International Journal of Pure and Applied Mathematics
Volume 116 No. 10 2017, 435-452
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

A NOVEL MULTI-LEVEL AUTHENTICATION SYSTEM USING TRIGON AND HYPER CHAOTIC LORENZ SYSTEM FOR SECURED COMMUNICATION

U. Latha
(Research Scholar, Department of Information Technology, Hindustan University, India.)

K. Ramesh Kumar
(Professor , Department of Information Technology, Hindustan University, India.)

ABSTRACT
The most authentication systems in our electronic society deals with knowledge based identification, token-based identification and bio-metric identification. The above mentioned identification methods are prone to vulnerable attacks when employed individually to an authentication system. Henceforth, in order to satisfy the society needs a novel method is developed by deploying knowledge based identification and bio-metric identification for a multi-level secured authentication system. The first level of our authentication system is knowledge based. The password is secured by trigon based method and it has been secured in both authentication server and backend server. The second level is using biometrics. Fingerprint authentication has been accepted throughout the world and is considered to be the most prominent biometric because of its characteristics such as universality, uniqueness and permanence. However, in terms of security measures the numerous fingerprint systems currently available still do not meet the stringent performance requirements of several important civilian applications. In that case a hyper chaotic system is developed with the 4D Lorenz system to encrypt the features extracted from the fingerprints. Such system is developed to with stand several side channel attacks when deployed in the real time applications.

Keywords token-based, bio-metric, Fingerprint, universality, civilian, hyper chaotic, 4D Lorenz

INTRODUCTION
The methods such as knowledge based identification; token-based identification and bio-metric identification are prone to vulnerable attacks when employed individually to an authentication system. In order to satisfy the society needs a novel method is developed by deploying knowledge based identification and bio-metric identification for a multi-level secured authentication system.
This system involves two levels of authentication

i) Password by Trigon based method
ii) Biometrics(Fingerprint) by hyper chaotic 4D Lorenz System

Trigon Method
The measurement of biological data is known to be Biometrics. The certification of an individual is done by investigating the physical characteristics such as fingerprints, handprints, eyes and voice, or the behavioral characteristics such as signature and the phrase biometrics are frequently used.
Fingerprint technology is the most broadly used technique in individual recognition and it has nearly become the synonym of biometrics.
A model that involves ridges and valleys is termed as a fingerprint image. Ridges are represented as dark lines while valleys are represented as light areas among the ridges.
Commonly ridges and valleys run corresponding to each other, and their patterns can be determined on a worldwide and local level. In the fingerprint pattern, minutiae are local discontinuities. Forged ridge arrangement may vary the individuality of input fingerprints. Ridges and valleys have a well-defined frequency and orientation in a local area form a sinusoidal-shaped plane wave. Massive numbers of fingerprints are captured and stored every day in a extensive range of applications such as forensics, access control, and driver license registration.
On the other hand, recognizing unfinished fingerprints from fingerprint database ruins a difficult challenge today. Emergence of incomplete fingerprint from a lot of scenarios can be found. Consequently, they may not provide accommodation for sufficient minutiae or ridge details for undertaking a normal matching process. As a result the repairing of incomplete regions in fingerprint images correctly and efficiently and thereby guaranteeing the subsequent matching and other processing has to be settled immediately. This paper describes the proposed fingerprint security protocol process.

Biometrics:

Identification of the user during authentication is a vital requirement for online web transactions. Shared secrets such as Personal Identification Numbers (PIN) or passwords and smart cards are not just enough for some applications. We require a dependable mechanism that could verify the person physically who is claimed to be. Biometric is one such technique that enhances the verification process in identifying the users. Biometric system allows the recognition of a live person based on his physiological characteristic or behavioral attributes.

Biometric authentication system primarily consists of two steps:

(i) Enrolment and
(ii)Authentication

Authentication formulates two functions namely verification and identification. Verification conducts one-to-one matching whereas identification looks for one-to-N matching. Though biometric based security system adequately improves the security of information over the other existing methods, security lapses still endure in this system and is vulnerable at various levels.

It is crucial to address the modification attack on the biometric database stored at the server side. As a step towards this direction, this paper has recommended N-sever based biometric authentication and key exchange (N-BAKE) protocol, which fortifies the authentication system against biometric database modification attack. The general framework of this paper is built on the fingerprint as a biometric for providing mutual authentication between the server and the user using threshold cryptography.

3D hyper chaotic system has two or more positive Lyapunov exponents, and the dynamic behavior of hyper chaotic system are more complex and difficult to predict. Hence, four-dimensional (4D) chaotic systems are widely studied, and adaptive control method for 4D chaotic systems also has been concerned. Other control methods are also developed such as feedback control, OGY method, sliding mode control, impulsive control and reduced-order adaptive control.

In this paper, based on the Lorenz chaotic system and another 4D hyper chaotic Lorenz system, a new 4D hyper chaotic Lorenz system is constructed and the basic dynamic behavior are studied, such as bifurcation diagram, symmetry, equilibrium point and stability, Lyapunov dimension and the impact of system parameters. Furthermore, based on Lyapunov stability theory, an adaptive controller is designed and the new 4D hyper chaotic Lorenz system is controlled at equilibrium point via the adaptive control method. Numerical simulation results are presented to illustrate the effectiveness of this method.

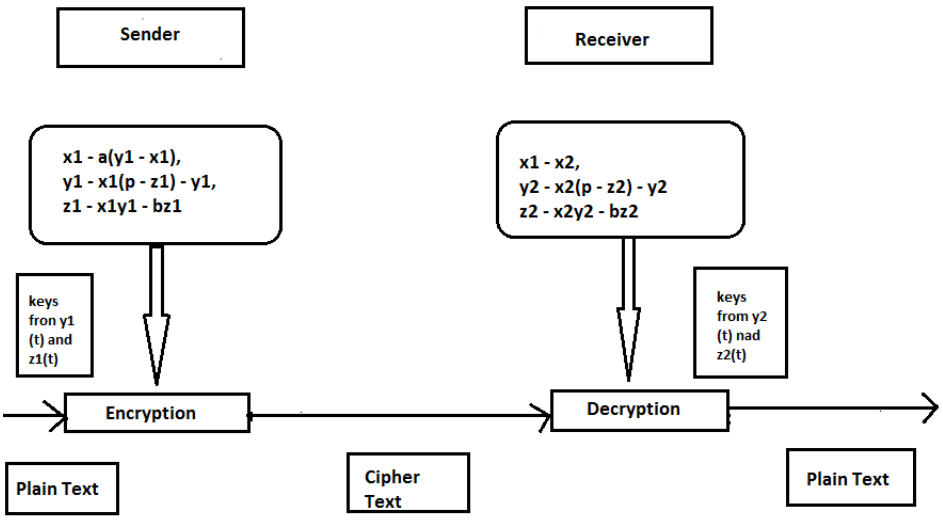


Figure 1. An illustration of generating the keys from a master-slave type of a synchronous chaotic system

Hyper Chaotic Lorenz System:

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. 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 -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.

Registration Process:
The 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.

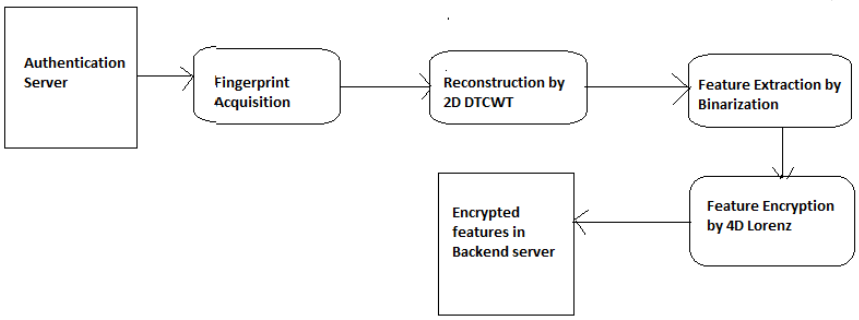


Figure 2. Architecture for fingerprint encryption

Authentication System:
The authentication system includes some common blocks which are used in registration process as shown in Fig2. 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.

PROPOSED SECURITY PROTOCOL
The proposed security system comprised of three phases, namely, fingerprint image reconstruction, feature extraction and development of security protocol. In our proposed system, the given input fingerprint image is reconstructed by the DTCWT and that reconstructed image features are extracted by the morphological operations. The extracted features from the fingerprint images are stored in the feature database and that database information is need to be protected from the unauthorized users. Hence, we provide a security for the fingerprint information by developing a trigon based security protocol using the valid user's username and password.

Fingerprint Image Reconstruction
The given input fingerprint image is to be reconstructed by decomposing the input cracked fingerprint images via 2D DTCWT. The reconstructed image is obtained by analyzing the sub band and the coefficients form the wavelet transform in different direction.

The steps for fingerprint reconstruction is,

(i) Initial Value Assignment by NN algorithm

(ii) 2D DTCWT Processing

(iii) Coefficients Thresholding and

(iv) Reconstruction

The value assignment process is initiated by finding the closest entries and replaced by the Nearest Neighbor (NN) algorithm. The fingerprint image is given to the wavelet process after the initial value assignment process. The M-band 2D dual Tree Complex Wavelet Transform (DTCWT) is used in our proposed technique which contains the unique geometrical features for frequency domain conversion. Local, multi-scale directional analysis is provided by this decomposition. We get the M-band trees obtained by performing two M-band multi resolution analyses in parallel in the real case, or four in the complex case respectively. The coefficients values are acquired from the wavelet transform and then the thresholding process is performed by initially creating the diagonal matrix is obtained.

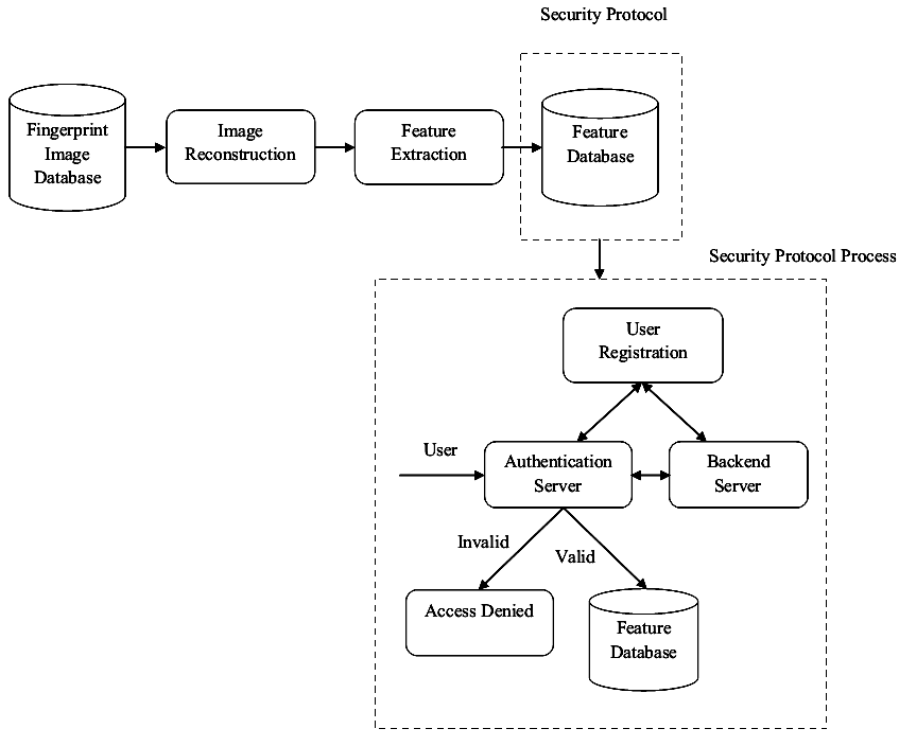


Figure 3. Structure of Our Proposed Security System

FEATURE EXTRACTION

After the image reconstruction process, the features are extracted from the fingerprint reconstructed images. The features extraction process is performed in two steps, namely, binarization and morphological operations. Before the binarization process the reconstructed fingerprint images are given to the segmentation and image enhancement process. In segmentation the image is divides into number of blocks and in each block the gradient value is calculated. Based on the gradients standard deviation and the threshold values the blocks values are filled with ones or zeros. Thus the segmented image is given to the image enhancement process to get the accurate minutiae point extraction. The segmented and enhanced image is provide to the binarization process.

Binarization

Binarization is the process of converting a grey level image into a binary image. It improves the contrast between the ridges and valleys in a fingerprint image, and thereby facilitates the extraction of minutiae. The output of binarization process is a binary image containing two levels of information, the foreground ridges and the background valleys.

Morphological Operation

Following the binarization process, morphological operators are applied to the binarized fingerprint image. The objective of the morphological operations is to eliminate obstacles and noise from the image. Furthermore, the unnecessary spurs, bridges and line breaks are removed by these operators. The process of removal of redundant pixels till the ridges become one pixel wide is facilitated by ridge thinning. The resultant fingerprint image produced by the morphological thinning algorithm composes of ridges each one pixel wide. This improves the visibility of the ridges and enables effective and effortless of minutiae points.

DEVELOPMENT OF TRIGON BASED SECURITY PROTOCOL

The trigon based security protocol is developed to protect the fingerprint feature information from the invalid users. The feature values i.e. the ridges values from the feature extraction process are stored in the feature database *fD*. The database *fD* comprised of three fields $fD = \{un, pn, Rn\}$ where *un* is the given input fingerprint image corresponding user name, *pn* denotes the password, *Rn* is the image ridge values and *n* represents the total number of users images. Based on the corresponding fingerprint image users, username and password the security protocol is to be developed.

The trigon based security protocol is composed of three steps,

(i) Registration process
(ii) Users Verification
(iii) Validation

Registration Process:

During the registration process, the valid users register their username and password in Authentication and Backend server. Initially, the database users register their username and password in the authentication Server. At that time, the Authentication server randomly generates two prime numbers $n1$, $n2$, which are considered as the two sides of a trigon. The angle between these two prime values $n1$, $n2$, is denoted as *ai*. Now, the authentication server can easily determine the opposite side of the angle *ai*, termed Units as $n3$. With these trigon parameters, the user determines *s*, $n1n2\ V$ and $n1n2\ P$ as follow where $n1$, $n2$ and $n3$ and are the three sides of the trigon, *s* is a strengthening parameter used as the index to represent user credentials, $n1n2\ V$ and $n1n2\ P$ are the Variance and the product of the sides $n1$ and $n2$ respectively. After the calculation of these 654 values, the Authentication Server stores the *s* and forwards the $n1n2\ V$ and $n1n2\ P$ to the Backend Server along with the username.

Users Verification:

After the valid users registration process, if any user enter to access the fingerprint information from the database *fD* means, the Authentication server checks whether the corresponding queried user is a valid user or not. The process of user's verification by the Authentication server is described below,

Step 1: Authentication Server gets the user name *un* and password *pn* from the nth user
Step 2: Authentication Server computes the key value for the password 10
Step 3: After that the Authentication server send the *sn* is sent to the backend server along with *un.*

Validation:

In validation, the backend servers validate the information from the Authentication Server. The backend Server receives the *sn* and the username *un* from the Authentication Server. After receiving the *sn* and *un*, Backend server searches the *sn* corresponding $n1n2\ V$ and $n1n2\ P$ values, which have been already stored in the server database during the registration. Based on the corresponding user values in Backend Server, computes the authentication

Token *ATn* and sends it to the Authentication server to authenticate the *ui*. The authentication server authenticates the user based on the token from the Backend server and the key value is calculated at the Authentication server. If the condition is satisfied means thus the given user is valid to access the feature database otherwise the access is denied.
They are allowed to access the feature database *fD*. By exploiting the aforementioned process our proposed trigon based security protocol protects the fingerprint information from the unwanted users.

HYPOTHESIS OF BIOMETRICS (FINGERPRINT):
The following assumptions have been made for design the proposed routing protocol

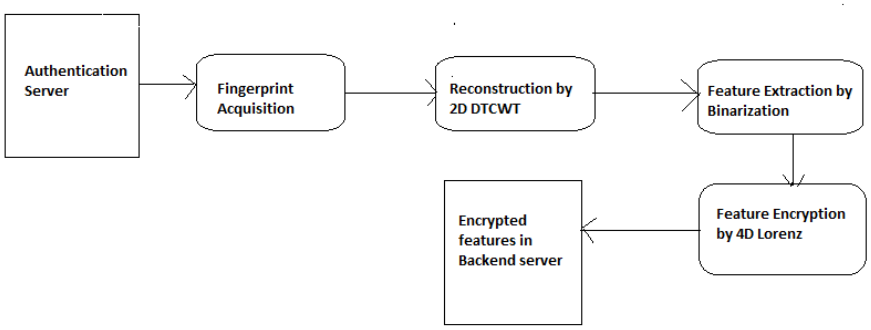


Figure 3: Architecture for fingerprint encryption

Extracted Feature Values

Image	Feature Values
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), (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)

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

$$\begin{vmatrix} X' \\ Y' \\ Z' \end{vmatrix} = \begin{vmatrix} a11 & a12 & 0 \\ a21 & a22 & 0 \\ 0 & 0 & a33 \end{vmatrix} \begin{vmatrix} X \\ Y \\ Z \end{vmatrix} + X \begin{vmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{vmatrix} \begin{vmatrix} X \\ Y \\ Z \end{vmatrix}$$

Now, introduce an additional state, u, and couple it to the second equation of the chaotic system, thereby obtaining a fourth-order system, where k is a constant to be determined later. Notice that the modified system satisfies the criteria for hyper chaos. As a result, system 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 is illustrated, as usual, mainly numerically.

$$\begin{vmatrix} X' \\ Y' \\ Z' \\ u' \end{vmatrix} = \begin{vmatrix} a11 & a12 & 0 & 0 \\ a21 & a22 & 0 & 1 \\ 0 & 0 & a33 & 0 \\ -k & 0 & 0 & 0 \end{vmatrix} \begin{vmatrix} X \\ Y \\ Z \\ u' \end{vmatrix} + X \begin{vmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{vmatrix} \begin{vmatrix} X \\ Y \\ Z \\ u' \end{vmatrix}$$

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

$$\begin{aligned} X' &= F(x, y, z, w); \\ Y' &= G(x, y, z, w); \\ Z' &= Q(x, y, z, w); \\ W' &= P(x, y, z, w); \end{aligned}$$

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, 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. In this work, we are interested in the hyper chaotic Lorenz system modeled as follows:

$$\begin{aligned} X' &= a(y-x); \\ Y' &= x(b-z) - y + w; \\ Z' &= xy - cz; \\ W' &= - fx; \end{aligned}$$

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 the final system, 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, making the following changes for the system, 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:

$$\begin{aligned} X' &= a(y - x); \\ Y' &= cx - xz - y + ew; \\ Z' &= x^4 + y^4 - bz \\ W' &= -dy \end{aligned}$$

There are five parameters in this new 4D hyper chaotic Lorenz system; they are more than two parameters for the Lorenz system. The nonlinear term in the third state equation of system is x4+y4 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.

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.

$$f(\Lambda) = (\Lambda + b)\,(\Lambda^3 + a_1\,\Lambda^2 + a_2\,\Lambda + a_3) = 0$$

During each iteration set 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 the point of fv for a, b, c and d
apply in 4D Lorenz State Eqn. As
X-coordinate in a,
Y-Coordinate in b,
Direction Θ in c,
ASCII value of Type of minutiae in d
and e is generated randomly
if (Lyapunov exponents satisfy the **4D hyper chaotic Lorenz** system conditions)
update new feature values (fvnew)
else adjust parametric values
endif end **for**

Steps for Encryption and Decryption:

a. Load the original binary image and extracted feature values.
b. *X-coordinate in a,Y-Coordinate in b, Direction Θ in c, ASCII value of Type of minutiae in d is* given as input.
c. Random number e is generated.
d. Apply feature values a, b, c and d along with random number e in 4D Lorenz state equation.
e. 4 Lyapunov exponents are got as output.
f. If Lyapunov exponents satisfy the hyper chaotic Lorenz system conditions then
g. Update the new feature values , otherwise
h. 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 set 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.

FINGERPRINT TESTING

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.

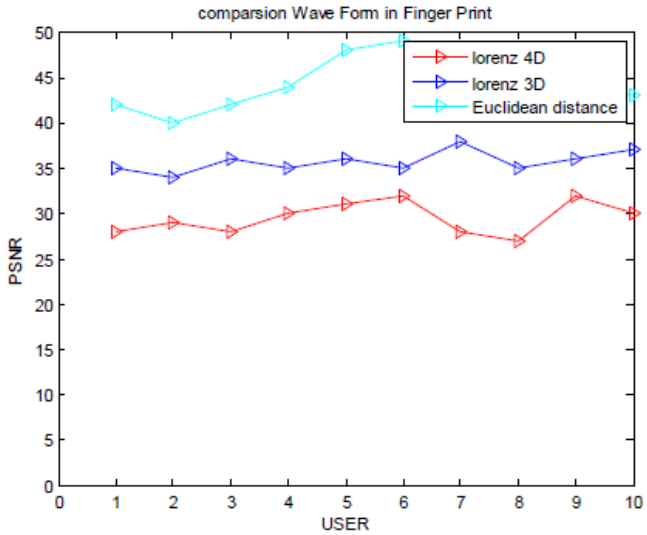
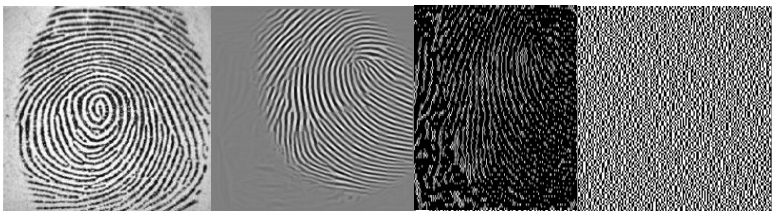


Figure 4: Comparison Wave Form in fingerprint

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)

Figure 5: Euclidean Distance Method:
(a) Input Image 101_1
(b) Enhanced Image
(c) Minutiae Detection



a) b) c) d)

Figure 6: 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.

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.

EXPERIMENTAL RESULTS AND DISCUSSION

Initially the given sample fingerprint images from the fingerprint database FVC 2002 are reconstructed by the DTCWT technique. The sample fingerprint and the reconstructed results images are shown in Fig.7 and Fig.8.

Figure 7. Sample Fingerprint Images

Figure 8. Reconstructed Image Results

a) b) c) d) e)

Figure 9. Result Images from Feature Extraction (a) Segmentation (b) Image enhancement (c) Morphological Operation (d) Minutiae Extraction and (e) Final result

The extracted feature values from the fingerprint images are stored in the feature database and that the database information is protected by our security protocol. The protocol is tested with five valid and five invalid users. Each of the five valid users has their own username and password. Initially, the user registration process is performed to evaluate the valid and invalid users in the feature database access. The fingerprint images and the corresponding username, password and trigon parameters of the five users are given. Usernames, Passwords and the trigon parameters at the time of registration

Number of users
User Name
Password ***s*** *n*1*n*2 *V n*1*n*2 *P*

1 U1 Hello -25 -5 14
2 U2 WELCOME 1.60E+01 4 77
3 U3 HAI 0 0 49
4 U4 Rose 2.50E+01 5 14
5 U5 sample -25 5 14

The five valid user's username, password and trigon parameters have been given in Table.1. These five users are the valid users to access the feature database. The values for the five valid users mentioned have been stored in the authentication server and *aa*'
V and *aa*'*P* have been stored in the Backend server for the corresponding usernames. When the servers authenticate any user, the servers determine some authentication elements based on the values which have been stored in the database and the login credential provided by the user. Our proposed security protocol performance result of five valid and invalid users' authentication elements and that database access is given.
Ten users can try to access the feature database *fD*. Among the ten users five users are authenticated and other users are unauthenticated users. The authenticated five user's authenticated elements are computed and verified by the authentication and backend servers. Based on the verification result from the both servers, the users are allowed to access the feature database. Other five users try to access the database by giving wrong passwords but the passwords are most similar to the authenticated user's password.

Table 1: Minutiae Data Extract from Figure 5(c)

X	Y	Minutiae Detection
230	86	2.364418605
206	126	1.324920635
138	147	0.62877551
137	163	0.530490798
227	173	1.002138728
205	174	0.86816092
162	176	0.610454545
106	185	0.262972973
243	187	0.989465241
102	202	0.194950495
163	211	0.462511848
207	248	0.524677419
181	252	0.408253968
131	260	0.193846154
146	262	0.247251908
232	268	0.555671642
168	270	0.312222222

Table 2: **Minutiae Data**

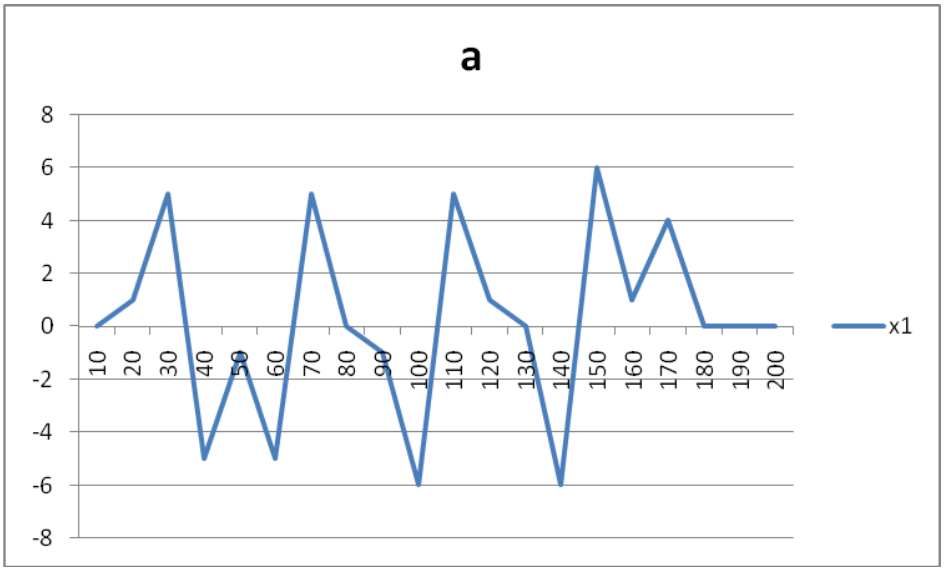
Minutiae Detection	Elapsed time	Encryption time	Decryption time
2.26	0	25	0
1.32	15	10	-3
0.63	-5	35	2
0.53	-4	18	1
1.1	-11	30	3
0.87	1	12	-2
0.61	0	31	2
0.27	10	13	-2
0.99	0	29	2
0.2	1	10	-2
0.47	-19	35	-1.8

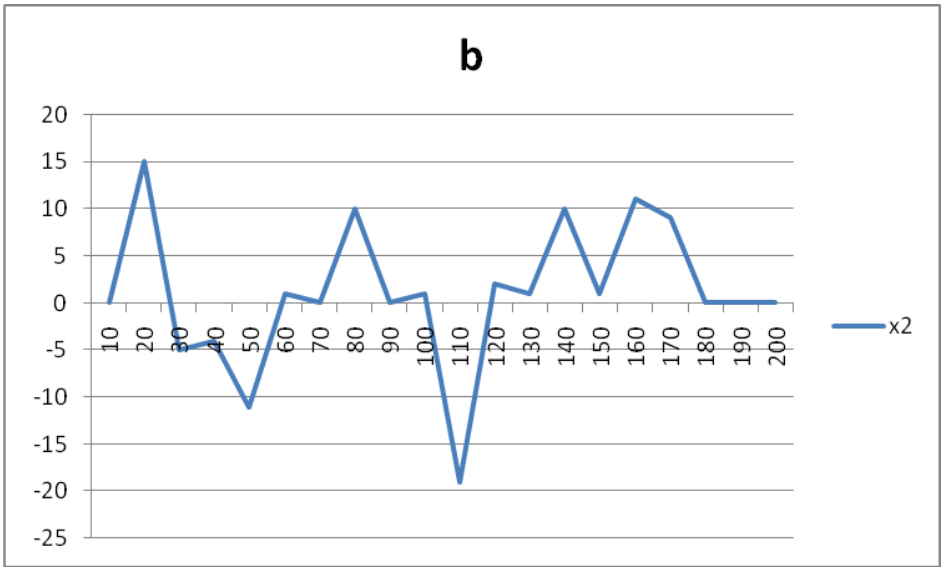
0.53	2	19	-2
0.49	1	30	-1
0.2	10	5	0
0.25	1	39	0
0.56	11	20	0
0.31	9	30	0
0	0	18	0
0	0	25	0
0	0	0	0

Table 3: **The status retorts of the controlled hyper chaotic 4D Lorenz system.**

x1	**x2**	**x3**	**x4**
0	0	25	0
1	15	10	-3
5	-5	35	2
-5	-4	18	1
-1	-11	30	3
-5	1	12	-2
5	0	31	2
0	10	13	-2
-1	0	29	2
-6	1	10	-2
5	-19	35	-1.8
1	2	19	-2
0	1	30	-1
-6	10	5	0
6	1	39	0
1	11	20	0
4	9	30	0
0	0	18	0
0	0	25	0
0	0	0	0

The chaotic attractor of hyper chaotic 4D Lorenz system is given in Figure . The system state responses trajectory of controller design is shown in Figure . When t=20 sec, it is obvious that the feedback control gain can guarantee stable of hyper chaotic 4D Lorenz. From the simulation results, it is shown that the proposed controller works well to guarantee stable.


a
8
6
4
2
0
-2
-4
-6
-8
10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200
x1


b
20
15
10
5
0
-5
-10
-15
-20
-25
10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190 200
x2

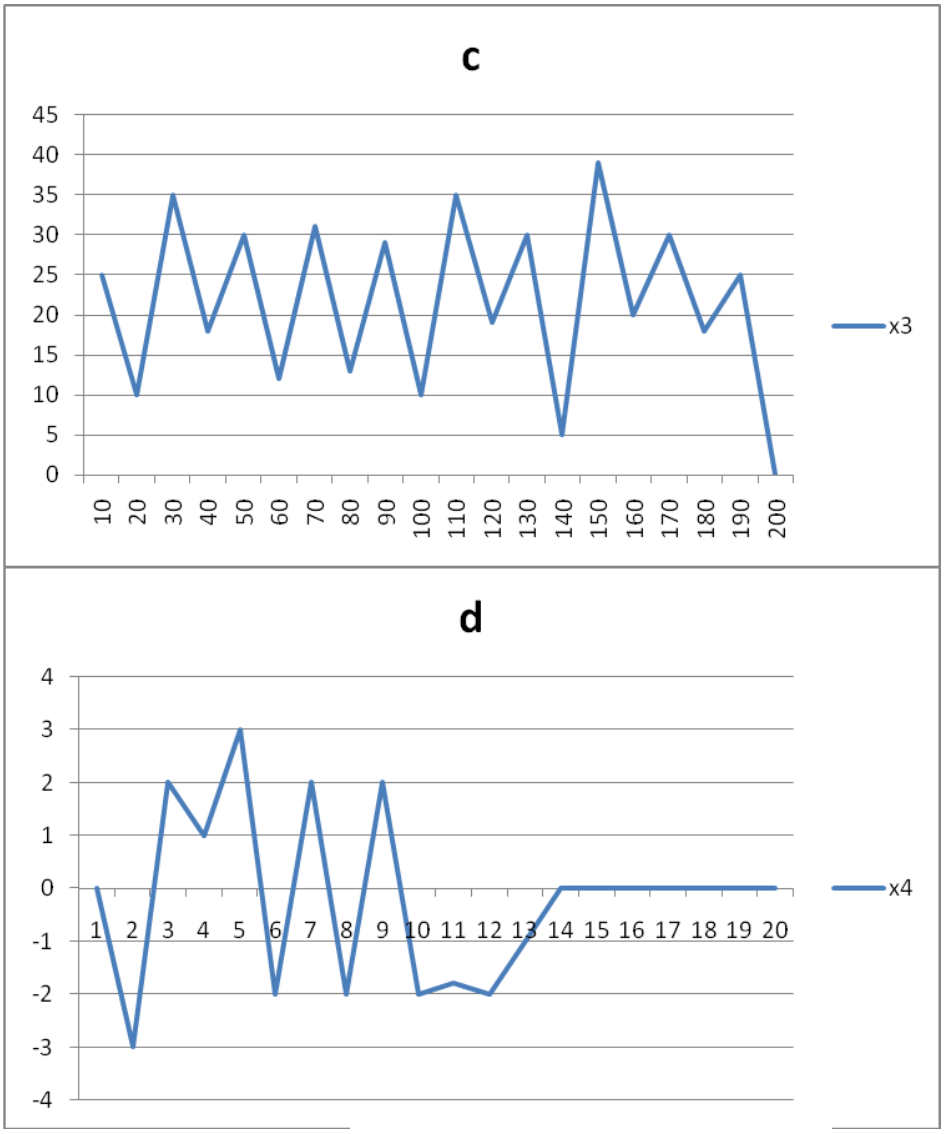


Figure 10: **(a,b,c,d) The status retorts of the controlled hyper chaotic 4D Lorenz system.**

After the finger has been detected in the image frame from, the application extracts the finger features from the image, converts it into a template with format discussed earlier, and goes through a loop to try to match the template with an existing template in the database. The index used to detect the threshold for the similarity between two templates (of each step in the loop) is called the False Rejection Rate (FRR) or False Acceptance Rate (FAR) respectively.

The FRR is approximately inversely proportional to FAR but might tend to be exponential at the extreme values. FAR is the acceptable error rate, to which two fingers are allowed to have similar features. FAR being an error should be kept as low as possible to increase accuracy and also taking the Rate of recognition into consideration. The FRR being reliability should be kept as high as possible to increase matching accuracy, and taking the rate of recognition into consideration. The FAR and FRR can be used alternatively without any form of setback or uncertainty, depending on representation preference. Table 2 and Table 3 shows the tests carried out by varying the values of the FAR and FRR of the application.

Table 4: False Acceptance Rate (FAR)

FAR (%)	Matching (approx.%)	Accuracy	Recognition Rate (%)

1	60	99
0.5	70	90
0.1	85	85
0.05	95	70
0.001	98	40
0.005	99	10

Table 5: False Rejection Rate (FRR)

FRR (%)	Matching Accuracy (approx. %)	Recognition Rate (%)
100	99	30
50	75	65
40	70	70
20	50	85
10	45	88
1	20	99

CONCLUSION

In this paper, we have proposed a trigon based security protocol to protect the fingerprint information from the prohibited users. The proposed fingerprint security protocol performance was evaluated by using the more number of fingerprint images. The experimental results proved that our proposed trigon based fingerprint security protocol has given high performance security when protect the fingerprint information from the illicit users. The proposed trigon based protocol performance in protecting fingerprint information was tested with authenticated and unauthenticated users. When the unauthenticated users try to access the feature database, our proposed security protocol eliminates their access based on their authenticated elements. Hence, it is proved that our proposed trigon based security protocol more securely protect the information from the illegitimate users. The authenticated elements are also computed for these unauthenticated users and verified by the authentication and backend servers. The servers easily find out these invalid users by comparing those users with the authenticated users. Thus our trigon based security protocol more secure in protecting the fingerprint information from the unwanted users. 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

Si Gang-Quan, Cao Hui, Zhang Yan-Bin., A new four-dimensional hyperchaotic Lorenz system and its adaptive control, Chin. Phys. B Vol. 20, No. 1 (2011) 010509.

Rajeswari Mukesh, Komathy,K., N-bake: Fingerprint Authentication Against Biometric Database Attack, Journal of Computational Information Systems 8: 24 (2012) 10315-10324.

Latha, U, Ramesh Kumar K., A Strong Security Protocol Against Fingerprint Database Attacks, ICTACT Journal On Image And Video Processing, August 2013, Volume: 04, Issue: 01, 652-656.

Jing WANG, Jingcui LI, Liulin CAO. \An Improved Fast Thinning Algorithm for Fingerprint Image and Its Application", Journal of Computational Information Systems 7: 7 (2011), pp. 2285-2292.

S. Prabhakar, S. Pankanti, A. K. Jain. Biometric Recognition: Security and Privacy Concerns, IEEE Security & Privacy Magazine 1 (2003), pp: 33-42, 2003.

A. K. Mohapatra, Madhvi Sandhu. \Biometric template Encryption", International Journal of Advanced Engineering & Application, Jan. 2010, pp. 282-284.

Islam, M. NEncryption and multiplexing of ngerprints for enhanced security , IEEE Proceeding of Systems, Applications and Technology Conference (LISAT), May 2011, pp. 1-4.

William Stallings. Cryptography and Network Security, Principles and Practices", 4th edition.

D. Boneh. The Decision Die Hellman Problem", Proc. Third international Algorithmic Number Theory Symposium., pp. 48-63, 1998.

Alvarez, G., Montoya, F., Romera, M. & Pastor, G. [1999b] "Chaotic cryptosystems," in L. D. Sanson, ed., Proc. 33rd Annual 1999 International Carnahan Conference on Security Technology, 332– 338(IEEE).

Alvarez, E., Fernandez, A., Garcia, P., Jimenez, J. & Marcano, A. [1999a] "New approach to chaotic encryption," Phys. Lett. A 263, 373–375.

Kocarev, L. [2001] "Chaos-based cryptography: A brief overview," IEEE Circuits and Systems Magazine 1, 6–21.

K. Rahul, "Estimation of all model parameters of chaotic systems from discrete scalar time series measurements," Physics Letters A, 346 (4) (2005), pp. 275–280.

Kocarev, L. [2001] "Chaos-based cryptography: A brief overview," IEEE Circuits and Systems Magazine 1, 6–21.

Wong, W.-K., Lee, L.-P. & Wong, K.-W. [2001] "A modified chaotic cryptographic method," Comp. Phys. Comm. 138, 234–236.

Muna F. Hanoon, "Contrast Fingerprint Enhancement Based on Histogram Equalization Followed by Bit Reduction of Vector Quantization", International Journal of Computer Science and Network Security, Vol. 11, No. 5, pp. 116-123, 2011.

Rajesh, M., and J. M. Gnanasekar. "Path observation-based physical routing protocol for wireless ad hoc networks." International Journal of Wireless and Mobile Computing 11.3 (2016): 244-257.

Rajesh, M., and J. M. Gnanasekar. "Congestion control in heterogeneous wireless ad hoc network using FRCC." Australian Journal of Basic and Applied Sciences 9.7 (2015): 698-702.

Rajesh, M., and J. M. Gnanasekar. "GCCover Heterogeneous Wireless Ad hoc Networks." Journal of Chemical and Pharmaceutical Sciences (2015): 195-200.

Rajesh, M., and J. M. Gnanasekar. "CONGESTION CONTROL USING AODV PROTOCOL SCHEME FOR WIRELESS AD-HOC NETWORK." Advances in Computer Science and Engineering 16.1/2 (2016): 19.

Rajesh, M., and J. M. Gnanasekar. "An optimized congestion control and error management system for OCCEM." International Journal of Advanced Research in IT and Engineering 4.4 (2015): 1-10.

Rajesh, M., and J. M. Gnanasekar. "Constructing Well-Organized Wireless Sensor Networks with Low-Level Identification." World Engineering & Applied Sciences Journal 7.1 (2016).

Rajesh, M. "Traditional Courses Into Online Moving Strategy." The Online Journal of Distance Education and e-Learning 4.4 (2016).

Brendan Babb, "Evolved Transforms Surpass the FBI Wavelet for Improved Fingerprint Compression and Reconstruction", Proceedings of the GECCO Conference Companion on Genetic and Evolutionary Computation, pp. 2603-2606, 2007.

Anitha K. K, Sudha S. G., Megala A and Aishwarya S, "Trigon Based Authentication Service Creation with Globus Middleware", Proceedings of the International Conference on Process Automation, Control and Computing, pp. 1-6, 2011.

Jie Zhang, Bo Zhang, Xinjing Liu and Xiaojun Jing, "A Matching-Improved Reparation Method for Incomplete Fingerprint", Proceedings of IEEE International Conference on Cloud Computing and Intelligence Systems, pp. 75-79, 2011.

Poramate Prasarn, Keokanlaya Sihalath and Somsak Choomchuay, "A dynamic enhancement method for fingerprint matching", The 3rd Biomedical Engineering International Conference, pp. 237-241, 2010.

Muhammad Umer Munir and Muhammad Younas Javed, "Fingerprint Matching using Gabor Filters", National Conference on Emerging Technologies, pp. 147-151, 2004.