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.

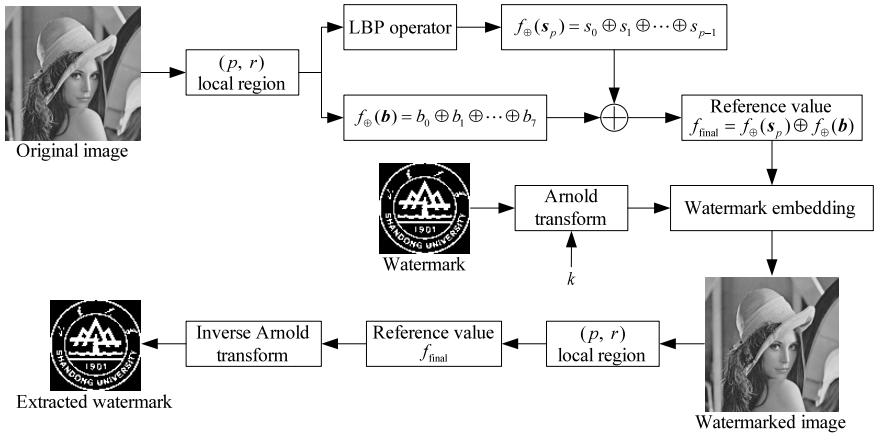

Fig. 9. Block diagram of the improved secure LBP-based watermarking scheme.

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.

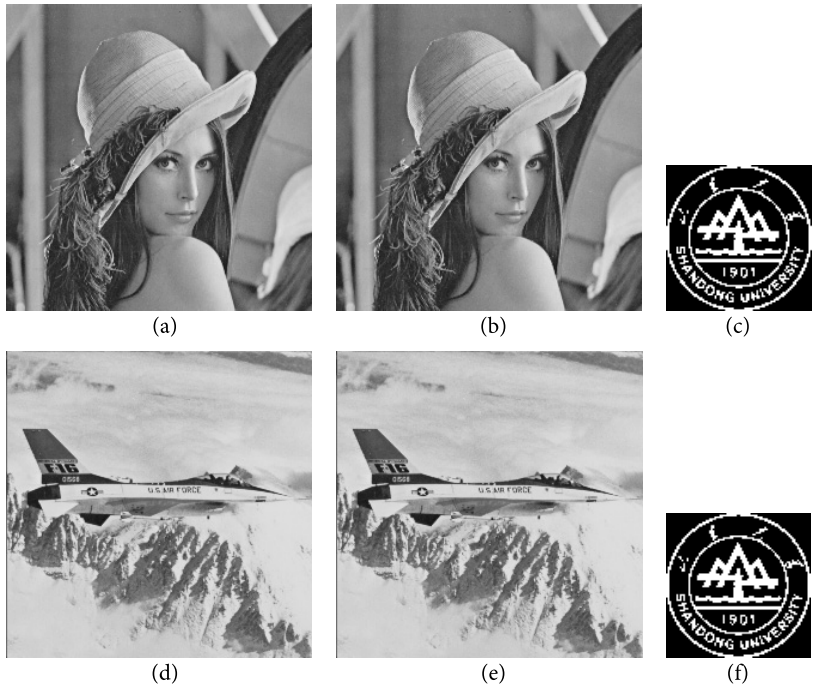

Fig. 10. Watermarked images and extracted watermarks without attacks: (a) original image Lena, (b) watermarked image Lena (PSNR=38.38 dB), (c) watermark extracted from image Lena (NC=1), (d) original image Airplane, (e) watermarked image Airplane (PSNR=35.33 dB), and (f) watermark extracted from image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

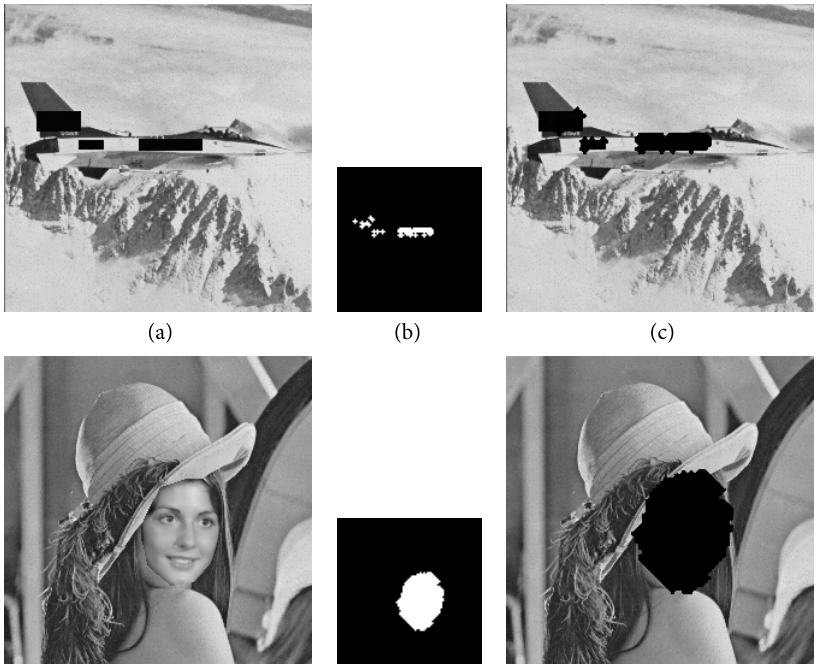

Fig. 11. Performance under baleful attacks: (a) tampered image Airplane, (b) tamper detection, (c) tamper location in host image, (d) tampered image Lena, (e) tamper detection, and (f) tamper location in host image.

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.

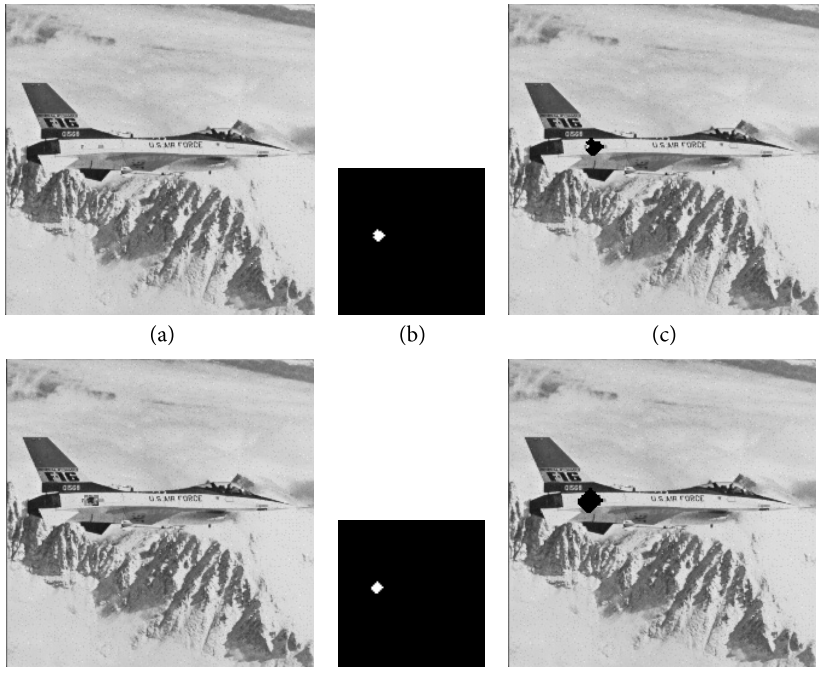

Fig. 12. Performance under the proposed attacks: (a) the first copy-paste attack, (b) tamper detection, (c) tamper location in host image, (d) the second copy-paste attack, (e) tamper detection, and (f) tamper location in host image.

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.