OPTIMIZED DUAL FINGERPRINT MECHANISM FOR PRIVACY PROTECTION

1 Sanjyoti Lakhe, Student of ME (CSE) , Government College of Engineering ,Aurangabad, Dr.Babasaheb Ambedkar Marathwada University, Aurangabad.

sanjyoti_lakhe@yahoo.com

ABSTRACT

The importance of digital image processing domain has been improved from last few decades due to its advanced study areas such as medicine, biometrics, services, robotics etc. In this work an important issue has taken as area of research namely protecting the solitude information from the unauthenticated users either as fortuitous or incidental ways. Although remarkable progress has been made in the past years on the protecting the privacy information by make use of biometrics namely fingerprint, palm print, iris etc. The custom of fingerprint in university, medical labs, and military has been increased from few years but in some scenarios these fingerprint mechanisms fails to meet the practical requirement. The proposed work presents an novel work where dual fingerprint mechanisms is utilized to protect the privacy information where the orientation from one fingerprint and miniature from another finger print has been taken into account to develop an template which looks alike of original fingerprint. The proposed template protects the information from the theft and as well as shows low error rate over traditional approaches. Finally when compared with conventional methods proposed method has better virtual identity which shows good results against incidental and accidental attacks.

Keywords:

Fingerprint, Biometric, Minutiae, Orientation, Template.

1. INTRODUCTION

1.1 Importance of Biometrics

In 21st century security has been the major area of concern and to provide good solution to the problems related to security and research on biometrics has increased thrice in the past few years. Nowadays internet related applications have increased a lot and the major issue related to the internet applications are creating authentication from the remote location which creates the security chain. In traditional approaches usage of passwords and tokens have been used which are easily stolen and guessed. To overcome the drawbacks related to traditional algorithms usage of biometric has been increased prominence for authentication and related identification of the respective entities.

1.2 What is Biometric?

The term biometric came from the great GREEK mythology where BIO means life and METRIC means to measure. The science of biometrics mainly relies to develop technological which can provide advance security by taking the persons.

Psychological characteristics into account. The taken user's unique characteristics are used further to identity and verify the individual user information in a reliable way.

Fingerprint biometric mechanism is most used mainly because of its simple nature, a fingerprint biometric mechanism can easily built by taking some points namely miniature.

Many fingerprint algorithms came into existence after intense research on miniature mainly ridges and Particulars are for the most part demonstrated as the terminations and bifurcations of the edge lines in a unique finger impression picture. The two most vital neighborhood edge qualities of particulars are the edge finishing and the edge bifurcation extraordinary. Edge closure is termed as the point where the edge closes unexpectedly. Edge bifurcation is termed as the point where an edge forks or veers into branch edges. A unique mark verification

framework can be by and large separated into two sections to be specific.

Biometric information is progressively utilized as a part of confirmation and distinguishing proof of people, supplanting secret key based security frameworks. Distinguishing proof and confirmation alludes to two distinct errands: discovering the personality of a man given the biometric versus confirming the personality given the biometric information and the asserted personality.

2. OVERVIEW AND ADVANTAGES OF PROPOSED APPROACH

2.1 Overview of the Proposed Approach

An optimized fingerprint mechanism is proposed in this paper to protect the privacy information in an accurate way. In past many algorithms and theoretical works has proposed based on single fingerprint which mainly lacks of secrecy and privacy, the algorithms based on single fingerprint mechanism fails to provide security to the authenticated fingerprints in the database and data can easily lost by incidental/accidental hacking. The important description and discussion steps in the proposed method are as follows:

(a) In First step, enrollment of fingerprints is done and later the authorized system captures the two different relevant fingerprints from the two respective different fingerprints.

(b) An innovative algorithm namely "combined minutiae template generation algorithm" which helps further in creating template from the two different fingerprints for providing the advanced privacy protection.

(c) In this step prominent information is evaluated which helps further to construct a template and the respective information are evaluated from two different fingerprint features namely minutiae positions and minutiae directions

d) The minutiae positions from one finger print and simultaneously the minutiae directions from second fingerprint are taken in this approach along with the some coding strategies.

(e) The generated Fingerprint look alike template is stored in the database for authentication.

(f) An optimized matching process has been implemented in this paper which gives accuracy of matching query between the two different fingerprints and the obtained template.

(g) The main intention of the proposed work is to protect the data from the incidental/accidental attacks by creating relevant template for the database authentication and theft of one template will not reveal all information and unauthenticated user can be manipulated by creating the real fingerprint look alike template which is resultant of the two different fingerprints combination.

(h) Finally combined minutiae template generation algorithm succeed in providing the secured fingerprint alike template which helps in creating the new virtual identity from the two different fingerprints and these two different information's from the fingerprints can be matched by using the fingerprint matching frameworks in an effective way.

(i) The proposed Algorithm succeeds to achieve the less false acceptance rate (FAR) and false rejection rate (FRR) over the conventional fingerprint algorithms.

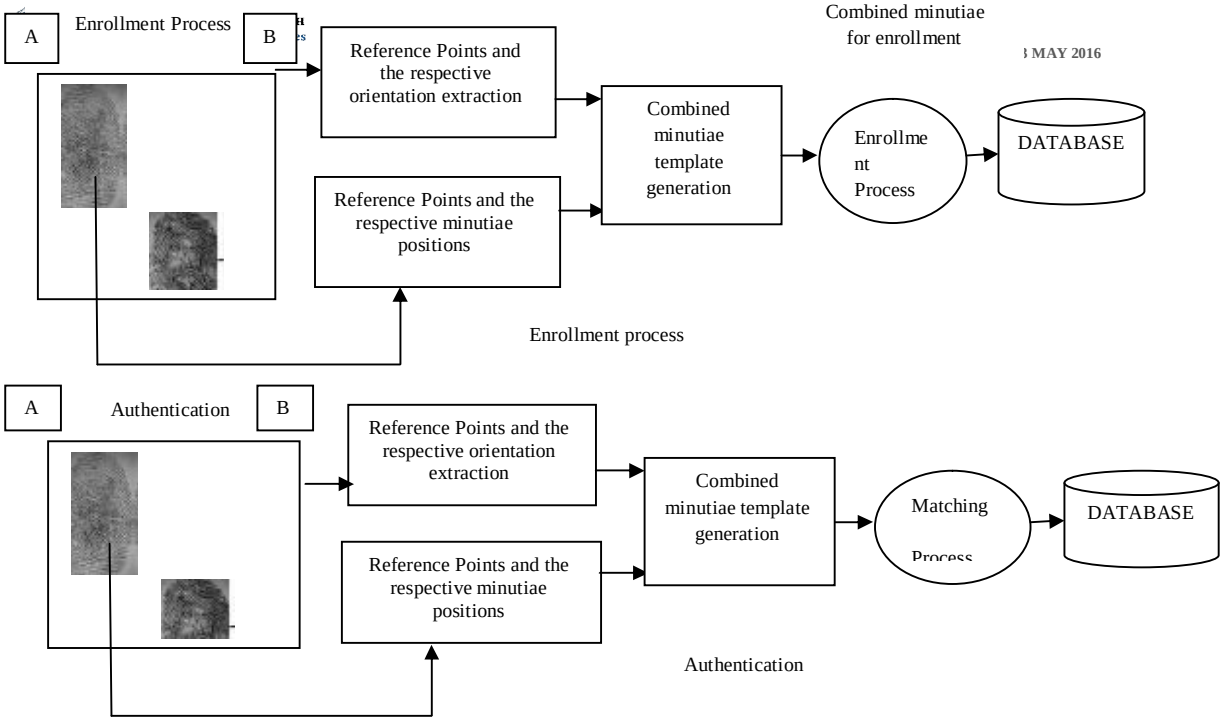

Figure1: Proposed Fingerprint model for the Privacy protection

2.2 The Advantages of Proposed Algorithm

(a) The security breach of privacy data in biometrics is mainly because of high error rate and high complexity respectively in all scenarios. The privacy protection of the authenticated data of the user by biometrics especially fingerprint biometric mechanism has been attracted many attention mainly due to its simple and advanced algorithmic approaches.

(b) Compare to the conventional works proposed in the literature the proposed algorithm has successful to meet the practical requirements such privacy protection by reducing the error rate which is 80% more than compares to the single scale fingerprint approaches.

(c) As reported in the literature the fingerprint biometric mechanism has been classified into two categories according to their respective characteristics namely the feature level and image level. Both approaches are fails to provide better protection the user privacy data and the data used in these approaches are more prone to theft. The Proposed work creates the combined minutiae template which look alike original fingerprint template which makes difficulty for authenticated users to distinguish original from combined template.

(d) AFTER the image level analysis in the above step the second approach namely image level approaches as discussed earlier in the above step are fails to provide the new virtual identity which creates hurdles to provide high level security to user data. The proposed method is able to construct the new virtual identity from the two different fingerprints which is reliable and accurate to protect the privacy information in all scenarios.

3. DUAL FINGERPRINT ALGORITHM

Let us consider the two fingerprints namely A and B respectively from the two different fingers, where this enrollment has done by the system which is further used these fingerprint to create the template and latter these template is used for the authentication of the authenticated person in all different application areas. The two important steps of the proposed algorithm are as follows:

(a) The main approach of the proposed algorithm is to use some techniques which helps to minutiae positions from the fingerprint mechanism A and the respective orientation from the another fingerprint.

(b) Then a combined minutiae template is generated successfully from the minutiae positions, orientations, reference points and finally some coding strategies to protect the privacy data.

3.1 Detection of Reference Points

Reference points detection are motivated by the conventional papers reported in the literature which are theoretical works and research works respectively. The proposed method motivated from the work which are proposed by Nilsson et al in which the detection of points are done by using the complex filters .The prominent steps in the reference points detection are as follows:

(a) The orientation extraction is the crucial step in the proposed approach where the orientation O from the respective fingerprint has been taken by using the orientation estimation algorithms which are reported in the literature.

(b) Based on the obtained statistics from the orientation estimation algorithms the orientation O in the complex domain is obtained as follows

$$Z = \cos(2\Theta) + j \sin(2\Theta) \ldots\ldots. \quad (1)$$

(c) The calculation of the certainty map of the orientation O are as follows, these calculation of certain map helps to find the best samples in next steps

$$C_{ref} = Z * \bar{T}_{ref} \qquad (2)$$

(d) Then the use of convolution operator finally gives the kernel reference points detection based on the convolution operator "*" as reported in the above step and the respective $\bar{T}_{ref}$ is the conjugate of

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

(e) Based on the figure 2 analysis the generation of combined minutiae template has started and the respective improved certainty map are stated as follows

$$C'_{ref} = \begin{cases} C_{ref}.\sin\left(Arg(C_{ref})\right) & if\ Arg(C_{ref}) > 0 \\ 0 & otherwise \end{cases} \qquad (4)$$

Where the term Arg (z) value represents the principle value from the all available values of the improved certainty map (defined from $-\pi$ to π)

(f) The localization of the reference point satisfying the two criteria's is based on two norms (1) amplitude in terms of local minimum and the threshold in terms of maximum.

(g) The above is repeated till all reference points which satisfy the two criteria's are located.

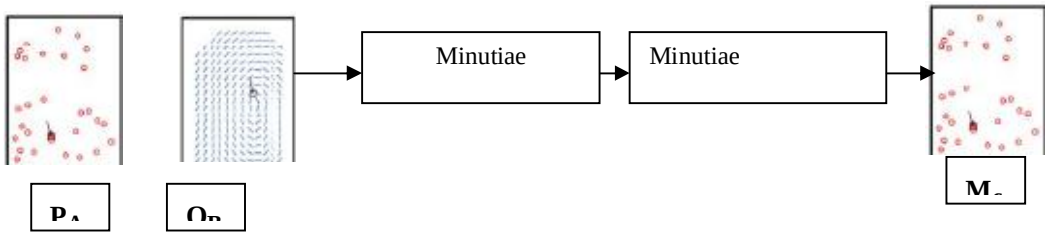

Figure 2: The Process of combined minutia template generation

(h) In some cases we are unable to fetch single reference point in that scenario whole fingerprint image taken into consideration based on maximum certainty value

3.2 The Generation of Combined Minutiae Template

The N minutiae positions from the fingerprint A, simultaneously the extracted orientation from the fingerprint B and finally combined minutiae template by references points of fingerprint A and B respectively as shown in the Figure 2.

3.2.1 Minutiae Position Alignment

(a) The minutiae position alignment has performed based on reference points where the reference points with maximum certainty value is considered as primary reference point and therefore we have two fingerprints. The reference points from two finger prints with maximum certainty value are stated as R_a and R_b respectively.

(b) Lets make an assumption that the reference point R_a is located at certain point with the angle $ß_a$ and simultaneously R_b is located at certain point with the angle $ß_b$.

(c) The final alignment process is completed by rotating and translating each and every minutiae point as shown in the following state

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

As we use convolution operator for the orientation in the complex domain, here in this minutiae positions usage of the transpose operator shows significant improvement to get positions in accurate way and this is completed after the completion of rotation and translating all minutiae positions as state below

$$H = [\cos(\beta_b - \beta_a), \sin(\beta_b - \beta_a), -\sin(\beta_b - \beta_a), \cos(\beta_b - \beta_a)] \quad (6)$$

In this alignment sometimes the chances of overlapping may also can occur in the two different fingerprints maximum certainty points values.

3.2.2 Minutiae Direction Assignment

The combined minutiae template process completed if the alignment is assigned to the reliable direction of the obtained minutiae positions and directions reference points. The respective align assign are stated as follows

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

Where

Pi is either 0 or 1 as it is integer

O_B is ranges from 0 to π

Θ_{ic} is ranges from 0 to 2π.

Finally the respective three coding strategies are stated as follows

$$\rho_i = \begin{cases} 1 & if\ mod(\theta_{ia} + \beta_b - \beta_a, \pi) - O_B(x_{ic}, y_{ic}) > 0 \\ 0 & otherwise \end{cases} \quad (8)$$

$$\rho_i = \begin{cases} 1 & if\ mod(ave_b(x_{ic}, y_{ic}), \pi) - O_B(x_{ic}, y_{ic}) > 0 \\ 0 & otherwise \end{cases} \quad (9)$$

$$ave_b(x_{ic}, y_{ic}) = \frac{1}{n}\sum_{k=1}^{n} \theta_b^k(x_{ic}, y_{ic}) \quad (10)$$

These coding strategies used to perform the best matching between combined minutiae templates and also to provide considerable good balance between the diversity and matching in reliable way.

3.3 Two Stage Fingerprint Matching

The accuracy of the matching scores is evaluated by combined minutiae template generation from the two different fingerprints is stated by this stage with the following formulas and descriptions as follows

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

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

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

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

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

$$D_\tau(u,v) = w_1 \cdot \sum_{j=1}^{3} |F_u(j) - F_v(j)| + w_2 \cdot \sum_{j=4}^{9} |F_u(j) - F_v(j)| \quad (16)$$

$$d_\tau = min_{u,v} D_\tau(u,v). \quad (17)$$

(a) The matching process is evaluated in effective way by considering the nearest, second nearest and finally third nearest. The coding strategies are used to know the differences between the respective two points and it is also helpful to detect the overlapping zonal areas.

(b) The respective matching is performed on all selected features till last selected reference so that a real fingerprint alike can be generated based on all this descriptions to protect the privacy data.

(c) The steps of matching based on angle, coding strategies and differences are repeated on all reference till final statistical result came.

(d) For each reference points two important operations are performed at this stage namely calculate the matching difference based obtained query minutiae generation. The second is getting final matching difference to get final output as combined template.

4. ALGORITHM FLOW

The dual fingerprint mechanism for privacy protection are based on the orientation and minutiae positions along with the coding strategies to obtain the template which provides the solution to the all existing problems. In past many algorithms and theoretical works has proposed based on single fingerprint which mainly lacks of secrecy and privacy, the algorithms based on single fingerprint mechanism fails to provide security to the authenticated fingerprints in the database and data can easily lost by incidental/accidental hacking. The proposed scheme provides good algorithm to provide better security to the privacy data and the important steps are as follows

(a) Estimation of Orientation O by using the orientation estimation algorithms on set of minutiae points.

(b) The Gabor filter usage makes task easy to analyze the local and global features without noise in orientations and minutiae positions without hassle.

(c) The FM AM model which is used in the past work as reported in the literature is used to estimate the phase image.

(d) Finally a reconstructed phase image is formed by combining the continuous phase image with the spiral phased image in order to get the accurate phase image.

(e) After performing the some necessary operations an improved phase is formed which is free of spurious points.

(f) Finally a real look alike fingerprint template is formed which is free of noise and provides great protection for privacy data.

5. SIMULATION RESULTS

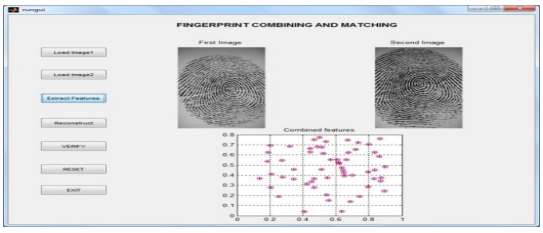

Figure 3: Extraction of minutiae points and its intersection

(a) From the above figure 3 we can get the extraction of minutiae points and its intersection, first load the image 1 then load the second image to extract the desired features.

(b) In the above image First image is totally different from the second image; here two different fingerprint approaches are
taken to get the combined minutiae features
(c) In this step the reconstruction process is performed and this task is performed in reliable way to get statistics for the verification step.

(d) Then verification of obtained features is carried on in this step to detect the reliable features, and this step is performed repeatedly to get all the reliable features as shown in the third content in the above figure.

(e) For each dual fingerprint this step is repeated by reset the previous approach.

(f) Combined features are generated from the two different fingerprints to obtain the relevant features and to obtain the relevant reconstructed mixed fingerprint which shown in figure 4.

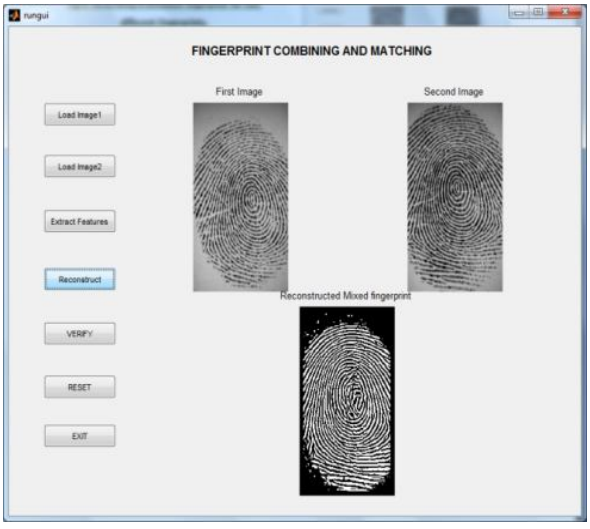

Figure 4: Generation of mixed Fingerprint

6. ANALYSIS

Table 1: Fingerprint sets with genuine and imposters value

Final Result Calculation	Combined Finger print set			
	1	2	3	4
False Acceptance rate (%)	0	0	0	0
False Rejection rate (%)	0	0.1	0.1	0.1

Table 2: Observed false acceptance and false rejection rate

Performance Analysis	Combined Finger print set			
	1	2	3	4
Total Genuine	10	10	10	10
Total Imposters	90	90	90	90
Total Combinations	100	100	100	100

Average FAR =0%
Average FRR = 0.075%

6. CONCLUSION

In this paper, we acquaint a typical arrangement for fingerprint privacy aegis by accumulation two altered fingerprints into a new identity. In the enrollment, the arrangement captures two fingerprints from two altered fingers. A combined minutiae arrangement absolute alone a fractional minutiae feature of anniversary of the two fingerprints will be generated and stored in a database. To accomplish the accumulated minutiae template attending absolute as an aboriginal development template, three different coding strategies are alien during the combined development

arrangement bearing process. In the authentication process, two concern fingerprints from the same two fingers are required. A two-stage fingerprint matching action is proposed for analogous the two concern fingerprints adjoin the enrolled template. Our combined minutiae arrangement has an agnate cartography to an original minutiae template. Therefore, we are able to amalgamate two different fingerprints into a new basic character by reconstructing a real-look a kin accumulated fingerprint from the accumulated development template. The beginning results show that our arrangement achieves an actual low absurdity amount with 0% FAR, It is as well difficult for an attacker to breach added acceptable systems by application the combined development templates. Compared with the state-of art technique, our address can accomplish a bigger new virtual character if the two altered fingerprints are randomly chosen. The assay shows that it is not simple for the antagonist to balance the aboriginal development templates from an accumulated development arrangement or a combined fingerprint.

7. REFERENCES

[1] S. Li and A. C. Kot, "A novel system for fingerprint privacy protection," in Proc. 7th Int. Conf. Inform. Assurance and Security (IAS), Dec. 5–8, 2011, pp. 262–266.

[2] B. J. A. Teoh, C. L. D. Ngo, and A. Goh, "Bio hashing: Two factor authentication featuring fingerprint data and tokenized random number," Pattern Recognition., vol. 37, no. 11, pp. 2245–2255, 2004.

[3] A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You, "An analysis of bio hashing and its variants," Pattern Recognition., vol. 39, no. 7, pp. 1359–1368, 2006.

[4] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 561–72, Apr. 2007.

[5] 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.

[6] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," IEEE Trans. Inf. ForensicsSecurity, vol. 2, no. 4, pp. 744–57, Dec. 2007.

[7] W. J. Scheirer and T. E. Boult, "Cracking fuzzy vaults and biometric encryption," in Proc. Biometrics Symp., Sep. 2007, pp. 34–39.

[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] A. Ross and A. Othman, "Visual cryptography for biometric privacy," IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 70–81,Mar. 2011.

[10] B. Yanikoglu and A. Kholmatov, "Combining multiple biometrics to protect privacy," in Proc. ICPR-BCTP Workshop, Cambridge, U.K., Aug. 2004.