Protecting the Privacy of Fingerprint

Mahabub Bi
PG Scholar, Dept. of CSE,
V.R Siddhartha Engineering College

S.Jayaprada
Senior Assistant Professor,
Dept. of CSE, V.R Siddhartha Engineering College

Abstract: Protecting the privacy of the fingerprint in authenticating systems is becoming a major issue now-a-days because of the widespread and the use of fingerprint recognition systems. Here we compare two systems in order to protect the privacy of fingerprint. This is mainly a two-step process. One is Enrolment and the other is Authentication. So we propose, an approach called Fingerprint Combination which contains the combination of fingerprints in order to form a new identity. At the first stage, two finger prints should be taken and then minutiae features have been taken from one hand and the Orientation points from the other and the Reference points from both the hands must be considered. By considering this we Form a new identity. Based on this extracted information, a combined template is generated and stored in the database. Then the Authentication process is done by comparing the features which we are considered and finally we apply some of the matching algorithms in order to protect the privacy of fingerprint.so, because of the similarity in topology, it is difficult for the attacker to differentiate a combined minutiae template from the original minutiae templates. With the help of existing techniques we are able to convert the combined template into a real-look like combined fingerprint. The experimental results show that our system can achieve a very low error rate with False Rejection Rate = 0.4% at False Acceptance Rate = 0.1%. Compared with the other techniques, our work has the advantage in creating a new virtual identity when the two different fingerprints are randomly considered.

IndexTerms:-Combination, Fingerprint, Minutiae, Orientation, Reference points, Privacy, and Protection.

I. INTRODUCTION

Fingerprints are one of one of the form of biometrics which is used to identify individuals and to verify their identity. Protecting the privacy of the fingerprint is becoming a major issue now a days[1]. These are used in many Applications like Banking Security , ATM security, card transaction, Physical Access Control (e.g. Airport), Information System Security, National ID Systems, Passport control, Prisoner, prison visitors, Identification of Criminals etc. The word '**Biometrics**' is divided in to two parts 'Bio' means Life and 'Metric' means **Measure.** Biometrics refers to technologies which are used for measuring and analysing a person's anatomical behavioural and characteristics. These unique characteristics are used to verify and recognise the individuals. These are mainly used for authentication purpose. Fingerprints are graphical flow like furrows present on fingers of every individual. These contain tiny **Ridges, Whorls** and **Valley** patterns on the tip of each finger. No two people will have the same fingerprints .These are totally unique. There's a one in 64 billion chance that the fingerprints will match up exactly with someone. A **ridge** is a curved line on a finger image. These ridges are sometimes like continuous curves, and others terminate at specific points called **Ridge endings** [2]. Sometimes, two ridges come together at a point called a **Bifurcation**. Ridge endings and bifurcations are known as **Minutiae**. All of the ridges of fingerprints form patterns called loops, whorls and arch's.**Arch**'s are the lines which enter from one side of finger, then forms an arch in middle and then end other side.**Loop**[3] are the ridges which enter from one side then forms a loop and then depart on same side. **Whorl's** are the lines which move through the median point of finger. These may be spiral or circular. Minutiae are defined as the points of interest in a fingerprint, such as bifurcations (a ridge splitting into two) and ridge endings. An orientation image is defined as an N x N image, where O (i, j) represents the local ridge orientation at pixel (i, j).Local ridge orientation is usually specified for a block rather than at each and every pixel; an image is divided into a set of n x n non-overlapping blocks and a single local ridge orientation is defined for each block.

In an image there is no difference between a local ridge orientation of 90°and 270°, since the ridges oriented at 90° and the ridges oriented at 270° in a local neighbourhood cannot be differentiated from each other. In the previous year's most of the existing techniques make use of the key for the fingerprint privacy protection. But if the key is stolen and fingerprints are stolen then the existing techniques get failure. Therefore in order to overcome the disadvantage of previous approaches now a days many of the techniques came in to existence.

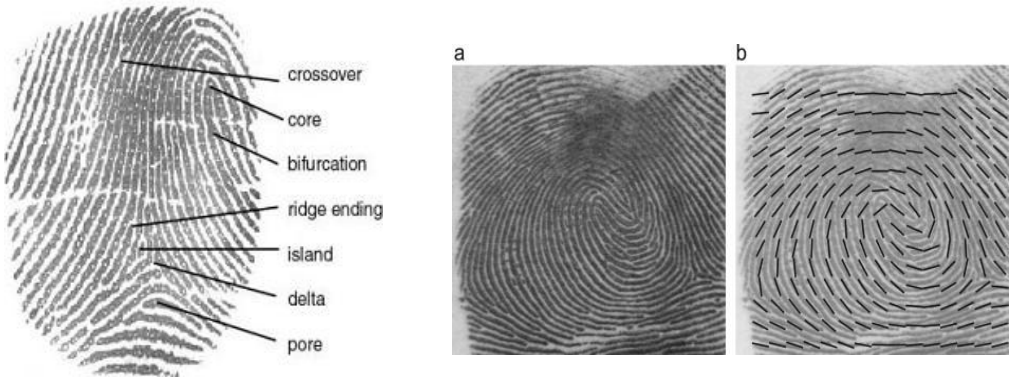

Figure 1: Minutiae and Orientation points

II. RELATED WORK

In existing methods, R. Malathy and K. Senthil Prasad proposed a **Livelyness Detection technique [**1**]** to distinguish between a legitimate and imposter user. **Quadrangle** based fingerprint authentication system is considered. This means a unique **Topography is** generated for the quadrangle structure**.** Each angle in the quadrangle is quantized into an **integer or binary** number. **Quadrangle** based fingerprint authentication system is considered. This means a unique **Topography code** is generated for the quadrangle structure**.** Each angle in the quadrangle is quantized into an **integer or binary** number. This method protects from anti spoofing. But this method fails when there is an increase of noise variation in the images.

Sayani Chandra, Sayan Paul [2] proposed an **Image decomposition** approach which contains one secret image and two cover images. During the authentication, the two sheets are overlaid in order to create a temporary fingerprint image for matching. Here **Floyd Steinberg Error Diffusion Algorithm** is used for half toning the input images. Then BBR algorithm is applied for encryption as well as decryption and finally pixel values are defined at some of the places. The minimum value will be considered as pixel value of the secret image. The advantage of this system is that the identity of the user is never exposed to the attacker in a single database. However, maintaining two separate databases will not work in all applications.

Vidya.P, Aswathy.R.S [3] proposed **RSA Encryption approach** in which encryption algorithm is applied on the combined template and then those fingerprints will be stored in the database. Here a pre-defined threshold value has been considered in order to authenticate the user. The advantage of this approach is that more accuracy can be achieved with a low error rate.

Aswathy Shankar, Angel.P [4] proposed **Adaptive fingerprint enhancement algorithm** which is used to enhance the images. By using this algorithm some one of the features need to be extracted and they will be stored in the database. Finally some of the matching techniques have to be applied in order to authenticate the user.

S.Karthikeyan and N.Radha [5] proposed **Bio Hashing algorithm** which follows the technique of cancellable biometrics in the fingerprint. This proposed method does not require the re-alignment of fingerprints as all the minutiae are converted into a pre-defined two dimensional space based on a reference minutiae which has been considered. After that, the proposed Bio Hashing method is used to consider the one-way property (non-invertibility) of the biometric template. The proposed method is very much resistant to minor translation error and rotation distortion. An Equal Error Rates (EER) of less than 1% is achieved in this approach and performance of the approach is also significant. The advantage of this approach is more accuracy can be achieved.

A. Othman and A. Ross [6] proposed **Mixed fingerprint approach** in which mixing of fingerprints is done at the image level in order to generate a new identity. This fingerprint consists of two components such as continuous and spiral. Then pre aligning of components is done in order to form a new identity [11]

S.Chaudhari and Girish K.Patnaik [7] proposed **Minutiae filtering method** to reduce the unwanted minutiae points. The experimental result shows that fingerprint combination using minutiae and orientation

achieves a better ERR with a FRR of 0.04% at FAR 0.1% when compared to minutiae combination technique. Moreover, it is not easy for the attacker to recover the original minutiae templates from a combined fingerprint.

A.Prasathkumar, V. Evelyn Brindha [8] proposed a Finger print enhancement technique called Laplacian pyramidal decomposition method to improve the fingerprint quality and which will also provide more help for law enforcement. Here different Biometric template protection methods had been applied in order to authenticate the user.

III. PROPOSED SYSTEM

The advantages of proposed technique over the existing fingerprint combination techniques are as follows:

- Compared with the feature level based techniques [1], [2], these techniques are able to create a new identity which is difficult to be distinguished from the original minutiae templates.
- Compared with the image level based techniques [3], [4], these techniques are able to create a new virtual identity and gives better results when the two different fingerprint images are randomly chosen.

The basic structure of this paper is as follows: section 2 presents the related work of the system. Section 3 explains our proposed system and section 4 gives the explanation of how to generate a combined template by considering two fingerprints. Section 5 represents the conclusion of our proposed system which is further followed by references.

Steps of algorithm:

Input : Fingerprint images

Output: User authenticity with user Id

Step 1: Fingerprint images are taken as input

Step 2: Enrollment

a) Consider Reference points, orientation points and minutiae points [1]

Step 3 : Combined Minutiae template generation [2]

Step 4 : Reconstruction of fingerprint

Step 5 : Storing in the database

Step 6 : Authentication

a) Consider Reference points, orientation points and minutiae points

Step 7 : Bio Stage Fingerprint Matching process [6]

Step 8 : Output is User Authenticity.

The input images can be considered either by scanning or by Acquisition of images. These images can be scanned by using Biometrics or scanners. Here the database which we have considered is **FVC2002DB2_B.**

Then the pre-processing process must be done. The main aim of pre-processing is improvement of the image data that suppresses no longer needed distortions or improves some image features for further processing. These contain different methods like noise removal, contrast enhancement, background reduction and some image enhancement algorithms. By using these t techniques more clear ridges can be obtained. Now in the enrolment phase, features such as Minutiae points, Orientation points and reference points need to be extracted.

Then a Combined Minutiae template [6] need to be generated and finally, fingerprint reconstruction must be done in order to remove the false Minutiae Points and that must be stored in the database. Now in the authentication phase continue the above steps and then the newly generated template must be matched with the template which is present in the database. Finally we get the output as user authenticity and we get the user Id of the person to whom it was matched.

The following figure shows the architecture of the proposed approach:

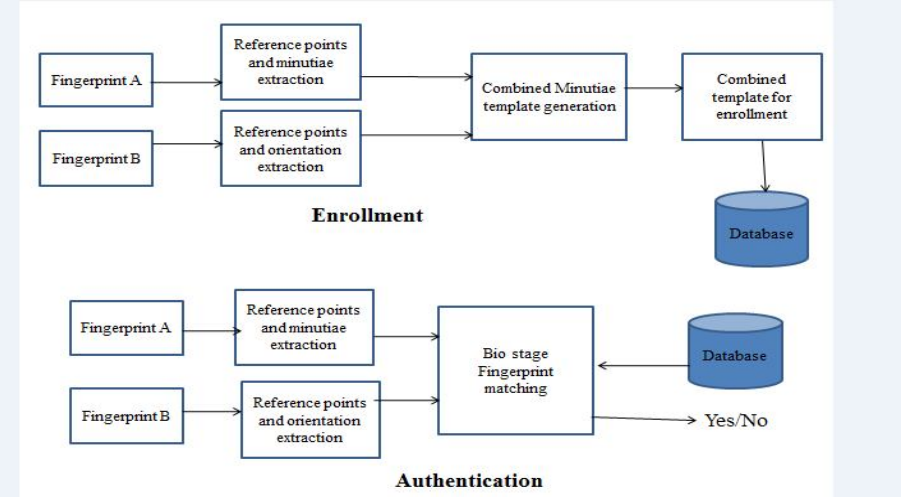

Figure 2: Proposed System for protecting the privacy

IV. ALGORITHMS

The following algorithms describe the detailed working of the proposed approach. Algorithm 1 states the Reference Point Detection; Algorithm 2 is used for Combined Minutiae Template generation; Algorithm 3 states the Bio stage Fingerprint Matching Process.

A) *Rerence poınt detectıon:*

- **Input :** Orientation point[6]
- **Output :** Reference point
- **Step** 1 **:**Consider the orientation point (O) from the fingerprint.[6]

  Z=cos (2O) +jsin (2O)

- **Step 2:**Calculate a certain map of reference points.

  C_{ref}= Z *Tref

  Where * is the convolution operator and T_{ref} is the conjugate of

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

- **Step 3:**Calculate an improved certainty map[3]

$$C'_{ref} = \begin{cases} C_{ref}.\sin\left(Arg(C_{ref})\right) & if\ Arg(C_{ref}) > 0 \\ 0 & otherwise \end{cases}$$

  Where Arg(z) returns the principal value of the argument of z(defined from $-\pi$ to π)

- **Step 4:** Consider the reference points which satisfy the two conditions

a)The amplitude of C'_{ref} point value should be of local maximum value and

b)The Local maximum value should be over a fixed threshold

- **Step 5:** Repeat this step until all the reference points are located
- **Step 6:** If no reference points are found in the fingerprint then consider the reference point with the maximum value in the complete fingerprint image

B. *Combined minutiae template generation:*

A combined MinutiaeTemplate can be generated by minutiae position alignment and minutiae direction assignment. Here given a set of Minutiae points PA = {Pia = (x_{ia}, y_{ia}), $1 \le i \le N$} of first fingerprint and orientation of second fingerprint and reference points from both the fingers. A combined Template can be generated by minutiae position alignment and Minutiae direction Assignment [5]

- **Input** : Minutiae positions, orientation and reference points from both the fingerprints.
- **Output** : A new Virtual Identity(Combined Minutiae Template.

Minutiae position alignment:

Among all the reference points of fingerprints we consider a maximum one as the reference point .so, we have two primary reference points R_a and R_b for fingerprints A and B. Now let us assume R_a is located at r_a = (r_{xa}, r_{ya}) with the angle β_a, and R_b is located at r_b = (r_{xb}, r_{yb}) with the angle β_b. The alignment can be performed by translating and rotating each minutiae point p_{ia} to p_{ic} = (x_{ic}, y_{ic})

where $(p_{ic})^T = H.(p_{ia}-r_a)^T+(r_b)^T$ and H is the rotation matrix

$$H = \begin{pmatrix} \cos(\beta_b-\beta_a).\sin(\beta_b-\beta_a) \\ -\sin(\beta_b-\beta_a).\cos(\beta_b-\beta_a) \end{pmatrix}$$

And sometimes R_a and R_b get overlapped when both are in the same position and in the same angle after position assignment.

MINUTIAE DIRECTION ASSIGNMENT:

Each minutiae position p_{ic} which are placed are assigned with a direction θ_{ic}. Where ρ_i is an integer that will be either 0 or 1. 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 are same as that of the minutiae directions from an original fingerprint. Following strategies are proposed for determining the value of

- ρ_i is randomly selected from {0, 1}.
- ρ_i is determined by

$$\rho_i = \begin{cases} 1 \text{ if } \mathrm{mod}(\theta_{ia}+\beta_b-\beta_a,\prod)-O_B(x_{ic}, y_{ic})>0) \\ 0 \text{ otherwise} \end{cases}$$

Where mod is the modulo operator and θ_{ia} is the original direction of a minutiae position p_{ia} in fingerprint A. ρ_i is determined by

$$\rho_i = \begin{cases} 1 \text{ if } \mathrm{mod}(ave_b(x_{ic}, y_{ic}),\prod)- O_B(x_{ic}, y_{ic}) >0) \\ 0 \text{ otherwise} \end{cases}$$

Where $ave_b(xic, yic)$ is the average direction of the n nearest neighboring minutiae points of the location (x_{ic}, y_{ic}) in fingerprint B

$$ave_b(x_{ic}, y_{ic}) = \frac{1}{n}\sum_{k=1}^{n}\theta_b^k(x_{ic}, y_{ic})$$

Where $\theta^k_b(x_{ic}, y_{ic})$ means the direction of the k nearest neighbor minutiae point of the location (x_{ic}, y_{ic}) in fingerprint B, and n value is usually set to 5 which will provide a good balance for matching the accuracy. Sometimes, p_{ic} may also be located outside of the fingerprint B, where $O_B(x_{ic}, y_{ic})$ is not well defined. In this type of cases, we need to predict $O_B(x_{ic}, y_{ic})$ before the direction is assigned. Here, we simply predict the value of $O_B(x_{ic}, y_{ic})$ as the value of nearest well defined orientation in O_B. Once the entire N aligned minutiae positions are assigned with directions, a combined minutiae template $M_C = \{m_{ic} = (p_{ic}, \theta_{ic}), 1 \le I \le N\}$ is used for enrolment. Sometimes, a global minutiae position translation may also be necessary for combined template such that all the minutiae points will be present inside the fingerprint image.

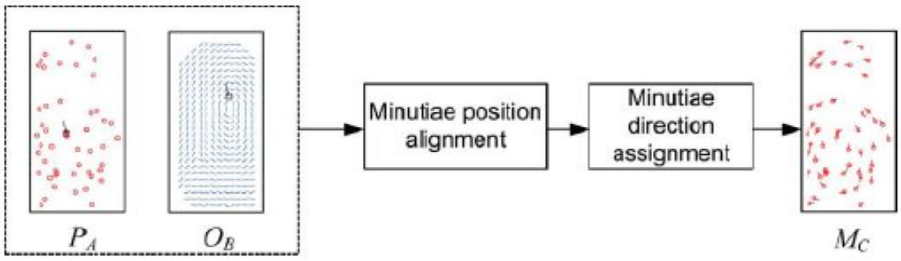

Figure 3: Combined Minutiae Template Generation Process

C. *Bıo stage fingerprınt matchıng:*

In this matching process we consider the minutiae points, orientations and reference points from both the query fingerprints. For this purpose we propose an algorithm called Bio stage Fingerprint Matching which contains Query Minutiae Determination Process.

Input: Minutiae points, Orientation and reference point from both the query fingerprints

Output: User authenticity

Query minutiae determination process:

Verification plays a vital role in fingerprint Verification process. So at first we should extract the local features from minutiae point M_c.So for an instance we consider that $m_{ic}$is a minutiae point in M_c and m_{jc} as another point.so for this point consider,

1) L_{ij} is the distance between m_{ic} and m_{jc}[5]

$$L_{ij} = \sqrt{(x_{ic} - x_{jc})^2 + (y_{ic} - y_{jc})^2}$$

2) Γ_{ij} is the difference between the directions of m_{ic} and m_{jc}

$$\gamma_{ij} = \theta_{ic} \bmod \pi - \theta_{jc} \bmod \pi$$

3) $\sigma_{ij}$is the radial angle then[6]

$$\sigma_{ij} = \Re(\theta_{ic} \bmod \pi, \operatorname{atan2}(y_{jc} - y_{ic}, x_{jc} - x_{ic}))$$

Where atan2(y, x) is a two argument tangent function in the range of (-∏, ∏) and

$$\Re(\mu_1, \mu_2) = \begin{cases} \mu_1 - \mu_2 & \text{if } -\pi < \mu_1 - \mu_2 \leq \pi \\ \mu_1 - \mu_2 + 2\pi & \text{if } \mu_1 - \mu_2 \leq -\pi \\ \mu_2 - \mu_1 + 2\pi & \text{if } \mu_1 - \mu_2 > \pi. \end{cases}$$

Now for the i^{th} minutiae point mic in M_c, we extract a set of local features F_i.

$$\mathbf{F}_i = \left(L_{ij}, L_{ik}, L_{il}, \gamma_{ij}, \gamma_{ik}, \gamma_{il}, \sigma_{ij}, \sigma_{ik}, \sigma_{il}\right)$$

Here we assume m_{jc} is the nearest and m_{kc} is also another nearest and m_{lc} is the third nearest point.

Now we detect k_1 as a reference point from fingerprint A' and k_2 as another reference point. Then

- **Step 1:** Consider reference points each from two different fingers. Assume them as R_a' and R_B'
- **Step 2 :** Consider the angles at which they are present. Now assume their angles as β_a' and β_b'
- **Step 3 :** By using reference points, orientation and minutiae generate a Combined Template for the new Fingerprint
- **Step 4:** Extract some of the local features from both the enrolled fingers as well as Authentication fingers. We assume F_u are the local features for the u^{th} minutiae point in Mc' and F_V are the local features for the v^{th} minutiae point in Mc[6].
- **Step 5 :** Calculate the difference between the features F_u and F_v then[4]

$$\Re(\mu_1, \mu_2) = \begin{cases} \mu_1 - \mu_2 & \text{if } -\pi < \mu_1 - \mu_2 \leq \pi \\ \mu_1 - \mu_2 + 2\pi & \text{if } \mu_1 - \mu_2 \leq -\pi \\ \mu_2 - \mu_1 + 2\pi & \text{if } \mu_1 - \mu_2 > \pi. \end{cases}$$

- **Step 6 :**Repeat all the above steps until all the possible pairs of reference points are considered and processed.
- **Step 7 :** Among all the tested minutiae the one which is having the minimum distance from enrolled Combined template will be considered as Query Minutiae.
- **Step 8 :** Calculate the matching score between the templates.
- **Step 9 :** output is User Authenticity.

D. *Combined Fingerprint Generation process:*

In order to make the fingerprint look as a real one we further apply some of the noisy and rendering steps and then the combined generation process is as follows:

Step 1: Calculate the orientation Field O from a set of minutiae points by using Orientation Reconstruction algorithm. [1]

Step 2: Generate a binary ridge pattern based on O and by using a predefined ridge frequency [3]

Step 3: Estimate the phase image of the binary ridge pattern

Step 4: Reconstruct the continuous image by removing the spirals in the image

Step 5: Combine the continuous and spiral components for constructing the new fingerprint [6]

Step 6: Eliminate the spurious minutiae points in order to form a reconstructed image.

Step 7: Apply noisy and rendering step in order to make the fingerprint look as a real one.

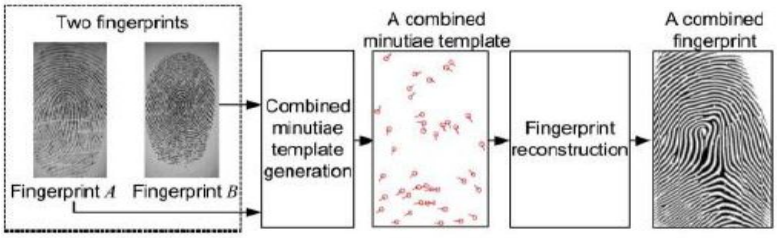

Figure 4: Generating a combined template for the Fingerprints

E. *Experimental results:*

Dataset: FVC2002DB2_B

Input data is collected in the form of images. Here the database which we have considered is FVC2002DB2_B. This database contains 560*296 sized gray scale images collected from different fingerprints. By using this we can achieve a very low error rate with FRR=0.4% and FAR=0.1%.

Figure 5: Dataset of Fingerprint

This is the dataset which we have considered. All the fingerprint images will be stored here

Figure 6: Enrollment and Authentication GUI

This is the User Interface in which the user must enrolls or gets authenticated by the system

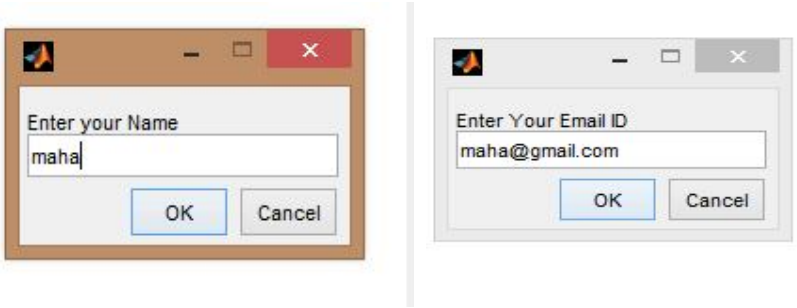

Figure 7: Enrollment GUI

When the user clicks on enrollment then the user name and email id is to be given. If the user is a valid user then the person can enroll his details. Here the person name and email id has already been stored in database**.**

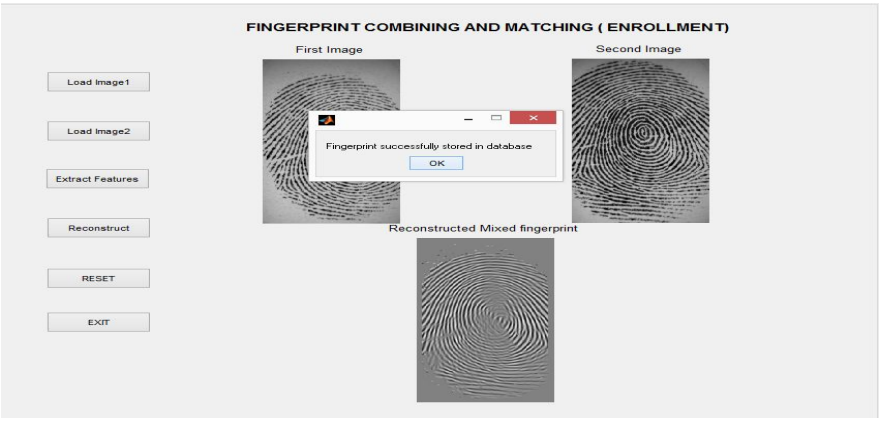

Figure8: Enrollment Process

Now, if the user is a valid user then the user finger prints will be considered then features from both the fingerprints will be considered and then a new reconstructed fingerprint is constructed and then it will be stored in database.

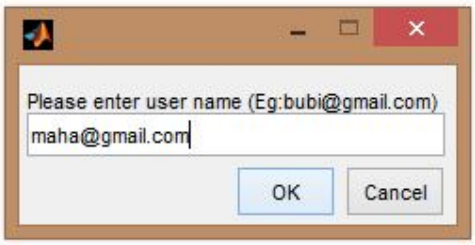

Figure 9: Authentication GUI

When the user is already a registered user then when the person need to be authenticated first the person need to give his email id and if it is a valid id then the person can give his fingerprints.

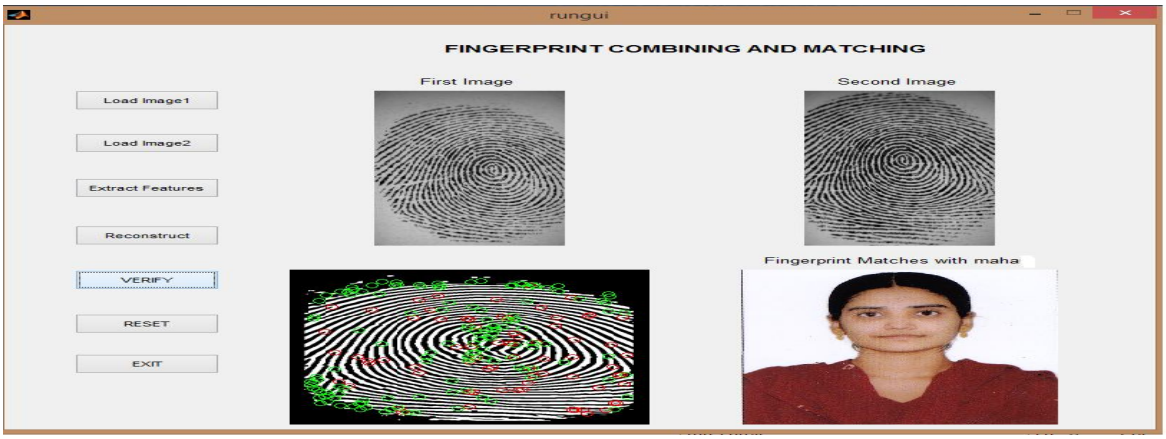

Figure 10: Authentication Process

If the user entered details are valid then the user identity can be confirmed by getting the corresponding user photograph on the display.

V. CONCLUSION

In this framework a new mechanism has been proposed for protecting the privacy by joining two fingerprints into a virtual identity. A combined template is generated by considering minutiae features, Orientation and Reference points from both the fingerprints and it will be stored in the database. To make it as a real one some of the noise will be added to the combined Template. Here, Bio-stage fingerprint matching process is put forward for matching the two query fingerprints against the enrolled template. This combined Template also has similar topology like an original template. Therefore, we are able to combine two different fingerprints into a new virtual identity by reconstructing a real -look alike combined finger-print from the combined template. So, it is also difficult for an attacker to break other traditional systems by using the combined templates. Here our techniques have achieved more performance when the two different fingerprints are accidentally choosen. By using this mechanism False Acceptance Rate get reduces. When compared to other traditional systems. In the future work, along with the Combined Fingerprints, Palm Identification Analysis can also be put forward in order to provide more privacy for the Integrity of the user Identity.

REFERENCES

[1] R.Malathy,K.Senthil Prasad, "Fingerprint Protection Based On Virtual Identity", ARPN Journal of Engineering and Applied Sciences, APRIL [2015]

[2] Sayani Chandra, Sayan Paul ,"Visual Cryptography for Biometric Privacy",International Journal of Science and Research(IJSR),JANUARY[2015]

[3] Vidya.P,Aswathy.R.S,"PrivacyImprovement Based On RSA",International Journal of Innovative Research in Science,Engineeringand Technology(IJIRSET), JULY [2014]

[4] Aswathy Shankar, Angel.P,"Enhanced Biometric Authentication System using Mixed Fingerprints",International Journal of Advanced Research in Computer Science Engineering and Information Technology ,APRIL[2014]

[5] S.Karthikeyan and N.Radha, "Fingerprint security using Bio Hash",International Journal of Network Security & Its Applications (IJNSA), JULY[2011]

[6] A. Othman and A. Ross, "On Mixing Fingerprints", IEEE Transcations on information Forensics and security , JANUARY[2013]

[7] S.Chaudhari and Girish K.Patnaik, "Implementation of Minutiae Based Fingerprint Identification System ", International Journal of Computer Trends and Technology (IJCTT) , FEBRUARY[2014]

[8] A.Prasathkumar, V. Evelyn Brindha ,"Biometric privacy by Laplacian decomposition", International Journal of Latest Trends in Engineering and Technology(IJTET) , JUNE[2011]

[9] Ansi R R, Anusree L , "Advanced Bio-Crypto System with Smart Card" ,International Journal of Engineering and Advanced Technology (IJEAT) AUGUST[2015]

[10] Lukesh N. Jain, Dr. R. G. Karandikar "Decision tree based fingerprint authentication",International Journal of Engineering and Technical Research (IJETR) ,MAY[2015]

[11] Aafa J S, Soja Salim"Fingerprint protection based on virtual identity", International Journal Engineering and Technical Research [2014]