American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-7, Issue-5, pp-183-199
www.ajer.org
Research Paper Open Access

Improving Privacy And Security Of Multi Biometric Fingerprint By Combining Orientation Fields With Wavelet And Cryptographic Algorithms In Ethiopian Banking Sector

[*1]Dr. N. Satheesh Kumar, [@2]Mr. Tibabu Beza, [#3]Mr. Gulelat Abebe
[*1] *Asso. Professor, Computer Science and Engineering Program, Adama Science and Technology University, Adama, Ethiopia.*
[@2] *Lecturer, Computer Science and Engineering Program, Adama Science and Technology University, Adama, Ethiopia.*
[#3]*Lecturer, Computer Science and Engineering Program, Adama Science and Technology University, Adama, Ethiopia.*
Corresponding Author: Dr. N. Satheesh Kumar

ABSTRACT: *Protecting the data by recognizing the fingerprint is one of the active research area nowadays. We are using biometric recognition like fingerprint to enhance the privacy and security.It became one among the most eminent identification system to identify the personnel in forensic labs like investigations, identifying the terrorists and national security issues. That is the reason, this technique becomes very popular, itis highly not possible to protect the fingerprint data with the traditional encryption techniques. The attacker may track the fingerprint image when it is decrypting if the methodology we are using for this is not so strong especially in banking sector. Therefore, significant efforts are needed to developspecific protection techniques for fingerprint for banking sector.*

In this research paper, we are considering the problem of combining two fingerprint images i.e. multi biometric to generate a new cancelable fingerprint and the combined mixed template was used to generate keys using wavelet, water marking and cryptographic algorithms. The mixed image which is to be generated consisting the properties of the both finger prints images. This mixed image will be kept in the database for future use.

Some of the banks are using biometric methods to protect the data from the internal employees. But the present methods are not upto the level of current cryptographic models. The hackers are always trying to attack the banking servers by seeking the help from internal and external human resources when it is connected to internet. In this context, we are trying to provide extra protection and privacy for the data which is available in the banking servers by multi biometric finger print.

Keywords: *Wavelet, Cryptography, Orientation, Multi Biometric*

Date of Submission: 27-04-2018 Date of acceptance: 12-05-2018

I INTRODUCTION

Biometrics is a technique used to identify, analyze, and measure a persons physical and behavioral properties [1]. We can easily identify a person with the ease of biometric in faster manner when we compare with the traditional methods like traditional knowledge based technique. The identification process may include

- Authentication Identification
- Verification
- Authorization

In general, a biometric system may be represented by four basic components as in figure 1.

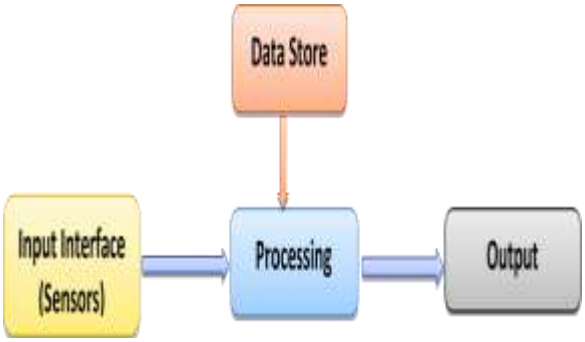

Figure 1. Basic Biometric System

Types of Biometric Modalities:

The table illustrates the different modalities –

Physiological Modality	**Behavioral Modality**	**Combination of Both Modalities**
This modality deals with the shape and size of the body. For example – • Fingerprint Recognition • Facial Recognition • Iris Recognition • Retinal Scanning • DNA Recognition	This modality is to identify the change in human behavior for a particular period of time. For example – • Walking style • Frequency in typing keys • Signature	This modality includes physical along with behavioral changes. For example – • Voice Recognition • It depends on health, size, and shape of vocal cord, nasal cavities, mouth cavity, shape of lips, etc., and the emotional status, age, illness behavior of a person.

A fingerprint refers to the flow of ridge patterns in the finger. The flow of ridgeexhibits anomalies in local regions of the fingertip (Figure 2), this position used to represent and match finger prints. The electronic era has ushered in a range of compact sensors that provide digital images of these patterns.

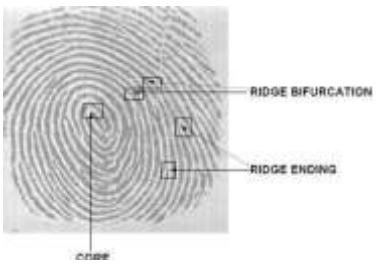

Figure 2. Ridge Flow

1.1. Finger print pattern types:

a) *Plain and Tented Arch***:** Plain Arch is a pattern that has ridges at one end, make a rise at the center, and tend to flow towards the opposite side as in Fig. 3

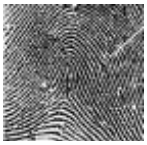

Fig. 3. Plain Arch

Tented Arch has resemblance to plain arch but, ridges create an angle or a steep thrust. It possesses some basic characteristics of the loop as in Fig. 4.

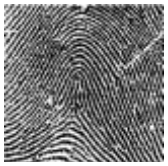

Fig. 4. Tented Arch

b) *Radial Loops and Ulnar Loops:* Ulnar loop pattern loops shown in Fig. 5 flow towards the little finger, while in Radial loop pattern as in Fig. 6, loops flow towards the thumbs.

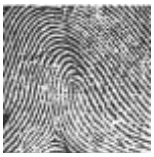

Fig. 5. Ulnar Loop

Fig. 6. Radial Loop

c) *Plain Whorl:* The imaginary line drawn between two deltas will touch or cross, at least one recurving ridge within the inner pattern area as in Fig. 7.

Fig.7.Plain Whorl

d) *Central Pocket loop Whorl*: It has a pattern with at least one recurving ridge as in Fig. 8. The imaginary line drawn between two deltas will not cut or touch the inner recurving ridge inside the pattern.

Fig.8.Central pocket loop whorl

e) *Double Loop Whorl*: It will be distinguished with two different loop formations. It is consists of two separate and distinct sets of shoulders and two deltas as in Fig. 9.

Fig.9. Double loop whorl

f) *Accidental Whorl***:** It is the only pattern which will be connected with minimum of two deltas. It unites two or more distinctive type of patterns excluding the plain arch as in Fig. 10 [7].

Fig.10. Accidental whorl

1.2. Biometric Banking Systems

Biometric in banking systems is an important solution to secure the transactions and prevent identity theft and fraud.

The use of biometrics in banking is increasing because more employees or costumers understand its potential as a predominant method of identifying themselves to get accessing of services from the banks like net banking, off line banking, ATM banking and banking from mobile.

Sophisticated technologies such as the use of biometrics for employee or customer identification are a major part of security strategies for financial services to secure information like individual details, personnel identity and provide a secure banking experience from anywhere.

II OBJECTIVES

The general objective of this research is to implement a fingerprint mixing method and add cryptographic algorithms in order to provide more security and privacy protection for the authorized user.
Following are the specific objectives of the research project:

- Collect different standard Fingerprint image database
- Perform preprocessing for the extraction of orientation and minutiae fields
- Apply the mixing mechanism to the extracted orientation and minutiae fields of two individual fingers.
- Apply the cryptographic algorithms to provide more security before storing into database.
- At the authentication phase compare the fingerprint template with the image available in the database. If matched it will accept the user otherwise it will reject.

III PROBLEM STATEMENT

Various banks in the country are using the finger print technology as a security tool to protect their data from unauthorized personals. But the finger print technique which is in usein present days are not meeting the full requirements of a particular bank. So there is a need of enhancing the security by incorporating more advanced techniques in the finger print technology to provide more security and privacy.

IV. RESEARCH METHODOLOGY

1.3. Research Design

A multi biometric fingerprint recognition systemcontains fingerprint acquiring device, minutia extractor.

Figure 11 A Simple Fingerprint Recognition System

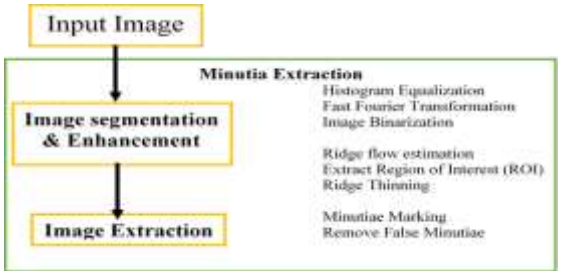

Figure 12Minutia point Extraction

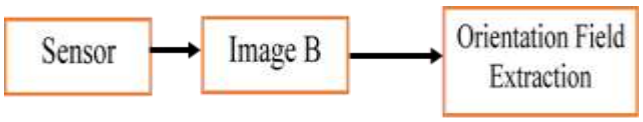

Figure 13 Fingerprint Recognition System with Orientation Field Extraction

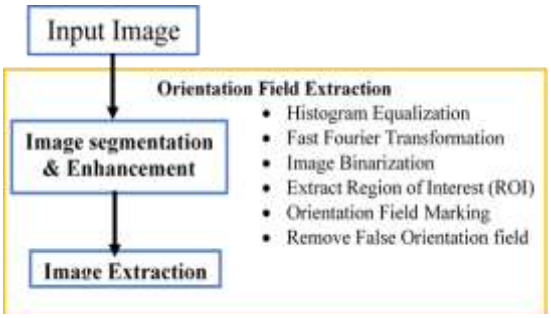

Figure 14 Orientation Field Extraction

In our proposed research, recognition system will do preprocessing along with extraction. The fingerprint images have to be selected in random basis and then it will combine them into a common template. The following figure describes the complete process of mixing two finger prints into single image, so that the newly formed image is used to check the whether the person is authorized or not.

In the enrollment phase, the proposed system accepts two fingerprint images as input from two different fingers, let us consider fingerprints 1 and 2 respectively. From the finger print 1 (Input 1) it will extract the minutiae positions and orientation points from finger print 2 (Input 2). By using the extracted minutiae and orientation points from the two different finger prints, the system will generate combined template.

At last, the generated mixed template has to send to the database and will be used during authentication process. Similar to the enrollment, in the authorization phase we extract the minutiae points or positions and orientation points from input 1 and input 2. Now compare this information with the mixed template available in the database. If matched the authentications is considered as successful otherwise that particular transaction is unsuccessful.

In this phase we are going to be testing or evaluating the various algorithms for the best suitable algorithm to our research which is able to solve the customer needs. The selection of this algorithm has to select depending on where we are going to implement the system. That means the data protection techniques may be varied from bank to bank, depending on their requirement we need to apply the set of algorithms to reach the objectives which are specified in this proposal. Similarly the concept of the wavelets is to be used to mix the multiple finger prints with orientation fields.

The step by step process is

In Enrollment or registration Phase:

- Scans the fingerprints from two fingers of the user
- Extract minutiae points from the first finger
- Extract orientation point's field from the second finger.
- Perform encoding and apply the cryptographic algorithms on the generated template.
- Then store the template in the database.

At Authentication Phase:

- Collect fingerprints from two fingers of the user
- Extract minutiae points from the first finger
- Extract orientation field from the second finger.
- Perform decoding and apply the decryption algorithms on the generated template.
- Then compare the generated template with template available in the database.
- Perform fingerprint verification, if it is matched then the user is allowed otherwise it will be rejected.

1.4. Design and Development

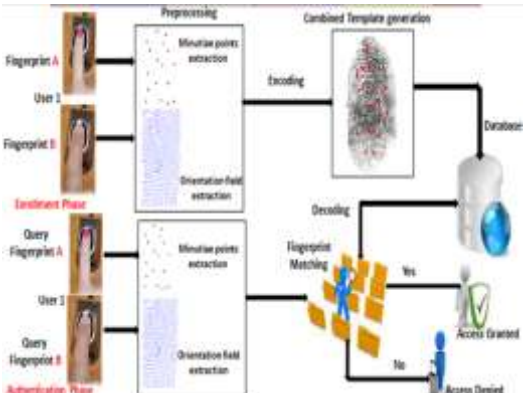

Figure 15: Proposed block diagram

Every person has unique finger prints and is a pattern of combining valleys along with ridges. This uniqueness is determined by relationships among the ridge characteristics in that region. A high quality fingerprint may contain minutiae points in between 40 to 100. Fingerprint recognition, is an application in pattern recognition, and is used in security to identity authentication. In matching the finger print there are three approaches called the matching based on correlation, matching based on minutiae and matching based on ridges. Among these, matching based on minutiae is widely accepted algorithm.

4.3. *Multi Biometric Fuzzy Vault*

4.3.1. Pre-processing

Multi biometric vault provides better recognition performance and higher security compared to a uni-biometric vault. While multi biometric systems overcome limitations such as non-universality and high error rates that affect uni-biometric systems, they require storage of various templates for the single user. Fuzzy vault is used typically to secure fingerprint templates. It is not feasible solution to secure various templates separately which belongs to single user in terms of security. To overcome this sort of problems, we are proposing methodology to secure multiple templates of a single user by creating multi biometric fuzzy vault. Multimodal biometric scheme will use multiple i.e. more than one biometric identity of a person to authenticate. The performance of the proposed system will be compared single model biometric system. The proposed multi biometric fuzzy vault contains the combined feature points from finger print 'A' and fingerprint 'B'. Initially, the enrolled image is preprocessed with the following steps.

i. Binarization
ii. Thinning
iii. Minutiae extraction
iv. Bifurcation
v. Termination
vi. Region of interest (ROI)

i)*Binarization:* The ridges in the fingerprint 'A' and finger print 'B' images are represented with black color and on the other side furrows are represented with white color. It transforms the 8-bit Gray image into a 1-bit by representing ridges as '0' and furrows as '1' as in figure 2.

Fig 16: Binarizing the fingerprints A and B

*ii) Thinning***:** Ridge thinning is to remove the pixels which are redundant from the ridges until it become wide of one pixel. The following figure will demonstrate the thinning images of both fingerprints A and B.

Fig 17: Demonstrating the thinning process

*iii) Minutiae extraction***:** A minutiae descriptor consists of ridge orientation and frequency at 76 equidistant points, uniformly spaced on 4 circles around minutiae. The four concentric circles, with radius 26, 44, 62 and 80 pixels, contain 9, 15, 21 and 27 points, respectively. The radius along with the number of points on every circle are opted in such a way that the values of descriptor capture the maximum information available in the neighborhood of minutiae. Here both bifurcation and termination of ridges in both the fingerprint 'A' and finger print 'B' are taken.

Fig 18: Extracting the minutiae points

To design a minutia extractor, a three-phasemechanism is used. These stages are preprocessing, extracting minutia and post processing phase. The following flowchart determines the algorithm for Minutiae extraction. Orientation field is generated which not only shows the angle formed by ridge. It also shows the directions of ridges in the fingerprint image.

Fig 19: Demonstrating the orientation field

iv)Region of Interest (ROI): Region of Interest is useful for the recognition of each fingerprint image. The image area which is not having the active ridges as well as furrows will be discarded. It depends on the locations of minutiae and the directions of ridges at the minutiae location. False minutiae are affecting the accuracy of matching. So, removing false minutiae are essential to keep the system effective.

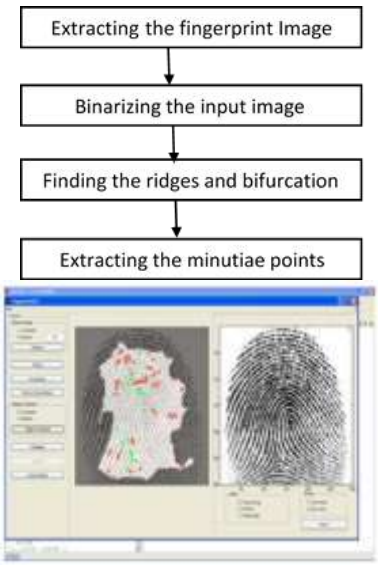

Fig 20: Identifying the region of interest

4.4. Orientation and Reference Point Detection:

Orientation involves the calculation of image gradient that is change of ridges in x and y direction. So calculate the image gradient in x and y direction. Reference point is the global feature of the fingerprint. It involves core and delta point. Core is the U turn in ridge pattern and Delta is a Y shaped ridge meeting. These are the singular points [SP].The detection of singular point for all the three finger print is proposed with the use of complex filters. The following process shows the detection of singular points:

a. Using existing orientation estimation algorithm, we can obtain the orientation OF of the fingerprint image. The orientation computed is then expressed in the complex domain Z, where

Z = cos(2OF) + j sin(2OF) ------(1)

We can identify the centroid of the reference point by calculating the certainty map of reference points.

$A_{ref} = Z * T_{ref}$ (2)

T_{ref} is the conjugate of T_{1ref} where "*" denotes the convolution operation.

$$T_{1ref} = (x + iy)\frac{1}{2\pi\sigma^2}.exp\left[-\frac{x^2+y^2}{2\sigma^2}\right] \quad (3)$$

b. The improved certainty map is calculated from T_{ref}

$$A'_{ref} = \begin{cases} A_{ref}.\sin\left(Arg(A_{ref})\right) & if\ Arg(A_{ref}) > 0 \\ 0 & Otherwise \end{cases} \quad (4)$$

Where Arg(z) returns the principal value of the argument z and A'_{ref} is referred as the certainty value.

c. Step 4 is repeated until the reference points are identified

4.4.1. Orientation Estimation:

From the second fingerprint the orientation field has to be calculated. Least mean square algorithm is proposed for finding the orientation field. To find the orientation normalization of the fingerprint is required. Normalization can be done either locally or globally. The scheme consists of two steps.

*Local Normalization:*It will reduce the variations locally so that it is possible to estimate the local orientation. It can normalize all the values into a defined mean and variance. However, because of the quality of the different parts of the fingerprint image, using the global mean and variance for normalization may not be appropriate. Therefore, we propose using a local normalization to reduce local variations in gray level values.

*Local Orientation:*An orientation image, O, is defined as an M X M image, where O (k, j) represents the local ridge orientation at pixel (k, j). Note that in a fingerprint image, there is no difference between a local ridge orientation of 90-degreeand 270-degree, since the ridges oriented at 90-degreeand the ridges oriented at 270degreein a local neighborhood cannot be differentiated from each other.

Each block uses a single-orientation value to reduce the computational complexity. This block-wise scheme, however, may be coarse, and it may be difficult to obtain a fine orientation field. In order to estimate orientations more accurately, we use a pixel-wise approach. For each pixel, a block with W × W centered on the pixel is used to compute the average orientation of the pixel. Because of the ambiguity of the orientation values for each position, an orientation smoothing method with a Gaussian window is used to correct the estimation, rather than a simple averaging.

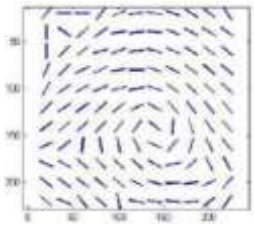

Fig 21: Extracting the orientation fields

4.5. ***Minutia Detection:***

With the help of detected reference points, ridge endings and ridge bifurcation is extracted from the fingerprints. The minutia cylinder consists of fixed length vectors known as cylinder codes that represent various possible minutia points present in local neighborhood of central minutia. The cylinder is enclosed inside a cuboid whose base is aligned according to the minutia direction Θ_m. The mapping is performed by

M: C → X

Where set 'C' is associated with the set 'x' of possible configuration of neighboring minutia represented by (x_p, y_p, θ_p). The neighbor positions (x_n, y_n, θ_n) with respect to the minutia (x_p,y_p,θ_p) is calculated as

$$\sqrt{(x_{p-}x_n)^2 + (y_{p-}y_n)^2 < r} \qquad (6)$$

Where 'r' is the radius of descriptor neighborhood. The description of the minutiae positions leads to a cylindrical shape with (x_p, y_p, θ_p). The value of the cylindrical shape is computed by estimating the probability of minutiae around the central minutiae. By using Gaussian distribution, the probability is computed by assuming the differences in location and direction of two corresponding minutiae with a different impression of fingers. The cylinder can be concatenated as a vector, and therefore the similarity between two minutiae cylinders can be efficiently computed.

4.6. Combined Minutiae Generation:

The combined minutia position C_m is obtained by combining the ridge ending positions of one fingerprint with the bifurcation positions of other finger print along with the reference point as follows. From the two fingerprints 'A' and 'B' the number of each ridge ending positions size (f1) and size (f2) are computed. The maximum size of the fingerprint is identified for the combining process. If the size(f1) is greater than size(f2) then the ridge endings of fingerprint 'A' is combined with the ridge endings of fingerprint 'B' and vice versa. The main steps of the combined minutia are summarized as follows:

a) From the fingerprints A and B the maximum size(f1) and size(f2) are computed.

```
if(size(f1) > size(f2))
    f1 ridge ending => f2 ridge ending
else
    f2 ridge ending => f1 ridge ending
end
```

b) Combining the extracted minutiae points with the reference points from two finger prints A and B the combined minutiae is generated as follows.

$C_m = \frac{h_0 f_1 + h_1 f_2}{|h_0|^2 + |h_1|^2}$ Where h_0 and h_1 are the weight values

*4.6.1. Combined Minutiae Template Generation:*Let us assume a given set of S minutiae positions P_A = { Pia = (X_{ia} , Y_{ia}), $1 \leq i \leq N$} of finger print 'A', the orientation O_B of finger print 'B' and the reference points of finger print 'A' and 'B', a combined minutiae template M_c is generated by minutiae position alignment and minutiae direction assignment as shown below.

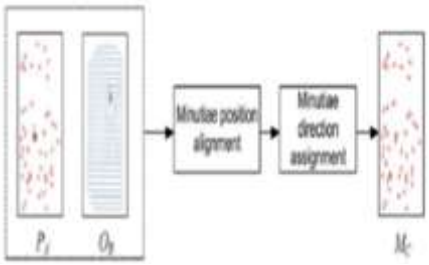

Fig 22: Combined minutiae template generation process

The combined fingerprint template is generated for various combinations of fingerprints. The templates can then be stored in a database which can be used as a reference during the authentication. In the following sections are described about how the two finger prints images are being combined to produce a new template which is real alike image of the original images. This can be achieved with different modules called

- Authentication
- Blind Cryptography
- Data Verification
- Report Generation

*4.6.1.1. Minutiae Position Extraction:*In the Minutiae template authentication module, every user will be authorized by the admin or the main controller of the process. The user should register with their personal info and have a secure key if additional authentication is needed. After the permission is granted by the admin controller they can access the processing units as well as transfer data.

While registering the users account to the admin, it's important to note the user IP and host where they are from. After the successful registration users can access data using the login process. Basically in login process the user needs to enter the user name with their corresponding password. In some other secure application, user needs to submit the secure key during authentication process (login).

The image of the fingerprint is being thinned. The minutiae points are extracted based on the following steps. The fingerprint is converted into binary image and it is thinned. All the ridges are compressed to one pixel width. The points with pixel value of one (ridge ending) as their neighbor or more than two ones (ridge bifurcations) in their neighborhood. This is done by Watermarking technique and it is explained in the next section.

Fig 23. (a) Finger Print Image (b) Thinned Image (c)Thinned Image along with minutiae points (d) Minutiae Position after detecting false points

4.6.1.2. Watermark Technique: By using this technique, we can create a new identity by combining two fingerprint images. This hides the details of how the template is being overlapped and combined.

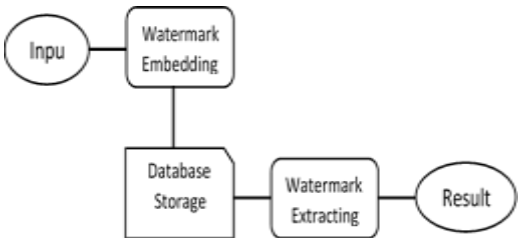

Fig 24: Implementation stages of Watermarking Technique

*Implementation Process:*This technique is implemented in two stages called Embedding and Extraction. In Watermark embedding Stage the two images are overlapped and a new template is created. So it becomes a difficult process for the attackers to identify the exact position of two fingerprints by which the security level increases.

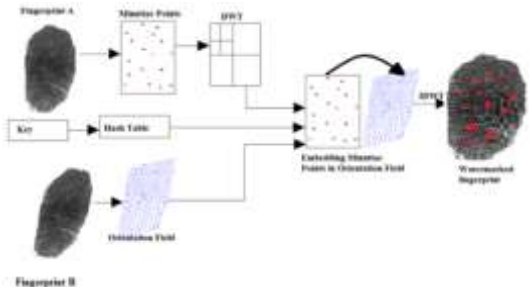

Fig 25: Watermark Embedding Process

The watermark embedding process will includes the following steps

- Discrete Wavelet Transform algorithm is applied on the fingerprint image A denoted as FA. The coefficients of the band contains the details of fingerprint image and hence it is not modified.
- The second LSB is replaced by one bit from fingerprint image B denoted as FB and is represented as:

$$F_w(i,j) = \begin{cases} LSB_2\left(F_A(i,j)\right) = F_B(x,y) \\ if\ Phase(F_A(i,j)) \geq 0\ and\ F_A(i,j) < n \\ F_A(i,j) \\ if\ Phase\left(F_A(i,j)\right) < 0 \end{cases} \quad \text{--- (1)}$$

- If the number of bit in fingerprint image B is less than the blocks of F_A, then all the bits are embedded or else the following procedure is implemented:

○ For each F_A block, a message block MB is formed by selecting the higher order bits and a key K is appended. The value of key is large such that it cannot be found by brute force attack.

○ The hash value of message block is calculated as

$H_A=H(MB)K$ ------- (2)

○ The value of [H_A mod(M*N)] gives the position to embed the watermark bit. If the MSB of H_A is 0 then the F_B bit is inserted unchanged or else the compliment is inserted.

○ Now, IDWT is applied in order to generate the secure watermarked fingerprint image. Any small change in F_A will result in a different hash value. The key vale K is unknown to the hacker so it is difficult to find the hash values.

Extraction Process: Watermark extraction process includes the following steps

- The image is synchronized with the block. DWT is applied on the image and sub-bands are divided into blocks of size (2M-1)*(2N-1).
- For each block synchronization is done as follows:

○ A message block MB is embedded and a key K is appended to it.

○ The hash vale is calculated based on equation (2).

○ The synchronized blocks are identified by comparing the last few bits of H_A with the LSB of neighboring blocks.

- From the synchronized blocks the coefficient with positive phase and less than threshold value η is extracted from watermarked image.
- The remaining bits by calculating the pixel position. The pixel position is calculated by [H_A mod(M*N)]. The MSB of H_A is checked to find if the bit is inserted as such or compliment is taken and is extracted.
- These extracted bits are again rearranged to form the fingerprint image F_B and IDWT is applied to generate the original fingerprint images F_A and F_B from the watermarked image.

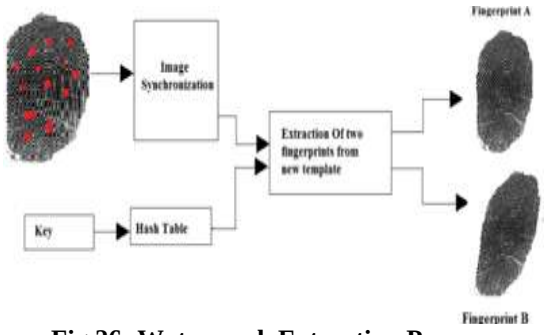

Fig 26: Watermark Extraction Process

We have used this watermark technique to match the images stored in the databases. Then the server matches by uploading the saved combined fingerprint image and registered image. At that time data wavelet algorithm is used to match the two combined fingerprint stored in server database and the other from client database, then matching result appears.

After the login process the user will enter into the main form which will contain the basic operations. To transfers the data user needs to include and make a verification data for it. Both the data and minutiae template verification data will encrypt to prevent unauthorized access. In this module using the MD5 algorithm convert the biometric data to cipher text, earlier conversion methods convert the data's in bytes code format or in text format, that's not enough for healthy communication, this process only make the exact Minutiae template authentication process.

In general, server chooses the random number for key authentication. As like the sender side it will also give the same key in another end to retrieve data. Using the random key value the further authentication process will be held. After the data verification blind secure protocol performs the additional security to the data which was contains the following steps,

a) Retrieve the key from server,
b) Initialize the doubling technique to change the server key,
c) A blind level of process also initialized for key generation,
d) New key will be generated based on the methods,
e) Transfers the data with new key,

The Biometric authentication process purely depends on the technique which the protocol uses. It may be addition or subtraction. Once the blind process completed the key was transferred to the receiver end, as well as verification data also sent.

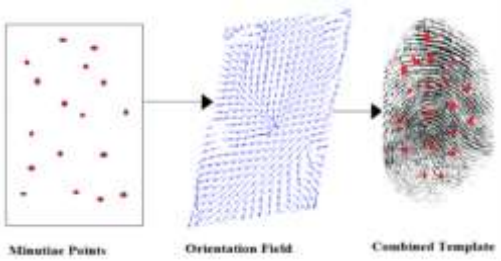

Fig 27: Combination of fingerprint images

4.6.1.3. Minutiae Position Alignment : We have two primary reference points R_a and R_b for fingerprint 'A' and Finger print 'B' respectively. Let us assume Ra is located at $r_a = (r_{xa}, r_{ya})$ with angle B_a, and Rb is located at rb $=(r_{xb}, r_{yb})$ with angle B_b. The alignment is performed by translating and rotating each minutiae point P_{ia} to Pic $= (X_{ic}, Y_{ic})$ by

$(P_{ic})^T = H. (P_{ia} - r_a)^T + (r_b)^T$ Where $( )^T$ is the transpose operator and H is the rotation matrix

$H = \cos(\beta_b - \beta_a)\sin(\beta_b - \beta_a)$

$$H = \begin{vmatrix} \cos(\beta b - \beta a) & \sin(\beta b - \beta a) \\ -\sin(\beta b - \beta a) & \cos(\beta b - \beta a) \end{vmatrix}$$

*4.6.1.4. Minutiae Direction Assignment:*The aligned minutiae positions has an assigned direction Θ_{ic} which is given as

$\Theta_{ic} = O_B (x_{ic} , y_{ic}) + P_i\pi$ here the range of $O_B(x_{ic} , y_{ic})$ is from 0 to π.

Therefore, the range of Θ_{ic} will be from 0 to 2π, which is the same as that of the minutiae directions of an original fingerprint. Sometimes the orientation which is derived from the fingerprint C falls outside the area of fingerprint. In this case the orientation value has to be predicted before the direction assignment. If the values of orientation are not well defined then here we predict the value as the nearest point of well-defined orientation in O_c. A combined minutia template C_c is generated for enrolment if all the directions are assigned to a particular position.

4.6.1.5. Combined Finger Print Generation: We set ρi as 0 or 1 randomly during the minutiae direction assignment, i.e., we add π randomly for each minutiae direction in such a coding strategy. We need to perform a modulo π operation for the minutiae directions during the fingerprint matching, so as to remove such randomness. To create a real-look alike fingerprint image from a set of minutiae points, we further apply a noising and rendering step after adopting the work, where the following stages are carried through as illustrated in the following figure.

Fig 28: Different types of new identities that are generated from two different fingerprints

In proposed system model contain multi biometric authentication. The process of this system as, user has to give their biometric samples. The biometric sample sent to server. The authentication server communicates to database and identify whether the user authorized person or not. If the user is unauthorized mean, the server gives the error message to that user. If the user authorized mean, the server give the acknowledgment to user for further actions. It is a secure way for communicate secret information over the online.

4.7. Two Stage Query Processing:

This section describes a fingerprint matching algorithm using BLPOC function. The algorithm consists of the three steps Rotation and displacement alignment, Common region extraction and Matching score calculation with precise rotation.

Rotation and Displacement Alignment: Normalized rotation and the displacement between the registered fingerprint image f(x1, x2) and the input fingerprint image g(x1, x2) in order to perform the high-accuracy fingerprint matching. First normalize the rotation by using a straightforward approach as. Generate a set of rotated images f'(x1, x2) of the registered fingerprint f(x1, x2) over the angular range $-50^\circ \leq \theta \leq 50^\circ$ with an angle spacing 1°. The rotation angle Θ of the input image relative to the registered image can be determined by evaluating the similarity between the rotated replicas of the registered image f'(x1, x2) ($-50^\circ \leq \theta \leq 50^\circ$) and the input image g(x1, x2) using BLPOC function.

Common Region Extraction: Next step is to extract the overlapped region (intersection) of the two images f(x1, x2) and g(x1, x2). This process improves the accuracy of fingerprint matching, since the non-overlapped areas of the two images become uncorrelated noise components. In order to detect the effective fingerprint areas in the registered image f(x1, x2) and the input image g(x1, x2), we examine the x1-axis projection and the x2-axis projection of pixel values. Only the common effective image areas, f(x1, x2) and g(x1, x2), with the same size are extracted for the use in succeeding image matching step.

Next, align the translational displacement between the rotation normalized image f'(x1, x2) and the input image g(x1, x2). The displacement can be obtained from the peak location of the BLPOC function between f'(x1, x2) and g(x1, x2). Thus, we have normalized versions of the registered image and the input image, which are denoted as g(x1, x2) and f(x1, x2).

4.8. Wavelet based Finger Print Enhancement:

The purpose of a fingerprint image enhancement algorithm is to improve the quality of an input image for facilitating the classification or recognition tasks.

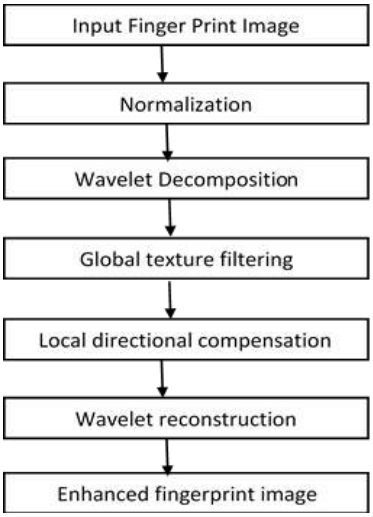

Fig. 29: The flowchart of the fingerprint enhancement algorithm

Calculation of Matching Score:

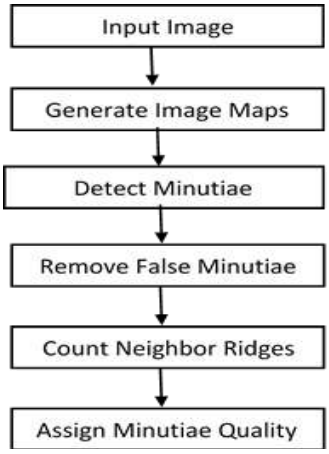

Fig 30: Extracting the Quality minutiae

V. RESULTS AND DISCUSSION

As per our proposal the registration and authentication phase was evaluated and the same process was described in this section

At the time of Enrollment or registration Phase:

1. Select "Enrollment" if you are registering otherwise go to authorization phase

Fig 31: Image showing the enrollment and Authentication phases

2. Give your name and Email id to accept your fingerprints

Fig 32: Getting the details of user like name and email at enrollment phase

3. If the email entered is already registered or available in the database it will not allow to register again with the same email id.

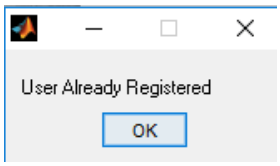

Fig 33: Message generated by the system for already registered email

4. The system will collect two individual finger prints

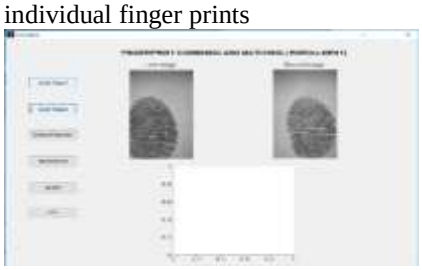

Fig 34: Figure showing the two finger prints accepted from individual fingers

5. Extracts the common features i.e. minutiae points from first finger print and orientation field from second finger print.

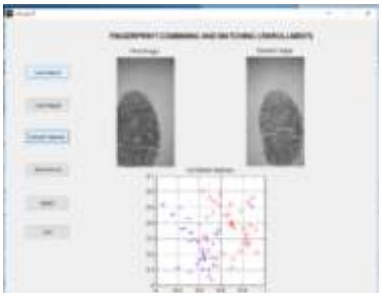

Fig 35: Identifying the common features from two finger prints

6. Reconstruct the combined finger print from the common features obtained from both first and second finger print by generating a template.

Fig 36: Template generation from the common features

7. Then store the template in the database after encoding the generated template.

At the time of Authentication Phase:

1. Select "Authentication" to get into authorization phase as shown in Fig 31.

2. It will accept the email id to process the authorization phase

Fig 37: Accepting Email for Authorization phase

3. If the email entered is valid then it will allow the user to proceed step 4 otherwise it will give error message "invalid user"

Fig 38: The message displayed when email is not matched with the database

4. Once it was confirmed as existing user it will accept two finger prints

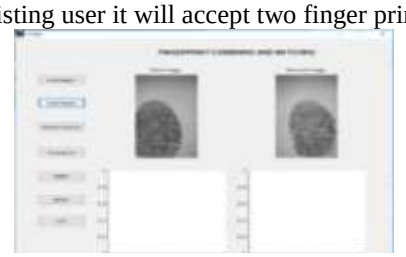

Fig 39: Accepting two finger prints similar to enrollment phase

5. Extracts the common features i.e. minutiae points from first finger print and orientation field from second finger print similar to step 4 in enrollment phase.

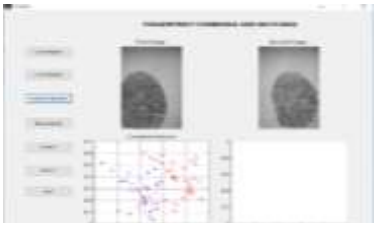

Fig 40: Identifying the common feature set from two finger prints

6. Reconstruct the combined finger print from the common features obtained from both first and second finger print by generating a template.

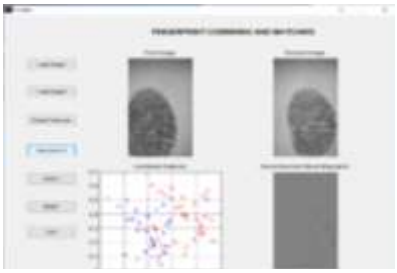

Fig 41: Generated template from the common features

7. Compare the generated templated with the template available in the database after decoding.

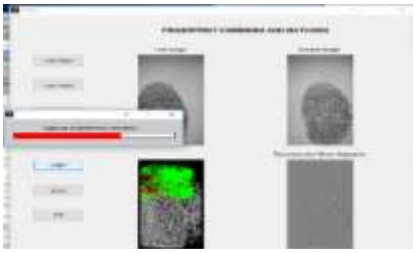

Fig 42: Comparing the generated template with the stored template

8. Perform fingerprint verification, if it is matched then the user is allowed otherwise it will be reject the user.

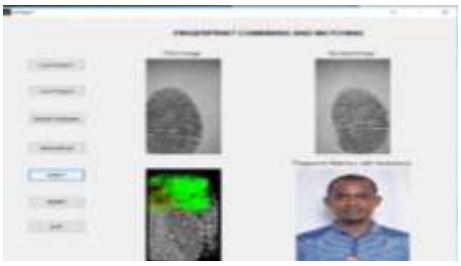

Fig 43: Displaying the user image from the database if template is matched

The experimental results show that the combined minutiae template generated by our proposed strategy is efficient and real look-alike of original image. The results shows a comparison of the original fingerprint images of A and B. Minutiae position extracted image and the combined template of our technique. The last image is combined template generated by conventional technique.

The performance comparison graph of the existing and proposed strategies. It shows that the combination of finger print template generated by our proposed system achieves very low error rate.

REFERENCES

[1]. S.G. Mallat, A theory for multiresolution signal decomposition: the wavelet representation IEEE Trans. Pattern Anal. Mach. Intell. 11 (7) (1989) 674–693.
[2]. Fingerprint Recognition using MATLAB by Zain S. Barham.
[3]. Y. J. Wang and K. N. Plataniotis, ―An analysis of random projection for changeable and privacy-preserving biometric verification, IEEE Transactions on Systems, MAN and Cybernetics — PART B: CYBERNETICS, vol. 40, no. 5, Oct. 2010.
[4]. Biometrics Quick Guide by tutorial points.
[5]. R. Ribalda, G. G. de Rivera, Á. de Castro, and J. Garrido, ―A mobile biometric system on-token system for signing digital transactions,‖ IEEE, March/April 2010. [5] M. Bishop and C. Irvine, ―New pathways in identity management,‖ IEEE, Nov./Dec. 2010.
[6]. S. Kumar and E. Walia, ―Analysis of various biometric techniques,‖ International Journal of Computer Science and Informatio
[7]. Technologies, vol. 2, no. 4, pp. 1595-1597, 2011.
[8]. D. Bhattacharyya, R. Ranjan, F. A. Alisherov, and M. Choi, ―Biometric authentication: a review, International Journal of u- and e-Service, Science and Technology, vol. 2, no. 3, Sep. 2009.
[9]. SangramBana and Dr. Davinder Kaur "Fingerprint Recognition using Image Segmentation", International Journal Of Advanced Engineering Sciences And Technologies, Vol No. 5, Issue No. 1, 012 – 023.

Dr. N. Satheesh Kumar. " Improving Privacy And Security Of Multi Biometric Fingerprint By Combining Orientation Fields With Wavelet And Cryptographic Algorithms In Ethiopian Banking Sector"American Journal of Engineering Research (AJER), vol. 7, no. 5, 2018, pp.183-199.