Biometric Authentication Using Multilevel Encryption And Decryption

Judy Ann Joy
PG Scholar, MMT
Karunya University

Ephin M
Assistant Professor SG/IT
Karunya University

Abstract

Security becomes an important issue nowadays in communication and storage of images. Encryption is one of the method used to ensure the high security of images. Due to the intrinsic features of the images such as bulk data capacity and high correlation among pixels the earlier encryption techniques such as DES, AES, RSA, etc are not suitable for practical applications. So nowadays chaos based encryption is used. In this paper we have two process. The first process is the training process and the second one is testing process. In the training process we will perform the encryption of different fingerprint images and then it will be stored. And in the testing process we will perform the authentication of the user. And the authentication is done after the decryption of the image. The encryption is done in both spatial domain and frequency domain. The spatial domain encryption is done using reversible hidden transform and the frequency domain encryption is done using piecewise linear chaotic map, fractional wavelet packet transform and singular value decomposition. The decryption process is the inverse of encryption process. And finally the authentication is done using support vector machine classifier.

1. Introduction

Information exchanges across the internet and the storage of data on open networks have created an environment in which it is very easy to disclose important information to illegal users. For this reason, encryption techniques were used. Encryption techniques protect the data from illegal tampering and use. Encryption of data has become an important way to protect data resources especially on the Internet, intranets and extranets. Encryption is the process of applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code. The main goal of security management is to provide authentication of users, integrity, accuracy and safety of data resources.

Today the web is going towards multimedia data [1]. The high percentage of multimedia data is images. Images are used in many fields such as biometric authentication, medical science, military, online personal photograph album, etc. Therefore it's very important to protect the image from unauthorized access. That is, it is necessary to assure confidentiality, authenticity and integrity of the digital images transmitted. Image encryption techniques try to convert original image to another image that is hard to understand and to keeps the image confidential between users. And without the decryption key no one can access the original images. Image encryption has applications in many fields such as military communication, internet communications, multimedia systems, medical imaging, telemedicine, etc [5]. Image encryption is different from text encryption [2]. Due to the intrinsic features of the images such as bulk data capacity and high correlation among pixels the earlier encryption techniques such as DES, AES, RSA, etc are not suitable for practical applications [3-11]. In this case chaos based encryption techniques are considered good for practical use.

Chaos theory was discovered by Edward N Lorenz in 1963 [12, 13]. Chaos theory has been established since 1970s by many different research areas, such as mathematics, physics, engineering, biology, economics, and philosophy, etc [14]. In common usage, chaos means a state of disorder. Since there is no universally accepted mathematical definition of chaos, a commonly used definition is that, for a dynamical system to be said as chaotic, it must satisfy the following properties: 1) Its periodic orbit must be dense, 2) It must be sensitive to initial conditions, and 3) It must be topologically mixing. Sensitive to initial conditions means that a small difference in the initial conditions will produce widely diverging outcomes for chaotic systems, so that long-term prediction is impossible. The topological mixing (or topological transitivity) property ensures the ergodicity of a chaotic map, which means that if we partition the state space into a finite number

of regions, no matter how many it is, any orbit of the map will pass through all these regions [13].

Since 1990s, many researchers have noticed that there exist the close relationship between chaos and cryptography [15-20]. The main difference between chaos theory and cryptography is that cryptosystems work on a finite field, while chaos is meaningful only on a continuum. Nevertheless, these two scientific notions are very closely related. Many fundamental concepts in chaos theory, such as mixing and sensitivity to initial conditions and parameters, actually coincide with those in cryptography. The mixing property is closely linked to the diffusion feature of cryptosystems [21]. The similarities and differences between the two subjects can be listed [18], as shown in Table 1. Chaotic maps and cryptographic algorithms have some similar properties: both are sensitive to tiny changes in initial conditions and parameters; both have random like behaviors; and cryptographic algorithms shuffle and diffuse data by rounds of encryption, while chaotic maps will spread a small region of data over the entire phase space via iterations. The only difference is that encryption operations are defined on finite sets of integers while chaos is defined on real numbers.

Due to the exceptional properties of mixing and sensitivity to the initial conditions and parameters of chaotic maps [22], chaos-based encryption is a new and efficient way to deal with the intractable problem of fast and highly secure image encryption. Chaos based algorithms provide a good combination of speed, complexity, high security, reasonable computational overheads and computational power.

Table 1. Similarities and differences between chaos and cryptography

Chaotic Systems	**Cryptographic algorithms**
Phase space: set of real numbers	Phase space: finite set of integers
Iterations	Rounds
Parameters	Key
Sensitive to initial conditions and parameters	Diffusion

Biometric authentication is gaining wide-spread popularity in recent years due to the advances in sensor technologies as well as improvements in the matching algorithms that make the systems both secure and cost-effective. For automatically recognizing or verifying the identity of a human being biometrics is used. Since the biometrics is unique it will identify the humans by their characteristics or traits. Biometric technologies are typically used to analyze human characteristics for security purposes. The most commonly used physical biometric patterns analyzed for security purposes are the fingerprint, eye, face, hand and voice.

2. Related Works

A new method based on Fractional Wavelet Packet Transform (FWPT) is introduced by L. Chen and D. Zhao to encrypt images [24], in which fractional order of fractional wavelet packet transform is used as the key. FWPT [23] is a Wavelet Packet Transform (WPT) realized in a Fractional Fourier domain. In this method first the image is decomposed into various subbands. Then some of the subbands are randomly selected and encrypted using fractional wavelet packet transform. The selected encryption with FWPT is more effective than that with WPT, because it is realized in the fractional Fourier domain and the information is more randomly distributed at fractional Fourier plane than at Fourier plane. This paper has an advantage to achieve data confidentiality. And it has a drawback of limited key space and limited perceptual quality [3]. Key space size is the total number of different keys that can be used for the encryption. A good encryption scheme should have the key space that should be large enough to make brute-force attacks infeasible. Limited perceptual quality means that we will get the glimpse of the original image after encryption.

Due to the drawback of weak security in one-dimensional chaotic cryptosystems Haojiang Gao, Yisheng Zhang, Shuyun Liang and Dequn Li presents a new Nonlinear Chaotic Algorithm (NCA). The one-dimensional chaotic map, for example logistic map have linear function. But the Nonlinear Chaotic Algorithm (NCA) uses power function and tangent function instead of linear function. In the encryption process, at first the encryption key is set. Then the NCA is iterated 100 times to obtain the encrypted image. After the encryption the encrypted image is send through the public communication channel and the encryption key is send through the secure communication channel. And at the receiver side the decryption is similar to encryption algorithm. This paper has the advantages of high level security and sensitive to key. And it have a disadvantage of small keyspace. [25]

Delong Cui introduced a novel image encryption algorithm based on Fractional Fourier transform and chaotic system. In that paper the encryption process includes two steps. At first the image is encrypted

double random phase using fractional fourier domain. Using a matrix generated by chaotic logistic map that image is again encrypted and thus the encrypted fingerprint image is obtained. The decryption process is similar to encryption process. It is the inverse of encryption process It will resist brute force attack. But it has small key space.[26]

3. Proposed Method

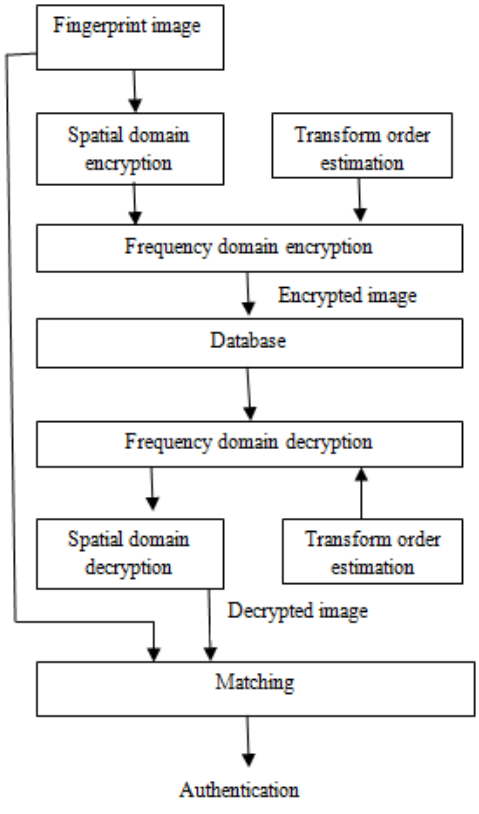


Figure 1. Block diagram of the proposed method

Figure 1 shows the block diagram of the proposed method. This paper aims to provide authentication and security to the fingerprint images. The security is achieved by encryption process. This paper has mainly two parts, at first we will perform training process and then the testing process. In the training process we will perform encryption of different fingerprint images. In the encryption method initially the original fingerprint image has undergone spatial domain encryption. The spatial domain encryption is achieved using reversible hidden transform [3]. Then, using Piece-wise Linear Chaotic Map (PWLCM) [27, 3] we have found the transform order. Then the transformed fingerprint image has undergone frequency domain encryption. In the frequency domain encryption the transformed image is decomposed into various subbands using fractional wavelet packet transform (FrWPT) [23, 3]. Then, each subband is deformed using chaotic map and singular value decomposition [3]. After the deformation we will perform inverse fractional wavelet packet transform to get the encrypted fingerprint image. The decryption process is the inverse of encryption process. And in the testing process we will use support vector machine classifier. In the testing process the authentication is done. Only after the decryption we will perform the authentication.

3.1 Reversible Hidden Transform

Based on some secret parameters Reversible Hidden Transform [3] is a simple integer transform that transforms an integer pair to another integer pair. In this, initially the image will be partitioned into pairs of pixels. Let $x = (x_1, x_2)$ be a pair of pixels and 'a', 'b' be two fixed numbers. The forward transform is

$$y = T(x) \quad (1)$$

where $y = (y_1, y_2)$ is the transformed pair of pixels, and its values are given by

$$y_1 = ax_1 + bx_2 \quad (2)$$

$$y_2 = bx_1 + ax_2 \quad (3)$$

since both x_1 and x_2 lie between [0, 255], there may be a situation of underflow ($y_1 < 0$ or $y_2 < 0$ or both) or overflow ($y_1 > 0$ or $y_2 > 0$ or both). The following conditions should be satisfied in order to avoid underflow and overflow of the transformed pixels,

$$0 \le y_1 \le 255;\ 0 \le y_2 \le 255 \quad (4)$$

This is possible only when 'a' and 'b' satisfy the relation

$$a + b = 1 \text{ and } 0 \le a, b \le 1 \quad (5)$$

The inverse transform is T^{-1}

$$\bar{x} = T^{-1}(y)$$

where $\bar{x} = (\overline{x_1}, \overline{x_2})$ is the reconstructed pair of pixels, and their values are given by

$$\overline{x_1} = \frac{ay_1 - by_2}{a^2 - b^2} \quad (6)$$

$$\overline{x_2} = \frac{by_1 + ay_2}{b^2 - a^2} \quad (7)$$

3.2 Piecewise Linear Chaotic Map

Extreme sensitivity to initial conditions, random noise-like behavior, the outspreading of orbits over the entire space, etc are the most attractive features of chaotic maps. 1-D chaotic maps are the simplest chaotic maps that have the advantages of high-level efficiency and

implicit nature. One of the simplest 1-D chaotic maps is the logistic map. The major drawback of the logistic map is nonuniformity. The existence of blank windows in the chaotic region is its second drawback. Piecewise linear chaotic map is a chaotic map that have better properties than the logistic map. This map has better dynamical and statistical properties than the logistic map and is composed of multiple line segments. In the proposed work, piecewise linear chaotic map is used to find the transform orders for Fractional Wavelet Packet Transform. Mathematically PWLCM is represented as follows

$$x(k+1) = C[x(k):\mu] = \begin{cases} \dfrac{x(k)}{\mu}, & if \quad x(k) \in [0,\mu) \\ \dfrac{x(k)-\mu}{0.5-\mu}, & if \quad x(k) \in [\mu,0.5) \\ C[1-x(k):\mu], & if \quad x(k) \in [0.5,1) \end{cases} \tag{8}$$

3.3 Fractional Wavelet Packet Transform

The Fractional Wavelet Packet Transform (FrWPT) [23] of a 1-D function $f(t)$ is given by

$$W_\alpha(u,s,T) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(t)K_\alpha(t,x)e^{-jux}\psi_{s,T}(x)dtdx \tag{9}$$

where s, T and α are the scale, translation parameters and transform order respectively. From the above equation it is clear that FrWPT is the realization of the wavelet packet transform in fractional Fourier domain. The unique property of Fractional Fourier transform (FrFT) is its ability to describe the information in both spatial and frequency domain. It is due to the rotation of time-frequency plane over an arbitrary angle. And wavelet packet transform has a multiresolution property. A combination of these two produce the fractional wavelet packet transform, that exhibits multiresolution property and describes the spatial and frequency domain information. In order to reconstruct the original signal back from the decomposed signal, the inverse FrWPT is defined as

$$f(t) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} W_\alpha(u,s,T)K_{-\alpha}(t,x)e^{jux}\psi_{s,T}(x)dudsdTdx \tag{10}$$

3.4 Singular Value Decomposition

The Singular Value Decomposition (SVD) is an important factorization of a rectangular real or complex matrix. Let A be a real or complex matrix of order m × n. The SVD of A is of the form A = USV^T , where U is an m × m unitary matrix over K, matrix S is an m × n diagonal matrix with nonnegative real numbers, and V^T denotes the conjugate transpose of V , which is an n × n unitary matrix over K. Such factorization is called an SVD of A.

3.5 Encryption Process

1) Perform Reversible Hidden Transform on the original fingerprint image, which is denoted by F .
2) Based on PWLCM and adopting keys K1 and K2 as the initial values, generate two different chaotic sequences K_i. And the final value of K_i are used as the transform orders for FrWPT.
3) Perform n-level FrWPT on F . Then it is decomposed into subbands.
4) Again based on PWLCM and adopting key K3 as the initial value, generate a chaotic sequence K_3. L3 = $m \times n$, where m and n are the dimensions of subband.
5) Map K_3 into an integer sequence $\tilde{K}_3$, such that every element lies in [0,255].
6) The obtained chaotic sequence $\tilde{K}_3$ is arranged in the form of a matrix of dimension $m \times n$, which is denoted by P and termed as matrix key.
7) Perform SVD on P, which gives P=$U_P S_P V_P^T$.
8) Deform all coefficients of each subband using orthonormal matrices U_P and V_P .
9) Perform inverse n-level FrWPT to get the encrypted fingerprint image ($\tilde{F}$).

3.6 Decryption Process

1) Perform n-level FrWPT on $\tilde{F}$, then it is decomposed into subbands.
2) Perform inverse deformation on coefficients of every subband.
3) Perform n-level inverse FrWPT.
4) Perform inverse Reversible Hidden Transform to get the decrypted image.

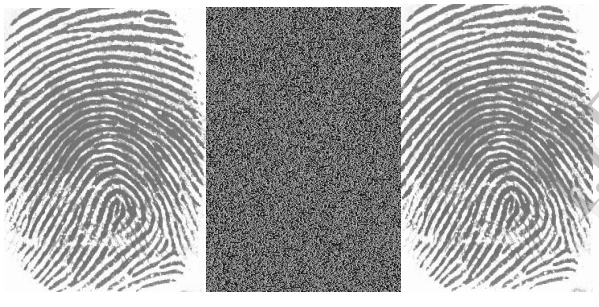
3.7 Support Vector Machine

Based on statistical learning theory Support Vector Machine is a powerful learning tool. It is a supervised learning model. A SVM is a binary classifier that makes its decision by constructing a linear decision boundary or hyper plane that optimally separate data points of the two classes in feature hyperspace [28] and also makes the margin maximized. One of the advantage of the SVM is that very few parameters need to be fixed by the user, almost all parameters are determined internally by the algorithm SVMs have many advantages over Neural Networks. Artificial

Neural Network (ANN) are prone to the danger of over training resulting in a solution over-fitted to the database being worked on. This could lead to overly optimistic results and accuracy outcomes. Secondly it has been found that SVMs are comparatively faster to train than ANNs.

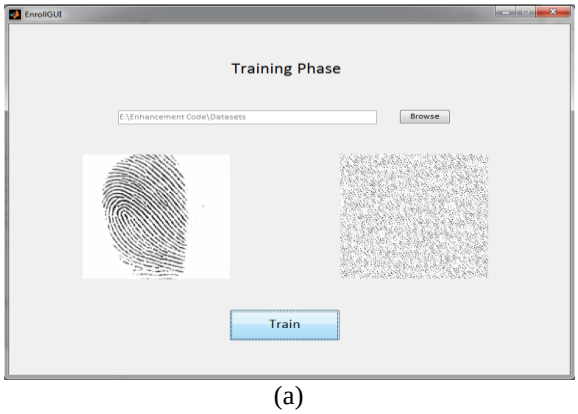
4. Results and Experimentations

The effectiveness of our proposed biometric authentication scheme is evaluated on the fingerprint database. The experiments are conducted in MATLAB with image processing Toolbox and on a machine with an Intel core 2 Duo CPU Processor. Below figures shows some experimental results. Figure 2(a) shows the original fingerprint image, Fig. 2(b) shows the encrypted fingerprint image and Fig. 2(c) shows the decrypted fingerprint image. Figure 3 shows the authentication process. Fig. 3(a) shows the training process. In that the encryption of different fingerprint image will occur. And Fig. 3(b) shows the testing process. In that the authentication process is done.

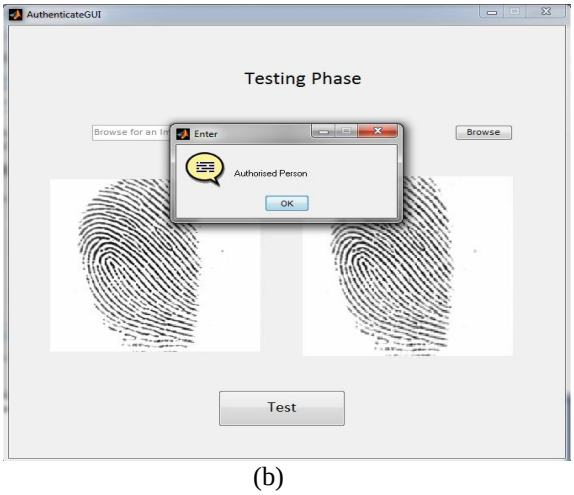


(a) (b) (c)

Figure 2: (a) Original fingerprint image, (b) Encrypted fingerprint image, (c) Decrypted fingerprint image.



(a)



(b)

Figure 3. Authentication: (a) Training process, (b) Testing process.

5. Conclusion

In this paper the security is provided to the fingerprint image through encryption. And the authentiation is done using support vector machine. The encryption is achieved in both spatial domain and in frequency domain. Since the encryption is done in both spatial and frequency domain it have more security and the encrypted image is perceptually efficient. The spatial domain encryption is done using Reversible Hidden Transform and the transform order is found using Piecewise Linear Chaotic Map. The transform order is used as the key for encryption. And the frequency domain encryption is done using fractional wavelet packet transform and singular value decomposition. And finally the support vector machine is used to authenticate the user.

6. References

[1] Monisha Sharma, Manoj Kumar Kowar, "Image encryption techniques using chaotic schemes: a review" *International Journal of Engineering Science and Technology*, Vol. 2(6), 2010, pp. 2359-2363.

[2] Payal Sharma, Manju Godara, Ramanpreet Singh, Digital "Image encryption techniques: A Review", *International journal of computing & business Research*, 2012

[3] Gaurav Bhatnagar, Q. M. Jonathan Wu; "Chaos-Based Security Solution for Fingerprint Data During Communication and Transmission" *IEEE trans. Instrumentation and measurement*, vol. 61, no.4, april 2012, pp. 876-887.

[4] Varsha S.Nemade, R.B.Wagh, "Review of different image encryption techniques", *World Journal of Science and Technology*, Volume-2, 2012, pp. 95-98.

[5] Abhinav Srivastava, "A survey report on Different Techniques of Image Encryption", *International Journal of*

Emerging Technology and Advanced engineering, vol. 2, June 2012, pp. 163-167.
[6] Fengling Han, Jiankun Hu, Xinghuo Yu, Yi Wang, "Fingerprint images encryption via multi-scroll chaotic attractors", *Applied mathematics and computation*, 2007, pp.931-939.
[7] S. Behnia, A. Akshani, H. Mahmodi, A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps", *Chaos Solutions and Fractals*, 2008, pp. 408-419.
[8] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encryption algorithm for image cryptosystems", *The Journal of systems and software*, 2001, pp. 83-91.
[9] Tapas Bandyopadhyay, B Bandyopadhyay, B N Chatterji, "Secure image encryption through key hashing and wavelet transform techniques", *International Journal of emerging technology and Advanced engineering*, vol. 2, Feb 2012, pp. 26-31.
[10] Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, Ganapati Panda, "Image encryption using advanced Hill Cipher Algorithm", *International Journal of Recent trends in Engineering*, vol.1, No. 1, may 2009, pp. 663-667.
[11] H. S. Kwok, Wallace K.S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation", *Chaos Solutions & Fractals*, 2007, pp. 1518-1529.
[12] Lorenz EN "The Essence of Chaos", *University of Washington Press, Seattle, WA*, 1993
[13] Yaobin Mao, Guanrong Chen, "Chaos-Based image encryption", *Handbook of geometric computing*, 2005, pp.231-265.
[14] Hao B. "Starting with parabolas: an introduction to chaotic dynamics". *Shanghai China: Shanghai Scientific and Technological Education Publishing House*, 1993
[15] Brown R., Chua LO, "Clarifying chaos: examples and counterexamples", *International journal of Bifurication Chaos*, 1996, pp.219-242.
[16] Fridrich J., "Symmetric ciphers based on two-dimensional chaotic maps", *International journal of Bifurication Chaos*, 1998, pp. 1259-1284.
[17] Dachselt F, Schwarz W "Chaos and cryptography". *IEEE Trans Circuits and Systems-I*, 2001, pp.1498 – 1509.
[18] Kocarev L "Chaos-based cryptography: a brief overview", *IEEE Circuits and Systems Magazine*, 2001, pp.6 – 21.
[19] Kocarev L, Jakimovski G "Chaos and cryptography: From chaotic maps to encryption algorithms*". IEEE Trans Circuits and Systems-I*, 2001, pp:163 – 169
[20] Schmitz R "Use of chaotic dynamical systems in cryptography". *J Franklin Institute*, 2001, pp:429 – 441.
[21] L. Kocarev, G. Jakimoski, T. Stojanovski, and U. Parlitz, "From chaotic maps to encryption schemes", in *Proc. IEEE Int. Symp. Circuits Syst., Monterey, CA*, vol. IV, 1998, pp. 514-517.
[22] Linhua Zhang, Xiaofeng Liao, Xuebing Wang, "An image encryption approach based on chaotic maps", *Chaos solutions & fractals*, 2005, pp. 759-765.
[23] Y. Huang and B. Suter, "The fractional wave packet transform", *Multidimensional Syst. Signal process*, vol. 9, no. 4, Oct. 1998, pp. 399-402.
[24] L. Chen and D. Zhao, "Image encryption with fractional wavelet packet method," *Optik—Int. J. Light Electron Opt.*, vol. 119, no. 6, May 2008, pp. 286–291.
[25] Haojiang Gao, Yisheng Zhang, Shuyun Liang,Dequn Li; "A new chaotic algorithm for image encryption" *chaos, solutions and fractals* , vol. 29, 2006, pp. 393-399.
[26] Delong Cui, "A novel fingerprint encryption algorithm based on chaotic system and fractional fourier transform", *in Proc. International conference on machine vision and human- machine interface*, 2010, pp. 168-171.
[27] Muhammad Khurram Khan, Jiashu Zhang, Khaled Alghathbar, "Challenge-respone-based biometric image scrambling for secure personal identification" *Future generation computer systems*, 2011, pp. 411-418.
[28] Vapnik, V. "The nature of statistical learning theory". *Springer-Verlag, Berlin*, 1995.