

Security Enhancements for Finger Print Templates on Minutiae

Dr G.VenkataRamiReddy¹, Vidyasree.P²

¹Professor of CSE, JNTUH,

²Scholar of SIT JNTUH

Abstract-Fingerprints are widely accepted as a reliable person identification technique through out our country. Each and every person has unique and unchangeable fingerprints. This contain immutable local features called minutiae, by extracting the minutiae helps in increasing the accuracy and accepting the right ones and rejecting the false and also helps in recovery from degraded and corrupted images due to different variations on the skin. Fingerprint images are not well defined due to their noise and corrupted features, thus initially enhancing the image is very much important than the minutiae extraction. The most crucial step is extracting the minutiae from the fingerprint image. Latent examiners use these minutiae extraction for matching of the fingerprints. Extraction of the minutiae this template is stored in to the database but unfortunately this template data get hacked. Enhancing the template security by hashing and also provides the matching between the two fingers based on minutiae correspondence. By fusion of different minutiae features helps in increase the matching accuracy rate than the entire fingerprint.

Keywords –Features, Fingerprint images, Fusion, Minutiae.

1. INTRODUCTION

Biometrics is the science helps in identifying the person uniquely with the help of physical and behavioral traits[7]. Traditionally different applications are protected by the passwords and makes the user to remember too many passwords and this may results overburden to remember all these passwords and user always has to do data mining in order to retrieve the data like what password to what application in that case user may keep the related passwords to many application results in hack of data. It has many drawback like huge cost for storing the data as it needs to retrieve the data from the database and password recovery leads to two or more hits to the database which results in increase of cost. Second drawback is user has to remember bulk number of passwords this may causes severe health problems for user. Third drawback is high cost for password resetting it may leads to waste of time where the user can two or more tasks in that particular time duration. ID cards forging and password hacking may leads to loss of private information of the user and it may disasters to hack of internal data. To solve these type of problems biometric traits are used as personal identification results in increase in security[8] and also helps in protecting the data. Biometric templates are generated at enrollment time and these are intervened on the basis of user requirements, got stored in to the database , templates[9] get retrieved for further process like Identification and verification. Different templates get generated from different traits like iris, DNA, palm, finger, face etc. Among all the biometric traits fingerprints[2] are mostly widely used trait for personal identification.

Fingerprint identification helps not only in attendance , door accessing and protecting the data but also helps in forensic science to aid criminal investigations.

Fingerprint recognition system is became a challenging task as due to wet skin and dry skin and cuts, damages on the skin may represents the less quality fingerprints , feature detector on these fingerprints leads to false minutiae[1]. By the solid sensor if it may captures only some portion of the finger it may miss the some genuine minutiae[11] in that case it leads to the results of unreliable decision of two fingerprints of same finger. Elastic deformation in ridges[10] and minutiae in order to eradicate this large boundary box technique is used but it leads to increase in false acceptance rate. A fingerprint surface has different local features[13] like ridges, valleys, loops etc. termed as minutiae which differ from person to person. A single curved segment on the finger called as a ridge and the region between the two ridges is termed as valley. Ridge determines various types of minor points among them ridge endings and bifurcations are most important one.

Detail Description of minutiae

Fingerprint recognition system, are used for unique identification of the person. This system most reliable one and it cost very less compared to other biometric recognition systems. As there is drastic increase in the fingerprint recognition system but due to non linear distortion accuracy get decreased. Hence in order to increase the performance and accuracy different types of minutiae[11] are taken into notice. Minutiae are special features while scanning the finger. These minutiae are termed as a endings or bifurcations or dots etc. Some of the minutiae types are detailed below

Different types of minutiae

1. Ridge endings:

Abruptly that ends are called ridges[10]. It is a minutiae point of a fingerprint[3] at the friction ridge ending fig1.

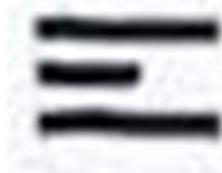


Fig 1: Ridge ending

2. Ridge bifurcations:

Ridge bifurcations are termed when a single ridge is divided into two ridges. The number of bifurcations will get vary from person to person fig2.



Fig 2: Ridge bifurcations

3. Spur:

A shorter ridge bifurcation branching off a longer ridge fig3.



Fig 3: Spur

4. Island

A ridge ending which does not connect to any of the edges . These are unique and helps in personal identification of the user fig4.



Fig 4: Island

PROPOSEDMINUTIAE EXTRACTTION AND FUSION

In the proposed system protection of the template[9] is gained by fusion two features of minutiae and providing the high level security[8] through hashing methodology. In this scenario first the user get enrolled with his name, address and with some other primary details and mostly with his fingerprint[2] . The enrolled data get cross checked and verified with database whether the user is a valid one or not. If the user is the newly registered user then an unique user ID get generated. During enrollment the enrolled template get send to preprocessing . In this preprocessing the image send to binarization[12], the process of altering the gray scale image into black and white image. Process of changing gray scale image to binary image where the white represents as one and black represents as zero. These can be done by the threshold process to the image. It basis upon the threshold value where the input value is less than threshold value then it is termed as zero and if the pixel value is greater than the threshold value then it is termed as one. The whole process is done on the analyzing the threshold values only.

After the binarization the binary image is send for the further process called thinning[6] it is also apart of preprocessing technique. In this thinning method the ridges lines are get thinned into one pixel width. So that unwanted wasted and dirt get removed from the fingerprint[3] image and it only displays the thinned and cleared image. Here it does not change any x –y coordinates or any orientation of the minutiae[4] it just only calculate the number of minutiae points like ridges and bifurcations on the fingerprint fig 5.

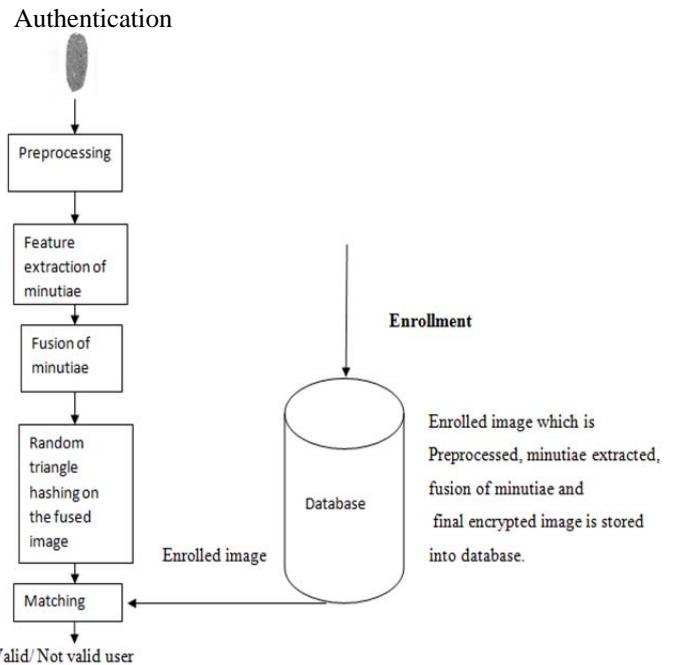


Fig5 : Overview of proposed system for fusion of minutiae

Feature extraction minutiae:

After the preprocessing the minutiae features get extracted fig 6 , there different types of minutiae extraction can be possible among them ridge endings and ridge bifurcations are been extracted for strong authentication. These features are get extracted with the technique called 3x3 window method it tells that if center is one and it is surrounded by only one neighbor value then it is ridge ending otherwise if it is surrounded by two or more neighbor values then it is termed as bifurcation[1].



Fig 6: Minutiae extraction

Fusion of minutiae:

By the feature level fusion the extracted features of ridges and ridge bifurcations are get fused after feature extraction. So that by this type of fusion the accuracy rate will get increase in person identification or verification process fig7.

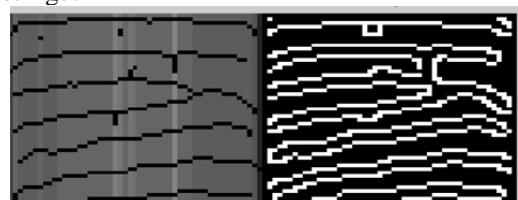


Fig 7: Fused image

Final fused image get encrypted by the random triangular hashing method where the triangle[6] are drawn on the fused image and by counting number of minutiae in the triangle[5] is taken and tend to convert into the binary value and this binary value get stored in to the database. During verification the binary hashed value get generated from the query image and get compared with the enrolled binary hash value which was stored in the database. If both hash values are same then that particular user is termed as a authenticated user otherwise the user is a unauthenticated one.

4. CONCLUSION

In present society providing security , protecting the data, finding the accurate person are the main issues and these leads to increase in false acceptance rate and false rejection rate . By fusion of different types of minutiae helps in increasing in high level accuracy rate and it reduces the cost and time during the user authentication process and this also includes input image to be binarized and thinned , for low-quality images efficient preprocessing is required for removal of dirt, unwanted waste , noises, etc. By fusion of the local area minutiae features of the finger print helps in increase of accuracy in identifying the authenticated user.

ACKNOWLEDGMENT

We thank our director Dr.GOVARDHAN & library of JNTUH, who have given their constant support in enriching our knowledge of research in the area of Biometrics. We would like to express our gratitude to all the referees authors of the research papers, who have helped directly or indirectly the possibility to complete this paper.

REFERENCES

- [1]. Manvjeet Kaur, Mukhwinder Singh, Akshay Girdhar, and Parvinder S. Sandhu," Fingerprint Verification System using Minutiae Extraction Technique", World Academy of Science, Engineering and Technology, pp. 497-502, 2008.
- [2] A.K. Jain, L. Hong, R. Bolle, On-line fingerprint verification, IEEE Trans. Pattern Anal. Mach. Intell. 19 (4) (1997) 302–313.
- [3] A. Ross, A.K. Jain, J. Reisman, A hybrid fingerprint matcher, Pattern Recognition 36 (7) (2003) 1661–1673.
- [4] M. Tico, P. Kuosmanen, Fingerprint matching using an orientationbased minutia descriptor, IEEE Trans. Pattern Anal. Mach. Intell. 25 (8) (2003) 1009–1014.
- [5] Z.M. KovQacs-Vajna, A fingerprint verification system based on triangular matching and dynamic time warping, IEEE Trans. Pattern Anal. Mach. Intell. 22 (11) (2000) 1266–1276.
- [6] A.M. Bazen, S. Gerez, Fingerprint matching by thin-plate spline modeling of elastic deformations, Pattern Recognition 36 (8) (2003)1859–1867.
- [7]. Dr.S.ViswanadhaRaju,P.Vidyasree, "Madhavi Gudavalli" Reinforcing The Security In India's Voting Process Through Biometrics" International conference on Advanced computer science and information technology Chennai September 2014.
- [8]. Dr.S.ViswanadhaRaju,P.Vidyasree, "Madhavi Gudavalli" Ameliorating The Security Of Palm Print Biometric Template Using FEC"National conference by NCETCS'14 in JNTU vijayanagaram.
- [9]. Dr.S.ViswanadhaRaju P.Vidyasree, Madhavi Gudavalli" Enhancing Security Of Stored Biometric Template In cloud Computing Using FEC"International conference on cloud computing Tirupathi January 2014.
- [10]. P.Vidyasree, Dr.G.VenkataRamiReddy " Protecting The Finger Print Template By Fusion Of Ridges And Texture" (IJCSIT) International Journal of Computer Science and Information Technologies.
- [11] J. C. Amengual, A. Juan, J. C. Prez, F. Prat, S. Sez, and J. M. Vilar, "Real-time minutiae extraction in fingerprint images", in Proc. of the 6th Int. Conf. on Image Processing and its Applications, 1997, pp. 871–875.
- [12] A. Farina, Z. M. Kovacs-Vajna, and A. Leone, "Fingerprint minutiae extraction from skeletonized binary images", Pattern Recognition, vol. 32(5), 1999, pp. 877–889.
- [13] J. Xudong and Y. Wei-Yun, "Fingerprint minutiae matching based on the local and global structures", in Proc. of International Conference on Pattern Recognition (ICPR), vol. 2, 2000, pp. 1038–1041.