

Fingerprint images encryption via multi-scroll chaotic attractors [☆]

Fengling Han ^{a,*}, Jiankun Hu ^a, Xinghuo Yu ^b, Yi Wang ^a

^a School of Computer Science and Information Technology, Royal Melbourne Institute of Technology, Melbourne, VIC 3001, Australia

^b School of Electrical and Computer Engineering, Royal Melbourne Institute of Technology, Melbourne, VIC 3001, Australia

Abstract

This paper proposes a chaotic fingerprint images encryption approach. An image of a fingerprint is encrypted via a two-dimensional (2D) chaotic sequence obtained from multi-scroll chaotic attractors. Initial values of the chaotic attractors are served as the private key, which can be generated from the pixel distribution of the binary images of the captured fingerprints. Due to the dynamic uncertainties in the acquisition process of fingerprint images, the keys generated from the pixel value distribution are virtually random. With the elaborately designed 2D chaotic sequence, the encrypted fingerprint images have balanced 0–1 ratio and ideal nonlinearity. Only with the valid private key can the images of fingerprint be recovered. Simulation results and 2D-DFT validate this chaotic encryption approach.

© 2006 Elsevier Inc. All rights reserved.

Keywords: Biometrics; Chaotic attractor; Fingerprint; Image encryption; Multi-scroll

1. Introduction

Biometric authentication refers to verifying individuals based on their physiological and behavioral characteristics. It is inherently more reliable than password-based authentication, as biometric characteristics cannot be lost or forgotten; they are extremely difficult to copy, share and distribute, and require the person being authenticated to be present at the time and point of authentication. Thus, biometrics-based authentication is a potential candidate to replace password-based authentication [1]. Among all the biometric technologies, fingerprints are the oldest and widely used in personal verification. Although not scientifically established, fingerprints are believed to be unique across individuals, and across fingers of the same individual. Even identical twins having similar DNA, are believed to have different fingerprints.

Fingerprints can be represented by a large number of features, including the overall ridge flow pattern, ridge frequency, location and position of singular points (core(s) and delta(s)), type, direction, and location

[☆] The work is financially supported by the ARC Linkage project LP0455324.

* Corresponding author.

E-mail addresses: fengling@cs.rmit.edu.au (F. Han), jiankun@cs.rmit.edu.au (J. Hu), x.yu@rmit.edu.au (X. Yu), alice@cs.rmit.edu.au (Y. Wang).

of minutiae points, ridge counts between pairs of minutiae, and location of pores [2]. There are two basic fingerprint authentication schemes, namely local fingerprint matching scheme and the centralized matching scheme. In the centralized matching scheme, fingerprint images captured at the local site are sent to the central point via the network, then to be matched against the minutiae templates stored in the central server. Currently nearly all ATM banking systems are using the central matching scheme. As digital images, after captured by live-scanner, the fingerprint images need to be protected before transmitted. Generally, there are two major approaches that are used to protect digital image/video from attacker. One is information hiding such as digital watermarking of image/video. The other is encryption, which includes conventional encryption and others such as chaotic encryption [3].

Due to some intrinsic features of images, such as bulk data capacity and high correlation among pixels, traditional encryption algorithms such as DES, IDEA and RSA are not suitable for practical image encryption [4]. On the other hand, the properties of chaotic systems, such as the sensitivity to initial conditions and system parameters, the mixing or topological transitivity, attract research interest on the topic of chaotic-cryptography [4–10]. Sensitivity to parameters causes the properties of the system to change drastically even when exists a very slightly perturbing of the parameters of the system. This property resembles that of a conventional cryptographic system. Mixing is the tendency of the system to quickly blend small portions of the state space into an intricate network of filaments. These characteristics can also make correlated information become scattered all over the phase space. These characteristics form a basis of chaotic data encryption [7].

In recent years, a number of digital chaotic cryptographic schemes have been proposed [6–10]. Based on chaotic map, an image encryption approach was proposed [3]. A permutation of the pixels of image was designed and the “XOR plus mod” operation was applied in the approach. The image encryption schemes based on 3D chaotic Cat maps [6] and Baker maps [7] were discussed. In [6], 3D Cat map was employed to shuffle the positions of image pixels, and another chaotic map was used to confuse the relationship between the cipher-image and the plain-image. In this way, the resistance to statistical and differential attacks is significantly increased. In [7], a Baker map was used to speed up image encryption while retaining its high level of security. In [8], a chaotic key-based algorithm (CKBA) for image encryption was developed. According to a binary sequence generated from a chaotic map, the pixels of images were XOR-ed or XNOR-ed to the pre-determined keys. The cryptanalysis of [8] was conducted in [9], which pointed out that the CKBA was very weak to the chosen/known-plaintext attack, and its security to brute-force ciphertext-only attack is overestimated by the authors. In [10], a fast image encryption algorithm based on vector quantization was proposed. Vector quantization is a low bit-rate image compression technique. The proposed method can reduce computation complexity of the encryption and decryption with the expense that the decrypted image being distorted slightly, but within the limitation of human perception.

It should be noted that digital images are usually represented as two-dimensional (2D) arrays. For protecting the stored 2D data, most existing chaotic image encryption methods are to convert the 2D data to one-dimensional (1D) arrays before using various traditional encryption techniques. This will increase the risk of correlation attack and also increase the processing overhead.

In our previous research [11–13], a scheme for generating multi-scroll chaotic attractors with linear second-order systems and hysteresis series was presented. The analysis and design of the multi-scroll chaos generation systems are possible as their dynamic behaviors are that of linear second-order systems on different sub-planes, which connected to one another via the switching of hysteresis function series. Furthermore, the scroll number can be chosen arbitrarily, and the scrolls can be located anywhere in the phase space. Based on this work, we propose a novel approach to encrypt the fingerprint images via the multi-scroll chaotic attractors. The basic idea of our method is to encrypt a fingerprint image with a chaotic balanced 0–1 distribution 2D image, which is the same size as the 2D fingerprint image. As the dynamic trajectories of chaotic systems are sensitive to initial conditions that are obtained from the unpredictable pixel value distribution of the fingerprint images, the generated keys are random. The 2D discrete chaotic images, which come from the multi-scroll chaotic attractors, can be well designed in terms of security. The proposed scheme has perfect statistic spectrum which has resolved the high correlation issue suffered by the original images.

The paper is organized as follows: Section 2 introduces the generation of multi-scroll chaotic attractors for fingerprint image encryption. Section 3 demonstrates how to encrypt and decrypt the fingerprint images via

the 2D discrete chaotic sequences obtained from the multi-scroll chaotic attractors. Section 4 evaluates the chaotic encryption approach. Conclusions are drawn in the last section.

2. Generation of the multi-scroll chaotic attractors

In this section, the multi-scroll chaotic attractors are generated which will be used to encrypt binary fingerprint images.

The multi-scroll chaotic attractors are generated via linear second-order systems with a feedback of hysteresis series. The input of the hysteresis series is a state variable of second-order systems. Let $H(x, n)$ represents the output of a hysteresis series as shown in Fig. 1. Mathematically, it can be described as:

$$H(x, n) = \sum_{i=1}^n h_i(x), \tag{1}$$

where $h_i(x) = h_1(x - (i - 1))$, $h_1(x)$ is a hysteresis function, and n is a positive integer that represents the number of hysteresis.

The nonlinear state equations for generating multi-scroll chaotic attractors can be described as:

$$\begin{cases} \dot{x} = y, \\ \dot{y} = -x + 2\alpha y + H(x, n), \end{cases} \tag{2}$$

where x and y are two state variables, α is a parameter.

Obviously, the equilibrium points of system (2) are located at the x -axis, which are given by $O_x = [0, 1, 2, \dots, n - 1, n]$. For $\alpha > 0$, the equilibrium points are unstable. With proper α and initial conditions, system (2) can generate $(n + 1)$ -scroll chaotic attractors. When $\alpha = 0.125$, $n = 4$, a 5-scroll chaotic attractor is as shown in Fig. 2. This attractor belongs to the piecewise linear type, and can be easily implemented by both software and hardware. The chaotic behaviour of the multi-scroll attractors has been proved theoretically in Refs. [11] and [13].

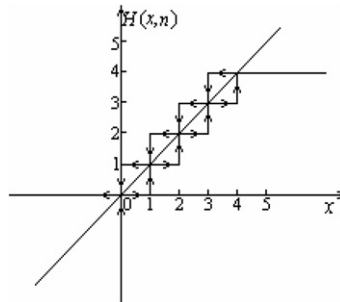


Fig. 1. Hysteresis series ($n = 4$).

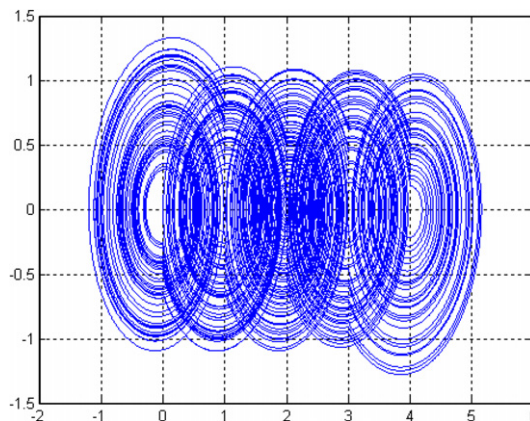


Fig. 2. Phase trajectory of a 5-scroll chaotic attractor.

The circuit implementation and the oscilloscope observed 9-scroll chaotic attractor are as shown in Fig. 3. There are two basic circuit cells in the circuit diagram of Fig. 3(a): the upper cell comprises the linear portion of the system realizing the two integers of the linear second-order continuous system, the lower cell is a hysteresis series $h(V_c, n)$. The input of the hysteresis series is state variables, V_c , and the output is feedback to second-order system. The hysteresis series is implemented with parallel connection of n double hysteresis blocks shown in Fig. 3(b), the detail procedure referenced to [12]. The oscilloscope observed 9-scroll chaotic attractor is as shown in Fig. 3(c).

The generation of the multi-scroll chaotic attractors is quite simple. Furthermore, the parameters α and n in system (2) can be classified as two different types: robust and sensitive, the phase trajectories of system (2) are sensitive to α and the initial conditions; while n is a positive integer, it can be considered as a robust parameter in the systems.

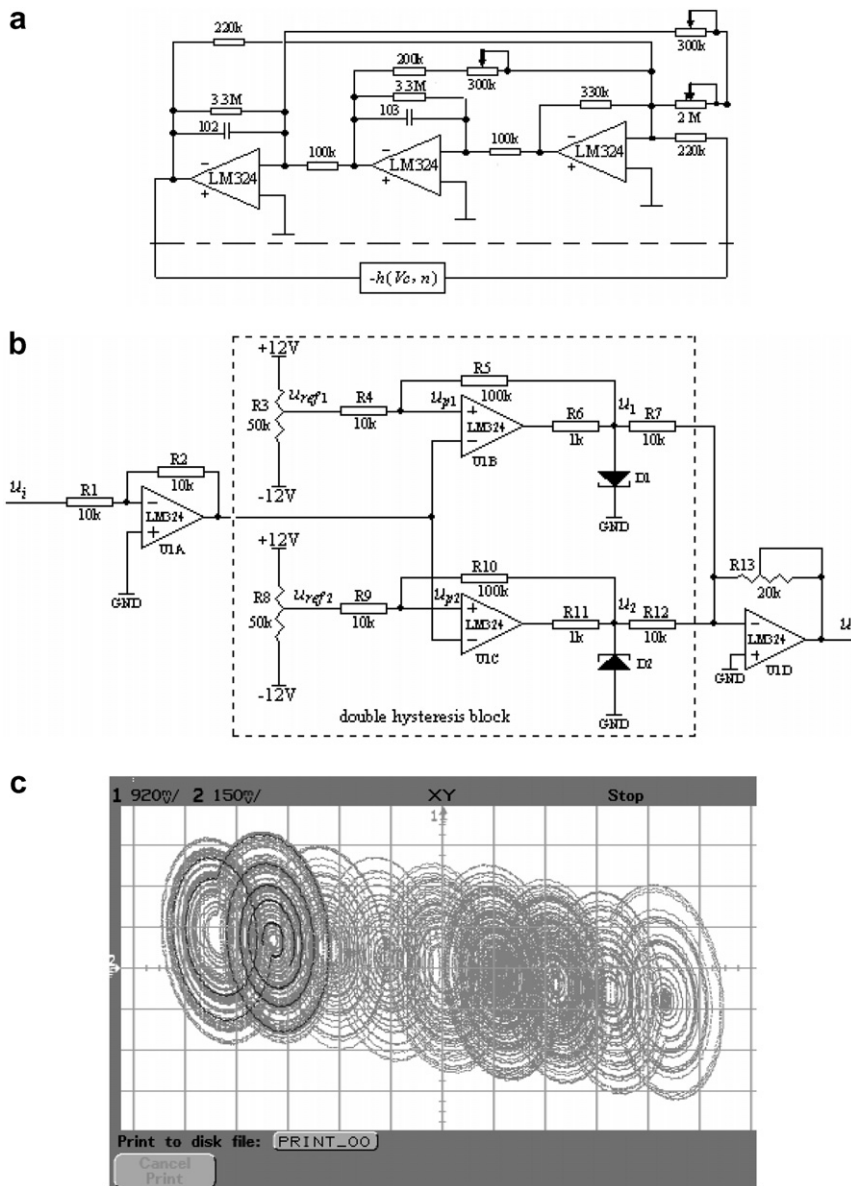


Fig. 3. Circuit implementation of the n -scroll chaotic attractors. (a) Circuit diagram of generating n -scroll chaotic attractors; (b) block diagram of double hysteresis block; (c) oscilloscope observed 9-scroll chaotic attractor.

3. Fingerprint images encryption via a 2D chaotic sequence

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Security products are being developed to address the security needs of an information intensive society [14]. There are two classes of key-based cryptographic algorithms, which are symmetric (private-key) and asymmetric (public-key) algorithms. Symmetric algorithms use the same key for both encryption and decryption, or the decryption key can easily be derived from the encryption key. Asymmetric cryptographic algorithms use different keys for encryption and decryption. The decryption key cannot be derived from the encryption key. In practice, public-key encryption schemes are many times slower than their symmetric-key counterparts [14].

In this section, an asymmetric approach to encrypt fingerprint images via a 2D chaotic sequence is proposed. In this approach, initial conditions of the systems are taken as the private key, which can be obtained from the 0–1 pixel distribution in the captured fingerprint images. The encryption and decryption steps are demonstrated. The simulation results are provided.

3.1. Key generation

Suppose the captured fingerprint images have been processed and the binary images are obtained. An effective method to encrypt a binary image is to mix image data with a message that has the same size as the original image. A XOR operation is a good option for the mixing. According to the basic principle of cryptology [15], a cryptosystem should be sensitive to the key, i.e., the cipher-text should have close correlation with the key [7]. In our scheme, the initial values of a system are selected as the key, which are directly generated from the random pixel distribution of each fingerprint impression.

For simplicity, we take a binary image of fingerprint (size 256×375) shown in Fig. 4 as an example. The two-dimensional input image array is denoted by $f(p, q)$, where p and q represent the horizontal and vertical coordinates respectively, which unit are pixel. The value of $f(p, q)$ is one or zero.

Usually, the fingerprint images (position and orientation angles) vary at different acquisitions due to the non-uniform pressure applied by the subject. This variation will result in different 0–1 pixel distribution in the images. The initial conditions of chaotic trajectory, which are used as the private key, are generated from this random 0–1 distribution of fingerprint images. There are many ways to generate the initial conditions for the chaotic systems. For example, the pixel number of value one in the first and last one-nth rows of a fingerprint images can be counted, the percentages or calculation based on the percentages may set for the initial values $x(0)$ and $y(0)$ of system (2).

3.2. Encryption and decryption of fingerprint images

In order to encrypt the fingerprint image in Fig. 4, it is very important to keep the 2D chaotic sequence which is employed to encrypt the fingerprint image behaves apparently irregular, and maintain a balanced



Fig. 4. A binary image of fingerprint.

0–1 pixel distribution. Considering these requirements, the following steps are conducted to accomplish the encryption and decryption:

- (1) generate two chaotic attractors, their trajectories are $\Phi_1(x_1, y_1)$ and $\Phi_2(x_2, y_2)$;
- (2) conduct $x_1(\cdot) + y_2(\cdot) \rightarrow x$, $y_1(\cdot) + x_2(\cdot) \rightarrow y$, and enlarge (x, y) as shown in Fig. 5(a);
- (3) select a window to match the size of fingerprint image as shown in Fig. 5(b);
- (4) discrete (x, y) , and get the integer sequence (x_k, y_k) as shown in Fig. 6(a);
- (5) diffuse the number of 0 (get a balance 0–1 distribution) to $\zeta_1(x_k, y_k)$;
- (6) repeat steps (3)–(5), get another chaotic sequence $\zeta_2(x_k, y_k)$;
- (7) the encrypted image is obtained by $Enf = f \oplus (\zeta_1 \oplus \zeta_2)$;
- (8) the recovered fingerprint image can be obtained by $Recf = Enf \oplus (\zeta_1 \oplus \zeta_2)$.

The 2D chaotic sequence employed to encrypt fingerprint image is as shown in Fig. 6(b); The encrypted image *Enf* is as shown in Fig. 6(c); And the recovered fingerprint image is as shown in Fig. 6(d). The trajectories of Φ_1 and Φ_2 correspond to a double-scroll ($n = 1$) and a triple-scroll ($n = 2$) chaotic attractor, respectively. In the two chaotic attractors, $\alpha = 0.125$ in system (2). The initial conditions are obtained from the percentage of pixels value zero in the first and the last one-sixth rows in the fingerprint image.

The advantage of this encryption approach can be well illustrated by the elaborately designed 2D chaotic trajectory in Fig. 5(b), and the 2D chaotic sequence in Fig. 6(b). It can be found that Fig. 6(b) has ideal frequency

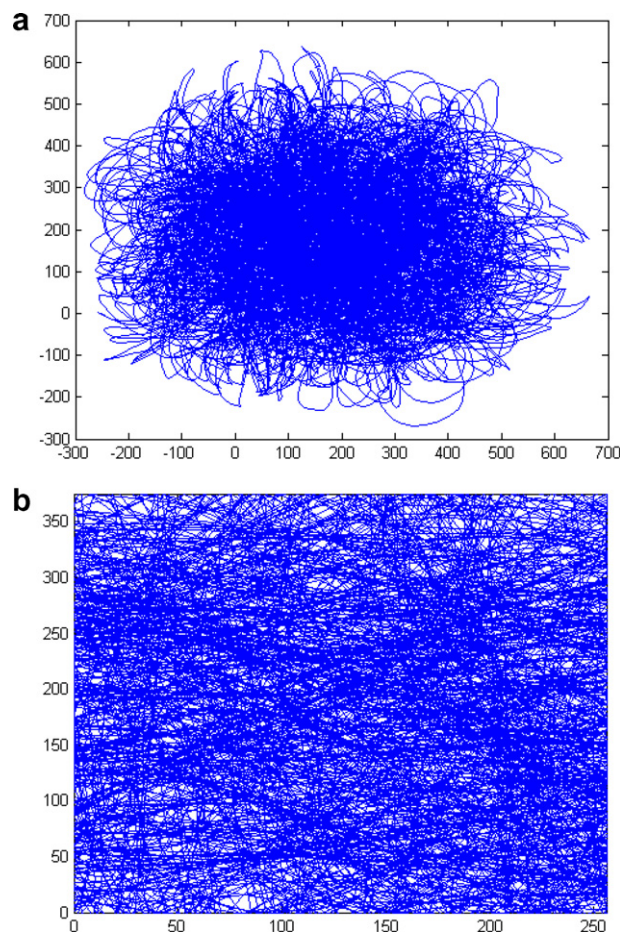


Fig. 5. Phase trajectories of the chaotic attractor. (a) Sum of a double-scroll $[(x_0, y_0) = (0.64585, 0.59803)]$ and a triple-scroll $[(x_0, y_0) = (0.65748, 0.46896)]$ attractor. (b) A window size 256×375 .

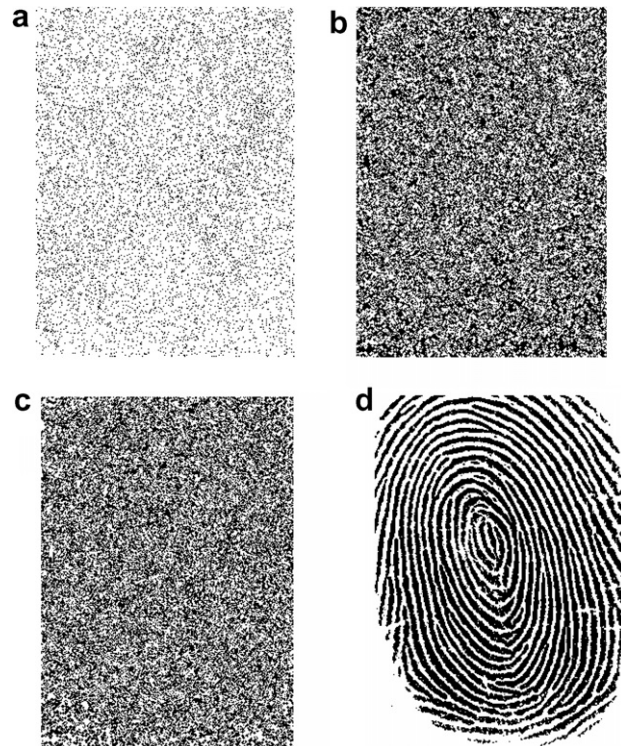


Fig. 6. The phase trajectories of images. (a) 2D chaotic image corresponds to a triple-scroll attractor; (b) 2D chaotic image; (c) encrypted fingerprint image; (d) recovered fingerprint image.

spectrum, randomness and is computationally unpredictable. From Fig. 6(c), one can see that the encrypted fingerprint image has balanced 0–1 ratio and ideal nonlinearity. This is achieved by the following steps:

- (1) The two chaotic attractors Φ_1 and Φ_2 are chosen with different scroll number, the 2D chaotic sequence comes from different combination of Φ_1 and Φ_2 , together with the unpredictable initial conditions, the proposed encryption approach is more resistive to statistic attack.
- (2) Step 5 is used to get a balanced 0–1 distribution while maintain a small computation rate. There are more than 30,000 black points (pixels value zero) in Fig. 6(a), one can see that the black points are still much less compared with the white background. The diffusion is completed by setting the neighbor pixels of zero to zero until a balanced 0–1 distribution is obtained.
- (3) Two chaotic sequences are XOR-ed to guarantee a satisfactory 2D chaotic sequence.

One can even design some schemes to represent specific features of fingerprint with the scroll number n . In this way, the biometric-encryption discussed in Refs. [1] and [16] may be achieved.

4. Evaluations

In addition to the randomness of initial conditions of chaotic attractors at different fingerprint acquisitions, the security of the proposed fingerprint images encryption approach can be further enhanced by agreement between the sender (encryption) and recipient (decryption) in the following aspects:

- (1) choose the parameters α and n of two chaotic attractors;
- (2) determine the algorithm of combination of two chaotic attractors;
- (3) select the suitable chaotic windows;
- (4) design the method to diffuse the number of 0 for a balance 0–1 distribution.

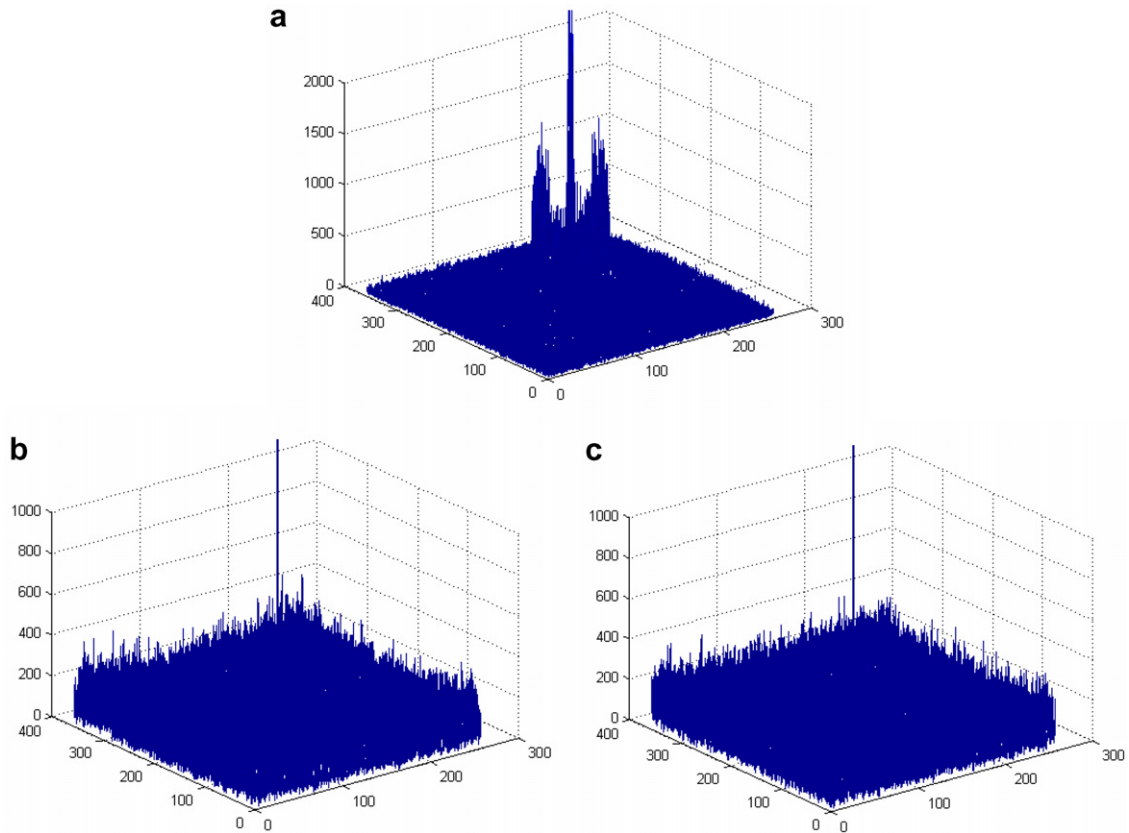


Fig. 7. The spectrums of the three images. (a) Original fingerprint image; (b) chaotic sequence image; (c) the encrypted fingerprint image.

In order to verify the effectiveness of the fingerprint encryption approach proposed in this paper, the two-dimensional discrete Fourier transform (2D-DFT) are used to analyze the relative images. The 2D-DFT algorithm is given below:

$$F(u, v) = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} f(p, q) e^{-j(2\pi/M)up} e^{-j(2\pi/N)vq}, \quad (3)$$

where p and q are coordinates pair of image; M and N are the size of image; $f(p, q)$ is the image value corresponding to the pixel (p, q) .

The spectrum of the original fingerprint image (Fig. 4), of the 2D discrete chaotic image (Fig. 6(b)) and the encrypted fingerprint image (Fig. 6(c)) are depicted in Fig. 7(a)–(c), respectively.

Note that in Fig. 7, the highest narrow spectrums in the middle correspond to the effectiveness of the image edge; they should be ignored in the spectrum analysis. From Fig. 7(a), it is observed that the frequency distribution of the original fingerprint image is concentrated in a small area, which suffers the risk of information leakage. While in our case, the frequency distribution of the chaotic sequence is flat. And through the encryption, the frequency distribution of encrypted fingerprint image has been flattened. Therefore, it has validated that the original fingerprint image is hidden perfectly against statistic attack with the proposed chaotic cryptographic approach.

5. Conclusion

A new fingerprint image encryption approach via a 2D chaotic sequence obtained from multi-scroll chaotic attractors has been proposed. The system parameters of the chaotic trajectories can be designed systematically

according to specific requirements. The initial conditions of the chaotic trajectory can be taken as the private key, which depends on the random pixel value distribution of captured fingerprint images. The encrypted image is the outcome of the XOR operation of the 2D discrete chaotic sequence and the fingerprint image. Only with the valid private key, i.e., the initial values of chaotic systems, can the image of fingerprint be recovered. Otherwise a drastically different image will be produced. Spectrum analysis has demonstrated that an excellent information hiding has been achieved.

References

- [1] U. Uludag, S. Pankanti, S. Prabhakar, A.K. Jain, Biometric cryptosystems: Issue and challenges, *Proceedings of the IEEE* 92 (6) (2004) 948–960.
- [2] S. Pankanti, S. Prabhakar, A.K. Jain, On the individuality of fingerprint, *IEEE Trans. on Pattern Analys. Machine Intellig.* 24 (8) (2002) 1010–1025.
- [3] L. Zhang, X. Liao, X. Wang, An image encryption approach based on chaotic maps, *Chaos, Solitons & Fractals* 24 (2005) 759–765.
- [4] L. Kocarev, G. Jakimoski, T. Stojanovski, U. Parlitz, From chaotic maps to encryption schemes, *Proc. IEEE Int. Symp. Circuits Syst.*, Monterey, CA, vol. IV, 1998, pp. 514–517.
- [5] G. Jakimoski, L. Kocarev, Chaos and cryptography: Block encryption ciphers based on chaotic maps, *IEEE Trans. Circuits Systems* 48 (2) (2001) 163–169.
- [6] G. Chen, Y. Mao, C. Chui, A symmetric encryption scheme based on 3D chaotic cat map, *Chaos, Solitons & Fractals* 21 (2004) 749–761.
- [7] Y. Mao, G. Chen, S. Lian, A novel fast image encryption scheme based on 3D chaotic baker maps, *Int. J. Bifurcat. Chaos* 14 (10) (2004) 3613–3624.
- [8] J.C. Yen, J.I. Guo, A new key-based design for image encryption and decryption, *Proc. IEEE Circuits Sys.* 4 (2000) 49–52.
- [9] S. Li, X. Zheng, Cryptanalysis of a chaotic image encryption method, *Proc. IEEE Int. Symp. Circuits Sys.*, Scottsdale, AZ, USA, vol. 2, (2002) 708–711.
- [10] C.C. Chang, M.S. Hwang, T.S. Chen, A new encryption algorithm for image cryptosystems, *J. Sys. Software* 58 (2001) 83–91.
- [11] F. Han, J. Lü, X. Yu, G. Chen, Y. Feng, Generating multi-scroll chaotic attractors via a linear second-order hysteresis system, *Dynamics of Continuous, Discrete and Impulsive Systems. Series B: Applications & Algorithms* 12 (2005) 95–110.
- [12] F. Han, X. Yu, Y. Wang, Y. Feng, G. Chen, N-scroll chaotic attractors by second-order system and double-hysteresis blocks, *IEE Electron. Lett.* 39 (23) (2003) 1636–1637.
- [13] F. Han, Multi-scroll chaos generation via linear systems and hysteresis series, Ph.D. thesis, Royal Melbourne Institute of Technology, Melbourne, Australia, 2004.
- [14] A. Menezes, P. Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
- [15] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, second ed., Wiley, New York, 1995.
- [16] S. Hoque, M. Fairhurst, G. Howells, F. Deravi, Feasibility of generating biometric encryption keys, *IEE Electron. Lett.* 41 (6) (2005) 309–310.