IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)
Volume 4, Issue 6, Ver. II (Nov - Dec. 2014), PP 32-46
e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197
www.iosrjournals.org

Nonlinear chaos - based security solution for fingerprint data during communication

Hema Ousephachan
(M. Tech student , Electronics and communication engineering department,
Federal institute of science and technology(FISAT), Angamaly, India)

Abstract: *Protecting privacy for exchanging information through the media has been a topic researched by many people. This work presents a security solution for transmitting fingerprint images over insecure channels. Here security is provided by an encryption technique based on reversible hidden transform (RHT), fractional wavelet packet transform (FrWPT), chaotic map and singular value decomposition (SVD). This scheme proposes the use of coupled two-dimensional piecewise nonlinear chaotic map (CTPNCM) for selecting the transform order of FrWPT. And here the inputs to this chaotic map act as the secret keys. By architecture itself this nonlinear chaotic map provides more security to the encryption scheme than the linear ones.*

Keywords: *Biometrics, fingerprint protection, fractional wavelet packet transform (FrWPT), coupled two-dimensional piecewise nonlinear chaotic map (CTPNCM), reversible hidden transform (RHT), singular value decomposition (SVD).*

I. Introduction

Bio-cryptography is emerging as a powerful solution for secret communication, which can combine the advantages of conventional cryptography and biometric security. A biometric is defined as a unique, measurable, biological characteristic or trait for automatically verifying or recognizing the identity of a human being. These days, biometric technologies are typically used to analyze human characteristics for security purposes. Biometrics like fingerprint, irises and DNA are permanent characteristics and unique identifiers of the individuals. Among these, fingerprints are the most widely used one. So while exchanging these information over internet or other open networks, security is more important. Because they are used in many fields like physical and logical access controls, attendance recording, payment systems, crime and fraud prevention and border security controls. So it is necessary to encrypt them while exchanging over open networks.

This work presents a security solution for transmitting fingerprint images over insecure channels. Here security is provided by an encryption technique based on reversible hidden transform (RHT), fractional wavelet packet transform (FrWPT), chaotic map and singular value decomposition (SVD). In this scheme the first step is the application of RHT algorithm for changing the gray values in the spatial domain of the fingerprint image. Next step is the application of FrWPT and deformation of its coefficients by using SVD and chaotic map. Then inverse FrWPT is performed to get the encrypted fingerprint image. So in this encryption scheme security lies in both spatial and frequency domains.

The transform order for FrWPT is generated by using chaotic maps. In this work two type of chaotic maps are compared, piece-wise linear chaotic map (PWLCM) and coupled two-dimensional piecewise nonlinear chaotic map (CTPNCM). And this work proposes the use of second map, because by architecture itself it is clear that the second map provides more security to this scheme.

At the decryption side, the reverse steps are needed to reconstruct the original fingerprint image. Finally, analyses like histogram analysis, numerical analysis and parameters like Key sensitivity, original fingerprint image sensitivity (OFIS) and time efficiency demonstrate the efficiency and robustness of this scheme.

This paper is organized as follows: In Chapter 2, literature survey details are given followed by the description of basic theory of schemes used in the encryption scheme in Chapter 3. The methodology of the encryption technique is thoroughly described in Chapter 4. The experimental setup, security analysis, and the efficiency of the technique are presented in Chapter 5. Finally, the concluding remarks are given in Chapter 6.

II. Literature Survey

In 2012 Gaurav Bhatnagar presented a security solution for fingerprint data [1]. In this scheme, as a first step the gray values in the special domain of input image is changed using reversible hidden transform (RHT), followed by the Fractional wavelet packet transform coefficients are deformed by singular value decomposition and chaotic map. In this work chaotic sequences are used to add more security and randomness to the encryption scheme. This is because of their special properties like pseudo randomness, ergodicity and great sensitivity to initial conditions. Here PWLCM is used, because this map has better balance property and has no black window in chaotic regions.

In today's modern world fast, accurate and secure transaction of data has great importance. Most of these activities occur through internet. While exchanging information over internet, security is very important as speed and integrity. For this reason encryption techniques were introduced and it has been a topic of research by many people.

In past, verified users have gained access to secure information systems, offices or equipments via multiple personal identification numbers, passwords, and unique identification cards and so on. These keys can be lost, stolen or forgotten. Most passwords are so simple and short, so they can be easily identified or broken by simple methods. Simple passwords are easy to crack and, thus, they compromise security. Complex passwords are difficult to remember, so users generally have the tendency to write down these passwords in easily accessible locations. Further, most people use the same password across different applications and, thus, if a single password is compromised, it may open many doors. Many of these limitations of the traditional passwords can be overcome by incorporation of better methods of user authentication. Nowadays biometric data (like fingerprints, DNA, irises etc) has been gaining great interest in these fields. Because, these information are the permanent characteristics and unique identifiers of an individual. Bio-cryptography is emerging as a powerful solution for security, which can combine the advantages of conventional cryptography and biometric security.

In 2004, U. Uludag, S. Prankati and S. Prabhakar presented a paper regarding issues and challenges of biometric cryptosystems [2]. In this work they compared different biometric technologies. Among all the biometrics, fingerprints are the oldest and widely used one in personal verification, because fingerprints are believed to be unique for individuals and across different fingers of the same individual. Even identical twins having similar DNA are believed to have different fingerprints. So security of fingerprint data is more evident than any other information.

In 1997 Anil Jain, Lin Hong, S. Pankanti and R. Bolle presented an identity authentication system using fingerprints [3]. They have developed an alignment based minutiae matching algorithm. In this work they compared different biometric techniques and proved that fingerprint verification is the most suitable biometric technique for personal identification. This conclusion is made by analyzing parameters like universality, uniqueness, permanence, collectability, acceptability etc.

In 1996 Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone have written a book namely Handbook of applied cryptography [4]. It explained some classical encryption techniques such as Advanced Encryption Standard, Rivest–Shamir–Adleman algorithm, Data Encryption Standard (DES), or International Data Encryption Algorithm. However, due to some intrinsic features of the biometrics images, such as bulk data capacity and high correlation among pixels, these classical encryption algorithms are not suitable for practical applications.

In 2006, D. Moon, Y. Chung, S. B. Pan, K. Moon, and K. I. Chung presented a secure and efficient protocol to transmit fingerprint images from a fingerprint sensor to a client [5]. This is done with the help of a standard encryption algorithm. In this scheme they select the least significant bit (LSB) of each pixel in the fingerprint image (called an LSB bit-plane) as random noise and take the exclusive-OR of the LSB bit-plane and all the pixels of the input fingerprint image. In this scheme, an opponent cannot recover the original fingerprint image without knowledge of the LSB bit-plane, and they also encrypt the LSB bit-plane by using a shared session key. As the sensor and client share the same session key, the client can recover the original fingerprint image by decrypting the encrypted LSB bit-plane and by then applying the same exclusive-OR operation. But this is a simple spatial domain technique.

In 2002 C. Ashok Narayan and K.M.M Prabhu presented a study regarding theory, implementation and error analysis of the fractional Fourier transform (FrFT) [6]. In this study they explained FrFT as a generalization of ordinary Fourier transform with an additional parameter α (order parameter). This FrFT becomes equal to Fourier transform if this order parameter becomes $\frac{\pi}{2}$. In this paper they discussed about the definition and properties of FrFT. And they also presented an algorithm for computing the discrete FrFT.

Using the concept of fractional Fourier transform with Eigen vector decomposition algorithm, Deepak Sharma, Rajiv Saxena and Ashutosh Rajput presented a robust image encryption scheme [7]. In this scheme DFrFT was used with the double random phase encoding. In this encryption scheme input image is first multiplied with a exponential random matrix, after that the DFrFT of order 'α' is applied and then the resulting matrix is multiplied by a second exponential random matrix, and again DFrFT of order 'β' is applied. Here the security is provided by combination of the DFrFT order and random phase matrix. But here encryption is performed only in frequency domain, so security lies only in frequency domain.

In 1998 M.S Baptista presented the idea of cryptography with chaos [8]. In this he used a simple one-dimensional logistic map equation to encrypt text. Here each character of the message is encrypted as an integer number of iterations performed in the logistic equation. This 1-D chaos system has merits of simplicity and high security. This scheme has some drawbacks also. The main drawback is the poor balance property (non-uniformity). The second one is the existence of black windows in the chaotic region.

The use of chaotic sequences is a new trend in image encryption. In 2011, Abhishek misra, Ashutosh Gupta and Damodar Rai analyzed the parameters of chaos based image encryption schemes [9]. They stated that chaotic encryption algorithms have some advantages over traditional algorithms like high sensitivity, speed, reasonable computational overheads etc. And this analysis provides a comparison between different chaotic image encryption schemes. From this study it is clear that piece-wise linear chaotic map (PWLCM) is better than logistic map. Nowadays, these sequences are also used in image encryption.

In 1996 Ying Huang and Bruce Suter presented the concept of Fractional wavelet packet transform (FrWPT) based on the idea of FrFT and wavelet packet transform (WPT) [10]. This FrWPT exhibits multi-resolution property and describes the spatial and frequency domain information. Here the first one is the unique property of WPT and second one is the property of FrFT.

In 2008 L. Chen and D. Zhao introduced a chaos based method to encrypt images using Fractional wavelet packet transform (FrWPT) [11], here fractional order of FrWPT is used as the key. FrWPT is the realization of wavelet packet transform (WPT) in fractional domain. It is powerful than FrFT because of random distribution of information due to fractional Fourier plane. This scheme is also a frequency domain encryption scheme. This paper has an advantage to achieve data confidentiality. And it has a drawback of limited key space and limited perceptual quality. 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 after encryption we will get any glimpse of the original image.

Using the concept of FrWPT and chaotic map, in 2012 Gaurav Bhatnagar presented a security solution for fingerprint data as discussed above.

In 2012, Seyed Mohammad Seyedzadeh and Sattar Mirzakuchaki proposed a new encryption algorithm [12] for color images using coupled two-dimensional piecewise nonlinear chaotic map, called CTPNCM. This map has nonlinear property, coupled structure and more number of initial parameters. Therefore it can enhance the security and sensitivity of the cryptosystem. And this scheme can overcome the drawbacks of small key space and weak security in the widely used one-dimensional logistic systems.

In this work, security solution during communication and transmission of fingerprint data is provided in the form of an encryption technique based on reversible hidden transform (RHT), fractional wavelet packet transform (FrWPT), singular value decomposition and chaotic map. The initial step of this scheme is to transform the original fingerprint image using the RHT. Then, the transformed fingerprint image is decomposed into various sub-bands using FrWPT and here transform orders in x axis and y axis are selected using coupled two-dimensional piecewise nonlinear chaotic map (CTPNCM). Now, each sub-band is deformed by SVD and chaotic map. Then inverse FrWPT is applied to get the encrypted fingerprint image. This deformation is chosen in such a way that the reverse deformation exists and can be used at the receiver to decrypt the image. Due to the application of RHT and FrWPT, here security solution relies on both in spatial and frequency domains. At the decryption/receiver end, the reverse process is done to decrypt the image.

III. Basic Theory Of The Encryption Scheme

Many disadvantages and limitations of the traditional passwords can be overcome by using better user authentication methods. Biometric authentication methods have been gaining great interest in these areas. In these methods, physiological and behavioral characteristics of individuals like face, fingerprint, hand geometry, iris, keystroke, signature, voice, etc are used for user verification. These methods are secure and better than traditional password-based authentication, because these biometric characteristics cannot be lost, stolen or forgotten (passwords may lost or forgotten). Biometric characteristics are extremely difficult to copy, share, and distribute and require the presence of the person being authenticated at the time and point of authentication. It is difficult to forge biometrics because this type of authentication requires more time, money, experience, and access privileges. Finally, one user's biometrics is no easier to break than another's; that is, biometrics of all users has relatively equal security level. Thus, biometrics-based authentication is a good one to replace password-based authentication methods.

Biometrics are permanent characteristics and unique identifiers of the individuals (like face, fingerprint, hand geometry, iris, keystroke, signature, voice, etc). Fig 3.1 shows examples of some biometric characteristics. Any individuals, physiological or behavioral characteristic can be used for personal identification. But it required satisfying the following requirements:

1. Universality : Every person should have the characteristic
2. Uniqueness : No two persons should have the same characteristic
3. Permanence : The characteristic should not vary with time and place
4. Collectability : It should be easy to collect the characteristic

5. Performance : The characteristic should have acceptable identification accuracy, and the working or environmental factors should not affect the identification accuracy
6. Acceptability : People should willing to accept the biometric system
7. Circumvention : It should be difficult to fool the system by fraudulent techniques

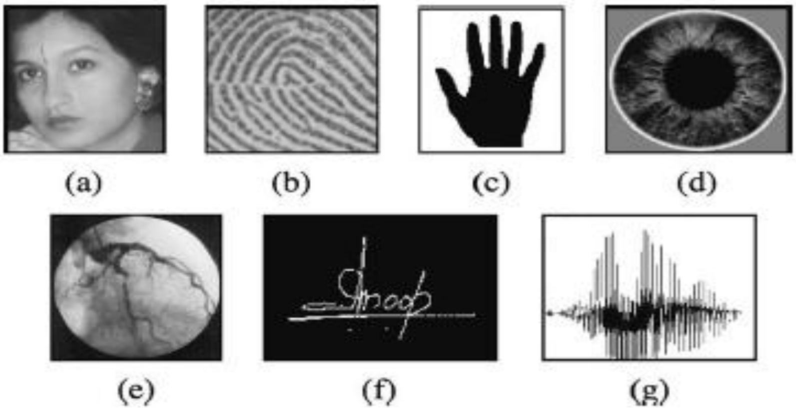


Figure 3.1: Examples of biometric characteristics (a) Face (b) Fingerprint (c) Hand geometry (d) Iris (e) Retina (f) Signature (g) Voice

Biometrics is a rapidly developing technology which has been widely used in many applications. Some of them are listed below:
1. Banking : Used to provide security in areas such as electronic fund transfers, ATM, check cashing, and credit card transactions.
2. Physical access control : Can be used for physical access control such as airport access control.
3. Information system security : Used to protect databases via login privileges.
4. Government benefits : Biometrics can be used for distribution of government benefits.
5. Customs and immigration : Biometrics can be used to check the authentication of individuals and makes immigration procedures faster.
6. National ID systems : Which provide a unique ID to the citizens and integrate different government services.
7. Voter and driver registration : Provides registration facilities for voters and drivers.
8. Forensics : Biometrics can be used for criminal identification and prison security.

Some of the important biometric techniques under investigation are face, fingerprint, hand geometry, hand vein, iris, retinal pattern, signature, voice-print, and facial thermo-grams. A brief comparison of these nine biometric techniques is provided in Table 3.1. From this it is evident that fingerprints are the most suitable method for personal identification.

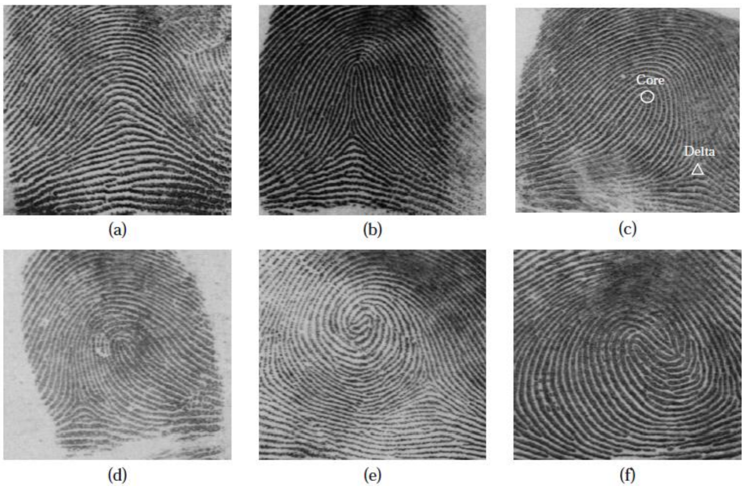


Figure 3.2 : Fingerprints and a fingerprint classification schema of six categories: (a) arch, (b) tented arch, (c) right loop, (d) left loop, (e) whorl, and (f) twin loop; critical points in a fingerprint, called core and delta, are marked on one of these images (c).

Security of these data is also very important. This work presents an encryption scheme for protecting fingerprint images. In this section, the steps in the design of this encryption scheme are discussed. It is based on reversible hidden transform (RHT), fractional wavelet packet transform (FrWPT), chaotic map and singular value decomposition (SVD).

Table 3.1 : Comparison of Biometric technologies

Biometrics	Univers-ality	Unique-Ness	Perma-Nence	Collecta-bility	Perfor-mance	Accept-Ability	Circum-vention
Face	High	Low	Medium	High	Low	High	Low
Fingerprint	Medium	High	High	Medium	High	Medium	High
Hand Geometry	Medium	medium	Medium	High	Medium	Medium	Medium
Hand Vein	Medium	Medium	Medium	Medium	Medium	Medium	High
Iris	High	High	High	Medium	High	Low	High
Retinal Scan	High	High	Medium	Low	High	Low	High
Signature	Low	Low	Low	High	Low	High	Low
Voice Print	Medium	Low	Low	Medium	Low	High	Low
F.Thermograms	High	High	Low	High	Medium	High	High

The first step is the application of RHT algorithm; it is used for shuffling the fingerprint image in the spatial domain. Then this shuffled image is decomposed into several sub-bands by using FrWPT. They coefficients of each sub-band is deformed using a matrix key, which is generated using piecewise linear chaotic map (PWLCM). Here deformation is done by SVD. After that inverse FrWPT is applied to get encrypted fingerprint image. At the decryption side, the reverse steps are needed to reconstruct the original fingerprint image. Next sections will explain each of these steps in detail.

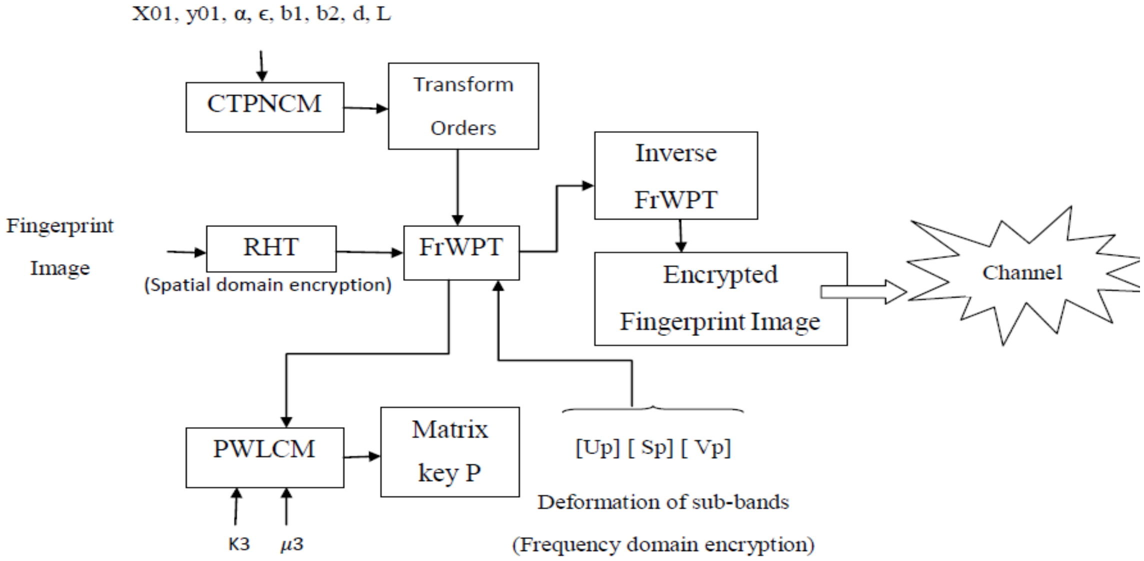


Figure 3.3 Block diagram of the encryption scheme

3.1 Reversible Hidden Transform (RHT)

As given in the block diagram (Fig 3.3), application of RHT is the first step in this encryption scheme. It is a simple integer transform that transforms an integer pair to another integer pair at considerably lower mathematical complexity based on some secret parameters.

Consider that [0 , L] is the image gray level range (where L=255 for 8 bit gray level images). To apply this algorithm, first image is partitioned into pair of pixels. Let (x1 , x2) be a pair of pixels in the fingerprint image and (α , β) be two fixed numbers. The forward transform is given as:

$$T : [0 , L] \times [0 , L] \longrightarrow [0 , L] \times [0 , L]$$

$$y = T(x) \qquad (3.1)$$

where y = (y1 , y2) is the transformed pair of pixels. And the values of y1 and y2 are given by the equations

$$y1 = \alpha\, x1 + \beta\, x2$$
$$y2 = \beta\, x1 + \alpha\, x2 \qquad (3.2)$$

since both x1 and x2 lie between [0, L], there may be a situation of underflow (y1 < 0 or y2 < 0 or both) or overflow (y1 > 0 or y2 > 0 or both). In order to avoid underflow and overflow of the transformed pixels, the following conditions should be satisfied:

$$0 \le y1 \le L; \;\; 0 \le y2 \le L. \tag{3.3}$$

This is possible only when α and β satisfy the relation

$$\alpha + \beta = 1 \text{ and } 0 \le \alpha, \beta \le 1. \tag{3.4}$$

After posing these constraints, the transform becomes simple because the secret parameter reduces to one, i.e., either α or β.

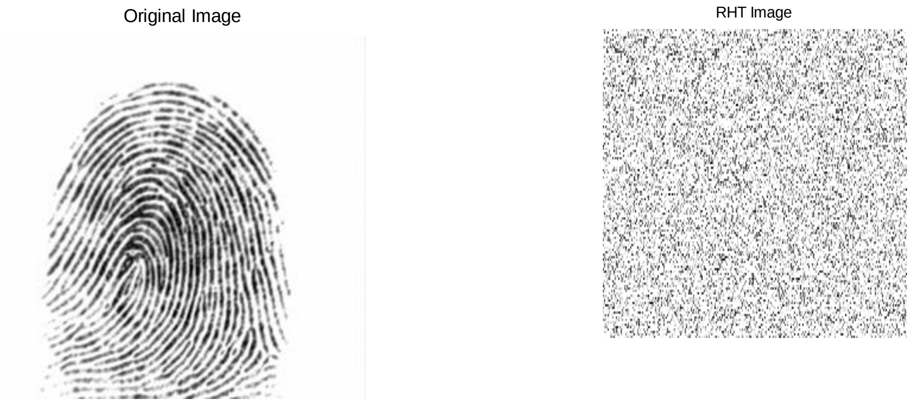
Finally, the inverse transform is:

$$T^{-1}: \; [0, L] \times [0, L] \longrightarrow [0, L] \times [0, L] \tag{3.5}$$

x = T ⁻¹(y) where x = (x1 ,x2) is the reconstructed pair of pixels, and their values are given by

$$x1 = \frac{\alpha y1 - \beta y2}{\alpha^2 - \beta^2} \quad ; \quad x2 = \frac{\beta y1 + \alpha y2}{\beta^2 - \alpha^2} \tag{3.6}$$

In the beginning, it is said that RHT is used to transform an integer into integer, but in some cases, a fractional part is obtained in the transformed pair of pixels. Hence, to avoid this, floor function is taken on the transformed value. If the forward transform uses floor function, then in the inverse transform, ceiling function is used and vice versa.



(a) (b)

Figure 3.4 : Reversible hidden transform (a) Original fingerprint image and (b) it's RHT image

3.2 PWLCM And CTPNCM

Next step in this encryption scheme is the application of FrWPT. The FrWPT is highly sensitive to the transform order. So here the transform order is used as the secret key. Therefore, without knowing correct values of transform order, no one can obtain a correct transformed domain and hence cannot decrypt the image. For choosing them this proposed scheme uses CTPNCM (Coupled two dimensional piecewise nonlinear chaotic map. It is a nonlinear chaotic map. Before discussing more details about this map, it is required to know other simple chaotic maps.

3.2.1 PWLCM

Chaos theory is one of the youngest of the sciences and most fascinating research areas in existence. Chaos theory is an aperiodic dynamic process represented in the form of maps, so it is also called as chaotic maps. The sequences produced by such functions have very good random nature and complexity. These functions have an extreme sensitiveness to initial conditions. The most attractive features of chaotic maps are its extreme sensitivity to initial conditions, random noise-like behavior, the outspreading of orbits over the entire space, etc. The simplest chaotic maps are 1-D maps that have the advantages of high-level efficiency and implicit nature.

The 1-D chaotic map can expressed as, C : U → U, where U ⊂ R generates a sequence of real numbers

$$X(n+1) = C[x(n) ; \mu] , \; x(n) \in U , \; \mu \in R \tag{3.7}$$

where n = 0, 1, 2, . . . denotes map iterations, and the coefficient μ is called the control parameter that controls the dynamic behavior of the chaotic map. Here this parameter is fixed, i.e, it is not affected by the iteration. The value x(0) is called the initial state or seed value of the generated sequence / orbit { x(n) : n = 1, 2, . . }.

One of the simplest 1-D chaotic maps is the logistic map that describes population growth over time by a recurrence relation described by

$$x(k+1) = C[x(k) ; \mu] = \mu \, x(k) \, [1 - x(k)] \tag{3.8}$$

where k = 1, 2, . . . , n, $0 \leq \mu \leq 4$. For the highly chaotic state, μ must be greater than 3.36995. Here also the control parameter is constant throughout each iteration. Logistic map is well studied and is widely used as a classical chaotic map nowadays. This map is very simple and deterministic but has very complicated dynamical behavior. Still, the logistic map has some performance drawbacks. The major drawback of the map is poor balance property (or non-uniformity). The second drawback is the existence of blank windows in the chaotic region. These windows are not relevant to the choice of the initial state, i.e., these windows always exist whatever be the initial state. Hence, some other chaotic map with better balance property and without blank windows in chaotic regions must be explored in order to enhance the security.

PWLCM is a different map with better properties than the logistic map. This map is composed of multiple line segments and has better dynamical and statistical properties than the logistic map. Mathematically it is expressed as:

$$x\,(k+1) = C\,[x(k)\,;\,\mu] = \begin{cases} \dfrac{x(k)}{\mu} & ,\text{if } x(k) \in [0\,,\,\mu) \\ \dfrac{x(k)-\mu}{0.5-\mu} & ,\text{if } x(k) \in [\mu\,,\;0.5) \\ C\,[\,1\text{-}\,x(k)\,;\,\mu] & ,\text{ if } x(k) \in [0.5\,,\;1) \end{cases} \qquad (3.9)$$

Where the positive real constant $\mu \in (0,\ 0.5)$ and $x(.) \in (0,\ 1)$. This is a typical map with four line segments. This map is comparatively better than the well known logistic map. The comparison is made with respect to the chaotic state of the maps. For this purpose, Lyapunov exponents and bifurcation are considered. Lyapunov exponents are the measure of the rate at which nearby orbits converge or diverge. Generally, a positive Lyapunov exponent is a signature of chaos.

Bifurcation diagram displays the qualitative information about equilibrium of the map. The Lyapunov exponents for both the maps are depicted in Fig. 3.5 (a) and (b), respectively. If the Lyapunov exponents of the logistic map are considered, then it can be easily observed that, for many values of μ, the Lyapunov exponent is either zero or negative, particularly in the chaotic region, whereas PWLCM has a positive Lyapunov exponent for all values of μ. Therefore, the chaoticity condition, i.e., $\lambda > 0$, is perfectly satisfied by PWLCM, but it is satisfied once in a while for the logistic map. Fig. 3.5 (c) and (d) shows the comparison between bifurcation diagrams of logistic and PWLC maps. If Fig. 3.5 (c) is observed, then the blank window (highlighted in red ellipse) is seen in the chaotic region of the logistic map, which effects its performance, whereas Fig. 3.5 (d) tells that PWLCM has no blank window. Moreover, the distribution of the values is also uniform, i.e., PWLCM perfectly covers the whole range [0,1], that which the logistic map fails to do. Therefore, PWLCM is a far versatile chaotic map with more complicated behavior than the logistic map.

In the encryption stage, PWLCM can also used to generate transform order for FrWPT and to obtain a random matrix that is further used as the matrix key. For this purpose, three different initial values are considered, and using Eq.(3.9), three different sequences are obtained. The final values of two sequences serve as transform order along the x- and y-axis, whereas of the third one is stacked in an array to create a random matrix.

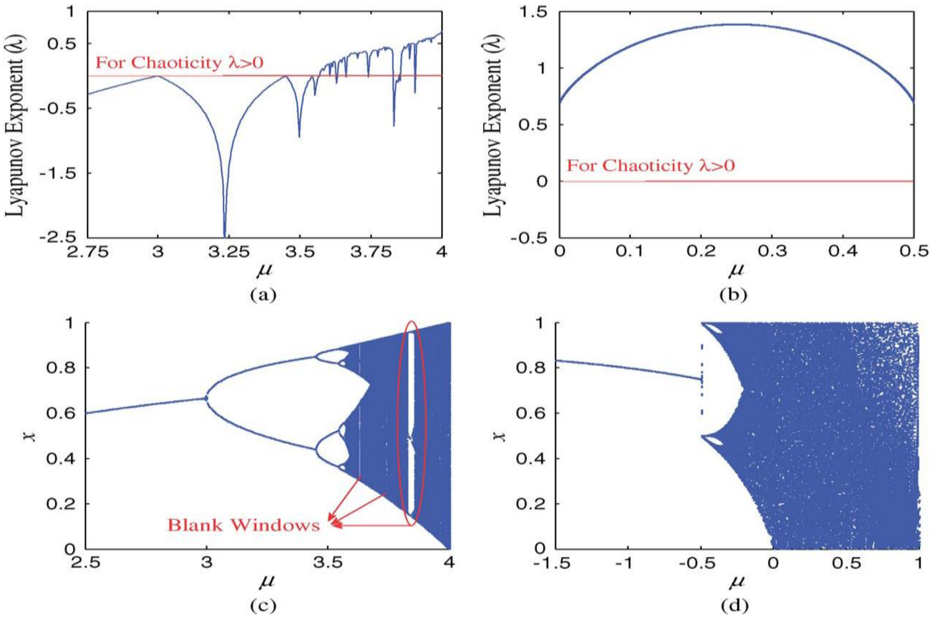


Figure 3.5 : Comparison between logistic and piece-wise linear chaotic maps Lyapunov exponent of a) logistic map and b) PWLCM ; bifurcation diagram of c) logistic map and d) PWLCM

3.2.2 CTPNCM

The cryptosystems based on widely used one-dimensional discrete chaotic maps suffer from fundamental drawbacks such as small key space, slow performance speed and weak security function. To overcome these limitations, this work proposes the use of Coupled Two-dimensional Piecewise Nonlinear Chaotic Map (CTPNCM). It uses nonlinear functions instead of linear functions.

In this design, two-dimensional piecewise nonlinear chaotic maps with invariant measure are defined as :

$$\phi_1 (x_n , \alpha) \quad = \quad \frac{4\, \alpha^2 yn\, (1-xn)}{1 + 4\, (\alpha^2 - 1)\, xn\, (1-xn)}$$

$$\phi_2 (y_n, b1, b2) \; = \; \begin{cases} \dfrac{4\, b1^2\, yn(1-yn)}{1+4\left(b1^2-1\right) yn(1-yn)} & x_n \in [0\, , \tfrac{1}{2}] \\[2ex] \dfrac{4\, b2^2\, yn(1-yn)}{1+4(b2^2-1)\, yn(1-yn)} & x_n \in [\tfrac{1}{2}\, , 1] \end{cases} \qquad (3.10)$$

where α, b1 and b2 are the system parameters. In these maps, the values of the two variables xn and yn at time-step n change into x_{n+1} and y_{n+1}at time step n+1. The points x_i , i = 1,. . .,N are the maximum or minimum points in the plot of x_{n+1} vs x_n.

The CTPNCM is defined as follows:

$$x_{n+1}\, (j) = (1- \epsilon)\ \phi_1(x_n(j),\alpha_j) + \epsilon\ \phi_1(x_n(j+1),\alpha_j)$$

$$y_{n+1}\, (j) = (1- \epsilon)\ \phi_2(y_n(j),b_1^j,b_2^j) + \epsilon\ \phi_2(y_n(j+1), b_1^j,b_2^j)$$

$$n = 0,1,\ldots..,L\text{-}1\ ;\ j= 1,2,3 \qquad (3.11)$$

Where x_0(j) and y_0(j) are the initial conditions of the coupled two dimensional piecewise nonlinear chaotic map.

The two-dimensional piecewise nonlinear chaotic maps have large numbers of positive Lyapunov exponents, bit diffusion, and confusion which are conducted in multiple directions of high-dimensional variable spaces. These features will enhance the security. Furthermore, the coupling structure in this design will greatly increase sensitivity to initial condition. For the CTPNCM, the two dimensional piecewise nonlinear chaotic maps of three lattices are first iterated in parallel mode. Then, the new state values are calculated according to the coupling relationship between the lattices. Although iterating the CTPNCM requires much more computational effort than a simple chaotic map, the simultaneous generation of the pseudo-random numbers should cause the CTPNCM to achieve higher speed performance than a simple chaotic map in each round.

The initial conditions are x_{01},y_{o1} and the parameters (α,b_1,b_2) . Then the new values are then derived as follows:

$$x_{02} \quad = \mathrm{mod}\ (x_{01} + d\ , 1)$$

$$x_{03} \quad = \mathrm{mod}\ (x_{02} + 2d\ , 1)$$

$$y_{02} \quad = \mathrm{mod}\ (y_{01} + d\ , 1)$$

$$y_{03} \quad = \mathrm{mod}\ (y_{02} + 2d\ , 1)$$

$$\alpha^{new} \ = (X_{n\times 1}(1) + Y_{n\times 1}(1) + \alpha^{old})\ \mathrm{mod}\ 1$$

$$b_1^{new} = (X_{n\times 1}(2) + Y_{n\times 1}(2) + b_1^{old})\ \mathrm{mod}\ 1$$

$$b_2^{new} \ = (X_{n\times 1}(3) + Y_{n\times 1}(3) + b_2^{old})\ \mathrm{mod}\ 1 \qquad (3.12)$$

It is evident that the chaotic maps are very sensitive to their initial seed. Therefore, a slight change in the initial seed will cause the significant change in their final value and in transform orders. Hence, there is very less possibility for the transform orders to be in proximity of the original transform order.

Next section explains how this concept is utilized in this encryption scheme. Here x01, y01,d, α ,ϵ, b1, b2 and L are taken as inputs. As a first step using x01 and y01, the remaining values x02, x03, y02 and y03 are calculated (refer Eq.(3.12)). Next step is the calculation of two sequences X1mat and Y1mat. For this we are using the remaining equations in the CTPNCM.

Consider Q1 and Q2 are sequences with two elements. Therefore as a first section of next step calculate the entries in Q1 and Q2 as a function of x01 and y01 using Eq.(3.10). Then using element in Q1, ϵ and α a new element xn is calculated using Eq.(3.11). Similarly using the same equation another element yn is calculated with the help of Q2, ϵ, b1 and b2. After this update the control parameters α, b1 and b2 and initial values x01 and x02. Here the calculated xn and yn values are selected as the new x01 and y02 respectively. And these steps are repeated for L times. Therefore at each time a new xn and yn values are formed. And these values are arranged back to back to form X1mat and Y1mat.

As a next section calculate the entries in Q1 and Q2 as a function of x02 and y02 using Eq.(3.10). And repeat the steps in first section then form another two sequences X2mat and Y2mat. Similarly, calculate the entries in Q1 and Q2 as a function of x03 and y03 using Eq.(3.10). And then form another two sequences X3mat and Y3mat.

Then by taking the average of X1mat, X2mat and X3mat form a sequence. In this way using Y1mat, Y2mat and Y3mat form another sequence. And here the final entries in these two sequences are selected as the transform orders in x axis and y axis.

3.3 FrWPT

The FrWPT is a realization of the wavelet packet transform in the fractional Fourier domain. Therefore, the forward FrWPT can be obtained by taking the FrFT with the optimal fractional order on the input signal followed by the wavelet packet transform, whereas inverse FrWPT can be done by taking the inverse wavelet packet transform followed by the inverse FrFT to return back to the plane of the input signal. The process for forward and inverse FrWPT is depicted in fig 3.6.

Forward FrWPT : FrFT + WPT

Inverse FrWPT : inverse WPT + inverse FrFT (3.13)

This transform is highly sensitive to the transform orders, so without knowing the correct values of transform orders, no one can obtain correct transformed domain and so no one can decrypt the image. This property makes FrWPT the best and suitable transform for the encryption techniques.

Due to the rotation of time-frequency plane over an arbitrary angle, Fractional Fourier transform (FrFT) has a unique property of describing the information of spatial and frequency domain. In similar way, wavelet packet transform has a multi-resolution property. As described above FrWPT is a combination of FrFT and WPT, therefore it exhibits multi-resolution property and describes the spatial and frequency domain information.

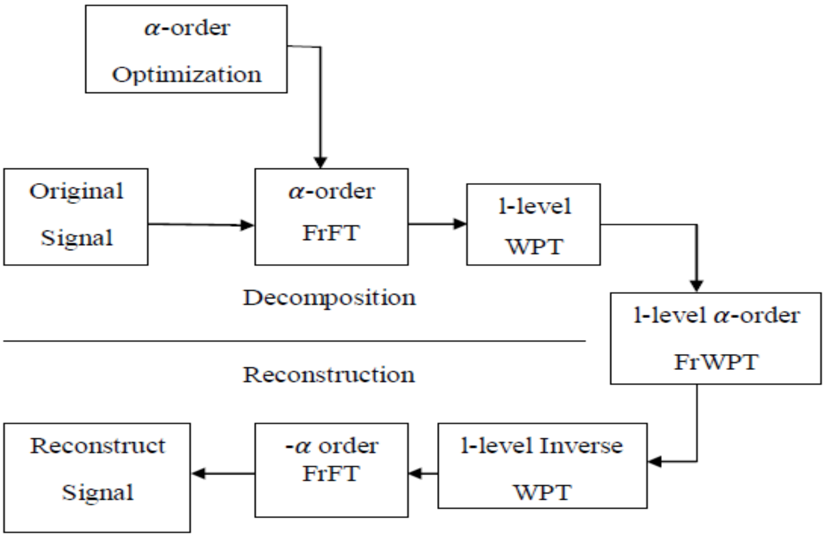


Figure 3.6 : Decomposition and reconstruction process for FrWPT

The FrWPT of a 1-D function f(t) is given by

$$W_{\alpha}(u,s,\tau) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(t) K\alpha(t,x) e^{-jux}\, \psi_{s,\alpha}(x)\, dt\, dx \qquad (3.14)$$

where s,τ, and α are the dilation (scale), translation (position) parameters, and transform order, respectively. Furthermore, $K_{\alpha}(t,x)$ is the transform kernel.

This transform kernel is given by

$$k_{\alpha}(t,x) = e^{\left(\frac{i}{2}\right)(t^2+x^2)\cot\bar{\alpha}} \quad \text{and } C_{\alpha} = e^{i\bar{\alpha}/2} / \sqrt{2\,\pi\, i\, \sin\bar{\alpha}.} \qquad (3.15)$$

It is clear that if $\alpha \overline{=} \alpha\, \pi/2,$ $C_{\alpha} = \sqrt{(1 - i\cot\alpha/2\pi)}$.

Consider the limiting case $\sin\alpha \overline{=} 0$, then the kernel reduces to a Dirac delta [$\delta(x \pm t)$]. From equation 3.14, it is clear that FrWPT is the realization of the wavelet packet transform in fractional Fourier domain. Due to the rotation of time-frequency plane over an arbitrary angle, Fractional Fourier transform (FrFT) has a unique property of describing the information of spatial and frequency domain. In contrast, wavelet packet transform has a multi-resolution property. As explained before FrFT is a combination of these two, so it exhibits multi-resolution property and describes the spatial and frequency domain information.

In order to construct the original signal back from the decomposed signal, the inverse FrWPT is defined as

$$f(t) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} W_{\alpha}(u,s,\tau)\, K_{-\alpha}(t,x)\, e^{jux}\, \boldsymbol{\psi}_{s,\tau}(x)\, du\, ds\, d\tau\, dx \qquad (3.16)$$

Since FrWPT satisfies separability property, 2-D transform can be obtained by successively taking 1-D transform along both the axis. Hence, the FrWPT of 2-D function $f(t_x,t_y)$ can written as

$$W_{\alpha x,\alpha y}(u,v,s1,\tau 1,s2,\tau 2) = \text{FrWPT}\ \underset{\alpha y}{ty \longrightarrow v}\ \{\ \text{FrWPT}\ \underset{\alpha x}{tx \longrightarrow u}\ \{f(t_x,t_y)\}\ \} \tag{3.17}$$

Where s1, s2, τ1, τ2 are the dilation (scale) and translation (position) parameters along the x and y direction, respectively.

3.3.1 FrFT

The fractional Fourier transform (FRFT) is a family of linear transformations generalizing the Fourier transform. It can described as the Fourier transform to the n-th power, and this n value need not be an integer - thus, this FrFT transforms the input function to a intermediate domain between time and frequency.

The FRFT of order α of x(t) is expressed as $X_\alpha(u)$, and it is given by eqn 3.18.

$$X_\alpha(u) = \int_{-\infty}^{\infty} x(t)K\alpha(t,u)dt \tag{3.18}$$

The inverse transform is given by,

$$X_\alpha(u) = \begin{cases} \sqrt{\frac{1-j\cot\alpha}{2\pi}}\ e^{j(u^2\cot\alpha/2)} \int_{-\infty}^{\infty} x(t)\ e^{j\left(t^2\ \cot\frac{\alpha}{2}\right)-jut\,\mathrm{cosec}\,\alpha}dt, & \text{if } \alpha \text{ is not a multiple of } \pi \\ x(t) & \text{, if } \alpha \text{ is a multiple of } 2\pi \\ x(-t) & \text{, if } \alpha+\pi \text{ is a multiple of } 2\pi \end{cases}$$

where K_α is the kernel and it is given as,

$$K_\alpha(t,u) = \begin{cases} \delta(t-u) & \text{, if } \alpha \text{ is a multiple of } 2\pi \\ \delta(t+u) & \text{, if } \alpha+\pi \text{ is a multiple of } 2\pi \\ \sqrt{\frac{1-j\cot\alpha}{2\pi}}\ e^{j\left(\frac{u^2+t^2}{2}\right)\cot\alpha-jut\,\mathrm{cosec}\,\alpha} & \text{, if } \alpha \text{ is not a multiple of } \pi \end{cases} \tag{3.19}$$

3.3.2 Interpretation of FrFT

The Fourier transform is usually interpreted as a transformation from time domain signal into a frequency domain signal. On the other hand, inverse Fourier transform is interpreted as a transformation of a frequency domain signal into a time domain signal. In this way, fractional Fourier transforms can describe as a transformation that transforms input signal (either in the time domain or frequency domain) into a domain between time and frequency: it is a rotation in the time-frequency domain.

Take Fig 3.7 as an example. Here we can see that, if the signal is rectangular in the time, it will become a sinc function in the frequency domain. But if we apply the fractional Fourier transform to the rectangular signal, the output will be in the domain between time domain and frequency domain.

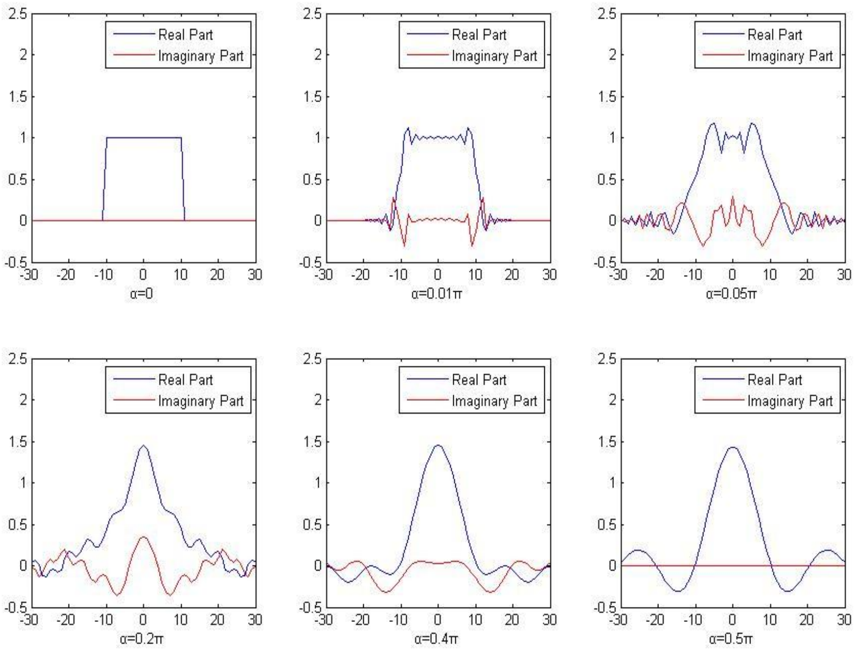


Figure 3.7 : Fractional fourier transform

Actually, fractional Fourier transform can be viewed as a rotation operation on the time frequency distribution. Consider that, fractional order α is equal to 0, then there will be no change after applying fractional Fourier transform, and for $\alpha = \pi/2$, fractional Fourier transform becomes a Fourier transform, which rotates the time frequency distribution with $\pi/2$. For other value of α, fractional Fourier transform rotates the time frequency distribution according to given α value.

Fig 3.8 shows the results of the fractional Fourier transform with different values of α.

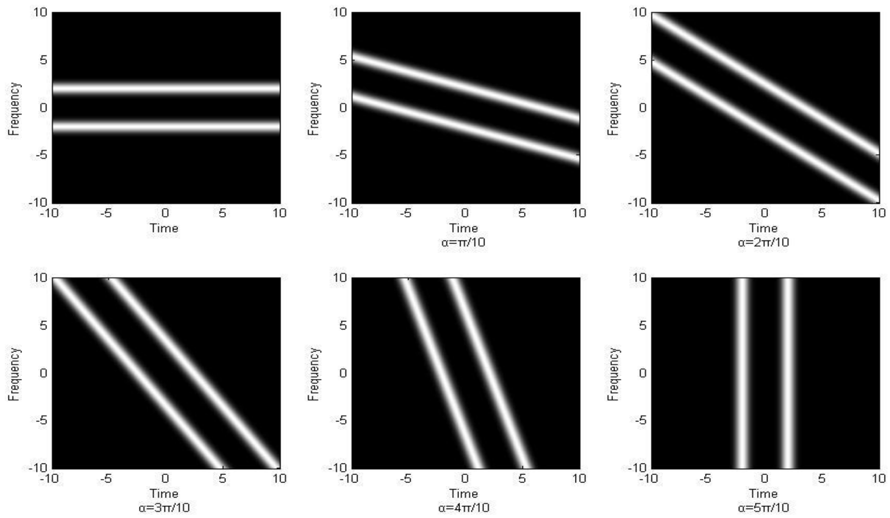


Figure 3.8 : Time/frequency distribution of fractional fourier transform

3.3.3 DFrFT

Here DFrFT is found out based on eigen decomposition of DFT matrix. In this DFrFT is defined by taking fractional eigen value powers of an eigen decomposition of the DFT matrix.

Consider f is the fourier transform, f = [f(0) f(2) ……… f(N-1)] then ,

$$\mathrm{FrFT} = F^{a} \times f \qquad \text{where } F^{a} = E \times \wedge^{a} \times E^{T} \tag{3.20}$$

3.3.4 WPT

After that WPT of this result is found using the function dwt2 ().The dwt2 command performs single-level two-dimensional wavelet decomposition with respect to either a particular wavelet or particular wavelet decomposition filters. Syntax is,

$$[cA,cH,cV,cD] = dwt2(X,'wname') \tag{3.21}$$

[cA,cH,cV,cD] = dwt2(X,'wname') computes the approximation coefficients matrix cA and details coefficients matrices cH, cV, and cD (horizontal, vertical, and diagonal, respectively), obtained by wavelet decomposition of the input matrix X. The 'wname' string contains the wavelet name.

The DWT of images is a transform based on the tree structure with D levels that can be implemented by using an appropriate bank of filters. Tree structure for single level DWT is given in Fig (3.9).

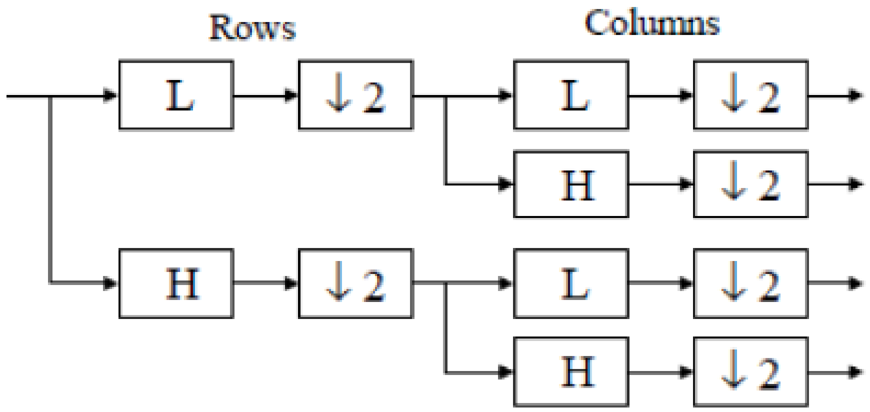


Figure 3.9 : Tree structure for DWT decomposition

Here L and H denote low and high pass filters respectively, ↓2 denotes sub-sampling. For two-dimensional pictures DWT is performed firstly for all image rows and then for all image columns. The main

feature of DWT is multi-scale representation of function. By using the wavelets, given function can be analyzed at various levels of resolution. The DWT is also invertible and can be orthogonal.
Output of this decomposition is given in Fig (3.10).

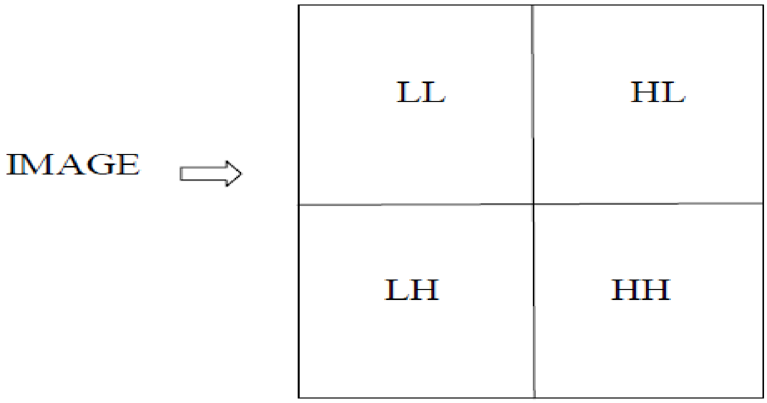


Figure 3.10 : Sub-bands of single level 2D - DWT

Next step is the deformation of FrWPT coefficients; it is done with the help of a matrix key (P) and SVD. This matrix key is generated by using PWLCM .

3.4 Singular Value Decomposition (SVD)

In linear algebra, the SVD is an important factorization of a rectangular real or complex matrix with many applications in signal/image processing and statistics. Let A be a real (complex) matrix of order m×n. The SVD of A is the factorization of the form $A = USV^T$, where U is m × m unitary matrix, matrix S is m × n diagonal matrix with nonnegative real numbers on the diagonal, V is an n × n unitary matrix and V^T denotes the conjugate transpose of V. Such factorization is called an SVD of A.

In this work, SVD is performed on the matrix key (found using PWLCM). Let P is the matrix key, then SVD on will give factorization in the given form.

$$P = U_p\, S_p\, V_p^T \tag{3.22}$$

3.5 Deformation Of Subbands And Inverse FrWPT

Next step is the deformation of FrWPT coefficients of each subband using orthonormal matrices U_P and V_P , as

$$f_n^{\theta,def} = \begin{cases} U_p\, f_n^{\theta}\, V_p^T\,, & \text{if } M \le N \\ V_p\, f_n^{\theta}\, U_p^T\,, & \text{if } M > N \end{cases} \tag{3.23}$$

Last step is inverse FrWPT to get the encrypted fingerprint image (say $\dot{F}$).

3.6 Decryption Scheme

To reconstruct the original fingerprint image from the encrypted image, the reverse steps are performed. Here the first step is the calculation of FrWPT. In the next steps inverse deformations are applied and inverse FrWPT is found out. As a last step, inverse RHT algorithm is required to reconstruct the original fingerprint image. General block diagram of this is illustrated in Fig 3.11.

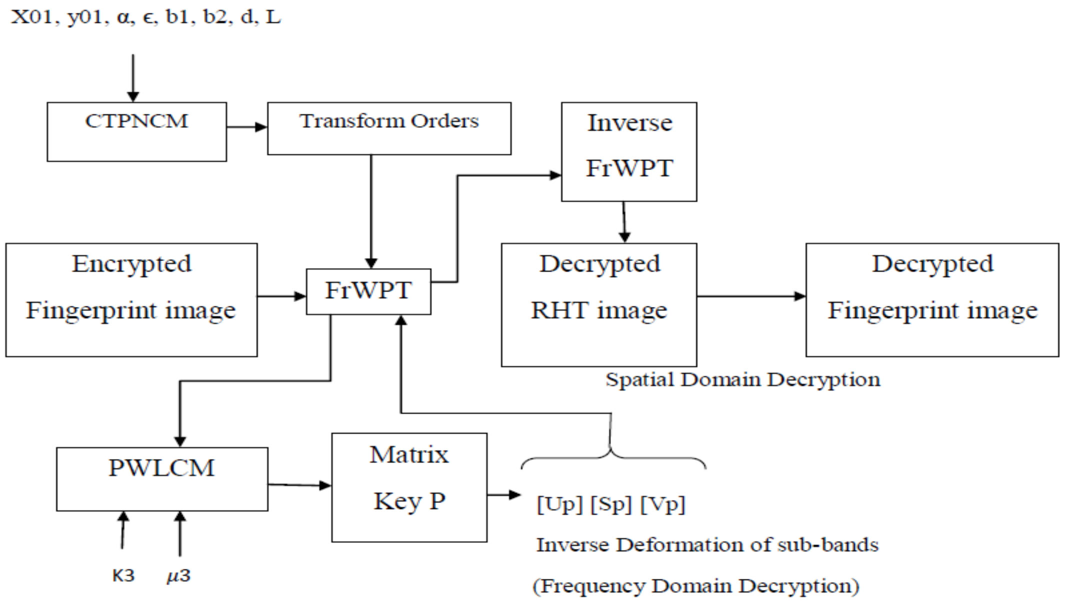

X01, y01, α, ϵ, b1, b2, d, L
CTPNCM
Transform Orders
Inverse FrWPT
Encrypted Fingerprint image
FrWPT
Decrypted RHT image
Decrypted Fingerprint image
Spatial Domain Decryption
PWLCM
Matrix Key P
[Up] [Sp] [Vp]
Inverse Deformation of sub-bands
(Frequency Domain Decryption)
K3
μ3

Figure 3.11 : Block diagram of the decryption scheme

Result of this encryption and decryption with correct keys is given below in Fig (3.12).

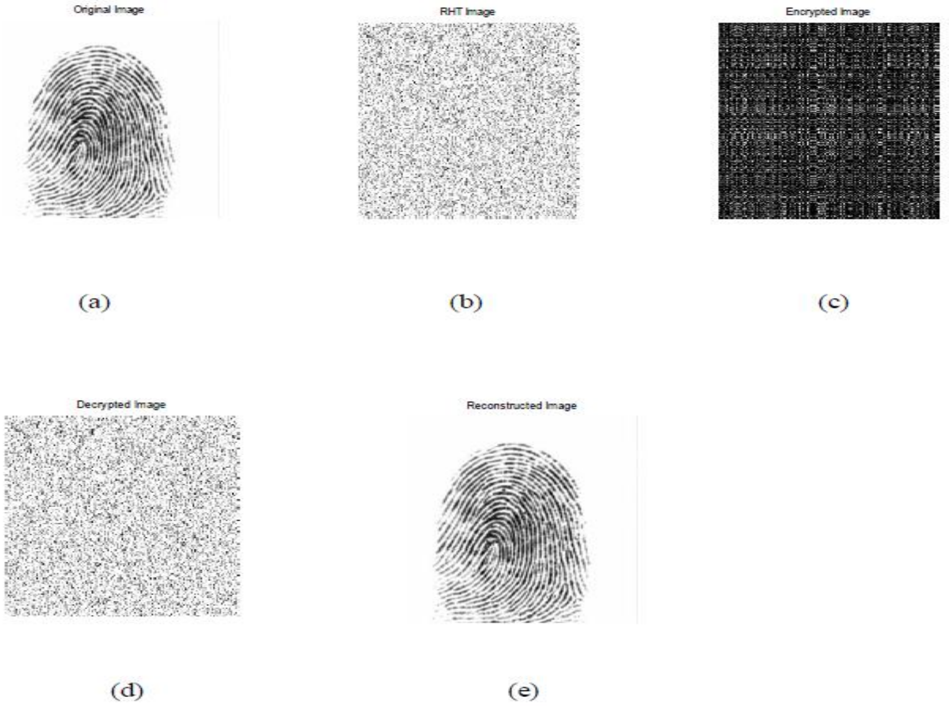


Fig.3.12 : Encryption and decryption using correct keys (a) Original fingerprint image (b) RHT image (c) Encrypted fingerprint image (d) Image obtained after doing inverse RHT (e) Reconstructed image using correct keys

Result of this encryption and decryption with wrong keys is given below in Fig (3.13).

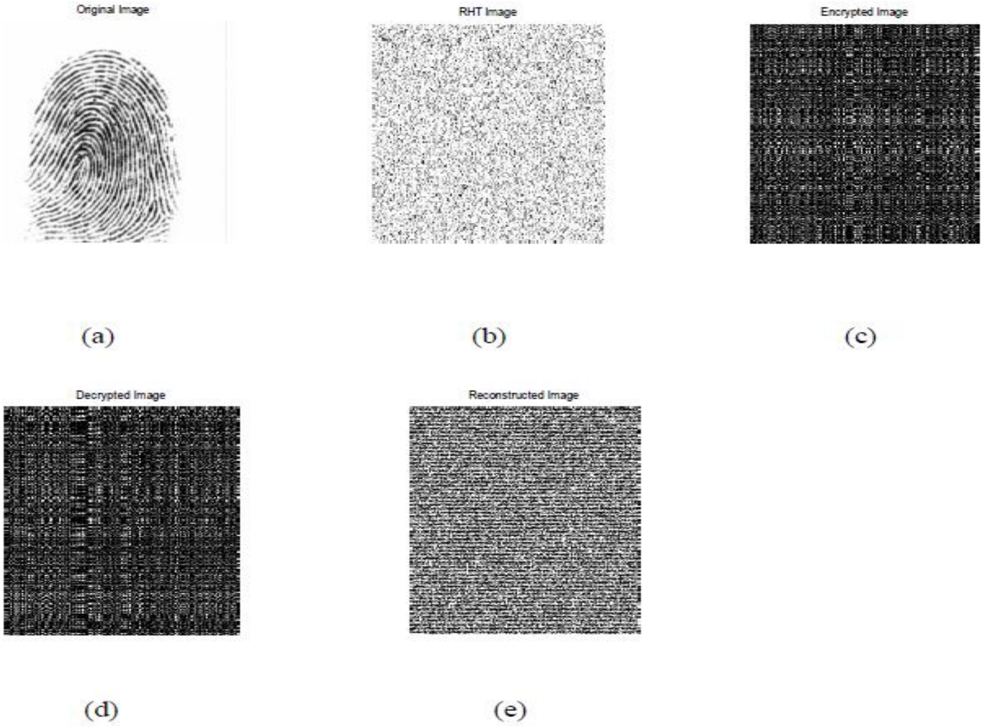


Figure 3.13 : Encryption and decryption with different keys (a) Original finger print image (b) RHT image (c) Encrypted fingerprint image (d) Image obtained after doing inverse RHT (e) Reconstructed image using wrong keys

From the analyses given in fig 3.12 and fig 3.13, it is clear that this proposed encryption scheme is very sensitive to secret keys used. This is because of the sensitiveness of FrWPT to the transform orders and randomness of CTPNCM. Because of these factors it is clear that without knowing the correct initial seeds and control parameters of chaotic maps, no one can reconstruct the original fingerprint image from the encrypted image.

IV. Conclusion

The encryption scheme presented is a simple and efficient security solution for fingerprint images. It is based on RHT, FrWPT, chaotic map and SVD. This proposed encryption scheme is very sensitive to secret keys used. This is because of the sensitiveness of FrWPT to the transform orders and randomness of CTPNCM. Because of these factors it is clear that without knowing the correct initial seeds and control parameters of chaotic maps, no one can reconstruct the original fingerprint image from the encrypted image.

The efficiency of the solution is carried out by the detailed discussion of key sensitivity, original fingerprint sensitivity, histogram analysis, numerical analysis, and time efficiency. This analysis demonstrates the high security of the proposed fingerprint encryption scheme.

Biometric Encryption is helpful for the linking and retrieval of digital keys, which can be used as a method for the secure management of cryptographic keys. The cryptographic key is generated independently from the Biometric Encryption algorithm and can be updated periodically via a re-enrollment procedure. The convenience and security provided by Biometric Encryption will definitely help to promote more widespread use of cryptographic systems.

References

[1]. Gaurav Bhatnagar “Chaos-based security solution for fingerprint data during communication and transmission”, IEEE transactions on instrumentation and measurement, vol 61, no 4, April 2012

[2]. U. Uludag, S. Pankanti, and S. Prabhakar, “Biometrics cryptosystems: Issues and challenges,” Proc. IEEE, vol. 92, no. 6, pp. 948–960, Jun. 2004.

[3]. A. K. Jain, L. Hong, S. Pankanti, and R. Bolle, “An identity-authentication system using fingerprints,” Proc. IEEE, vol. 85, no. 9, pp. 1365–1388, Sep. 1997.

[4]. A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, “Handbook of Applied Cryptography”, Boca Raton, FL: CRC Press, 1996.

[5]. D. Moon, Y. Chung, S. B. Pan, K. Moon, and K. I. Chung, “An efficient selective encryption of fingerprint images for embedded processors,” ETRI J., vol. 28, no. 4, pp. 444–452, Aug. 2006.

[6]. C. Ashok Narayanan, k.M.M Prabu, “The fractional fourier transform: theory, implementation and error analysis”, Elsevier J.,June 2003, pp. 511-521

[7]. Deepak Sharma, Rajiv Saxena and Ashutosh Rajput , “Bobust image encryption using discreate fractional fourier transform with eigen vector decomposition algorithm”, Advances in Microelectronic Engineering (AIME) Volume 1 Issue 4, October 2013

[8]. M.S Baptista, “Cryptography with chaos”, 1998

[9]. Abhishek misra, Ashutosh Gupta and Damodar Rai, “Analysing the parameters of chaos based image encryption schemes” World Applied Programming, Vol (1), No (5), December 2011. 294-299

[10]. Y. Huang, B. Suter, “The fractional wave packet transform”, Multidimensional Syst. Signal Process., vol. 9, no. 4, pp. 399–402, Oct. 1998.

[11]. L. Chen, D. Zhao, “Image encryption with fractional wavelet packet method,” Optik-Int. J. Light Electron Opt., vol. 119, no. 6, pp. 286–291, May 2008.

[12]. Seyed Mohammad Seyedzadeh and Sattar Mirzakuchaki “A fast color encryption algorithm based on coupled two-dimensional piecewise chaotic map”, IEEE Signal processing 92 (2012) 1202-1215

[13]. Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, “Image quality assessment: From error visibility to structural similarity”, IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600-612,Apr. 2004.

[14]. Zhou Wang and Alan C. Bovik “A Universal Image Quality Index”, IEEE Signal Processing Letters, 2001.