Biometric Template Generation with low Error Rate

[1] Prof.Zainab Mizwan & [2]Vaidehi Atmaram. Patil
[1] Head of Department, Electronics and Telecommunication
Shree L.R. Tiwari College Of Engineering, [2] Student, ME Electronics and Telecommunication
Shree L.R. Tiwari College Of Engineering,
Kanakia Park, Mira Road East, Thane - 401 107

Received: January 23, 2019 Accepted: March 01, 2019

ABSTRACT: *Security presentation through fingerprint template creation is a system for protecting fingerprint privacy by fusion of two different biometric fingerprints into a new identity in the registration process; two fingerprints are captured from two different fingers. Then the minutiae positions from fingerprint, the orientation from the other fingerprint and the reference point from both fingerprints are drawn out based on this information and coding strategies fused minutiae template is created, more accurate and precise results the process of root threading is applied on the fuse template and this template is stored in the database. In the authentication, the system needs uses two queries from the same fingers which are used in the registration process. In the existing system the only security is password authentication so the hackers easily stole out password & try to access authentication server, so system security may degrade. In this system we generate an algorithm to create fuse minutiae template of two fingerprints. We are able to create a combined template which is a real look alike of single fingerprint. Thus a unique identity is created with very low error rate with FRR=0.2% & FAR=0.01%.*

Key Words: *Fused Template, minutiae position, orientation, root threading.*

I. INTRODUCTION

Fingerprint techniques have widespread of applications in authentication systems. Hence protecting the privacy of the fingerprint becomes an important issue. Conventional encryption methods are not sufficient for protecting the privacy of the fingerprint, because decryption technique is needed before the fingerprint matching process [21]. This technique exposes the fingerprint to the intruders or attackers. Therefore, to avoid this many methods have been developed which helps in developing specific fingerprint protection techniques. In order to protect the privacy of the fingerprint most of the existing methods make use of key. This creates much inconvenience in the privacy. These techniques become inefficient when both the key and the fingerprint are stolen. Therefore, in recent years, significant efforts have been put into developing specific protection techniques for fingerprint [21].

II. LITERATURE SURVEY

Robust Combination Method for Privacy Protection Using Fingerprint and Face Biometrics by Miss Dhanashri J. Ghate, Mrs. Savitri B. Patil [1] this include a Secure advance system for fingerprint privacy protection by combining different biometrics fingerprint and face into a new identity is proposed. The two-step fingerprint matching algorithm is used for matching the fingerprint of same person against the generated combined minutiae template. Fingerprint Combination for Privacy Protection by,Sheng Liand, Alex C. Kot, [2] In this paper, in the enrollment, two fingerprints are captured from two different fingers, then the minutiae positions from one fingerprint is extracted, the orientation from the other fingerprint, and the reference points from both fingerprints. In the authentication, the system requires two query fingerprints from the same two fingers which are used in the enrollment. Finger Print Combination for Privacy Protection and Security by kanagalasurya chaitanya1, ch.Cury [3] in this paper, the system captures two fingerprints from two different fingers. This introduced a combined minutiae template generation algorithm, to create a combined minutiae template from the two fingerprints. In such a template, the minutiae positions are extracted from one fingerprint, while the minutiae directions depend on the orientation of the other fingerprint and some coding strategies. S. Li and A. C. Kot, "A novel system for fingerprint privacy protection,"[8]A fingerprint authentication system for the privacy protection of the fingerprint template stored in a database is introduced here.K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," [9] Reliable information security mechanisms are required to combat the rising magnitude of identity theft in our society. While cryptography is a powerful tool to achieve information security, one of the main challenges in

cryptosystems is to maintain the secrecy of the cryptographic keys. Teoh et al.[10] has propose the bio hashing approach by generating the inner products resource between end user's fingerprint features and orientation and random pseudo random number (i.e., the key). An accuracy of this approach is totally depends on the key. Here it is that assumed that key never gets stolen. Ratha et al.[11] has propose for generating cancelable fingerprint templates by applying the non-convertible transforms on the minutiae template.

III. PROBLEM STATEMENT

The existing techniques make use of the key for the fingerprint privacy protection, which creates the inconvenience. I adopt this approach for generating a combined fingerprint from a combined minutiae template.

With the wide spared applications of fingerprint techniques in authentication systems, protecting the privacy of the fingerprint becomes an important issue.

Present fingerprint protection systems make use of encryption in which decryption is also required; this exposes the fingerprint to the attacker [21].

Most of existing techniques make use of the key for the fingerprint privacy protection, which creates the inconvenience; they may also be none of use when both the key and the protected fingerprint are stolen [3].

Previous results has error rate with FRR=0.4% & FAR=0.1%. This gives low error rate with FRR= 0.2% & FAR=0.01% [2].

Therefore, in this project we are going to focus on major problem of:

- In existing techniques the most practical way of addressing the privacy invasion problem is to combine two or more factor authenticators [21].
- The use of multiple biometric measurement devices will certainly impose significant additional costs, more complex user-machine interfaces and additional management complexity [21].
- The problem of mixing two fingerprint images in order to generate a new cancelable fingerprint image [23].
- In multimodal biometric verification system combining fingerprint and voice modalities is proposed. Multiple biometric modalities has been shown to decrease error rates, by providing additional useful information to the classifier [24].

IV. THE PROPOSED ADVANCED SECURE FINGERPRINT TEMPLATE CREATION SYSTEM

In "Biometric Template Generation with low Error Rate" proposed an adaptive encryption based privacy improvement for fingerprint recognition [21]. During enrolment, two fingerprints are captured from two different fingers and then extract the minutiae positions from one fingerprint, the orientation from the other fingerprint, and the reference points from both fingerprints [3]. Based on this extracted information a combined minutiae template is generated and stored in a database after performing RSA encryption. In the authentication, the system requires two query fingerprints from the same two fingers which are used in the enrolment.

ROOT THREADING

Root threading is a image processing strategy to achieve maximum security and high accuracy. In this process end roots of fingerprints are extracted and processed by image processing algorithm. By using this technique FRR up to 0 .01% and FAR up to 0.01 can be achieve.

The aim of this project is to implement a unique identity of fingerprint by combining two different fingerprints. In the enrollment, two fingerprints are captured from two different fingers. We extract the minutiae positions from one fingerprint, the orientation from the other fingerprint, and the reference points from both fingerprints. In the authentication, the system requires two query fingerprints from the same two fingers which are used in the enrolment [3]. A new virtual identity is created for the two different fingerprints, which can be matched using minutiae-based fingerprint matching algorithms [11].

Compared with the state-of-the-art technique, our work has the advantage in creating a better new virtual identity when the two different fingerprints are randomly chosen.

The objectives of this project are as follows:

1. The identity of the biometrics is never exposed to the attacker in a single database.
2. It is difficult for the attacker to distinguish a mixed fingerprint from the original fingerprints.
3. The effectiveness of the projected two stage fingerprint matching, assess the enactment of our system by using a straight minutiae matching method for the similar fingerprint.

4. Our system is able to achieve a very low error rate with FRR= 0.01% when FAR= 0.01%. Compared with the feature level based technique, we are able to create a new identity (i.e., the combined minutiae template) which is difficult to be distinguished from the original minutiae templates [3].
5. Compared with the image level based technique, we are able to create a new virtual identity (i.e., the combined fingerprint) which performs better when the two different fingerprints are randomly chosen [1].

V. BLOCK DIAGRAM

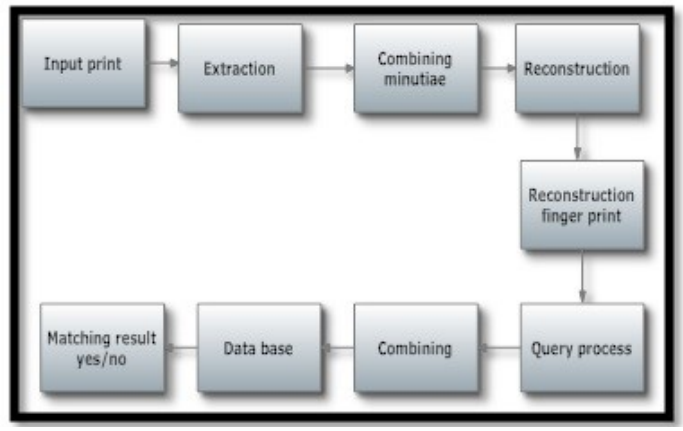


Fig1 Block diagram

Firstly, minutiae points and orientation is extracted from one fingerprint and reference points from both the biometrics are extracted using some coding strategy.
The two-stage fingerprints verification process is then proposed for matching the two query fingerprints against the combined template. Topology of a combined template is similar to the original minutiae templates, so it is converted into the real resource alike combined fingerprint by using an older fingerprint reconstruction method.

IV. SEQUENCE DIAGRAM

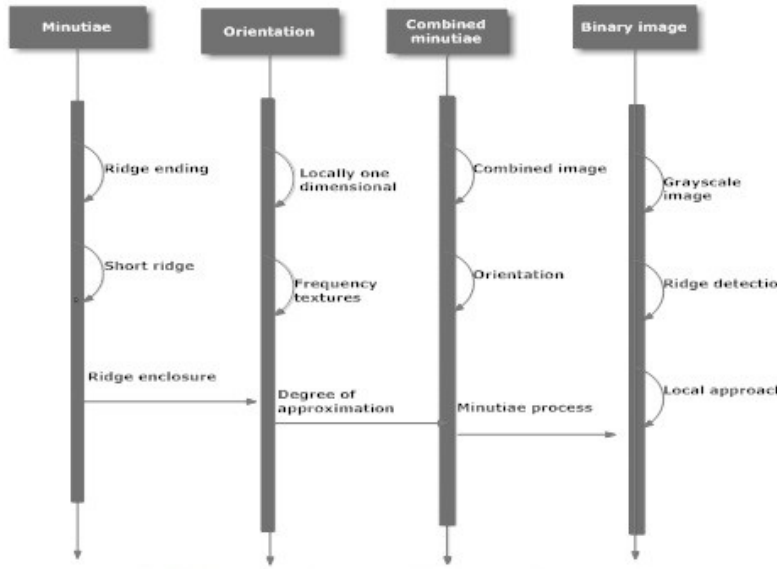


Fig3 Secure Fingerprint template creation

A. REFERENCE POINTS DETECTION

The reference point detection process is comes from Nilsson [12], who first proposes to use complex filters for singular point detection. Given fingerprint, the reference point's detections are summarized as follows:

- Using orientation estimation algorithm [13], compute the orientation O from the fingerprint obtain

the orientation Z in complex domain, where

$$Z = Cos(2O) + j\,Sin(2O) \quad (1)$$

- Calculate a certainty map of reference points [12].

$$C_{ref} = Z * \overline{T}_{ref} \quad (2)$$

- Where "*" is the convolution operator and $\overline{T}_{ref}$ is the conjugate of

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

This is the kernel for reference point's detection.

- Calculate improved certainty map [14]

$$\dot{C}_{ref} = C_{ref}.\,sin\left(Arg(C_{ref})\right) if\ Arg(C_{ref}) > 0$$
$$\dot{C}_{ref} = 0\ Otherwise \quad (4)$$

Where Arg (z) returns the principal value of the argument of z (defined from –π to π)

- Locate the reference point satisfying two criterions: 1.the amplitude of $\dot{C}_{ref}$ of the point (hereinafter termed as the certainty value of simplicity) is a local maximum, and 2.the local maximum should be over fixed threshold T. suppose we locate a reference point at (r_x, r_y), the corresponding angle can be estimated as Arg ($\dot{C}_{ref}$ (r_x, r_y),).
- Repeat step 4) until all ref points are located.
- If no reference point is found for all fingerprints' in step 4) & 5) (e.g., an arch fingerprint), locate the ref point with maximum certainty value in the whole fingerprint image.

B. COMBINED MINUTIAE TEMPLATE GENERATION

Given a set of N minutiae positions $P_A = \{P_{ia} = (X_{ia}, Y_{ia}), 1 \le i \le N\}$ of fingerprint A, the orientation OB of fingerprint B and ref point of fingerprints A & B, a combined minutiae template MC is generated by minutiae position alignment & minutiae direction assignment.

MINUTIAE POSITION ALIGNMENT

Among all the reference points of a fingerprint for enrollment, we define a reference point with the maximum certainty value as the primary reference point. Therefore, we have two primary reference points R_a and R_b for fingerprint A and B respectively. Lets' assume Ra is located at $r_a = (r_{xa}, r_{ya})$ with the angle β_b. The alignment is performed by translating & rotating each minutiae point p_{ia} to $p_{ic} = (x_{ic}, y_{ic})$ by

$$(P_{ic})^T = H.(P_{ia} - r_a)^T + (r_b)^T \quad (5)$$

Where $()^T$ is the transpose operator and H is the rotating matrix where

$$H = \begin{bmatrix} Cos(\beta_b - \beta_a) & Sin(\beta_b - \beta_a) \\ -Sin(\beta_b - \beta_a) & Cos(\beta_b - \beta_a) \end{bmatrix} \quad (6)$$

As such Ra and Rb are overlapped both in the position & the angle after the minutiae position alignment.

MINUTIAE DIRECTION ASSIGNMENT

Each aligned minutiae position p_{ic} is assigned wit direction θ_{ic} as follows:

$$\theta_{ic} = O_B(x_{ic}, y_{ic}) + \rho i\pi \quad (7)$$

Where ρi is an integer that is 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 0to 2π, which is the same as that of the minutiae directions from an original fingerprint, following three coding strategies are proposed for determining the value of ρi.

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

$$\rho i = 1\ if\ mod\ (\theta_{ia} + \beta_b - \beta_a, \pi) - O_B(x_{ic}, y_{ic}) > 0$$

$$0\ Otherwise \quad (8)$$

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

$$\boldsymbol{\rho i = 1\ if\ mod\ (a\vartheta eb(x_{ic}, y_{ic}), \pi - O_B(x_{ic}, y_{ic}) > 0} \quad \textbf{(9)}$$
$$\textbf{0 Otherwise}$$

Where $(a\vartheta eb(x_{ic}, y_{ic})$ is the average direction of the n nearest neighboring minutiae points of the location (x_{ic}, y_{ic}) in fingerprint B

$$\boldsymbol{a\vartheta eb(x_{ic}, y_{ic}) = \frac{1}{n}\sum_{k=1}^{n} \theta_b^k(x_{ic} - y_{ic})} \qquad (10)$$

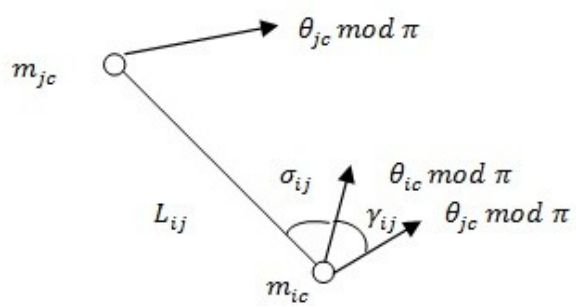
Where $\theta_b^k(x_{ic} - y_{ic})$ mean the direction of the Kth nearest neighboring minutiae point of the location $(x_{ic} - y_{ic})$ in fingerprint B, and n is empirically set as 5 which is able to provide a good balance between the diversity and matching accuracy of the combined minutiae templates.

In the following discussions, these three coding strategies are termed as coding strategy 1, coding strategy 2, 7 coding strategy 3 respectively. Note that some additional strategy 2, where the block diagram of our system shown in fig 1 should be modified accordingly. sometimes, p_{ic} may be located outside the area of fingerprint B, where $\boldsymbol{O_B(x_{ic}, y_{ic})}$ is not well defined. In such cases, we need to predict $\boldsymbol{O_B(x_{ic}, y_{ic})}$before the direction assignment. Some existing work for modeling the fingerprint orientation can be adopted to do the prediction. For example, the work in [15] can estimate the missing orientation structure even for the partial fingerprint. Here, we simply predict the value of $\boldsymbol{O_B(x_{ic}, y_{ic})}$ (if it is not well defined) as the value of nearest well defined orientation in $\boldsymbol{O_B}$.
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 created for enrollment. In some cases, a global minutiae position translation may be necessary for M_C such that all the minutiae points are located inside the fingerprint image.

C. TWO STAGE FINGER PRINT MATCHING

Given the minutiae positions Pa of fingerprint B and the reference point of the two query fingerprints. In order to match the Mc stored in the database, we propose a two stage fingerprint matching process including query minutiae determination and matching score calculation.
Query Minutiae Determination: The Query minutiae determination is a very important step during the fingerprint matching. In order to simplify the description of our algorithm, we first introduce local features extracted for minutiae.

Fig.4. Illustration parametersL_{ij},γ_{ij} and σ_{ij}



Point in Mc. The local feature extraction is similar to the work proposed. Given a minutiae point m_{ic} and another minutiae point m_{jc} in L_{ij} , we define

1. L_{ij} as the distance between m_{ic} & m_{jc}.

$$\boldsymbol{L_{ij} = \sqrt{(x_{ic} - x_{jc})^2 + (y_{ic} - y_{jc})^2}} \quad \textbf{(11)}$$

2. γ_{ij} as the difference between the directions (after module π) of m_{ic} & m_{jc} .

$$\gamma_{ij} = \theta_{ic} mod\pi - \theta_{jc} mod\, \pi \quad (12)$$

3.σ_{ij} as a radial angle:

$$\sigma_{ij}=\Re(\theta_{ic} mod\pi, atan2(y_{jc} - y_{ic,} x_{jc} - x_{ic})) \quad (13)$$

Where atan2(x,y) is a two-argument arctangent function in the range (-π, π) and

$$\Re(\mu_1, \mu_2 = \{\mu_1\text{-}\mu_2 \quad \text{if } -\pi<\mu_1 - \mu_2 \leq \pi$$
$$=\mu_1\text{-}\mu_2+2\,\pi \quad \text{if } \mu_1 - \mu_2 \leq \text{-}\pi$$
$$=\mu_2\text{-}\mu_1+2\,\pi \quad \text{if } \mu_1 - \mu_2 > \pi \quad (14)$$

An illustration of the definitions of L_{ij},γ_{ij} **and** σ_{ij} **are shown in fig 4. For the** i^{th} **minutiae point** m_{jc} in m_c , we extract a set of local features F_i as follow:

$$F_i=(L_{ij}, L_{ik}, L_{il}, \gamma_{ij}, \gamma_{ik}, \gamma_{il}, \sigma_{ij}, \sigma_{ik}, \sigma_{il}) \quad (15)$$

Where we assume m_{jc} is the nearest m_{kc} is the second nearest and m_{lc} is the third minutiae point of m_{jc}.
Suppose we detect K_1 (K_1≥1) reference point from fingerprint A' and K_2 (K_2≥1) reference point from fingerprint B'. The query minutiae are determined as follows:
Select a pair of reference points: one from fingerprint A'(say R_a) and the other from fingerprint B' (say R_b). Assume R_a is located at r_a'=(r_{xa}, r_{ya}) with the angle β_a'R_b, is located at r_b'=(r_{xb}, r_{yb}) with the angle β_b Respectively.
Perturb β_a by τ= β_a'+k· Δ, where k is an integer and Δ is a perturbation size. We choose Δ=2×$\frac{\pi}{180}$ radians. (i.e., 2 degrees) and -5≤k≤5. Thus, we have L=11 perturbed angles for the reference point R_a'.
Generate a combined minutiae template $M_c^{'}(\tau)$ for testing (hereinafter simply termed as a testing minutiae) fromP_A, O_B, R_A' (with a perturbed angle τ) and R_b' using the proposed combined minutiae template generation algorithm . Note that the same coding strategy should be adopted for generating $M_c^{'}(\tau)$ and $M_c^{'}$ .In total, we generate K testing minutiae$M_c^{'}(\tau)$.
Suppose F_u are the local features extracted for the Uth minutiae point in $M_c^{'}(\tau)$, while Fv are the local features extracted for the Vth minutiae point in $M_c^{'}$ .calculate the difference between F_u and F_v by

$$D_r(u, v) = \omega_{1.\sum_{j=1}^{3}|F_u(j)-F_v j|}$$

$$+u_2.\sum_{j=4}^{9}|F_u(j) - F_v j| \quad (16)$$

Where $F_i(j)$ refers to the jth component ofF_i, ω_1 *and* ω_2 are the weights for different features .we follow the same weight settings as , where ω_1 *and* ω_2 are empirically set as ω_1=1 & ω_2=0.2*180/π . the we define the difference between $M_c^{'}(\tau)$ and $M_c^{'}$ as

$$d_r=min_{u,v}\, D_r(\mathrm{u,v}) \quad (17)$$

Repeat step 1) to 4) until all the possible pairs (in total K× $k_1 \times k_2$ pairs) if reference points are selected & processed. Among all the testing minutiae (K× $k_1 \times k_2$ *in total*). The one which has minimum difference from $M_c^{'}$ (i.e. minimum dτ) will be consider as query minutiaeM_q.

MATCHING SCORE CALCULATION

For the combined minutiae templates that are generated using coding strategy 1, we do a modulo π for all minutiae directions in M_q andM_c, so as to remove randomness. After the modulo operations, we use an existing minutiae matching algorithm to calculate a matching score between M_q and M_c for the authentication decision. For other combined minutiae templates, we directly calculate a matching score between M_q and M_c using an existing minutiae matching algorithm.

D. PARTIAL FINGER PRINT MATCHING

Our system works on the minutiae-based representation of a fingerprint context, are the various ridge discontinuities of a fingerprint. More than 100 different types of minutiae have been identified, among

which ridge bifurcations and endings are the most widely used. Minutiae based representation of fingerprints is an ANSINIST standard & contains only local information without relying on global information such as singular points or center of mass of fingerprints. Matching two fingerprints (in minutiae-based representation) is to find the alignment and correspondences between minutiae on both prints. For matching regular sized fingerprint images, a brute-force matching. Which examines all the possible solutions, is not feasible since the number of possible solutions increases exponentially with the number of feature points on the prints. In order to increase the efficiency of matching process, other methods instead of brute force matching must be applied. Intuitively, a pre-alignment method may obtain the alignment parameters of two fingerprints. Pre-alignment methods that depend on the global singular points are not suitable for partial fingerprint matching. Other pre-alignment techniques need to reprocess all the images thus they cannot be used on already existing database.

There are two major types of features that are used in fingerprint matching: local and global features. Local features such as the minutiae information that is in a local area only and invariant with respect to global transformation. On the other hand, global features, such as number , type and position of singularities, spatial relationship and geometrical attributes of ridge lines, size and shape of the fingerings, are characterized by the attributes that capture the global spatial relationships of a fingerprint. Because of the nature of the partial fingerprints, partial fingerprint matching requires asset of local features have the ability to tolerate more distortions has shows that the geometric deformations on local areas can be more easily controlled by global deformations.

E. SECONDARY FEATURES

The secondary features are derived from minutiae information. We use the minutiae extraction techniques described with some modifications to remove the false minutiae on the edge of the fingerprint foreground to generate the minutiae for our system. The method first gets the image quality maps by checking the low contrast areas, low flow blocks, and high curve regions. And then, a binary representation of a fingerprint is constructed by applying a rotated grid on the ridge flows of the fingerprint. Minutiae generated by comparing each pixel neighborhood with a family of minutiae templates. Finally a series of heuristic rules is used to merge and filter out the spurious minutiae. Use relative distance, radial and minutiae type to generate the features that we use are similar but the minutiae type and ridge count elements are removed. Minutiae types are difficult to distinguish when impress pressure varies on different applications. Furthermore, ridge count is not universally available and not all minutiae representation in existing databases contains this information.

F. EXPECTED RESULT

We introduce an Advance secure fingerprint template creation by combining different biometrics into a new identity as template is proposed. In the registration process; two fingerprints are captured from two different fingers. Then the minutiae positions from fingerprint, the orientation from the other fingerprint and the reference point from both fingerprints are drawn out. After a root threading process generated template is stored into a data base. In the authentication, the system needs uses two queries from the same fingers which are used in the registration process. In this system we generate an algorithm to create fuse minutiae template of two fingerprints. We are able to create a combined template which is a real look alike of single fingerprint. Thus a unique identity is created with very low error rate with FRR=0.02% & FAR=0.01%. So basically we expect to reach up to maximum Security with FRR = 0.02% FAR = 0.01%.

REFERENCES

1. Robust Combination Method for Privacy Protection Using Fingerprint and Face Biometrics Miss Dhanashri J. Ghate, Mrs. Savitri B. Patil 2015 IEEE.
2. Sheng Li Student Member, IEEE, and Alex C. Kot, Fellow, IEEE," Fingerprint Combination for Privacy Protection", IEEE transactions on information forensics and security, vol. 8, no.2, February 2013.
3. Finger Print Combination for Privacy Protection and Security By Kanagala Surya Chaitanya1, Ch. Cury2 August-2015.
4. B. Yanikoglu and A. Kholmatov, "Combining multiple biometrics to protect privacy " in Proc. ICPR-BCTP Workshop, Cambridge, U.K., August 2004.
5. A. Ross and Othman," Mixing fingerprints for templates security and privacy" in Proc. 19th Eur. Signal Proc. Conf. (EUSIPCO), Barcelona, Spain,29 August - 2 September, 2011.
6. A. Othman and A. Ross," Mixing fingerprints for generating virtual identities," in Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS), Foz do Iguacu, Brazil, 29 November- 2 December 2011.

7. S. Li and A. C. Kot, "Attack using reconstructed fingerprint," in Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS), Foz do Iguacu, Brazil, 29 November- 2 December 2011.
8. S. Li and A. C. Kot, "Privacy protection of fingerprint database," IEEE Signal Process. Lett., vol. 18, no. 2, pp. 115–118, Feb. 2011.
9. K. Nandakumar, A. K. Jain and S. Pankanti," Fingerprint-based fuzzy vault: Implementation and performance," IEEE Trans. Inf. Forensics Security, vol. 2, no. 4, pp. 744-57, December 2007.
10. B. J. A. Teoh, C. L. D. Ngo, and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and tokenized random number ," Pattern Recognit., vol. 37, No.11, pp. 2245-2255, 2004.
11. N. K. Ratha , S. Chikkerur, J. H. Cornnell, and R. M. Bolle," Generating cancelable fingerprint templates," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 561-72, April 2007.
12. K. Nilsson and J. Bigun," Localization of corresponding points in fingerprints by complex filtering," Pattern Recognit. Lett., vol. 24, no. 13, pp. 2135-2144, 2003.
13. L. Hong, Y. F. Wan, and A. Jain, "Fingerprint image enhancement: Algorithm and performance evaluation," IEEE Trans. Pattern Anal. Mach. Intell., vol. 20, no. 8, pp. 777–789, Aug. 1998.
14. S. Chikkerur and N. Ratha, "Impact of singular point detection on fingerprint matching performance," in Proc. Fourth IEEE Workshop on Automat. Identification Advanced Technologies, Oct. 2005, pp. 207–212.
15. Y. Wang and J. Hu, "Global ridge orientation modeling for partial fingerprint identification," IEEE Trans. Pattern Anal. Mach. Intell., vol. 33, no. 1, pp. 72–87, Jan. 2011.
16. J. Feng and A. K. Jain, "Fingerprint reconstruction: From minutiae to phase," IEEE Trans. Pattern Anal. Mach. Intell., vol. 33, no. 2, pp. 209–223, Feb. 2011.
17. R. Cappelli, A. Erol, D. Maio, and D. Maltoni, "Synthetic fingerprintimage generation," in Proc. 15th Int. Conf. Pattern Recognition, Sep. 3–7, 2000, vol. 3, pp. 471–474.
18. U. Ulugdag, "Secure Biometric Systems," Ph.D. thesis,Michigan State Univ., East Lansing, MI, 2006.
19. C. L.Wilson, G. T. Candela, and C. I.Watson, "Neural network fingerprint classification," J. Artif. Neural Netw., vol. 1, no. 2, pp. 203–228, 1994
20. Y. Chen, "Extended Feature set and Touchless Imaging for FingerprintMatching," Ph.D. thesis,Michigan State Univ., East Lansing, MI, 2009.
21. B. J. A. Teoh, C. L. D. Ngo, and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and tokenised random number," Pattern Recognit., vol. 37, no. 11, pp. 2245–2255, 2004.
22. A. Nagar, K. Nandakumar, and A. K. Jain, "Biometric template transformation: A security analysis," in Proc. SPIE, Electron. Imaging, Media Forensics and Security, San Jose, Jan. 2010.
23. A. Ross and A. Othman, "Mixing fingerprints for template security and privacy," in Proc. 19th Eur. Signal Proc. Conf. (EUSIPCO), Barcelona, Spain, Aug. 29–Sep. 2, 2011.
24. E. Camlikaya, A. Kholmatov, and B. Yanikoglu, "Multi-biometric.