16th European Signal Processing Conference (EUSIPCO 2008), Lausanne, Switzerland, August 25-29, 2008, copyright by EURASIP

# IMAGE AUTHENTICATION BASED ON CHAOTIC SYSTEM WITH FEEDBACK AND PALM CHARACTERISTICS

*Rongrong Ni, Qiuqi Ruan, Yao Zhao, and Yanxia Wang*

Institute of Information Science, Beijing Jiaotong University
Beijing 100044, P.R.China
phone: + (86)-10-51683695, email: rrni@bjtu.edu.cn

## ABSTRACT

An image authentication scheme is proposed based on a chaotic system with feedback and palm characteristics. With a Trusted Third Party (TTP), the integrity of an image can be detected, meanwhile, the sender of the image can be identified reliably. During embedding period, an image is first divided into non-overlapped blocks. An authentication code is produced based on two adjacent blocks using a chaotic system with feedback. To identify the sender of an image and prevent denying event, biometrics information of the sender is applied in our scheme. A feature vector of palm is extracted and converted to a stream of bits. Whereafter, the authentication codes and the palm feature bits are encrypted using the public key of TTP. Then the encrypted information are transmitted to TTP, who will decrypt the received message and interleave them in a secret manner. The interleaved message is given back to the sender, and embedded in the corresponding image blocks. During authentication, a user detects the image integrity and localizes the tampered regions. At TTP, the sender is identified because of the reliable palm recognition. If the sender denies an image, TTP can capture his palm image on site, extract a feature vector, and compare it with the feature hidden in the image to confirm identity. Experiments reveal the effectiveness of our scheme.

## 1. INTRODUCTION

With the development of the Internet and computer science, information delivery and resources share are more and more convenient. However, information content is facing menace of security, such as property, integrity, and usability and so on.

A number of core techniques are researched to reliably protect the authenticity and integrity of information contents. Digital signature is one famous scheme based on the public-key infrastructure, which encrypts the digest of original message using a secret key of a sender, then transmits both the original message and the encrypted digest to a receiver. The receiver decrypts the digest with a public key of the sender, and generates a digest of the received message. Then both digests are compared to authenticate the integrity of the message. However, this scheme changes the size of file, and has high requirements on keys management. The leak of secret key will cause great loss, and arise denying behavior. In addition, localization to the tampered regions is unavailable.

Digital watermarking can resolve the above problems at a certain extent, which arose in 1990's to protect the copyright, authenticate the integrity, trace the fingerprinting, and control copy, etc. [1]. Most authentication watermarking systems combine digital signature to protect the content. The sender regards the encrypted digest as a watermark, and embeds it in the cover invisibly. The receiver firstly extracts the watermark, then authenticates the integrity of the media. Whereas, these systems cannot localize the tampered regions. Moreover, the loss of secret key may induce invertible result, which makes it possible for the sender to deny sending fact.

To locate the tampered regions, many algorithms are designed based on blocks. Nevertheless, most block-based algorithms are vulnerable to the vector quantization (VQ) attack [2], which uses the block-wise independence to counterfeit a collage image. Recently Celik et al. have proposed a hierarchical watermarking method using the lowest level for the capability of localization and a high level for resisting VQ attack [3, 4]. In their algorithm, digital signature was used to produce the watermark, which affected the block size and the precision of tamper localization. Some methods used keys or image block index to identify the image blocks [5]. But if the owner uses the same key for all his images, VQ attack will affect the authentication result.

In this paper, an image authentication scheme is proposed based on a chaotic system with feedback and palm characteristics. A Trusted Third Party (TTP) charges in the mechanism of message exchange and management. Biometrics information is introduced to identify the sender and avoid denying behavior. The palm feature vector of a sender is extracted and formed as a stream of bits. The content authentication code and palm feature stream are transmitted to TTP and interleaved under control of TTP. Then the interleaved signals are given back to the sender and embedded in the corresponding image blocks. During authentication, the integrity of image can be authenticated by a user, and the tampered regions can be marked. At TTP, the sender can be identified reliably, and denying event can be prevented effectively. Experimental results will demonstrate the merits of our scheme.

The rest of the paper is organized as follows, section 2 describes the embedding algorithm, authentication process is given in section 3, experiments are conducted in section 4, and section 5 draws the conclusions.

## 2. WATERMARK EMBEDDING

In this section, an authentication watermarking scheme is described in details, which fuses the biometrics information. This scheme establishes some relationship between one block and its neighboring blocks to produce an authentication code. Thus different authentication codes are attained even if blocks replacement occurs. The use of biometrics information can identify the sender. The embedding process consists of four steps as follows,

### 2.1 Image segmentation

An $X \times Y$ image $I$ is partitioned into non-overlapped blocks with size $p \times q$. So there are $N = (X \times Y)/(p \times q)$ blocks. And the image $I$ can be expressed as follows,

$$I = \{I_n(t), 1 \le n \le N, 1 \le t \le pq\} \tag{1}$$

$n$ indicates the image block position, $t$ represents the pixel index in an image block.

### 2.2 Construction of authentication code

A hybrid optical bistable chaotic system is used in this paper, which has the following form [6].

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

In each block, the authentication code is produced mainly according to pixels values of one block and its right(/left) neighboring block. The production process is based on a chaotic system with feedback, which is sensitive to the initial value. For an image $I$, one block $I_n$ and its neighboring block $I_{n+1}$ contain $2p \times q$ pixels, denoted as $s(k), k = 1, 2, \cdots, 2pq$. All $2pq$ pixels are input to a chaotic system with feedback in turn. In details, an initial value is fed to the chaotic system to execute $G$ times iterations. $G$ is larger than the length of authentication code $L$. The $G^{th}$ result acts as a feedback of the chaotic system. Each input pixel and the feedback value from the chaotic system are combined to calculate the next initial value $c(k,0)$, which can be expressed as,

$$c(k,0) = \lfloor s(k)/2 \rfloor + c(k-1,G) \tag{3}$$

Here, when the first pixel is input, i.e., $k = 1$, $c(0,G)$ is set as 0. Function $\lfloor \cdot \rfloor$ returns an integer that is not larger than the independent variable. Substitute $c(k,0)$ for $x_n$ in Eq.(2), and perform $G$ iterations. $c(k-1,G)$ is the $G^{th}$ iterations output when the $(k-1)^{th}$ pixel is input. The feedback ensures that each pixel in $s(k)$ has an equivalent contribution to produce the authentication code.

A sequence $\{c(2pq,g), g = 1, 2, \cdots, G\}$ is generated after the last pixel in $s(k)$ is input, from which $L$ elements are selected as the authentication code denoted as $W_o = \{w_o(t), t = 1, 2, \cdots, L\}$. Since components in $W_o$ are float numbers, they cannot be directly applied in our scheme. Each element in $W_o$ is converted to a binary value, i.e. $W_a = \{w_a(t), t = 1, 2, \cdots, L\}$. If $w_o(t)$ is larger than a threshold $T$, set $w_a(t)$ as 1, otherwise set $w_a(t)$ as 0. Here, $T$ is set to 8/3.

The construction of the authentication code is expressed in Fig. 1.

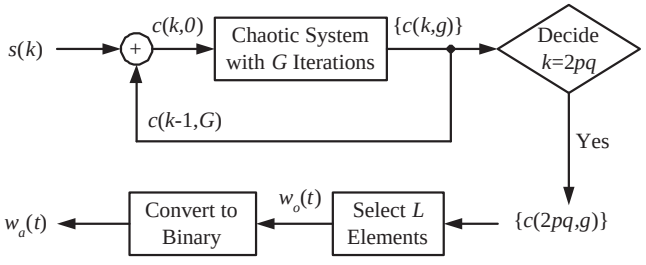



Figure 1: Construction of authentication code

For block $n$, the corresponding authentication code is denoted as $W_{a,n}$.

It is difficult to launch VQ attack because of the introduction of the neighboring block, and the sensitivity of chaotic model to the initial value.

### 2.3 Extraction of palm feature

Biometrics are the characteristics closely relative to one person, and have advantages on security, convenience, and reliability, etc. Our scheme extracts the Fisher feature vector of the sender's palm image [7, 8]. In details, a palm image is captured first, whose central part is cut and normalized to $64 \times 64$. Calculate a 27-dimensions feature vector, in which feature values are signed real numbers with two numbers after radix point. Every feature value is converted to a stream of binary bits occupying 20 bits, where 1 bit presents the sign of the real number ($'1'$ means a positive number and $'0'$ means a negative number), 12 bits stand for integer part, and decimal fraction uses 7 bits. Therefore, the palm feature vector occupies 540 bits, denoted as $W_b$.

It is noticeable that the 2-dimension Fisher feature matrix should be saved at TTP. For a registered user, the feature template is also saved at TTP.

### 2.4 Watermark construction and embedding

The produced authentication code and the palm feature vector are combined to construct a to-be-embedded watermark with the aid of a Trusted Third Party, who guarantees the reliable authentication. A user concatenates the authentication code and his own palm feature stream, and encrypts them using the public key of TTP. The encryption can ensure the security of the sender's biometrics information. Consequently, the encrypted signal is transmitted to TTP. After receiving it, TTP uses the secret key to decrypt and achieve the authentication code and the palm feature vector.

Because the length of palm feature bitstream is far less than the embedding capacity of an image. As well as to improve the correct identification rate, the palm feature bitstream is repeated several times according to the image size and the length of authentication code. Then the expanded feature bitstream is permuted and denoted as $W_p$. Subsequently, $W_p$ is partitioned into $N$ short bitstreams for each image block, that is $W_{p,n}$ for block $n$.

To achieve accurate localization, the authentication code of each block should be embedded in itself. TTP interleaves the authentication code of image block and the corresponding short feature bitstream in a secret manner based on a key of TTP. The interleaved signals are regarded as the watermark $W = \{W_n, 1 \le n \le N\}$ and sent back to the user.

The process of watermark construction is shown in Fig. 2.

The user embeds the watermark in the least significant bit-planes of the current block to get a new block, i.e., embeds $W_n$ in block $n$. This embedding process is completed according to Eq. (4),

$$\tilde{I}_n(t) = 2\lfloor I_n(t)/2 \rfloor + w_n(t) \tag{4}$$

When all blocks are operated, a new image $\tilde{I}$ containing the watermark is obtained. The embedding frame is shown in the top of Fig. 3.

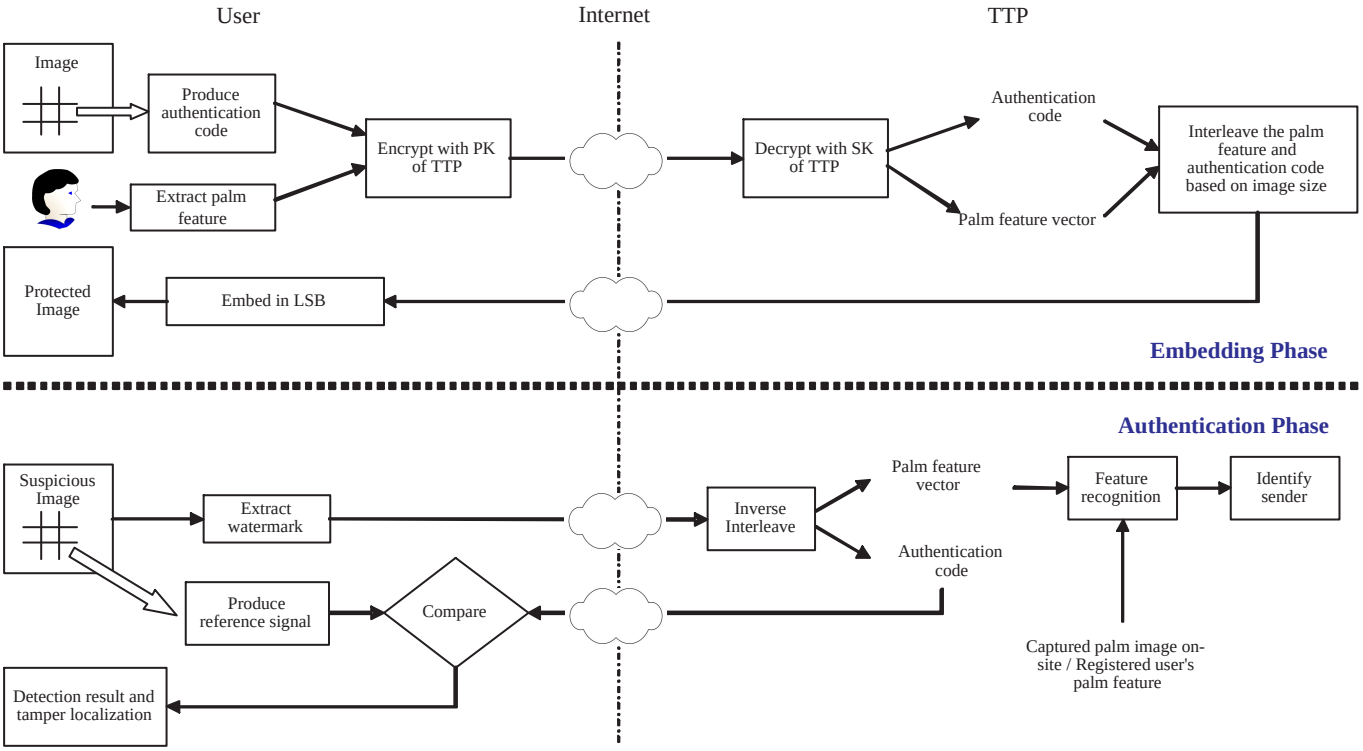



Figure 3: Framework of watermark embedding and integrity authentication

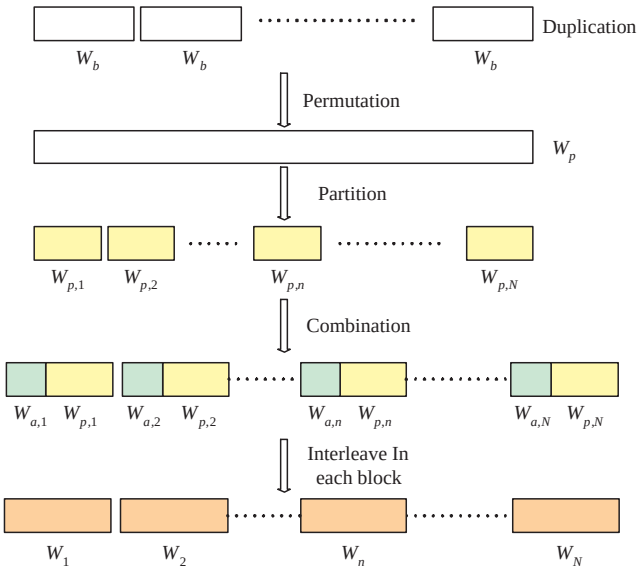



Figure 2: Construction of watermark

## 3. EXTRACTION AND AUTHENTICATION

As given in the bottom of Fig. 3. The verification of image integrity is composed of five steps.

Firstly, segment the suspicious image $\bar{I}$ into non-overlapped blocks with size $p \times q$.

Secondly, in each block $\bar{I}_n$, read the least significant bit-planes to extract the watermark.

Thirdly, send the extracted watermark to TTP, who separates the authentication code and the palm feature bitstream correctly. The palm feature bitstream is then changed to signed decimal numbers. Subsequently, the authentication code is transmitted to the user to complete the integrity authentication. The identification of palm feature is carried out at TTP later.

Fourthly, the user produces a reference signal using the method of authentication code construction in embedding process. Then, the extracted authentication code and the produced reference signal are compared to decide whether the image block is tampered or not. If all components in the two signals are same, the block is authentic; otherwise, the block is considered as a tampered one.

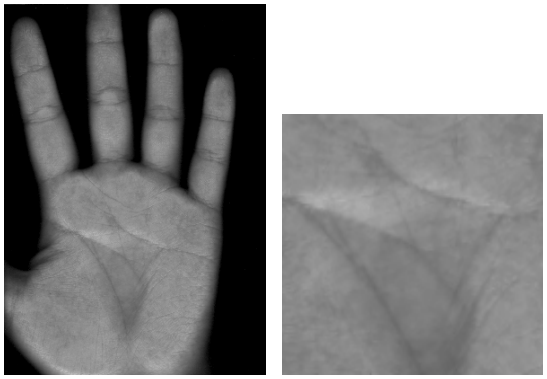
An error image is given to locate the tampered regions. If the block is decided as a non-tampered one, its corresponding mark $E_n$ in the error image is in white; otherwise, it is shown as suspicious image block. The extraction and authentication process is exactly blind because both original image and original watermark are not required.

Finally, TTP completes the task of palm recognition. If the sender is a registered user in TTP, he can be identified correctly. Thus, the sender cannot deny his delivering behavior. If an un-registered sender denies an image, TTP can capture his palm image on site, extract a feature vector, and compare it with the feature extracted from the image to confirm identity.

## 4. EXPERIMENTAL RESULTS

Lake image with size $256 \times 256$ is to be protected. Block size is set as $4 \times 4$ and $L$ is equal to 6. Fig. 4(a) is a palm image captured in our experiments, while its center part is normalized as $64 \times 64$, which contains the most information of one's

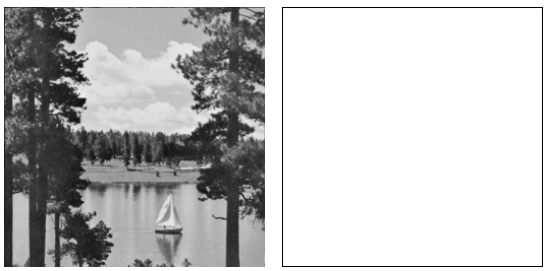
palm, given in Fig. 4(b). Fisher feature is extracted to form a 27-dimensions feature vector. Because the values in feature vector are signed real number, 1 bit is used to record the sign. The integer part of the feature vector is denoted by 12 bits, and decimal fraction part is represented using 7 bits. The bitstream of palm feature is repeated and interleaved with the authentication code to construct the watermark to be embedded.



(a) Palm image (b) Center of palm image

Figure 4: A palm image captured in our scheme

Fig. 5(a) is the watermarked Lake, whose PSNR is 51.11dB. Fig. 5(b) is an error image without tampering. In the case of non-tampering, the error image is in white, from which we cannot find the tampered regions. The sender is identified at TTP. In our experiments, the palm database contains 3000 palm images of 150 persons. The correct identification rate can attain 97.5%.

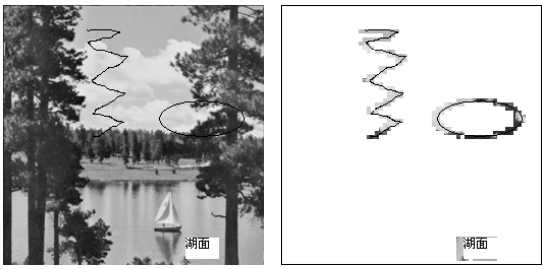


(a) Watermarked Lake (b) Error image without tampering

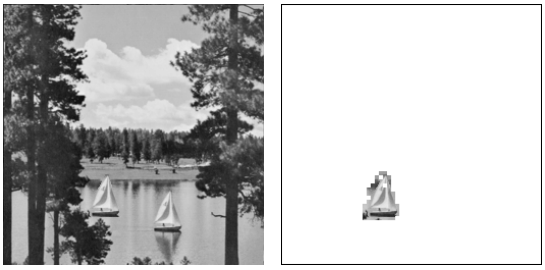
Figure 5: Embedding of watermark and authentication result without tampering

There are two common tamper operations: one is to change the contents of an image directly; the other is to crop a part of an image and paste it in the same image or in another image. Both tampering can be detected easily based on the proposed authentication method. Further more, the detection precision can reach two blocks, i.e. $4 \times 8$ pixels because the change of a block only affects itself and its neighboring block. This precision is better than that of Celik's scheme, which is at least larger than 64 pixels due to the use of digital signature.

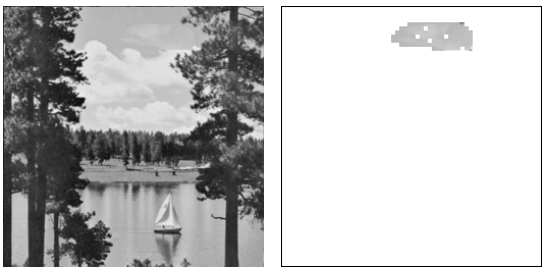
When the watermarked image is tampered, an error image is used to demonstrate the changes. Fig. 6(a), Fig. 6(c), Fig. 6(e) and Fig. 6(g) are the tampered versions of Fig. 5(a), and Fig. 6(b), Fig. 6(d), Fig. 6(f) and Fig. 6(h) are the corresponding error images. In Fig. 6(a), some parts in the image are tampered by directly changing the content in the background, the detection result is given in Fig. 6(b). In Fig. 6(c), the attacker cuts a ship on the lake, and pastes it on the other place of the lake, the detection result can reveal the tampering operation, as shown in Fig. 6(d). In Fig. 6(e), the attacker cuts the image blocks from another watermarked image, and pastes it on the watermarked Lake. Fig. 6(f) shows the corresponding error image. In Fig. 6(g), the attacker cuts a part of image from an unwatermarked image, and pastes it on the watermarked Lake. Fig. 6(h) shows the corresponding error image. It is obvious that the detector can find the changes difficult to be discovered by human eyes.



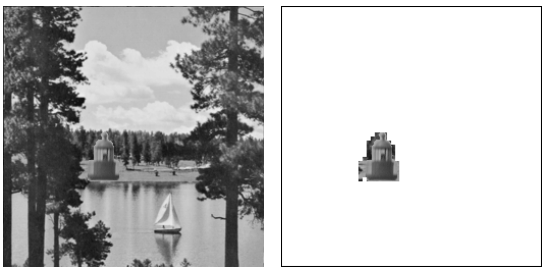
(a) Tampered Lake (b) Error image of (a)



(c) Tampered Lake (d) Error image of (c)



(e) Tampered Lake (f) Error image of (e)



(g) Tampered Lake (h) Error image of (g)

Figure 6: Tampered images and the authentication results

## 5. CONCLUSIONS

An image authentication scheme is proposed based on a chaotic system with feedback and palm characteristics. A mechanism of image authentication and management is constructed according to the proposed algorithm, in which a Trusted Third Party (TTP) makes an important role. The watermark to be embedded consists of two parts: one is a produced authentication code that reflects the content of an image, the other is the palm feature of a sender that prevents the denying behavior. Both parts are fused under the control of TTP. The embedding process and the integrity authentication are completed by the user. Due to the reliable palm recognition, the sender is identified at TTP. If the sender deny an image, TTP can capture his palm image on site, extract a feature vector, and compare it with the feature hidden in the image to confirm identity.

### Acknowledgment

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).

## REFERENCES

[1] I. J. Cox, M. Miller,J. Bloom, *Digital Watermarking*, USA: Morgen Kaufmann Publishing, 2001.

[2] M. Holliman,N. Memon, "Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes," *IEEE Trans. on Image Processing*, vol.9, no.3, pp.432-441, 2000.

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

[4] M. Celik, G. Sharma, and A. Tekalp, "Lossless watermarking for image authentication: a new framework and an implementation," *IEEE Trans. on Image Processing*, vol.15, no.4, pp.1042-1049, 2006.

[5] R. Ni, Q. Ruan, and H. Cheng, "Scalable authentication watermarking with high precise based on chaotic sequence," *International Conference on Computer Vision, Pattern Recognition and Image Processing*, Salt Lake City, Utah, USA, July 2005, pp.608-611.

[6] 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*, pp.231-235, 1986.

[7] D. Zhang, W.K. Kong; J. You and M. Wong, "Online Palmprint Identification Pattern Analysis and Machine Intelligence," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 25, no. 9, pp.1041-1050, Sept. 2003.

[8] X.Q. Wu, D. Zhang and K.Q. Wang, "Fisherpalms based palmprint recognition," *Pattern Recognition Letters*, Vol. 24, no. 15, pp. 2829-2838, November, 2003.