Available online at www.sciencedirect.com
ScienceDirect
Forensic Science International 179 (2008) 54–62
Forensic Science International
www.elsevier.com/locate/forsciint

Pinpoint authentication watermarking based on a chaotic system

Rongrong Ni *, Qiuqi Ruan, Yao Zhao

Institute of Information Science, Beijing Jiaotong University, Beijing 100044, China

Received 26 August 2006; received in revised form 16 April 2008; accepted 17 April 2008

Abstract

Watermarking technique is one of the active research fields in recent ten years, which can be used in copyright management, content authentication, and so on. For the authentication watermarking, tamper localization and detection accuracy are two important performances. However, most methods in literature cannot obtain precise localization. In addition, few researchers pay attention to the problem of detection accuracy. In this paper, a pinpoint authentication watermarking is proposed based on a chaotic system, which is sensitive to the initial value. The approach can not only exactly localize the malicious manipulations but reveal block substitutions when Holliman–Memon attack (VQ attack) occurs. An image is partitioned into non-overlapped regions according to the requirement on precision. In each region, a chaotic model is iteratively applied to produce the chaotic sequences based on the initial values, which are determined by combining the prominent luminance values of pixels, position information and an image key. Subsequently, an authentication watermark is constructed using the binary chaotic sequences and embedded in the embedding space. At the receiver, a detector extracts the watermark and localizes the tampered regions without access to the host image or the original watermark. The precision of spatial localization can attain to one pixel, which is valuable to the images observed at non-ordinary distance, such as medical images and military images. The detection accuracy rate is defined and analyzed to present the probability of a detector making right decisions. Experimental results demonstrate the effectiveness and advantages of our algorithm.

Keywords: Image authentication; Localization precision; Detection accuracy rate; Chaotic system

1. Introduction

Development of the Internet and digital multimedia provides us great advantages. People can easily get lossless digital media by copy or download operations, and arbitrarily change them using multimedia edit tools. As a result, when we achieve an image, two things are naturally raised: Who has created it? And is the image true? To answer these two questions, two kinds of research branches and applications in digital watermarking arise [1]: copyright management and integrity authentication. Applications of copyright management [2] include copyright protection and digital fingerprinting, which protect the owner's intellectual property or trace the source of the illegal copies. Researches on integrity authentication aim to verify the authenticity of the media [3]. That is, the detection result can decide if the medium has been altered or not, furthermore localize the tampered regions. In this paper, we focus on the authentication watermarking techniques.

In general, watermarking techniques used for integrity authentication have the following properties [4]:

- *Tamper detection*: This is the fundamental feature to a tamper-proofing system, in the sense that the detector in the system should determine whether an image is authentic.
- *Localization of modification*: The extraction and verification result should be able to reflect and locate the modification regions.
- *Perceptual transparency*: An embedded watermark should be perceptually invisible under normal observation.
- *Blind detection*: The authentication process does not require the host image. Furthermore, some schemes do not need the original watermark.
- *Robust or fragile property*: Most fragile and semi-fragile algorithms aim to detect the malicious tamper operations. However, robust schemes can also serve this purpose [5].
- *Security*: The marking key spaces should be large enough to promise the security of watermarking.

* Corresponding author. Tel.: +86 10 51683695.
E-mail address: rrni@bjtu.edu.cn (R. Ni).

0379-0738/$ – see front matter.
doi:10.1016/j.forsciint.2008.04.016

As for some kinds of images, such as military images, remotely sensing images, and medical images and so on, it is desired to differ the believable regions from the tampered regions very subtly. For example, the objects or military equipments are perhaps small parts in the remotely military images. Another example is that an early cancer region in medical images is possibly shown as a small point. At this circumstance, a remote receiver should authenticate the integrity of the image, and decide its availability later. However, few literatures pay attention to precise localization watermarking, or they easily fail to verify the authenticity. Walton et al. [6] divided an image into 8×8 blocks and embedded the checksum in the LSB of each block. His algorithm can only locate 8×8 regions. In addition, if the blocks with the same position are exchanged between two different images, the detector cannot give right result. Yeung and Mintzer [7] made use of a look-up table (LUT) to embed a watermark. But the accuracy is not expected and extern memory is needed for LUT. Wu et al. designed a LUT for DCT coefficients to embed a binary watermark [8]. Their scheme has the same shortcomings as [7]. Fridrich proposed a robust watermarking method to detect alterations [5], which can only locate the blocks with size 64×64. Moreover, most block-based algorithms are vulnerable to the vector quantization (VQ) attack proposed by Holliman and Memon [9], which uses block-wise independence to counterfeit a collage image. Recently Celik et al. proposed a hierarchical watermarking [10,11], which used the lowest level to guarantee the capability of localization and employed a high level to resist VQ attack. However, using digital signature to produce the watermark affects the block size and the precision of tampering localization. Wu et al. presented a pixel-level method to achieve the precise localization, in which the change of one pixel value affected its neighboring pixels [12]. But, the application of shuffle resulted in the spread of tampering marks. Up to now, few literatures study the problem of detection accuracy in details, which is caused by the limited precision of digitals.

In this paper, we propose an authentication watermarking based on a chaotic system, which can exactly locate the tampered regions according to the requirement on precision. An image is divided into non-overlapped regions. Using a chaotic system, an authentication watermark of each region is produced based on the prominent intensity values, position information and the image key. Then, the generated watermark is embedded into the embedding space of the region. During detection, a detector generates a reference signal and compares it with the extracted watermark to authenticate the integrity and locate the possible tampered regions. This is done without access to the host image or the original watermark. The detection accuracy rate is proposed to analyze the probability of a detector making right decisions. Experiments show that this algorithm can flexibly localize the tampered parts, and the detection accuracy rate is proved right.

The rest of the paper is organized as follows. In Section 2, the proposed scheme is described in details. The analysis to the properties is discussed in Section 3. The experimental results are given in Section 4. The paper is concluded in Section 5.

2. Proposed scheme

Generally, an image is displayed in a 2-dimension plane, such as Fig. 1(a). hAxis represents the horizontal orientation, and vAxis means the vertical orientation. If the intensity value of pixels is regarded as the third orientation, a 2-dimension image can be shown in a 3-dimension mesh (Fig. 1(b)). The axis of intensity is denoted as gAxis, which is vertical to the plane hAxis–vAxis.

2.1. Embedding of the authentication watermark

Assume that an original image X with size $M \times N$ is the host image. The image segmentation is executed on the plane hAxis–vAxis, while the orientation of gAxis is regarded as the embedding depth. The watermark embedding process consists of four steps:

Step 1. Segment an image.

The image is segmented to non-overlapped blocks with size $p \times q$, and the rth image region is noted as X_r, $r = 1, 2,$

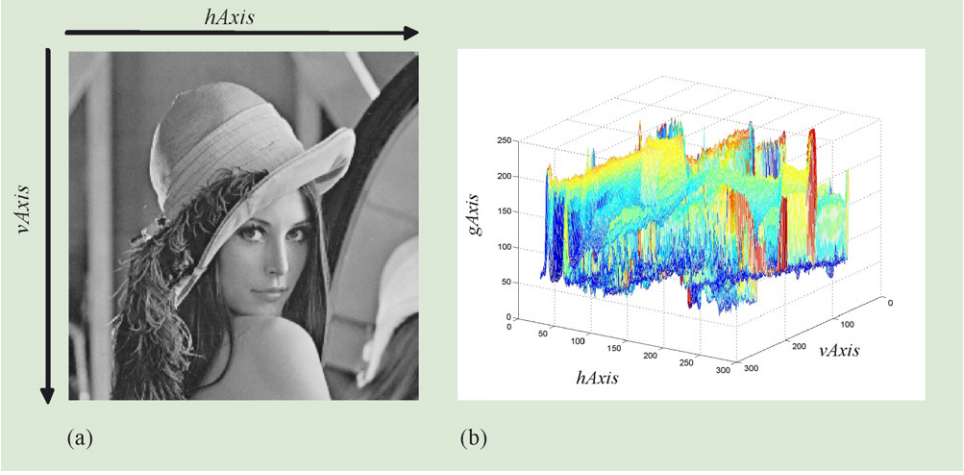

Fig. 1. An image is shown in a 3-dimension mesh. (a) Lena and (b) 3-dimension representation of Lena.

$\ldots(M \times N)/(p \times q)$. In each region, set the watermark embedding depth l, which further determines the embedding space, i.e., all bit-planes lower than the embedding depth. Thus the length of embedding space L equals $l \times p \times q$.

Step 2. Acquire the initial value for a chaotic system.

The regions with different pixels or positions should produce different chaotic sequences. In addition, the regions with same pixels and positions but in different images should also generate different chaotic sequences. These requirements can be satisfied based on different initial values because a chaotic system is highly sensitive to its initial value.

A general chaotic model is described by the equation below,

$$x_{n+1} = f(x_n) \tag{1}$$

where $f(\cdot)$ can be realized by iteration equations, non-linear equations, and partial differential equations, etc. This equation is iteratively executed to produce a chaotic sequence. When the parameters in $f(\cdot)$ satisfy a certain requirements, a sequence in chaotic status will be achieved.

In this paper, a hybrid optical bistable chaotic system is used [13],

$$x_{n+1} = 4\sin^2(x_n - 2.5) \tag{2}$$

In each region, the authentication watermark is produced mainly according to the prominent values of the pixels. An image region X_r contains $p \times q$ pixels, denoted as $s(k)$, $k = 1, 2, \ldots, pq$. These pq pixels are input to a chaotic system, respectively, and produce pq chaotic sequences.

For each pixel, an initial value is determined based on its prominent intensity value, the position index, and the image protection key. Then, the initial value is input to the chaotic system to execute G-time iterations. G is larger than L.

The variable pos represents the position index of an image pixel. The image protection key is represented in a numerical form nkey. Thus, an initial value is,

$$c(k,0) = a \times \left\lfloor \frac{s(k)}{2^l} \right\rfloor \times 2^l + b \times \mathrm{pos} + c \times \mathrm{nkey} \tag{3}$$

where a, b and c are predefined constants. The introduction of the position information and the protection key prevents the VQ attack.

Step 3. Calculate the chaotic sequences and corresponding binary watermark.

A chaotic sequence is generated by substituting $c(k,0)$ for x_n in Eq. (2) and performing G iterations. After the last pixel in $s(k)$ is processed, pq chaotic sequences are achieved.

For the kth pixel, the produced sequence can be expressed as $C_k = \{c(k,g),\ g = 1, 2, \ldots, G\}$, in which the components are float numbers. Because they cannot be directly applied in our scheme, it is necessary to convert them to binary values. Thus, a binary sequence $W_k = \{w(k,g),\ g = 1, 2, \ldots, G\}$ is generated. In details, If $c(k,g)$ is larger than a threshold T, set $w(k,g)$ as 1; otherwise, set $w(k,g)$ as 0. The converting process is shown in Eq. (4).

$$w(k,g) = \begin{cases} 1, & c(k,g) > T \\ 0, & \text{Otherwise} \end{cases} \tag{4}$$

where T is set to 8/3 based on a number of tests to attain approximately equal numbers of '0' and '1'. Whereafter, the elements with the same position are processed using XOR operation. Therefore, pq sequences W_k are combined to one sequence $W_o = \{w_o(g),\ g = 1, 2, \ldots, G\}$. That is,

$$w_o(g) = c(1,g) \oplus c(2,g) \oplus \cdots \oplus c(k,g) \oplus \cdots \oplus c(pq,g) \tag{5}$$

Since the length of embedding space is L and the size of W_o is G, a mapping function $M(\cdot)$ is applied to obtain a watermark W with an appropriate size. The mapping function M: $V_G \rightarrow V_L$ converts G-dimensional space to L-dimensional space by exclusive-or operations.

Step 4. Embed the watermark.

Replace the bits in the embedding space with the authentication watermark. In this way, a new watermarked region is obtained. When all the regions are operated, a new image $\tilde{X}$ containing the watermark is produced.

The embedding process is shown in Fig. 2.

2.2. Extraction and authentication process

Read the bit-planes in the embedding space to extract the watermark. Integrity authentication is completed by comparing the extracted watermark and the reference sequence produced

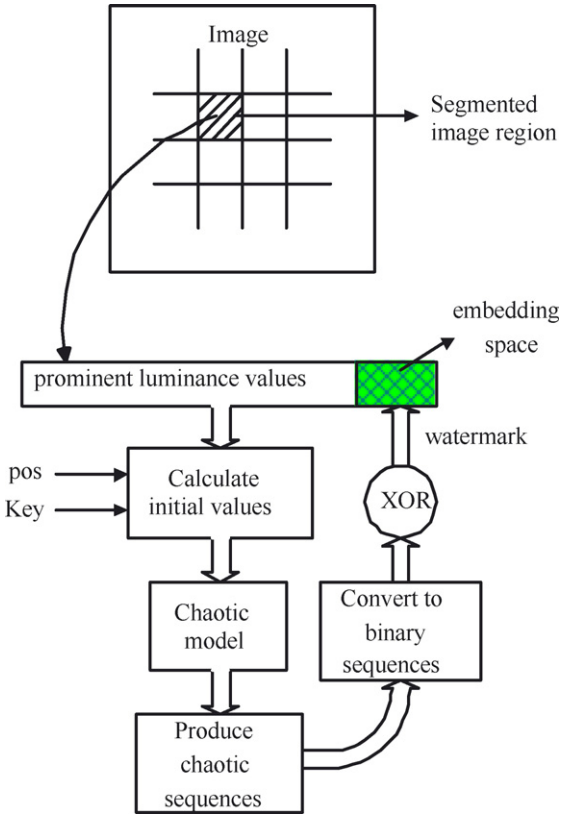

Fig. 2. Watermark embedding process.

using the watermark construction method in the embedding process. If the extracted watermark is equal to the produced sequence, the region is considered as a non-tampered one. Otherwise, the region is tampered. The extraction and authentication process is exactly blind because both the original image and the original watermark are not required. The comparison result is shown as an error image, which can reflect the tampered position intuitively.

The authentication process is comprised of three steps:

Step 1. Segment a suspicious image to non-overlapped regions with size $p \times q$. In each region, read the bits in the embedding space, and denote the extracted signal as $\tilde{W}$.

Step 2. Chaotic sequences and corresponding binary sequences are generated based on the pixels' prominent luminance values, the position information and the protection key. Subsequently, XOR is operated to the G-dimensional binary sequences, and mapping function $M(\cdot)$ is applied to achieve an L-dimensional reference sequence W_s. The details are the same as the watermark construction during embedding process.

Step 3. Compare the extracted $\tilde{W}$ and the produced W_s to get an error image. When $\tilde{W}$ is equal to W_s, denote the corresponding region in the error image as 0 (shown in black); otherwise, denote the corresponding region in the error image as 1 (shown in white). In this way, the error image can reflect the tampered positions intuitively.

The authentication process is sensitive to the changes in the image, which is important to the applications that require high quality images, like the fields of medicine and military affairs.

The authentication process is shown in Fig. 3.

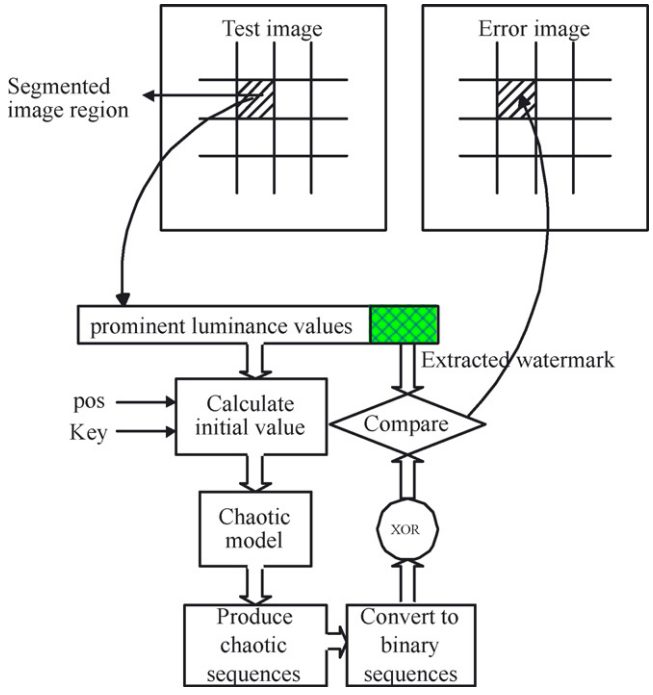

Fig. 3. Integrity authentication process.

3. Analysis to the properties and discussions

3.1. Analysis to detection accuracy rate

No matter how different the produced chaotic sequences are, their destinations are binary sequences containing 0 and 1. Because of the finite precision some different sequences may transform to a same binary sequence, which induces a wrong detection. We find that detection accuracy is relative with the size of embedding space L, i.e., the number of bits used to embed the authentication watermark in one region. Take one bit for example, i.e., $L = 1$. Fig. 4 shows all possible permutations and combinations. The extracted watermark and the produced binary sequence have $2^L = 2^1 = 2$ possible values, respectively, and they have $2^{2L} = 2^2 = 4$ combinations.

During the authentication process, the detector compares the extracted watermark and the produced reference sequence. If they are different, the detector regards the region is tampered. If they are same, the detector will decide the region is not tampered, shown as the parallel lines in Fig. 4. But in fact, there is only one parallel line containing the right decision. For example (Fig. 5), when the true watermark is "0", the parallel line connecting "1" and "1" should induce a wrong detection. Moreover, the parallel line between "0" and "0" may contain a wrong detection, which corresponds to the case that the changed luminance values produce a binary value "0". Therefore, even if tamper operations occur, the reference signal may just equal the extracted signal, which results in a wrong decision. The reason of the error is the limited precision. When the prominent values of the pixels are fed to the chaotic model and post-processed to a binary bit stream, it is possible to produce the same stream as that in low bit planes of the pixels. The probability of the very same is relative with the length of the bit stream, i.e., the size of the embedding space. Let p_e be the probability of the very same, and suppose $p_e = 1/2^L$.

The assumption is based on a number of tests. For the unwatermarked images, the prominent values of the pixels are processed using the same chaotic system to achieve a stream of bits, which is then compared with the stream in low bit planes. Take $L = 1$ for example, we conducted the tests on 500 natural

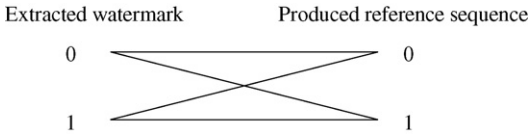

Fig. 4. Possible permutations and combinations ($L = 1$).

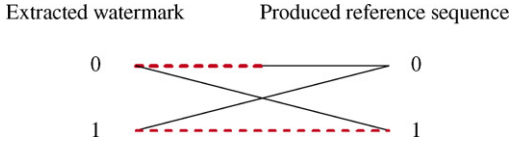

Fig. 5. Possible permutations and combinations ($L = 1$). When the true watermark is "0", real lines mean right decisions, and dashed lines mean wrong decisions.

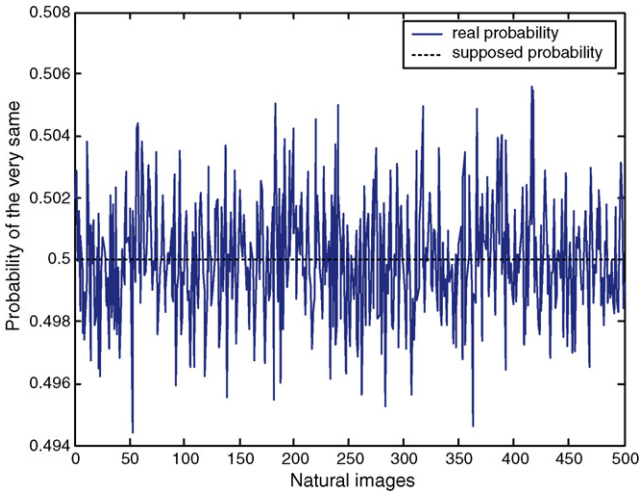

Fig. 6. Probability of the very same when $L = 1$.

images, and computed the probability of the very same. As shown in Fig. 6, the dashed line is equal to the supposed probability 1/2, and the curve is the real probability. The maximum bias is equal to 0.0056.

Define DAR (Detection Accuracy Rate) as the probability of making right decisions by the detector. Detection accuracy rate of the non-tampered regions is different from that of the tampered regions. Use $\mathrm{DAR_{nt}}$ to denote the detection accuracy rate of the non-tampered regions; and use $\mathrm{DAR_t}$ to denote the detection accuracy rate of the tampered regions. While DAR expresses the detection accuracy rate of the whole image.

Thus,

$$\begin{aligned}\mathrm{DAR_{nt}} &= P(\text{no tamper in detection}|\text{no tamper in reality}) \\ &= \frac{P(\text{no tamper in detection, no tamper in reality})}{P(\text{no tamper in reality})} \\ &= \frac{1/2^{2L}\cdot(1-p_e)}{1/2^{2L}\cdot(1-p_e)} = 1\end{aligned} \tag{6}$$

Therefore, the non-tampered regions in the image can be detected accurately.

As for the tampered regions, when the extracted watermark is different from the produced reference value, the detector will give a right decision, corresponding to the bias lines in Fig. 5. That is, the bias lines correspond to the right decisions, having probability of $(2^{2L}-2^L)/2^{2L}$. When the extracted watermark is the same as the produced reference value, the detector will decide that it is not tampered. At this circumstance, the decisions are wrong, corresponding to (2^L-1) parallel lines and a part of another parallel line. Thus,

$$\begin{aligned}\mathrm{DAR_t} &= P(\text{tamper in detection}|\text{tamper in reality}) \\ &= \frac{P(\text{tamper in detection, tamper in reality})}{P(\text{tamper in reality})} \\ &= \frac{(2^{2L}-2^L)/2^{2L}}{(2^{2L}-1)/2^{2L}+1/2^{2L}\cdot p_e} \\ &= \frac{2^{2L}-2^L}{2^{2L}+p_e-1} = \frac{2^{2L}-2^L}{2^{2L}+1/2^L-1} = \frac{2^{3L}-2^{2L}}{2^{3L}-2^L+1}\end{aligned} \tag{7}$$

For the entire image, DAR can be computed as the ratio between the number of accurately detected regions and the number of total regions. While the number of regions detected accurately is the sum of that both in non-tampered and tampered part. Suppose the number of tampered regions is N_t, and the number of total regions is M_t. Thus,

$$\begin{aligned}\mathrm{DAR} &= \frac{\text{number of regions detected accuartely}}{\text{number of total regions}} \\ &= \frac{(M_t-N_t)\cdot \mathrm{DAR_{nt}} + N_t\cdot \mathrm{DAR_t}}{M_t} \\ &= \frac{(M_t-N_t)\cdot 1 + N_t\cdot \mathrm{DAR_t}}{M_t} \\ &= \frac{M_t - N_t + N_t\cdot(2^{3L}-2^{2L})/(2^{3L}-2^L+1)}{M_t}\end{aligned} \tag{8}$$

For instance, for a 256×256 image, set the size of the region as 1×1 pixel and the embedding depth as 1 bit. When N_t is 64, DAR is equal to 99.95%; when N_t is 256, DAR is equal to 99.83%.

3.2. Improvement on the accuracy

To improve the accuracy of detection, we can increase the length of embedding space, which is determined by the embedding depth and the size of image regions. Therefore, two approaches help increase the detection accuracy. The first approach is to reduce the transparency while keeping the localization precision. The second approach is to expand the image region while keeping the transparency.

For example, if the localization precision is maintained as 1×1 pixel, more low bit-planes can be chosen to embed the authentication watermark. This improvement on accuracy impairs the image transparency. When two bit-planes are used as embedding space, i.e., $L = 2$. Fig. 7 shows all the possible permutations and combinations. The extracted watermark and the produced binary reference sequence both have $2^L = 2^2 = 4$ possible values, and they have $2^{2L} = 2^4 = 16$ combinations. Similarly, there is only one parallel line containing the right decision when the extracted watermark equals the reference sequence. That the extracted watermark is different from the reference sequence means tamper operations and right decisions.

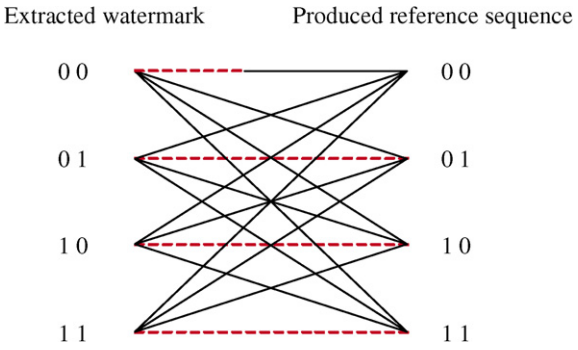

Fig. 7. Possible permutations and combinations ($L = 2$). When the true watermark is "00", real lines mean right decisions, and dashed lines mean wrong decisions.

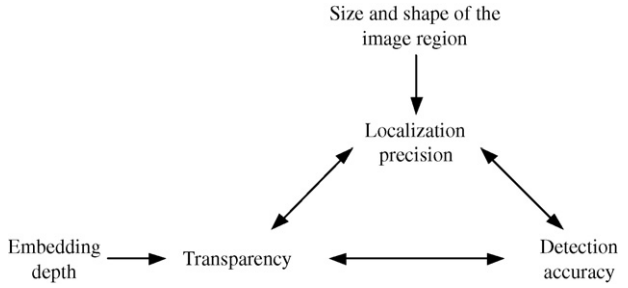

Fig. 8. Relationship among transparency, localization precision and detection accuracy.

In Fig. 7, when the true watermark is "00", the parallel lines concerning "01", "10" and "11" should induce wrong detections. Moreover, the parallel line between "00" and "00" also contains a wrong detection. Hence, the real lines mean right decisions, and the dashed lines mean wrong decisions.

In this case, for a 256 × 256 image, when N_t is 64, DAR is equal to 99.98%; when N_t is 256, DAR is equal to 99.92%. It is obvious that the accuracy of detection is increased.

3.3. Relationship among transparency, localization precision and detection accuracy

The size and shape of the image region directly decides the localization precision; the embedding depth directly decides the image transparency. The above two factors affect the embedding space together, then decide the detection accuracy rate.

Accordingly, transparency, localization precision and detection accuracy are relative each other, as shown in Fig. 8. If the transparency is preserved, small image regions are required to achieve high localization precision, which will decrease the detection accuracy. If the localization precision is preserved, short embedding depth is required to attain high transparency, which will diminish the detection accuracy. If the detection accuracy is preserved, the embedding space will be maintained. In this case, when small image regions are preferred to get high precision of localization, the embedding depth is required to be expanded. As a result, the transparency decreases.

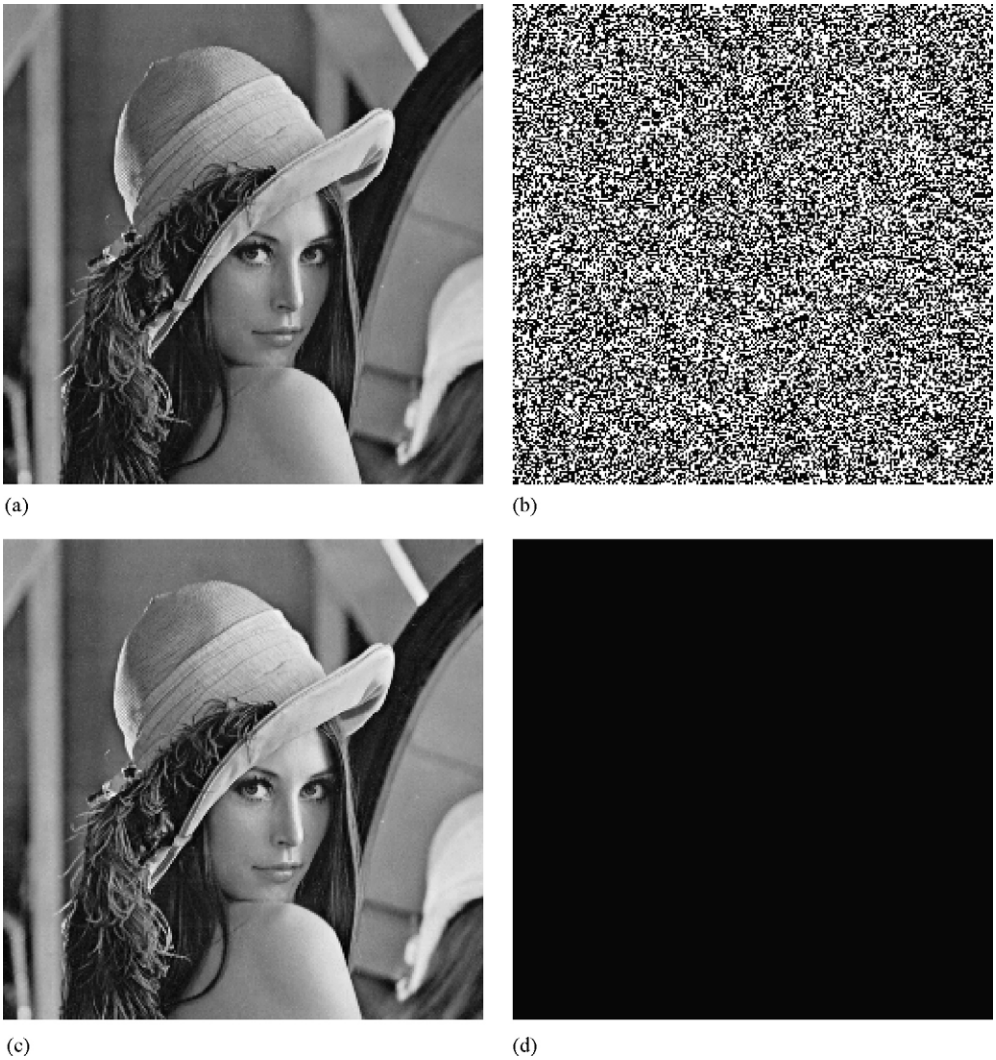

Fig. 9. Embedding of watermark and authentication process without tampering. (a) Original Lena, (b) watermark, (c) watermarked Lena, (d) error image.

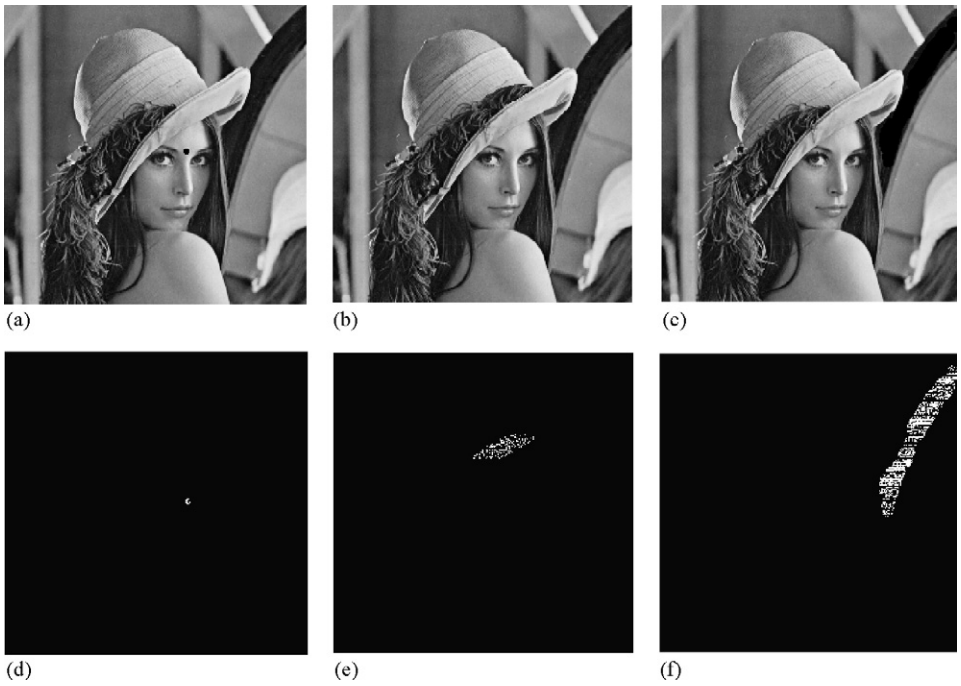

Fig. 10. Tampered results of Fig. 9(c) and corresponding error images. Images on top are tampered versions, and images at bottom are corresponding error images. (a) Tampered Lena (Lena's face has changes), (b) tampered Lena (the hat has changes), (c) tampered Lena (the background has changes), (d) error image of (a), (e) error image of (b) and (f) error image of (c).

4. Experiments

An image ''Lena'' with size 256×256 is the original image to be protected, shown in Fig. 9(a). When the image region is 1×1 pixel and the embedding depth is 1 bit, the embedding space L is equal to 1 bit. Fig. 9(b) is the produced authentication watermark, in which white points represent ''1''s and black points represent ''0''s. Fig. 9(c) is the watermarked ''Lena'', whose *PSNR* with the original image is 51.19 dB. Fig. 9(d) is the error image between the extracted watermark and the produced reference sequence when no tampering occurs.

Fig. 11. Watermarked Lena when the embedding space equals 2 bits.

When the watermarked image is tampered, the error image can show the changes intuitively. In Fig. 10, images on the top row are tampered versions of Fig. 9(c), and images at bottom are corresponding error images. In Fig. 10(a), some black points are added on Lena's face, and the detection result is given in Fig. 10(d). In Fig. 10(b), the attacker cuts some decoration on Lena's hat and pastes it on the other place of the hat. The detection result can reveal the tamper operation, as shown in Fig. 10(e). In Fig. 10(c), some parts of the image are tampered by directly changing the content in the background. The detection result is given in Fig. 10(f).

The detector can find the changes difficult to be discovered by human eyes, such as Fig. 10(b) and (c). However, the decisions are not absolutely right as discussed in Section 3.1. The tampering marks in the error images are not entirely white, but black and white. It is because that some tamper operations are not detected, or some tampered pixel values are just the same as the watermarked ones.

When the precision of localization is fixed, the detection accuracy rate can be improved by adding the embedding depth to increase the embedding space. Let $L = 2$, Fig. 11 is the watermarked image whose PSNR is 44.63 dB. In Fig. 12, images on top are tampered versions of Fig. 11, and images at bottom are corresponding error images. The number of white points increased clearly, which means the

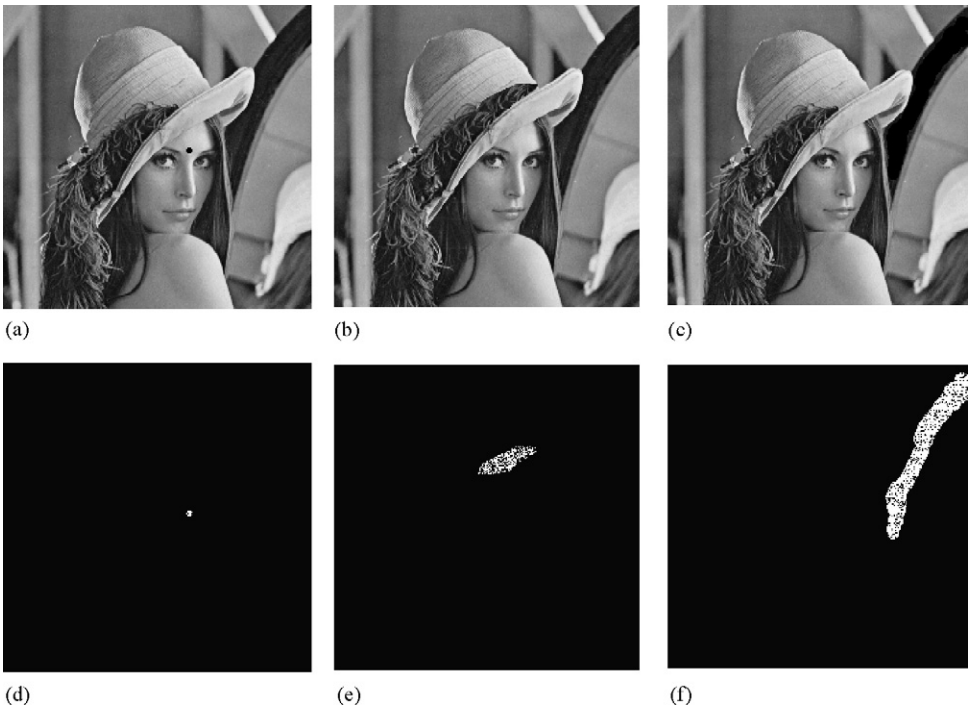

Fig. 12. Tampered results of Fig. 11 and corresponding error images. Images on top are tampered versions, and images at bottom are corresponding error images. (a) Tampered Lena (Lena's face has changes), (b) tampered Lena (the hat has changes), (c) tampered Lena (the background has changes), (d) error image of (a), (e) error image of (b) and (f) error image of (c).

improvement on detection accuracy rate in the tampered regions.

The detection accuracy rate can be verified by the curves in Fig. 13. In the experiments, similar tamper operations are conducted to the watermarked Lena images (Fig. 9(c) and Fig. 11). A top-left square region with size side × side in the watermarked image is cut and replaced with another image block having the same size. Since N_t is the number of tampered regions, it is set as side × side to calculate the theory value of DAR. The horizontal coordinate expresses the value of side, and the vertical coordinate expresses the value of detection accuracy rate. The curve marked with '+' is the theoretic DAR when L is 1, while the curve marked with '□' is the corresponding practical DAR; the curve marked with 'o' is the theoretical DAR when L is 2, while the curve marked with '△' is the corresponding practical DAR. It is obvious that the reality values are consistent with the theory values. The departure between them is caused by the hypothesis we set, such as $p = 1/2^L$. Another reason is that the tampered region values maybe equal the watermarked ones. No matter in theory or in reality, increasing the embedding space can get higher detection accuracy rate.

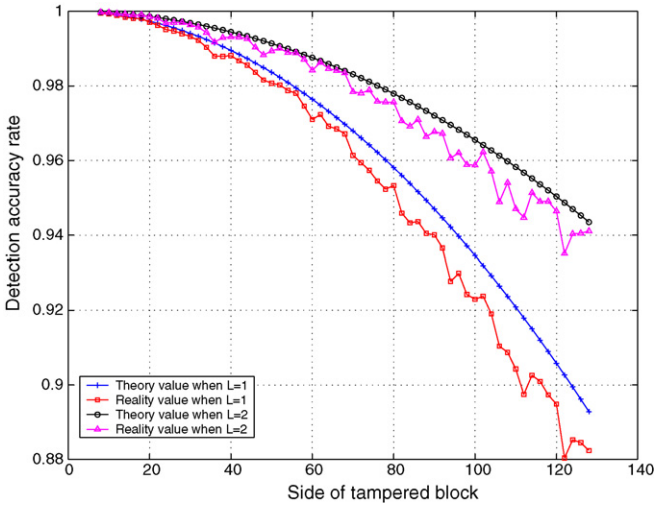

Fig. 13. Comparisons of the detection accuracy rate.

When the embedding depth is preserved as 1 bit, the detection accuracy rate can be increased by enlarging the size of image regions. If the localization precision is set as 2 × 2 pixels, the embedding space is 4 bits, i.e., $L = 4$. By doing so, *PSNR* of the watermarked image is 51.13 dB. In Fig. 14, when the watermarked image is tampered, an error image is used to demonstrate the changes. In Fig. 14(a), the attacker cuts some decoration on Lena's hat and pastes it on the other place of the hat. The detection result is given in Fig. 14(d). In Fig. 14(b) and (c), the attacker cuts the image blocks from an un-watermarked image, and pastes them on the watermarked Lena. The corresponding error images are shown in Fig. 14(e) and (f), respectively. It is obvious that the detection accuracy is also improved.

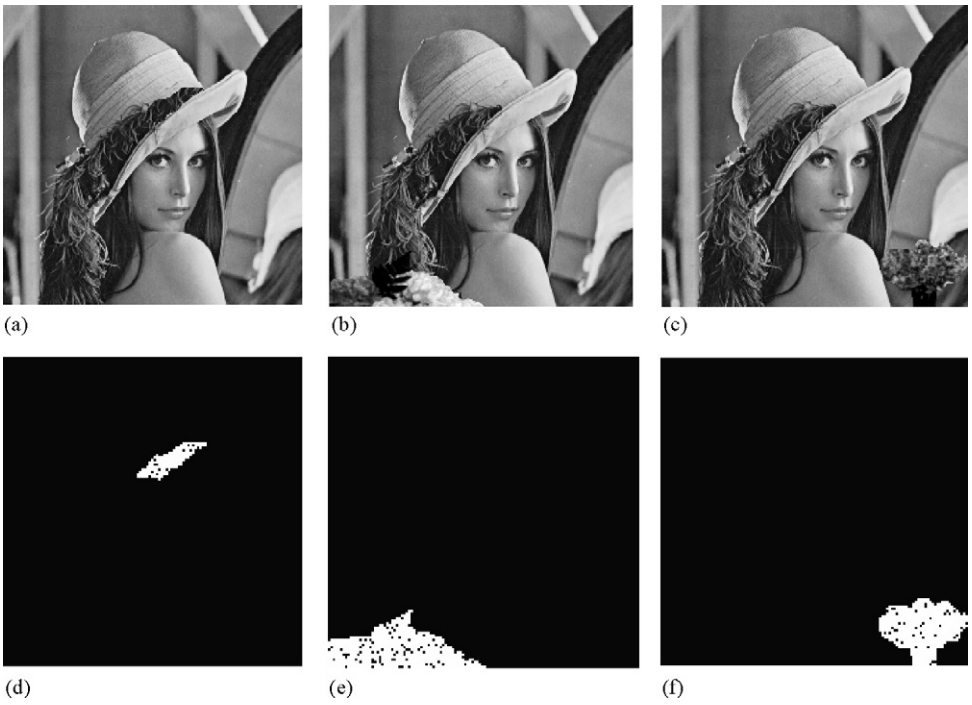

Fig. 14. Tampered versions and corresponding error images when embedding space is 4 bits. Images on top are tampered versions, and images at bottom are corresponding error images. (a) Tampered Lena (the hat has changes), (b) tampered Lena (the lower left part has changes), (c) tampered Lena (the lower right part has changes), (d) error image of (a), (e) error image of (b) and (f) error image of (c).

5. Conclusions

In this paper, a pinpoint authentication watermarking is proposed based on a chaotic system, which is sensitive to the initial value. This algorithm can precisely locate the tampered parts according to the requirement on precision. The prominent luminance values, the position information of the pixels and a key are used to construct the initial value for the chaotic model. The authentication watermark is produced dynamically and embedded in the image region. The application of the chaotic system increases the security of the algorithm because the chaos dynamic equation and corresponding parameters used are unknown to the others. At the receiver, a detector extracts the watermark and decides the tampered regions without the host image or the original watermark. In addition, the performances and properties are discussed in details. A detection accuracy rate is defined and analyzed to describe the probability of making right decisions. Experimental results demonstrate the effectiveness and advantages of our algorithm.

Acknowledgements

This paper is supported in part by National 973 program (No. 2006CB303104), National Natural Science Foundation of China (No. 90604032, No. 60702013, No. 60776794), Beijing Natural Science Foundation (No. 4073038), Specialized Research Foundation of BJTU (No. 2006XM008, No. 2005SZ005), Postgraduate Innovation Foundation of BJTU (No. 48106).

References

[1] I.J. Cox, M. Miller, J. Bloom, Digital Watermarking, Morgen Kaufmann Publishing, USA, 2001.
[2] R.R. Ni, Q.Q. Ruan, H.D. Cheng, Secure semi-blind watermarking based on iteration mapping and image features, Pattern Recogn. 38 (2005) 357–368.
[3] G.C. Langelaar, I. Setyawan, R.L. Lagendijk, Watermarking digital image and video data, IEEE Signal Process. Mag. (2000) 20–46.
[4] S.J. Han, I.S. Chang, R.H. Paik, Semi-fragile watermarking for tamper proofing and authentication of still images, in: International Workshop on Digital Watermarking, Korea, (2003), pp. 347–358.
[5] J. Fridrich, Image watermarking for tamper detection, in: IEEE Inter. Conf. on Image Processing, Chicago, Illinois, USA, (1998), pp. 404–408.
[6] S. Walton, Image authentication for a slippery new age, Dr. Dobb's J. 20 (1995) 18–26.
[7] M. Yeung, Mintzer, Invisible watermarking for image verification, J. Electron. Imag. 7 (1998) 578–591.
[8] M. Wu, B. Liu, Watermarking for image authentication, in: Proceedings of the IEEE International Conference on Image Processing, Chicago, Illinoise, US, (1998), pp. 437–441.
[9] M. Holliman, N. Memon, Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes, IEEE Trans. Image Process. 9 (2000) 432–441.
[10] M.U. Celik, G. Sharma, E. Saber, A.M. Tekalp, Hierarchical watermarking for secure image authentication with localization, IEEE Trans. Image Process. 11 (2002) 585–595.
[11] M. Celik, G. Sharma, A. Tekalp, Lossless watermarking for image authentication: a new framework and an implementation, IEEE Trans. Image Process. 15 (2006) 1042–1049.
[12] J. Wu, B. Zhu, S. Li, F. Lin, A secure image authentication algorithm with pixel-level tamper, in: International Conference on Image Processing, Singapore, October, (2004), pp. 1573–1576.
[13] H.J. Zhang, J.H. Dai, P.Y. Wang, J.C. Ding, Bifurcation and chaos in an optically bistable liquid-crystal device, J. Opt. Soc. Am. B: Opt. Phys. (1986) 231–235.