Anti-counterfeit Algorithm Based on Chebyshev Chaotic Neural Networks

Ajin Zou
Information College, Guangdong Ocean University, Zhanjiang 524088, China

Shilong Zhang *, Yana Tang, Yuli Shen
School of Information Science and Technology, Zhongkai University of Agriculture and Engineering, Guangzhou 510225, China

Renfa Li
Department of Computer and Communication, Hunan University, Changsha 410012, China

***Abstract*—In this study, an anti-counterfeiting algorithm is proposed to prevent the traceability code from being forged. The traceability code is enciphered using the encryption matrix generated by Chebyshev chaotic neural networks, which is then hidden as an invisible watermark in the package label. If the watermark can not be extracted from the package label, or the watermark extracted does not accord with the original traceability code, then it can be determined that the traceability code is counterfeit. The simulation results clearly indicate that this measure can effectively prevent the traceability code from being forged, thus help the enterprises to safeguard their legitimate rights and interests.**

Keywords-traceability code; anti-counterfeit; food safety; encryption;hiding.

I. INTRODUCTION

Food safety incidents in China have been increasing at an alarming rate over the recent years, such as the illegal use of Sudan I Red dye in fast food, melamine in milk powder, malachite green in fish, dioxin in chickens, clenbuterol in pork, and Ampullaria gigas (colony angiostrongyliasis) [1-3]. Indeed, food safety has become a matter of considerable public concern, and thus has been high on the political and business agenda in many countries. Traceability is compulsory for food business operators at all stages of the food chain from farm to consumer in the European Union, the United States, Japan, and many other countries. The GS1 Global Traceability Standard is a business process standard that describes the traceability process independently, in terms of key operations for any choice of enabling data management technologies. It is developed by a group of 73 experts from 18 countries, and has found wide applications in food industries worldwide. China has taken the initiative to implement food traceability system since 2000, and now a variety of traceability standards have been successfully developed by AQSIQ (General Administration of Quality Supervision, Inspection and Quarantine).

The traceability systems imply the use of a unique piece of data which can be traced through the entire production flow, linking all the business sections of raw material supply, production and manufacture, storage and transportation, marketing, after-sale service, and quality control. Thus, it could help to make the whole process more transparent and allow for a more stringent supervision by the authorities [8]. However, the traceability code (TC) is potentially at the risk of being forged or reproduced [9-11], because the product information is accessible from the traceability system. As a result, it is very possible for counterfeit products to also have a TC on the package, thus making it extremely difficult for customer to distinguish between counterfeit and genuine products. In this study, the TC is enciphered using the encryption matrix generated by Chebyshev chaotic neural networks (CCNN), which is then hidden as an invisible watermark in the package label. The effectiveness of the proposed method is demonstrated by a simulation example.

II. ALGORITHM FOR THE ENCRYPTION MATRIX OF CHEBYSHEV CHAOTIC NEURAL NETWORKS

A novel algorithm has been proposed previously to obtain the encryption matrix [13]. First, a chaotic sequence generated by CCNN is converted to a series of low-order integer matrices, from which encryption matrices are selected; then a higher-order encryption matrix is constructed by tensor product based on the selected encryption matrices.

The steps of the algorithm are as follows:

Step1: Let x_0 be a positive real number and n be an appropriate positive integer. A chaotic sequence $X = x_0 x_1 \cdots x_n$ is generated by the standard Logistic chaos $x_{k+1} = 4.0 x_k (1 - x_k)$.

Step2: Let X be the training sample of Chebyshev neural networks $y = \sum_{i=1}^{n} w_i T_i(x)$, where w_i is the weight between hidden and output layer, n is the number of hidden-layer neurons, and $T_i(x)$ is a group of Chebyshev orthogonal polynomials calculated by a recurrence formula $T_1(x) = 1,\ T_2(x) = x, T_{i+2}(x) = 2xT_{i+1}(x) - T_i(x) \quad i = 1, 2, \cdots, n-2$ The CCNN model is shown in Fig. 1.

Step3: Get the sequence $x = x_1 x_2 \cdots x_q$, where x_1 is the input of CCNN, and q is the length of the sequence.

Let $i=1$, the model is denoted as m and the encryption matrix as $\boldsymbol{A}_{n\times n}$.

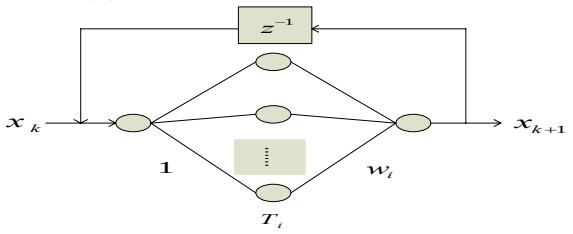

Figure 1. CCNN model

Step4: Transform all elements of $x' = x_i x_{i+1} \cdots x_{i+n^2-1}$ into integers between 0~m by $y = \mathrm{mod}(1000x', m)$, $i \leftarrow i+1$; If $i \le q - n^2$, go to Step 5; otherwise, end the process.

Step5: Transform y into an $n\times n$ matrix A, *i.e.* $\boldsymbol{A} = \mathrm{reshape}(y, n, n)$, if, $\det(\boldsymbol{A}) = 1$ output A and turn to Step 4; Otherwise, go to Step 4.

III. ENCRYPTION AND HIDING ALGORITHM

TC is potentially at the risk of being forged or reproduced [9-11], as the product information is accessible from the traceability system. To solve this problem, the encrypted TC is designed as a digital watermark and then embedded in the package label. The anti-counterfeiting principle is schematically shown in Fig. 2, where $\odot$ is the encryption algorithm and $\oplus$ is the hiding algorithm.

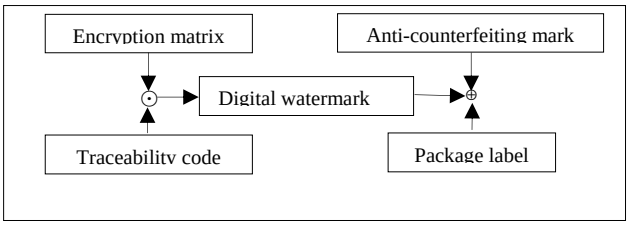

Figure 2. The principle of encryption and hiding algorithm.

A. Hiding of TC

Step1: Select an encryption matrix A. The TC T is encrypted by the encryption algorithm to obtain the digital watermark $W = A \odot T$.

Step2: Select any package label P as the vector. The invisible watermark is embedded in P to obtain the anti-counterfeiting information $D = W \oplus P$.

B. Verification of TC

Step1: Scan D' of products to be verified to extract the watermark W'.

Step2: Decrypt W' to obtain T'. If $T' = T$, the TC is true; otherwise, it is false.

IV. A SIMULATION EXAMPLE

A simulation was performed using a TC of 90×90 pixels in resolution and 0-255 in gray scale, and a package label of 150×150 pixels in resolution and 0-255 in gray scale, as shown in Fig.3a and Fig.3c, respectively.

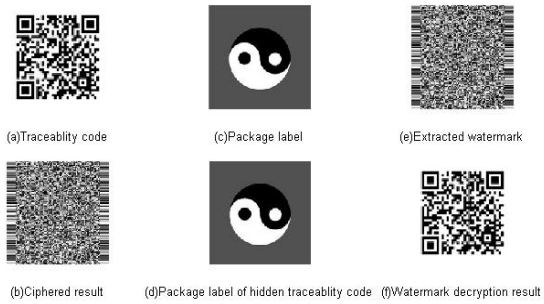

Figure 3. A schematic diagram of encryption and hiding of traceability mark.

The algorithm is as follows:

Step 1: The encryption matrices are generated by CCNN as follows [13]:

$$A_1 = \begin{bmatrix} 12 & 7 & 12 \\ 1 & 14 & 14 \\ 3 & 10 & 11 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 6 & 13 & 12 & 13 & 10 \\ 7 & 1 & 3 & 11 & 7 \\ 13 & 3 & 2 & 10 & 5 \\ 6 & 12 & 9 & 7 & 3 \\ 4 & 3 & 5 & 11 & 12 \end{bmatrix},$$

$$A_3 = \begin{bmatrix} 3 & 1 \\ 11 & 4 \end{bmatrix}, \quad A_4 \begin{bmatrix} 8 & 5 & 1 \\ 13 & 9 & 7 \\ 10 & 7 & 6 \end{bmatrix},$$

$$\boldsymbol{A}_5 = \begin{bmatrix} 1 & 8 & 13 & 6 \\ 0 & 4 & 5 & 4 \\ 10 & 13 & 8 & 9 \\ 7 & 7 & 13 & 0 \end{bmatrix}, \boldsymbol{A}_6 = \begin{bmatrix} 0 & 4 & 1 & 2 \\ 1 & 14 & 2 & 5 \\ 4 & 7 & 14 & 7 \\ 1 & 11 & 10 & 9 \end{bmatrix},$$

$$\boldsymbol{A}_7 = \begin{bmatrix} 0 & 12 & 5 & 6 \\ 10 & 15 & 1 & 5 \\ 2 & 11 & 15 & 8 \\ 7 & 3 & 10 & 3 \end{bmatrix}, \boldsymbol{A}_8 = \begin{bmatrix} 2 & 7 & 10 & 13 \\ 2 & 0 & 11 & 11 \\ 1 & 0 & 5 & 5 \\ 0 & 2 & 8 & 9 \end{bmatrix}.$$

The encryption matrix is $A = \bigotimes_{i=1}^{4} A_i$, where $\otimes$ is the tensor product of the matrix.

Step2: Calculate $W = \mathrm{mod}(AT, 256)$ to obtain the encryption results, as shown in Fig. 3b.

Step3: Calculate $D = \lambda W + (1-\lambda)P$, where $0 < \lambda < 1$. If λ is small enough, W can be embedded in P. Let $\lambda = 0.0001$, the anti-counterfeiting result D obtained by the above formula is shown in Fig. 3d.

Step4: Extract the digital watermark: $W' = 10000D - 9999P$, as shown in Fig. 3e.

Figure 4. Inspection results.

Step5: Decrypt: $T' = \mathrm{mod}(A^{-1}W', 256)$, as shown in Fig. 3f.

Step6: Security inspection: Let *V=T-T'*, Inspection results as shown in Fig. 4. If *V=0*, TC is true; If *V≠0*, then *T≠T'*, it is white or other pattern, at this time TC is forged.

V. SECURITY ANALYSIS

Different Logistic chaotic initial values x_1 in CCNN result in different chaotic sequences $x = x_1 x_2 \cdots x_q$, which in turn result in different encryption matrices A [13]. Thus, the algorithm proposed in this study can produce a "one-time pad cipher" encryption matrix with high security, which is theoretically undecipherable according to Shannon's information theory.

We calculated the correlations of the horizontally, vertically or diagonally adjacent pixels in both original and ciphered images according to Eq. (1) [14]:

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{1}$$

$$\begin{cases} \mathrm{cov}(x, y) = \dfrac{1}{N}\sum_{i=1}^{N}(x_i - E(x_i))(y_i - E(y_i)) \\ E(x) = \dfrac{1}{N}\sum_{i=1}^{N} x_i, D(x) = \dfrac{1}{N}\sum_{i=1}^{N}(x_i - E(x_i))^2 \end{cases} \tag{2}$$

Where x and y are gray values of the two adjacent pixels. The correlations of the horizontally, vertically, and diagonally adjacent pixels in the original and ciphered images are shown in Fig. 5a and 5b, Fig. 6a and 6b, and Fig. 7a and 7b, respectively.

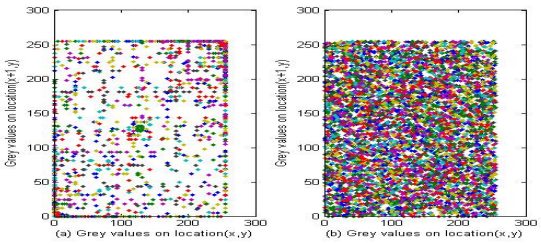

Figure 5.Correlations of horizontally adjacent pixels.

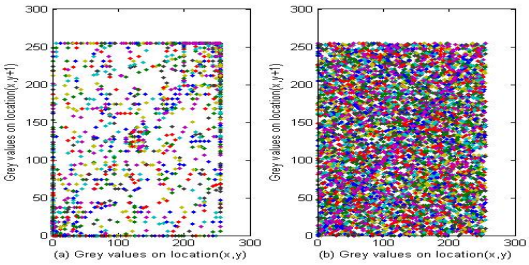

Figure 6. Correlations of vertically adjacent pixels.

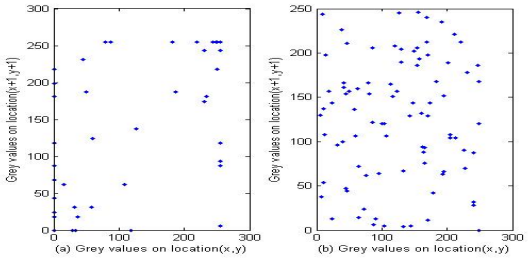

Figure 7. Correlations of diagonally adjacent pixels.

Table 1 shows the correlation coefficients of horizontally, vertically, and diagonally adjacent pixels of the traceability image and ciphered image. Obviously, it approaches 1 in the traceability image, indicating that the pixels are highly correlated; on the opposite, it approaches 0 in the ciphered image, indicating that the pixels are almost uncorrelated. Thus, the statistical nature of the traceability code has been well proliferated into the stochastic ciphered image.

TABLE I. CORRELATION COEFFICIENTS OF TWO ADJACENT PIXELS

No.	Direction	Traceability image	Ciphered image
1	Horizontal	0.7374	-0.0106
2	Vertical	0.7236	0.2620
3	Diagonal	0.8178	0.0074

VI. ENCRYPTION EFFICIENCY COMPARISON

Fig.8a. is a standard image Lena (the picture size is 256×256 pixels and the gray level equals 0~255) provided by Matlab. In order to comparison of the encryption result generated by different encryption algorithms, let $\boldsymbol{A}' = \bigotimes_{i=5}^{8} \boldsymbol{A}_i$, then the correlation coefficients of horizontal, vertical, and the diagonal adjacent pixels of ciphered image Lena are 0.0010, -0.0027 and 0.0657. The encryption and Decrypted result as shown in the Fig.8b. and 8c., the correlations coefficients of horizontally adjacent pixels in the original image and ciphered image as shown in the Fig.9a. and 9b., respectively.

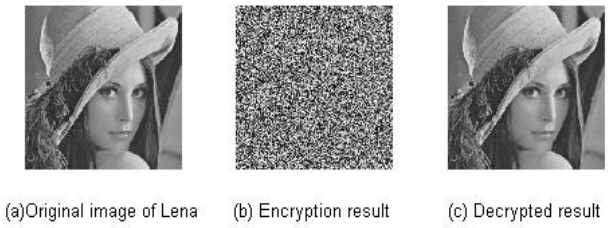

Figure 8. Encryption and Decrypted result.

The correlation coefficients encryption results of image Lena by different encryption algorithms are given in Table 2. Generally speaking, the adopted algorithm gives better encryption results at horizontal and vertical direction than ones presented by Refs. [15-20].

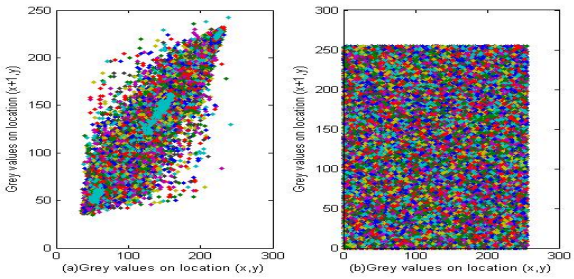

Figure 9. Correlations coefficients of horizontally adjacent pixels

TABLE II. THE COMPARISON OF CORRELATION COEFFICIENTS GENERATED BY DIFFERENT ENCRYPTION ALGORITHMS

No.	Algorithm	Horizontal	Vertical	Diagonal
1	Paper	0.0010	-0.0027	0.0657
2	Ref. [15]	0.0058	0.0072	0.0031
3	Ref. [16]	0.0102	-0.0035	-0.0161
4	Ref. [17]	0.0026	0.0034	-0.0019
5	Ref. [18]	0.0046	0.0040	0.0017
6	Ref. [19]	-0.0069	-0.0188	-0.0235
7	Ref. [20]	0.0024	0.0012	0.0016

VII. CONCLUSIONS

In this study, an anti-counterfeiting algorithm is proposed to prevent the traceability code from being forged. First, the traceability code is enciphered using the encryption matrix generated by Chebyshev chaotic neural networks, which is then hidden as an invisible watermark in the package label. If the watermark can not be extracted from the package label, or the watermark extracted does not accord with original code, then it can be determined that the traceability code is counterfeit. The simulation results clearly indicate that this measure can effectively prevent the traceability code from being forged, and help the enterprise to safeguard their legitimate rights and interests.

ACKNOWLEDGEMENTS

The research work was supported by the National Natural Science Foundation of China (No. 61173036), Guangdong Provincial Natural Science Foundation (No. S2012010009976), Guangdong Provincial Science and Technology Plan Project (No. 2011B020313021, 2011B040200074, 2012B020314007, 2012B010100048), and Zhanjiang Municipal Plan Project for Science and Technology Development (No. 2011C3105001).

REFERENCES

[1] Lin, J., Xie, R., He, X.T., On .Net-based food quality and safety tracing technique and its implementation. *Computer Applications and Software,* 27(1), pp.145-147, 2010.

[2] Yu, H., Wu, Z.H., Algorithm for agricultural product trace code. *Jiangsu Agricultural Sciences,* 39(6), pp. 622-624, 2011.

[3] Wang, Y.F., Yang, Y., Liu, A.J., Design of Traceability System for the Fresh Meat Product Entire Processes Based on RFID Technology. *Modern Scientific Instruments,* 21(1), pp.15-17, 2012.

[4] Liu, J.Y., Shang, X.B., Current state and development trends of food electronic trace code. *China Quality Supervision,* (12), pp.51, 2012.

[5] Meng, M., et al., Coding Research of Circulation Code and Back Yards of Agricultural Products. *Chinese Journal of Tropical Agriculture,* 30(1), pp.82-85, 2010.

[6] Yu, H., Wu, Z.H., Study on the agricultural product trace coding. *Scientia Agricultura Sinica,* 44(23), pp.4801-4806, 2011.

[7] Chen, T., Mao, L., Mao, Y., Design and implementation of the intelligent terminal system for agricultural product trace coding. *Jiangsu Agricultural Sciences,* 41(6), pp.273-275, 282, 2013.

[8] Li, W.Y., et al., Design and implementation of encryption algorithm for agricultural products traceability code based on embedded platform. *Transactions of the Chinese Society of Agricultural Engineering,* 28(17), pp.253-259, 2012.

[9] Gao, Y.S., Xu, C.G., Study on a safe and practical two-dimension code. *Netinfo Security,* (10), pp.47-50, 2012.

[10] Wang, K., Yu, P., Study of authentication method with photo for forgery detection in printed materials based on digital watermark technology. *Manufacturing Automation,* 34(4), pp.34-37, 2012.

[11] Liu, W., Design of smart tag-based anti-counterfeiting system. *Science & Technology Information,* (9), pp.6-7, 2013.

[12] Li, W.Y., et al., Design and implementation of encryption algorithm for aquatic products traceability code. *Transactions of the Chinese Society for Agricultural Machinery,* 43(4), pp.106-112, 2012.

[13] Zou, A.J., Wu, W., Li, Y.J., Construction of the encryption matrix based on Chebyshev chaotic neural network. *Journal of Electronics,* 29(3/4), pp.248-253, 2012.

[14] Gao, T.G., Chen, Z.Q., A new image encryption algorithm based on hyper-chaos. *Physics Letters A, ,* 372, pp.394–400. 2008

[15] Rasul, E., Abdul H.A., Ismail F.I., Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. *Optics and Lasers in Engineering,* (56), pp.83-93, 2014.

[16] Zhou, Y.C., Cao, W.J., Chen, P.C.L, Image encryption using binary biplane. *Signal Processing,* (100), pp.197-207, 2014.

[17] Armand Eyebe Fouda , J.S., Yves Effa , J., Sabat, S.L., Ali, M., A fast chaotic block cipher for image encryption. *Commun Nonlinear Sci Numer Simulat,* (19), pp.578–588, 2014.

[18] Zhang, Q., Liu, L.L., Wei, X.P., Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps. *International Journal of Electronics and Communications (AEÜ),* (68), pp.186-192, 2014.

[19] Sui, L.S., Lu, H.W., Wang, Z.M., Sun, Q.D., Double-image encryption using discrete fractional random transform and logistic maps. *Optics and Lasers in Engineering* (56), pp.1-12, 2014.

[20] Zhang, Q., Wei, X.P., A novel couple images encryption algorithm based on DNA subsequence operation and chaotic system. *Optic.* (124), pp. 6276-6281, 2013.