FINGERPRINT AUTHENTICATION FOR ATM

Project Guide
Mr. Ojesh Pathak

Conducted by
Parul Varshney
Paras Garg
Upendra N. Giri

INTRODUCTION

- A fingerprint is the feature pattern of fingers (Figure 1), and each fingerprint is unique, and every person has unique fingerprints. So fingerprints have being used for identification.
- A fingerprint is composed of many ridges and furrows, fingerprints are not distinguished by their ridges And furrows, but by Minutiae, which are some abnormal points on the ridges (Figure 2).
- Two types of minutiae are called termination, which is the immediate ending of a ridge and the other called bifurcation, which is the point on the ridge from which two branches derive.

Figure 1

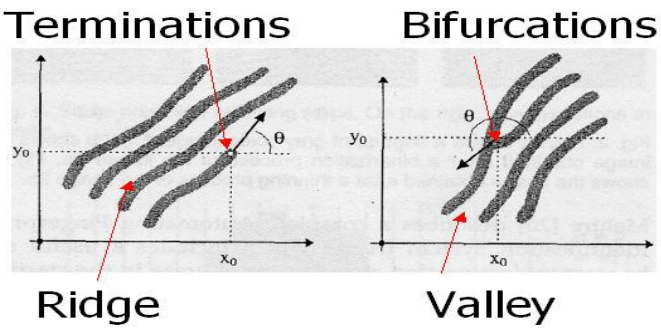

Figure 2

- The fingerprint authentication problem can be grouped into two sub-domains i.e. fingerprint verification and fingerprint identification.
- Fingerprint verification is to verify the authenticity of one person by his fingerprint and PIN Code and Fingerprint identification is by matching the information of user such as PIN Code and Fingerprint matching.

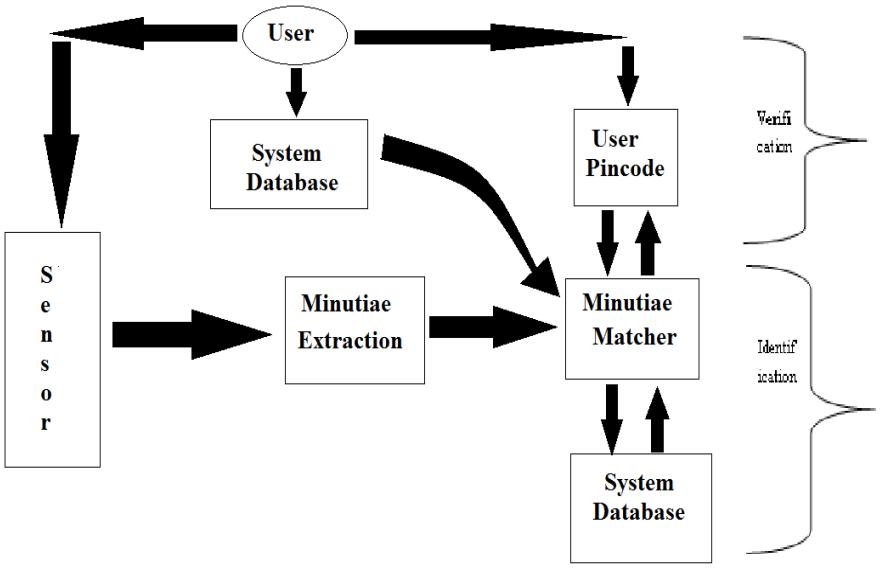

Figure 2.2. Verification vs. Identification

OBJECTIVE & SCOPE

The objective of our project is to provide biometric security through fingerprint authentication in ATM application.

- The underlying principle is the phenomenon of biometrics "AUTHENTICATION", in this project we propose a method for fingerprint matching based on matching algorithms.

SPECIFICATION

The experiment is carried out considering the following specifications:

Front End = Visual Studio 2010

Framework = .NET Framework 4.0

Database System = MS SQL Server 2008 R2

Sensor = Optical Fingerprint Sensor

Image size = 260 x 300 pixels

Pattern size = 16.1mm x 18.2 mm

Resolution = 500 DPI

METHODOLOGY

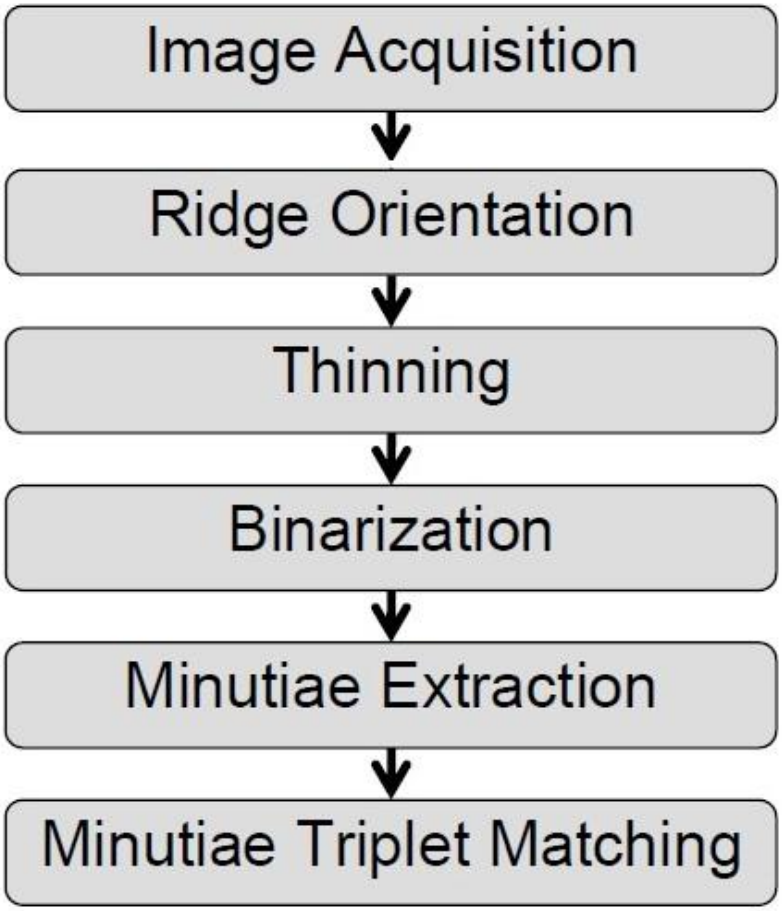

IMAGE ACQUISITION

Image acquisition is the creation of digital images, typically from a physical scene. The term is often assumed to imply or include the processing, compression, storage, printing, and display of such images. The most usual method is by digital photography with a digital camera, digital pictures with image scanners but other methods are also employed.
Here, we are using the digital image for the image processing which will we taken by the image scanners and image sensors.

RIDGE ORIENTATION

Ridge orientation is the process of obtaining the angle of the ridges throughout the image. Ridge orientations are calculated on a block-basis for a WxW block, where, W is generally equal to 16 i.e. 16x16 block.

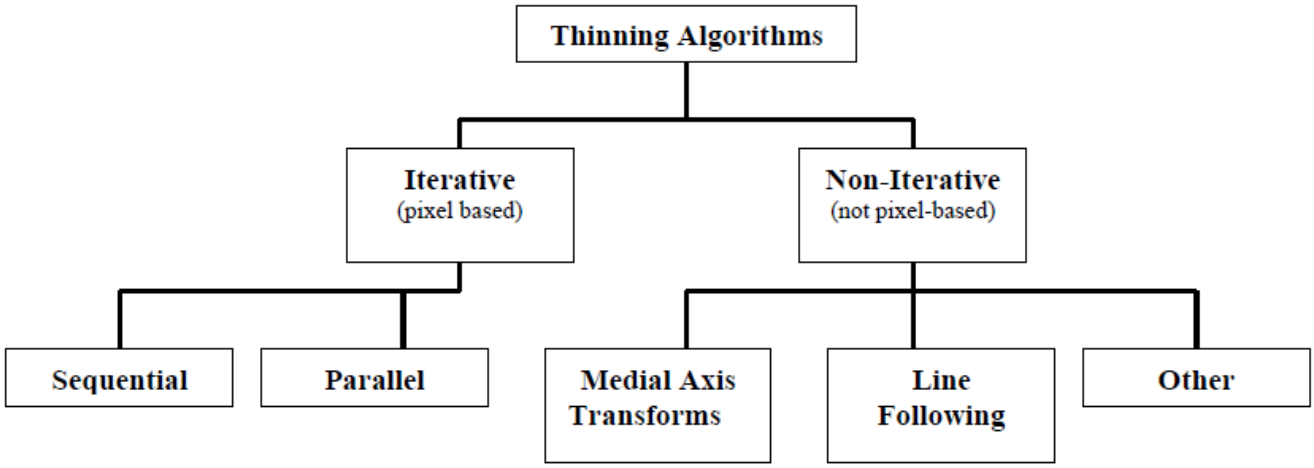

Figure 5.2 Classification of the Thinning algorithms

The table above shows a classification of thinning algorithms. The second class of sequential thinning algorithms is parallel.

In parallel thinning algorithms the decision for individual pixel deletion is based the results of the previous iteration. Like sequential algorithms, parallel thinning usually considers a 3*3neighborhood around the current pixel. A set of rules for deletion is applied based on pixels in the neighbourhood. Fully parallel algorithms have trouble maintaining connectedness, so they are often broken into sub-iterations where only a subset of the pixels is considered for deletion.

Non-iterative thinning methods are not based on examining individual pixels. Some popular non-pixel based methods include medial axis transforms, distance transforms, and determination of centrelines by line following. In line following methods, midpoints of black spaces in the image are determined and then joined to form a skeleton. This is fast to compute but tends to produce noisy skeletons. It has been conjectured that human beings naturally perform thinning in a manner similar to this.

Another method of centreline determination is by following contours of objects. By simultaneously following contours on either side of the object a continual centreline can be computed. The skeleton of the image is formed from these connected centrelines.

Medial axis transforms often use gray-level images where pixel intensity represents distance to the boundary of the object. The pixel intensities are calculated using distance transforms. In Figure below the maximum pixel intensity would increase toward the dark lines at the centres of the circles. Note that there are other methods of computing medial axis transforms.

The following is the result of the Thinning algorithm when applied to a binary image:-

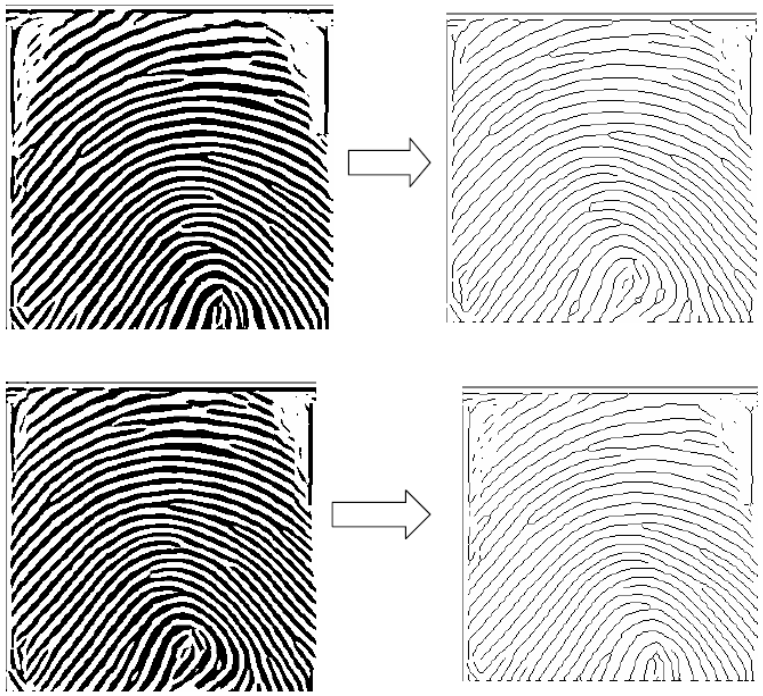

Figure 5.3 showing the result of thinning algorithm

BINARIZATION

Fingerprint binarization is to transform the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows. After the operation, ridges in the fingerprint are highlighted with black colour while furrows are white.

A locally adaptive binarization method is performed to binarize the fingerprint image. Such a named method comes from the mechanism of transforming a pixel value to 1 if the value is larger than the mean intensity value of the current block (16x16) to which the pixel belongs (Figure 5.4).

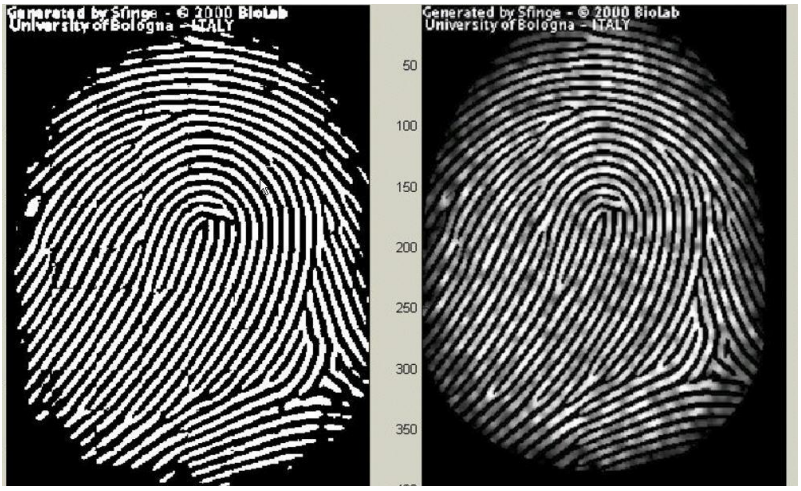

Figure 5.4 the fingerprint image after adaptive binarization binarized image (left), enhanced gray image (right)

MINUTIAE EXTRACTION

Our implementation of fingerprint identification and verification is based the topological structural matching of minutiae points. We only consider two kinds of minutiae; ridge endings and bifurcations as shown in the following figure:

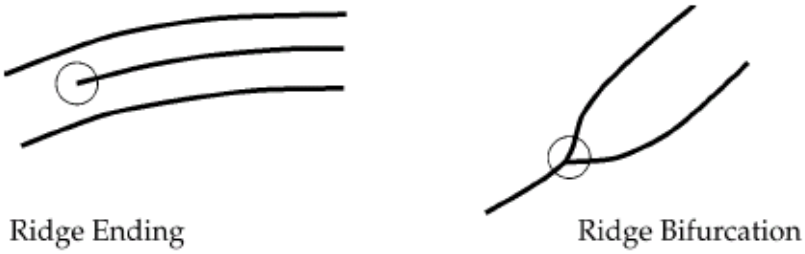

Figure 5.5 Ridge ending (left) & ridge bifurcation (right)

Minutiae extraction from a perfectly thinned ridge-map of a fingerprint image is a trivial task. All we need to do is to count the number of ridge pixels, every ridge pixel on the thinned image is surrounded by it.

However, due to noise, limitation on image acquisition, skin deformations etc the fingerprint image obtained is never ideal. As a result there are a lot of spurious minutiae that crop up if we simply follow the above approach to minutiae detection. To solve the problem, various heuristics have been proposed and we have implemented the following rules to remove most of the spurious minutiae, resulting from noise in the thinned image:

- If several minutiae form a cluster in a small region, then remove all of them except for the one nearest to the cluster centre.

- If two minutiae are located close enough, facing each other, but no ridges lie between them, then remove both of them In addition to the noise in the fingerprint image, the thinned image may not be ideal. If such is the case, minutiae extraction may not yield the correct results.

In addition to the noise in the fingerprint image, the thinned image may not be ideal. If such is the case, minutiae extraction may not yield the correct results.

MINUTIAE TRIPLET MATCHING

Minutiae triplet matching are the step which comes after minutiae extraction and it is here that we match the minutiae obtained from two sample fingerprint images and test whether they are from the same fingerprint or not.

However, a crucial step that needs to be carried out before we can use brute force and match minutiae on two images is alignment of the images. Alignment is necessary so that we correctly match the images. We also need to take care of difference in positioning of minutiae due to plastic deformations in the finger. The algorithms prevalent for minutiae-matching either include the use of details of ridges on which minutiae are present, or use the Hough transform. Both these methods and most other methods are difficult to implement and several complicated functions need to be implemented.

Hence, we decided to implement a minutiae matching algorithm which was inspired by the techniques involving computation of local and global minutiae features.

As the name suggest, it check and compare the three main component of the image during the image processing. It simultaneously check for the ridges-ending, bifurcation, and ridges-pixels. So, the accurate matching could be achieved by eliminating the risk of unnecessary matching.

CONCLUSION

A smartcard based ATM fingerprint authentication scheme has been proposed. The possession (smartcard) together with the claimed user's Biometrics (fingerprint) is required in a transaction. The smartcard is used for the first layer of mutual authentication when a user requests transaction. Biometric authentication is the second layer. The fingerprint image is encrypted via 3D map as soon as it is captured, and then is transmitted to the central server via symmetric algorithm. The encryption keys are extracted from the random pixels distribution in a raw image of fingerprint. The stable features of the fingerprint image need not to be transmitted; it can be extracted from the templates at the central server directly.

After this, the minutia matching is performed at the central server. The successful minutia matching at last verifies the claimed user. Future work will focus on the study of stable features (as part of encryption key) of fingerprint image, which may help to set up a fingerprint matching dictionary so that to narrow down the workload of fingerprint matching in a large database.

BIBLIOGRAPHY

1. Bhanu Bir, Tan Xuejun, Computational Algorithms for Fingerprint Recognition
2. Kluwer Academic Publishers, 20 Das, K. *Design and Implementation of an Efficient Thinning Algorithm*
3. Bachelor of Technology thesis, Department of Computer Science and Engineering, Indian Institute of Technology, Kanpur
4. Hong, L., Wan, Y. and Jain, A. Fingerprint Image Enhancement: Algorithm and Performance Evaluation.
5. IEEE Transactions on Pattern Analysis and Machine Intelligence,1998