International Journal of ChemTech Research
CODEN (USA): IJCRGG, ISSN: 0974-4290, ISSN(Online):2455-9555
Vol.11 No.05, pp 450-457, 2018

False acceptance and False Rejection Rate for minutiae extraction process for different users in biometric encryption.

K.Thamaraiselvi[1]*, A.Karthikeyan[1]

[1]Malla reddy College of Engineering, Telangana, India

Abstract : Fingerprint recognition is one of the most trustworthy &optimistic personnel identification techniques like aadhar, etc. Every person has unique identification fingerprint. Biometric Fingerprint identification has immense in forensic science & criminal investigations. Here we proposed storing and sharing of personal health records (PHR) in cloud environment by access using fingerprint recognition. The automatic fingerprint recognition systems are based on local ridge features called as minutiae. Minutiae are automatic identification systems based on ridge bifurcations and terminations. Here we calculated time taken for minutiae extraction process along with false acceptance rate and rejection rate for different user.
Keywords: Fingerprint, PHR and minutiae.

1. Introduction

Hospitals are in the process of transforming themselves by digitizing patient records to provide quick, safe, enhanced and cost-effective care. However this process is not without its share of problems. Passwords that are used to protect hospital computer systems from unauthorized users are not completely secure and may just provide a false sense of security. There is also a possibility of patient health records getting mixed up, misplaced or it may contain incomplete information which might result in wrong medication. Furthermore, one patient's information could be transferred into another person's record or records could pass to a wrong person resulting in medical identity fraud.

Data integrity is crucial to maintaining electronic health records as any corruption or errors could literally mean the difference between life and death. Passwords are not the best way to secure critical health records of patients. It is observed that often people forget or share their passwords or even write them down on "post-it" notes. Again some passwords are easily guessed which allows unauthorized access to hospital computer systems. The problem with traditional authentication mechanisms such as passwords, smart cards or personal identification numbers is that they can be easily shared or stolen. This jeopardizes patient confidentiality and health records leading to security breaches.

A biometric fingerprint system can effectively help to reduce these problems as it authorizes or

DOI= http://dx.doi.org/10.20902/IJCTR.2018.110548

identifies individuals based on their unique biometric characteristic. Fingerprints are inherent to individuals and thus it is undeniably the most accurate and authentic way for verifying individual identity.[1]

2. Literature Survey

K.Thamaraiselvi et.al[2], proposed minutiae identification applied to image enhancement techniques based on ridge based on ridge bifurcations and terminations and solve the problem of prone to degradation and corruption of fingerprint images due to certain factors such that skin variations and impression such as dirt, humidity, scars and non- uniform.

Shen, Kot and Koo[3], A biometric fingerprint is a normal fingerprint taken by a computer, probably to access secured areas, or to enter a person into an identification database. Fingerprints are most widely used their high acceptability, immutability and individuality. Here immutability refers unchangeable. The most automatic system for fingerprint comparison are based on minutiae matching.

V. Matyáš and Z. Říha[4], In this paper, biometric encryption is used for identification of a person at fast, accurate, unique and traditional knowledge based methods. Various biometric characters have been created which are used to authenticate the person's identity. A biometric system contains mostly an image capturing module, a feature extraction module and an example matching module. Unique finger impression is an example matching biometric strategy that is frequently used in a security setting.

K.Thamaraiselvi et.al[5] Proposed to sharing of secret images by using public and private encryption technique to solve the hidden or misuse of authenticated information to protect from particular environment.

Rinesh.S et.al[6], In this paper discussed with PHR stored secured environment along with PHR can be view only by authorize user based on biometric finger print The MA-ABBE ensures great security, authentication and efficient data sharing .

3. System Model

3.1.Minutiae extraction techniques

A good quality image is absolutely essential for minutiae extraction. However, sometimes the image quality might be poor due to various reasons and hence it becomes necessary to enhance the fingerprint images before minutiae matching of fingerprints. The minutiae extraction methods are classified into two broad categories.

1. Methods that work directly on gray-scale fingerprint images.
2. Given below is a diagram showing the different categories of minutiae extraction techniques.

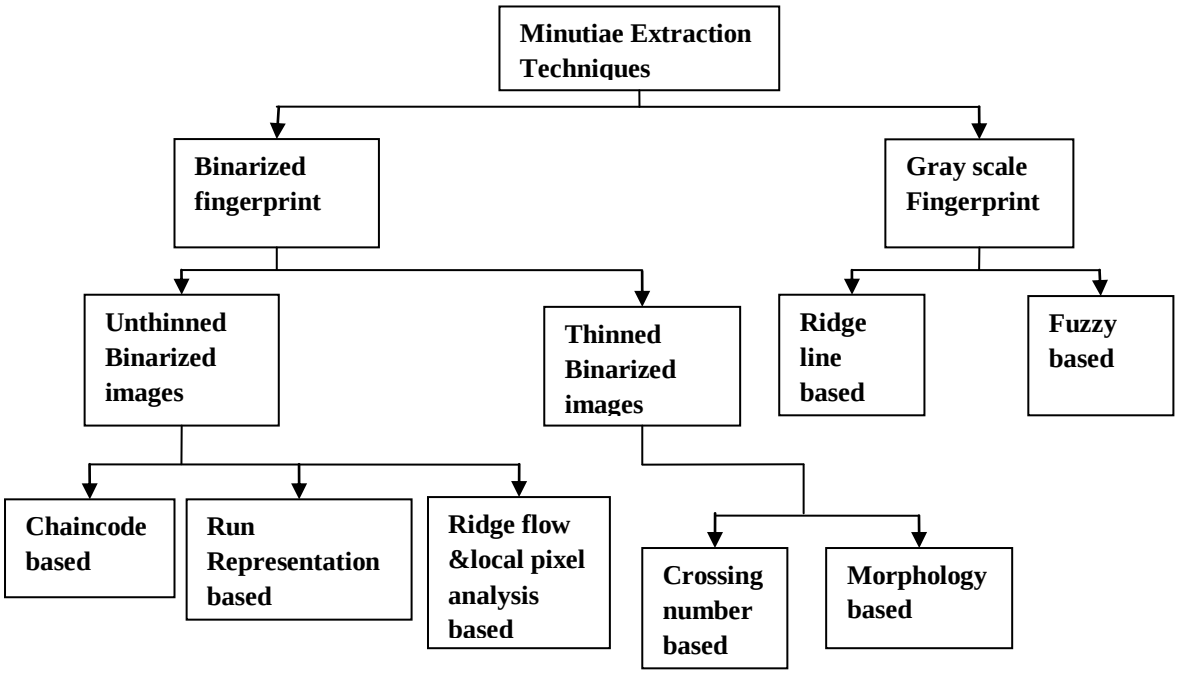

Figure 1.Classification of Minutiae Extraction Techniques

Minutiae are essentially terminations and bifurcations of the ridge lines that constitute a fingerprint pattern. *Automatic minutiae detection (AMD)* is an extremely serious process, especially in low-quality fingerprints where noise and contrast deficiency can originate pixel configurations similar to minutiae or hide real minutiae. Human fingerprints are unique to every individual, ensuring the individual's character. Since direct matching between the obscure and known fingerprint examples is exceedingly touchy to errors (e.g. various noises, damaged fingerprint regions, or the finger being set in distinctive territories of fingerprint scanner window and with diverse introduction angles, finger misshaping throughout the scanning methodology and so on.). Current systems concentrate on concentrating minutiae (points where tube lines have branches or closes) from the fingerprint image, and check matching between the sets of fingerprint features (Figure 2).

Two fingerprints have been thought about using discrete features called minutiae. These features incorporate points in a finger's friction skin where ridges end or split. The area of every minutia is represented by a direction area inside the fingerprint's image from a beginning in the lowest part left corner of the image. Minutiae orientation is represented in degrees, with zero degrees indicating horizontal and the right, and increasing degrees undertaking counter-clockwise. A decent dependable fingerprint processing procedure requires sophisticated algorithms for solid processing of the fingerprint image i.e., noise elimination, minutiae extraction, Rotation and translation-tolerant fingerprint matching.

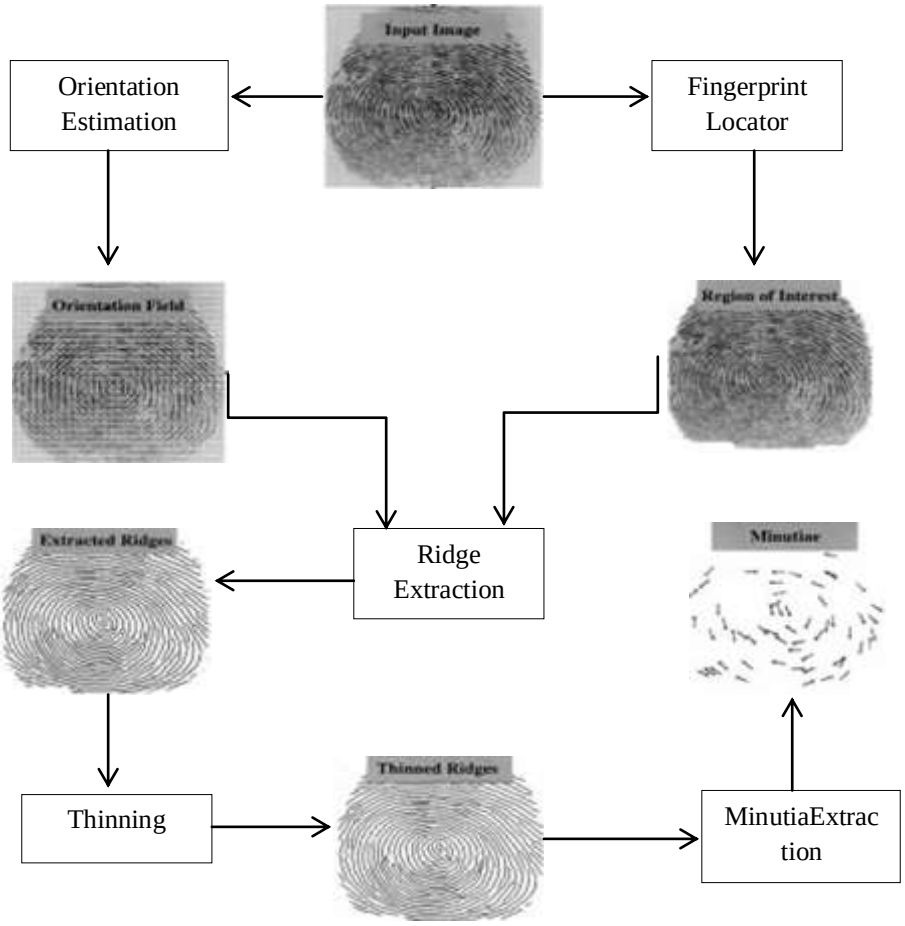

Figure 2. Minutiae Detection – Extraction Process

Due to broken ridges, fur effects, and ridge endings near the margins of an image, we have to remove the fake minutiae as described as Two endings are too close (within 8 pixels), An ending and a bifurcation are too close (< 8 pixels), Two bifurcations are too close (< 8 pixels), Minutiae are near the margins (< 8 pixels)

Fake minutia pixels include:

- Ending that lie on the margins of the region of investment.
- Two closest endings with the same ridge orientation.
- Ending and bifurcation that are associated and close enough.
- Two bifurcations are excessive.

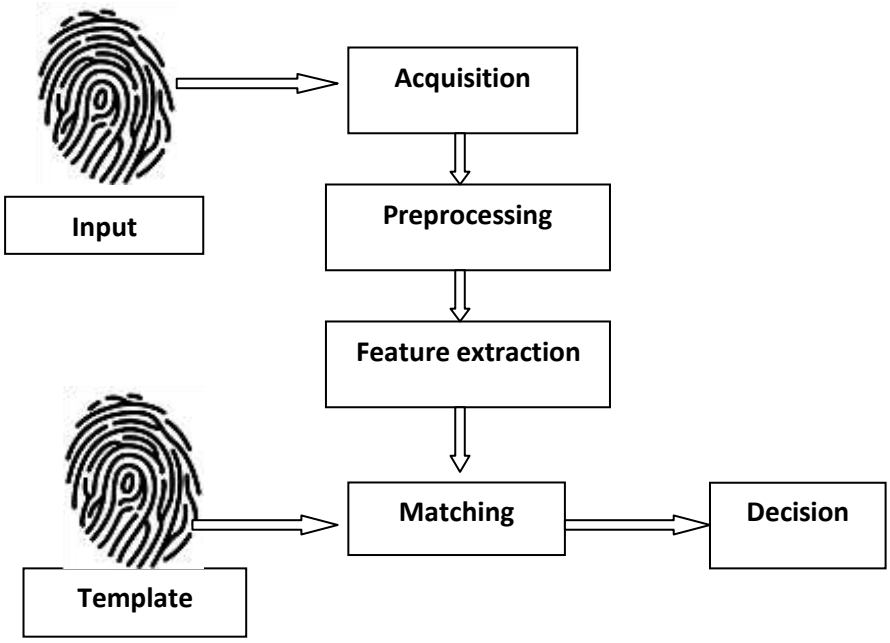

Figure 3. Processing finger print minutiae

(i) Processing of Image

Capture the fingerprint images and process them through a series of image processing algorithms to obtain a clear unambiguous skeletal image of the original gray tone impression, clarifying smudged areas, removing extraneous artifacts and healing most scars, cuts and breaks in Figure 4.

Original image **Undesirable features marked** **Final image**

Figure 4.Image processing

(ii) Fingerprint Matching

The fingerprint matcher compares information from the data hunt print against all suitable records in the database to figure out whether a possible match exists. Minutia connections, one to an alternate are compared. Not as areas inside an X-Y co-ordinate system, yet as joined connections inside a worldwide context. Every format comprises a multitude of data chunks, each data piece speaking to a minutia and comprising a site, a minutia inclination and a neighborhood. Each one site is spoken to by two coordinates. [l = (x, y)]. The neighborhood comprises of positional parameters concerning a selected minutia for a decided beforehand figure of neighbor minutiae. In single exemplification, a neighborhood outskirt is suffocating about the picked minutia and neighbor minutiae are browsed the encased region.

The next step in the algorithm is to mark all the minutiae points on the duplicate image of the input fingerprint with the lines much clear after feature extraction. Then this image is covered onto the input image with marked minutiae points as shown in the Figure.5, If the input fingerprint is matching with the original finger print after that only the health details are shared with the corresponding user. Otherwise it does not

exchange the any data among the user. Here using the biometric fingerprint is guaranteed for ensuring the authentication in personal health record.

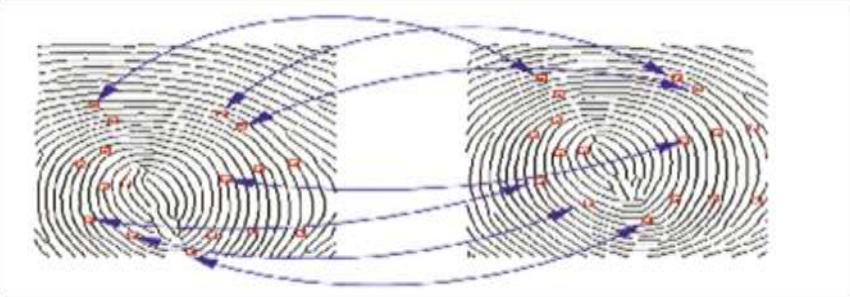

Figure.5 Performance of Minutiae Matching

4. Result and Discussion

The Fingerprint data was collected from about 50 individuals and used for evaluation based on minutiae processing techniques. Scores for each biometric trait are generated respectively. The fingerprint scores are obtained followed by the fusion technique, and calculating False Acceptance Rate and False Rejection Rate in Table 1. The preprocessing techniques are adopted from various techniques. And hence the execution time for this entire process is reduced considerably. The time taken for the minutiae extraction process are given in Table 2.

Table 1. Finger Print Vales for different user

User	**Finger print** False Acceptance Rate	**Finger print** False Rejection Rate
1-10	0.45	91.4
11-20	0.44	91.2
21-30	0.42	92.1
31-40	0.46	93.0
41-50	0.48	92.6

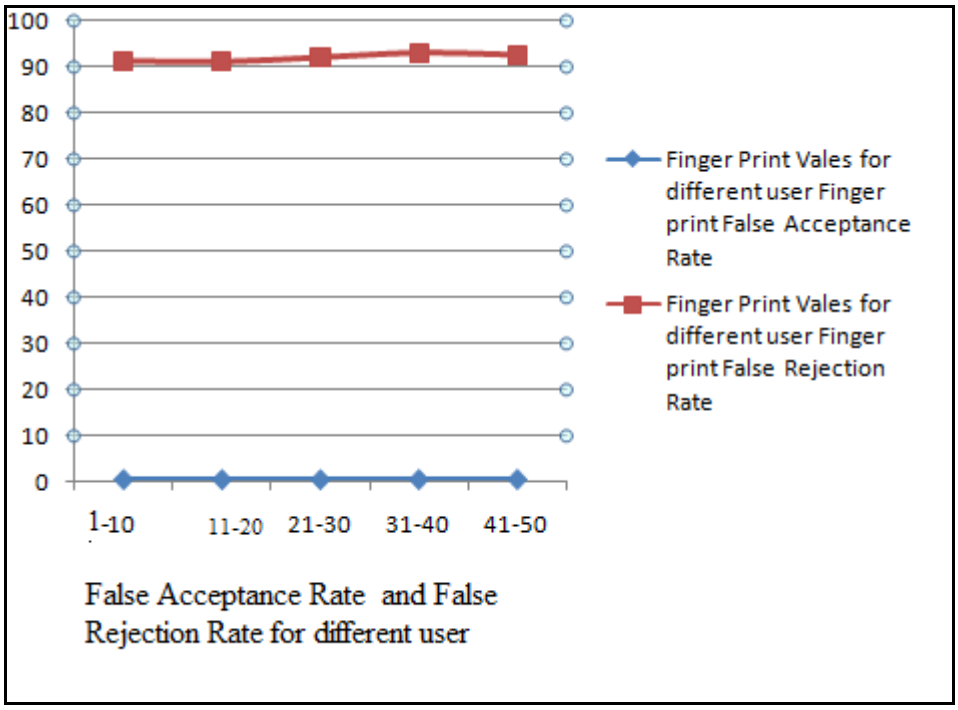

Figure: 6. Graph Shows False acceptance and Rejection rate of different user.

Table:2 Time taken for minutiae extraction process

Processing of Minutiae	**Time(Sec)**
Preprocessing	0.60
Feature extraction	0.59
Decision	0.3
Total	1.49

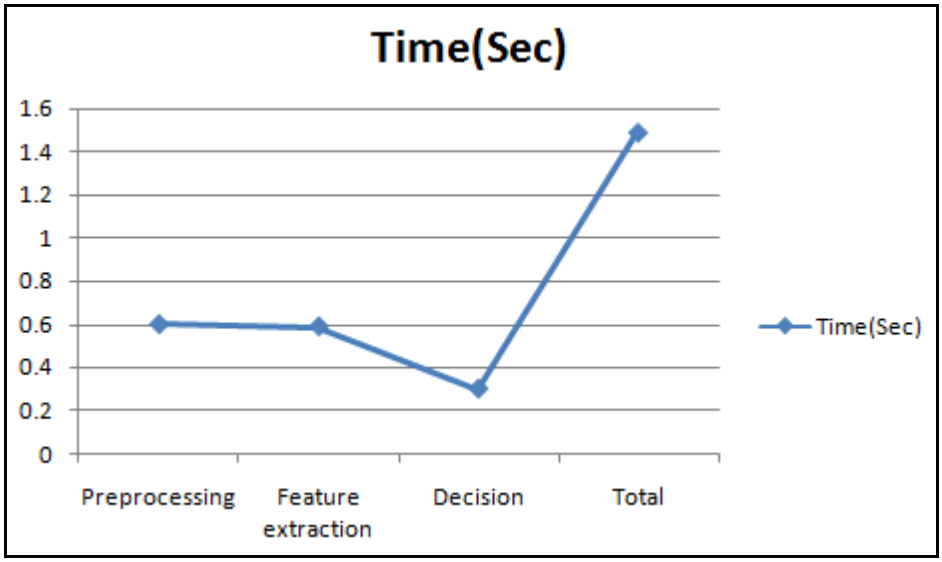

Figure: 7. Graph Shows Time taken for minutiae extraction process

5. Conclusion

In this paper, we discussed the minutiae detection and extraction process and minutiae matching techniques and we calculated time taken for minutiae extraction process along with false acceptance and false

rejection rate for different user. As a challenging field in the area of biometrics, fingerprint analysis is one of the emerging techniques used for verification and identification of an individual.

6. References

1. K. D. Mandl, P. Szolovits, and I. S. Kohane, "Public standards and patients' control: how to keep electronic medical records accessible but private," BMJ, vol. 322, no. 7281, p. 283, Feb. 2001,https://www.bayometric.com/use-of-biometric-fingerprint-readers-in-hospitals/
2. K.Thamaraiselvi,Dr.A.Mummoorthy,S.Rinesh,Dr.A.Karthikeyan,"Novel approaches of Biometric finger print minutiae detection and extraction process", International Journal of Mechanical Engineering and Technology(IJMET),vol.8,issue 12,pp.469-477,2017.
3. Shen, Kot and Koo, "Quality Measures Of Fingerprint Images", In Proc. Int. Conf. On Audio And Video Based Biometric Person Authentication.
4. V. Matyáš and Z. Říha, "Security of Biometric Authentication Systems", IJCISIM, vol. 3 (2011), pp.174–184, 2011.
5. K.Thamaraiselvi, K. Dineshkumar, A.Mummoorthy, "Cryptographic Techniques Using extracts undisclosed Image", International Journal of Advanced and Innovative Research,vol.5,issue 3,march 2016.
6. Rinesh.S, Dr.K.Baskaran,,K.Thamaraiselvi, "Secure and Resourceful Data Sharing In Cloud Using Multiple Authority Attribute Based Biometric Encryption",International Journal of Applied Engineering Research(IJAER),vol.10,number(21)2015special issues,pp.20437-20449,2015. https://www.ripublication.com /Volume/ijaerv10n21spl.htm.
7. Kim.Y, Yoon.J, JooJ.H and Yi, K. "Robust lightweight fingerprint encryption using random block feedback". DOI:10.1049/el.2013.3775 , Vol.50 , Issue 4. 2014, P: 267 - 268
8. Avinash Pokhriyal and Sushma Lehri, "A new method of fingerprint authentication using 2d wavelets," Journal of Theoretical and Applied Information Technology, 2010.
9. M. Chase and S.S. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 121-130, 2009.
10. C Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, no. 2, pp. 362– 375, 2013.

*****