Multimedia Tools and Applications (2019) 78:22727–22742
https://doi.org/10.1007/s11042-019-7560-1

Commutative fragile zero-watermarking and encryption for image integrity protection

Ming Li[1] • Di Xiao[2] • Ye Zhu[3] • Yushu Zhang[4,3] • Lin Sun[1]

Received: 5 March 2018 / Revised: 28 January 2019 / Accepted: 2 April 2019 /
Published online: 24 April 2019

Abstract

With the increasing demands of privacy protection and integrity protection of digital images, attention has been drawn to the commutativity of watermarking and encryption. In some of the existing works, watermarking and image encryption are commutative, but watermark detection and image decryption are not commutative. Meanwhile, in some other schemes, watermark detection and image decryption are commutative, but the order of watermarking and image encryption is fixed. The existing schemes cannot meet the requirement of commutativity. Therefore, we propose a novel commutative zero-watermarking and encryption scheme, in which the commutativity is equipped in both the phases of watermarking and image encryption and the phases of watermark detection and image decryption. The proposed scheme is fragile, and the zero-watermarking will not cause any modification of the image. Experiments show that the proposed scheme is effective and feasible. The illegal tampered area of the zero-watermarked image can be accurately detected and located.

Keywords Commutative · Zero-watermarking · Encryption · Integrity protection · Fragile

1 Introduction

Encryption is a widely used technology to protect the content of digital images from unauthorized access. Meanwhile, watermarking is deployed for ensuring authenticity, copyright violation detection, and proof of ownership or distributorship of the content [24, 25]. The two

✉ Di Xiao
xiaodi_cqu@hotmail.com

[1] College of Computer and Information Engineering, Henan Normal University, Xinxiang 453007, China

[2] College of Computer Science, Chongqing University, Chongqing 400044, China

[3] School of Information Technology, Deakin University, Burwood, Victoria 3125, Australia

[4] Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China

kinds of technologies can be used together to enhance the protection of the image. For example, at the sender side, the information of ownership or the authentication bits are firstly embedded into the original image as watermarking to protect the copyright or the content of the host image. Then, when the watermarked image is going to be communicated on the public channel, it is always encrypted for the purpose of privacy protection. In this application, watermarking is performed before encryption [15, 17]. Besides, sometimes the untrusted third-parties such as cloud servers and database managers need to manage the encrypted host images stored in the open network environment in a privacy-preserved way by embedding some additional bits such as identification information, time stamp. Therefore, watermarking after encryption is also studied [8, 12, 16, 18]. At the receiver side, there are two different applications too [12, 27]: the first is that watermark detection before image decryption, which is especially appropriate for the privacy-preserved management of host images by the untrusted third-party, and also suitable for the user to extract watermarks in a large number of encrypted images in order to save a lot of execution time of image decryption; the second is that watermark detection after image decryption. For example, the watermark is a time stamp. In this case, it is not necessary for the user authenticity, but it can be used to trace the history of the image in future. Clearly, to meet the requirement of uncertain environment, the capability of watermark embedding and watermark extraction in both plain and encrypted domain is required [2, 5, 28]. In addition, some computational cost will be saved in some applications using the commutative schemes [7]. Therefore, the study of the commutative watermarking and encryption (CWE) [2, 5, 7, 28] becomes quite noticeable in recent years.

Some of the CWE schemes are based on partial encryption [2, 5, 28], in which the images are divided into two independent parts, i.e., the most significant part to human vision is encrypted to make the image unintelligible and the least significant part is watermarked. However, in [7], the encryption and watermarking operations are applied to the same part of data. Since the two operations are homogenous with commutative properties, their orders can be commutated. In these methods, watermarking and image encryption are commutative; however, the commutativity of watermark detection and image decryption are not considered. In [27], the latter two phases, i.e., watermark detection and image decryption, are commutative, but the order of watermarking and image encryption is fixed.

Different from the existing CWE algorithms, the proposed scheme achieves the commutativity not only in watermarking and image encryption, but also in watermark detection and image decryption. In addition, the image is fully encrypted to protect its privacy. To avoid distortion of the protected image, the technique of zero-watermarking [6, 10, 11, 19, 20, 22, 23, 26] is utilized. The basic idea of the zero-watermarking technique is to construct an image-dependent watermark (IDW) directly from its own features of digital images, and then combine it with an actual watermark to form some zero-watermarking information, and finally store them in the intellectual property databases. Obviously, the zero-watermarking technique breaks through the conventional idea of embedding watermark by modifying the spatial values or transform domain coefficients of the original multimedia. Some of them equip fragility [6, 19], while others equip robustness [20, 22, 23, 26]. Fragile zero-watermarking is rare. However, the fragility is required in the applications such as tamper detection and tamper location, just like the existing fragile watermarking schemes [1, 3, 14, 15]. The proposed zero-watermarking is fragile. The key finding of our work is that a commutative algorithm of matrix calculating and rearranging is developed, based on which we proposed a commutative fragile zero-watermarking and encryption scheme to protect the integrity of digital images. The characteristics of the proposed method are summarized as follows:

(1) The encryption of the image is complete, and the zero-watermarking can be implemented in the encrypted domain, which is the same as that performed in the plain domain.
(2) In order to protect the image integrity, the tampered area can be detected and located precisely. In addition, the quality of the protected image is not degraded by zero-watermarking.
(3) Not only watermarking and image encryption but also watermark detection and image decryption are commutative.
(4) The proposed method can be widely used in different applications, e.g., the privacy-preserved management by the untrusted third-party on the cloud where watermarking is after image encryption and watermark detection is before image decryption, secure image distribution where the watermark serves as a time stamp or fingerprint that can be detected after image decryption, etc.

2 The proposed method

The sketch of the proposed method is shown in Fig. 1.The original image can be watermarked and encrypted without fixed order, and the obtained encrypted images and zero watermarks (XORing the IDW and the actual watermark) in the two cases are consistent. Specifically, the original image can be processed by the watermark generation firstly to obtain the IDW, and then the image encryption to obtain the encrypted image. Alternatively, the original image can be processed by the image encryption firstly to obtain the encrypted image which is the same as that stated above, and then the watermark generation to obtain the same IDW. The encrypted image would not be changed after watermark generation. Then, the zero watermark can be obtained by XORing the IDW and the actual watermark. Similar to the image encryption and the watermark generation, the two phases of image decryption and watermark detection do not affect each other, and the verification to obtain the extracted IDW can be performed on both the encrypted image and the decrypted image. Specifically, the encrypted image can be processed by the image decryption firstly to obtain the decrypted image, and then the watermark detection to obtain the extracted IDW. The decrypted image would not be modified by watermark detection. Alternatively, the encrypted image can be processed by watermark detection to obtain the same extracted IDW, and then the image decryption to obtain the same decrypted image. By executing XOR between the extracted IDW and the zero watermark, the final watermark can be extracted.

Prior to encryption or watermark generation, the original image should be divided into non-overlapping blocks with the same size, e.g., 8 × 8. For each block, we transform all of the

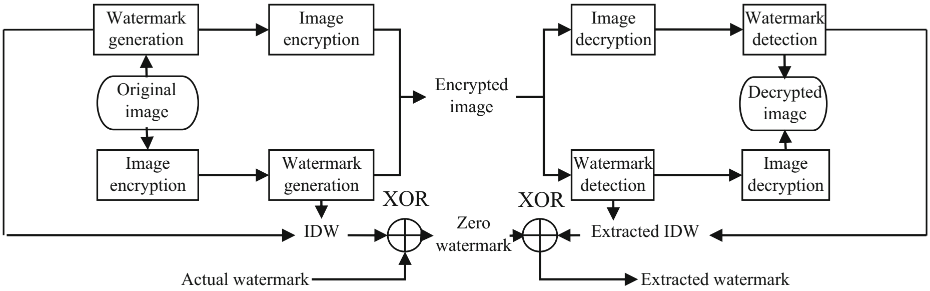


Fig. 1 The sketch of the proposed method

pixels into binary representations to form bit planes as shown in Fig. 2a. Then, the entire bit planes are rotated 90 degrees horizontally to form Fig. 2b so as to disturb the pixel values form bit level. Figure 2c is another representation of the data cube shown in Fig. 2b, and it can be converted into another two-dimensional matrix (called converted block) by merging the new bit planes. When encryption or watermark generation is finished, each converted block is rotated in reverse to get back to the original state. So are image decryption and watermark detection phases. Thus, all the four phases including watermarking, image encryption, image decryption and watermark detection are operated on the converted blocks, which helps to improve the encryption effect. As stated before, image encryption and watermarking are commutative; image decryption and watermark detection are also commutative. We explain the details of the four phases separately in the following subsections. The proof of the commutativity and experiments will be given in Section 3.

2.1 Image encryption

For each converted block, firstly divide it into two two-dimensional matrices of size 8 × 4, denoted by A and B respectively, as shown in Fig. 3. Then, rearrange the elements of A and B in the same way using the encryption key.

The encryption key is the initial parameter α and initial value q_0 of the chaotic system:

$$q_{i+1} = \alpha q_i (1-q_i),\ \ q_i \in (0,1) \tag{1}$$

with a parameter $\alpha \in (3.6, 4]$, the system is in the chaotic state [9]. The encryption of the nth block can be described as follows:

Step 1: Convert the block as shown in Fig. 2.

Step 2: Iterate the chaotic system $n \times 32$ times, and get the last 32 values $\{q_{(n-1)\times 32+1}, q_{(n-1)\times 32+2}, \ldots, q_{n\times 32}\}$.

Step 3: Sort the obtained 32 values to obtain $\left\{\overline{q}_{(n-1)\times 32+1}, \overline{q}_{(n-1)\times 32+2}, \cdots, \overline{q}_{n\times 32}\right\}$, then find the position of values $\left\{\overline{q}_{(n-1)\times 32+1}, \overline{q}_{(n-1)\times 32+2}, \cdots, \overline{q}_{n\times 32}\right\}$ in $\{q_{(n-1)\times 32+1}, q_{(n-1)\times 32+2}, \ldots, q_{n\times 32}\}$, and mark down the transform position $H = \{h_1, h_2, \ldots, h_{32}\}$.

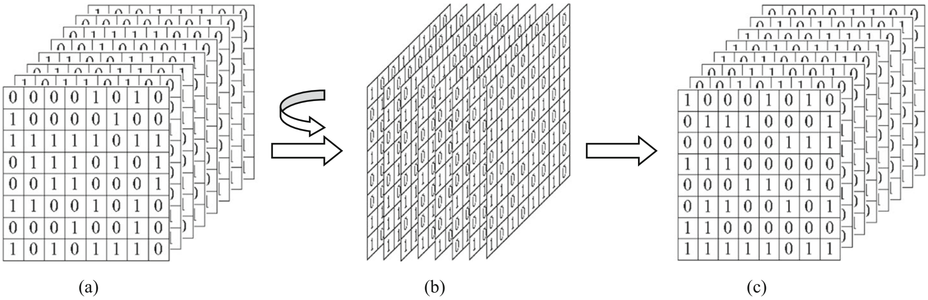


Fig. 2 Block conversion. **a** The bit planes of the original block; **b** the rotated bit planes; **c** another representation of (b)

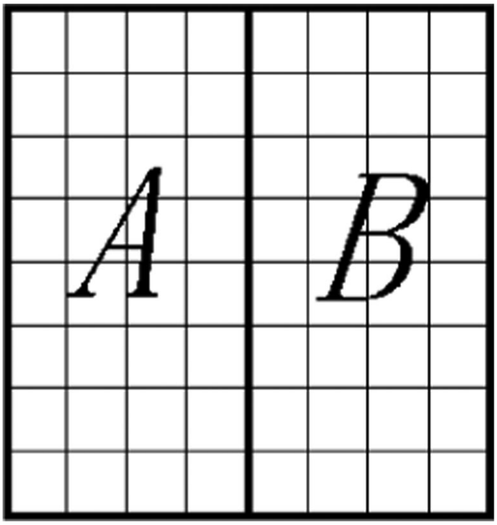


Fig. 3 The division of the converted block

Step 4: According to H, rearrange the 32 elements of A and B in the same way to obtain A' and B'. That is, move the kth ($k \in [1, 32]$) element of A and B into the h_kth position to form the permuted matrixesA' and B'. In this way, the orders of the 32 rearranged elements in A' and B' are identical to each other. Then, exchange A' and B' to form the encrypted converted block.

Step 5: Convert the block into reverse to restore its original state.

2.2 Watermarking

Assuming that the original image is a grey level image of size 512 × 512, and the actual watermark is a binary image of size 256 × 256. Let each block of size be 8 × 8 in the original image corresponding to the block of size 4 × 4 in the actual watermark that locates at the same relative position. The watermarking steps are:

Step 1: Convert the block as shown in Fig. 2.

Step 2: Compute f or f for each converted block from (2) or (3):

$$f = \left(A \cdot B^T\right) \mathrm{mod} 2^{16} \tag{2}$$

$$f' = \left(A' \cdot B'^T\right) \mathrm{mod} 2^{16} \tag{3}$$

where "·" denotes the inner product, x^T denotes the transposed x. If the image block was not encrypted before, f is computed from (2); else, f is computed from (3). After that, transform f or f into binary form and split it to obtain 16 IDW bits of the block.

Step 3: Perform the XOR operation between the 16 IDW bits and the 16 pixels of the corresponding block in the actual watermark one to one to obtain the zero watermark.

Step 4: Convert the block into reverse to restore its original state.

It is noted that the watermarking will not make any changes to the original image or the encrypted image due to the fact that the watermark information is stored outside of the image.

2.3 Image decryption

Image decryption is also performed on the converted blocks. According to the decryption key which is the same as the encryption key, the encrypted matrixes A' and B' can be easily restored to their initial state A and B. The procedure is similar to that of image encryption. Thus, the image can be decrypted.

2.4 Watermark detection

To detect the watermark of the encrypted or decrypted image, the value f or f' should be firstly computed from (2) or (3) to obtain the extracted IDW, then, execute XOR operation between the extracted IDW and the zero-watermark bit by bit to obtain the extracted watermark, as shown in Fig. 1.

3 Proof and experiments

3.1 Proof of the commutativity

Based on the presentation above, one can observe that the commutativity of the proposed scheme is equipped if and only if $f=f'$, which are obtained from (2) and (3) respectively.

Proposition 1 Suppose that the two matrixes A and B are both sized $r \times s$, rearranged as A' and B' of size $r \times s$, in which the orders of the rearranged elements are identical with each other. Define:

$$\begin{cases} f = A \cdot B^T \\ f' = A' \cdot B'^T \end{cases} \tag{4}$$

where"·" denotes the inner product, x^T denotes the transposed x. Then, $f=f'$.

Proof Let $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1s} \\ a_{21} & a_{22} & \cdots & a_{2s} \\ \vdots & \vdots & & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rs} \end{bmatrix}$, $B = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1s} \\ b_{21} & b_{22} & \cdots & b_{2s} \\ \vdots & \vdots & & \vdots \\ b_{r1} & b_{r2} & \cdots & b_{rs} \end{bmatrix}$, then

$f = A \cdot B^T = \sum_{i=1}^{r} \sum_{j=1}^{s} a_{i,j} b_{j,i}$. Similarly, $f' = A' \cdot B'^T = \sum_{i=1}^{r} \sum_{j=1}^{s} a'_{i,j} b'_{j,i}$.

Since the rearrangement of A and B are identical with each other, we have $a_{i,j} = a'_{i',j'}$ and $b_{j,i} = b'_{j',i'}$, where the coordinates (i',j') in A' or B' denote the rearranged position of (i,j) in A or B. Thus, $a_{i,j}b_{j,i} = a'_{i',j'}b'_{j',i'}$.

For $\sum\limits_{i'=1}^{r}\sum\limits_{j'=1}^{s} a'_{i',j'}b'_{j',i'} = \sum\limits_{i=1}^{r}\sum\limits_{j=1}^{s} a'_{i,j}b'_{j,i}$, we obtain

$$f' = \sum_{i=1}^{r}\sum_{j=1}^{s} a'_{i,j}b'_{j,i} = \sum_{i'=1}^{r}\sum_{j'=1}^{s} a'_{i',j'}b'_{j',i'} = \sum_{i=1}^{r}\sum_{j=1}^{s} a_{i,j}b_{j,i} = f. \tag{5}$$

3.2 Experiments and comparisons

As shown in Fig. 4, the original image of size 512 × 512 is given in Fig. 4a, and the encrypted image is Fig. 4b. For each divided 8 × 8 block of the original image or the encrypted image, the obtained 16 IDW bits are used to form one 4 × 4 IDW block, thus the IDW can be represented by a binary image of size 256 × 256, whose size is the same as that of the actual watermark. The two IDWs of the original image and the encrypted image are illustrated in Fig. 4c and d, respectively, and they are identical with each other, indicating that the commutativity of image encryption and watermark generation is equipped. Figure 5a shows the decrypted result of Fig. 4b. Fig. 5b gives the extracted IDW from the decrypted Baboon, and it is the same as that obtained directly from the encrypted image or the original image, i.e., Fig. 4d and c. Figure 5c and d show the extracted IDW from Fig. 4b and the decrypted Baboon from Fig. 4b after IDW extraction. Figure 5c and d are the same as Fig. 5b and a respectively, meaning that the commutativity of image decryption and watermark extraction is equipped. To get the zero watermark as shown in Fig. 6b, one should execute XOR between the extracted IDW (Fig. 4c or d) and the actual binary watermark (Fig. 6a). Similarly, by XORing the zero watermark (Fig. 6b) and the extracted IDW (Fig. 5b), the extracted watermark is formed, as given in Fig. 6c.

The security of the encryption is assessed in Fig. 7 and Tables 1 and 2. Fig. 7a and b shows the histograms of the original image Baboon and the encrypted Baboon, i.e., Fig. 4a and b respectively. Clearly, the encrypted result has flat histograms, indicating that there is no meaningful statistical information available in the encrypted image. Table 1 shows the

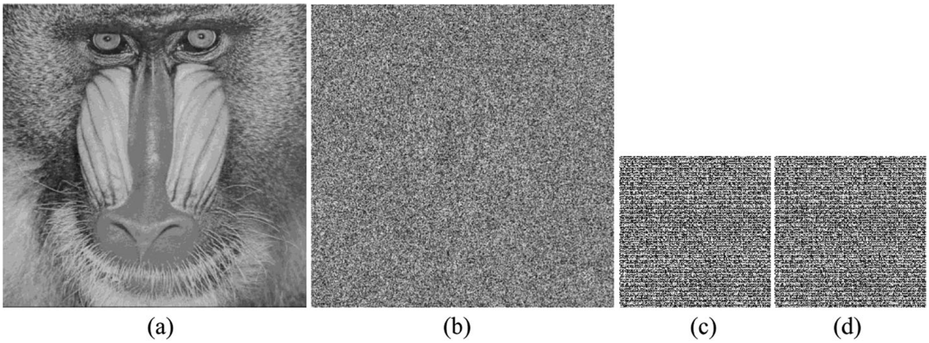

(a) (b) (c) (d)

Fig. 4 Encryption and IDW creation. **a** The original image Baboon; **b** the encrypted image; **c** the IDW of (a); **d** the IDW of (b)

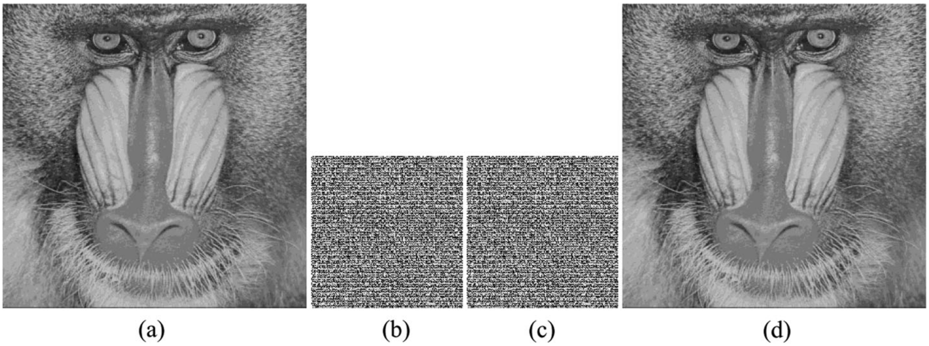


Fig. 5 The decrypted result and the extracted IDW. **a** The decrypted Baboon from Fig. 4b; **b** the extracted IDW from (a); **c** the extracted IDW from Fig. 4b; **d** the decrypted Baboon from Fig. 4b after IDW extraction

correlation coefficients of adjacent pixel pairs of different images in horizontal, vertical and diagonal directions. The ideal correlation coefficients in encrypted images are 0 s. It can be seen that the proposed method shows better encryption performances than [4, 13, 21] in most cases. The information entropy comparison is given in Table 2. The idea information entropy of an encrypted image is 8. The more close to 8, the more random the encrypted image is. It can be seen that the entropies of the proposed method are satisfactory.

If the encrypted or the decrypted image is tampered illegally, the watermark can be used to detect and locate the tampered areas due to the fact that each block of the watermark corresponds to one block of the encrypted or the decrypted image in the same relative position. Figure 8 shows the results of tampered area detection. Figure 8a and b are the decrypted Baboon and encrypted Baboon tampered with the same logo respectively, and Fig. 8c and d are the extracted watermarks from the two tampered imagesrespectively. Figure 8e, g, g and h) show the Bridges images tampered with asymmetric shape and the corresponding watermarks. Figure 8i, j, k and l) show the experimental results on Peppers images using random noise pollution. Figure 8m, n, o and p) show the experimental results on Lena images using rotation attack. It is clear that the tampered area can be detected and located accurately. The noise polluted areas in the extracted watermarks mirror the tampered areas in the original images or the encrypted images.

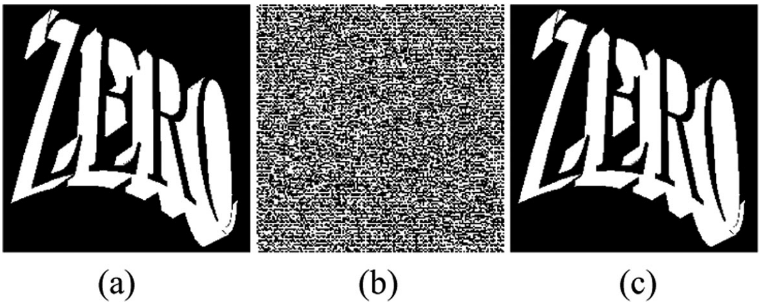


Fig. 6 Actual watermark, zero watermark and extracted watermark. **a** The actual watermark; **b** the zero watermark; **c** the extracted watermark

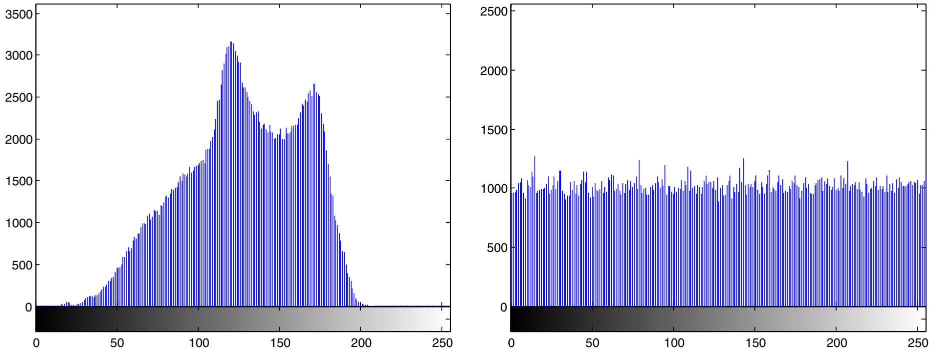


Fig. 7 Histogram comparison. **a** Histogram of Fig. 4a; **b** histogram of Fig. 4b

The functionalities of the proposed method are also compared with other similar works, as shown in Table 3. The compared works include fragile zero-watermarking [6, 19], robustness zero-watermarking [20, 22, 23, 26] and fragile watermarking [1, 3, 14, 15]. The fragile watermarking schemes are common. However, to the best of our knowledge, only two kinds of fragile zero-watermarking are found, one is used for database relations [6], and the other is used for audio signals [19]. There is lack of the one used for digital images. For the robust zero-watermarking schemes, both audio [26] and image [20, 22, 23] can be processed. It can be seen from Table 3 that only the proposed method can be implemented in the encrypted domain. Also, only the proposed method equips commutativity. The tamper detection capability is equipped in most of the schemes, except [26]. And there may exists some undetectable tampered areas in [22, 23]. In the zero-watermarking schemes, including the robust and fragile ones, only the proposed scheme can locate the tampered areas. And the precision of tamper localization of the proposed scheme is the same as that of common fragile watermarking schemes [1, 3, 14, 15], which are all based on blocks.

Table 1 Correlation coefficients ofadjacent pixel pairs in three directions

Image	Direction	Plain Image	Algorithms			
			[21]	[4]	[13]	Proposed
Lena	Horizontal	0.9456	−0.0066	0.0011	0.0058	−0.0057
	Vertical	0.9727	−0.0089	0.0098	0.0015	−0.0014
	Diagonal	0.9213	0.0424	−0.0227	0.0083	0.0059
Peppers	Horizontal	0.9660	0.0194	0.0071	−0.0043	0.0042
	Vertical	0.9738	−0.0091	−0.0065	0.0020	−0.0046
	Diagonal	0.9422	0.0123	−0.0165	−0.0030	0.0061
Bridge	Horizontal	0.9664	0.0023	−0.0339	0.0099	0.0008
	Vertical	0.9344	−0.0187	0.0186	0.0067	0.0009
	Diagonal	0.9110	−0.0225	−0.0001	−0.0106	0.0016
Baboon	Horizontal	0.8066	−0.0164	0.0180	0.0069	−0.0039
	Vertical	0.8507	−0.0181	0.0061	−0.0031	−0.0047
	Diagonal	0.8765	0.0004	−0.0079	0.0132	0.0041

Table 2 Information entropy comparison

Image	Plain image	[21]	[4]	[13]	Proposed
Lena	7.5812	7.9970	7.9038	7.9942	7.9961
Peppers	7.2216	7.9908	7.9057	7.9961	7.9981
Bridge	7.6830	7.9908	7.9017	7.9956	7.9979
Baboon	7.4704	7.9956	7.9009	7.9933	7.9958

4 Conclusion and discussion

In this paper, a novel commutative fragile zero-watermarking and encryption scheme is proposed to meet the requirements of privacy protection and integrity protection of digital images. It has the desired commutativity property not only in image encryption and watermarking, but also in image decryption and watermark detection. Since the zero-watermarking will not cause any modification of the original image or the encrypted image, the quality of the protected image will not be compromised. Our experiments reveal that the illegal modification of the zero-watermarked image can be detected and located accurately, regardless of the tampering appeared on either the decrypted image or the encrypted image. Our future work propositions are given below:

1) Generalization of the proposed scheme. The key problem of the commutative zero-watermarking is that some information of the host image can be computed in the encrypted domain, which is the same as that obtained from the plaintext domain. In other words, the encryption effect can be eliminated to some extent by the processing in encrypted domain. Therefore, other algorithms equipping this property may also be suitable for the processing procedure of this paper. For example, the XOR operation in [28]:

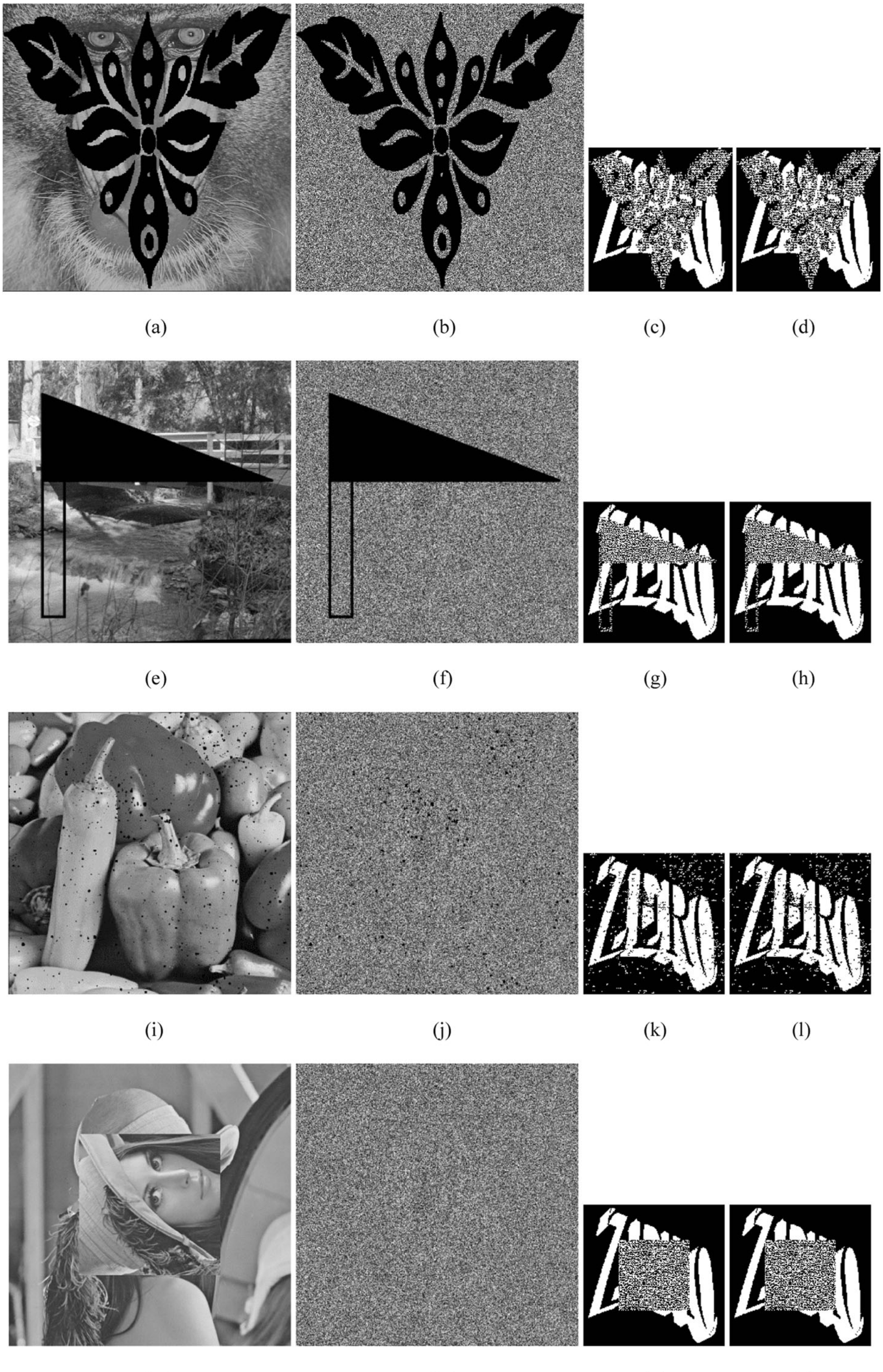
$$c_1 \oplus c_2 = (p_1 \oplus r_1) \oplus (p_2 \oplus r_2) = p_1 \oplus p_2, \text{if } r_1 = r_2,$$

and

$$\begin{aligned}(c_1 + c_2)\text{mod}256 &= ((p_1 + r_1)\text{mod}256 + (p_2 + r_2)\text{mod}256)\text{mod}256 \\ &= (p_1 + p_2)\text{mod}256, \text{if } (r_1 + r_2)\text{mod}256 = 0,\end{aligned}$$

where c_1 and c_2 denote the encrypted pixels, p_1 and p_2 denote the plaintext pixels, and r_1 and r_2 denote the random numbers of the key streams.

Fig. 8 Tampered area detection. **a** The tampered decrypted Baboon with logo; **b** the tampered encrypted Baboon with logo; **c** the extracted watermark from (a); **d** the extracted watermark from (b); **e** The tampered decrypted Bridge with asymmetric shape; **f** the tampered encrypted Bridge with asymmetric shape; **g** the extracted watermark from (e); **h** the extracted watermark from (f). **i** The tampered decrypted Peppers with noise; **j** the tampered encrypted Peppers with noise; **k** the extracted watermark from (i); **l** the extracted watermark from (j); **m** The tampered decrypted Lena with rotation; **n** the tampered encrypted Lena with rotation; **o** the extracted watermark from (m); **p** the extracted watermark from (n) ▶



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

(e) (f) (g) (h)

(i) (j) (k) (l)

(m) (n) (o) (p)

Table 3 Comparison with other works

Scheme	Encrypted domain	Commutative	Tamper detection	Tamper localization	Precision	Type	Application
Proposed	Y	Y	Y	Y	Block	Fragile	Image
[6]	N	N/A	Y	N/A	N/A	Fragile	Database relations
[19]	N	N/A	Y	N/A	N/A	Semi-fragile	Audio
[26]	N	N/A	N	N/A	N/A	Robust	Audio
[22]	N	N/A	Inadequate	N/A	N/A	Robust	Image
[20]	N	N/A	Y	N/A	N/A	Robust	Image
[23]	N	N/A	Inadequate	N/A	N/A	Robust	Image
[14]	N	N/A	Y	Y	Block	Fragile	Image
[15]	N	N/A	Y	Y	Block	Fragile	Image
[1]	N	N/A	Y	Y	Block	Fragile	Image
[3]	N	N/A	Y	Y	Block	Fragile	Image

2) The key novelty of the proposed method can be considered as the commutativity of matrix calculating and matrix permutation, and commutative zero-watermarking and encryption is one kind of application. There are some other potential applications to be developed using the proposed technology, such as image encryption, cryptanalysis, and data hiding in encrypted domain.
3) Our work equips fragility but not robustness. Therefore, common image processing attacks including geometric attacks, cropping, noise, JPEG compression, etc., would be only detected and located, but not resisted. In order to avoid the effect of unintentional attacks, our future work may turn to the design of image zero-watermarking in which both the fragility and robustness are equipped.

Acknowledgements The work was funded by the National Natural Science Foundation of China (Grant Nos. 61602158, 61572089, 61502399, 61772176), the Natural Science Foundation of Chongqing Science and Technology Commission (Grant No. cstc2017jcyjBX0008), the Guangxi Key Laboratory of Trusted Software, the Science and Technology Research Project of Henan Province (182102210374), the Science Foundation for the Excellent Youth Scholars of Henan Normal University (YQ201607) and the Chongqing Postgraduate Education Reform Project (Grant No. yjg183018).

References

1. Bravo-Solorio S, Calderon F, Li CT, Nandi AK (2018) Fast fragile watermark embedding and iterative mechanism with high self-restoration performance. Digital Signal Processing 73:83–92
2. Cancellaro M, Battisti F, Carli M, Boato G, De Natale FGB, Neri A (2011) A commutative digital image watermarking and encryption method in the tree structuredHaar transform domain. Signal Process Image Commun 26(1):1–12
3. Fan M, Wang H (2018) An enhanced fragile watermarking scheme to digital image protection and self-recovery. Signal Process Image Commun 66:19–29

4. Hua Z, Zhou Y, Pun CM, Chen P (2015) 2D Sine Logistic modulation map for image encryption. Inf Sci 297:80–94
5. Jiang L, Xu Z, Xu Y (2014) Commutative encryption and watermarking based on orthogonal decomposition. Multimed Tools Appl 70(3):1617–1635
6. Khan A, Husain SA (2013) A fragile zero watermarking scheme to detect and characterize malicious modifications in database relations. Sci World J 2013:796726
7. Lian S (2009) Quasi-commutative watermarking and encryption for secure media content distribution. Multimed Tools Appl 43(1):91–107
8. Liu S, Hennelly BM, Guo C, Sheridan JT (2015) Robustness of double random phase encoding spread-space spread-spectrum watermarking technique. Signal Process 109(43):345–361
9. Liu Y, Tian S, Hu W, Xing C (2012) Design and statistical analysis of a new chaotic block cipher for wireless sensor networks. Commun Nonlinear Sci Numer Simul 17(8):3267–3278
10. Liu X, Zhao R, Li F, Liao S, Ding Y, Zou B (2017) Novel robust zero-watermarking scheme for digital rights management of 3D videos. Signal Process Image Commun 54:140–151
11. Liu Y, Zhu Y, Xin G (2015) A zero-watermarking algorithm based on merging features of sentences for chinese text. J Chin Inst Eng 38(3):391–398
12. Ma K, Zhang W, Zhao X, Yu N, Li F (2013) Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption. IEEE Transactions on Information Forensics and Security 8(3):553–562
13. Mondal B, Kumar P, Singh S (2018) A chaotic permutation and diffusion based image encryption algorithm for secure communications. Multimed Tools Appl 77(23):31177–31198
14. Nazari M, Sharif A, Mollaeefar M (2017) An improved method for digital image fragile watermarking based on chaotic maps. Multimed Tools Appl 76(15):16107–16123
15. Qin C, Ji P, Zhang X, Dong J, Wang J (2017) Fragile image watermarking with pixel-wise recovery based on overlapping embedding strategy. Signal Process 138:280–293
16. Savelonas MA, Chountasis S (2010) Noise-resistant watermarking in the fractional fourier domain utilizing moment-based image representation. Signal Process 90(8):2521–2528
17. Simitopoulos D, Zissis N, Georgiadis P, Emmanouilidis V, Strintzis MG (2003) Encryption and watermarking for the secure distribution of copyrighted MPEG video on DVD. Multimedia Systems 9(3):217–227
18. Subramanyam A, Emmanuel S, Kankanhalli MS (2012) Robust watermarking of compressed and encrypted JPEG2000 images. IEEE Transactions on Multimedia 14(3):703–716
19. Tang X, Ma Z, Niu X, Yang Y (2015) Compressive sensing-based audio semi-fragile zero-watermarking algorithm. Chin J Electron 24(3):492–497
20. Thanh TM, Tanaka K (2017) An image zero-watermarking algorithm based on the encryption of visual map feature with watermark information. Multimed Tools Appl 76(11):13455–13471
21. Wang X, Liu L, Zhang Y (2015) A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt Lasers Eng 66:10–18
22. Wang CP, Wang XY, Chen XJ, Zhang C (2017) Robust zero-watermarking algorithm based on polar complex exponential transform and logistic mapping. Multimed Tools Appl 76(24):26355–26376
23. Wang C, Wang X, Xia Z, Zhang C (2019) Ternary radial harmonic Fourier moments based robust stereo image zero-watermarking algorithm. Inf Sci 470:109–120
24. Xiang L, Li Y, Hao W, Yang P, Shen X (2018) Reversible natural language watermarking using synonym substitution and arithmetic coding. Computers, Materials and Continua (CMC) 55(3):541–559
25. Yang C, Luo X, Lu J, Liu F (2018) Extracting hidden messages of MLSB steganography based on optimal stego subset. Science China Inf Sci 61(11):119103
26. Yu Y, Lei M, Liu X, Qu Z, Wang C (2016) Novel zero-watermarking scheme based on DWT-DCT. China Communications 13(7):122–126
27. Zhang X (2012) Separable reversible data hiding in encrypted image. IEEE Transactions on Information Forensics and Security 7(2):826–832
28. Zhang X (2013) Commutative reversible data hiding and encryption. Security and Communication Networks 6(11):1396–1403

Ming Li received the Master's degree in Science from College of Physics and Information Engineering, Henan Normal University, Henan, China in 2010. He received the Ph. D. degree from College of Computer Science of Chongqing University, Chongqing, China in 2014. Currently, he is an associate professor at College of Computer and Information Engineering, Henan Normal University, China. His research interests include multimedia security, information hiding, and compressive sensing.

Di Xiao received the Ph. D. degree in computer software and theory from Chongqing University, Chongqing, China in 2005. From 2006 to 2008, he has done postdoctoral research at Chongqing University. From 2008 to 2009, he has been a visiting scholar funded by the Chinese government at the Department of Computer Science, New Jersey Institute of Technology, USA. Currently, he is a professor at College of Computer Science, Chongqing University, China. His research interests include image processing, chaos based cryptography, image and graphics watermarking, etc. He is a member of IEEE and ACM. More than 80 academic papers have been published since 2000.

Ye Zhu received his Ph.D. degree in Artificial Intelligence with a Mollie Holman Medal for the best doctoral thesis of the year from Monash University in 2017. He is a lecturer with the School of Information Technology, Deakin University, Australia. He joined Deakin University in 2017 as a research fellow of complex system data analytics. His research works focus on clustering analysis, anomaly detection, and their applications for pattern recognition and information retrieval.

Yushu Zhang received the Ph.D. Degree from the College of Computer Science, Chongqing University, Chongqing, China, in Dec. 2014. He has held various research positions at Southwest University, City University of Hong Kong, University of Macau, and Deakin University. He is now a Professor with College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, China. His research interests include multimedia security, compressive sensing security, cloud computing and big data security. He has published over 70 refereed journal articles and conference papers in these areas.

Lin Sun is currently an Associate Professor at the College of Computer and Information Engineering, Henan Normal University, China. He received B.Sc. and M.S. degrees in Computer Science and Technology from Henan Normal University in 2003 and 2007, respectively, and a Ph.D. degree in Pattern Recognition and Intelligent Systems from Beijing University of Technology in 2015. He has authored or co-authored over 70 articles. His main research interests include medical image processing, intelligent information processing, and data mining. He has served as a reviewer for several prestigious peer-reviewed international journals.