An Automatic Identification Algorithm for Encrypted Anti-counterfeiting Tag Based on DWT-DCT and Chen's Chaos

Qianning Dai[1], Jingbing Li[1,2(✉)], Uzair Aslam Bhatti[1], Jieren Cheng[1], and Xiaobo Bai[3]

[1] College of Information Science and Technology, Hainan University, Haikou 570228, China
dqn0526@163.com, Jingbingli2008@hotmail.com, uzairslambhatti@hotmail.com, cjr22@163.com

[2] State Key Laboratory of Marine Resource Utilization in the South China Sea, Hainan University, Haikou 570228, China

[3] Hainan College of Software Technology, Qionghai 57400, Hainan, China
baixiaobols@163.com

Abstract. The production, distribution, and consumption of counterfeit goods have been increasing at an alarming rate around the world. In order to resist the bad influence of fake and inferior products, an automatic encryption algorithm for anti-counterfeiting tags based on DWT-DCT and Chen's chaos is proposed in this paper. Chen's chaos is used to encrypt anti-counterfeiting tags on the basis of anti-counterfeiting technology in the algorithm, and the feature vectors are extracted from the encrypted tags by DWT-DCT. Then we set up the corresponding feature vector database. The normalized correlation coefficient (NC) is used to realize the automatic identification of encrypted anti-counterfeit tags. The experimental results show that the algorithm has a good robustness to common and geometrical attacks and has a larger key space to resist attacks such as brute-force attack and other deciphering methods. The results of our experiments indicate that the proposed algorithm is satisfactory in term of the higher security and extraordinary speed as compared to the existing algorithms.

Keywords: Automatic identification · DWT-DCT · Feature extraction · Chaos encryption · Anti-counterfeiting

1 Introduction

With the rapid development of the market economy, fake and inferior products have become rampant and seriously infringe the rights and interests of consumers. Therefore, in order to resist fake and inferior products a lot of research has been done in the past 20 years, anti-counterfeiting technology has developed rapidly. At present, the most widely used Quick Response code [1–3] and barcode anti-counterfeiting methods can realize automatic identification fast, but it is easy to copy and imitate because of its surface printing. However, the research hotspot in the field of anti-counterfeiting at

X. Sun et al. (Eds.): ICAIS 2019, LNCS 11634, pp. 596–608, 2019.
https://doi.org/10.1007/978-3-030-24271-8_53

present – RFID anti-counterfeiting technology [4–6] are difficult to apply to the market due to its high cost. In view of the existing problems of anti-counterfeiting technology, some engineers have proposed a new anti-counterfeiting technology–authentic anti-counterfeiting technology [7].

Authentic work anti-counterfeiting is a new anti-counterfeiting technology which makes use of special textpatterns. Each word in the selected phrase is rotated at random angles and then carved randomly according to the text to form a unique text pattern. This kind of unique character design tag made randomly is used for anti-counterfeiting [8].

In this paper, the anti-counterfeiting tags are encrypted and stored in the cloud on the basis of authentic work anti-counterfeiting. Experiments show that the security performance of encrypted anti-counterfeiting tags is improved without loss of robustness [9]. Compared with the low-dimensional chaotic system which has the defect of small secret keyspace and low security [10, 11], the high dimensional chaotic image encryption algorithm proposed in this paper has higher complexity, randomness, and unpredictability, and able to resist attacks such as brute attack and other deciphering methods better.

2 The Fundamental Theory

2.1 Logistic Map

The logistic map is one of the most famous chaotic maps, which is a simple dynamic nonlinear regression with chaotic behavior. Even small changes in the initial value can cause significant differences in the output sequence [10–12], and it has statistical properties similar to white noise. Its mathematical definition can be expressed as follows:

$$x_{k+1} = \mu x_k(1 - x_k) \tag{1}$$

where $0 \leq \mu \leq 4$ and $xk \in (0, 1)$ are the system variable and parameter respectively, and k is the number of iteration. Logistic Map system works under haotic condition when $3.569945 \leq \mu \leq 4$. It can be seen that a small difference in initial conditions would lead to a significant difference of chaotic sequences. These statistical characteristics are the same as white noise, so the above sequence is an ideal secret key sequence. In this paper, we set $\mu = 4$, and the chaotic sequences are generated by different initial values.

2.2 Chen's Chaotic System

In 2002, Lü et al. connected the Lorenz system and Chen's system with a new three-dimensional chaotic system [13], calling it a unified chaotic system. Its mathematical definition can be expressed as follows:

$$\begin{cases} \dot{x} = (25a + 10)(y - x), \\ \dot{y} = (28 - 35a)x - xz + (29a - 1)y, \\ \dot{z} = xy - (8 + a)z/3 \end{cases} \tag{2}$$

Where $(x, y, z) \in R^3$ is the state of the system,and the system parameter $a \in [0, 1]$. The unified system has the characteristic of regional chaos. When $a \in [0, 0.8]$ the system belongs to the generalized Lorenz system; when $a = 0.8$ the system belongs to the generalized Liu system; when $a \in [0.8, 1]$ the system belongs to the generalized Chen's system [14]. Here we take $a = 1$ to construct the encryption key of the image with the chaotic sequence generated by the generalized Chen's system. Chen's chaotic system is very similar to Lorenz chaotic system, but it is not topological equivalent to Lorenz chaotic system, which is a new system with more complex dynamic characteristics than Lorenz chaotic system [15]. Here we take x(0) = 0, y(0) = 1, z(0) = 0 as the initial value; integration time step h = 0.001 [16]. The fourth-order Runge-Kutta method is used to solve the differential Eq. (2) to obtain the trajectory curve of the system phase space. As shown in Fig. 1, it can be seen that the phase space trajectory of Chen's chaotic system is composed of many discrete points, which indicates that the system has complex chaotic characteristics.

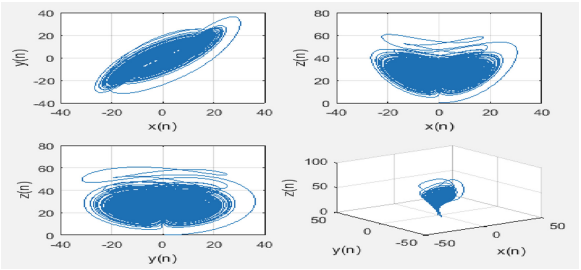

Fig. 1. Chaotic behavior of Chen's system: $x(n), y(n), z(n)$ are the Chen's chaotic sequences.

2.3 The Discrete Wavelet Transform (DWT)

The wavelet transform is a time-frequency transform, which can be used for multiresolution analysis. It is aimed to use the wavelet function to decompose the signal. The discrete wavelet transform is obtained by discretization of scale and shift of basic wavelet. Define the wavelet function $\psi_{a,b}(t)$ as the base, and the wavelet transform of $f \in L^2(R)$ by is defined as:

$$W_{f(a,b)} = \int_R f(t)\bar{\psi}_{a,b}(t)dt \quad k \in Z \tag{3}$$

Where the wavelet function $\psi_{a,b}(t)$ is obtained by translating and scaling the same base ψ.

$$\psi_{a,b}(t) = |a|^{-1/2}\psi((t-b)/a) \quad a, b \in R, a \neq 0 \tag{4}$$

Where ψ is called the base wavelet, a is the dilation factor, b is the translation factor. Mallat wavelet algorithm decomposition formula is as follows:

$$c_{j+1,k} = \sum_{n=Z} c_{j,n}\bar{h}_{n-2k} \quad k \in R \tag{5}$$

$$d_{j+1,k} = \sum_{n=Z} c_{j,n}\bar{g}_{n-2k} \quad k \in Z \tag{6}$$

Mallat wavelet algorithm reconstruction formula is as follows:

$$c_{j,k} = \sum_{n=Z} c_{j+1,n}h_{n-2k} + \sum_{n=Z} d_{j+1,n}g_{n-2k} \quad k \in Z \tag{7}$$

After one-level wavelet decomposition is performed on the image, a low-frequency subgraph and three high-frequency subgraphs can be obtained.

2.4 The Discrete Cosine Transform (DCT)

The discrete cosine transform (DCT) is similar to the Fourier transform. The discrete cosine transform takes only the real part of the Fourier transform. Discrete cosine transform has a very important property–energy concentration characteristics: After discrete cosine transform of the image, the energy is concentrated in the low-frequency part of the spectrogram. When applied to an M × N size image or matrix, the 2D-Discrete Cosine Transform (DCT) is as follows:

$$F(u,v) = c(u)c(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\cos\frac{\pi(2x+1)u}{2M}\cos\frac{\pi(2y+1)v}{2N} \tag{8}$$
$$u = 0,1,\cdots,M-1; v = 0,1,\cdots,N-1;$$

In the formula:

$$c(u) = \begin{cases} \sqrt{1/M} & u = 0 \\ \sqrt{2/M} & u = 1,2,\cdots,M-1 \end{cases}$$

$$c(v) = \begin{cases} \sqrt{1/N} & v = 0 \\ \sqrt{2/N} & v = 1,2,\cdots,N-1 \end{cases}$$

Where M × N is the anti-counterfeiting image size, $f(x,y)$ correspond to the value of the anti-counterfeiting image at the point (x,y) and $F(u,v)$ is the DCT coefficient at the point (u,v) in the frequency. The Formula shows that the sign of the DCT coefficient is related to the phrase of the component.

3 The Algorithm

In this paper, an authentic work anti-counterfeiting tag is selected as the original anti-counterfeiting tag. It is written as $F = \{F(i,j)|F(i,j) \in [0,255]; 1 \le i \le M, 1 \le i \le N\}$,

where $F(i,j)$ represents the pixel grayscale value of the original authentic work anti-counterfeiting tag. The specific algorithm is as follows. The algorithm process is shown in Fig. 2.

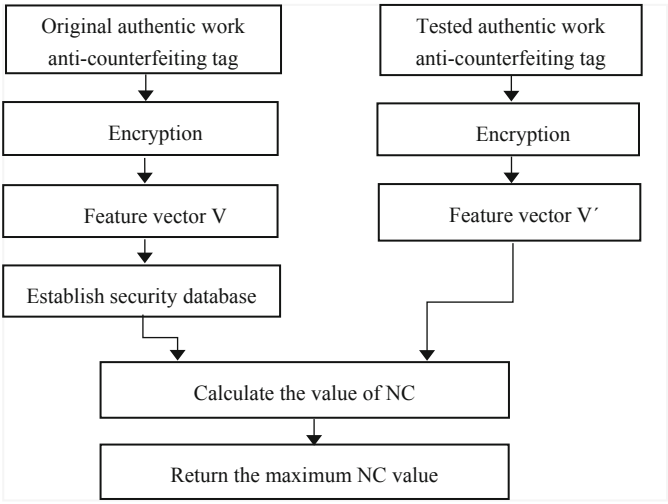

Fig. 2. Automatic identification of encryption security tag based on transform domain.

3.1 Establishing an Encrypted Anti-counterfeiting Tag Feature Database

Original Authentic Work Anti-counterfeiting Tag Encryption. The encryption algorithm flow is shown in Fig. 3.

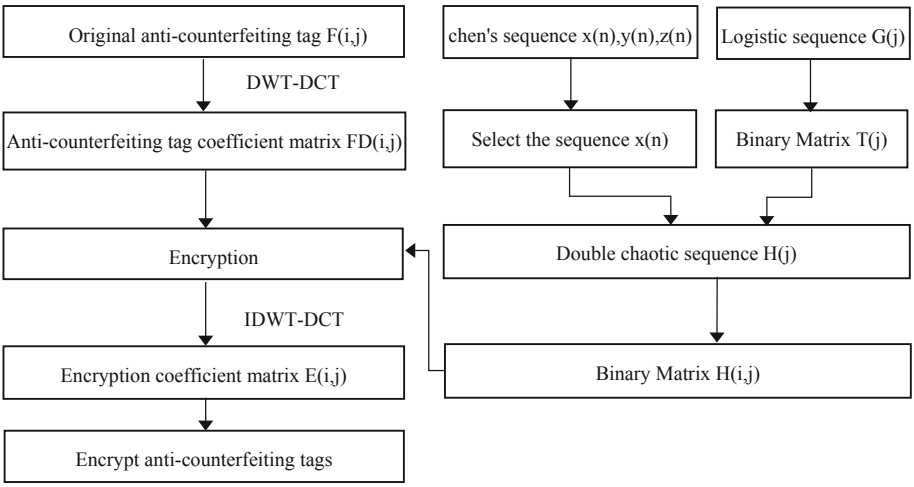

Fig. 3. Original anti-counterfeit tag encryption process.

The anti-counterfeiting tag is encrypted as follows:

Step 1: The DWT transform is performed on the anti-counterfeiting tag to obtain f_A,f_B,f_C,f_D subband wavelet coefficients.

$$\{f_A,f_B,f_C,f_D\} = DWT2(F(i,j)) \tag{9}$$

Step 2: The DCT transform is performed on wavelet subband coefficients f_A,f_B, f_C,f_D to obtain DCT coefficients $FD(i,j)$.

$$FD(i,j) = DCT2(f_A,f_B,f_C,f_D) \tag{10}$$

Step 3: Generate chaotic sequence $G(j)$ from the initial value by using Logistic map, and binarize it to get $T(j)$, from the initial $x(0), y(0), z(0)$, Chen's chaotic real-valued sequence $x(n), y(n), z(n)$ is generated by the Runge-Kutta fourth-order method. Selecting one of Chen's chaos sequences such as $x(n)$ and performing point multiplication with $T(j)$ to obtain a double chaotic sequence $H(j)$.

Step 4: Construct a binary sequence. According to the chaotic sequence $H(j)$, a threshold function $sng(x)$ is set to obtain a sequence of binary symbols, and a binary matrix $H(i,j)$ is formed according to the size of the anti-counterfeiting tag, where $1 \le i \le M$, $1 \le j \le N$.

$$sng(H(j)) = \begin{cases} 1 & H(j) \ge 0.5 \\ -1 & H(j) < 0.5 \end{cases} \tag{11}$$

Step 5: Multiply the coefficient matrix with the binaries matrix to obtain $D(i,j)$.

$$D(i,j) = FD(i,j). * H(i,j) \tag{12}$$

Step 6: Perform inverse DCT transformation on $D(i,j)$ to obtain an encrypted anti-counterfeit tag $ED'(i,j)$ and obtain an encrypted sub band wavelet coefficient sequence matrix after reconstruction.

$$ED'(i,j) = IDCT \;\; 2(D(i,j)) \tag{13}$$

Step 7: Perform IDWT transformation on $ED'(i,j)$ to obtain an encrypted anti-counterfeiting tag.

$$E(i,j) = IDWT2(ED'(i,j)) \tag{14}$$

Figure 4 shows 8 different authentic work anti-counterfeiting tags, and Fig. 5 shows the corresponding encrypted anti-counterfeiting tags. The original image of the encrypted image is invisible to the naked eye, so it is of no value to others after the leak. In this way, the security and reliability of anti-counterfeiting tags are improved.

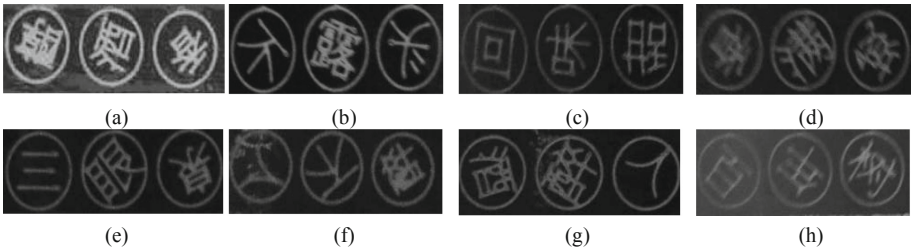

Fig. 4. 8 different anti-counterfeit tags.

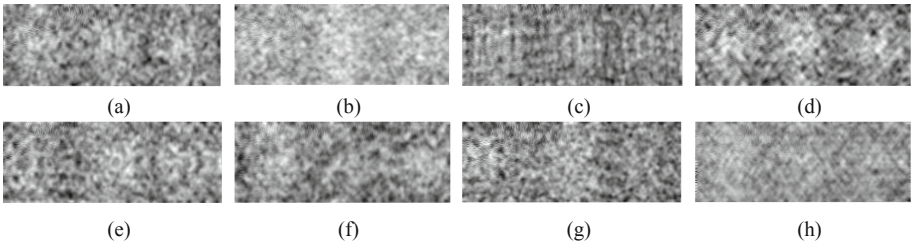

Fig. 5. 8 corresponding encrypted anti-counterfeit tags.

Key Sensitivity and KeySpace. The initial values of the chaotic system used for decryption are: $x'(0) = x(0) + 10^{-8}$, $y'(0) = y(0)$ and $z'(0) = z(0)$.. Only $x'(0)$ differs by 10^{-8} from the value $x(0)$ used for encryption, the decryption results are shown in the figure below. As you can see, the subtle differences in the key make it undecipherable. The sensitivity test results to $y(0)$ and $z(0)$ indicate that when $y(0)$ and $z(0)$ change 10^{-8} respectively, they cannot be decrypted. The above results show that the algorithm is highly sensitive to keys. If the initial value of the chaotic system is the initial key, represented by a double-precision real number that is accurate to 9 decimal places, so the key space is $10^9 \times 10^9 \times 10^9 = 10^{27} \approx 2^{90}$ which equivalents to a 90-bit long keyspace. It means that extending the key space of 90 bits long on the basis of one-dimensional chaos. Therefore, the password system is strong enough to resist attacks such as brute-force attack and other deciphering methods.

Fig. 6. When x(0) error is 1×10^{-8}: (a) original anti-counterfeiting tag; (b) decrypted tag.

Extract the Feature Vector of the Encrypted Anti-counterfeiting Tag. First, we carry out the first level DWT transform of the original anti-counterfeiting tag to obtain

Table 1. Change of DWT-DCT low-frequency coefficients under different attacks to encrypted tag.

Image processing	PSNR (dB)	C1	C2	C3	C4	C5	C6	C7	C8	Sequence of coefficient signs	NC
Encrypted original image	90.19	164.09	−2.68	−0.09	0.42	0.79	−0.67	−14.13	−0.11	10011000	1.00
Gaussian noise (5%)	13.23	163.62	−2.26	−1.09	0.10	1.16	−1.18	−13.87	0.31	10011001	0.84
JPEG compression (5%)	24.28	163.72	−3.10	−0.08	0.42	1.37	−0.79	−14.58	−0.11	10011000	0.75
Median filter [3 × 3] (10 times)	26.95	162.58	−3.00	−0.72	0.17	0.18	−0.78	−14.69	−0.20	10011000	0.85
Zoom (×2.0)		325.95	−5.25	−0.22	1.00	1.88	−0.62	−28.12	−1.03	10011000	0.85
Zoom (×0.5)		83.16	−1.50	−0.08	0.05	0.15	−0.69	−7.16	0.29	10011001	0.97
Translation (2%, left)	18.32	161.91	0.81	−3.36	4.06	−2.29	4.59	−16.85	0.43	11010101	0.71
Translation (2%, down)	19.26	156.70	−2.65	−0.30	0.42	0.72	−0.67	−13.39	−0.21	10011000	0.78
Shearing (3%, Y direction)		162.27	−2.67	−0.12	0.45	0.82	−0.75	−13.80	−0.07	10011000	0.85
Shearing (2%, X direction)		162.71	−2.90	0.25	0.06	1.38	−2.23	−13.86	1.47	10111001	0.82

four subgraphs. Second, we take the low-frequency subgraph for global DCT transform. Then the low intermediate frequency coefficient is extracted after transformation. "one" is used to represent the positive coefficients, and "zero" is used to represent the negative coefficients. Thus, we can obtain a series of binary logic sequences based on the DWT-DCT transformed coefficient symbols. We take this binary logical sequence as the feature vector of the authentic anti-counterfeiting tag. In order to verify the robustness of the feature vector extracted by this method. We selected eight number of DWT-DCT to transform low intermediate frequency coefficients (C1, C2, …, C8), which is shown in the third column to the tenth column of Table 1. The corresponding binary logical sequence is shown in column eleven of Table 1. We can see the normalized correlation coefficient (NC) of the feature vectors obtained under various types of attacks is relatively large with that of the feature vectors of the original encrypted tag from column twelve in table one. In conclusion, we can think that DWT-DCT transform after the coefficient symbol sequence can be used as tag's feature [17, 18].

Table 2. Correlation coefficients of feature vector of different encrypted tags.

	V1	V2	V3	V4	V5	V6	V7	V8
V1	1.00	0.03	−0.08	0.16	0.14	0.18	0.28	0.06
V2	0.03	1.00	0.20	0.13	0.42	−0.23	0.25	0.09
V3	−0.08	0.20	1.00	0.01	0.08	−0.02	−0.19	0.10
V4	0.16	0.13	−0.01	1.00	0.02	0.04	0.25	−0.03
V5	0.14	0.42	0.08	0.02	1.00	0.08	0.03	0.07
V6	0.18	−0.23	−0.02	0.04	0.08	1.00	−0.22	0.19
V7	0.28	0.25	−0.19	0.25	0.03	−0.22	1.00	−0.09
V8	0.06	0.09	0.10	−0.03	0.07	0.19	−0.09	1.00

The DWT-DCT coefficient unit is 1.0e+002, and the correlation coefficient is 64 bit.

From Table 2, it is not hard to find that the correlation coefficient is 1, only when the encrypted anti-counterfeiting tag is compared with their own, which is smaller when the encrypted tag is compared with other tags. Those with a minimum of −0.23 and a maximum of 0.42 are generally less than 0.5. The more similar the tag is, the greater the correlation coefficient is, and vice versa. Therefore, it can be seen that it is feasible to select the low medium frequency coefficient as the feature vector of the encrypted anti-counterfeiting tag.

3.2 Automatic Identification of Encrypted Anti-counterfeiting Tags

An anti-counterfeiting tag $F'(i,j)$ is selected to be tested, which perform the same encryption processing and feature extraction as the steps described in the previous section, and we get the feature vector $V'(j)$ to be measured. Then calculate the peak signal-to-noise ratio (PSNR) and the normalized correlation coefficient (NC). The PSNR reflects the quality of the anti-counterfeit tag image after being attacked. The higher the PSNR value, the better the image quality. The NC value reflects the similarity between the two graphs. The larger the NC value, the higher the similarity between the two graphs.

$$PSNR = 10 \lg \left[\frac{MN \max\limits_{i,j} \left(I_{(i,j)}\right)^2}{\sum\limits_i \sum\limits_j \left(I_{(i,j)} - I'_{(i,j)}\right)} \right] \tag{15}$$

$$NC = \frac{V(i) \times V'(j)}{V^2(j)} \tag{16}$$

Where $I(i,j)$ is the pixel value of each image, $\Gamma(i,j)$ is the average pixel value of the image and M and N are the rows and columns of the texture image. Finally, determine whether NC value is greater than 0.5. If the NC value is greater than 0.5, the detected maximum NC value and his corresponding tag are returned to the consumer. If the NC value is less than 0.5, a message is returned to the consumer: the product is false.

4 Simulation and Analysis

In the MATLAB R2016a simulation platform, we selected an encrypted anti-counterfeiting tag to perform a common attack and geometric attack simulation experiments. Select 1000 sets of independent pseudo-random binary logic sequences (values 1 or 0) with a length of 32 bits. Among these 1000 sets of data, one set (this article uses the 500th set of data) is selected as the embedded feature vector. The original encrypted anti-counterfeit tag is shown in Fig. 6 who is denoted as $F(i,j)$, $1 \leq \mathrm{i} \leq 220, 1 \leq \mathrm{j} \leq 76$. The corresponding DWT-DCT coefficient matrix is denoted as $FD(i,j)$. Considering the complexity and speed of the algorithm, we select the low intermediate frequency $4 \times 8 = 32$ coefficients for symbolic operations to obtain the feature vector V(j).

In the simulation results, the PSNR value is used to measure the quality of the anti-counterfeit tag to be tested, and the NC value is used to evaluate whether the image to be tested is the original encryption anti-counterfeiting tag. We set the determination threshold of the NC value to 0.5. If the NC value is greater than or equal to 0.5, we consider that the encryption anti-counterfeiting tag under test is the original encryption anti-counterfeiting tag. If the NC value is less than 0.5, it is determined that the encrypted anti-counterfeiting tag to be tested is not the original encrypted anti-counterfeiting tag. We can see from Tables 3, 4, 5 and 6, compared with the original anti-counterfeiting tags, the security performance of the encrypted anti-counterfeiting tags is improved without loss of robustness. The NC values between the 1000 available pseudo morph sequences and the extracted feature vector is achieved by using DWT-DCT and symbolic operation.

4.1 Gaussian Attack

Gaussian noise intensity coefficient is measured the added noise interference size in the encrypted anti-counterfeiting tag. Under the Gaussian attack, the corresponding NC valuels is shown in the Table 3. NC1 corresponds to the NC value of the encrypted image, while NC2 corresponds to the NC value of the original image. We still can extract the encrypted anti-counterfeiting image at this situation. Table 3 shows that the algorithm can resist Gaussian attack.

Table 3. The PSNR and NC values under Gaussian noise.

Noise intensity/%	1	2	3	5	10	15
PSNR/dB	19.95	16.88	15.11	13.23	10.9	9.89
NC1	0.89	0.87	0.90	0.84	0.75	0.62
NC2	0.88	0.82	0.82	0.87	0.65	0.68

4.2 JPEG Compression Attack

The percentage of the compression quality is examined the impact after JPEG compression for the encrypted anti-counterfeiting tag. Under the Gaussian attack, the

corresponding NC valuels is shown in the Table 4. NC1 corresponds to the NC value of the encrypted image, while NC2 corresponds to the NC value of the original image. The encrypted anti-counterfeiting image can still be accurate to extract. Table 4 shows that the algorithm can resist JPEG compression attack.

Table 4. PSNR and NC values under JPEG compression attack.

Compression quality/%	2	5	10	20	30	40
PSNR/dB	21.50	24.28	27.33	29.83	31.05	31.65
NC1	0.79	0.75	0.85	1.00	1.00	0.90
NC2	0.75	0.75	0.93	1.00	1.00	0.82

4.3 Scaling Attack

Under the Gaussian attack, the corresponding NC valuels is shown in the Table 3. NC1 corresponds to the NC value of the encrypted image, while NC2 corresponds to the NC value of the original image. We still can extract the encrypted anti-counterfeiting image accurately. Table 5 shows that the algorithm can resist scaling attack.

Table 5. The PSNR and NC values under scaling attack.

Percentage	0.2	0.5	0.8	1.1	1.5	2.0
NC1	0.55	0.97	0.87	0.87	0.85	0.85
NC2	0.88	1.00	1.00	0.94	1.00	1.00

4.4 Shearing Attack

The encrypted anti-counterfeiting tag is sheared from the Y-axis direction. Under the Gaussian attack, the corresponding NC valuels is shown in the Table 3. NC1 corresponds to the NC value of the encrypted image, while NC2 corresponds to the NC value of the original image. The encrypted anti-counterfeiting image can still be accurate to extract. Table 6 shows that the algorithm can resist shearing attack.

Table 6. The PSNR and NC values under shearing attack.

Parameter/°	1	3	5	6	7	8
NC1	0.97	0.85	0.69	0.69	0.69	0.59
NC2	1.00	0.85	0.59	0.56	0.56	0.46

5 Conclusion

In order to improve the security performance of the anti-counterfeiting tag, the paper presents an automatic identification algorithm based on DWT-DCT and Chen's chaos for anti-counterfeit tags. The feature vector is extracted by a DWT-DCT transform from the encrypted authentic work anti-counterfeiting tags. The identification of anti-counterfeiting tags is completed by calculating the normalized correlation coefficient (NC). Experiments show that the algorithm has the good robustness to common attack and geometric attack and larger keyspace against powerful attacks. Compared with the original anti-counterfeiting tags, the security performance of the encrypted anti-counterfeiting tags is improved without loss of robustness. It has high security and simple operation. This algorithm only requires the use of the Internet and the ordinary photo-taking function to realize the identification of encrypted tags, which is convenient and fast, and it is an identification method adapted to large data [19].

Acknowledgments. This work is supported by the Key Research Project of Hainan Province [ZDYF2018129], and by the National Natural Science Foundation of China [61762033] and the Natural Science Foundation of Hainan [20166227, 617048, 2018CXTD333] and the Key Innovation and Entrepreneurship Project of Hainan University [Hdcxcyxm201711].

References

1. Wang, W.W.: Research and application of commodity anti-counterfeiting system based on mobile QR code technology. Beijing University of Posts and Telecommunications (2012)
2. Liu, S.Y.: Anti-counterfeit system based on mobile phone QR code and fingerprint. In: Intelligent Human-Machine Systems and Cybernetics (IHMSC), pp. 236–240 (2010)
3. Sun, A.D., Sun, Y., Liu, C.X.: The QR-code reorganization in illegible snapshots taken by mobile phones. In: Fifth International Conference on Computational Science and Applications (ICCSA), pp. 532–538 (2007)
4. Choi, S.H., Yang, B., Cheung, H.H., et al.: RFID tag data processing in manufacturing for track-and-trace anti-counterfeiting. Comput. Ind. **68**, 148–161 (2015)
5. Yan, B., Huang, G.W., et al.: Application of RFID and internet of things in monitoring and anti-counterfeiting for products. In: Business and Information Management (ISBIM), pp. 392–395 (2008)
6. Chen, C.L., Chen, Y.Y., Shih, T.-F., et.al.: An RFID authentication and anti-counterfeit transaction Protocol. In: Computer, Consumer and Control (IS3C), pp. 419–422 (2012)
7. Zhang, Y.: Research on the automatic identification algorithm of genuine and anti-counterfeiting tags. Hainan University (2017)
8. Li, F.: Text security, bar code combination identification structure and methods, China, 2012101185260 [P] (2012)
9. Zhang, Y., Li, J.B.: An automatic identification authentic work anti-counterfeiting algorithm based on DWT-DCT. Int. J. Secur. Appl. **10**, 135–144 (2016)
10. Liao, X.F.: Analysis and improvement of image encryption algorithm based on Logistic chaotic system. Softw. Guide **16**(5), 39–41 (2017)
11. Rostami, M.J., Shahba, A., Saryazdi, S., et al.: A novel parallel image encryption with chaotic windows based on logistic map. Comput. Electr. Eng. **62**, 348–400 (2017)

12. Sabery K, M., Yaghoobi, M.: A new approach for image encryption using chaotic logistic map. In: Proceedings of 2008 International Conference of the IEEE on Advanced Computer Theory and Engineering, pp. 585–590 (2008)
13. Lü, J.H., Chen, G.R., Zhang, S.C.: The compound structure of a new chaotic attractor. Chaos, Solitons Fractals **14**(5), 669–672 (2002)
14. Liu, C.X., Liu, T., Liu, L., et al.: A new chaotic attractor. Chaos, Solitons Fractals **22**(5), 1031–1038 (2004)
15. Lü, J.H., Lu, A., Chen, S.H.: Chaos Time Series Analysis and Its Application. Wuhan University Press, Wuhan (2002)
16. Zhu, C.X., Chen, Z.G., et al.: A new image encryption algorithm based on generalized Chen's chaotic system. J. Cent. S. Univ. (Nat. Sci. Ed.) **37**, 1142–1148 (2006)
17. Cheng, J.R., Xu, R.M., Tang, X.Y., et al.: An abnormal network flow feature sequence prediction approach for DDoS attacks detection in big data environment. Comput. Mater. Contin. **55**(1), 95–119 (2018)
18. Cheng, J.R., Zhou, J.H., Liu, Q., Tang, X.Y., Guo, Y.X.: A DDoS detection method for socially aware networking based on forecasting fusion feature sequence. Comput. J. **61**(7), 959–970 (2018). https://doi.org/10.1093/comjnl/bxy025
19. Cui, J.H., Zhang, Y.Y., Cai, Z.P., et al.: Securing display path for security-sensitive applications on mobile devices. CMC: Comput. Mater. Contin. **55**(1), 017–035 (2018)