ATLANTIS PRESS
Advances in Intelligent Systems Research (AISR), volume 142
2017 International Conference on Information Technology and Intelligent Manufacturing (ITIM 2017)

A Robust Dual Watermarking Encryption Algorithm for Financial Fraud Detection Using High and Low Frequency Components

Jijun Wang
School of information and statistics
Guangxi University of Finance and Economics
Nanning 530003, china

***Abstract*—In this paper we study the robust dual watermarking algorithm in financial fraud detection. We propose a novel dual watermarking algorithm to protect the financial note from unauthorized tampering. First, the target watermark image is converted to binary format. We adopt the reversible and visible watermark to protect private information. Second, the secret key is generated from chaotic Tent map. We use the chaotic encryption to further protect the invisible watermark. Experimental results show that the proposed dual watermark encryption method is effective for financial note authentication. It may prevent potential financial fraud and improve information security.**

Keywords—Dual watermark, image encryption, chaotic sequence, reversible watermark

I. INTRODUCTION

Digital watermark plays an important role in copyright protection, image forensics, and financial proof authentication. It is an interdisciplinary research area that closely related to information hiding, cryptography, image processing, and social engineering.

Various encryption algorithms[1, 2] can be applied to watermarking, among which chaotic sequence can be used to protect the watermark due to its sensitivity to initial state [3]. Maleki et al. [4] proposed to use the multi-dimensional chaotic functions to enhance the encryption security. Huang et al.[5] proposed to adjust the inter-word distance to represent the watermark. However their work was limited to text images. Sun et al.[6] proposed a watermarking solution for documents authentication, and the algorithm is not compression robust.

In traditional visible watermarking methods [7, 8, 9, 10], watermark pattern is irremovable from the protected image, so that the unauthorized editing is prevented. However, in some applications, such as digital information protection and recovery, a removable watermark is preferred. The removable watermarks can be classified into two categories, the irreversible watermark and the reversible watermark. In this paper we focus on the financial note authentication, and the reversible watermark is a better choice.

This work was supported by the Research Funding of Guangxi Natural Science Foundation under grant No.2015GXNSFBA139255, Guangxi higher education research project under grant No.YB2014352 & No.KY2015YB267, Quantitative Economics Key Laboratory Program of Guangxi University of Finance and Economics under grant No.2014SYS17, Key discipline construction project of Guangxi University of Finance and Economics under grant No.2016KY28,Research project of Guangxi University of Finance and Economics research project under grant No 2016B033

The general flowchart of the information hidden process and the message decryption process is shown in Fig.1. The secret key is generated by encryption algorithm and the original image serves as a carrier. The message is then embedded and transferred. At the receiving end, the extracting algorithm recovers the hidden message using the same secret key.

Previous works in the reversible watermark research include modulo arithmetic [11], bijective transform [12], difference expansion [13], and lowest levels replacement[14]. Researchers have extended the reversible watermarking methods to the visible watermarking. Hu et al. [15] introduced an embedding method using significant bit plane. The efficiency was improved while the quality of the original image was influenced. Yip et al. [16], proposed to use pixel value matching to implement lossless visible watermarking. Tsai et al. [17] invented a novel algorithm based on the reconstruction of packet for restoration. However, their work did not solve the blind recovery where the original image was unknown.

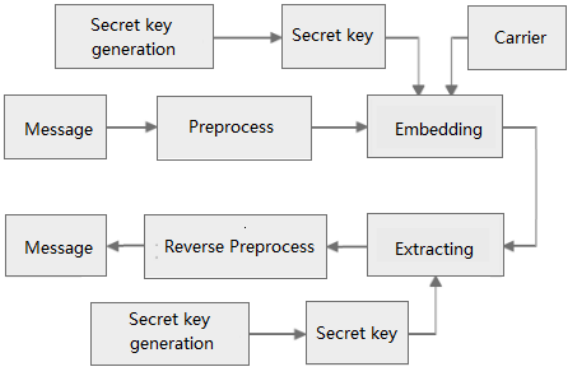

Fig. 1. A dipiction of the information hidden process in watermarking.

In this paper, we propose to use dual watermarking to protect the financial note from unauthorized editing. The first layer of watermark is the visible watermark pattern that declares the copyright information. The second layer of the watermark is encrypted and only visible to an authorized party who has the chaotic key. The contributions of this work are two-fold: i) we study a novel chaotic encryption method that protect the hiding watermark pattern; ii) we propose an effective dual watermarking algorithm that effectively prevents financial frauds. Experimental results on the actual financial data show that the proposed method is reliable and it can be used to improve the financial security.

II. Chaotic Encryption

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

Chaotic Tent map is an encryption method in chaotic dynamics theory. In mathematics, the definition of the Tent map can be represented as:

$$f_u = u \times min\{x, 1-x\} \tag{1}$$

where u is a real-valued parameter, and x is the input number. Iteratively, we can set $x_{n+1} = f(x_n)$, where $x_0 \in [0,1]$. It will give a sequence x_n, and an example of Tent map is illustrated in Fig.2. Tent map has a simple structure and it is effective in computer implementation. The watermark, which can be converted to binary sequence, is then encrypted by this chaotic sequence.

When we set the initial value to $x_0 = 0.6$, in each iteration it is used as the encryption key. The original watermark image will be encrypted by chaotic Tent sequence and transformed into a new image.

The chaotic sequence is denoted as $\{x_i\}$, and the $N \times N$ original image is converted into an $N \times N$ binary sequence $\{s_i\}$. We further convert the real value sequence $\{x_i\}$ into binary form $\{b_i\}$. The XOR (exclusive or) operation is performed on s_i and b_i to generate the encrypted watermark y_i, where $i = 1,2,...N \times N$

$$y_i = b_i \otimes s_i, i = 1,2,...N \times N \tag{2}$$

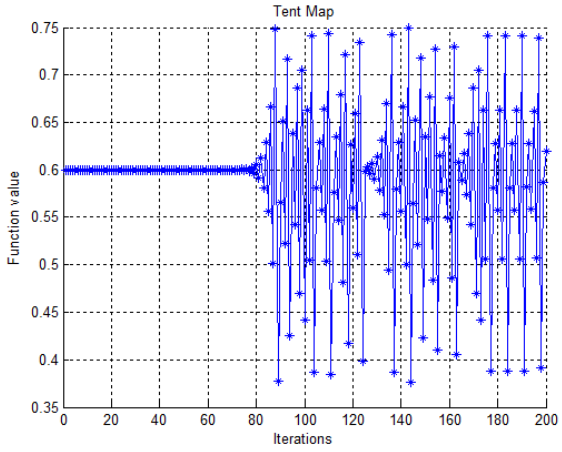

Fig. 2. A dipiction of Tent map, with parameter and initial value at 0.6.

III. Reversible Visible Watermark

The reversible watermark algorithm adopted in this section, can ensure the visibility and the reconstruction of the watermark image [18]. The target watermark image is converted to the binary format, which contains only bit 1 and bit 0. The averaged pixel value for bit 1 is denoted as n, and for bit 0 it is denoted as m. Two offsets a and b are used:

$$a = floor(m/2) \tag{3}$$

$$b = floor(n/2) \tag{4}$$

The embedding method is based on the pixel intensity and the watermark binary sequence:

$$I_{pw}(i,j) = \begin{cases} a + floor\left(\dfrac{I_w(i,j) \times 2^{p-1}}{2^p}\right) & W(i,j) = 0 \\ b + floor\left(\dfrac{I_w(i,j) \times 2^{p-1}}{2^p}\right) & W(i,j) = 1 \end{cases} \tag{5}$$

where W denotes the watermark. Offsets a and b can be used to adjust the range of pixel values.

The prediction of the original image is based on the embedding process:

$$\begin{cases} 2^p \times \dfrac{I_{rw}(i,j) - a}{2^{p-1}} & W(i,j) = 0 \; and \; I_{rw}(i,j) > 2a \\ I_{rw}(i,j) & W(i,j) = 0 \; and \; I_{rw}(i,j) \le 2a \\ 2^p \times \dfrac{I_{rw}(i,j) - b}{2^{p-1}} & W(i,j) = 1 \; and \; I_{rw}(i,j) < 2b \\ I_{rw}(i,j) & W(i,j) = 1 \; and \; I_{rw}(i,j) \ge 2b \end{cases} \tag{6}$$

IV. Dual Watermark Embedding

Invisible watermark usually contains copyright information and it can be used to prevent unauthorized editing. However the authentication process of the digital note requires complex algorithms and expensive computing equipment. In many financial fraud, the general public do not have the opportunity to verify the digital proof with professional equipment.

In these cases, the visible watermark is very important since it may be used as a notation of the authorized source and the applicable situations of the financial note. A depiction of the flow chart of the dual watermarking is shown in Fig.3. The dual embedding method consists of two major steps. First, the target image is decomposed as low frequency component and high frequency component. The visible watermark image is embedded in the low frequency component of the original image pixels according to Eq.5. Second, the invisible watermark is embedded to the high frequency component and it is encrypted by the Tent map sequence according to Eq.2.

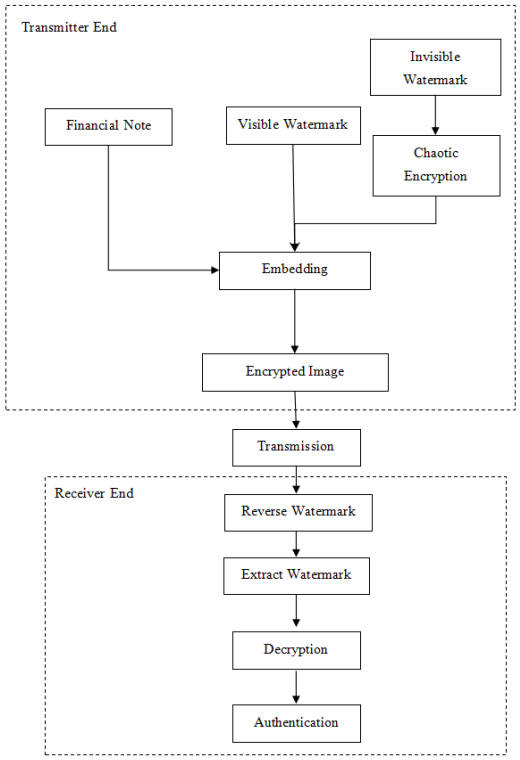

Fig. 3. A dipiction of the dual watermarking process.

V. Experimental Results

Invisible watermark usually contains copyright information and it can be used to prevent unauthorized editing. However the authentication process of the digital note requires complex algorithms and expensive computing equipment. In many financial fraud, the general public do not have the opportunity to verify the digital proof with professional equipment.

In this experiment, the chaotic key sensitivity is demonstrated to show the effectiveness of the proposed methods. The sensitivity to the secret key values is a desired property for watermark security. When the image is decrypted using a wrong key, the results are totally different from the original watermark image, as shown in Fig.4.

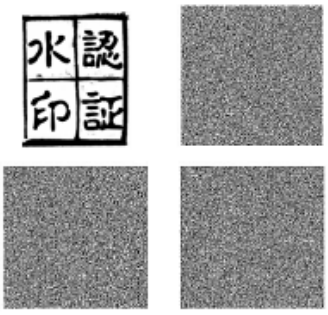

Fig. 4. Sensitivity of chaotic key: the upper left is the original watermark, the upper right is the encrypted image, the lower left and the lower right are the decrypted images using wrong secret keys

We further verify that the proposed algorithm is robust to additive noise. We test the PSNR(Peak Signal-To-Noise Ratio) of the decrypted watermark image. As the noise level increases, the PSNR decreases, as shown in Tab.1. We can see that the proposed algorithm is more robust than the traditional direct watermark embedding.

TABLE I. Robustness against noise condition.

Additive Noise (dB)	PSNR value	Traditional algorithm
80	70.1	65.4
75	73.5	70.1
70	76.8	73.4
65	82.1	78.3
60	86.8	81.5
55	87.5	84.3
50	90.1	87.5

The reversible visible watermarks are shown in Fig.5 and Fig.6. We can see that the visible watermark can be used to identify the source of the financial note. It can also be used to protect the sensitive information. Due to its reverse property, the financial note can be fully recovered after removing the visible watermark.

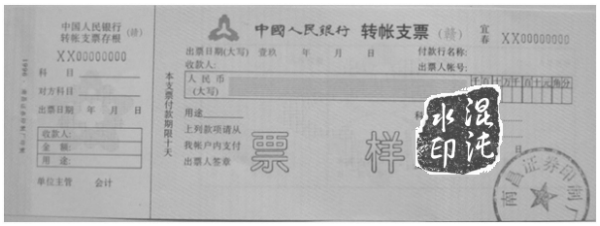

Fig. 5. Visible watermark for the protection of sensitive data.

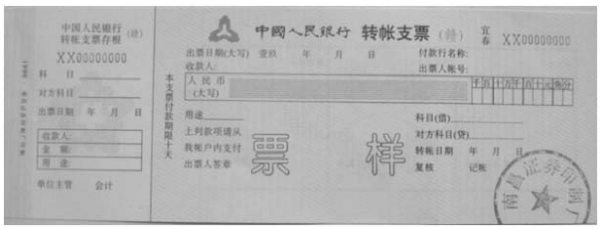

Fig. 6. Reversible property of the visible watermark.

VI. CONCLUSIONS

In this paper we study a novel chaotic encryption method and its application in digital watermark. The target image is protected by the dual watermark, the first layer of watermark protects the sensitive information and declares the copyright. It is visible and reversible using the state-of-the-art watermarking technique. The second layer of the watermark adopts the chaotic encryption algorithm. It is sensitive to the encryption key and it is only visible to the authorized party. The results on the financial application are promising. In the future work we will extend our method to digital audio watermark applications and more chaotic encryption algorithms will be investigated.

Acknowledgment

This work was supported by the Research Funding of Guangxi Natural Science Foundation under grant No.2015GXNSFBA139255, Guangxi higher education research project under grant No.YB2014352 & No.KY2015YB267, Quantitative Economics Key Laboratory Program of Guangxi University of Finance and Economics under grant No.2014SYS17, Key discipline construction project of Guangxi University of Finance and Economics under grant No.2016KY28,Research project of Guangxi University of Finance and Economics research project under grant No 2016B033

References

[1] A. Skander, M. Nadjim and B. Malek, "Synchronization chaotic communications with closed cryptographic systems", ICIC Express Letters, vol.2, no.3, 2008, pp.269-274.

[2] W. Xiang, "Equilibrium points and bifurcation control for Lorenz-Stenflo system", ICIC Express Letters, vol.3, no.1, 2009, pp.61-66.

[3] V. Gupta and A. Barve, "A review on image watermarking and its techniques", International Journal of Advanced Research in Computer Science and Software Engineering, vol.4, no.1, 2014, pp.92-97.

[4] H. Maleki, M. T. Sharabyan, "Presentation of a method for Watermarking by Multi-dimensional Chaotic Functions", Journal of Applied Environmental and Biological Sciences, vol.5, no.3, 2015, pp.174-180.

[5] D. Huang and H. Yan, "Interword distance changes represented by sine waves for watermaking text images", IEEE Transactions on Circuits and System, vol.11, no.12, 2001, pp.1237-1245.

[6] Q. B. Sun, P. R. Feng and R. Deng, "An optical watermarking solution for authenticating printed documents", Proc. of International Conference on Information Technology, 2001, pp.65-70.

[7] S. P. Mohanty, K. R. Ramakrishnan and M. S. Kankanhalli, "A DCT domain visible watermarking technique for images", Proc. of IEEE International Conference on Multimedia Expo, New York, USA, vol.2, 2000, pp.1029-1032.

[8] B. B. Huang and S. X. Tang, "A contrast-sensitive visible watermarking scheme", IEEE Transactions on Multimedia, vol.13, no.2, 2006, pp.60.

[9] R. Lukac and K. N. Plataniotis, "Secure single-sensor digital camera, Electronic Letters", vol.42, no.11, 2006, pp.627-629.

[10] J. Meng and S. F. Chang, "Embedding visible video watermarks in the compressed domain", Proc. of IEEE International Conference on Image Process, Chicago, IL, October, vol.1, 1998, pp.474-477.

[11] C. W. Honsinger, P. W. Jones, M. Rabbani, and J. C. Stoffel, "Lossless recovery of an original image containing embedded data", U.S. Patent, No.6278791, August, 2001.

[12] C. De Vleeschouwer, J. F. Delaigle, and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management", IEEE Transactions on Multimedia, vol.5, no.1, 2003, pp.97-105.

[13] J. Tian, "Reversible data embedding using a difference expansion", IEEE Transactions on Circuits and Systems for Video Technology, vol.13, no.8, 2003, pp.890-896.

[14] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding", IEEE Transactions on Image Process, vol.14, no.2, 2005, pp.253-266.

[15] Y. J. Hu and B. Jeon, Reversible visible watermarking and lossless recovery of original images, IEEE Transactions on Circuits and Systems for Video Technology, vol.16, no.11, pp.1423-1429, 2006.

[16] S. K. Yip, O. C. Au, C. W. Ho, and H. M. Wong, Lossless visible watermarking, Proc. of IEEE International Conference on Multimedia Expo, Toronto, ON, Canada, 2006, pp.853-856.

[17] H. M. Tsai and L. W. Chang, A high secure reversible visible watermarking scheme, Proc. of IEEE International Conference on Multimedia Expo, Beijing, China, 2007, pp.2106-2109.

[18] H. Gao, X. Deng and Z. Chen Z., Medical image privacy protection scheme based on reversible visible watermarking, Journal of Computer Applications, vol.34, no.1, 2014, pp.119-123.