ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
https://doi.org/10.17559/TV-20160517113602

FORGERY DETECTION USING CHAOTIC WATERMARKING IN IMAGE KEY AREAS

Rui Tao, Yanjing Sun, Weidong Liu

Preliminary communication

In this paper we study watermarking algorithm for compressed images in the application of antiforgery in financial bills. First, the basic watermarking algorithm based on image edge information is studied. The encrypted watermark is converted into binary values and embedded into the edges, meanwhile the original edge shape is preserved from noticeable destruction. Second, the flip-invariant SIFT features are used to localize the key content area like digits and letters in the image. Third, Tent map and a hash function is used to further protect the secrete watermark. The property of Tent map ensured the sensitivity towards changes in the initial value. Therefore we can better protect and encrypt the original watermark. The operations performing on the binary coded image are based on the encryption sequences generated from chaotic map. Different operations are chosen to generate robust encrypted watermark. Finally, we verify our algorithm in antiforgery detection. The sensitivity towards secrete key values is further investigated. The proposed system is sensitive to the key values, hence it effectively protects the watermark from attack. The computational cost is also measured for practical application of the chaotic watermarking. Experimental results show that the proposed method is reliably efficient.

Keywords: *antiforgery; binary image; chaotic system; digital watermark*

Otkrivanje falsifikata pomoću kaotičnog vodenog žiga u ključnim dijelovima slike

Prethodno priopćenje

U radu proučavamo algoritam za nanošenje vodenog žiga na komprimiranim slikama u primjeni protiv falsifikata na novčanicama. Najprije se proučava osnovni algoritam za nanošenje vodenog žiga na osnovu informacije o rubu slike. Šifrirani vodeni žig se pretvara u binarne vrijednosti i ugrađuje u rubove, a u međuvremenu se originalni oblik ruba štiti od vidljivog uništenja. Zatim se uz pomoć flip-invariantnih SIFT karakteristika lokalizira ključno područje sadržaja poput brojki i slova na slici. Treće, primjenjuju se Tent mapa i hash funkcija u daljnjoj zaštiti tajnog vodenog žiga. Svojstvo Tent mape osiguralo je osjetljivost na promjene u početnoj vrijednosti. Stoga možemo bolje zaštititi i prikriti originalni vodeni žig. Izvršenje operacija na binarno kodiranoj slici zasniva se na kodiranim nizovima dobivenim iz kaotične mape. Odabrane su razne operacije kako bi se generirao robustni prikriveni vodeni žig. Konačno smo verificirali naš algoritam u otkrivanju falsifikata. Istraživala se i osjetljivost prema tajnim ključnim vrijednostima. Predloženi je sustav osjetljiv na ključne vrijednosti pa učinkovito štiti vodeni žig od napada. Trošak izračuna se također mjerio u praktičnoj primjeni kaotičkog vodenog žiga. Eksperimentalni rezultati pokazuju da je predložena metoda pouzdano učinkovita.

Ključne riječi: *binarna slika; digitalni vodeni žig; kaotički sustav; protufalsifikat*

1 Introduction

Digital image is widely used for scanning, copying and transmitting the banking notes in daily business. However the fraud in electronic bills is one of the major drawbacks in e-business. With the latest development of computer technology, using digital watermark has become an important method in financial bill authentication and detection of frauds. Chaotic systems have drawn a lot of attention from many researchers [1÷4], and the watermarking algorithm based on chaotic method has been applied to encryption problems [5÷6].

The watermarking process is difficult due to the unique character of binary image format comparing with the grey image format. Researchers have studied various image features, which can be modified for localization and avoid destroy the original image. Mici et al. [7] in 2005 and Brassil et al. [8] in 1999 studied the copyright protection and provided methods of digital watermarking on binary images. They adjusted the space between lines and words. Inspired by Brassil's methods, Huang et al. [9] used the width of the characters to encode desired information, and it was combined with blind detection for robustness against noise. However, this type of algorithm can only deal with limited information. Villan et al. [10] proposed to solve Gel'fand-Pinsker problem for binary image. Sun et al. [11] proposed to modify the black areas into a sequence of discrete bars and dots. There are several existing methods that can localize the fraud in binary images [12-14]. However their methods cannot protect the large areas in binary image, if the large areas are deleted in the original image, the detection algorithm will fail.

In Figure 1 the flowchart of the watermarking system is depicted. Edge information is first detected on the input image. We adopt an efficient method of edge detection from reference [15].

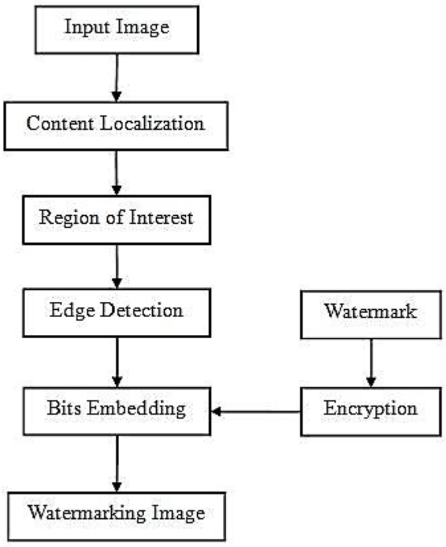

Figure 1 Flow chart of watermarking system

For model matching purpose the extracted edges are grouped into several segments and the watermark image is generated based on the proper edge models.

In order to protect the watermark, the chaotic Tent map is used. Any modifications to the key areas of the financial bills will be detected due to the high sensitivity of the chaotic system.

Using watermark to protect the authentication of financial bills has a great practical value. It provides a fast and ubiquitous technology to fight against financial frauds. The automatic watermark detection algorithms can process large amount of bank notes and achieve real-time responding goal.

In Sec.1 the details of the proposed methods are described. In Sec.2 the corresponding experiments are provided. Finally, we give a brief discussion and conclusion in Sec. 3.

2 Methodology

2.1 Watermarking using edge information

Binary images are simple to produce and easy to store, therefore many of the current documents are captured in binary image forms, such as TIFF (Tagged Image File Format) images. Compared to grey scale images, it has less colour information and information hiding in such images is harder.

In this paper we make use of the edge information of the binary images to embed digital watermark. Examples of usable edges [16] in binary images are given in Fig. 2. The usable pairs of two edges should be able to be converted to each other, by moving block 3 we can change edge type a to edge type b, and likewise [16]. Therefore, it can be used to represent either bit 0 or bit 1 in digital watermarking algorithm.

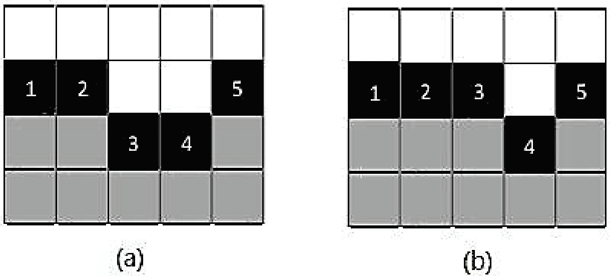

Figure 2 Examples of usable edge pair, (a) stands for bit 1 and (b) stands for bit 0.

The extraction of watermark is the opposite process of embedding one, which is demonstrated in Fig. 1. The extraction consists of the following steps.

Step 1: Image edge extraction and grouping.

Step 2: Model matching and edge type classification.

Step 3: Re-composition of bit-wise information to form bit stream.

Step 4: Decoding watermark from the extracted bit stream.

When a distortion is made artificially to the binary image, the hidden information in the image edges will be destroyed and the fraud detection will fail. In the key areas of a digital image, when someone modifies the content of that area, the edges will generally be changed spontaneously.

We apply a pre-trained object recognizer to detect region of digits and letters in an image.

The object detector is based on the state-of-the-art flip-invariant SIFT (Scale-Invariant Feature Transform) features [17].

2.2 Image content detector

The image content detector is adopted for detecting the key areas in an electronic bill. First the positive images and the negative images are collected for training. The positive sample set consists of a sequence of chopped images that contain numbers or characters. The negative sample set consists of a sequence of images that contain random backgrounds without any key information. Second, the image samples are aligned and normalized. Training samples are resized into the same size for modelling.

The flip-invariant SIFT features are then extracted from the positive images and the negative images forming a sequence of feature points.

The extracted features are then computed to generate fixed dimension length vectors for modelling convenience.

Finally, two classification algorithms are adopted for modelling the detector to classify the key content area from the others. Support Vector Machine (SVM) and Artificial Neural Network (ANN) are used for comparison.

SVM is an optimized classifier especially useful under a small sample size. It is developed from the statistical learning theory. In SVM classifier we aim to learn the mapping: $X \rightarrow Y$, in our case X is the feature set and Y is the class content label. Let's denote the classifier as:

$$y = f(x, \alpha) \tag{1}$$

The classification problem is represented as:

$$f(x, \{w, b\}) = sign\,(wx + b) \tag{2}$$

where w and b are the parameters for the hyperplane, determined by support vectors.

ANN is another option we choose to compare with the SVM classifier. ANN is inspired by the ability of animals to react adaptively to the environment. The simulation of the nervous system may produce similar responses in computer systems. Neurons work by processing information. They receive and provide information in form of spikes. In a typical artificial neural network, there are many neurons that are linked together according to specific network architecture. In our situation, the objective of the neural network is to transform the image feature inputs into content labels. We adopt a three layer ANN and use BP algorithm to optimize its parameters. First layer takes in the image features and the third layer outputs the content labels.

$$y_{\text{out}} = \boldsymbol{W}^{\mathrm{T}} X \tag{3}$$

where $\boldsymbol{W}$ is the matrix of all weight vectors.

2.3 Chaotic tent map

In this section we further investigate the performance of encryption algorithms based on chaotic sequences. We propose an effective method for watermark encryption for e-banking notes.

Digital images generally contain redundant information, and the neighbouring areas of pixels are strongly correlated. Since its content is based on signal generated from stochastic process, it is less sensitive compared with binary sequences in communication. The popular encryption algorithms, such as DES, RSA, etc., cannot be used for real time image transfer since they usually require a large amount of computational time.

Chaotic Tent map [19] is a popular method in non-linear dynamics. In mathematics, the definition of the Tent map is given as follows:

$$f_u = u \times \min\{x, 1 - x\} \tag{4}$$

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. 3. Tent map has a simple structure and it is effective in computer implementation. The watermark, which is a binary image, is then encrypted by this chaotic sequence.

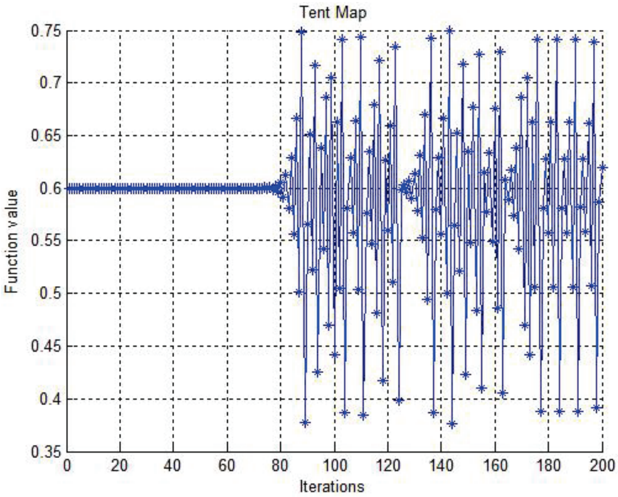

Figure 3 A depiction of Tent map, parameter μ = 1,5, and initial value is 0,6.

Take the initial value x_0 = 0,6 for iteration as the encryption key. The original watermark image will be processed by Tent map and transformed into an encrypted watermark image.

The chaotic sequence is denoted as $\{x_i\}$, and the N×N original image is converted into an N×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 ×N.

$$y_i = b_i \otimes s_i,\ i = 1, 2, ..., N \times N \tag{5}$$

The Tent map based methods have shown efficient ways to implement image encryption in image and video transfer. In the encryption process different operations are chosen to convert the pixel value of watermark. The operation is controlled by the chaotic map.

2.4 One-way hash function

A novel one-way hash function based on Logistic map proposed by Ting-Ting He [20] is adopted for further securing the watermark from artificial modification. The pseudo-random sequence produced by the hash function can be used as additional authentication proof.

A slight modification in the watermark will cause great difference in the sequences. Therefore it can be used for detecting forgery in digital bills.

According to Ting-Ting He's work, Logistic mapping is adopted [20]:

$$x_{n+1} = ux_n(1 - x_n) \tag{6}$$

where the state variable $x_n \in [0,1]$, and parameter $u \in [0,4]$. Hash function is defined by [20]:

$$h = H(M) \tag{7}$$

where M is the message with variate length.

The system initial value is set to satisfy [20]:

$$\begin{gathered} x_n = ax_{n-1} (\text{mod } B) \\ (x_0, B) = 1, r_n = \frac{x_n}{B} \end{gathered} \tag{8}$$

where B is the modulus, and r_n is a random variable. Details can be found in their publication.

2.5 Encryption and decryption of chaotic watermark

The decryption of the chaotic watermark is the opposite operation of the encryption. As shown in Fig. 4 the encryption key is agreed beforehand, and it is managed and noticed by the authentication agent in a secured way knowing the encryption key will enable the chaotic system to generate the exact sequence used in encryption. The sequence is very similar to a serial of random numbers but it is generated by chaotic map. The decryption process recovers the watermark which is masked by the chaotic sequence. By checking the distortion between the original watermark and the recovered watermark, we may decide whether the financial bill has been changed, modified, or destructed.

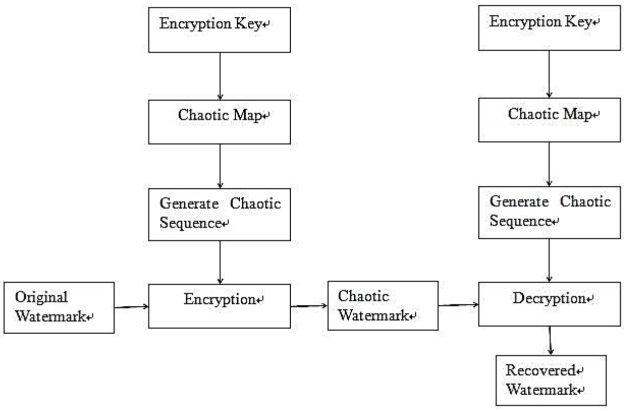

Figure 4 Encryption process and decryption process of the chaotic watermark

3 Experimental results

3.1 Localization experiments

Synthetic examples of images that contain digits, letters and various backgrounds are used to verify the effectiveness of the image content detector, as shown in Fig. 5. The numbers and letters are located at various parts of the original image. Although the location is arbitrarily chosen, it is close to the real situation of a banking note. The background of the contents in real banking note is usually simple patterns, and so is the synthetic image. The detected location is converted into a black bounding box through empirical size setting, which can also be learned from training samples.

The size of the bounding box is preset and it is normalized into a fixed size according to the size of the image. The results are shown in Fig. 5 and Fig. 6. We can see that the areas that contain digits and letters, which have clearly different appearance and features, are detected and localized in the original image.

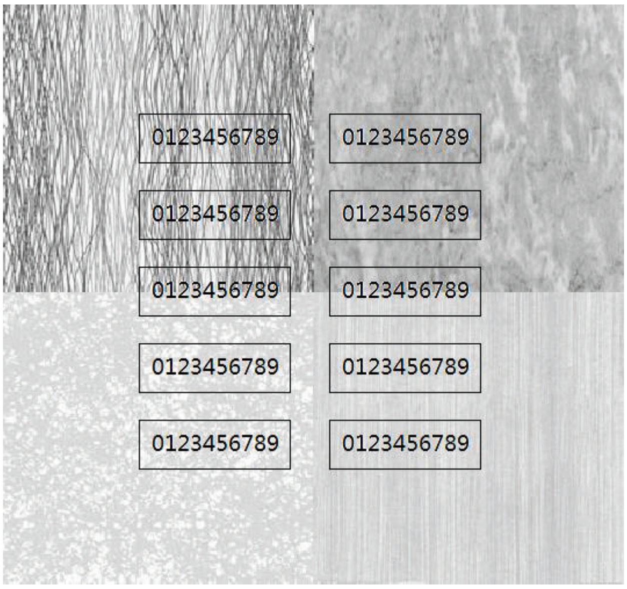

Figure 5 Synthetic example of images contains printed numbers.

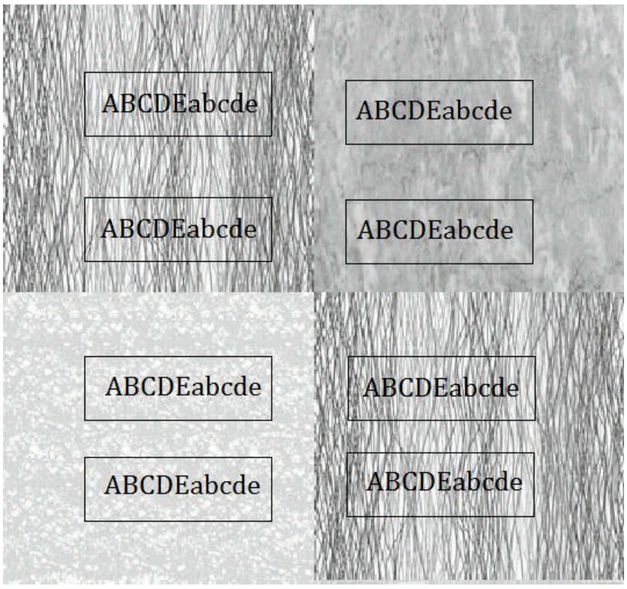

Figure 6 Synthetic example of images contains printed letters.

In this way, we are able to find the key areas in actual banking bills. Performing encryption on the key areas will reduce the cost and help to locate fraud.

Experimental results show that the SVM is more reliable than the ANN. Errors in the overlapping of the bounding boxes are listed in Tab. 1.

Table 1 Error of the overlapping bounding box using SVM and ANN

Method	Digits	Letters	Averaged
SVM-based	12 %	14 %	13 %
ANN-based	23 %	29 %	26 %

An example of the bank check is shown in the binary image in Fig. 7. The number areas are detected using template matching by a sliding window with default ranging size over the entire image. The resulting bounding box around one digit is then merged into the neighbouring and provides that the distance between them is not exceeding the upper boundary threshold. Only the sequences of digits are shown, the isolated digit is removed in order to reduce the false detection, as shown in Fig. 8. In practice one to three key number areas are adopted for watermarking protection. The computational efficiency can be improved.

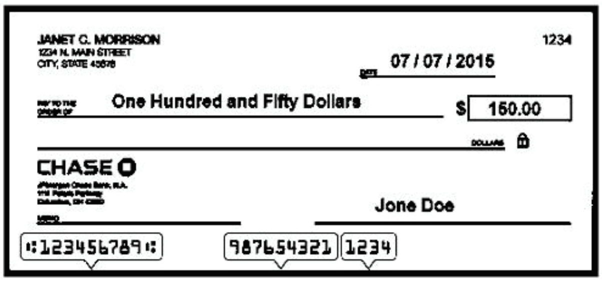
JANET C. MORRISON
1234 N. MAIN STREET
CITY, STATE 45678
1234
DATE
07 / 07 / 2015
PAY TO THE ORDER OF
One Hundred and Fifty Dollars
$
150.00
DOLLARS
CHASE
Jone Doe
MEMO
⑆123456789⑆
987654321
1234

Figure 7 Example of a bank check

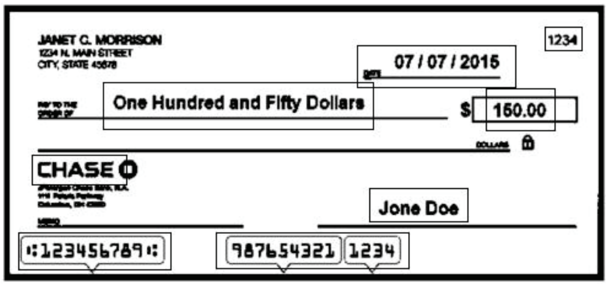
JANET C. MORRISON
1234 N. MAIN STREET
CITY, STATE 45678
1234
DATE
07 / 07 / 2015
PAY TO THE ORDER OF
One Hundred and Fifty Dollars
$
150.00
DOLLARS
CHASE
Jone Doe
MEMO
⑆123456789⑆
987654321
1234

Figure 8 Detected key areas using the merged bounding boxes for watermarking.

3.2 Encryption and decryption experiments

The pixel value in the watermark images is shown in Fig. 9 and Fig. 10. The correlation between the adjacent pixels shows that after encryption the dependency is removed. The processed images are very similar to randomized noise.

Key sensitivity tests are further carried out to evaluate the proposed methods. A good encryption method should be as sensitive to the secret key values as possible. When we decrypt the watermark with wrong key values, the results are totally different from the original watermark image, as shown in Fig. 11.

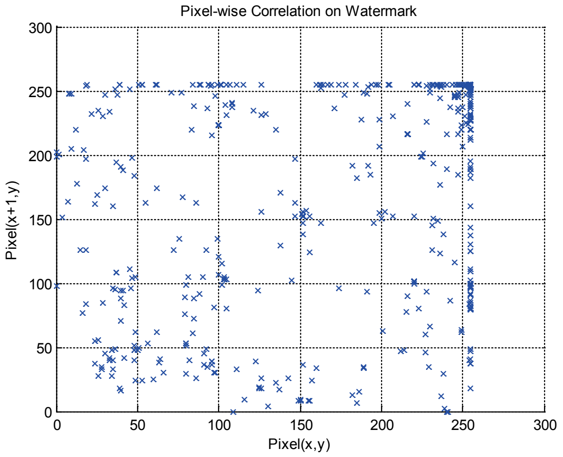

Figure 9 Correlation between adjacent pixels on watermark

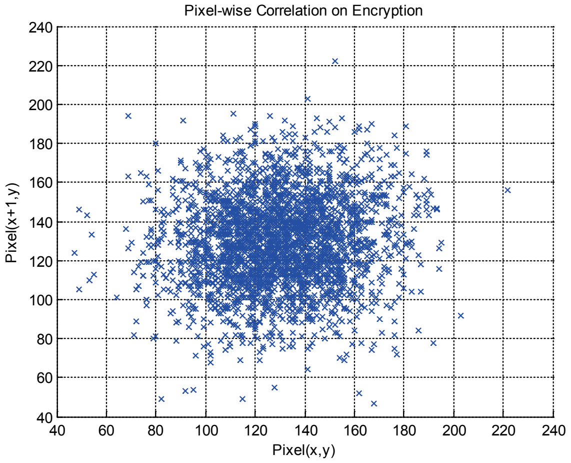

Figure 10 Correlation between adjacent pixels on encrypted watermark

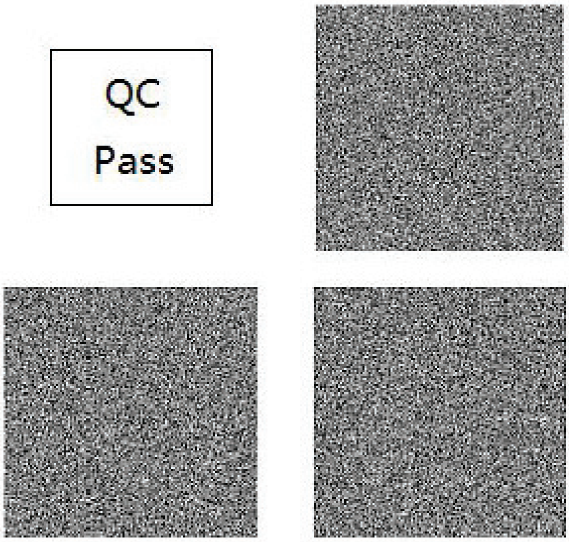

Figure 11 Sensitivity of secret key: the upper left is the original watermark, the upper right is the encrypted image, the lower left and the lower right are the decrypted images using wrong secret keys.

3.3 Time analysis

The running speed is an important factor to influence the performance of watermarking in actual applications. The averaged computational time cost for different image sizes is shown in Fig. 12. The measurement has been carried out on CORE-i5 with 1G RAM computer.

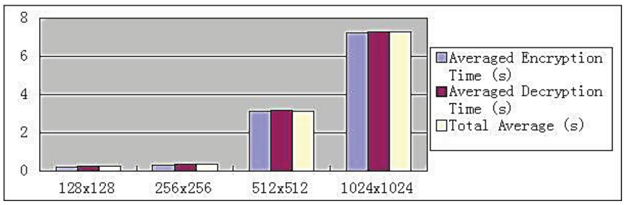

Figure 12 Measurement of computational time on various image sizes.

4 Conclusion

In this paper we studied the chaotic method of watermarking on financial bills. Many of the financial frauds can be avoided with stronger protection of the original bill images. Therefore, we adopted the edge information in the binary image to encode the watermark sequences. The key content area is then located using image features and efficient classifier methods. Since most of the deliberate changes are made to the letters or numbers on the bill, by protecting the key content we may detect those changes. We further adopt the Tent map and hash function to authenticate the watermark. The initial value is used as encryption key. The experimental results show that the proposed system is efficient in protecting financial bills, especially it can protect the numbers and letters from artificial modification. The proposed algorithm has limitation in the recognition of uncommon characters. In our future work we will investigate the improvement of hand writing characters with deep convolution network. Optimized structures in the neural network will be studied to save memory space and improve processing speed.

Acknowledgements

This work is supported by the Fundamental Research Funds for the Central Universities under Grant (2014ZDPY16).

5 References

[1] Skander, A.; Nadjim, M.; Malek, B. Synchronization chaotic communications with closed cryptographic systems. // ICIC Express Letters. 2, 3(2008), pp. 269-274.

[2] Chen, H.; Ding, Q.; Ding, L. Experimental study on secure communication of different scroll chaotic systems with identical structure. // ICIC Express Letters. 2, 2(2008), pp. 201-206.

[3] Xiang, W. Equilibrium points and bifurcation control for Lorenz-Stenflo system. // ICIC Express Letters. 3, 1(2009), pp. 61-66.

[4] Nakano, H.; Utani, A.; Miyauchi, A. An efficient data gathering scheme using a chaotic PCNN in wireless sensor networks with multiple sink nodes. // ICIC Express Letters. 3, 3(2013), pp. 10-14.

[5] Jalil, Z.; Jaffar, M. A.; Mirza, A. M. A novel text watermarking algorithm using image watermark. // International journal of innovative computing, information, and control. 7, 3(2010), pp. 1255-1271.

[6] Juang, W. S.; Fan, C. I.; Chen, M. T. Efficient Fair Content Exchange with Robust Watermark Ownership. // International Journal of Innovative Computing, Information and Control. 7, 8(2011), pp. 4653-4667.

[7] Mici, A.; Radenkovic, D.; Nikolic, S. Authentication of text documents using digital watermarking. // International

Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services, 2005, pp. 503-505.

[8] Brassil, J.; Low, S.; Maxemchuk, N. F. Copyright protection for the electronic distribution of text documents. // IEEE International Conference on Image Processing. 87, 7(1999), pp. 1181-1196. https://doi.org/10.1109/5.771071

[9] Huang, D.; Yan, H. Interword distance changes represented by sine waves for watermaking text images. // IEEE Transactions on Circuits and System. 11, 12(2001), pp. 1237-1245. https://doi.org/10.1109/76.974678

[10] Villan, R.; Voloshynovskiy, S.; Koval, O. Text data-hiding for digital and printed documents. // International Conference on Security, Steganography, and Watermaking of Multimedia Contents, 2006, pp. 1-4. https://doi.org/10.1117/12.641957

[11] Sun, Q. B.; Feng, P. R.; Deng, R. An optical watermaking solution for authenticating printed documents. // International Conference on Information Technology. 2001, pp. 65-70.

[12] Lu, H. P.; Kot, A. C.; Cheng, J. Secure data hiding in binary document images for authentication. // International Symposium on Circuits and Systems. 2003, pp. 806-809.

[13] Yang, H. J.; Kot, A. C. Binary image authentication with tampering localization by embedding cryptographic signature and block identifier. // Signal Processing Letters. 13, 12(2006), pp. 741-744. https://doi.org/10.1109/LSP.2006.879829

[14] Patra, J. C.; Ang, K. K.; Ang, E. L. Hierarchical multiple image watermarking for image authentication and ownership verification. // International Conference on Image Processing. 2004, pp. 2661-2664. https://doi.org/10.1109/ICIP.2004.1421651

[15] Kim, C.; Park, J.; Yi, J.; Turk, M. Structured light based depth edge detection for object shape recovery. // IEEE Computer Society Conference on Computer Vision and Pattern Recognition. 2005, pp. 106-108.

[16] Zhong, S. The copyright protection for the binary image based on boundary watermarking. // Master Thesis, Zhongshan University, 2015.

[17] Zhao W. L.; Ngo, C. W. Flip-invariant SIFT for copy and object detection. // IEEE Transactions on Image Processing. 22, 3(2013), pp. 980-991. https://doi.org/10.1109/TIP.2012.2226043

[18] Delalandre, M.; Iwata, M.; Kise, K. Fast and optimal binary template matching application to manga copyright protection. //11th IAPR International Workshop on Document Analysis Systems. 2014, pp. 298-303. https://doi.org/10.1109/DAS.2014.80

[19] Nejati, H.; Beirami, A.; Massoud, Y. A realizable modified tent map for true random number generation. // 51st Midwest Symposium on Circuits and Systems. 2011, pp. 1-4.

[20] He, T. T.; Luo, X.; Liao, Z.; Wei. C. A new chaos mapping hash function structural method and its application. // Acta Physica Sinica. 61, 11(2012), pp. 110506.

Authors' addresses

Rui Tao
School of Information and Control Engineering
China University of Mining and Technology
No. 1 Daxue Road, Xuzhou 221116, Jiangsu, China
E-mail: sxtaxtr@163.com

Yanjing Sun
School of Information and Control Engineering
China University of Mining and Technology
No. 1 Daxue Road, Xuzhou 221116, Jiangsu, China
E-mail: yjsun@cumt.edu.cn

Weidong Liu
Corresponding author
School of Information and Control Engineering
China University of Mining and Technology
No. 1 Daxue Road, Xuzhou 221116, Jiangsu, China
E-mail: lwdcumt@163.com