Advances in Engineering Research, volume 140
2nd International Conference on Electrical, Control and Automation Engineering (ECAE 2017)

Analysis on the Copy-move and Splicing Forgery of Fragile Watermarking Based on Local Binary Pattern

Peifei Song[1,*], Zhen Yue[2], Rundong Yang[1], Jie Shi[1]and Zichen Li[1]
[1]Beijing Institute of Graphic Communication, School of Information Engineering, Beijing, China
[2]Beijing University of Posts and Telecommunications, Information Security Center, Beijing, China
[*]Corresponding author

***Abstract*—In the process of transmission, the various factors can effect easily the multimedia information. The receiver can't distinguish whether the received multimedia data has been tampered. The fragile watermarking can authenticate the authenticity and integrality of the multimedia data. The paper analyzes the fragile watermarking based on local binary pattern. Experimental results demonstrate that, in a copy-move and splicing forgery, the existing algorithms can't determine whether a digital image is original or doctored.**

Keywords—fragile watermarking; local binary pattern; copy-move forgery; splicing forgery

I. INTRODUCTION

The development of network technology and digital multimedia technology has brought great convenience to people, while it also raises a number of security issues. During network transmission, digital media can easily be copied, processed, disseminated and exposed, so, how to identify the authenticity and integrity of digital multimedia data has become an urgent problem.

The fragile watermarking algorithm applied to the authenticity and integrity of multimedia data is a common technique by experts. Under the premise that the multimedia information satisfies certain perceived quality, digital watermark will be embedded in multimedia data. Even minor changes to the digital work, it can destroy the watermark. According to its sensitivity and the change of watermark information extracted from the works, legal users can judge whether digital works are tampered, and even indicate the tamper position and the nature of attack.

Local Binary Pattern (LBP) proposed by Ojala [1,2] is texture descriptor. The LBP texture descriptor represents the relation between the gray value of the 8 neighborhood sampling point and the center pixel. Pattern recognition is carried out by extracting the LBP texture feature. Ojala et al. [3] applied rotation invariant LBP histogram to the texture feature classification. According to the LBP's simple and efficient, literature [4] obtains a good classification effect on the texture database. LBP can also be widely used in face recognition [5,6], dynamic texture recognition [7], morphological localization [8], etc.

Zhang et al. [9] introduced LBP into watermark for the first time and proposed a semi-fragile watermarking algorithm based on the LBP operators. Firstly, it computes the LBP feature sequences and the relation between the gray value of the 8 neighborhood sampling point and the center pixel for each image block with 3 × 3 pixels. Then it determines the embedded position of the watermark information. Finally, the binary watermark is embedded into the host image and it obtains the watermarked image. The algorithm achieves good invisibility. At the same time, it is robust against the additive noise, luminance change, content tamper attacks, etc. However, it cannot concern the performance of tamper recovery.

On the basis of the method [9], Chang et al. [10] proposed the fragile watermarking algorithm for tamper detection and location with recover ability based on LBP. In the watermark generation and embedding stage, the two LSBs of each pixel firstly set to zero. Then it computes the LBP feature sequences (S and W) and the corresponding mean value (M) from the non-overlapping 3*3 blocks based on the LBP algorithm. Finally, S, W and M will be embedded into the 2-LSBs of the current block, then the watermarked image is formed. In the image tamper detection and recovery stage, the calculated watermark bits S' and W' will be compared with extracted watermark bits S'' and W''. If they are not the same, the current image block is judged as "tampered block", then recover it by the extracted pixel mean with M vector. The scheme has efficient tamper detection, but it does not describe how to tamper and the tamper recovery.

On the basis of the literature [10], literatures [11,12] proposed the modified fragile watermarking algorithm based on LBP. In the watermark generation and embedding stage, the algorithm has no scrambling pre-operation and does directly deal with the non-overlapping 3*3 blocks. Then the scheme processes the similar embedding manipulation with the literature [10]. Finally, the watermarked image is formed. In the image tamper detection stage, the calculated watermark bits S', W' and M' will be compared with extracted watermark bits S'', W'' and M''. If they are not the same, the current image block is judged as "tampered block". The tamper detection rate of this scheme are better than the literature [10], but the literatures [11,12] have no detailed description of tampering and tampering recovery.

In the paper, our main work is to find the copy-move and splicing forgery question about the fragile watermarking based on LBP. Through experimental analysis and comparison, the previously proposed algorithms fail to detect the corresponding 3*3 blocks copy-move and splicing attack. Additionally, experiments demonstrate that the algorithm can't detect

Copyright © 2018, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

properly the copy-move and splicing attack because of the one or two pixel bits translation.

The rest of this paper is organized as follows. Section 2 briefly reviews basis knowledge of LBP. Section 3 thoroughly analyzes the copy-move and splicing forgery of the fragile watermarking algorithm based on LBP. Experiment results are presented in Section 4 and Section 5 concludes the paper.

II. LOCAL BINARY PATTERN

Local binary pattern [1, 2] is image texture descriptor based on image spatial local operator. The core concept of LBP is that the gray value of the center pixel compares with its circularly symmetric 8 neighborhood, then the corresponding block will be taken the 2-valued mathematical operation. The gray level of pixels is 256. For the LBP number of (x_c, y_c), we describe it as follows:

$$LBP_{(P,R)}(x_c, y_c) = \sum_{i=0}^{P-1} S(g_i - g_c) \times 2^i,$$

$$S(g_i - g_c) = \begin{cases} 1, g_i - g_c \geq 0 \\ 0, otherwise \end{cases}.$$

Where, (x_c, y_c) is the coordinate of the center pixel C, its pixel value is g_c. g_i is the pixel value of the i-th neighborhood pixel. R represents the research radius in pixel, P represents the number of sampling points. For example, the (P, R) values can select $(8, 1)$, $(16, 2)$, etc. Figure 1 shows the computing processes of the LBP number.

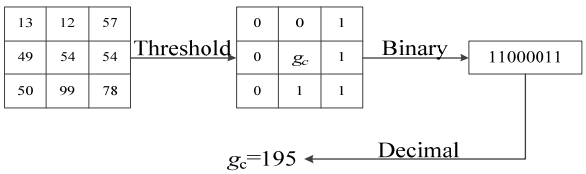


FIGURE I. THE COMPUTING PROCESSES OF THE LBP NUMBER

III. ANALYSIS OF THE FRAGILE WATERMARKING ALGORITHM BASED ON LBP

The rule of LBP [10,11,12] is different from the original LBP. According to the 8 neighborhood relationship of the center pixel, it can obtain the 8-bit binary watermark authentication information $S\left(S = \left(s_7 s_6 s_5 s_4 s_3 s_2 s_1 s_0\right)\right)$, where, s_i is the sign of each neighboring pixel. Specific implementation is shown by Figure 2.

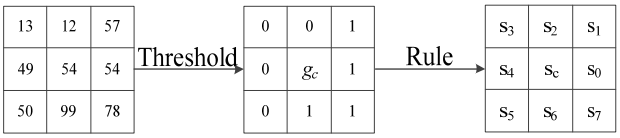
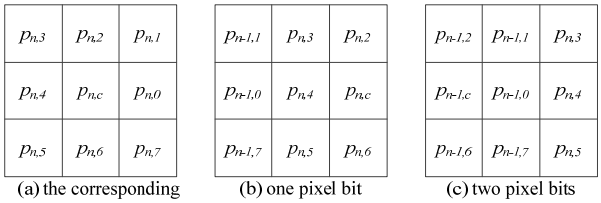


FIGURE II. THE CALCULATION PROCESS OF S SEQUENCE OF LBP [10,11,12]

Combining the rule of LBP with the Figure 3, we can discuss whether it can detect tampering, when the algorithm is affected by the corresponding 3*3 blocks copy-move and splicing attack. When the algorithm is corrupted by the copy-move and splicing attack because of the one or two pixel bits translation (Figure 3 (b) and (c) are as shown), whether it can effectively detect tampering.



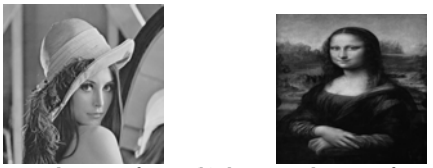
(a) the corresponding 3*3 block (b) one pixel bit translation (c) two pixel bits translation

FIGURE III. THE CASES OF 3*3 BLOCKS

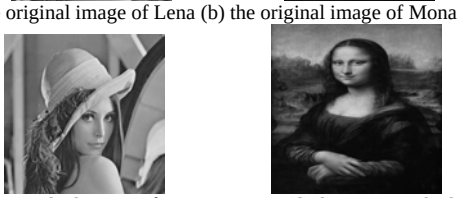
IV. EXPERIMENTAL RESULTS

In this chapter, we present and analyze the copy-move and splicing problems of LBP fragile watermark based on the experimental results. The experimental process is performed using MATLAB R2010b, on a PC with 8G RAM, 240G SSD and the Intel Core i5-6500 CPU @ 3.20 GHz.

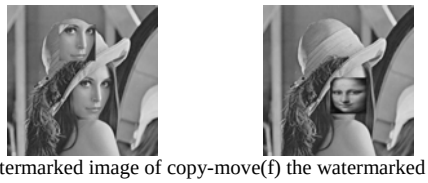
We select 512*512 images (Lena and Mona Lisa) for LBP-based fragile watermarking experiments. The experimental results are shown in Figure 4. Figure 4 (a) and (b) is respectively the original image Lena and Mona Lisa. Figure 4 (c) and (d) are the watermarked image after the fragile watermarking algorithm based on LBP. Figure 4 (e) is the watermarked image by the copy-move attack. Figure 4 (f) is the watermarked image by the splicing attack. When the algorithm is tampered with Figure 4 (e) and (f), it can't be effectively detected and determine whether the tampering.



(a) the original image of Lena (b) the original image of Mona Lisa



(c) the watermarked image of Lena (d) the watermarked image of Mona Lisa



(e) the watermarked image of copy-move(f) the watermarked image of splicing

FIGURE IV. THE EXPERIMENT RESULTS

TABLE I. THE COPY-MOVE AND SPLICING ATTACK AND THE TAMPER DETECTION RATE OF THE ALGORITHM

Method	the corresponding 3*3 blocks	the one pixel bit translation	the two pixel bits translation
method[10]	0%	68.67%	67.65%
method[11]	0%	68.57%	67.35%
method[12]	0%	68.57%	67.35%

As the Tables 1 show, the algorithms [10,11,12] fail to detect the corresponding 3*3 blocks copy-move and splicing attack. When the algorithm is corrupted by the copy-move and splicing attack because of the one or two pixel bits translation, the tamper detection rate of the algorithm can reach about 68%. The algorithms can't meet the needs of practical application. So, the algorithm can't detect properly the copy-move and splicing attack because of the one or two pixel bits translation.

In particular, such as military orders and medical records, such algorithms can't be effectively and correctly detect copy-move and stitching problems. It will result in serious consequences.

V. CONCLUSIONS

In the paper, the research and analysis of the previously proposed fragile watermarking algorithm based on LBP finds that the algorithm can't detect the corresponding 3*3 blocks copy-move and splicing attack. Additionally, experiments demonstrate that the algorithm can't detect properly the copy-move and splicing attack because of the one or two pixel bits translation. Furthermore, how to solve the copy-move and splicing forgery of fragile watermarking based on local binary pattern is also worthy of the further study.

ACKNOWLEDGMENT

This research was supported by Projects of National Natural Science Foundation(61370188); The Scientific Research Common Program of Beijing Municipal Commission of Education (KM201610015002,KM201510015009); The Beijing City Board of Education Science and technology key project (KZ201510015015,KZ201710015010); Project of Beijing Municipal College Improvement Plan (PXM2017_014223_000063); Cooperative education project between Ministry of education and Qualcomm Corp(201602034017).

REFERENCES

[1] T. Ojala, M. Pietikainen, and D. Harwood (1994), "Performance evaluation of texture measures with classification based on Kullback discrimination of distributions", Proceedings of the 12th IAPR International Conference on Pattern Recognition (ICPR 1994), vol. 1, pp. 582 - 585.

[2] T. Ojala, M. Pietikainen, and D. Harwood (1996), "A Comparative Study of Texture Measures with Classification Based on Feature Distributions", Pattern Recognition, vol. 29, pp. 51-59.

[3] T. Ojala, M. Pietikainen, T. Maenpaa, Multiresolution gray-scale and rotation invariant texture classification with local binary patterns [J]. IEEE Trans. Pattern Analysis and Machine Intelligence, 24 (7) (2002) 971-987.

[4] T. Ojala, T. Maenpaa, M. Pietikainen, J. Viertola, J. Kyllonen, and S. Huovinen, "Outex – new framework for empirical evaluation of texture

[5] analysis algorithm," in Proc. International Conference on Pattern Recognition, 2002, pp. 701-706.

[6] T. Ahonen, A. Hadid, M. Pietikainen, Face recognition with local binary patterns. Proceedings of European Conference on Computer Vision, Prague, Czech, 2004, p. 469.

[7] T. Ahonen, A. Hadid, and M. Pietikäinen, "Face recognition with Local Binary Patterns: application to face recognition," IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 28, no. 12, pp. 2037-2041, 2006.

[8] G. Zhao, and M. Pietikainen, "Dynamic texture recognition using Local Binary Patterns with an application to facial expressions," IEEE Trans. On Pattern Analysis and Machine Intelligence, vol. 27, no. 6, pp. 915-928, 2007.

[9] X. Huang, S. Z. Li, and Y. Wang, "Shape localization based on statistical method using extended local binary pattern," in Proc. International Conference on Image and Graphics, 2004, pp.184-187.

[10] Z. Wenyin, Frank Y. Shih, "Semi-fragile Spatial Watermarking Based on Local Binary Pattern Operators," Optics Communications, Vol. 284, Issues 16–17, 2011, pp. 3904-3912.

[11] Jun-Dong Chang, Bo-Hung Chen, and Chwei-Shyong Tsai, "LBP-based fragile watermarking scheme for image tamper detection and recovery", IEEE 2nd International Symposium on Next- Generation Electronics (ISNE), pp. 173-176, February 2013.

[12] Shakil A. Pinjari, Nitin N. Patil,"A Modifed Approach of Fragile Watermarking Using Local Binary Pattern (LBP)", International Conference on Pervasive Computing (ICPC) -1-4799-6272-3/15(c)2015 IEEE.

[13] T Sindhu, D. Madhu, "An Advanced Method of Fragile Watermarking Using Local Binary Pattern (LBP)", International Journal of Computer Science and Technology (IJCST), 2(7), 2016, pp.212-215