Scalable authentication watermarking with high precision based on chaotic sequence

Rongrong Ni[1], Qiuqi Ruan[1], H. D. Cheng[2, 1] and Jun Lu[1]

[1] Institute of Information Science, Beijing Jiaotong University, Beijing 100044, China

[2] Department of Computer Science, Utah State University, Logan, Utah, USA

rongrong_ni@hotmail.com or nirongrong@263.net

Abstract

Scalable precise authentication watermarking proposed is based on chaotic sequence, which is sensitive to initial value. The basic luminance value, position information of an embedding region and image protection key are used to construct the initial value for the chaotic model, which is sensitive to its initial value and dynamically produces the watermark. At receiver side, the detector extracts the watermark and decides the tampering regions without access to host image or the original watermark. The detection accuracy rate is first proposed and analyzed to present the probability of making a proper decision by the detector. Experiments show that this algorithm is scalable, and the localization precision and detection accuracy rate can be controlled by user.

Keywords: Authentication, chaotic sequence, localization precision, detection accuracy rate

1. Introduction

For some images, such as military images, remote sensing images, and medical images, etc., it is desired to distinguish the believable regions from the tampering regions very precisely. Authentication watermarking can detect the tampered regions in images [1]. However, few literatures pay attention to precise localization watermarking, or they easily fail to verify the authenticity. Walton divided an image into 8 ×8 blocks and embedded the checksum in the LSB of each block [2]. His algorithm can only locate 8×8 regions. In addition, if the blocks at the same position in two different images exchange, the detector cannot give right result. Yeung, et al. used a look-up table (LUT) to embed a watermark [3]. But the accuracy is not high and additional memory is needed for LUT. Wu, et al. applied the LUT method to DCT domain [4]. Fridrich proposed a robust watermarking to detect tampering, which could locate the block of size 64× 64 [5]. Most block-based algorithms are vulnerable to vector quantization (VQ) attack proposed by Holliman and Memon [6]. Recently Celik et al. proposed a hierarchical watermarking, which used the lowest level to guarantee the capability of localization and employ the higher level to resist VQ attack [7]. However, localization ability of their algorithm is restricted by the size of the blocks on the lowest level of the hierarchy, which is affected by the length of signature. Moreover, few literatures study the problem of detection accuracy.

In this paper, we propose a scalable authentication watermarking based on chaotic sequence, which is regionwise and can precisely locate the tampering regions with high accuracy. The region size is determined by the localization requirement, and the watermark payload is determined by both the size of region and longitudinal depth.

2. Proposed scheme

2.1. Embedding of authentication watermark

If a 2D image is presented as a 3D mesh, the conventional image surface can be regarded as transverse orientation, and the luminance value of image X can be regarded as the third dimension: longitudinal orientation.

According to the localization precision required, the size and shape of transverse non-overlapped region in image, which can be pixels, regular or non-regular blocks, are determined. The r^{th} transverse region is noted as X_r, r=1,2,⋯. In each region, the longitudinal depth for watermark embedding is also determined.

This project is supported by Beijing Jiaotong University RenCai Fundation:2005RC009.

For a transverse region X_r, the basic luminance value of it is indicated as $X_{r,b}=\{x_{r,b}(k,l)\}$, where k and l are position tag of each pixel in X_r. $x_{r,b}$ is formed by setting the bit-planes lower than prescribed longitudinal depth to zero.

An initial value of the chaotic model is calculated based on the basic luminance value, region position and image protection key. The variable *pos* represents the position index of image region. The image protection key can be represented in a numerical form *nkey*. The initial value of the chaotic sequence at region X_r , $c_{r,0}$, is:

$$c_{r,0} = InitialValue(X_{r,b},\ pos,\ nKey) = \overline{X}_{r,b} + pos \times 10^{-3} + nKey \times 10^{-3} \quad (1)$$

where, $\overline{X}_{r,b}$ is the mean of $X_{r,b}$.

The authentication watermark is dynamically produced by a hybrid optical bistable chaotic model, which has the following form [8].

$$x_{n+1} = 4\mathrm{Sin}^2(x_n - 2.5) \quad (2)$$

Substitute $c_{r,0}$ for x_n in chaotic functions, and G iterations are performed. Then, a chaotic sequence is generated, i.e., $\{ c_{r,g},\ g = 1,2,3,\cdots G \}$. Since components in the sequence are float numbers, they cannot be directly applied in our scheme. It is necessary to convert $\{ c_{r,g} \}$ to a binary sequence $\{ s_{r,g},\ g = 1,2,3,\cdots G \}$. If $c_{r,g}$ is larger than c_t, set $s_{r,g}$ to 1, otherwise set $s_{r,g}$ to 0. This process is shown in Eq. (3).

$$s_{r,g} = \begin{cases} 1, c_{r,g} > c_t \\ 0, \text{Otherwise} \end{cases} \quad (3)$$

where, c_t is set to 8/3.

The watermark to be embedded in transverse region is generated through the mapping function $f: V_G \rightarrow V_n$, which converts G-dimensional space to n-dimensional space by exclusive-or operation. n is the sum of longitudinal depth in the transverse region.

Embed the watermark in the bit-planes of transverse region, which are lower than prescribed longitudinal depth, to get a new region. When all the regions are operated, a new image, $\tilde{X}$ containing the watermark is produced.

It is difficult to launch VQ attack because of the introduction of region index and image protection key, and the sensitivity of the chaotic model to the initial value.

2.2. Extraction and authentication

Read the bit-planes lower than the specified longitudinal depth to extract the watermark. Integrity authentication is completed by comparing the extracted watermark and the produced reference sequence. The produced chaotic sequence and binary reference sequence are obtained based on the basic luminance value, which are the same as those in embedding process. If the extracted watermark is equal to the produced sequence, the region is considered non-tampering. Otherwise, the region is tampered. The extraction and authentication process is exactly blind because both the original image and original watermark are not required. The comparison result is shown as an error matrix, which can reflect the tampering position intuitively.

3. Detection accuracy rate analysis

No matter how different the produced chaotic sequences are, their destinations are binary sequences. For example, Fig.1 shows all the possible permutation and combination for n = 1. The extracted watermark and the produced binary reference sequence both have $2^n = 2^1 = 2$ possible values, and they have $2^{2n} = 2^2 = 4$ combinations.

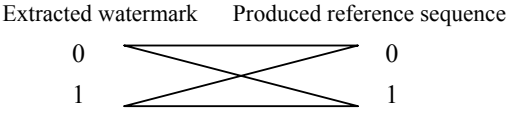


Fig. 1 Possible permutation and combination

Define *DAR* (Detection Accuracy Rate) as the probability of making a proper decision by the detector. *DAR* of the region that is tampered is different from the one of the region that is not tampered. Use DAR_{nt} to denote the detection accuracy rate of the non-tampered region; and use DAR_t to denote the detection accuracy rate of the tampered region. While *DAR* expresses the detection accuracy rate of the whole image.

In fact, in Fig. 1, there is only one parallel line that contains the proper decision. For example, when the true watermark is 0, the parallel line between 1 and 1 must correspond a wrong detection, while the parallel line between 0 and 0 may probably contain a wrong detection. The later corresponds the case that the changed pixel value produces a binary value 0. Let p be the probability of the wrong detection in the later parallel. And $p=1/2^n$, then

$$\begin{aligned} DAR_{nt} &= P(\text{no tamper in detection} \mid \text{no tamper in reality}) \\ &= \frac{P(\text{no tamper in detection}, \text{no tamper in reality})}{P(\text{no tamper in reality})} \\ &= \frac{1/2^{2n} \cdot (1-p)}{1/2^{2n} \cdot (1-p)} = 1 \end{aligned} \quad (4)$$

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

As for the tampered region, when the extracted watermark is different from the produced reference

value, the detector will give a proper decision that it is tampered, corresponding to the bias lines in Fig. 1. For example, if the extracted watermark is 0 and the produced value is 1, the detector will decide that the region is tampered. So the bias lines in Fig. 1 correspond to the proper decision. When the extracted watermark is the same as the produced value, the detector will decide that it is not tampered. But this decision could be wrong. Thus,

$$\begin{aligned} DAR_t &= P(\text{tamper in detection} \mid \text{tamper in reality}) \\ &= \frac{P(\text{tamper in detection}, \text{tamper in reality})}{P(\text{tamper in reality})} \\ &= \frac{(2^{2n}-2^n)/2^{2n}}{(2^{2n}-1)/2^{2n}+1/2^{2n}\cdot p} \\ &= \frac{2^{2n}-2^n}{2^{2n}+p-1} = \frac{2^{2n}-2^n}{2^{2n}+\frac{1}{2^n}-1} = \frac{2^{3n}-2^{2n}}{2^{3n}-2^n+1} \end{aligned} \tag{5}$$

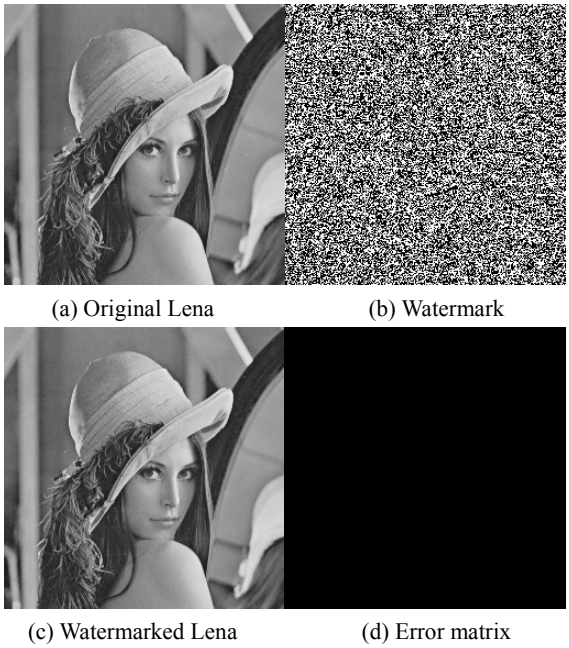
For the entire image, *DAR* is equal to the ratio between the number of accurately detected regions and the number of total regions. Suppose the number of tampered regions is N_t, and the number of total regions is M_t. Thus,

$$\begin{aligned} DAR &= \frac{\text{number of regions detected accuartely}}{\text{number of total regions}} \\ &= \frac{(M_t-N_t)\cdot DAR_{nt}+N_t\cdot DAR_t}{M_t} \\ &= \frac{(M_t-N_t)\cdot 1+N_t\cdot DAR_t}{M_t} \\ &= \frac{M_t-N_t+N_t\cdot\dfrac{2^{3n}-2^{2n}}{2^{3n}-2^n+1}}{M_t} \end{aligned} \tag{6}$$

4. Experiments

Lena image of size 256×256 is to be protected, shown in Fig. 2(a). Fig. 2(b) is the corresponding authentication watermark dynamically produced by the chaotic model. Fig. 2(c) is the watermarked image, whose *PSNR* with the original image is 51.191dB. Fig. 2(d) is the error matrix between the extracted watermark and the produced reference sequence when there is no tampering.

When the watermarked image is tampered, the error matrix can show the changes. Fig. 3(a) and Fig. 3(c) are tampered versions, and Fig. 3(b) and Fig. 3(d) are corresponding error matrices. The detector can find the changes that is difficult to be discovered by human eyes. Here *n* is set to 1. However, the decision is not absolutely right. The tampering marks in the error matrix is not entirely white, but some are white and some are black. It is because that some tampering is not detected, or some tampering values are even the same as the original ones.



(a) Original Lena (b) Watermark

(c) Watermarked Lena (d) Error matrix

Fig. 2 Embedding of watermark and authentication process

When the transverse region is fixed, the detection accuracy rate can be improved by adding the longitudinal depth. Let n = 2, Fig. 3(e) and Fig. 3(g) are the tampered versions, and Fig. 3(f) and Fig. 3(h) are corresponding error matrices. The number of white points increased clearly, which means the improvement of detection accuracy rate in the tampered region.

The comparisons of the detection accuracy rate are shown in Fig. 4. In the experiments, the top-left square with block of side×side in the watermarked image is cut and replaced with another image block. Set N_t in Eq. (6) to be side×side to calculate the theory value. The horizontal coordinate expresses the value of the side, and the vertical coordinate expresses the value of

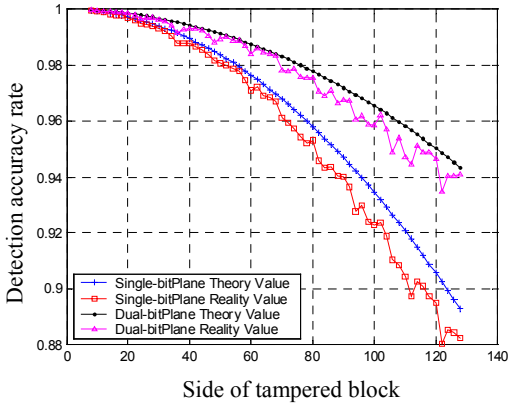


Fig. 4 Detection accuracy rate curves in theory and reality

detection accuracy rate.

The curve marked with '+' is the theoretic *DAR* when *n* is 1, the curve marked with '□' is the corresponding practical *DAR*; the curve marked with '•' is the theoretical *DAR* when *n* is 2, the curve marked with '△' is the corresponding practical *DAR*. No matter in theory or in reality, using two bit-planes can get higher detection accuracy rate than using single bit-plane.

5. Conclusions

In this paper, a precise authentication watermarking is proposed based on chaotic sequence. Localization precision and detection accuracy rate can be controlled by user, and have the retractility. The watermark is dynamically produced by the chaotic model, which makes the detection require neither the host image nor the original watermark. In addition, the use of chaotic sequence increases the security of the algorithm because the chaotic functions and corresponding parameters used are unknown to the others. Experimental results verify the detect ability of the algorithm and the theoretical analysis on detection accuracy rate.

References

[1] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking Digital Image and Video Data", *IEEE Signal Processing Magazine*, pp.20-46, 2000.

[2] S. Walton, "Image Authentication for a Slippery New Age", *Dr. Dobb's Journal*, vol.20, pp.18-26, 1995.

[3] M. Yeung, and Mintzer, "Invisible Watermarking for Image Verification", *Journal of Electronic Imaging*, 7(3), pp.578-591, 1998.

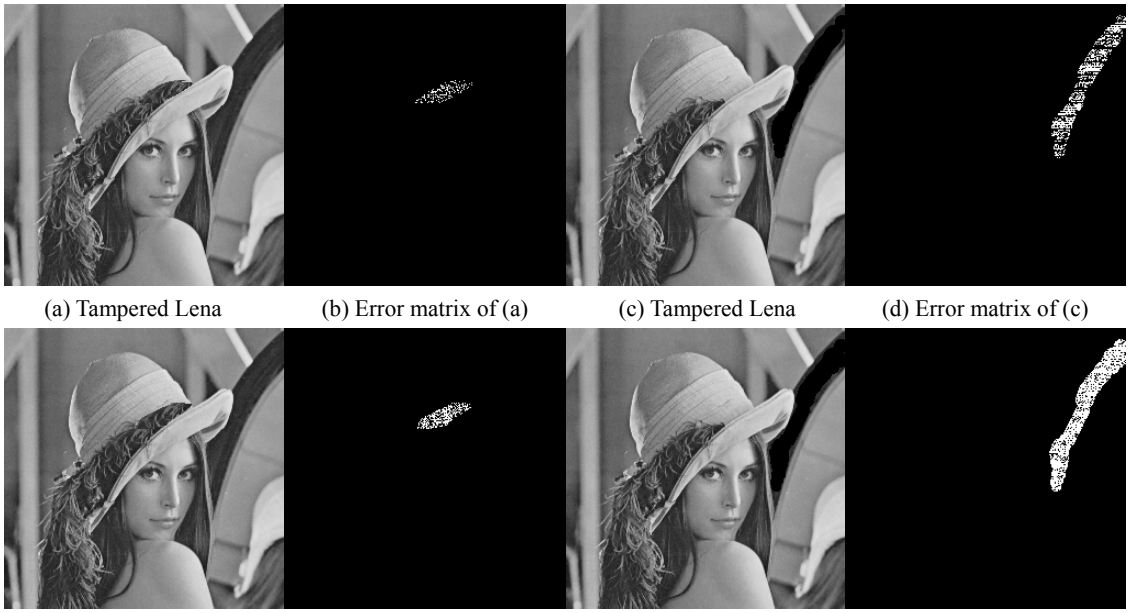
[4] M. Wu, and B. Liu, "Watermarking for Image Authentication," *Proceedings of the IEEE International Conference on Image Processing*, vol.2, pp. 437-441, Chicago, Illinoise, 1998.

[5] J. Fridrich, "Image watermarking for tamper detection", *IEEE Inter. Conf. on Image Processing*, pp. 404-408, Chicago, Illinois, USA, 1998.

[6] Holliman, M. and Memon, N., ¨ Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes, 〃 IEEE Trans. on Image Processing, vol. 9, no. 3, pp. 432-441, Mar. 2000.

[7] Celik, M. Sharma, U., Saber, G., E., and Tekalp, A. M., ¨ Hierarchical watermarking for secure image authentication with localization, 〃 IEEE Trans. on Image Processing, vol. 11, no. 6, pp. 585-595, June 2002.

[8] H. J. Zhang, J. H. Dai, P. Y. Wang, and J. C. Ding, "Bifurcation and chaos in an optically bistable liquid-crystal device", *Journal of the Optical Society of America B: Optical Physics*, 1986, 3(2), pp.231-235.



(a) Tampered Lena (b) Error matrix of (a) (c) Tampered Lena (d) Error matrix of (c)

(e) Tampered Lena (f) Error matrix of (e) (g) Tampered Lena (h) Error matrix of (g)

Fig. 3 Tampered images and corresponding error matrices