Secure Fingerprint Identification System and Matching by Using Image Registration and Key Matching Techniques

Priyanka Patel
Rungta College of Engineering & Technology,
Bhilai, Chhattisgarh, India

Manisha Rajpoot
Rungta College of Engineering & Technology,
Bhilai, Chhattisgarh, India

Abstract

Fingerprint identification is a traditional field today. The paper proposes a secured fingerprint identification system. This paper use biometrics based key generation technique for the security of the fingerprint image. Biometric key generation techniques are being widely used for ensuring the privacy and realism of information. The proposed system having two types of matching, this increases the accuracy of the system. In this system firstly, feature matching image registration process is done. In these process minutiae features matching are done. The crossing number method is used for minutiae extraction of image. Another type of matching is key matching. The substitution method is used for key generation. In this type of matching if, the key generated by enrolled image is same as the key generated by input image, then image is matched otherwise not matched.

Keywords— *Fingerprint Identification System, Minutiae Extraction, Crossing Number, Biometric Key Generation, Minutiae points Matching.*

1. Introduction

A biometric is defined as a unique, measurable, biological characteristic for automatically recognizing or verifying the identity of a human being. These days, biometric technologies are typically used to analyze human characteristics for security purposes. Five of the most common physical biometric patterns analyzed for security purposes are the fingerprint, hand, eye, face, and voice. Because of the constancy and individuality, fingerprint is widely used in biometric identification. A fingerprint is made of a number of ridges and valleys on the surface of the finger. Ridges are the upper skin layer segments of the finger and valleys are the lower segments.

Fingerprint registration becomes an important issue for the success of reliable fingerprint verification using small solid state fingerprint sensors. Image registration is the process of aligning two or more images of the same scene. This process involves designating one image as the reference (also called the fixed or base image), and applying spatial transformations to the others so that they align with the reference. Images can be misaligned for a variety of reasons. Commonly, the images are captured under variable conditions that can change camera perspective. Misalignment can also be the result of lens and sensor distortions or differences between capture devices. A spatial transformation maps locations in one image to new locations in another image (for more details, see Spatial Transformations). The step of determining the correct spatial transformation parameters is key to the image registration process.

Image registration is often used as a preliminary step in other image processing applications. For example, you can use image registration to align satellite images or to align medical images captured with different diagnostic modalities. Image registration allows you to compare common features in different images. For

example, you might discover how a river has migrated, how an area became flooded, or whether a tumor is visible in image.

The uniqueness of a fingerprint can be determined by the pattern of ridges and valleys as well as the minutiae points. Biometric identification consists of two stages: enrollment and verification. During the enrollment stage, a sample of the designated biometric is acquired. Some unique characteristics or features of this sample are then extracted to form a biometric template for subsequent comparison purposes. During the verification stage, an updated biometric sample is acquired. As in enrollment, features of this biometric sample are extracted. These features are then compared with the previously generated biometric template. It is convenient to distinguish between the two main objectives of biometric systems: identification and authentication. Biometric identification is the process of matching an individual to one of a large set of system users, whereas biometric authentication simply verifies that the individual is who he or she claims to be. The performance of Fingerprint Recognition System is highly defined by the similarity of effective features in fingerprints. Minutia is one of the most widely used local features in fingerprint matching. Fingerprint recognition systems have the advantages of both ease of use and low cost. The fingerprint recognition system is used for person authentication and identification in industries and many commercial appliances [1]. A fingerprint can be defined as a pattern of ridges and valleys on the tip of the finger. A fingerprint is described by the uniqueness of the local ridge features and their relationships. Minutiae points denote these local ridge characteristics that appear either at a ridge ending or a ridge bifurcation [2]. Biometrics and cryptography play a significant role in the field of security. Cryptography & biometrics are merged to achieve high level security systems. The advantage that Biometrics presents is that the information is unique for each individual. A blend of these two technologies can produce a high level of security system [3] [8].

The main reasons for the attractiveness of fingerprint identification are

• Its success in various applications in the forensic, government, and companies for employee's attendance management;
• The existence of large databases; and
• The ease of use of compact and relatively economical fingerprint readers.

Fingerprint identification is growing a popular biometric identification technology. It includes fingerprint verification and fingerprint recognition. Both of them use minutiae, such as end points and bifurcation points, as features. Therefore, how to correctly extract minutiae from fingerprint images becomes an essential step in fingerprint identification [11].

The goal of fingerprint identification is to establish the identity of a person. In general, fingerprint identification involves comparing a query fingerprint with a large number of fingerprints stored in a database, which is time consuming. To reduce search time and lower computational complexity, fingerprint classification is often employed to partition the database into smaller subsets. The key idea is assigning a given fingerprint to a broad category using high-level features such as ridge density and ridge direction. During identification, a query fingerprint needs to be matched only against fingerprints belonging to the same category with the query [12]. Automatic Fingerprint Identification System (AFIS) is an important biometric technology. Fingerprint images can be obtained from ink impressions or by direct live scanning of the fingerprints by sensors [13].

1. Related Work

Josphineleela.R et al. [1] have described an automatic attendance system by using fingerprint reconstruction technique. Here, the reconstruction algorithm is used to automate the whole process of taking attendance, manually which is a lengthy and complex work and misuse a lot of time. In this system the fingerprint is taken as an input for attendance management and it is organized into the following modules Pre-processing, Minutiae Extraction, Reconstruction, Fingerprint Recognition, Report generation. There are two steps in Pre-processing Segmentation & Normalization. Minutiae points are extracted from composite phase image of fingerprint image which is obtained byadding spiral phase to the continuous phase. There are two steps in reconstruction Orientation Field Reconstruction & Phase Reconstruction. After reconstruction, fingerprint recognition is performed. If reconstructed fingerprint is matches with the original image, the fingerprint is recognized.

Dr.R.Seshadri et al. [2] are described here, a biometric-crypto system which generates a cryptographic key from the Fingerprints for calculating the MAC value of the information. Here, considered fingerprint because it is unique and permanent throughout a person's life. Password can be hacked by trial and error basis. But it is not possible to break the biometrics based security system.

M. Subha et al. [3] have presented a biometric security system for ATM access. Here, the multimodal biometric information is combined for mutual authentication and key generation. The use of

multimodal biometrics for key generation provides better security, as it is made difficult for an intruder to spool multiple biometric behaviors simultaneously. It is suitable for online web applications due to its efficiency in terms of both computation and communication.

A. Jagadeesan et al [4] have presented an efficient approach based on Multimodal biometrics (Iris and fingerprint) for generating a secure cryptographic key, where the security is enhance with the complexity of factoring large numbers. At first, the features, minutiae points and texture properties are extracted from the fingerprint and iris images respectively. Then, the extracted features are merged at the feature level to obtain the multi-biometric template. Finally, a multi-biometric template is used for generating a 256-bit cryptographic key. This results the security of the proposed approach to produce user-specific cryptographic key is improved.

M.S. Altarawneh et al. [5] have presented an approach to generate encryption key from fingerprint. The idea is based on slicing Window partitioning the area of extracted minutiae, using the Euclidean distance between detected core point and extracted minutiae points then vector generation used to derive a biometric key that can be used to encrypt a plaintext message and its header information. The decryption process starts with the attainment of additional biometric samples, using same steps of Bio-Key derivation to get matched plaintext.

Anil K. Jain et al. [6] have presented an automated fingerprint recognition system and identify key challenges and research opportunities in the field. Several challenging problems in fingerprint recog-nition are yet to be solved. The ever-increasing demand for reducing the error and failure rates of automated fingerprint recognition systems and the need for enhancing their security have opened many interesting research opportunities that include multiple domains such as image processing, computer vision, statistical modeling, cryptography, and sensor development.

P.Arul et al. [7] have described a Biometric-Crypto system which generates a cryptographic key from the fingerprints for encrypting and decrypting the voice data packets for VoIP Security. The system encrypts the VoIP data packets using Advanced Encryption Standard (AES) with the novel method of Biometrics based Key Generation technique.

A.Jagadeesan et al. [8] have described a system in which secure cryptographic key is generated from multimodal biometrics.

Stark Draper et al. [9] have presented here secure storage of fingerprint biometrics using Slepian-wolf codes. The system is secure because the stored data suffices to validate a probe fingerprint but not to recreate the original fingerprint biometric.

Jianwei Yang et al. [10] have presented a fingerprint feature extraction method through which minutiae are extracted directly from original gray-level fingerprint images without binarization and thinning. This algorithm improves the performance of the existing ones along this stream. This approach can achieve better Performance in both efficiency and robustness.

Uday Rajanna et al. [11] have presented a comparative study involving four different feature extraction methods for fingerprint classification and propose a rank-based fusion scheme for improving classification performance. They have compared two well-known feature extraction methods based on orientation maps and Gabor filters with two new methods based on ‘‘minutiae maps’’ and ‘‘orientation collinearity’’. The results indicate that orientation maps have the best performance, both in terms of accuracy and time.

Venu Govindaraju et al. [12] have described a feature extraction method using the chaincode representation of fingerprint ridge contours is presented for use by Automatic Fingerprint Identification Systems. This paper introduced the use of chaincode representation as an efficient alternative for processing fingerprint images. It circumvents most of the problems associated with thinning and skeleton images.

Feng Zhao et al. [13] have developed several simple and efficient preprocessing techniques for minutiae extraction from the valley instead of ridge of fingerprint. This minutiae extraction technique detect all the minutiae, including both true and false minutiae, using the simple Crossing Number on the skeleton images after validating all the bug pixels introduced at the thinning stage. This allows the true minutiae preserved and false minutiae removed in post-processing stages.

Algimantas Malickas et al. [14] have described a fingerprint registration algorithm based on feature consensus method, according to which geometric transformation relating two fingerprints is decomposed into a sequence of simpler transformations described by a single parameter, and each transformation is estimated by calculating the votes castled by pairs of the features from the two

fingerprints for the transformation consistent with the pair.

2. Proposed System

We develop a secured fingerprint identification system by using biometric key generation technique. In fig. 1 shows the flowchart of proposed system.
Steps used in proposed system as follows:
Step: 1 Input a fingerprint image.
Step: 2 Preprocessing of fingerprint image.
Step: 3 Minutiae points extraction of fingerprint image.
Step: 4 Perform feature matching image registration.
Step: 5 Generate biometric key from minutiae points of fingerprint image.
Step: 6 An image come for matching.
Step: 7 Preprocessing of fingerprint image.
Step: 8 Minutiae points extraction of fingerprint image which is come for matching.
Step: 9 Generate biometric key from minutiae points of fingerprint image.
Step: 10 Perform matching between both keys.

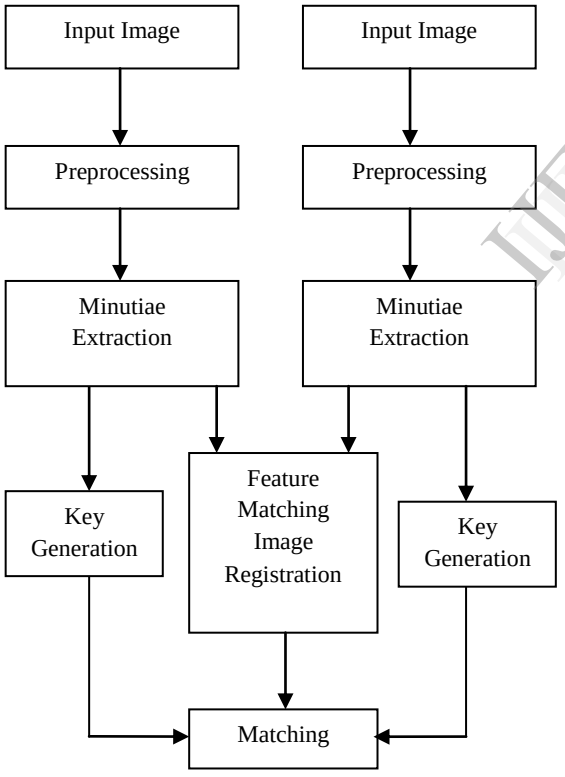

Figure-1 Flowchart of proposed system.

Minutiae points are extracted as follows:
Preprocessing
Thinning
Minutiae point extraction

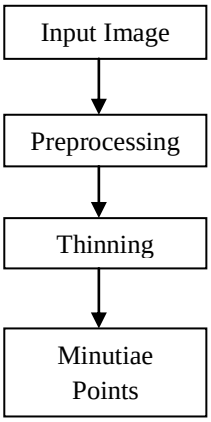

Figure 2- Flowchart of Minutiae Points Extraction

2.1 Preprocessing

In preprocessing step, in the input image the histogram equalization and binarization process is done. Histrgram equalization is used to expand the pixel value distribution of an image so as to increase the perceptional information. After histogram equalization the visualization effect is enhanced. A grey level image is translated into a binary image in the process of binarization, by which the contrast between the ridges and valleys in a fingerprint image is improved. The grey-level value of every pixel in the enhanced image is analyzed in the binarization process.

2.2 Thinning

Then thinning process is performed to reduce the thickness of the lines so that the lines are only represented excluding the other regions of the image. Clean operator, Spur operator and Thinning are the morphological operators applied.

2.3 Minutiae Points Extraction

Ridge Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. After the fingerprint ridge thinning, marking minutiae points is easy.
Minutiae are extracted by crossing number (CN) concept.
It involves various steps:
• Use of the skeleton image where the ridge flow pattern is eight connected.
• Minutiae are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3×3 window.

• CN value is computed which is half the sum of the differences is between pairs of adjacent pixels in the eight neighborhood.
The ridge pixel can then be classified as ridge ending, bifurcation, or non minutiae point.
For example:

CN	Property
0	Isolated points
1	Ridge ending point
2	Continuing ridge point
3	Bifurcation point
4	Crossing point

To perform minutiae extraction CN method is used. This method extracts the ridge endings and bifurcation from the thinned image by examining the local neighborhood of each ridge pixel using a 3×3 window. The CN for a ridge pixel P is given by

$$CN = 0.5 \sum_{i=1}^{8} |P_i - P_{i+1}|, \quad P_9 = P_1$$

Where P_i is the pixel value in the neighborhood of P For a pixel P, its eight neighboring pixels are scanned in an anti-clockwise direction [13].
After this the pixel can be classified according to the property of its CN value. For each extracted minutiae point the following information is recorded.

X and y coordinate.

Orientation of each associated ridge segment.

Types of minutiae (ridge ending and bifurcation).

After minutiae points extraction image registration is occurs. For image registration, automated feature matching technique is used. In image registration step the threshold point is fixed, which is 400, means if 400 or above the 400 minutiae features are matched then the fingerprint image is matched otherwise image is unmatched. After registration, generate a biometric key from minutiae points by using substitution method. Then these keys stored in database. When any input image come for matching then preprocessing is done then, minutiae points are extracted from input image. After this, feature matching process is done. Then, key generated from minutiae points and then key matching process is done. If keys stored in database is same as key generated from input image means image is matched.
Some advantages of proposed system:

1) Proposed system is more efficient than previous system.
2) Proposed system is more accurate than previous system.
3) It improves the security of the database in the system.

3. Conclusion

The proposed system will make a way for perfect management of students, employees and staff attendance and produce more accuracy than previous system. The key has been generated using minutiae points of image. It is not possible to break the biometrics based security system. This system enhances the security of the fingerprint image. This system improves the accuracy of the system.

4. Future Work

The work can be extended to increase the results by adopting
more effective optimization algorithms and models for estimating the image. The work can be extended by using this methodology for the multimodal biometric. The work can be extended by using different minutiae extraction algorithms to increase the performance of the fingerprint matching system, by using different key generation techniques to increase the security of the system.

References

[1] Josphineleela.R and Dr.M.Ramakrishnan, "An Efficient Automatic Attendance System Using Fingerprint Reconstruction Technique", *(IJCSIS) International Journal of Computer Science and Information Security*, Vol. 10, No. 3, March 2012.
[2] Dr.R.Seshadri and T.Raghu Trivedi, "Generate a key for MAC Algorithm using Biometric Fingerprint", *International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC)*, Vol.1, No.4, December 2010.
[3] M. Subha and S. Vanithaasri, "A Study on Authenticated Admittance of ATM Clients Using Biometric Based Cryptosystem", *International Journal of Advances in Engineering & Technology*, Sept 2012
[4] A. Jagadeesan, T.Thillaikkarasi, and Dr.K.Duraiswamy, "Cryptographic Key Generation from Multiple Biometric Modalities: Fusing Minutiae with Iris Feature", *International Journal of Computer Applications*, (0975 – 8887) Volume 2 – No.6, June 2010.
[5] M.S. Altarawneh, L.C. Khor, W.L. Woo, and S.S. Dlay, "Crypto Key Generation Using Slicing Window Algorithm",
[6] Anil K. Jain, Jianjiang Feng, and Karthik Nandakumar, "Fingerprint Matching" *IEEE Computer Society*, 0018-9162/10/$26.00 © Feb. 2010.
[7] P.Arul, and Dr.A.Shanmugam, "Generate A Key For AES Using Biometric For VOIP Network Security", *Journal of Theoretical and Applied Information Technology* © 2005 – 2009.
[8] A.Jagadeesan, and Dr. K.Duraiswamy, "Secured Cryptographic Key Generation from Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris", *(IJCSIS) International Journal of Computer Science and Information Security*, Vol. 7, No. 2, February 2010.
[9] Stark Draper, Ashish Khisti, Emin Martinian, Anthony Vetro, and Jonathan Yedidia, "Secure Storage of Fingerprint Biometrics Using Slepian-Wolf Codes", *Mitsubishi Electric Research Laboratories*, http://www.merl.com, TR2007-006 January 2007.

[10] Jianwei Yang, Lifeng Liu, and Tianzi Jiang, "An Improved Method for Extraction of Fingerprint Features", *National Laboratory of Pattern Recognition*,.

[11] Uday Rajanna, Ali Erol, and George Bebis, "A comparative study on feature extraction for fingerprint classification and performance improvements using rank-level fusion", *Springer-Verlag London Limited*, 2009.

[12] Venu Govindaraju, Zhixin Shi and John Schneider, "Feature Extraction Using a Chaincoded Contour Representation of Fingerprint Images", March 24, 2003.

[13] Feng Zhao and Xiaoou Tang, "Preprocessing for Skeleton-Based Fingerprint Minutiae Extraction", *CISST'02 International Conference.*

[14] Algimantas MALICKAS and Rimantas VITKUS, "Fingerprint Registration Using Composite Features Consensus", *Institute of Mathematics and Informatics (INFORMATICA),* Vol. 10, No. 4, 1999.