International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 4 (2015) pp. 8925-8933

http://www.ripublication.com

# Encryption of Fingerprint Template By Hyper Chaotic 4D Lorenz System

**Latha.U,**
*Department of IT, Dhaanish Ahmed College of Engg.,*
*Tamil Nadu, Chennai, India,*
*latha_umapathy1@yahoo.co.in*

**Ramesh Kumar.K,**
*Department of IT, Hindustan University,*
*Tamil Nadu, Chennai, India,*
*krkumar@hindustanuniv.ac.in*

## Abstract

An efficient finger print classification and recognition system which is subject to versatile security access may be contend with noisy data, vulnerable attacks, and unacceptable error. These parametric limitations can be swept away by employing with hyper chaotic 4D-Lorenz system in this novel authentication system. The pre-processing stage i.e. finger print reconstruction is influenced by M-band Dual Tree Complex Wavelet Transform (DTCWT) which is intended to transform the finger print images to frequency domain. Over this process different levels of crack variance finger prints are reconstructed. This proposed scheme is developed in four stages, fingerprint enhancement, reconstruction, feature extraction, and encryption. An autonomous hyper chaotic 4D Lorenz system is developed for generating stream cipher communications, where the synchronization between the user and the authentication system is very important. By this, our novel authentication system reduces the matching errors like FAR, FRR, FTC and FTE and the attacks of biometric system is prevented and secured communication can be done on the fingerprint databases. The authentication system is tested over a set of fingerprint images from FVC 2002 database and numerical simulations are done to estimate the effectiveness and reliability of the authentication system.

**Keywords:** Fingerprint; Reconstruction; Hyper chaos; FFT; 4D Lorenz system; Encryption

## Introduction

Accurate automatic personal identification is vital in a variety of applications in our electronically interconnected society. Biometrics that refers to identification, based on physical or behavioral characteristics, is being progressively adopted to produce identification with a high degree of confidence. Among all the biometric techniques, fingerprint-based authentication systems have received the foremost attention as a result of the long history of fingerprints and there in depth use in forensics [2-3]. However, the various authentication systems presently on the market still don't meet the tight performance necessities of many vital civilian applications. To secure the fingerprint templates the feature values are encrypted using chaos based random number key generation and hyper chaotic 4D Lorenz system. To assess the performance limitations of standard minutiae based fingerprint verification system, we tend to in theoretically estimate the likelihood of a false correspondence between two fingers

## Architecture For Authentication System

The proposed Authentication system is sub-divided into two segments, Registration process and Authentication process. The overall architectural design of such system is shown in Fig1. The database system which is placed at the backend server plays as a mutual block for registration as well as authentication system.

A. Registration Process

The initial process i.e. registration process starts with the authentication server. The designed system prompts for fingerprint acquisition stage. The reconstruction process is adopted from the previous work [1]. The reconstruction process is done by decomposing the cracked input fingerprint images via 2D DTCWT in four different stages which includes Initial value assignment, 2D DTCWT process, coefficients thresholding and finally reconstruction.

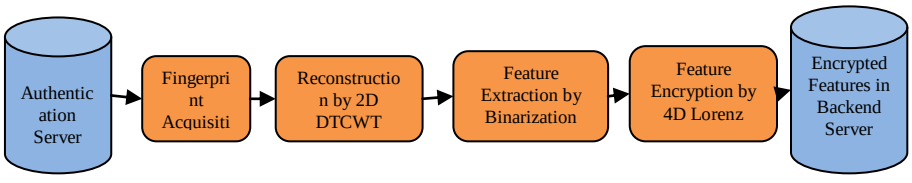



**Figure 1:** Architecture for fingerprint encryption

In the case of feature extraction, related work is done in [5]. In [5] binarization technique is used for feature extraction. The preprocessing stage includes segmentation and enhancement of the image. The enhancement of image is done by

FFT. The essential motive behind adopting binarization is because it improves the contrast between the ridges and valleys in a fingerprint image by converting the image from gray level to binary level.

**Table 1:** Extracted Feature Values for a test fingerprint input.

| **Image** | **Feature Values** |
|---|---|
| 101_1 | (82,19), (45,40), (193,40), (182,42), (159,45), (117,46), (78,54), (129,57), (85,60), (115,60),(131,75), (147,81), (121,85), (227,86), (138,88), (162,88), (40,89), (49,101), (136,121), (195,123), (80,136), (161,157), (44,161), (227,161), (124,34), (133,34), (142,34), (167,37), (56,38), (55,50), (144,50), (35,57), (206,58), (101,60), (106,68), (33,72), (76,74), (223,74), (19,76), (61,81), (63,82), (87,87), (76,96), (248,97), (147,100), (161,100), (147,101), (127,103), (166,106), (168,116), (242,118), (90,122), (244,122), (147,123), (80,124), (144,131), (38,134), (243,141), (166,145), (57,146), (185,148), (182,162) |

B. Authentication System

The authentication system includes some common blocks which are used in registration process as shown in Fig1. The feature values are stored in the backend database system after the encryption and it is used for the acquisition of feature values for decryption and fingerprint matching. Here, the matching is done through Minutiae based matching [6].

## Encryption By Hyper Chaotic 4d Lorenz System

Due to some intrinsic features of the images, such as bulk data capacity and high correlation among pixels the earlier encryption techniques such as AES, DES, RSA, etc are not suitable for practical applications. In this case chaos based encryption techniques are considered good for practical use. Chaos has the following properties 1) It must be sensitive to initial conditions, 2) Its periodic orbit must be dense, and 3) It must be topologically mixing.So in this novel approach encryption is done by hyper chaotic 4D Lorenz system.

Consider the following generalized Lorenz system [11]

$$\begin{bmatrix}\dot{x}\\ \dot{y}\\ \dot{z}\end{bmatrix} = \begin{bmatrix}a_{11} & a_{12} & 0\\ a_{21} & a_{22} & 0\\ 0 & 0 & a_{33}\end{bmatrix}\begin{bmatrix}x\\ y\\ z\end{bmatrix} + x\begin{bmatrix}0 & 0 & 0\\ 0 & 0 & -1\\ 0 & 1 & 0\end{bmatrix}\begin{bmatrix}x\\ y\\ z\end{bmatrix} \quad (1)$$

Now, introduce an additional state, u, and couple it to the second equation of the chaotic system (1), thereby obtaining a fourth-order system in (2).Where k is a

constant to be determined later. Notice that the modified system (2) satisfies the criteria for hyper chaos. As a result, system (2) gives a chance for hyper chaos, i.e. possessing two positive Lyapunov exponents along with one zero and one negative Lyapunov exponent. In the following, the existence of hyper chaotic attractor in the modified system (2) is illustrated, as usual, mainly numerically.

$$\begin{bmatrix} \dot{x} \\ \dot{y} \\ \dot{z} \\ \dot{u} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & 0 & 0 \\ a_{21} & a_{22} & 0 & 1 \\ 0 & 0 & a_{33} & 0 \\ -k & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \\ u \end{bmatrix} + x \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \\ u \end{bmatrix} \tag{2}$$

In general, autonomous continuous hyper chaotic systems are modeled by the following four non-linear differential equation systems:

$$\dot{x} = F(x, y, z, w)\ ;\ \dot{y} = G(x, y, z, w)\ ;$$
$$\dot{z} = Q(x, y, z, w)\ ;\ \dot{w} = P(x, y \tag{3}$$

Where *F*, *G*, *Q*, and *P* are non-linear equations and *x*, *y*, *z*, and *w* are the four state variables of the dynamical system. For computing the solutions of the system (3), we use the fourth order Runge-Kutta (RK-4) numerical method for resolving the continuous chaotic system models because it produces a more accurate estimate of the solution [10]. In this work, we are interested in the hyper chaotic Lorenz system modeled as follows [10]:

$$\begin{aligned} \dot{x} &= a(y - x) \\ \dot{y} &= x(b - z) - y + w \\ \dot{z} &= xy - cz \\ \dot{w} &= -fx \end{aligned} \tag{4}$$

As is well known, the 3D Lorenz chaotic system has only one positive Lyapunov exponent. However, hyper chaotic system must satisfy the following two necessary conditions:

- For autonomous system, four- dimension (4D) is required at least;
- Two or more positive Lyapunov exponents and the sum of all the Lyapunov exponents is less than 0.

In [11], it has been proven that this 4D Lorenz system exhibits hyper chaotic behaviors and presents a two dimensional bifurcation diagram for the following parameter conditions: $a = 10$, $c = 8/3$, $0 < b < 30$, and $0 < f < 15$. Therefore, the system preserves its hyper chaotic behavior and bifurcation diagram for the following considered parameter values $a = 10$, $b = 28$, $c = 8/3$, and $f = 5$ and with the initial conditions $x0 = y0 = z0 = w0 = -10$. By referring [9] the 4D hyper chaotic Lorenz system (5), making the following changes for the system (4), a new 4D hyper chaotic Lorenz system is constructed. By increasing the fourth state variable *w* with parameter *e* in the second state equation of Lorenz system and the change rate of the fourth state variable *w*, furthermore changing nonlinear term in the third state equation of Lorenz system, state equations are expressed as:

$$\dot{x} = a(y - x)$$
$$\dot{y} = cx - xz - y + ew$$
$$\dot{z} = x^4 + y^4 - bz$$
$$\dot{w} = -dy \quad (5)$$

There are five parameters in this new 4D hyper chaotic Lorenz system (5); they are more than two parameters for the Lorenz system. The nonlinear term in the third state equation of system (5) is $x^4+y^4$ which are different from the systems (3) and (4). Four Lyapunov exponents of the new 4D hyper chaotic Lorenz system (3) are $\Lambda_1$ = 0*:*60613, $\Lambda_2$ = 0*:*28066, $\Lambda_3$ = 0, and $\Lambda_4$ = -11.489. The sum of all the Lyapunov exponents is less than 0. These results satisfy the above two necessary conditions.

A. Encryption and Decryption

The key focus of this security protocol lies on the foot of the encryption/decryption technique. Such high level cryptography is achieved by hyper chaotic 4D Lorenz systems. The encryption is process is described step by step. For each fingerprint input its corresponding feature values are extracted as shown in Table1.

$$\mathbf{f(\lambda) = (\lambda + b)(\lambda^3 + a_1\lambda^2 + a_2\lambda + a_3) = 0} \quad (5)$$

During each iteration two sets of feature values are given as input to (5) and its corresponding renewed (encrypted) values are stored in the database. The 4D hyper chaotic characteristic is verified concurrently with the characteristic equation (6). The decryption process can be performed as an inverse process of the encryption technique.

*Pseudo code for encryption:*
***Load*** *binary image (I) & feature values (fv)*
***Initialize*** *parametric values a, b, c and d*
***for*** *all fv*
*Select two sets of fv a, b, c and d*
*Chaos based Random number e is generated*
*apply a, b, c, d and e in 4D Lorenz State Eqn.*
***if*** *(Lyapunov exponents satisfy the 4D hyper chaotic Lorenz system conditions)*
***update*** *new feature values (fv$_{new}$)*
***else***
***adjust parametric*** *values*
***endif***
***end for***

Steps for Encryption and Decryption:

1. Load the original binary image and extracted feature values.
2. Two sets of feature values a, b, c, and d is given as input.
3. Random number e is generated.
4. Apply feature values a, b, c and d along with random number e in 4D Lorenz state equation.
5. 4 Lyapunov exponents are got as output.

6. If Lyapunov exponents satisfy the hyper chaotic Lorenz system conditions then
7. Update the new feature values , otherwise
8. Adjust the parametric values and update the feature values.

The Random number is generated by using Chaos based for encryption. The extracted features values are stored in backend server. Two sets of feature values a, b, c, d are given as input. So in the first iteration by getting the two sets of feature values as input along with the random number e as a parameter is generated. So the values of a, b, c, d, and e are applied in 4D Lorenz Equation. Many number of iteration is carried out for all the sets of feature values which is stored in the backend server. Finally the is encrypted and the encrypted feature values are stored in the backend database. For matching the fingerprint image decryption process is done. The decryption is done by inverse process.

## Results and Discussion

The full authentication system is tested with FVC 2002 database [7]. The PSNR which is used to measure the quality of the image and if only the image is with good quality and intensity, correct minutiae will be detected and matching is done perfectly. So for each image PSNR is estimated and it is compared with the 3D Lorenz system and Euclidean distance method and is shown in the Figure 2.The input image is enhanced so that minutiae is detected using binarization and morphological operators.

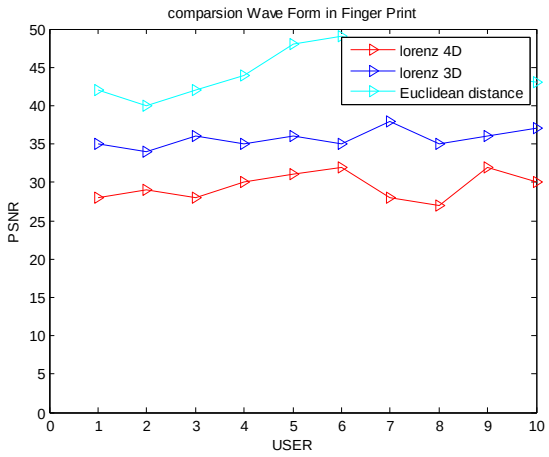
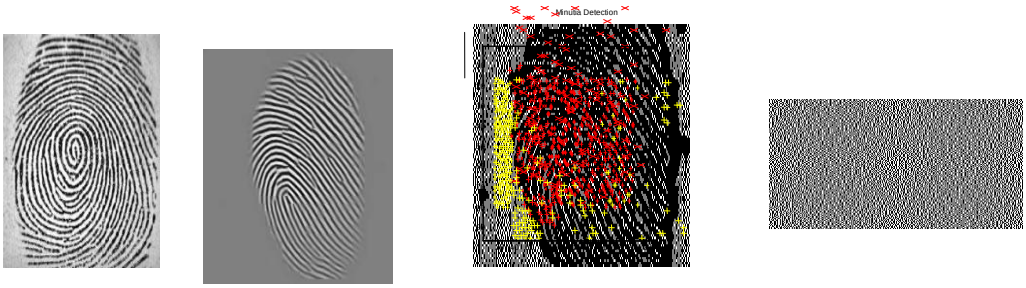



**Figure 2:** Comparison Wave Form in fingerprint

The extracted feature values are given as a input and by hyper chaotic 4D Lorenz system these feature values are encrypted. The encrypted image was stored in the database. The decryption is done by inverse process. By using hyper chaotic 4D Lorenz system, the peak signal noise ratio of an image ranges from 30 to 40. So that the quality of the image is high. We can prevent the attacks that could happen in the data bases and it provides a high security.

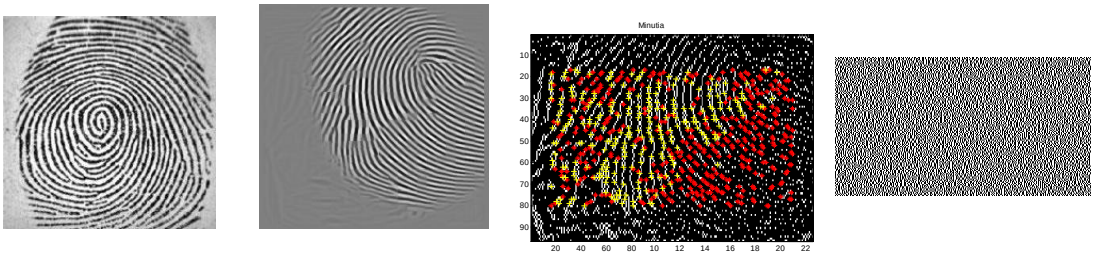
(a) (b) (c)

**Fig. 3** -Euclidean Distance Method : (a) Input Image 101_1 (b) Enhanced Image (c) Minutiae Detection



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

**Figure 4:** 3D Lorenz System : (a) Input Image 101_1 (b) Enhanced Image (c) Minutiae Detection (d) Encrypted image



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

**Figure 5:** 4D Lorenz System : (a) Input Image 101_1 (b) Enhanced Image (c) Minutiae Detection (d) Encrypted Image

Various attacks can occur in fingerprint template database and these attacks can be prevented and high security is given to the database by this approach. The modification attack can also be prevented .The following are the attacks which occur in the fingerprint database.

- **Basic Brute Force**- Attacker tries every possible bit combination till they guess the correct original feature data or key.

- **Correlation Attack**- From a cryptanalysis point of view, a good stream cipher should be resistant against a known-plaintext attack. In a known-plaintext attack the cryptanalyst is given a plaintext and the corresponding cipher text, and the task is to determine a key K. For a synchronous stream cipher, this is equivalent to the problem of finding the key K that produces a given key stream z1, z2,..., zN.
- **Known Key Attack**- Evaluate whether or not the fixed permutation with a randomly chosen key is ideal.
- **Substitution Attack**- "How difficult will it be to break into a folder containing biometric signatures and replace them with an attacker's biometric signature so that the attacker can get in with his/her own signature easily?"
- **Decidability Attack**- Exploit available information to link across databases.
- **Doppelganger Attack**- If the FAR is 1 in *X*, then an attacker can try more than *X* different prints.
- **Hill climbing Attack-**Security attacks based on generating artificial data, injecting it in the system and after analyzing the output and modifies the data.

## Conclusion

This Encryption technique is elaborated to restrict finger print information to be accessed by illegal entry; the multi level M-band 2D Dual Tree Complex Wavelet Transform (DTCWT) is performed to reconstruct the finger print images; by the influence of binarization, feature vales are extracted from the reconstructed image and then the featured values are encrypted by using 4D hyper chaotic Lorenz system and stored in the feature database. The performance issues are tested for the security protocol and evaluated for various cases. The performance analysis result shows that our design has an advantage of high security to meet out the current trends in a reliable way. This proposed architecture design lays a road map for hardware realization of the system.

## References

[1] Dr.K.Rameshkumar, U.Latha, "Efficient fingerprint image reconstruction by 2D DTCWT",International journal of Adv Comp, Vol 35, Issue 10, pp 415-421, 2012.

[2] Z.M.Kovacs-Vajna, "A fingerprint verification system based on Triangular Matching and Dynamic Time Wrapping", IEEE Trans on Pattern Anal. and Machine Intell, Vol. 22, No. 11, 2000

[3] Yoyo, P.Frasconi, M.Pontil, "Fingerprint classification with combination of support vector machines", Proc 3rd Intl. conf. on Audio-and Video-Based Biometric Person Authentication, pp 253-258, Sweden, June 6-8, 2001.

[4] Liu C X and Liu L 2009 Chin Phys. B 18 2188

[5] U.Latha, K.Rameshkumar, "Feature Extraction for fingerprints using binarization and morphological operators", Intl. Journal of Asian Acad Research Associates, Vol.1 Issue 13, Sept 2013.
[6] Rajeswari Mukesh, K Komathy, "N-bake: Fingerprint Authentication Against Biometric Database Attack", J. of Comp Inf Sys. 8:24(2012) pp10315-10324
[7] FCV finger print database http://bias.csr.unibo.it/fvc2002/.
[8] S Sadoudi, C Tanougast, M S Azzaz, "Design and FPGA implementation of a wireless hyper chaotic communication system for secure real-time image transmission", EURASIP Journal on Image and Video Processing 2013:43.
[9] S Gang-Quan, Cao Hui, Z Yan-Bin, "A new four-dimensional hyper chaotic Lorenz system and its adaptive control", Chin Phys. B Vol.20 No.1 2001(010509).
[10] Yuxia Li, Wallace K S. Tang, G Chen, "Hyper chaos evolved from the generalized Lorenz equation", Int. J. Circ. Theory. Appl. 2005; 33:235-251.