kakkirala, "Local binary patterns for digital image watermarking," in *Proceedings of the 3rd International Conference on Artificial Intelligence, Modelling and Simulation*, Kota Kinabalu, Malaysia, 2015, pp. 159-162.

[18] Z. J. Liu, L. Xu, T. Liu, H. Chen, P. F. Li, and S. T. Liu, "Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains," *Optics Communications*, vol. 284, no. 1, pp. 123-128, 2011.

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 at 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 at Shandong University, Weihai, China. Her current research interests include channel estimation, image communication, and image watermarking.