Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Computer Science 10 (2012) 442 – 449

Procedia Computer Science

The 3rd International Conference on Ambient Systems, Networks and Technologies (ANT)

A Novel Chaotic Encryption Framework for Securing Palmprint Data

Gaurav Bhatnagar, Q.M. Jonathan Wu*

Department of Electrical and Computer Engineering, University of Windsor, Windsor, Ontario, ON, N9B 3P4, CANADA

Abstract

In this paper, a chaotic encryption framework based on fractional wavelet packet transform (FrWPT) is proposed for securing palmprint data. The palmprint image is first transformed into FrWPT domain with chaotically generated transform orders followed by the alteration of FrWPT coefficients using Hessenberg decomposition. Finally, a reliable decryption scheme is presented to reconstruct original plamprint image from the encrypted data only with the valid keys. Simulated results and analysis validate the efficiency and robustness of the proposed technique.

Keywords: Biometrics, Palmprint Protection, Chaotic Map, Fractional Wavelet Packet Transform, Hessenberg decomposition.

1. Introduction

Biometrics [1] is an automated method that uses measurable, physical or physiological characteristics or behavioral traits to recognize the identity or authenticate the claimed identity of an individual. Usually, biometrics can be divided into two categories viz. physiological and behavioral biometrics. Physiological biometrics is related to the shape of the body and includes fingerprint, iris, face, DNA, hand and palm geometry, odour/scent, signature, keystroke dynamics etc. On the other hand, behavioral biometrics is related to the behavior of a person and includes typing rhythm, gait, voice etc. Biometrics is a unique characteristic of an individual and it is believed that the chance of two persons, even identical twins, having the same biometrics is probably less than one in a billion. This property makes biometrics not only a very powerful tool for matching different pieces of information of individuals across multiple databases, but also attempts to enhance security. The main applications of biometrics include physical and logical access controls, attendance recording, payment systems, security, crime/fraud prevention/detection and border security controls.

In the recent years, biometrics is gaining increasing support and interest from the research community for security purposes [2, 3]. Almost all security systems based on biometrics use either biometric recognition or authentication. For this purpose, the biometrics of an individual is usually compared to a previously

*Corresponding author: Q.M. Jonathan Wu (jwu@uwindsor.ca)
Gaurav Bhatnagar (goravb@uwindsor.ca)

1877-0509
doi:10.1016/j.procs.2012.06.057

stored template and determines validity or authenticity based on this comparison. However, biometrics is not a panacea for security because it has some risks of being hacked, modified and reused during communication and transmission over insecure network channels. Hence, there is a strong need to protect biometrics during communication and transmission. The latest trend to protect biometric data is via chaotic encryption techniques [4, 5, 6, 7, 8, 9, 10]. Chaotic encryption techniques has many unique characteristics different from peers algorithms such as the sensitive dependence on initial conditions, non-periodicity, non-convergence and control parameters. These schemes provide a simple process of high complexity and mixing such that a small deviation in the local area cause a dramatic change in the whole space [11].

In this paper, a new chaotic encryption framework is proposed for palmprint data based on fractional wavelet packet transform (FrWPT), chaotic map and Hessenberg decomposition. This combination of fractional domain with chaos inherits the virtues of fractional domain and randomness to provide enhanced security. Further, this offers the transform orders as an extra key, in addition to the keys offered by any existing chaos based encryption technique. In the present work, we concentrated our efforts on the palmprint biometric. The palmprint biometric is selected because these are the recent advancement in the area of biometrics. A palmprint is covered with the same kind of skin as finger tips and is larger in size than a finger tip, hence it is quite natural to think of using palmprint to recognize a person rather than fingerprint. The palmprints have many unique features that can be used for personal identification. The principal lines, wrinkles, ridges, minutiae points, singular points, and texture are regarded as useful features for palmprint representation [12, 13]. Although the proposed encryption technique works efficiently for other biometric images, such as fingerprint, iris, face, signatures etc, but the visual results are given for palmprint images. The core idea of the proposed encryption framework is to decompose palmprint image by the means of FrWPT. Now, FrWPT coefficients are deformed using a reversible process based on Hessenberg decomposition and chaotic map followed by inverse fractional wavelet packet transform to get the encrypted palmprint image. The results of several experiments demonstrate that the proposed technique provides an efficient and secure way for palmprint image encryption and storage.

The rest of the paper is organized as follows: in Section 2, the preliminaries to the proposed work are illustrated followed by the thorough description of the proposed chaotic encryption technique in Section 3. The experimental setup, security analysis and the efficiency of the proposed technique are presented in section 4. Finally, the concluding remarks are given in section 5.

2. Preliminaries

This section gives the basic background, primarily the theory of fractional wavelet packet transform, Hessenberg decomposition and chaotic map on which we base our security solution. These are as follows.

2.1. Fractional Wavelet Packet Transform

The fractional wavelet packet transform (FrWPT) [14] of a 1D continuous function $f(t) \in L^2(\mathbb{R})$ is given by

$$W_\alpha(u, s, \tau) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(t) K_\alpha(t, x) e^{-jux} \psi_{s,\tau}(x) dt dx \tag{1}$$

where s and τ are the dilation (scale) and translation (position) parameters whereas α is the transform order (or angle) and $K_\alpha(t, x)$ is the transform kernel, given by.

$$K_\alpha(t, x) = \begin{cases} \sqrt{1 - i \cot \alpha}\ \exp\left(i \frac{t^2+x^2}{2} \cot \alpha - ixt \csc \alpha\right), & \alpha \neq n\pi \\ \delta(t - x), & \alpha = 2n\pi \\ \delta(t + x), & \alpha = 2n\pi \pm \pi \end{cases} \tag{2}$$

where n is a given integer. If the definition given in Eqn. 1 is observed than one can see that the FrWPT is the combination of the two well known transforms viz. fractional fourier transform (FrFT) and wavelet packet transform (WPT) which can be viewed as the fractional Fourier transform of a signal ($f(t)$) windowed

with a wavelet that is dilated by s and translated by τ. Therefore, FrWPT domain is the combination of time and frequency domains and depends on an angle α. Since, FrWPT is the combination of time and frequency domains hence if α close to $\pi/2$, for example $3\pi/4 \geq |\alpha| \geq \pi/4$, the FrWPT is dominant in the dual frequency (Fourier wavelet packet) domain whereas for small $\alpha(< \pi/4)$, the FrWPT is dominant in the single frequency (wavelet packet) domain. Further, due to separability, two dimensional transform can be obtained by successively taking one dimensional transforms along both the axis.

2.2. Hessenberg Decomposition

Hessenberg Decomposition [15] is the factorization of a general square matrix A by orthogonal similarity transformations into the form

$$A = QHQ^T \tag{3}$$

where Q is an orthogonal matrix and H is an upper Hessenberg matrix, meaning thereby $h_{ij} = 0$ whenever $i > j + 1$. Hessenberg decomposition is typically computed using Householder matrices. Householder matrix (P) is the orthogonal matrix of the form

$$P = I_n - 2uu^T/u^T u$$

where u is a non-zero vector in R^n and I_n is the $n \times n$ identity matrix. There are $n - 2$ steps in the overall procedure when A is of size $n \times n$. Therefore, Hessenberg decomposition is computed as

$$H = (P_1 P_2 ... P_{n-3} P_{n-2})^T A (P_1 P_2 ... P_{n-3} P_{n-2}) \Longrightarrow H = Q^T AQ \Longrightarrow A = QHQ^T \tag{4}$$

2.3. Piece-wise Linear Chaotic Map (PWLCM)

A piecewise linear chaotic map (PWLCM) is a 1D chaotic map composed of multiple linear segments. This map has better dynamical and statistical properties than a single segment chaotic maps [16]. Mathematically,

$$x(k+1) = C[x(k);\mu] = \begin{cases} \dfrac{x(k)}{\mu}, & \text{if } x(k) \in [0, \mu) \\ \dfrac{x(k) - \mu}{0.5 - \mu}, & \text{if } x(k) \in [\mu, 0.5) \\ C[1 - x(k);\mu], & \text{if } x(k) \in [0.5, 1) \end{cases} \tag{5}$$

where the positive real constant $\mu \in (0, 0.5)$ and $x(\cdot) \in (0, 1)$. This is a typical map with four line segments and was firstly introduced by Zhou. The PWLCM map possesses the numerous properties which can be considered as the motivation of considering the PWLCM map in the design of proposed module. These properties include [16],

- It is a non-invertible transformation of unit interval onto itself.
- It is ergodic, and has uniform invariant measure in [0, 1].
- It has a large key space and has no periodic windows in the chaotic region.
- It can be executed faster than some other existing maps.

3. Proposed Encryption Framework for Palmprint Data

In this section, some motivating factors in the design of proposed approach are discussed. The proposed algorithm uses a palmprint image and gives an encrypted palmprint image which is further transmitted/communicated through an insecure channel. Without loss of generality, assume that F represents the original fingerprint image of size $M \times N$. The proposed chaotic encryption framework for palmprint is depicted in figure 1 and is described as follows.

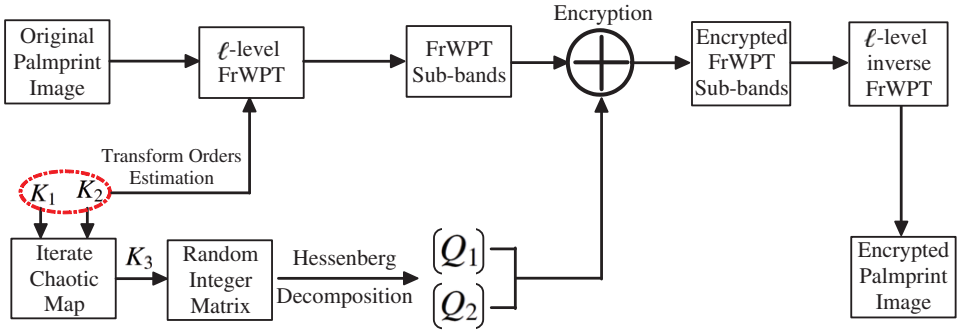


Fig. 1. Block diagram of proposed encryption framework for palmprint images.

3.1. Encryption Process

1. Based on the PWLCM map and adopting keys K_1 and K_2 as the initial values, to generate two different chaotic sequences $\mathcal{K}_i = \{0 < k(g_i) < 1 | \, 1 \le g_i \le L_i, \; i = 1, 2\}$, where L_i is the pre-defined length of the chaotic sequences. The final values of $\mathcal{K}_i$ are used as the transform orders for FrWPT.
2. Again based on the PWLCM map and adopting key K_3 as the initial value to generate a chaotic sequence $\mathcal{K}_3 = \{0 < k(h) < 1 | \, 1 \le h \le L_3\}$ such that $L_3 = m \times n$ where m, n are the dimensions of the f_n^θ.
3. Map $\mathcal{K}_3$ into an integer sequence $\widetilde{\mathcal{K}}_3$, such that every element lies in [0, 255], as follows

$$\text{if } \frac{j}{m \times n} \le \mathcal{K}_3(i) \le \frac{j+1}{m \times n}, \text{ then } \widetilde{\mathcal{K}}_3(i) = j \pmod{255} \tag{6}$$

4. The obtained chaotic sequence $\widetilde{\mathcal{K}}_3$ is arranged in the form of a matrix of dimension $m \times n$, which is denoted by P and termed as *matrix key*. This matrix key is further transformed into two matrices, say P_1 and P_2, of size $m \times m$ and $n \times n$ respectively, as

$$P_1 = PP^T \text{ and } P_1 = P^T P \tag{7}$$

5. Perform Hessenberg decomposition on the P_1 and P_2, which gives

$$P_1 = Q_1 \, H_1 \, Q_1^T \text{ and } P_1 = Q_2 \, H_2 \, Q_2^T \tag{8}$$

6. Perform ℓ-level $(\mathcal{K}_{L_1}, \mathcal{K}_{L_2})$ order FrWPT on F, which is denoted by f_n^θ, where $\theta \in \{\text{A,H,V,D}\}$ and n denotes the level.
7. Deform all coefficients of each sub-band using orthonormal matrices Q_1 and Q_2, as

$$f_n^{\theta,\, def} = \begin{cases} Q_1 f_n^\theta Q_2^T, & \text{if } m \le n \\ Q_2 f_n^\theta Q_1^T, & \text{if } m > n \end{cases} \tag{9}$$

8. Perform inverse ℓ-level $(\mathcal{K}_{L_1}, \mathcal{K}_{L_2})$ order FrWPT to get the encrypted palmprint image (say $\widetilde{F}$).

3.2. Decryption Process

1. By adopting keys K_1, K_2, K_3 and μ, **step 1** to **step 5** of encryption process are performed to get transform orders $(\mathcal{K}_{L_1}, \mathcal{K}_{L_2})$ and matrix key $\mathcal{K}$.
2. Perform ℓ-level $(\mathcal{K}_{L_1}, \mathcal{K}_{L_2})$ order FrWPT on $\widetilde{F}$, which is denoted by $\widetilde{f}_n^\theta$, where $\theta \in \{\text{A,H,V,D}\}$ and n denotes the level.
3. Perform inverse deformation on coefficients of every sub-band, as follows

$$\widetilde{f}_n^{\theta,\, def} = \begin{cases} \text{inv}(Q_1) \, \widetilde{f}_n^\theta \, \text{inv}(Q_2^T), & \text{if } m \le n \\ \text{inv}(Q_2) \, \widetilde{f}_n^\theta \, \text{inv}(Q_1^T), & \text{if } m > n \end{cases} = \begin{cases} Q_1^T \, \widetilde{f}_n^\theta \, Q_2, & \text{if } m \le n \\ Q_2^T \, \widetilde{f}_n^\theta \, Q_1, & \text{if } m > n \end{cases} \tag{10}$$

4. Perform inverse ℓ-level $(\mathcal{K}_{L_1}, \mathcal{K}_{L_2})$ order FrWPT on $\widetilde{f}_n^{\theta,\, def}$, to get the decrypted palmprint image.

4. Results and Discussions

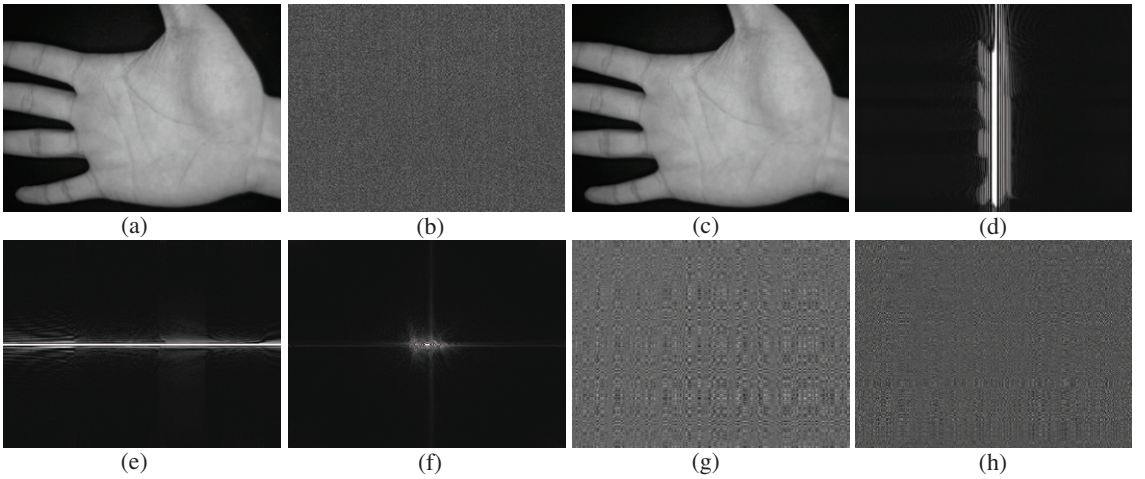
The robustness and validity of the proposed scheme are demonstrated using MATLAB platform. Different palmprint images are used as experimental images in our experiments. The palmprint images are acquired from the CASIA-Palmprint database (downloaded from `http://www.cbsr.ia.ac.cn/english/Palmprint%20Databases.asp`), which contains 5502 palmprint images captured from both left and right palms of 312 subjects. The initial values for PWNLCM are considered to be $K_1 = 0.0546$, $K_2 = 0.9985$ whereas the values of μ are taken to be 0.3, 0.1 with the lengths $L_1 = 800$, $L_2 = 600$. The final value of the first sequence i.e. sequence obtained with parameters $K_1 = 0.0546$, $\mu = 0.3$ and $L_1 = 800$ is used as the transform order along x-axis whereas the final value of the second sequence is used as the transform order along y-axis. The matrix key is generated by filling the elements of chaotic sequence with initial parameters as $K_3 = 0.6328$ and $\mu = 0.42$ in an array row wise. The size of matrix key is equal to the size of FrWPT sub-bands therefore L_2 is fixed to be $m \times n$. In the proposed method, values K_1, K_2, K_3, μ and L_1, L_2, L_3 play a vital role of keys. Since, without knowing these values, transform orders and matrix key cannot be generated and hence, no intruder can decompose the image in the correct domain, resulting in less possibility of decrypting the image. Figure 2 shows the original palmprint, encrypted palmprint, decrypted palmprint images with correct and wrong keys respectively. Figure 2(c) shows the decrypted palmprint image with all correct keys. Figures 2(d)–(h) show the results when only K_1, only K_2, both K_1 and K_2, only K_3 and all of the above keys are wrong. In all of the above mentioned cases, decryption is not done perfectly. Hence, the proposed scheme is highly sensitive to its keys.

Security is the main thrust of the encryption techniques. Some security analysis has been performed on the proposed encryption technique which includes key space, edge distortion, randomness, statistical (histogram and correlation) and numerical analysis. The security analysis for the proposed technique are discussed as follows.

4.1. Key Space Analysis

The information system should be secure even if everything about the system, except the key, is publicly available. Hence, the keys play a very vital role in the security of information system. According to the principle, the key space should be large enough for a good encryption scheme. In the proposed technique, four keys ($K_i | \ i = 1, 2, 3$ and μ) are used as the initial value of PWNLCM. Here, the key space is calculated for only one key K_1 as:

Generate two different sequence $\mathcal{K}_1$ and $\widetilde{\mathcal{K}_1}$ by using K_1 and $K_1 + d$ as initial values and a pre-defined length L_1 i.e. $\mathcal{K}_1 = \{0 < k(g) < 1 | \ 1 \le g \le L_1\}$ and $\widetilde{\mathcal{K}_1} = \{0 < \widetilde{k}(g) < 1 | \ 1 \le g \le L_1\}$. Now, the key space is



(a) (b) (c) (d)

(e) (f) (g) (h)

Fig. 2. a) Original palmprint image b) Encrypted palmprint image; Decrypted palmprint image with c) correct keys d) wrong key K_1 e) wrong key K_2 f) wrong keys K_1 and K_2 g) wrong key K_3 h) all wrong keys.

calculated by the mean absolute error between two generated sequences i.e.

$$MAE(\mathcal{K}_1, \widetilde{\mathcal{K}}_1) = \frac{1}{L_1} \sum_{g=1}^{L_1} |k(g) - \widetilde{k}(g)| \tag{11}$$

The key space for K_1 is equal to $1/d_0$, where d_0 is the value of d for which $MAE = 0$. After simulations, the value of d_0 comes out to be $1.0256 \times 10^{-21} \approx 10^{-21}$. Similarly, the key spaces for other keys can be computed. After simulations, the total key space of whole framework comes out to be 10^{84} which is enough large key space and ensures the high security of the proposed system.

4.2. Edge Distortion Analysis

Edges are the most common features within an image. They are local variations in the image function. Typically, edges reflect the inherent properties to the objects (such as surface markings and surface shape) and the geometry of the scene. For a good encryption technique, these properties might not have revealed from their encrypted counterparts. For this purpose, the edge distortion analysis is evaluated using edge distortion ratio (EDR), which usually reelects the deviation in the edges. Let f and g denote original and corresponding encrypted images with their respective edge binary matrix B_f and B_g. The mathematical definition of EDR is given as follows.

$$EDR = \frac{\sum_{i=1}^{M} \sum_{i=1}^{N} \left| B_f(i,j) - B_g(i,j) \right|}{\sum_{i=1}^{M} \sum_{i=1}^{N} \left(B_f(i,j) + B_f(i,j) \right)} \times 100\% \tag{12}$$

Here, the edge binary matrix can be obtained using standard edge detection methods such as Sobel, Prewitt, Canny detector, etc. In our experiments, Canny edge detector is used due to its better performance [17]. Higher values of EDR are required for a good encryption technique. The value of EDR for palmprint image comes out to be 99.78%, which reflects that more than 99% of the edges in the original palmprint image is displaced from their positions in encrypted image. Hence, the inherent properties and geometry of palmprint image cannot be revealed from the proposed encryption framework.

4.3. Randomness Analysis: Information Entropy Analysis

The entropy is considered amongst the most important features of randomness. The information entropy $H(s)$ of a source s with 2^N symbols s_i is defined as

$$H(s) = -\sum_{i=1}^{2^N-1} \mathbb{P}(s_i) \log_2 \mathbb{P}(s_i) \tag{13}$$

where $\mathbb{P}$ denotes the probability of the symbol s_i being emitted from s. If s is a truly random source and $\mathbb{P}(s_i) = 2^{-N}$, $\forall i$ then $H(s) = 2^N 2^{-N} \log_2 2^N = N$. Therefore, information entropy must be 8 for a random source emitting 256 symbols. For the encrypted palmprint image, the information entropy comes out to be 7.9994, which is very close to the ideal value of 8. This means that the encrypted palmprint image is close to a random source and hence the proposed algorithm is secure against the entropy attack.

4.4. Statistical Analysis

Another method to evaluate encryption technique is statistical analysis. This analysis is composed of two terms viz. 1) Histogram analysis 2) Correlation analysis. According to first term, for a good encryption technique, there is uniform change in the image histogram after encryption. Figure 3(a,b) show the histograms of both original and encrypted images. From figures, it is clear that after encryption histogram becomes uniform and therefore none can judge the pixel distribution which further resists information leakage. The second term says that a good encryption technique must break the correlation among the adjacent

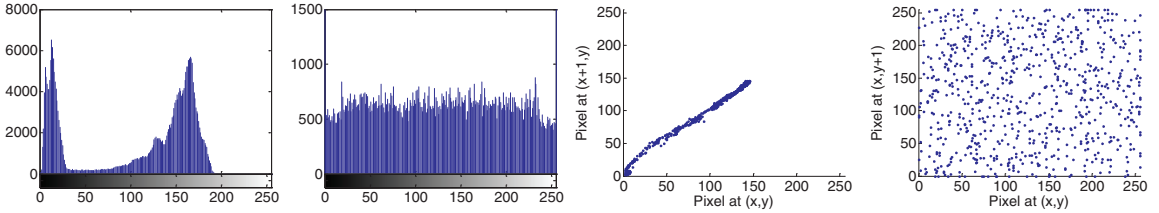


Fig. 3. Histogram of a) Original palmprint b) Encrypted palmprint images; Correlation distribution of two horizontally adjacent pixels in the c) Original palmprint b) Encrypted palmprint images.

Table 1. Correlation coefficients of two adjacent pixels in original and encrypted palmprint image.

Direction	Correlation in	
	Original Image	Encrypted Image
Horizontal	0.9979	0.0069
Vertical	0.9986	0.0065
Diagonal	0.9999	-0.0454

Table 2. Numerical analysis of proposed technique.

Metric	Between Original and	
	Encrypted Image	Decrypted Image
PSNR	6.3564	241.7319
SD	375.0985	1.9035×10^{-12}
UIQ	0.0005	1
SSIM	0.0001	1

pixels of the image. For this purpose, the correlation between two adjacent pixels are calculated and it is said to be good encryption if correlation come to be as far as from 1. First, randomly select $\mathcal{P}$ pairs of adjacent pixels (either in horizontally or vertically or diagonally) and then calculate their correlation as

$$r_{x,y} = \frac{E(x - E(x))(y - E(y))}{\sqrt{E(x^2) - (E(x))^2}\ \sqrt{E(y^2) - (E(y))^2}} \tag{14}$$

where x and y are the gray levels of two adjacent pixels in the image and $E()$ denotes the expected (mean) value. Figures 3(c,d) show the correlation distribution of two horizontally adjacent pixels in the original and encrypted image. The correlation coefficients in all directions are shown in table 1, which are far apart. Therefore, proposed technique is able to break the high correlation among the pixels and hence proposed framework is robust against statistical attacks.

4.5. Numerical Analysis

Numerical analysis is the process of evaluating an encryption technique via some objective metrics. For this purpose, Peak Signal to Noise Ratio (PSNR), Spectral Distortion (SD), Universal Image Quality Index (UIQ) and Structural Similarity Index Measure (SSIM) are used as quality metrics. PSNR and SD reflect the similarity in spectral information whereas UIQ and SSIM reflect the similarity in structural information. The mathematical definitions of objective metrics can be found in [18]. In principle, the lower value of SD whereas higher values of PSNR, UIQ and SSIM indicates the better similarity. Since, the dynamical range for UIQ and SSIM is [0, 1] therefore, higher values can be interpreted as the values close to 1. Therefore, for an efficient encryption(decryption) process, SD must be higher(lower) whereas another metrics must be lower(higher). The values of objective metrics between original-encrypted and original-decrypted palmprint images are depicted in table 2 with correct keys. From the table, clearly the values of objective metrics are higher/lower according to their definition. Therefore, the proposed technique is able to encrypt and decrypt the biometrics images perfectly.

5. Conclusions

In this paper, a simple yet efficient security solution for palmprint data is proposed, which uses fractional wavelet packet transform, chaotic map and Hessenberg decomposition. To increase the security of the scheme, piece-wise linear chaotic map is used to give randomness to the process in the form of keys to

FrWPT as transform orders. The efficiency of the proposed solution is carried out by the detailed discussion of key sensitivity, key space analysis, edge distortion analysis, randomness analysis, statistical analysis and numerical analysis. These analysis demonstrates the high security of the proposed palmprint encryption framework.

Acknowledgements

This work was supported in part by the Canada Chair Research Program and the Natural Sciences and Engineering Research Council of Canada.

References

[1] D. Maltoni, D. Maio, A.K. Jain and S. Prabhakar, Handbook of Fingerprint Recognition, *Springer Verlag, Berlin*, Germany, 2003.
[2] N.K. Ratha, J. Connell and R. Bolle, Enhancing security and privacy in biometrics-based authentication systems, *IBM System Journal*, 40, 2001, pp. 614–634.
[3] U. Uludag, S. Pankanti and S. Prabhakar, Biometric cryptosystems: issues and challenges, *Proc. of IEEE*, 92, 2004, pp. 948–960.
[4] D. Moon, Y. Chung, S.B. Pan, K. Moon and K.I. Chung, An efficient selective encryption of fingerprint images for embedded processors, *ETRI Journal*, 28, 2006, pp. 444–452.
[5] F. Han, J. Hu, X. Yu and Y. Wang, Fingerprint images encryption via multi-scroll chaotic attractors, *Applied Mathematics and Computation*, 185, 2007, pp. 931–939.
[6] L. Chen and D. Zhao, Image encryption with fractional wavelet packet method, *Optik-International Journal for Light and Electron Optics*, 119(6), 2008, pp. 286–291.
[7] M.K. Khan, J. Zhang and K. Alghathbar, Challenge-response-based biometric image scrambling for secure personal identification, *Future Generation Computer Systems*, 27(4), 2011, pp. 411–418.
[8] G. Bhatnagar, Q.M.J. Wu and B. Raman, Fractional dual tree complex wavelet transform and its application to biometric security during communication and transmission, *Future Generation Computer Systems*, 28(1), 2012, pp. 254–267.
[9] G. Bhatnagar and Q.M.J. Wu, Security Solution for Fingerprint Data During Communication and Transmission, *IEEE Transactions on Instrumentation and Measurement*, 61(4), 2012, pp. 876–887.
[10] G. Bhatnagar, Q.M.J. Wu and B. Raman, A new Fractional Random Wavelet Transform for Fingerprint Security, *IEEE Transactions on SMC Part-A*, 42(1), 2012, pp. 262-275.
[11] Y. Mao and G. Chen, Chaos-Based Image Encryption, *Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neurocomputing and Robotics, Springer-Verlag*, Berlin, 2003, pp. 231–265.
[12] D. Zhang, W. Kong, J. You and M. Wong, Online Palmprint Identification, IEEE Transactions on Pattern Analysis and Machine Intelligence, 25(9), 2003, pp. 1041–1050.
[13] J. Chen and Y. Moon, Using SIFT features in palmprint authentication, *Proc. Int. Conf. on Pattern Recognition*, 2008, pp. 1–4.
[14] Y. Huang and B.Suter, The Fractional Wave Packet Transform, *Multidimensional Systems and Signal Processing*, 9(4), 1998, pp. 399–402.
[15] G.H. Golub and C.F.V. Loan, Matrix computations, *Johns Hopkins University Press*, 1996.
[16] H. Zhou, A design methodology of chaotic stream ciphers and the realization problems in finite precision, *Ph.D. thesis*, Department of Electrical Engineering, Fudan University, Shanghai, China, 1996.
[17] R. Deriche, Using Canny's criteria to derive a recursively implemented optimal edge detector, *International Journal Computer Vision*, 1, 1987, pp. 167–187.
[18] Z. Wang and A.C. Bovik, Modern Image Quality Assessment, Synthesis Lectures on Image, Video & Multimedia Processing, *Morgan & Claypool Publishers*, 2006.