IJARSE, Vol. No.4, Issue 03, March 2015 ISSN-2319-8354(E)

AN AUTHENTICATION METHOD USING FINGERPRINT RECOGNITION FOR ELECTRONIC BANKING (E-BANKING)

Nisha M[1], Aravindan M[2]

[1]*M .Tech, Embedded System Technology, Dept. of ECE/SRM University, (India)*

[2]*Assistant Professor, Department of ECE/SRM University. (India)*

ABSTRACT

Authentication is a fundamental issue to any trust oriented computing system and also a critical part in many security protocols. Passwords or smartcards have been the most widely used authentication methods due to easy implementation and replacement; however, memorizing a password or carrying a smartcard, or managing multiple passwords /smartcards for different systems is a significant overhead to users. In this paper we present an authentication using fingerprint recognition system, in which the passwords are replaced by fingerprints. Among all the biometric systems, the fingerprint recognition system is most efficient method. The system consists of image acquisition module in which the fingerprints are collected and matched with the database stored. In the proposed system, novel thinning algorithm is used along with minutae extraction method for further enhancements. The fingerprint module is implemented in ARM7 board.

Keywords: Arm7 (LPC2148), Finger print recognition, Image Acquisition Module, Minutiae Extraction, Novel-Thinning

I INTRODUCTION

Biometrics refers to the automatic identification of a person based on his/her physiological or behavioural characteristics. This method of identification is preferred over traditional methods involving passwords and PIN numbers for various reasons: the person to be identified is required to be physically present at the point-of identification; identification based on biometric techniques obviates the need to remember a password or carry a token. With the increased use of computers as vehicles of information technology, it is necessary to restrict access to sensitive/personal data. By replacing PINs, biometric techniques can potentially prevent unauthorized access to or fraudulent use of ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. PINs and passwords may be forgotten, and token based methods of identification like passports and driver's licenses may be forged, stolen, or lost. Thus biometric systems of identification are enjoying a renewed interest. Various types of biometric systems are being used for real-time identification; the most popular are based on fingerprint recognition.as it provides more easy and secured recognition when compared to iris and face recognition. Further enhancements are done using various algorithms.

II EXISTING SYSTEM

In present system for electronic banking(e-banking) ,the user opens his account using his login which contains a username and the password provided by the bank for first time logging in.after opening the account he/she can compose of his own password. When logging in every time he/she has to enter the username and password for accessing the account. After opening the account for doing transaction the user has to enter an one time password (OTP) which will be send by the bank to the user mobile number. Once the OTP is entered the transaction is done successfully.

III DISADVANTAGES OF THE EXISTING SYSTEM:

If the username and password was stolen by anyone they change the account password of their choice. The OTP can be entered by any person if the mobile number given in the bank used by the so the bank doesn't know whether it is entered by the account owner or somebody else.

IV PROPOSED SYSTEM

In the proposed system, an additional feature is added for accessing the account that is fingerprint recognition system. For this bank has to maintain the fingerprint database when the user access the he/she gives the fingerprint it has to check with the database whether it is matching or not.

The account will be opened only if the fingerprint is matched. The fake fingerprints cannot be given as the proposed system uses thinning algorithm for enhancement.

V PROPOSED SYSTEM STRUCTURE AND PROTOTYPE DESIGN

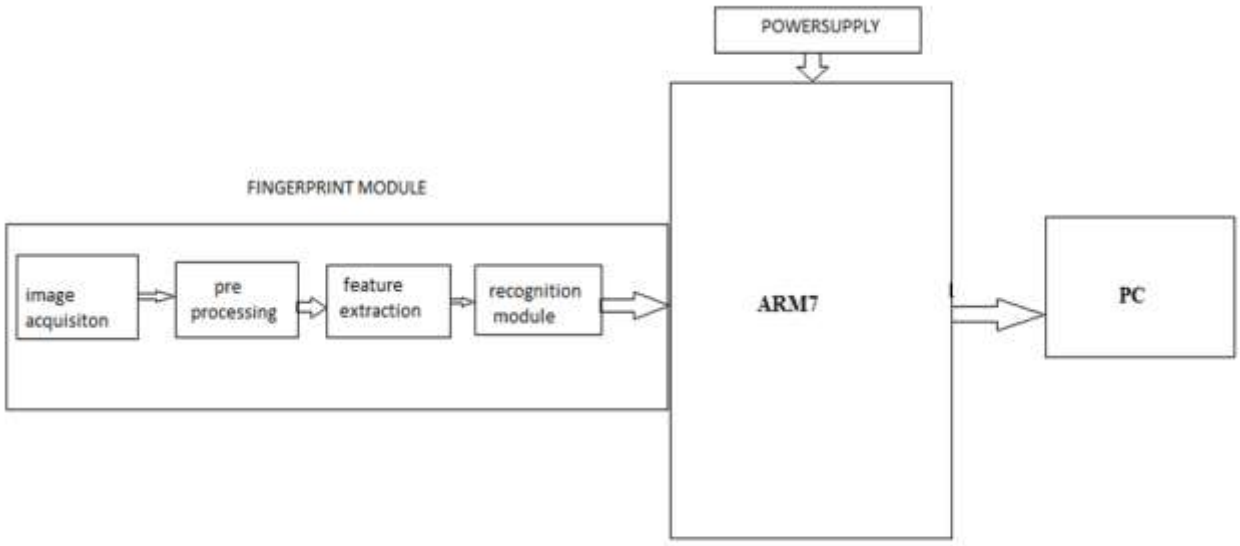

Fig 1.Block Diagram of the Proposed System

5.1 Analysis of the Hardware Structure

ARM7TDMI: ARM architecture is based on*Instruction Set Computer* (RISC) Principles. The RISC Instruction set, and related decode mechanism are much simpler than those of Complex Instruction Set Computer (CISC) designs. This simplicity gives:

- A high instruction throughput
- An excellent real-time interrupt response
- A small, cost-effective, processor macro cell.

LPC2148 is the widely used IC from arm-7 family.it is manufactured by Philips and it is pre-loaded with many inbuilt peripheralsmaking it more efficient and a reliable option. 8 to 40 kb of on-chip static RAM and 32 - 512kb of on-chip flash program memory.128 bit wide interface/accelerator enables high speed 60mhz operations.in system or in application programming(ISP/IAP) via on-chip boot loader software. Single flash sector are full chip erase in 400ms and programming of 256 bytes in 1ms.embedded ICE RT and embedded trace interfaces offer real time debugging with theon-chip real monitor software and high speed tracing of instruction execution.USB2.0 full speed compliant device controller with 2kb of end point RAM.in addition, the LPC2146/8 provides 8kb of on-chip RAM accessible to USB by DMA.multiple serial interfaces including two UART s (16C550),two fast 12C-bus (400kbit/sec),SPI and SSP with buffering and variable data length capabilities'.Individual enable /disable of peripheral function as well as peripheral clock scaling for additional power optimisation.

Fingerprint scanner:A fingerprint sensor device is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching.

5.2 Building the Prototype System

Initially the users will enrol their fingerprint images that will be saved in the data base when you are opening a account in the bank. Fig 1.block diagram of the project.

When the person whoever wants to do transaction from his account he/she has to enter his username and password. Then fingerprints should be scanned through the fingerprint module. Then the account can be accessed by generating OTP.For giving fingerprint as a input ,mouse with scanning feature can be used. When doing transaction through mobile phones, fingerprint scanner should be added in the bank webpage. If the fingerprint does not match then your account will be closed by giving a warning message. The fingerprints will be very accurate as we are using thinning algorithm which will measure only a particular of interest. The fig2 will show the complete system flow of the design.

VI SYSTEM DESIGN FLOW

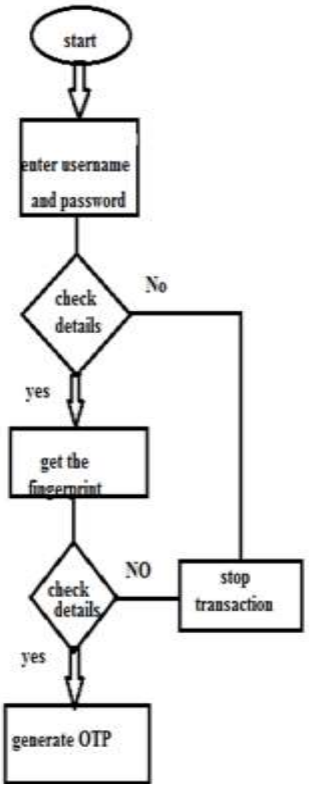

Fig2.Block Diagram of the System Flow

VII BIOMETRIC RECOGNITIONMODULE

The Biometric Recognition Systems are used to identify the person based on the feature vectors of any one of the biometric that the person possesses. These systems are person authorized systems hence offer more secure and convenient process of identification compared to alternative methods of identification. Each person has to establish the identity ranging from drivers' license to gaining entry into a country to the passport. The biometric system uses the individual's physical characteristics like fingerprint, hand geometry, face, voice or iris. A simple biometric system consists of four modules: Image acquisition, Pre-processing, Feature extraction and Recognition

7.1 Image Acquisition Module

This is the first module to acquire the biometric input. The input can be image according to the selection of biometrics. The sensors like high resolution CCD camera or recorder can be used to capture the biometric image. The distance between the sensor and human should be constant, the lighting system as well as physical capture system should be constant to acquire standard biometric input.

7.2 Pre-processing Module

Once the input is captured, the original input image or voice signal is processed to remove the noise and blurring

effect. The image is localized to extract the region of interest. The voice signal is framed to extract the desired signal. Then this processed input is given to feature extraction module

7.3 Feature Extraction Module

In the feature extraction module, the pre-processed image is used to extract the features. The feature extraction algorithms are applied to get feature vector of the biometric image. There are various feature extraction techniques like Independent Component Analysis, Linear discriminate component, principal component analysis, wavelet transform, LPC, MFCC, etc. According to the biometrics selected and its
Application the feature extraction technique can be applied.

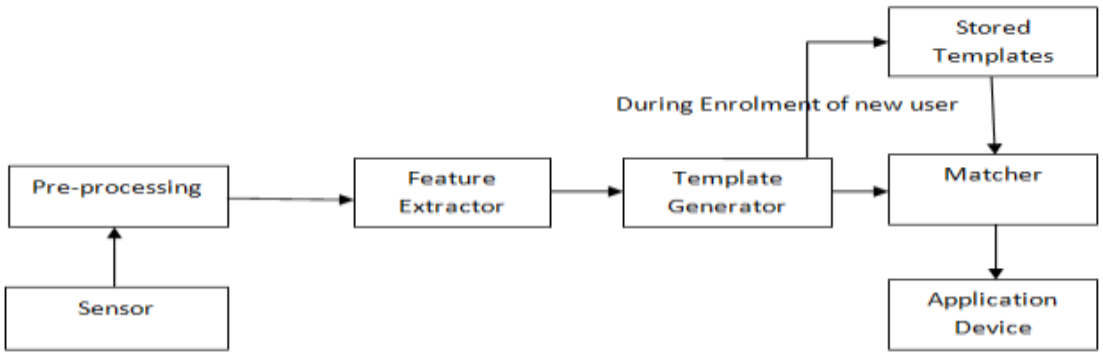

Fig 4 Block Diagram Of Fingerprint Recognition System

7.4 Recognition Module

The feature vectors, generated in the Feature Extraction Module are used in this module to classify the biometric data. There are the classifiers like hamming distance, Euclidian distance, and Support vector machine classifier. The rules are defined for recognition of a person with his /her biometrics. According to the biometric applications, the suitable classifiers can be used to get better performance of the system. The feature vectors are used to write the decision making rules. In this module user's identity is established or a claimed identity is accepted or rejected.

VIII FINGERPRINT PATTERNS

The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns. It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies.

The three basic patterns of fingerprint ridges are the **Arch, Loop,** and **Whorl.**

- An arch is a pattern where the ridges enter from one side of the finger, rise in the centre forming an arc, and then exit the other side of the finger.

- The loop is a pattern where the ridges enter from one side of a finger, form a curve, and tend to exit from the same side they enter.
- In the whorl pattern, ridges form circularly around a central point on the finger. Scientists have found that family members often share the same general fingerprintpatterns, leading to the belief that these patterns are inherited

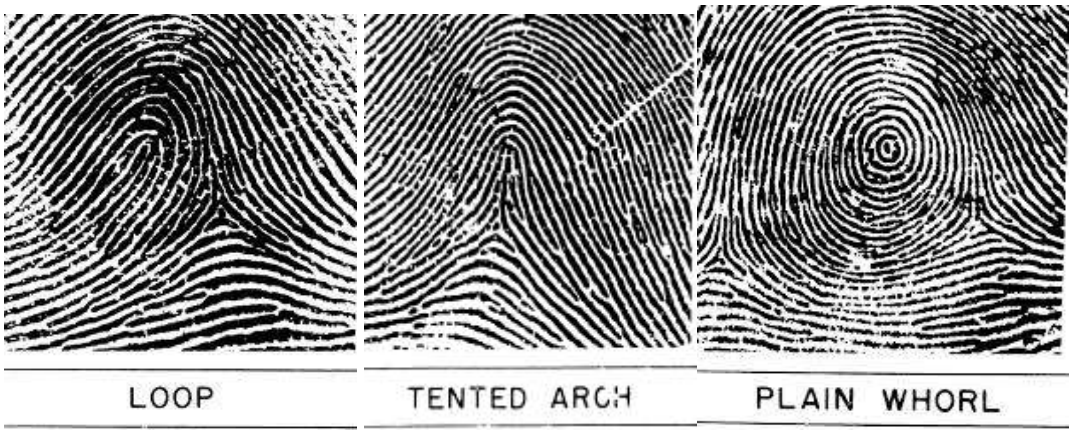

Fig 4 Fingerprint Patterns

8.1. Techniques of Fingerprint Patterns

The large number of approaches to fingerprint matching can be coarsely classified into three families:

- **Correlation-Based Matching**: Two fingerprint images are superimposed and the correlation between corresponding pixels is computed for different alignment (eg.various displacements and rotations).
- **Minutiae-Based Matching**: This is the most popular and widely used technique, being the basis of the fingerprint comparison made by fingerprint examiners.Minutiae are extracted from the two fingerprints and stored as sets of points in the two- dimensional plane. Minutiae-based matching essentially consists of finding the alignment between the template and the input minutiae sets that results in the maximum number of minutiae pairings.
- **Ridge Feature-Based Matching**: Minutiae extraction is difficult in very low-quality fingerprint images. However, whereas other features of the fingerprint ridge pattern (e.g., local orientation and frequency, ridge shape, texture information) may be extracted more reliably than minutiae, their distinctiveness is generally lower. The approaches belonging to this family compare fingerprints in term of features extracted from the ridge pattern. In principle, correlation- and minutiae-based matching could be conceived of as subfamilies of ridge feature-based matching, in as much as the pixel intensity and the minutiae positions are themselves features of the finger ridge pattern.

IX ENHANCEMENT TECHNIQUES

9.1. Image Binarisation

A binary image is a digital image that has only two possible values for each pixel. Typically the two colors used for a binary image are black and white though any two colors can be used. Numerically, the two values are often

0 for black, and either 1 or 255 for white. The color used for the object in the image is the foreground color while the rest of the image is the background color.

For an input image, some processing stages should be used before extracting minutiae. One of these stages is binarization. In this stage the gray-scale image converts into a binary image. A binary image can be processed well than a gray-scale image.

Binarisation can be done based on the threshold values. The basic idea in thresholding is to select a threshold (T) to extract an object or several objects with the same value from background. We limit our discussion to one-level thresholding for gray-scale images. Equation (1) can be used to binarize gray scale images:

$$G(x, y) = \{1, \text{iff}(x,y) > T$$

$$0, \text{if } f(x, y) < T \qquad (1)$$

Where f(x, y) is the value of a pixel in grey-scale image and g(x,y) is the binarized image. In adaptive thresholding, the image is divided into series of blocks. A threshold will be defined for each block. All pixels in the block will compare with this threshold.

Firstly, each image is divided into number of equal blocks. Next, the threshold value is calculated inside each block. Thirdly, the mean gray scale value of all blocks is calculated. Then binarisation process is carried out.

In case of fingerprint image, the image is divided into matrices which consist of rows and columns. The region of interest is selected based upon the threshold value which varies for each image. This binarisation process results some morphological changes in the image. Gabor filters are used to remove noise content the image.The disadvantage of binarization is that the ridges termination near the boundary is considered as minutia even though it is not actual minutia. The problem of binarization is eliminated in thinning process

9.2. Thinning Process

Thinning is a process of extracting a skeleton from an object in a digital image. It can also be defined as act of identifying those pixels belonging to an object that are essential for communicating the object's shape these are the skeletal pixels, and form a set. Thinning provides a convenient and condensed representation of image object information. Skeleton of an object can preserve topological properties, reduce storage requirements and reduce the transmission time. Thinning is also termed as skeletonization. Skeletonization is widely used in many image pre-processing applications, such as character recognition, pattern recognition, image coding and biological shape description.

All the thinning algorithms are classified into two broad categories:

- Iterative thinning algorithm
- Non iterative thinning algorithm

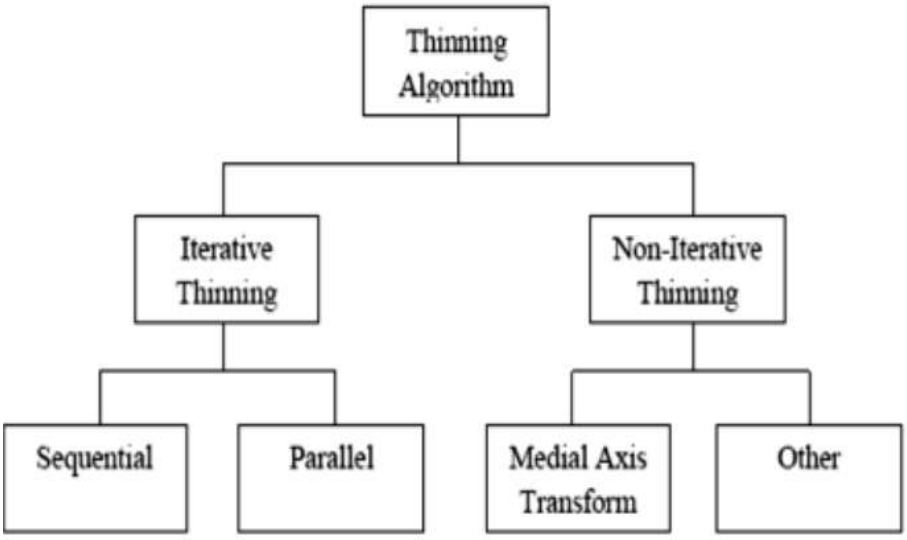

Fig5.Taxonomy of Thinning Algorithm

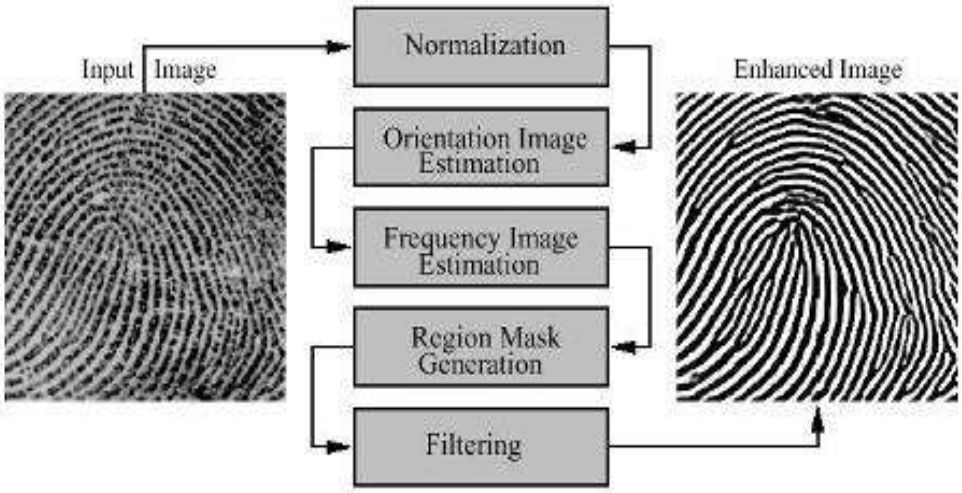

Fig.6 Steps Involved In Thinning Process

Normalization is a process that changes the range of pixel intensity values. Applications include photographs with poor contrast due to glare, for example. Normalization is sometimes called contrast stretching or histogram stretching. In more general fields of data processing, such as digital signal processing, it is referred to as dynamic range expansion

Normalization transforms an dimensional grayscale image with

$I_N : \{X \in R^n\} \rightarrow \{newmin, newmax\}$ *Eqn(2)*

Intensity values in the range (Min, Max), into a new image.

The linear normalization of a grayscale digital image is performed according to the formula

$$I_N = \frac{\{I-MIN\}Newmax-Newmin}{(max-min)} + Newmin \quad eqn(3)$$

The orientation image represents an intrinsic property of the fingerprint images and defines invariant coordinates for ridges and valleys in a local neighbourhood. By viewing a fingerprint image as an oriented texture, a number of methods have been proposed to estimate the orientation field of fingerprint images.

Given a normalised image G,the main steps of algorithm are as follows:

- Divide G into blocks of size wxw (16 x 16)
- Compute the gradient at pixel
- Estimate the local orientation of each block centered at each pixel.

Due to the presence of noise, corrupted ridge and valley structures, minutiae, etc. in the input image, the estimated local ridge orientation, $q(i, j)$, may not always be correct. Since local ridge orientation varies slowly in a local neighbourhood where no singular points appear, a low-pass filter can be used to modify the incorrect local ridge orientation. In order to perform the low-pass filtering, the orientation image needs to be converted into a *continuous vector field*, which is defined as follows

$$Fx(i, j) = \cos(2q(i, j)), \qquad \text{eqn (4)}$$

In frequency image estimation,the image is converted with respect to the position correspond to changes in the spatial image. In this no ridges and valleys appear. The gray levels along ridges and valleys can be modelled as a sinusoidal-shaped wave along a direction normal to the local ridge orientation. Therefore, local ridge frequency is another intrinsic property of a fingerprint image.

As mentioned early, a pixel (or a block) in an input fingerprint image could be either in a recoverable region or an unrecoverable region. Classification of pixels into recoverable and unrecoverable categories can be performed based on the assessment of the shape of the wave formed by the local ridges and valleys. In our algorithm, three features are

Used to characterize the sinusoidal-shaped wave: amplitude (a), frequency (b), and variance (g).

1) a = (average height of the peaks - average depth of the valleys).

2) $b = 1/T(i, j)$, where $T(i, j)$ is the average number of pixels between two consecutive peaks.

The configurations of parallel ridges and valleys with well-defined frequency and orientation in a fingerprint image provide useful information which helps in removing undesired noise. The sinusoidal-shaped waves of ridges and valleys vary slowly in a local constant orientation. Therefore, a band pass filter that is tuned to the corresponding frequency and orientation can efficiently remove the undesired noise and preserve the true ridge and valley structures. Gabor filters have both frequency-selective and orientation selective properties and have optimal joint resolution in both spatial and frequency domains.

Finally all the above processes are carried out in the image using matlab and thinned image is obtained.

MATLAB (matrix laboratory) is a multi-paradigm numerical computing environment and fourth-generation programming language. Developed by Math Works, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, Java, FORTRAN and Python

X RESULTS AND DISCUSSIONS

Theinput image is taken from the fingerprint module and it is binarisedin order to get binary image

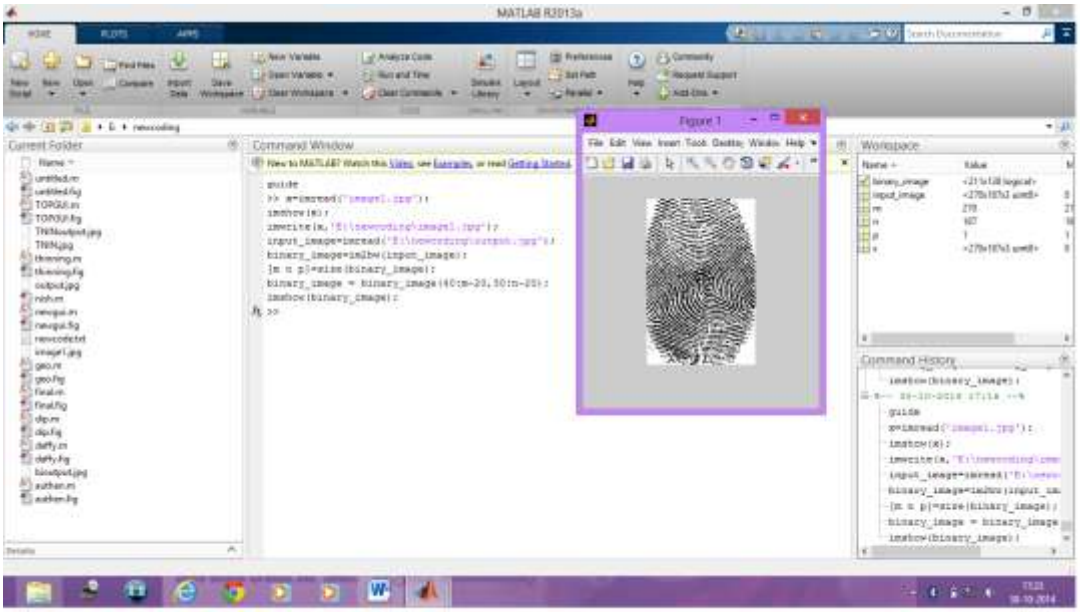

Fig.7. Simulation Output of Binarised Image

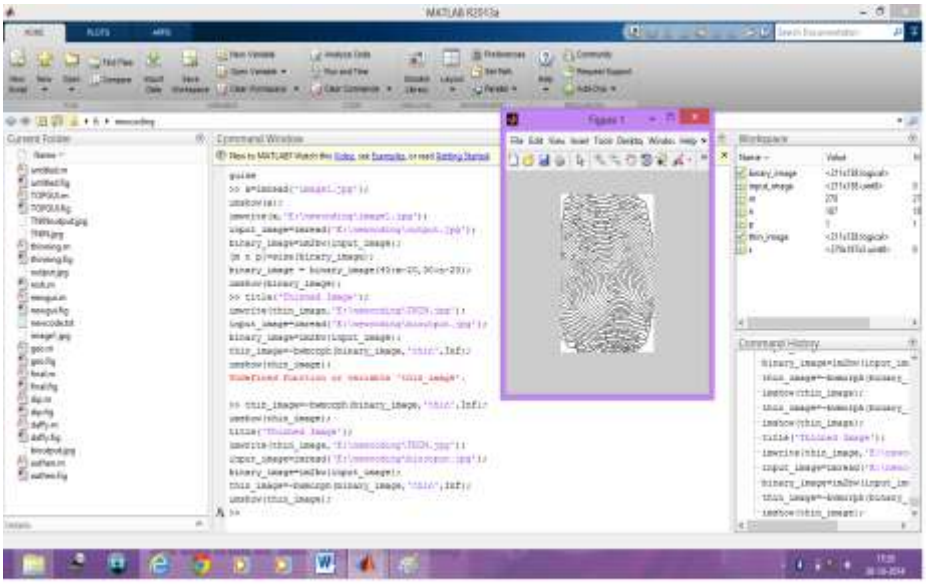

Fig 8 Simulation Output of Thinned Image

Finally the given fingerprint input is processed and enhanced using thinning algorithm to remove unwanted noise. The enhanced fingerprint is matched with the bank database.

XI CONCLUSION

Biometrics plays an important role in all authentication system. The existing system in internet banking uses only password as an authentication. The proposed systemuses fingerprints for more secured transaction. The fingerprints are enhanced with different image enhancements algorithms

REFERENCES

[1] Vaibhav.R.Pandit, Kirti.A.Joshi, *ATM Terminal Security Using Fingerprint Recognition*, International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868.

[2] khatmode Ranjit.P, *Arm7 Based Smart ATM Access & Security System Using Fingerprint Recognition& GSM Technology*, International Journal Of Emerging Technology And Advance engineering,Vol.4.Issue 2 Feb 2014.

[3] D.Shekhar Gaud, Ishaa M, *A Secured Approach For Authentication System Using Fingerprint and Iris*, Global Journal Of Advanced Engineering Technologies,Vol1, Issue3-2012,ISSN2277-6370

[4] Snehal.O.Mundhada, *Image Enhancements &Its Various Techniques*, International Journal ofAdvanced Research In Computer Science And Software Engineering,vol2,issue4,april 2012,ISSN 2277-1288.

[5]Sasan Golabi, Said Baadat, Ashcan Tashk, *A Novel Thinning Algorithm With Fingerprint MinutaeExtraction Capability*, International Journal Of Computer Theory And Engineering, Vol4, Aug 2012