Multimed Tools Appl (2013) 64:757–776
DOI 10.1007/s11042-011-0974-z

Multi-block dependency based fragile watermarking scheme for fingerprint images protection

Chunlei Li · Yunhong Wang · Bin Ma · Zhaoxiang Zhang

Published online: 7 January 2012

Abstract For traditional fragile watermarking schemes, isolated-block tamper which will destroy the minutiae of the fingerprint image can hardly be efficiently detected. In this paper, we propose a multi-block dependency based fragile watermarking scheme to overcome this shortcoming. The images are split into image blocks with size of 8×8; a 64-bit watermark is generated for each image block, and then equally partitioned into eight parts. Each part of the watermark is embedded into another image block which is selected by the corresponding secret key. Theoretic analysis and experimental results demonstrate that the proposed method not only can detect and localize the isolated-block tamper on fingerprint images with high detection probability and low false detection probability, but also enhances the systematic security obviously.

Keywords Fragile watermarking · Fingerprint · Isolated-block · Tamper detection

1 Introduction

A biometric verification system automatically identifies individuals based on their distinct physical or behavioral characteristics, such as fingerprint, face, voice, iris, etc. Compared with traditional person identification techniques like passwords and PIN codes, biometrics have been increasingly used for accurate identification

C. Li (✉) · Y. Wang · B. Ma · Z. Zhang
School of Computer Science and Engineering, Beihang University, Beijing, China
e-mail: lichunlei1979@cse.buaa.edu.cn

Y. Wang
e-mail: yhwang@buaa.edu.cn

B. Ma
e-mail: mabin@cse.buaa.edu.cn

Z. Zhang
e-mail: zxzhang@buaa.edu.cn

in diverse business (e.g., security, e-commerce, remote authentication) since they cannot be misplaced or forgotten. Specifically, fingerprint biometrics, has exhibited high performance in terms of distinctiveness, permanence, and performance. As the wide use of fingerprint verification system has attracted more and more attacks, there is an urgent need for enhancing system security. One particular component of such verification system would have to rely on secure transmission, storage and content authentication of the raw fingerprint images [22].

Digital watermarking of fingerprint images appears to be an excellent solution for countering sophisticated attacks on the identification systems. Yeung et al. [22] embedded the authentication watermarks into fingerprint image to localize tampered region. The authors concluded that the watermarking technique does not lead to a significant performance loss in fingerprint verification. However, the watermarking scheme is vulnerable to vector quantization (VQ) attack [12] and collage attack [7]. Ratha et al. [17] proposed an algorithm for secure data hiding in wavelet compressed fingerprint images. Assuming the image capture device is secure and only the decompressor on the server can locate the embedded message and thereby validate the submitted image. Noore et al. [15] embedded the face and demographic text data into the selected texture regions of a fingerprint image using discrete wavelet transform. The integrity of the fingerprint image is verified through the high matching scores obtained from automatic fingerprint identification system. Zebbiche et al. [24] described an efficient watermarking technique to protect fingerprint images. The rationale is to embed watermarks into the ridges area of fingerprint images so that the technique is inherently robust, yields imperceptible watermarks, and resists cropping and segmentation attacks. Ahmed et al. [1] proposed a phase-encoding-based digital watermarking technique for fingerprint image protection. The authors extracted a signature from the one-dimensional Fourier phase of the original fingerprint images and then embedded it back into the image using a variation of phase-shift keying modulation and spread-spectrum method. However, the last four methods can only detect whether the fingerprint images have been changed, but can not localize the tampered region. Therefore, it creates a demand for developing a secure method for tamper detection and localization of fingerprint images.

As we known, fingerprint comprises a distinctive and unique ridge pattern structure. For fingerprint images, attackers can manipulate the structure only by

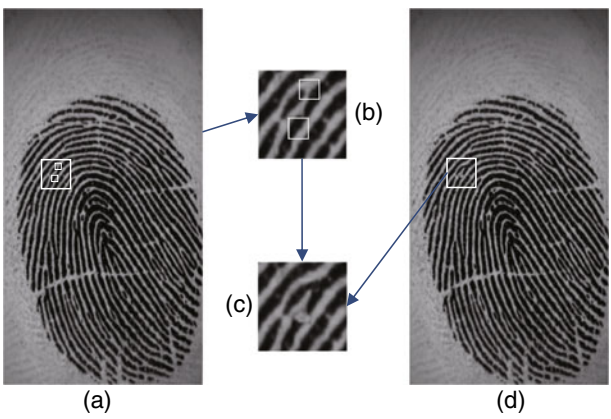

Fig. 1 Isolated-block tampers on fingerprint image. **a** Original live-scan fingerprint image with size of 560 × 296; **b** Portions of the image are magnified to show sample ridge bifurcation and ridge ending; **c** Tampered sample ridge bifurcation and ridge ending from **b**; **d** Tampered fingerprint image

slight isolate-block tampering, which is not salient to human vision. An example of a fingerprint image is shown in Fig. 1a, and a example of ridge ending and bifurcation is magnified in Fig. 1b. We can tamper two isolated-blocks as shown in Fig. 1b. The tampered ridge ending and bifurcation are shown in Fig. 1c. In Fig. 1d, although we cannot visually determine whether the fingerprint images suffer from tamper. In fact, the minutiae feature of original fingerprint image has already been destroyed. Whereas, this ill-operation cannot be detected by the conventional block-wise dependent fragile watermarking scheme. Therefore, attackers can implement DoS (denial of service) attack by tampering isolated block to prevent legitimate use of the biometric system. In this paper, a multi-block dependency based fragile watermarking scheme is proposed to protect fingerprint image from isolated-block tampering. The novelty of the proposed method includes the following three aspects: (1) we present isolated-block tamper for fingerprint images, and demonstrate this tamper can destroy the fingerprint features; (2) aim at solving the problem that the conventional block-wise dependent fragile watermarking cannot detect these isolated-block tampers, we propose an improved multi-block dependency based fragile watermarking scheme; (3) theoretic analysis of localization accuracy is presented.

The remainder of the paper is organized as follows. In Section 2, we analyze the performance of the conventional fragile watermarking scheme; Section 3 gives the proposed fragile watermarking scheme; Section 4 presents the security strength analysis; In Section 5, the theoretic analysis of tamper localization is discussed; Section 6 shows the experimental results; and finally, Section 7 concludes the proposed scheme.

2 Analysis of block-wise fragile watermarking scheme

To verify the integrity of digital images, many fragile watermarking schemes have been proposed. It is designed to detect any slight changes of watermarked images. Therefore, the generated watermarks and the embedding watermarks should be vulnerable to any changes. At present, most of conventional fragile watermarking schemes generate authentication watermarks depending on the image contents and embed watermarks into their least significant bits(LSBs) of images [2–5, 8–11, 13, 14, 16, 18, 20, 25].

The performance of different fragile watermark schemes is mainly evaluated using two criteria: tamper localization accuracy and security strength. Pixel-based fragile watermarking schemes [2, 14, 20, 25] have highest localization accuracy, but it is vulnerable to Oracle attack [21]. In order to resist this attack, block-based fragile watermarking scheme is proposed. They divide a host image into small blocks and then embed fragile watermarks into each block, which can detect and localize the malicious tamper. In 1998, Wong et al. [20] proposed the block-wise fragile watermarking scheme. It is capable to detect and localize any unauthorized tampered block, but the block-wise independency of their method is vulnerable to vector quantization (VQ) codebook attack [22] and collage attack [12]. In 2006, Chang et al. [4] proposed a block-wise image authentication scheme which can withstand counterfeiting attacks by combining the local and global features to obtain the authentication data. Li et al. [13] proposed a fragile watermarking scheme that exploits nondeterministic dependence information to resist counterfeiting attacks.

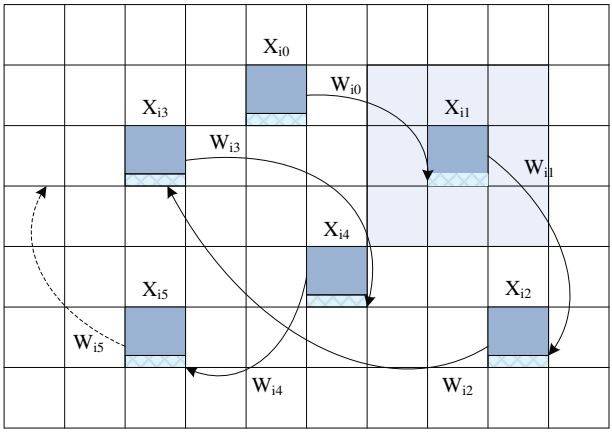

Fig. 2 Block-wise dependency based watermarking scheme

He et al. [9, 11] proposed a block-wise dependency based fragile watermarking method and the nondeterministic dependency is built based on block-chain to resist VQ and collage attacks. The above improved schemes effectively break block-wise independency, and make the watermarking schemes not vulnerable to the counterfeiting attacks. The embedding process is depicted in Fig. 2. Unfortunately, the chain scheme fails to detect the isolated-block tampers owing to the continuous tamper assumption. For example, we assume X_{i1} suffers from tampering, then the watermark generated from X_{i1} does not agree with the watermark embedded in X_{i2}, and the watermark generated from X_{i0} is also inconsistent with the watermark inserted in X_{i1}. The traditional methods regard X_{i0} and X_{i1} as candidate tampered blocks, then detect the neighborhood block of X_{i0} and X_{i1}, respectively, to determine which one is the genuine tampered block based on the fact that the tampered region is continuous. However, if the neighborhood of X_{i1} is not tampered, the genuine tampered block X_{i1} will be omitted.

3 Proposed authentication watermarking scheme

For block-wise fragile watermarking scheme, there is a tradeoff between localization accuracy and security strength, and security strength is determined by block size [11]. Considering security requirement, 8×8 block is the optimal choice for localization. In order to detect and localize isolated-tamper block, a 64-bit watermark is generated from each image block; and it is equally partitioned into eight parts. Each part is embedded into another image block to construct multi-block dependent structure (see Fig. 3). This multi-block dependent structure guarantees the proposed method can detect isolated-block tamper. Table 1 shows the notations and parameters used in this paper.

3.1 Flowchart of watermark embedding

The process of watermark generation and embedding is shown in Fig. 4. The Least significant bits (LSBs) of the original image X is set to zero, noted as $\overline{X}$. Then $\overline{X}$ is

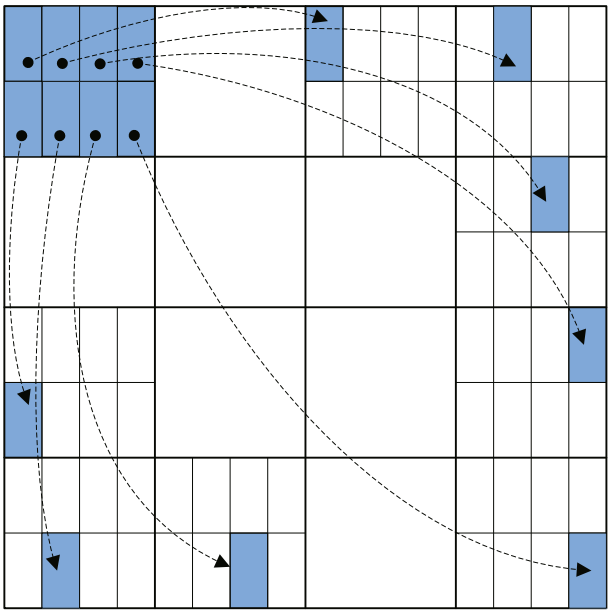

Fig. 3 Multi-block dependent structure

divided into image blocks $\overline{X}_i, i = 1, 2, \cdots, N_b$ with size 8×8. For each image block, a 64-bit watermark is generated using cryptographic hash function MD5, and it can be written as follows:

$$C_i = H(\overline{X}_i, i) = \left(c_{i1}, c_{i2}, \cdots, c_{i64}\right) \tag{1}$$

We generate the random sequence by utilizing logistic chaotic map to encrypt the hash code [26], denoted as *Random*() in Algorithm 1.

$$y_{n+1} = \lambda y_n \left(1 - y_n\right) \tag{2}$$

where $n = 1, 2, 3, \cdots$ is the map iteration index. For system parameter $3.47 < \lambda < 4$, the sequence is non-periodic, non-convergent, and very sensitive to the initial value y_0. Thus, the secret key k_1 is formulated as follows: $k_1 = \{\lambda, y_0\}$. In this paper, λ and y_0 are set to 3.78 and 0.53, respectively. Then, we binarize this sequence to a binary string $s_m \in 0, 1$, and split the binary string into the sub-string $S_i = s_{i1}, s_{i2}, \cdots, s_{i64}$, $i = 1, 2, \cdots, N_b$. Exclusive-OR (XOR) operation is used to encrypt the hash code

Table 1 Notations and parameters

k_1, k_2:	Secret key
N_b:	Number of image block
X:	Original image
$\overline{X}$:	7MSBs of original image
Y:	Watermarked image
Y^*,$\overline{Y}^*$:	Tested image, 7MSBs of test image
X_i,Y_i,Y_i^*:	image block. $1 \le i \le N_b$

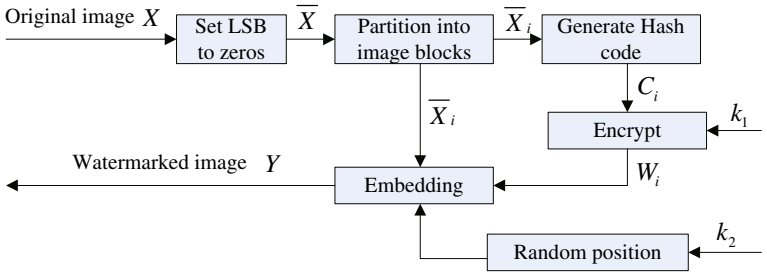

Fig. 4 Flowchart of watermark embedding

according to (3), and the encrypted hash code is used as the generated authentication watermark bits $W = W_1, W_2, \cdots, W_{N_b}$.

$$w_{i,j} = c_{ij} \bigoplus s_{ij} \tag{3}$$

where $1 \le i \le N_b$, $1 \le j \le 64$.

To select the embedding position, eight random sequences $I^k = \{I_1^k, I_2^k, \cdots, I_{N_b}^k\}$, $k = 1, 2, \cdots, 8$ are generated using secret key k_2. And the process is described as follows [23].

Step 1 Generate eight random sequences $R^k, k = 1, 2, \cdots, 8$ of length N_b with secret keys k_2, where R^k can be represented as $R^k = \{r_1^k, r_2^k, \cdots, r_{N_b}^k\}$.

Step 2 Sort $R^k, k = 1, 2, \cdots, 8$ with stable sorting algorithm, obtain the sorted sequence $R_I^k = (r_{I_1^k}^k, r_{I_2^k}^k, \cdots, r_{I_{N_b}^k}^k)$, and index sequences $I^k = (I_1^k, I_2^k, \cdots, I_{N_b}^k)$.

The generated index sequences I^k are used as the random position sequences.

After generating eight random position sequences $I_i^k, i = 1, 2, \cdots, N_b, k = 1, 2, \cdots, 8$, we equally split the generated watermark W_i into eight parts $W_i^k, k = 1, 2, \cdots, 8$ of length 8-bits, denoted as *Partition*() in Algorithms 1 and 2. Each part is embedded into the LSBs of the corresponding part of the image block whose positions is selected by the generated position sequences. The k^{th} part uses the k^{th} position sequence. Watermark generation and embedding procedures are described in Algorithm 1.

Algorithm 1 (Generation and embedding of W)

1. for $i \leftarrow 1$ *to* N_b
2. $C_i \leftarrow H(\overline{X}_i, i)$, $S_i \leftarrow Random(k_1)$,
   $W_i \leftarrow C_i \bigoplus S_i$ //Generate and encrypted watermarks.
3. $\{W_i^1, W_i^2, \ldots, W_i^8\} \leftarrow Partition(W_i)$
4. $I^k = (I_1^k, I_2^k, \ldots, I_{N_b}^k), k = 1, 2, \ldots, 8$
   //Generate eight random position sequences.
5. $LSB(\overline{X}_{I_i^k}^k) \leftarrow W_i^k$ // Embed watermarks
6. $Y_i \leftarrow \overline{X}_i$

The embedding equation for each pixel can be represented as follows.

$$Y_{m,n} = 2 \times \lfloor X_{m,n}/2 \rfloor + W_{m,n}, m = 1, 2, \cdots, M$$
$$n = 1, 2, \cdots, N \tag{4}$$

where $M \times N$ is the size of images. The metrics of quality of the watermarked image which are often used include Signal to Noise Ratio (SNR), Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Watson Distance (WD). In this paper, Peak Signal to Noise Ratio (PSNR) is used as the metrics.

$$PSNR = 10log10[b/MSE] \tag{5}$$

Where b is the square of the largest value of the signal (typically 255). And the square error (MSE) is the mean square by (6).

$$MSE = \frac{\sum_{i,j}\left[f(i,\, j) - f_w(i,\, j)\right]^2}{M \times N} \tag{6}$$

The watermark is embedded into 1-LSB of the image. We assume that the distribution of 1-LSB and watermarks are uniform. For 1-LSB plane, the occurrence probabilities of "0" and "1" are equal to 0.5. After embedding the watermark, the probability of "0" switching to "1" is 0.5; the same is for "1". If any bits is changed and the corresponding changed value of 1-LSB is 2^0. Therefore, the average energy of distortion caused by watermarking on each pixel is:

$$\left|x_w(i,\, j) - x(i,\, j)\right| = \left(0.5^2 + 0.5^2\right) \times 2^0 = 0.5 \tag{7}$$

Then the average PSNR of the watermarked image is approximately,

$$PSNR = 10log10[b/MSE] = 10log10\left(255^2/0.5^2\right)$$
$$= 54.15dB \tag{8}$$

3.2 Watermark extraction and tamper localization

The process of watermark extraction and localization is exhibited in Fig. 5. Let Y^* represent the test image, which can be a tampered watermarked image or unaltered one. Firstly, we set LSBs of the test image Y^* to zero, noted as $\overline{Y}^*$, and split the image $\overline{Y}^*$ into image blocks $\overline{Y}_i^*, i = 1, 2, \cdots, N_b$. For each image block, W_i^* is generated as done in the watermark embedding process, and partitioned into eight parts,

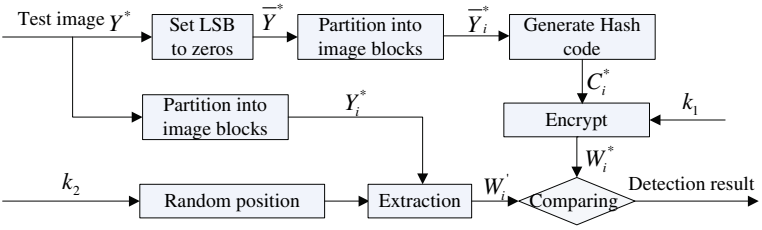

Fig. 5 Flowchart of watermark extraction and tamper detection

noted as $W_i^{*k}, k = 1, 2, \cdots, 8$. Secondly, we extract eight embedded watermarks $W_i' = W'_{I^1(i)}, W'^2_{I^2(i)}, \cdots, W'^8_{I^8(i)}$ from the 1-LSB of the other eight image blocks whose positions are selected by the generated random position sequences using secret key k_2. Finally, for each image block, only all the W_i^{*k} are inconsistent with $W'^k_{I_i^k}$, the image block Y_i^* will be marked as tampered. Extraction and detection procedures are described in Algorithm 2.

Algorithm 2 (Extraction and detection)

1. for $i \leftarrow 1 \quad to \quad N_b$
2. Generate W_i^*//Generate and encrypt watermarks.
3. $\{W_i^{*1}, W_i^{*2}, \ldots, W_i^{*8}\} \leftarrow Partition(W_i^*)$
4. Generate random position sequences using secret k_2
5. $W_i' = \{W'_{I_i^1}{}^1, W'_{I_i^2}{}^2, \ldots, W'_{I_i^8}{}^8\}$ //Extract watermarks
   //from the other eight image blocks
6. $d_i^k = \begin{cases} 0, & W'_{I_i^k}{}^k = W_i^{*k} \quad k = 1, 2, \ldots, 8 \\ 1, & \text{elsewise} \end{cases}$
   //Get eight tamper signs for each image block
7. $D_i = \begin{cases} 1, & \sum_{k=1}^{8} d_i^k = 8 \\ 0, & \text{elsewise} \end{cases}$ //Get detection result

4 Security strength analysis

Security of fragile watermarking techniques refers to "the inability by unauthorized users to manipulate the watermarked authentic image without being detected" [6]. In order to quantitatively evaluate the watermarking security under exhaustive search (ES) attack, we adopt the security strength (SS) as defined in [8]:

$$SS = minlog_2\left(\frac{1}{P_{ESA}}\right) \tag{9}$$

where $P_{ESA} = 1/N_s$ refers to the probability that a manipulated image block is undetected by the verification system, and such manipulation refers to various possible attacks. In order to forge an image block, the attackers must get the information about the encrypted watermarks generated from the image block and the embedding position. The m-bits watermark has 2^m possible sequences, and the embedding position has N_b possible positions, where N_b is the number of the image block. As a result, without the secret keys, the attacker needs $2^m \times N_b$ tries to traverse the entire search space, thus $N_s = 2^m \times N$. $min(\cdot)$ is the smallest one in all elements.

In Yeung et al. [22], the fragile watermarking scheme is pixel-based, we can regard the image block with size 1×1. One bit watermark is generated using a binary look up table (LUT) for each pixel, and embedded into the least significant bit plane (LSB) of this pixel. During the procedure of tamper detection, the watermark information is generated from each image pixel, and the hiding watermark bits are also extracted from its LSB. Then the tamper detection can be determined by comparing the generated watermark with the extracted watermark. Because the detection procedure is content independent, we can only modulate the embedded

watermark bit in LSB to pass through verification. Therefore it only takes one trial to forge an image pixel, the P^1_{ESA} of the scheme in Yeung et al. [22] under the ES attack is 1, thus the security strength $SS_1 = log_2(1) = 0$.

In He et al. [9], a 64-bit watermark is generated for each image block, and it has N_b possible embedding positions. Then, the P_{ESA} of the scheme in He et al. [9] under the ES attack is:

$$P^2_{ESA} = 1/\left(2^{64} \times N_b\right) \tag{10}$$

Accordingly, the security strength is:

$$SS_2 = 64 + log_2^{N_b} \tag{11}$$

In our proposed method, for each image block, eight 8-bit watermarks are generated and embedded into the other eight image blocks. For each 8-bits watermark, the embedding position has N_b possible positions. The P_{ESA} of the proposed method under ES attack is:

$$P^3_{ESA} = 1/\left(N_b \times 2^8\right)^8 = 1/\left(2^{64} \times N_b^8\right) \tag{12}$$

The security strength is:

$$SS_3 = 64 + log_2^{N_b^8} = 64 + 8log_2^{N_b} \tag{13}$$

we can get the following relation:

$$SS_3 > SS_2 > SS_1 \tag{14}$$

The larger SS the of the verification system is, the stronger the security strength. Therefore, our method has superior security than the method in [22] and the method in [9].

5 Analysis of localization accuracy

Aiming at evaluating the performance of our proposed watermarking scheme, we conduct an elaborate theoretic analysis on the probability of tamper detection inspired by Yu et al. [23], and simulation results validate the correctness of the theoretic results.

5.1 The probability of tamper detection under tampered region

Under tampered region, if any pixel of the image block Y_i^* is changed, W_i^* generated from Y_i^* is correspondingly altered. As a trivial fact, the probability that "0" or "1" switches is 0.5 under tampered region. For each part of W_i^*, if one bit changed, we think this part is tampered. The probability of $W_i^{*k}(k = 1, 2, \ldots, 8)$ with 8-bits keeping unaltered is about 0.5^8, then the probability of $W_i^{*k}(k = 1, 2, \ldots, 8)$ changed is about $1 - 0.5^8$. Let $p_1, p_2, \ldots, p_8$ represent the following probabilities: if an image block under tampered region, there exists $0, 1, \ldots, 8$ altered $W_i^{*k}(k = 1, 2, \ldots, 8)$, respectively. They can represent as Table 2.

As described in Yu et al. [23], the region tamper not only affects the image block, but also affects the watermark embedded into the image block. If the proportion

Table 2 ($p_0 \sim p_8$)

$p_0 = (0.5^8)^8$	$p_1 = C_8^1(1-0.5^8)(0.5^8)^7$
$p_2 = C_8^2(1-0.5^8)^2(0.5^8)^6$	$p_3 = C_8^1(1-0.5^8)^3(0.5^8)^5$
$p_4 = C_8^4(1-0.5^8)^4(0.5^8)^4$	$p_5 = C_8^5(1-0.5^8)^5(0.5^8)^3$
$p_6 = C_8^6(1-0.5^8)^6(0.5^8)^2$	$p_7 = C_8^7(1-0.5^8)^7(0.5^8)$
$p_8 = (1-0.5^8)^8$	

of the tampered region versus the whole image is a, the block Y_i^* located in the tampered region is also a, and out of the tampered region is $1-a$. Suppose that W_i^{*k} keeps unchanged after Y_i^* undergoes region tampering, if $Y_{I_i^k}{}^*$ in which W_i^{*k} locate is out of tampered region, the probability W_i^{*k} that will be marked tampered is 0; and if $Y_{I_i^k}{}^*$ locate in tampered region, the probability of W_i^{*k} will be marked tampered is $1-0.5^8$. Thus, the probability p_f that W_i^* has been marked as tampered provided that it keeps unchanged after Y_i^* undergoes region tampering can be written as follows.

$$p_f = (1-a)\times 0 + a\times\left(1-0.5^8\right) = \left(1-0.5^8\right)a \tag{15}$$

The probability p_t represents that W_i^{*k} has been considered as tampered on the assumption that its value altered. If $Y_{I_i^k}{}^*$ in which W_i^{*k} locate is out of tampered region, the probability that W_i^{*k} will be marked tampered is 1, and if $Y_{I_i^k}{}^*$ locate in tampered region, the probability of W_i^{*k} will be marked tampered is $1-0.5^8$. Thus, the probability p_t can be written as follows.

$$p_t = (1-a)\times 1 + a\times\left(1-0.5^8\right) = 1-0.5^8 a \tag{16}$$

As mentioned in the process of tamper detection, only all the eight W_i^{*k} have been marked tampered, the image block Y_i^* will be marked un-tampered. The detection probability P_d can be described as the following:

$$\begin{aligned} P_d = {} & p_0\times p_f^8 + p_1\times p_f^7\times p_t + p_2\times p_f^6\times p_t^2 + p_3 \\ & \times p_f^5\times p_t^3 + p_4\times p_f^4\times p_t^4 + p_5\times p_f^3\times p_t^5 \\ & + p_6\times p_f^2\times p_t^6 + p_7\times p_f\times p_t^7 + p_8\times p_t^8 \end{aligned} \tag{17}$$

The first segment of the (17) represents that eight $W_i^{*k}(k=1,2,\ldots,8)$ are all same, the probability that the eight W_i^{*k} have been marked as tampered; the second segment of this formula represents that only one of eight W_i^{*k} changed, the probability that the eight W_i^{*k} have been marked as tampered; the third segment represents that three of W_i^{*k} changed; and so on.

5.2 The probability of false tamper detection

When the un-tampered blocks have been marked as tampered region, the false detection occurs. In this section, we will deduce the probability of false detection. Suppose that the proportion of the tampered region is a, the probability that the image blocks located in the un-tampered region is $1-a$. The generated watermark

W_i^{*k} from un-tampered keeps unchanged. If the $Y_{I_i^k}{}^*$ in which W_i^{*k} locate is out of tampered region, the probability W_i^{*k} that will be marked tampered is 0; and if $Y_{I_i^k}{}^*$ locate in tampered region, the probability of W_i^{*k} will be marked tampered is $1-0.5^8$. Thus, the probability that W_i^{*k} will be detected as tampered can be represented as follows.

$$p_{nt} = (1-a) \times 0 + a \times \left(1 - 0.5^8\right) = 1 - 0.5^8 a \tag{18}$$

For an image block, only if all the eight watermarks W_i^{*k} have been marked tampered, the image block will be marked tampered. Thus, the false tamper detection probability P_{fd} can be obtained according to (19):

$$P_{fd} = p_{nt}^8 \tag{19}$$

5.3 Simulation validation

We carry out numerous simulations to validate the value of theoretic deduction P_d and P_{fd}. In order to quantitatively evaluate the simulation results, two measures are adopted: tamper detection probabilities (EP_d) and false alarm probabilities (EP_{fd}).

$$EP_d : R_d = N_d / N_b \times 100\% \tag{20}$$

$$EP_{fd} : F_d = F_d / N_b \times 100\% \tag{21}$$

where N_d is the number of tampered blocks which are correctly detected, F_d is the number of valid blocks which are marked as tamper.

A set of images are chosen in out simulations, which comprises eight images of size 512×512, as shown in Fig. 6, and the average PSNR of the watermarked images

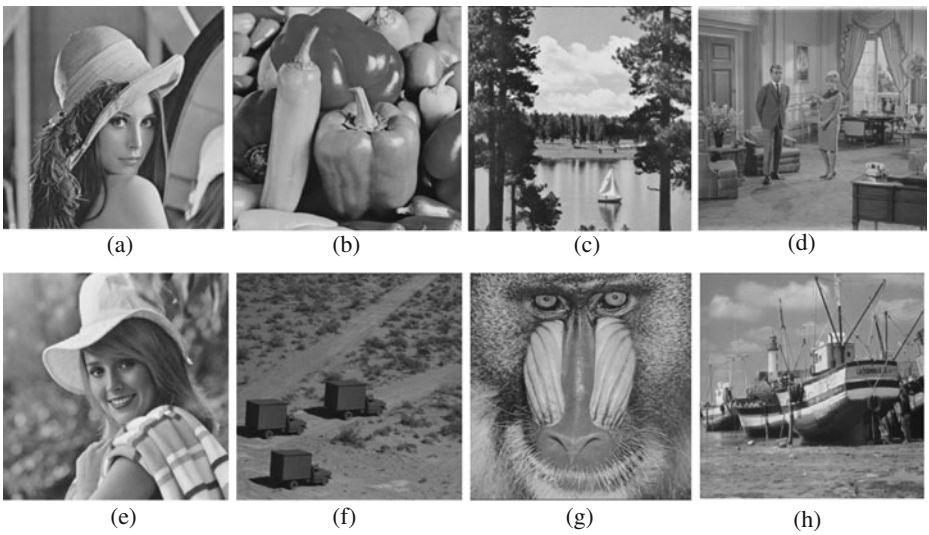

Fig. 6 Test images (512×512) used in our experiments: **a** Lena **b** Pepper **c** sailboat **d** couple **e** Elaine **f** trunk **g** mandrill **h** ship (all images are from USC-SIPI)

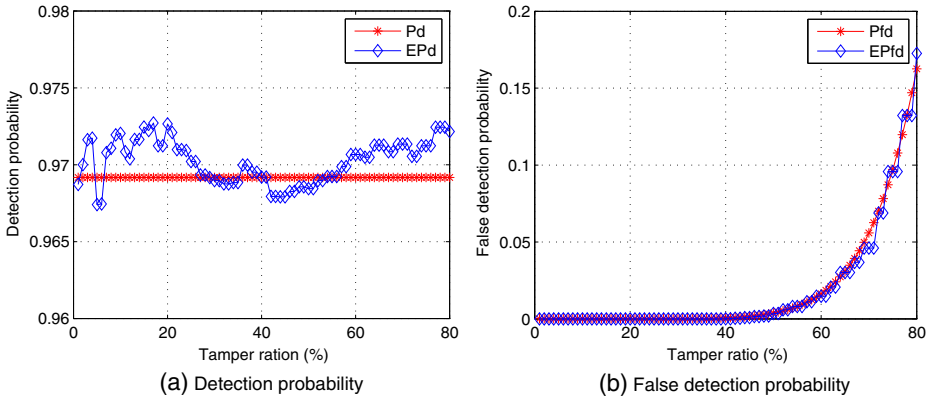

Fig. 7 Localization accuracy

is 54.26dB, which is consistent with our theoretic values obtained by (8). Suppose the proportion of the tampered region is in [0.01, 0.8] with the interval of 0.01; for each a, we carry on region tampering for 20 times, and get the average simulation values for EP_d and EP_{fd}, respectively. We draw the theoretic values and simulation results on Fig. 7a and b, where P_d and P_{fd} represents theoretic values, and EP_d and EP_{fd} represents simulation values. From Fig. 7a and b, we can conclude that our simulation results are close to theoretic values, which verifies the rightness of the probabilities we have deduced for tamper detection. It is also noticed from Fig. 7a that the value of P_d is close to 97% at various tempering ratio from 1 to 80%; at the same time, Fig. 7b shows that the value of P_{fd} is quietly perfect (close to zeros) at low and moderate tampering ratio (less than 50%), and is acceptable (no more than 16%) even at very high tampering ratio around 80%. Therefore, we can conclude that the proposed method can detect and localize the tamper with high detection probability and low false detection probability.

6 Experimental results

6.1 Detection performance under region tamper of general image

The first experiment considers small region tamper. The watermarked image 'Trunk' with size of 512 × 512 is shown in Fig. 8a, and we tamper the watermarked image as shown in Fig. 8b by adding two copies of the trunk at the bottom of the picture. The tamper detection results by He et al. [9] and our proposed method are shown in Fig. 8c and d, respectively. From the two figures, we can see that our method and He et al. [9] can localize the two tampered regions with high detection probability and low false detection probability. The second experiment considers the case when the tamper ratio is up to 70%. We tamper the image Fig. 9a by replacing one patch using another image as shown in Fig. 9b, c and d show the detection result by He et al. [9] and our proposed method, respectively. The method in He et al. [9] can nearly localize all tampered blocks except some blocks located at the boundary of the tampered region, and the value of tamper detection probability (P_d) and

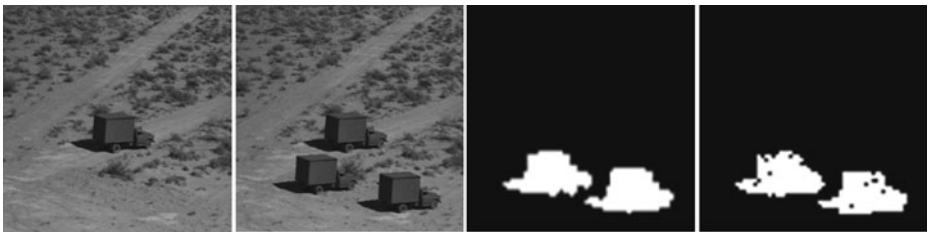

Fig. 8 Tamper detection result: **a** Watermarked image **b** Tampered image **c** Detection result by He et al. [9] **d** Detection result by our method

false detection probability (P_{fd}) are 98.53 and 3.76%, respectively. Our method can also clearly localize the tampered region with $P_d = 96.78\%$ and $P_{fd} = 4.49\%$, respectively. From the experimental results, we can see that our proposed can localize the region tamper with high probability as the conventional block-chain fragile watermarking scheme.

6.2 Detection performance under isolated-block tamper of fingerprint images

The following experiments consider the protection of fingerprint images using the proposed method. We conduct the experiments on the FVC DB2 database which consists of 110 subjects, and each person has six images. Two fingerprint images are randomly selected from one person, one is used as the reference image, and the other is the test image. Meantime, the method in Tsai et al. [19] is adopted to extract minutiae of fingerprint image and calculate matching score. In this method, the image quality maps by checking the low contrast areas, low flow blocks, and high curve regions are generated. And then, a binary representation of the fingerprint is constructed by applying a rotated grid on the ridge flows of the fingerprint. Minutiae are generated by comparing each pixel neighborhood with a family of minutiae templates. Finally, the heuristic rule is used to merge and filter out the spurious minutiae. After extracting minutiae,the convex hulls for a given reference point pair generates the overlapped areas of query and reference fingerprints. The convex hull constructed from feature points on query fingerprint (I) is denoted as C_I. For every feature point on the reference fingerprint (R), if it falls inside C_I, we say it is in the

Fig. 9 Tamper detection (70%): **a** Watermarked Lena image **b** tampered image **c** Detection result by He et al. [9] **d** Detection result by our method

overlapped area with I. Similarly, we would have a set of feature points on I that fall in the overlapped area with R. Thus, we can have the numbers (O_I and O_R) of feature points on overlapped areas of I and R. In the end, the similarity score is calculated by combine all the information from n, O_I, O_R, and S_{avg}, as described in the following (22).

$$Similarity_{\text{score}} = n^2 \times S_{\text{avg}}/(O_I \times O_R) \tag{22}$$

where n is the number of matched minutiae on both prints. S_{avg} is the average score of all the matched features.

Firstly, in order to illustrate the effect of watermarks on the fingerprint image, we watermark the test fingerprint images using our proposed method, and keep the reference images unchanged, then calculate the matching score between test set and reference set, and between watermarked test set and reference set for each person, as shown in Fig. 10. The perfect coincidence of the two curves demonstrates the watermark has little effect on the distinguish-ability of the fingerprint image.

Secondly, the effect of isolated-block tamper corresponding detection result on fingerprint image is considered. Isolated-block tamper and detection is shown in Fig. 11. Figure 11a illustrates the original fingerprint images. We randomly tamper the isolated-block of the original fingerprint image over the whole images, and the tamper ratio is only 1 and 5%, respectively, as shown in Fig. 11b. Meantime, Fig. 11a and b show the minutiae extracted from the original fingerprint images and the tampered images, where the green and red points represent the matched and mismatched minutiae. These red points demonstrate that the tamper has affected the fingerprint feature. To further evaluate the feature distortion, we draw the curve of matching scores between test images and reference images, and between tampered test images and reference images, as depicted in Fig. 12. Figure 12a shows the match score when the tamper ratio is only 1%, the match score only undergoes a slight change. When the tamper ratio is 5%, half of the fingerprint match scores decrease significantly, as shown in Fig. 12b. The above curves show that isolate-tampers affect

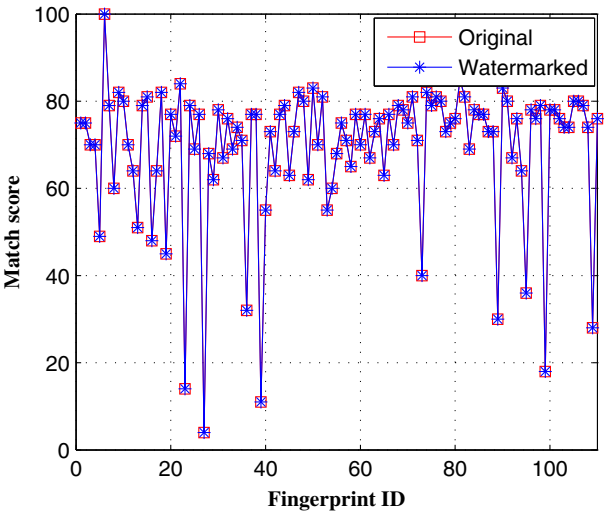

Fig. 10 Match score of fixed reference set with various test sets: original test image vs. watermarked test image

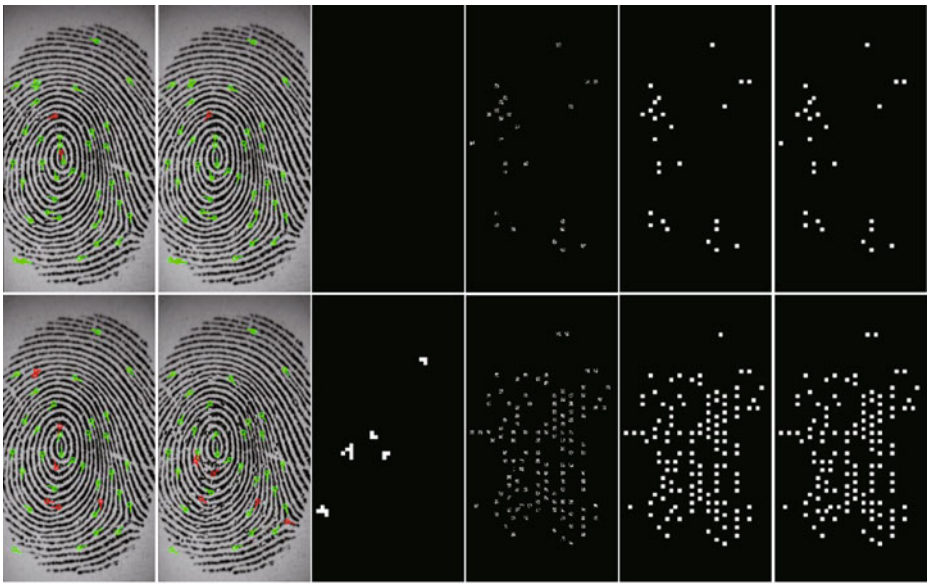

Fig. 11 Tamper detection under different tamper ratio: 1 and 5%, **a** original images and its minutiae **b** tampered image and its minutiae **c** detection result by He et al. [9] **d** detection result by Yeung et al. [22] **e** detection result by our method **f** tamper mask

the distinguish-ability of the fingerprint images, and with the increase of tamper ratio, the distinguish-ability of the fingerprint image decrease very quickly. Figure 11c shows the tamper result by He et al. [9], Fig. 11d shows the tamper result by Yeung et al. [22], and Fig. 11e shows the tamper result by our method. Comparing with the tamper mask as shown in Fig. 11f, we can conclude that our method and the method

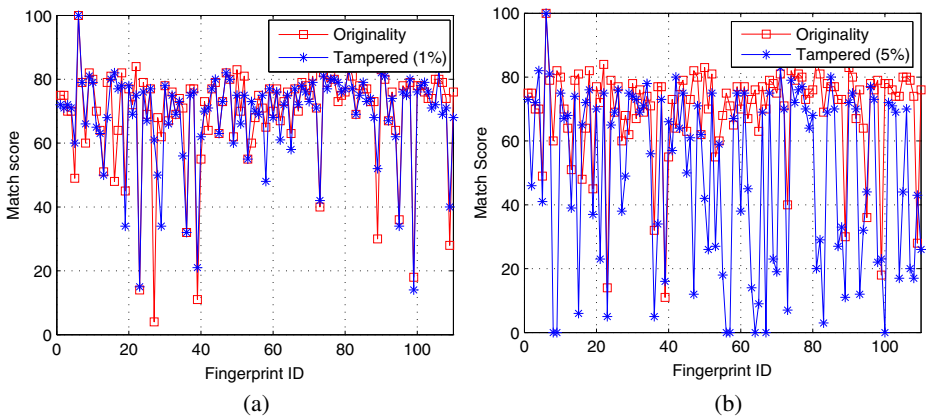

Fig. 12 Match score of fixed reference set with various test sets: **a** original test image vs. tampered test image (1%); **b** original test image vs. tampered test image (5%)

Fig. 13 Tamper detection under collage **a** fingerprint 1# and its minutiae **b** fingerprint 2# **c** tampered fingerprint 1# and its minutiae **d** detection result by Yeung et al. [22] **e** detection result by our method **f** tamper mask

of Yeung et al. [22] can localize the isolated-tamper block with high probability while He's method [9] hardly works.

6.3 Security under collage attacks

In this section, we will compare the security of our method with the scheme of Yeung et al. [22] under collage attack. Two fingerprint images, fingerprint 1# and fingerprint 2#, are watermarked using our method and the scheme in Yeung et al. [22] with the same secret key. The watermarked images are shown in Fig. 13a and b, respectively. We replace several isolated blocks of 'fingerprint 1#' with the same blocks of 'fingerprint 2#', and the result is shown in Fig. 13c. Meantime, the minutiae extracted from the original fingerprint images and the tampered images as shown in Fig. 13a and c, where the green and red points represent the matched and mismatched minutiae. These red points demonstrate that the tamper has affected the fingerprint feature. Figure 13d shows the tamper result by Yeung et al. [22], and Fig. 11e shows the tamper result by our method. Comparing with the tamper mask as shown in Fig. 11f, we can conclude that the method of Yeung et al. [22] cannot detect the forged isolated blocks, which is vulnerable to collage attack. This is due to the fact that the detection procedure is content-independent. Our proposed method is based on multi-block dependency, therefore, can localize the isolated blocks under collage attack.

The comparison between our algorithm and the other methods can be found in Table 3. The method in Yeung et al. [22] not only can localize isolated-block

Table 3 Comparisons with other methods

Methods	Categories	Security strength	Localize region tamper	Localize isolate-block tamper
Method in [22]	Fragile	0	√	√
Methods in [1, 15, 17, 24]	Robust	–	×	×
Method in [9]	Fragile	$log_2^{N_b}$	√	×
Our method	Fragile	$8 \times log_2^{N_b}$	√	√

tamper, but also can localize region tamper. However, it is block independent, thus is vulnerable to VQ attack and collage attack. The methods in [1, 15, 17, 24] are used to verify the authenticity of fingerprint images, but cannot localize the tampered region. The schemes in [4, 9, 11, 13] break the block independency by block-chain to improve security strength; however, they cannot detect isolated-block tampers. Our proposed multi-block dependency based fragile watermarking scheme can not only detect and localize isolated-block tampers in fingerprint images, but also possesses high security strength. Meanwhile, additional experiments also illustrate that the proposed method performs as well as the state of the art when applied on natural images.

7 Conclusions

Traditional fragile watermarking schemes based on block-wise dependence can hardly detect the isolated-block tamper. However, this tamper will destroy the content of fingerprint image, and even result in a false recognition. In this paper, we propose a security fragile watermarking scheme based on multi-block dependent structure to detect isolated-block tamper on the fingerprint image. Experimental results show the embedded watermarks are visually imperceptible and maintain the recognition rate of fingerprint images. Meanwhile, theoretic analysis and experimental results demonstrate that the proposed method can detect and localize both isolated-block tamper and region tamper with high detection probability and low false detection probability. In addition, multi-block dependent structure guarantees that our method can resist VQ attack and collage attack.

Acknowledgements This work was supported by the National Natural Science Foundation of China (No. 60873158), the National Basic Research Program of China (No. 2010CB 327902), the Fundamental Research Funds for the Central Universities, and the Opening Funding of the State Key Laboratory of Virtual Reality Technology and Systems.

References

1. Ahmed AF, Selvanadin KB (2008) Fingerprint reference verification method using a phase encoding based watermarking technique. J Electron Imaging 17:1–9
2. Anthony TS, Zhu XZ, Shen J (2008) Fragile Watermarking based on encoding of the zeroes of the Z-Transform. IEEE Trans Inf Forensics Security 3(3):567–569
3. Celik M, Sharma G, Saber E (2002) Hierarchical watermarking for secure image authentication with localization. IEEE Trans Image Process 11:585–595
4. Chang CC, Hu YS, Lu TC (2006) A watermarking-based image ownership and tampering authentication scheme. Pattern Recogn Lett 27:439–446
5. Chen WC, Wang MS (2009) A fuzzy c-means clustering-based fragile watermarking scheme for image authentication. Expert Syst Appl 36:1300–1307
6. Deguillaume F, Voloshynovskiy S (2003) Secure hybrid robust watermarking resistant against tampering and copy attack. Signal Process 83:2133–2170
7. Fridrich J, Goljan M, Memon N (2002) Cryptanalysis of the Yeung-Mintzer fragile watermarking technique. J Electron Imaging 11:262–274
8. He HJ, Zhang JS, Tai HM (2008) Digital watermarking scheme exploiting nondeterministic dependence for image authentication. IHW 5284:147–160
9. He HJ, Zhang JS, Chen F (2009) Adjacent-block based statistical detection method for self-embedding watermarking techniques. Signal Process 89:1557–1566
10. He HJ, Zhang JS, Tai HM (2009) Self-recovery fragile watermarking using block-neighborhood tampering characterization. IHW 5806:132–145

11. He HJ, Zhang JS, Tai HM (2010) A neighborhood-characteristic-based detection model for statistical fragile watermarking with localization. Multimed Tools Appl 1:1–18
12. Holliman H, Memon N (2000) Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes. IEEE Trans Image Process 9:432–441
13. Li CT, Yuan Y (2006) Block-chain based fragile watermarking scheme with superior localization. Opt Eng 45:1–6
14. Liu SH, Yao HX, Gao W, Liu YL (2007) An image fragile watermark scheme based on chaotic image pattern and pixel-pairs. Appl Math Comput 185:869–882
15. Noore A, Singh R, Vatsa M, Houck M (2007) Enhancing security of fingerprints through contextual biometric watermarking. Forensic Sci Int 169:188–194
16. Ohkita K, Yoshida M, Kitamura I, Fujiwara T (2009) Improving capability of locating tampered pixels of statistical fragile watermarking. In: Proceedings of the 8th international workshop on digital watermarking, vol 5703, pp 279–293
17. Ratha NK, Villanueva MAF, Connell JH, Bolle RM (2004) A secure protocol for data hiding in compressed fingerprint images. Lect Notes Comput Sci 3087:205–216
18. Suthaharan S (2004) Fragile image watermarking using a gradient image for improved localization and security. Pattern Recogn Lett 25:1893–1903
19. Tsai YJ, Venu GJ (2005) A minutia-based partial fingerprint recognition system. Pattern Recogn 38:1672–1684
20. Wong P (1998) A public key watermark for image verification and authentication. In: Proc Int Conf Image Processing 1:455–459
21. Wu JH, Bin B, Zhu BB, Li SP, Lin FZ (2004) Efficient oracle attacks on Yeung–Mintzer and variant authentication schemes. In: IEEE international conference on multimedia & Expo (ICME), pp 931–934
22. Yeung MM, Pankanti S (1999) Verification watermarks on fingerprint recognition and retrieval. In: Proc. of SPIE conference on security and watermarking of multimedia contents, San Jose, pp 66–78
23. Yu M, He HJ, Zhang JS (2007) A digital authentication watermarking scheme for JPEG images with superior localization and security. Sci China F Inf Sci 50:491–509
24. Zebbiche AK, Khelifi F, Bouridane A (2008) An efficient watermarking technique for the protection of fingerprint images. In: EURASIP journal on information security, pp 1–20
25. Zhang XP, Wang SZ (2007) Statistical fragile watermarking capable of locating individual tampered pixels. IEEE Signal Process Lett 14:727–730
26. Zhang J, Tian L, Tai HM (2004) A new watermarking method based on chaotic maps. In: Proc. IEEE ICME'04, vol 89, pp 157–163

Li Chunlei received the Bachelor degree in Computer Science department from Zhengzhou University of China in 2001. He received the master degree from Hohai University of China in 2004. From 2004 to 2008, he worked in Zhongyuan University of Technology of China. He is now a doctor at Computer Science School, Beihang University. His current research interests include digital watermarking, multimedia security and pattern recognition.

Wang Yunhong received a M.S. degree and a Ph.D. degree in electronic engineering from Nanjing University of Science and Technology in 1995 and 1998 respectively. She worked at the National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, Beijing, China, from 1998 to 2004. Since 2004, she has been a Professor with the School of Computer Science and Engineering, Beihang University, Beijing, China. Her research interests include biometrics, pattern recognition, computer vision, data fusion and image processing. She is a member of IEEE and IEEE Computer Society.

Ma Bin received a B.E. degree from Zhengzhou university, Zhengzhou, china, in 2008. Since 2008, he is working toward the Ph.D. degree in Beihang University, Beijing, China. His research interests include image processing, biometrics, pattern recognition, digital image watermarking.

Zhang Zhaoxiang received a Ph.D. degree in the National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, Beijing, China, in 2009. Since 2009, he has been a lecture with the School of Computer Science and Engineering, Beihang University, Beijing, China. His research interests include biometrics, pattern recognition, computer vision, and image processing.