Image Watermarking Encryption Scheme Based on Fractional Order Chaotic System

Dawei Ding [1], Zongzhi Li [2] and Shujia Li [3]

School of Electronic Information Engineering,

Anhui University, Hefei 230601, China.

Email: [1] dwding@ahu.edu.cn, [2] 493756119@qq.com,

[3] 1352288370@qq.com

Abstract. Now the chaotic system and wavelet transform are more and more widely used in the watermarking technology. At the same time, the fractional order chaotic system has more complex dynamic characteristics than the integer order system. So a new image watermarking scheme based on the fractional order Chen chaotic system and discrete wavelet transform is proposed. Chaotic sequences generated by chaotic system are used to encrypt the watermark image, and the processed watermark information is embedded into the original image by the discrete wavelet transform. Finally, the security analysis of the proposed watermarking algorithm is presented. The experimental results show that the proposed watermarking scheme has high security, and it has stronger robustness and invisibility compared with the previous work.

Keywords: fractional order chaotic system, discrete wavelet transform(DWT), image watermarking, security, robustness, invisibility

1. Introductiong

With the rapid development of network technology,all kinds of digital media are more convenient to spread through the network,the security of digital media becomes more and more important in the network. Copyright protection is one of the important aspects.Digital watermarking technique is a kind of information hiding technique, it can be used as a kind of more effective copyright protection of digital works and anti fake technology.

At present, the chaotic system is more and more widely used in the watermarking technology and has achieved good results, a considerable part of chaos-based image watermarking schemes are proposed[1 – 6]. Poonkuntran and Rajesh proposed a new imperceptible image watermarking scheme for active authentication for images[1]. The scheme used chaotic system to process the watermark, and used the integer transform to embed the watermark information. Tong Xiaojun et al. proposed an image watermarking technique based on scrambling and self restoration[2]. A coupled chaotic map was used to scramble the original image block by block. Behnia et al. proposed an image watermarking scheme based on double chaotic map[3]. One map was used to encrypt the embedded position, and another one was used to determine the pixels of the host image. Gao Tiegang et al. proposed an image watermark authentication method based on neural network with hyper chaotic characteristics[4]. The method used the authentication password as the key, and the pixel value was used as the input of the neural network. Mooney et al. used the combination of white noise and chaotic sequence to encrypt the watermark[5].

Gao Guangyong et al. used composite chaos to encrypt the watermarking image, and resisted the geometric attack based on a composite-chaos optimized support vector regression(SVR) model [6].

Watermarking methods can mainly be divided into three types according to the restore information: non-blind, semi-blind and blind watermarking methods[7]. Non-blind methods need all the information of the original image and the key. Semi-blind methods need watermark sequence and the key, and blind methods need key only.

Watermarking methods can be divided into two other types according to the embedding strategy:

1) Spatial domain watermarking: the value of the image element is changed directly, and the hidden content is added in the brightness of the image element, however, this method is easy to be obtained, and the robustness of the image processing is poor.

2) Transform domain watermarking: use a mathematical transformation to transform the image into the transform domain, and add the information by changing some transform coefficients of image, and then use the inverse transform to recover the hidden watermark information and image.

The advantages of using transform technique include the ability to ensure that the watermark is not visible and resistance to the corresponding lossy compression.

Keyvanpour et al. proposed a watermarking method based on chaotic map and operation of transform domain[8]. The coding process was special and the key was generated by chaotic map, the wavelet quantization process was used to transfer the sequence. Zhang Dengyin et al. proposed a watermarking algorithm based on one-dimensional (1-D) chaotic map in wavelet transform (WT) domain[9]. The watermark was encoded by a chaotic sequence and embedded into the low-and intermediate-frequency bands of three-layer WT domain. Barni et al. proposed a watermarking method based on discrete wavelet transform, the embedded operation was done in the high frequency part[10]. In addition, there are many examples of the combination of wavelet transform and other operations[11-13]. Therefore, it is feasible to use discrete wavelet transform(DWT) and chaotic system to encrypt the watermark.

At the same time, the research shows that the low dimensional chaotic system has the defects of the limited key space and the worrying security, but the high dimensional chaotic systems have higher complexity, randomness and unpredictability, and it can better resist the attack of phase space reconstruction and other methods[14]. The Chen’ s system is a three-dimensional chaotic system with complex topology than Lorenz attractor. The fractional order chaotic dynamics system has more complex and richer dynamic characteristics than the integer order system, and it has the advantage of increasing the randomness and unpredictability, Moreover, the fractional order system can also provide more key parameters and increase the key space for the encryption system, so it will improve the encryption effect of the system.

Inspired by above analysis, a new image watermarking scheme based on the fractional order Chen chaotic system and discrete wavelet transform is proposed. Firstly chaotic sequences generated by chaotic system are used to encrypt the watermark image. Then the processed watermark information is embedded into the original image by the discrete wavelet transform.

The main content of the study is as follows. In Section 2, the related theoretical works are introduced in detail. In Section 3, the process of the proposed watermarking algorithm is described in detail. Experimental results and security analysis are given in Section 4. The final conclusion is shown in Section 5.

2. Related Works

2.1 The fractional-order Chen's chaotic system

Consider the fractional-order Chen' s chaotic system[15] described by

$$\begin{cases} \dfrac{d^{\alpha}x}{dt^{\alpha}} = a(y-x) \\ \dfrac{d^{\beta}y}{dt^{\beta}} = (c-a)x - xz + cy \\ \dfrac{d^{\gamma}z}{dt^{\gamma}} = xy - bz \end{cases} \tag{1}$$

where α, β, γ are fractional derivative orders, $(x, y, z) \in \mathbb{R}^3$ are state variables, $a > 0, b > 0, c > 0$ are parameters of the system.

The Grunwald-Letnikov of fractional calculus[16] is defined as:

$${}_aD_t^{\upsilon} f(x) = \lim_{h \to 0} \frac{1}{h^{\upsilon}} \sum_{j=0}^{[(t-a)/h]} (-1)^j \frac{\Gamma(\upsilon+1)}{j!\Gamma(\upsilon-j+1)} f(x-jh); \upsilon > 0 \tag{2}$$

where and are lower bound and upper limit of integral, is fractional derivative order, is integration time step, [x] represents integer part of variable x. Its mathematical expression is shown in the Eq.3:

$${}_aD_t^{\alpha} f(t) = \lim_{h \to 0} h^{-\alpha} \sum_{j=0}^{[(t-a)/h]} (-1)^j \binom{\alpha}{j} f(t-jh) \tag{3}$$

where $\binom{\alpha}{j} = \dfrac{\alpha(\alpha-1)...(\alpha-j+1)}{j!}$

Simplified Eq. 3 get Eq. 4:

$${}_0D_t^{\alpha} y(t_m) = h^{-\alpha} \sum_{j=0}^{m} \omega_j^{(\alpha)} y_{m-j} \tag{4}$$

where $\omega_j^{(\alpha)} = (-1)^j \binom{\alpha}{j}; j = 0, 1, 2...$.

According to Eq. 4, change Eq. 1 :

$$\begin{cases} h^{-\alpha} \sum_{j=0}^{m} \omega_j^{(\alpha)} x_{m-j} = a(y_m - x_m) \\ h^{-\beta} \sum_{j=0}^{m} \omega_j^{(\beta)} y_{m-j} = (c-a)x_m - x_m z_m + cy_m \\ h^{-\gamma} \sum_{j=0}^{m} \omega_j^{(\gamma)} z_{m-j} = x_m y_m - bz_m \end{cases} \tag{5}$$

Simplified Eq. 5:

$$\begin{cases} x_m = (ah^\alpha y_m - \sum_{j=1}^{m} \omega_j^{(\alpha)} x_{m-j}) / (1+ah^\alpha) \\ y_m = (h^\beta (c-a-z_m) x_m - \sum_{j=1}^{m} \omega_j^{(\beta)} y_{m-j}) / (1-ch^\beta) \\ z_m = (h^\gamma x_m y_m - \sum_{j=1}^{m} \omega_j^{(\gamma)} z_{m-j}) / (1+bh^\gamma) \end{cases} \tag{6}$$

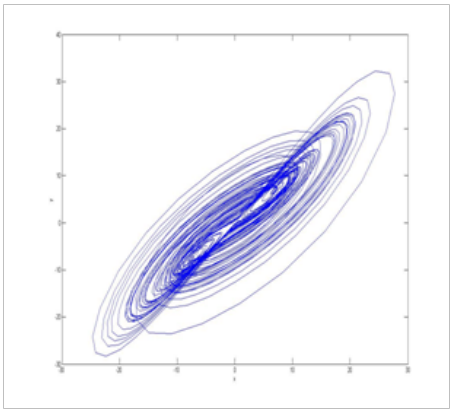
where x_m, y_m, z_m are implied. The iterative algorithm is used to express them:

$$\begin{cases} x_m^{(l)} = (ah^\alpha y_m^{(l-1)} - \sum_{j=1}^{m} \omega_j^{(\alpha)} x_{m-j}^{(l-1)}) / (1+ah^\alpha) \\ y_m^{(l)} = (h^\beta (c-a-z_m^{(l-1)}) x_m^{(l-1)} - \sum_{j=1}^{m} \omega_j^{(\beta)} y_{m-j}) / (1-ch^\beta) \\ z_m^{(l)} = (h^\gamma x_m^{(l-1)} y_m^{(l-1)} - \sum_{j=1}^{m} \omega_j^{(\gamma)} z_{m-j}) / (1+bh^\gamma) \end{cases} \tag{7}$$

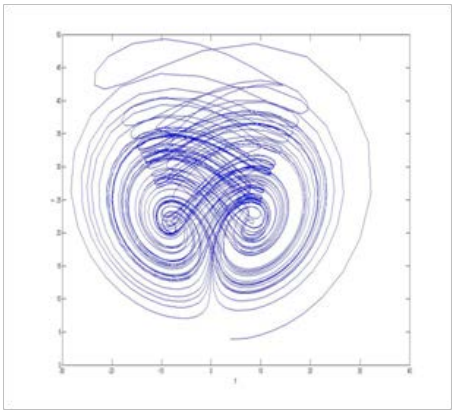
where l is iteration number .

When $\left|x_m^{(l)} - x_m^{(l-1)}\right| < \delta, \left|y_m^{(l)} - y_m^{(l-1)}\right| < \delta, \left|z_m^{(l)} - z_m^{(l-1)}\right| < \delta$ (δ is very small, such as $\delta = 10^{-5}$), $x_m^{(l)} = x_m^{(l-1)}, y_m^{(l)} = y_m^{(l-1)}, z_m^{(l)} = z_m^{(l-1)}$ .System will exhibit chaotic behavior when initial conditions are set as: $h = 0.01$, $(\alpha, \beta, \gamma) = (0.97, 0.98, 0.99)$, $a = 35, b = 3, c = 28$, $(x_0, y_0, z_0) = (1, 3, 4)$ .The projections of the attractor are shown in Fig.1.

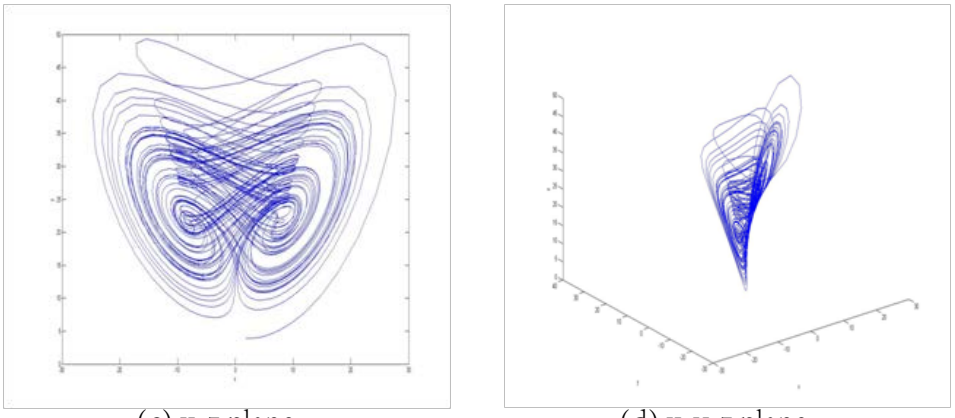
Chaotic system will produce chaotic sequence, and these sequences are used to encrypt watermark image. The result will produce a chaotic encrypted image, which will be then used for embedding the wavelet coefficients [17].



(a) x-y plane



(b) y-z plane



(c) x-z plane (d) x-y-z plane

Figure.1 The attractors of system described in Eq. (1)

2.2 Discrete wavelet transform

In the process of image processing, the lossy compression can cause damage to the digital watermark. So the characteristics of lossy compression must be used to find the maximum robustness in the process of embedding and extracting digital watermark. The DWT is a local transformation and has the ability of multi scale analysis. By using wavelet transform, the original image sequence can be decomposed into multi frequency sub images which can adapt to the visual characteristics of the human eye, and the watermark embedding and detection can be carried out in a plurality of levels. Wavelet transform domain digital watermarking method has the advantages of both temporal and spatial domain method and DCT transform domain method.

A two-dimensional image can be decomposed into different frequency components, and the image can be decomposed into 4 parts at each level of the transformation. For example, the first level of decomposition, i.e. LL_1, LH_1, HL_1, HH_1 [18]. A wide range of information is contained in the low frequency component LL_1 part. LH_1, HL_1, HH_1 are high frequency components which contain the specific details. Wavelet decomposition can continue be used to decompose LL_1 to get LL_2, LH_2, HL_2, HH_2. Repeat this process until the required decomposition level is obtained, i.e. LLn, where n represents the decomposition level. These wavelet coefficients can be used in the future to restore the original image, this inverse process of DWT is known as IDWT.

3. Proposed Watermarking Algorithm

This part gives a detailed introduction of the watermark embedding algorithm and extraction algorithm. The size of the original image I is $M \times N$ and the size of binary watermark image W is $m \times n$.

3.1 Embedding watermarking

The different fractional derivative orders and initial conditions for Eq.(1) are given as:

$$(x_0, y_0, z_0), (x_1, y_1, z_1), (\alpha_0, \beta_0, \gamma_0), (\alpha_1, \beta_1, \gamma_1) \quad .$$

The specific steps of the embedding watermarking algorithm are as follows:

Step1. Perform operations on the original image according to a two level DWT, and four parts are obtained, i.e. LL2, LH2, HL2, HH2. Embedding operation is performed on this four parts.

Step2. The chaotic system can produce two chaotic sequences by input the key, and the watermarking

will be scrambled and encrypted. It is defined as U.

Step3. The encrypted binary watermarking is embedded into the original image according to the formula below:

$$I_2'(i,j) = I_2(i,j) + \alpha U(i,j) \tag{8}$$

where α represents visibility factor , its value is 0.05 for proposed scheme, $I\ (i,j)$ represents the second level wavelet coefficient. Embedding computing in four parts is all like this, i.e. LL_2, LH_2, HL_2, HH_2.

Step4. Perform operations on each part according to a two level IDWT of $I_2'(i,j)$, the watermarked image for each part $I_2''(i,j)$ is obtained.

Step5. Combine four parts to get the watermarked image.

The flow chart of embedding watermarking is shown in Fig. 2

3.2 Extracting watermarking

The process of extracting watermarking is the reversed order of the embedding procedure. It can be briefly introduced as follows:

Step1. Perform operations on the watermarked image according to a two level DWT and extract all the parts.

Step2. Perform operations on the original image according to a two level DWT.

Step3. With the help of the chaotic system, chaotic sequences will be generated.

Step4. Extract wavelet coefficients of the embedded watermarking, All four parts are calculated according to the formula below:

$$U'(i,j) = (I_2''(i,j) - I_2(i,j)) / \alpha \tag{9}$$

Step5. Use chaotic sequence to decrypt the encrypted watermarking

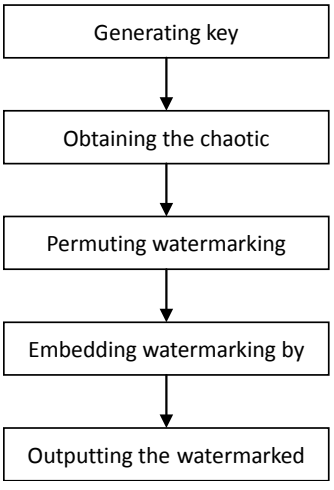


Figure.2 The flowchart of embedding watermarking

4. Experimental Results and Security Analysis

This section presents the experimental results and security analysis of the proposed algorithm. Firstly, the experimental results are given and the embedding efficiency is calculated, and the results of the proposed scheme under various different attacks are also given. Then the test results of encryption security for proposed scheme are given, such as the grey histogram, the space of key, key sensitivity.

4.1 Experimental results

Watermarking scheme usually need to satisfy some properties, such as "embedding efficiency" and "attacks". The experimental results of these properties are as follows.

1) Experimental results

In this section, the standard Lena image with 256×256 is used as host image and binary logo with 64×64 is used as watermark image. Initial conditions are set as:

$(x_0, y_0, z_0) = (1,3,4)$, $(x_1, y_1, z_1) = (2,7,5)$, $(\alpha_0, \beta_0, \gamma_0) = (0.97, 0.98, 0.99)$,

$(\alpha_1, \beta_1, \gamma_1) = (0.97, 0.98, 0.99)$.

The results of watermarking embedding and extraction are obtained as shown in Fig 3.

The embedding of watermarking can be seen as effective if raw data and processed data cannot be distinguished. In order to show the effect of the proposed scheme more directly, the peak signal-to-noise ratio (PSNR) was used to evaluate the image quality, the calculation formula is as follows:

$$PSNR = 10\times\log_{10}\frac{255^2}{MSE}(dB) \tag{10}$$

The mean squared error (MSE) between the original image and watermarked image can be defined as:

$$MSE = \frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[I(i,j) - I_2''(i,j)\right]^2 \tag{11}$$

where $I(i,j)$ and $I_2''(i,j)$ represent the pixel values on the location (i,j) , while the image size is $M\times N$.

In this study, the bit error rate (BER) of extracted watermarking is used to test reliability, the calculation formula is as follows:

$$BER = \frac{B}{M\times N}\times100 \tag{12}$$

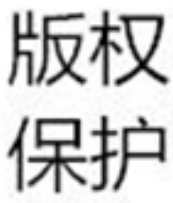
where B represents the number of erroneously detected bits, and the size of extracted watermark image is $M\times N$.

The PSNR value of the watermarked image is 41.33 dB, and the BER value of the extracted watermarking is zero. Therefore, there is almost no obvious perceptual distortion between original image and watermarked image; the process of embedding watermarking does not affect the quality of image.

(a)Host image

(b) Watermark image

(c) Watermarked image



(d) Extracted watermark image

Figure.3 Experimental results

2) Attacks

In order to test the robustness, several different attacks are given. Common signal processing attacks include:

(1) ***JPEG compression:*** JPEG is the abbreviation of Joint Photographic Experts Group, JPEG image compression algorithm can provide good compression performance, and has a good reconstruction quality, it is widely used in the field of image and video processing [19, 20]. The compression ratio of the proposed scheme is 50:1.

(2) ***Filtering:*** Filtering can filter out the specific band frequency of the signal, it is an important measure to restrain and prevent interference.

(3) ***Noise addition:*** The probability density function of Gaussian noise obeys Gauss distribution (i.e. normal distribution). If the amplitude distribution of a noise obeys Gauss distribution, and its power spectrum density is uniformly distributed, it is called Gaussian white noise [21, 22, 23]. The proposed scheme adds the Gaussian noise, whose mean value is 0 and the variance is 0.01.

(4)***Histogram equalization:*** Histogram equalization is a method to adjust the contrast in the field of image processing using image histogram [21, 22, 23].

(5) ***Contrast adjustment:*** Contrast of the watermarked image is improved by 50%.

(6) ***Gamma correction:*** Gamma correction can edit the gamma curve of image, recognize the dark part and light part of the image signal, and increase the proportion of the image. The gamma value of the proposed theme is reduced to 0.6.

The test results for watermarked image are given in Table 1. It can be clearly displayed from the Table 1 that the proposed scheme performs better.

Table 1 Comparsion result of PSNR values between proposed scheme and previous work

PSNR[dB]		
Attacks	Proposed scheme	Rawat ea al[7]
Gaussian Noise	19.69	13.37
Contrast Enhancement	21.51	19.008
Average Filtering	37.24	29.26
Median Filtering	32.05	31.03
Gamma Correction	17.25	15.43
Histogram Equalization	25.71	19.4
JPEG(Q=50)	39.26	34.96

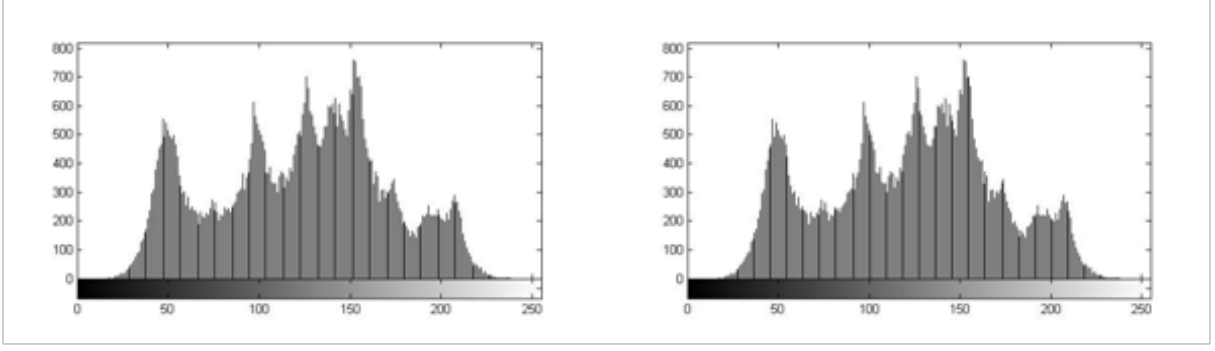
4.2 Security analysis and simulation for proposed scheme

1) The grey histogram analysis

The histogram reflects the basic statistical characteristics of the image. Compare the grey histograms of the original image and the watermarked image, the statistical performance is analyzed. Fig.4 shows the histograms of the original image and the watermarked image. From the figure, it is clear that two histograms are almost the same. The real information of the watermark image has been well hidden, it is not easy to use statistical characteristics to attack the watermarked image. So, the proposed algorithm can well resist statistical attack.

2) The space of key

For an encryption scheme, key space should be enough large to resist brute-force attack. In proposed scheme, the initial key consists of many elements. So the key of the system can be set $(\alpha_0, \gamma_0, a, b)$, each key parameter is independent of each other. In practical design, a and b are impossible to be infinitely large, their range can be set $0 < a, b < 100$. According to the precision of the double precision floating point of the computer, the scheme takes 8 bytes and 15 effective numbers to analyze the data. So the key space is equivalent to $10^{14} \times 10^{14} \times 10^{15} \times 10^{15} = 10^{58}$, which is able to resist the brute-force attack.



(a) The histogram of the original image (b) The histogram of the watermarked image

Figure.4 The grey histograms

3) Key sensitivity

A good encryption scheme needs not only a large key space, but also it must be sensitive to the key parameters. Only in this way can it be able to resist the differential attack. In the test, the key used in the scheme is (0.97, 0.99, 35, 3). In order to test the sensitivity of the algorithm to the key, some error keys are used to extract the watermark image. As can be clearly seen from Fig.5, the proposed scheme is very sensitive to the key parameters, even if a single key parameter is only 0.001 of the deviation, it will lead to a completely different extraction result.

(a)Extracted watermark by the correct key: (0.97,0.99,35,3)

(b) Extracted watermark by the wrong key: (0.971,0.99,35,3)

(c) Extracted watermark by the wrong key: (0.97,0.99,35,3.001)

Figure.5 Extraction result

5. Conclusion

Through research, a new image watermarking scheme based on the fractional order Chen chaotic system and discrete wavelet transform is proposed. The fractional order Chen chaotic system is used to increase the overall complexity of the algorithm. Chaotic system is used to deal with the digital watermarking, and the watermarking information is embedded into the original image which is processed by discrete wavelet transform. By analyzing and comparing the experimental results show that the proposed watermarking scheme has high security and stronger robustness and invisibility. All these characteristics demonstrate that the proposed scheme is in favor of image watermarking encryption.

Acknowledgment

This work was supported by National Nature Science Foundation of China (No: 61201227).

References

[1] S. Poonkuntran, R.S. Rajesh. “Chaotic model based semi fragile watermarking using integer transforms for digital fundus image authentication”, Multimedia Tools & Applications, vol. 68, no.1,pp. 79-93, 2014.

[2] X.J.Tong, Y.Liu, M.Zhang, et al. “A novel chaos-based fragile watermarking for image tampering detection and self-recovery”, Signal Process Image Commun, vol. 28, no.3,pp. 301-308, 2013.

[3] S.Behnia, M.Teshnehlab, P.Ayubi. “Multiple-watermarking scheme based on improved chaotic maps”, Communications in Nonlinear Science & Numerical Simulation, vol. 15, no.9,pp. 2469-2478,2010.

[4] T.G.Gao, Q.L.Gu, S.Emmanuel. “A novel image authentication scheme based on hyper-chaotic cell neural network”, Chaos Solitons&Fractals, vol. 42, no.1,pp. 548-553, 2009.

[5] A.Mooney, J.G.Keating, I.Pitas. “A comparative study of chaotic and white noise signals in digital watermarking”, Chaos Solitons&Fractals, vol. 35, no.5,pp. 913-921,2008.

[6] G.Y.Gao, G.P.Jiang. “Zero-bit watermarking resisting geometric attacks based on composite-chaos optimized SVR model”, The Journal of China Universities of Posts and Telecommunications, vol. 18, no.2,pp. 94-101,2011.

[7] S.Rawat, B.Raman. "A publicly verifiable lossless watermarking scheme for copyright protection and ownership assertion", AEU-International Journal of Electronics and Communications, vol. 66 ,no.11,pp. 955-962,2012.

[8] M.R.Keyvanpour, F.M.Bayat. "Blind image watermarking method based on chaotic key and dynamic coefficient quantization in the DWT domain", Mathematical&Computer Modelling, vol. 58,pp. 56-67,2013.

[9] D.Y.Zhao, J.P.Chen, J.C.Sun. "Design and implementation of improved watermarking system in WT domain", The Journal of China Universities of Posts and Telecommunications, vol. 14,no.2,pp. 58-63,2007.

[10] M.Barni, F.Bartolini, A.Piva. "Improved wavelet-based watermarking through pixel-wise masking", IEEE Transactions on Image Processing A Publication of the IEEE Signal Processing Society, vol. 10,no.5,pp. 783-791,2001.

[11] B.Y.Lei, D.Ni, S.P.Chen, et al. "Optimal image watermarking scheme based on chaotic map and quaternion wavelet transform", Nonlinear Dynamics, vol. 78,no.4,pp. 2897-2907,2014.

[12] O.Benrhouma, H.Hermassi, S.Belghith. "Tamper detection and self-recovery scheme by DWT watermarking", Nonlinear Dynamics, vol. 79,no.3,pp. 1-17,2014.

[13] J.Song, Z.Zhang. "A Digital Watermark Method Based on SVD in Wavelet Domain", International Journal of Advancements in Computing Technology, vol. 3,no.8,pp. 205-214,2011.

[14] G.P.Tang, X.F.Liao, Y.Chen. "A novel method for designing S-boxes based on chaotic maps", Chaos Solitons&Fractals, vol. 23,no.2,pp. 413-419,2005.

[15] C.P.Li, G.J.Peng. "Chaos in Chen's system with a fractional order", Chaos Solitons&Fractals, vol.22,no.2,pp. 443-450,2004.

[16] S.M.Kenneth, R.Bertram. "An introduction to the fractional calculus and fractional differential equations", Wiley-Interscience, vol. 65,no.9,pp. 1000-1003,1993.

[17] J.H.Song, J.W.Song, Y.H.Bao. "A Blind Digital Watermark Method Based on SVD and Chaos", Procedia Engineering, vol. 29,no.29,pp. 285-289,2012.

[18] T.H.Chen, G.B.Horng, W.B.Lee. "A publicly verifiable copyright-proving scheme resistant to malicious attacks", IEEE Transactions on Industrial Electronics, vol. 52,no.1,pp. 327-334,2005.

[19] W.B.Pennebaker, J.L.Mitchell. JPEG Still Image Data Compression Standard, New York: Van Nostrand Reinhold, 1993.

[20] T.Acharya, P.S.Tsai. JPEG2000 Standard for Image Compression: Concepts, Algorithms and VLSI Architectures,New York: John Wiley & Sons, 2004.

[21] R.C.Gonzalez, R.E.Woods. Digital Image Processing, New York: Addison-Wesley Longman Publishing Co., Inc., 2001.

[22] W.K.Pratt. Digital Image Processing,New York: Wiley & Sons, 1991.

[23] A.Rosenfeld A, A.C.Kak. Digital Picture Processing,Cambridge, Massachusetts: Academic Press,1982.

Author Brief and Sponsors:

Dawei Ding, he is an associate professor with School of Electronics and Information Engineering at Anhui University, Hefei, China. His research area include communications networks, the nonlinear circuit network, the network congestion control, non- linear dynamics and chaos, bifurcation, etc..