International Journal of Security and Its Applications
Vol. 10, No. 6 (2016) pp.135-144
http://dx.doi.org/10.14257/ijsia.2016.10.6.14

An Automatic Identification Authentic Work Anti-counterfeiting Algorithm Based on DWT-DCT

Yue Zhang and Jingbing Li*

College of Information Science and Technology,
Hainan University, Haikou, 570228, China
artistyue@163.com, jingbingli2008@hotmail.com

Abstract

In order to restrain the bad influences of fake and inferior products, an automatic identification authentic work anti-counterfeiting algorithm is proposed in this paper. The authentic work anti-counterfeiting uses a unique random character structure to carry out security. The algorithm is convenient for customers to distinguish the anti-counterfeiting tag by both naked eye and mobile. There is not yet a similar algorithm published. In the algorithm, the feature vectors are extracted using DWT-DCT. Using extracted feature vectors from anti-counterfeiting tag to realize automatic identification. Therefore, this algorithm saves the storage space and improves the identification rate. In addition, the experimental results show this algorithm have strong robustness under common attacks, geometrical attacks.

Keywords*: Anti-counterfeiting; Automatic identification; Feature vector; DWT-DCT; Robustness*

1. Introduction

Anti-counterfeit got quick development in a short span of twenty years [1], because the number of proliferation of fake and inferior increase swift. Meanwhile, they try different anti-counterfeiting technologies to reduce the loss caused by fake products [2]. Traditional external packaging methods have many drawbacks, such as reproducibility, short period, so that restricted technology application [3-4]. In previous years, bar code, two-dimensional code are popular anti-counterfeiting technologies. These technologies can realize automatic identification, but have the shortcomings of being easily forged, and being difficult to be recognized by consumers [5-7]. Recent anti-counterfeiting research hotspot is RFID [8-10]. RFID is very good but expensive. At the same time, there are some anti-counterfeiting technologies combine new technologies such as biology, chemistry [11]. However, these anti-counterfeiting technologies need special identification conditions. This paper presents an automatic identification authentic work anti-counterfeiting algorithm. Each security label has a unique text pattern that is randomly carved, so it can prevent the labels from being copied. We establish security database of feature vectors based on DWT-DCT coefficient signs. This algorithm can be easy identification of consumers and mobile, and has good robustness.

2. The fundamental Theory

2.1. The Discrete Wavelet Transform (DWT)

Wavelet transforms, which proposed by Daubechies and Mallat, are generated from simple orthogonal transforms. Wavelet transform can be used for various applications of

* Corresponding Author

ISSN: 1738-9976 IJSIA

image processing [12]. Define the wavelet function $\Psi_{a,b}(t)$ as the base, and the wavelet transform of $f \in L^2(R)$ by Ψ is defined as:

$$W_{f(a,b)} = \int_R f(t)\bar{\psi}_{a,b}(t)dt \tag{1}$$

where, the wavelet function $\Psi_{a,b}(t)$ is obtained by translating and scaling the same base Ψ.

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

Where, Ψ is called the base wavelet, a is the dilation factor, b is the translation factor.

The decomposing equation of the Mallat algorithm is as follows:

$$c_{j+1,k} = \sum_{n \in z} c_{j,n} \bar{h}_{n-2k} \qquad k \in z \tag{3}$$

$$d_{j+1,k} = \sum_{n \in z} c_{j,n} \bar{g}_{n-2k} \qquad k \in z \tag{4}$$

The reconstruction equation of the Mallat algorithm is given by:

(5)

After the decomposing, we got four sub images (One is the low frequency approximation sub image, and the other three are the high frequency detail sub images.).

2.2. The Discrete Cosine Transform (DCT)

Discrete cosine transform (DCT) is the orthogonal transformation method proposed by N.Ahmed *et. al.*, in 1974 [13]. DCT transform uses the nature of the Fourier transform transforming the image into even function form, and then doing 2-D Fourier transform so that get results with cosine form. All DCT multiplications are on real numbers. When applied to an M×N size image or matrix, the 2D-Discrete Cosine Transform will compresses all the energy information of the image and concentrates it in a few coefficients located in the upper left corner of the resulting real-valued M×N DCT/frequency matrix [14]. 2-D discrete cosine transform is defined as:

$$F(u,v) = c(u)\,c(v) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \cos\frac{\pi(2x+1)\mu}{2M} \cos\frac{\pi(2y+1)v}{2N} \qquad v = 0,1,\cdots,N-1;\ u = 0,1,\cdots,M-1; \tag{6}$$

where M×N is anti-counterfeiting image size, $f(x, y)$ corresponds 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 frequency domain. The Formula shows that the sign of DCT coefficients are related to the phase of the component.

2.3. Authentic Work Anti-Counterfeiting

Authentic work anti-counterfeiting technology scheme used in this paper is defined as follow. First, select words or phrase. Secondly, arbitrary rotate every words. Then sculpture these words on commodity packaging at random. Finally, we get a unique random character structure to carry out security.

2.4. A Method to Obtain the Feature Vector of Authentic Work Anti-Counterfeiting Image

Choose an image to handle by DWT. Then we obtain four sub images. The high frequency detail sub images contain the edge information of the image, so that it is vulnerable to external interference. However, the low frequency approximation sub image contains the basic information of the image and has little influenced of external interference. So we handle the low frequency approximation sub image by DCT. Then we choose 8 low-frequency DCT coefficients (C1, C2, … , C8), which are shown in Table 1. We can find the sign of DCT coefficients are almost unchanged even after attacks, shown as Table 1. Therefore, we let "1" represents a positive or zero coefficient, and "0" represents a negative coefficient so that we get a sign sequence of low-frequency DCT coefficients as feature vector of authentic work anti-counterfeiting image, as shown in column "L11" in Table 1. Finally, we compute the value of the normalized cross-correlation (NC) which used 32 bits sign sequence low-frequency DCT coefficients to obtain accurate calculation results. After kinds of attacks, the value of NC is "1.0" or near "1.0", as shown in column "L12" in Table 1. Consequently, the sequence of DCT coefficient signs can be used as the feature vector of authentic work anti-counterfeiting image.

In order to further prove this conclusion, we selected 10 authentic work anti-counterfeiting images which shown as Figure 1, to extract the feature vector and compared the correlation coefficients. And from Table 2, we can find the correlation coefficients of different images are very small. In addition to the correlation coefficient between V5 and V8 is relatively large. That's reason is V5 and V8 are almost the same image.

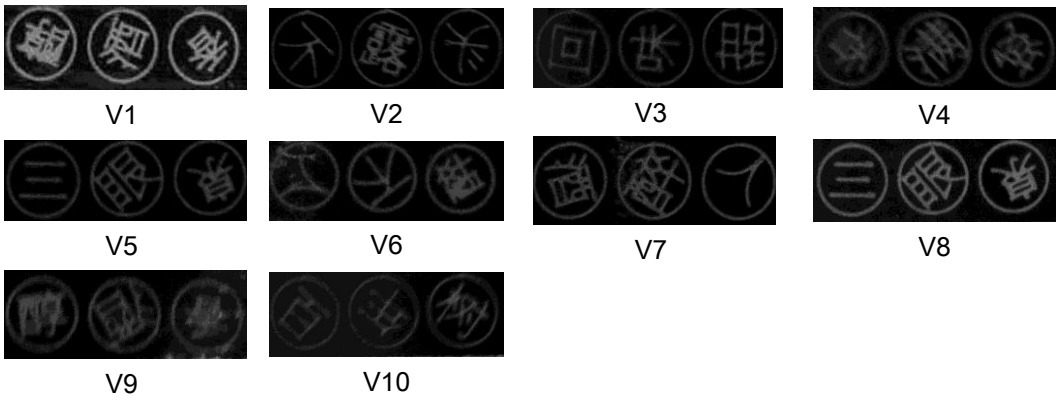


Figure 1. 10 Different Authentic Work Anti-Counterfeiting Images

3. The Algorithm

We choose an authentic work anti-counterfeiting image as the original authentic work anti-counterfeiting image. It is described as: $F = \{ f(i, j) \mid f(i, j) \in R; 1 \le i \le N1, 1 \le j \le N2 \}$

Where f(i, j) means the pixel gray value of the original texture image.

3.1. Establish Security Database of Authentic Work Anti-Counterfeiting Image Feature Vectors

Step 1: Acquire the feature vectors of the original authentic work anti-counterfeiting images using DWT-DCT

Table 1. Change of DCT Low-Frequency Coefficients with Respect to Different Attacks

L1	L2	L3	L4	L5	L6	L7	L8	L9	L10	L11	L12
Image processing	PSNR (dB)	C 1	C2	C3	C4	C5	C6	C 7	C8	Sequence of coefficient signs	NC
Original image	86.48dB	62.10	4.44	0.43	0.05	-0.06	0.24	-20.73	-0.76	1111 0100	1.0
Gaussian noise (2%)	14.42dB	67.88	4.18	0.97	0.03	-0.19	-0.55	-19.11	-0.66	1111 0000	0.82
JPEG compression (3%)	17.89dB	63.82	5.00	0.16	-0.56	-0.63	0.18	-19.33	-0.45	1110 0100	0.75
Median filter [3x3]	23.14dB	61.22	4.46	0.15	0.18	-0.26	0.10	-21.60	-0.78	1111 0100	0.94
Rotation (2°)	14.96dB	60.85	3.91	0.45	0.03	-0.03	0.41	-20.52	-0.43	1101 0100	0.94
Scaling (×2)		12.42	0.89	0.09	0.01	-0.01	0.05	-4.15	-0.15	1111 0100	1.0
Scaling (×0.5)		31.07	2.22	0.21	0.03	-0.02	0.13	-10.34	-0.39	1111 0100	1.0
Left translation (2%)	11.82dB	61.72	6.31	0.20	2.33	-0.38	4.69	-20.30	-2.90	1111 0100	0.94
Down translation (2%)	14.30dB	61.29	4.36	0.42	-0.01	-0.06	0.18	-20.76	-0.78	1110 0100	0.82
Cropping (2% from Y)		62.11	4.42	0.42	-0.01	-0.06	0.19	-21.03	-0.79	1110 0100	0.88
Cropping (2%fromX)		62.39	3.29	1.53	-1.29	1.67	-2.77	-19.63	0.47	1110 1001	0.63

Unit of transform coefficient: 1.0e+002, NC used 32 bits sign sequence low-frequency DCT coefficients to obtain

Firstly, handle the original image F(i,j) by DWT to obtain the low frequency approximation sub image FA(i,j). Secondly, handle the low frequency approximation sub image by DCT to obtain the coefficient matrix FD(i,j). select the previous 4×8 coefficients to compose FD32(i,j). Finally, do the symbol operation on coefficients to obtain the feature vectors V(j). The procedure is described as:

$$\boldsymbol{FA}(i,j) = \mathrm{DWT2}\left(\boldsymbol{F}(i,j)\right) \tag{7}$$

$$\boldsymbol{FD}(i,j) = \mathrm{DCT2}\left(\boldsymbol{F}(i,j)\right) \tag{8}$$

$$\boldsymbol{V}(j) = \mathrm{Sign}\left(\boldsymbol{FD}_{32}(i,j)\right) \tag{9}$$

Step 2: Save the feature vectors of the original authentic work anti-counterfeiting images in database

Repeat operations as step 1, till all authentic work anti-counterfeiting images are handled. Then Save these feature vectors in security database.

Table 2. Correlation Coefficients of Feature Vector of Different Images

	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10
V1	1.00	0.154	0.071	0.189	0.126	0.288	0.118	0.076	0.118	0.126
V2	0.154	1.00	0.159	0.156	0.406	-0.062	0.155	0.248	-0.221	0.156
V3	0.071	0.159	1.00	0.125	0.125	0.029	-0.122	0.105	-0.122	0.188
V4	0.189	0.156	0.125	1.00	0.063	-0.031	0.125	0.032	0.313	0.125
V5	0.126	0.406	0.125	0.063	1.00	0.156	0.00	0.791	0.00	0.188
V6	0.288	-0.062	0.029	-0.031	0.156	1.00	-0.217	0.068	0.096	0.219
V7	0.118	0.155	-0.122	0.125	0.00	-0.217	1.00	0.212	0.184	-0.063
V8	0.076	0.248	0.105	0.032	0.791	0.068	0.212	1.00	-0.042	0.158
V9	0.118	-0.221	-0.122	0.313	0.00	0.096	0.184	-0.042	1.00	0.125
V10	0.126	0.156	0.188	0.125	0.188	0.219	-0.063	0.158	0.125	1.00

3.2. The Automatic Identification of Authentic Work Anti-Counterfeiting Image

Step 3: Acquire the feature vector of the tested image

To acquire the feature vector V'(j) of tested image F'(i,j), do operations which is similar as step 1. The procedure is described as:

$$\boldsymbol{FA}'(i,j) = \mathrm{DWT2}\left(\boldsymbol{F}'(i,j)\right) \tag{10}$$

$$\boldsymbol{FD}'(i,j) = \mathrm{DCT2}\left(\boldsymbol{F}'(i,j)\right) \tag{11}$$

$$\boldsymbol{V}'(j) = \mathrm{Sign}\left(\boldsymbol{FD}_{32}'(i,j)\right) \tag{12}$$

Step 4: Calculate the Peak Signal to Noise Ratio (PSNR)

PSNR is used to assess the quality of the image. The bigger PSNR represents the better quality of the image. It is defined as:

$$PSNR = 10\lg\left[\frac{MN\max_{i,j}\left(I_{(i,j)}\right)^2}{\sum_i\sum_j\left(I_{(i,j)} - I'_{(i,j)}\right)^2}\right] \tag{13}$$

Step 5: Calculate the normalized cross-correlation (NC) to determine whether the original image

Calculate the normalized cross-correlation (NC) using the formula as follow:

$$NC = \frac{\boldsymbol{V}(i) \times \boldsymbol{V}'(j)}{\boldsymbol{V}^{2}(j)} \tag{14}$$

The larger the value of NC is, the more approximation between the tested authentic work anti-counterfeiting image ***F'(i, j)*** and the original authentic work anti-counterfeiting image ***F(i, j)***.

Step 6: Return the maximum value of NC to the user's phone

All steps above are shown in the Figure 2.

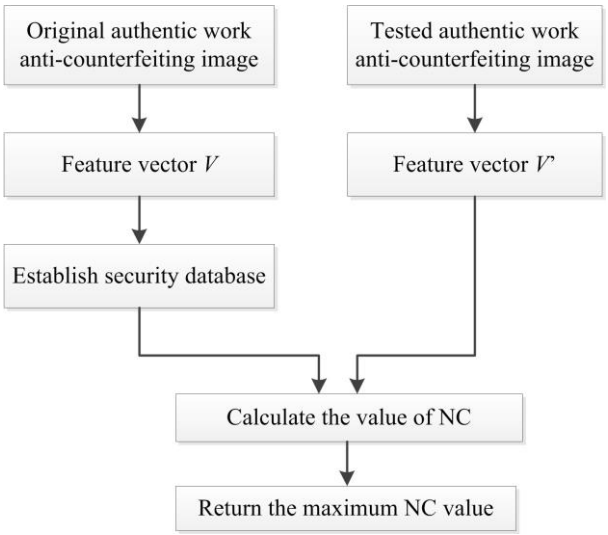


Figure 2. Authentic Work Anti-Counterfeiting Algorithm Figure

4. Experiements

In our experiments, we use 1000 groups of independent binary pseudo morph sequences. Every sequence consists of 32 bits. In the experiments, the 500th group is selected at random from the 1000 groups as the embedded feature vector. The size of authentic work anti-counterfeiting image is 220×76, the image is shown in Figure 3(a). The original authentic work anti-counterfeiting image is denoted as ***F(i,j)***, where $1 \le i \le 220$, $1 \le j \le 76$. The corresponding coefficient matrix is ***FD(i,j)***. We select the 32bits sequence of coefficient signs as the feature vector ***V(j)*** selected from ***FD(i,j)***, where $1 \le i \le 4$, $1 \le j \le 8$. Security database is comprised of 32bits feature vectors so that database can save more space than authentic work anti-counterfeiting images. By this way, we improve the rate of automatic identification.

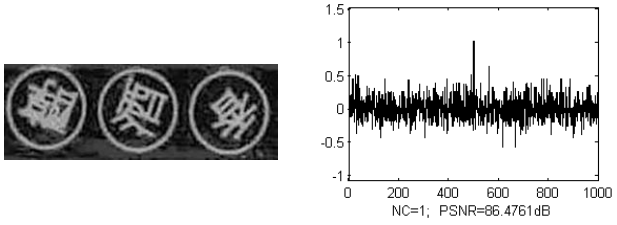
In this simulation, PSNR is used for objectively evaluating the quality of the tested image, and the NC is used to objectively evaluate the results of similarity detection.

Figure 3(b) is the NC values between the 1000 available pseudo morph sequences and the extracted feature vector, which is achieved by using DWT-DCT and symbolic operation. It can be seen from Figure 3(a) that the original authentic work anti-counterfeiting image. The similarity can be detected clearly, NC=1.0.

4.1. Common Attacks

4.1.1. Gaussian noise attacks： Table 3 is the experimental data of anti-Gauss noise interference of anti-counterfeiting image. When the Gauss noise intensity of up to 15%, the PSNR of the anti-counterfeiting image down to 6.81dB, the image is obscure. Then extract the anti-counterfeiting image, So we can conclude that the algorithm has strong

anti-Gauss noise ability. Figure 4(a) shows the authentic work anti-counterfeiting image under Gaussian attacks (2%). The value PSNR is 14.35dB. The similarity can be detected with NC=0.94, as shown in Figure 4(b).

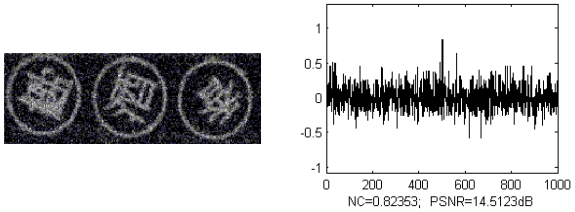


(a) (b)

Figure 3. Original Authentic Work Anti-Counterfeiting Image and Detecting NC without Attacks: (a) Original Authentic Work Anti-Counterfeiting Image; (b) Similarity Detector

Table 3. Anti-Gauss Noise Data

Noise Intensity (%)	1	2	3	5	10	15
PSNR(dB)	17.24	14.42	12.81	10.78	8.18	6.81
NC	0.88	0.82	0.76	0.76	0.65	0.68



(a) (b)

Figure 4. Gaussian Noise (noise intensity=2%): (a) Adding Gaussian Noise; (b) Similarity Detector

4.1.2. JEPG attacks： Table 4 is anti-JPEG compression experimental data for anti-counterfeiting image. When the compression quality is only 2%, the image has blocking artifacts. NC=0.75, we still can extract the anti-counterfeiting image at this situation. The results show that the algorithm is robust to JPEG attacks. The authentic work anti-counterfeiting image with JPEG attacks (2%) is shown in Figure 5(a). PSNR=17.12dB. The similarity can still be detected, NC=0.75, as shown in Figure 5(b).

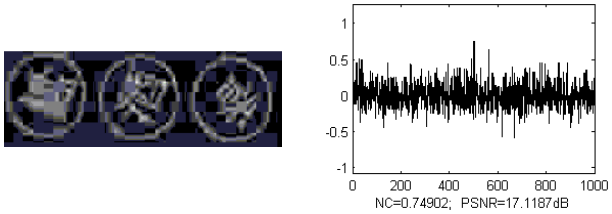
Table 4. Anti-jpeg Compression Data

JPEG Compression (%)	2	5	10	20	30	40
PSNR(dB)	17.12	20.60	24.01	27.24	29.11	30.33
NC	0.75	0.75	0.93	1.0	1.0	0.82

4.2. Geometrical Attacks

4.2.1. Rotation attacks： Table 5 is anti-rotation attacks experimental data for anti-counterfeiting image. We can see when the anti-counterfeiting image clockwise rotation 10°, NC=0.69, the anti-counterfeiting image can still be accurate to extract. Figure 6(a) shows the authentic work anti-counterfeiting image rotated clockwise by 3°, PSNR

=12.97dB.Figure 6(b) shows that the similarity can be detected with NC=0.75. Therefore we can conclude that our scheme is robust against rotation attacks.

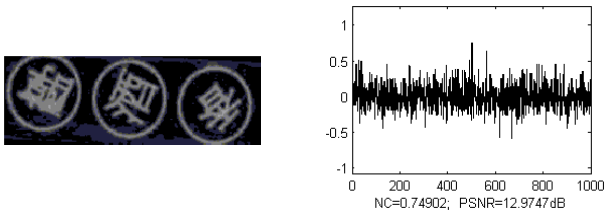


(a) (b)

Figure 5. JPEG Compression (2%): (a) Image After JPEG Compression; (b) Similarity Detector.

Table 5. Anti-Rotation Attacks Data

Rotational Degree	0°	1°	2°	3°	4°	5°	6°	7°	10°
PSNR(dB)	86.48	19.67	14.96	12.97	12.05	11.60	11.31	11.06	10.51
NC	1.0	1.0	0.94	0.75	0.67	0.55	0.68	0.76	0.69



(a) (b)

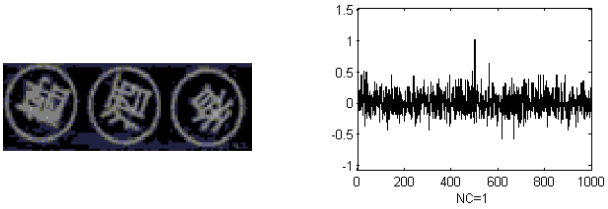
Figure 6. Rotation Attacks (3°): (a) Under Rotation Attack; (b) Watermarking Detector

4.2.2. Scaling attacks：Table 6 is anti-scaling attacks experimental data for anti-counterfeiting image. When the anti-counterfeiting image scaling factors low to 0.2, NC=0.94, we can extract the anti-counterfeiting image. When the anti-counterfeiting image scaling factors up to 2.0, NC=1.0, we also can extract the anti-counterfeiting image. Figure 7(a) shows the authentic work anti-counterfeiting image shrunk with a scale factor of 0.5. Figure 7(b) shows that the similarity can be detected with NC=1.0. Hence, our algorithm is robust to scale attacks.

Table 6. Anti-Scaling Attacks Data

Scaling Factors	0.2	0.5	0.6	0.7	0.8	1.1	1.5	2.0
NC	0.88	1.0	1.0	1.0	1.0	0.94	1.0	1.0

4.2.3. Translation attacks：Table 7 is anti-left translation attacks experimental data for anti-counterfeiting image. When the anti-counterfeiting image left translation 6%, NC=0.57, the anti-counterfeiting image can be accurate to extract. When the anti-counterfeiting image down translation 6%, NC=0.57. Therefore we can conclude that our scheme is robust against translation attacks. Figure 8(a) shows the authentic work anti-counterfeiting image after left translation 4%. Figure 8(b) shows that the similarity can be detected with NC=0.69.

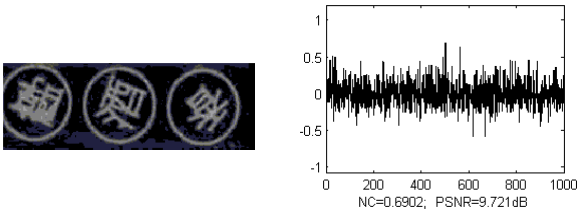


(a) (b)

Figure 7. Scaling Attacks (×0.5): (a) Under Scaling Attack; (b) Similarity Detector

Table 7. Anti-Translation Attacks Data

	Left Translation				Down Translation			
Translation distance (%)	1	2	4	6	1	2	4	6
PSNR(dB)	14.23	11.82	9.72	9.46	19.27	14.30	9.98	9.41
NC	1.0	0.94	0.69	0.57	1.0	0.82	0.64	0.57



(a) (b)

Figure 8. Left Translation Attacks (4%): (a) Under Translation Attack; (b) Similarity Detector

5. Conclusion

An automatic identification algorithm of the authentic work anti-counterfeiting labels based on DWT-DCT is proposed in this paper. Authentic work anti-counterfeiting is a novel anti-counterfeiting algorithm. It is convenient for consumers to identify with both naked eyes and automatic identify. The experimental results show this algorithm can realize automatic identification and have strong robustness by combining DWT, DCT, feature vector, and data base. In addition, the algorithm can improve the rate of identification and save a lot of storage space.

References

[1] S. Sheng and X. Wu, "A new digital anti-counterfeiting scheme based on chaotic cryptography", ICT Convergence (ICTC)., Jeju Island, **(2012)**, pp. 687-691.
[2] Y. Guan, J. Hu and Y. Li, "A new anti-counterfeiting method: fluorescent labeling by safranine T in tobacco seed", Acta Physiol Plant, vol. 33, **(2011)**, pp. 1271-1276.
[3] X. Tie and J. Zou, "A Novel Digital Watermarking Method for Commercial Bills Based on V Systems", Pervasive Computing and Applications (ICPCA), **(2007)**, pp. 389-393.
[4] Y. Tian, Z. Li and F. He, "A novel anti-counterfeiting method: Application and decomposition of RB for broad bean seeds (Vicia faba L.)", Industrial Crops and Products, vol. 61, **(2014)**, pp. 278-283.
[5] S. Liu, "Anti-counterfeit system based on mobile phone QR code and fingerprint", Intelligent Human-Machine Systems and Cybernetics (IHMSC)., **(2010)**, pp. 236-240.

[6] A. Sun, Y. Sun and C. Liu, "The QR-code reorganization in illegible snapshots taken by mobile phones", Fifth International Conference on Computational Science and Applications (ICCSA), **(2007)**, pp. 532-538.
[7] X.-c. Yang, J.-p. Li and J.-p. Mou, "An anti-counterfeiting method based on VCS for mobile phone's identification", International Conference on Wavelet Active Media Technology and Information Processing (ICWAMTIP), **(2012)**, pp. 169-172.
[8] S. H. Choi, B. Yang and H. H. Cheung, "RFID tag data processing in manufacturing for track-and-trace anti-counterfeiting", Computers in Industry, vol. 68, **(2015)**, pp. 148-161.
[9] B. Yan and G. Huang, "Application of RFID and Internet of things in monitoring and anti-counterfeiting for products", Business and Information Management (ISBIM), **(2008)**, pp. 392-395.
[10] C.-L. Chen, Y.-Y. Chen and T.-F. Shih, "An RFID authentication and anti-counterfeit transaction Protocol", Computer, Consumer and Control (IS3C), **(2012)**, pp. 419-422.
[11] M. Radziwon, S. Johansen and H.-G. Rubahn, "Anti-Counterfeit Solution from Organic Semiconductor", Procedia Engineering, vol. 69, **(2014)**, pp. 1405-1409.
[12] Dr. S. D. Thepade and P. Bidwai, "Iris Recognition using Fractional Coefficients of Transforms, Wavelet Transforms and Hybrid Wavelet Transforms, International Conference on Control, Computing, Communication and Materials (ICCCCM),**(2013)**, pp. 1-5.
[13] Abhiram, M. H., Sadhu, C. and Manikantan, K., "Novel DCT based feature extraction for enhanced Iris Recognition", International Conference on Communication, Information & Computing Technology (ICCICT)], **(2012)**, pp. 1-6.
[14] H.-T. Yin and P. Fu, "Face recognition based on DCT and 2DLDA", in Proc. of the Second International Conference on Innovative Computing, Information and Control, Kumamoto, Japan, **(2007)**, pp. 581-584.

Authors

Yue Zhang, was born in JiLin province, China, in 1991. She received the B.S. in Hainan University, Haikou, major in Electronic Information Engineering. Now she is a graduate student at Hainan University.

Jingbing Li, was born in 1966. He received the M.S. in Beijing Institute Of Technology, in 1996, and Doctor degree in Chongqing University, in 2007. Now he is a professor in Hainan University. His main research directions are image processing, multimedia information security, digital watermarking, artificial intelligence technology, computer automatic control.

