ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (268-275), Month: October - December 2015, Available at: www.researchpublish.com

Enhancing Security for Online Banking Using Fingerprint Biometrics

Priyanka Mahajan[1], Supriya Malekar[2], Anuja More[3], Amol Wairagade[4], Prof. B. Mahalakshmi[5]

Department of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune, India

Abstract: **Nowadays, the banking and financial systems have been totally changed due to the environment and globalization changes and competition of business services. Internet Banking or Web Banking is used to describe banking transactions through internet application. Internet Banking means user can get connected to his bank's website with personal computer system and web browser. But there are many security problems like fraudulent websites, fake emails from banks, capturing user IDs and passwords, hacking personal bank accounts and steal money etc. To overcome these problems, this gives a solution with a Fingerprint biometric.**

Keywords: **Secure Internet banking, Finger print recognition, Banking transaction, Minutiae.**

1. INTRODUCTION

Nowadays Online Banking Transaction is increasing everywhere in the world. Users are using their ATM cards, Credit cards, Debit Cards, etc. for making Online Payment for various types of purchase of goods or bill payments. Users use their Username, Password, Card number, CVV, etc. for making Online Transactions. After User enters these details he gets a One Time Password (OTP) on his registered Mobile number. When user enters this OTP correctly then and only then the transaction gets proceeded successfully. But nowadays Hackers can easily Hack the users Bank Account and get the details of his Username, Password and Mobile number. So he can easily misuse with the users Account. So security is very much important aspect while performing Online Transactions. We need to make the transaction more secure so that the only User can access his Account and no one else.

Therefore, there should be strong authentication provided for the Online Transaction process. Our system provides this authentication by using the biometrics of the User. The biometrics is in the form of Fingerprint of the user. In our system along with the Username and Password of the User he needs to provide his fingerprint biometric for the transaction. For this the bank initially stores all the user details along with his fingerprint. Our system will check for the biometrics of the user and match it with the original biometrics stored in the bank's Database. If a valid match is found then only the user is Authenticated and treated as valid. Otherwise even if there is a small mismatch in the fingerprint the user is not allowed to access the Bank Account. Our system mainly focuses on the objective to provide security for online transaction and to see that the valid User should always get access to his account without any inconvenience.

2. LITERATURE SURVEY

TYPES OF BIOMETRICS:

There are two types of biometrics: behavioral and physical.

Behavioral biometrics: Mostly used for verification.

- Speaker Recognition - Analyzing vocal behavior.

- Signature- Analyzing signature dynamics.
- Keystroke - Measuring the time spacing of typed words

Physical biometrics: Used for either identification or verification.

- Fingerprint - Analyzing fingertip patterns.
- Facial Recognition - Measuring facial characteristics.
- Hand Geometry - Measuring the shape of the hand.
- Iris recognition - Analyzing features of colored ring of the eye.
- Retinal Scan - Analyzing blood vessels in the eye.

In our system we will prefer to use the fingerprint biometric as it is the most ancient method used to identify a person. Table below shows fingerprint versus other biometric technologies where it is ranked as 1(worst) – 5(best).

Table 1 : Comparison between different biometrics

Technology	Accuracy	Convenience	Cost	Size
Fingerprint	5	5	4	4
Voice	1	5	5	5
Face	2	3	4	3
Hand	3	3	2	2
Iris	5	2	3	3

Advantages of using Fingerprint Biometric:

- Universality–Fingerprint is universally available with every individual. Only some rare people do not have fingers.
- Uniqueness–Each individual has a unique fingerprint. No two people have same fingerprint patterns.
- Permanence–Fingerprint remains permanently with the user right from the development of seven months fetus until the person dies.
- Biometrics cannot be forgotton, lost, duplicated or stolen.
- It is more secure as it cannot be shared or used by others.
- No need to remember passwords or any PINs.
- Physical human characteristics are very much difficult to forge than passwords, security codes, or even some encryption keys.
- Biometrics gives the promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for many applications.

Disadvantages:

- Biometric systems must be able to accommodate changes to the biometric over time which may be caused by ageing, illness or injury.
- Using the fingerprint scanner can lead to false rejections.
- Using the fingerprint scanner can lead to false acceptances.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (268-275), Month: October - December 2015, Available at: www.researchpublish.com

3. EXISTING SYSTEM

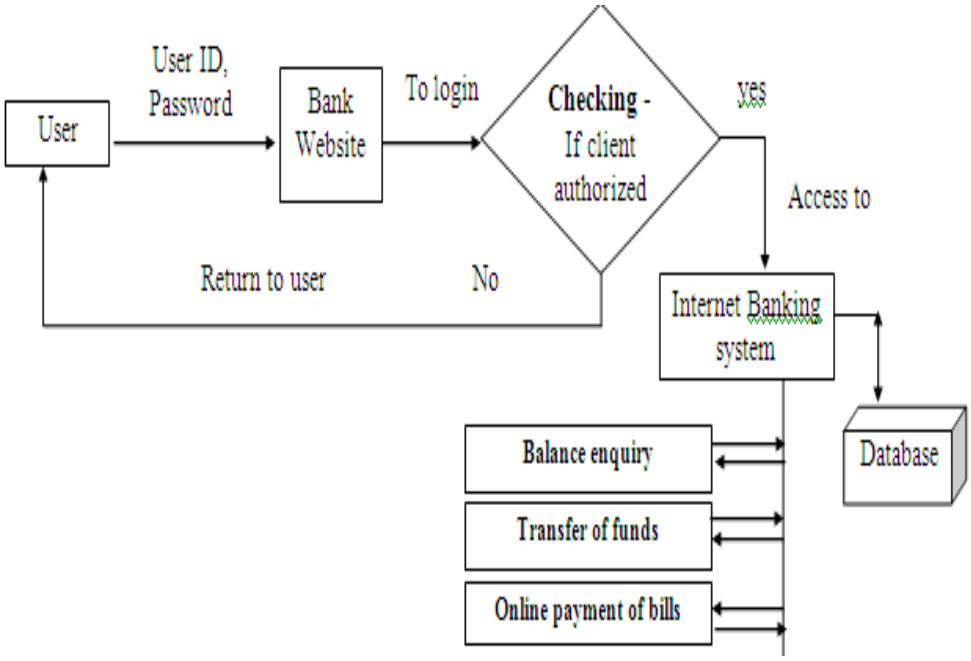

Figure 1 – Exixting system flowchart

In the existing system the banking transactions are done by online using the username and password. After entering the amount the system sends an One time Password(OTP) on the registered mobile number and then after entering the correct OTP the transaction is processed successfully. But it is not much secure as the OTP can be stolen or changed by anyone if our mobile is hacked or stolen. Thus, we need a more secure method for making our online transactions. Therefore, we use a fingerprint biometric for identification of the user.

4. PROPOSED SYSTEM

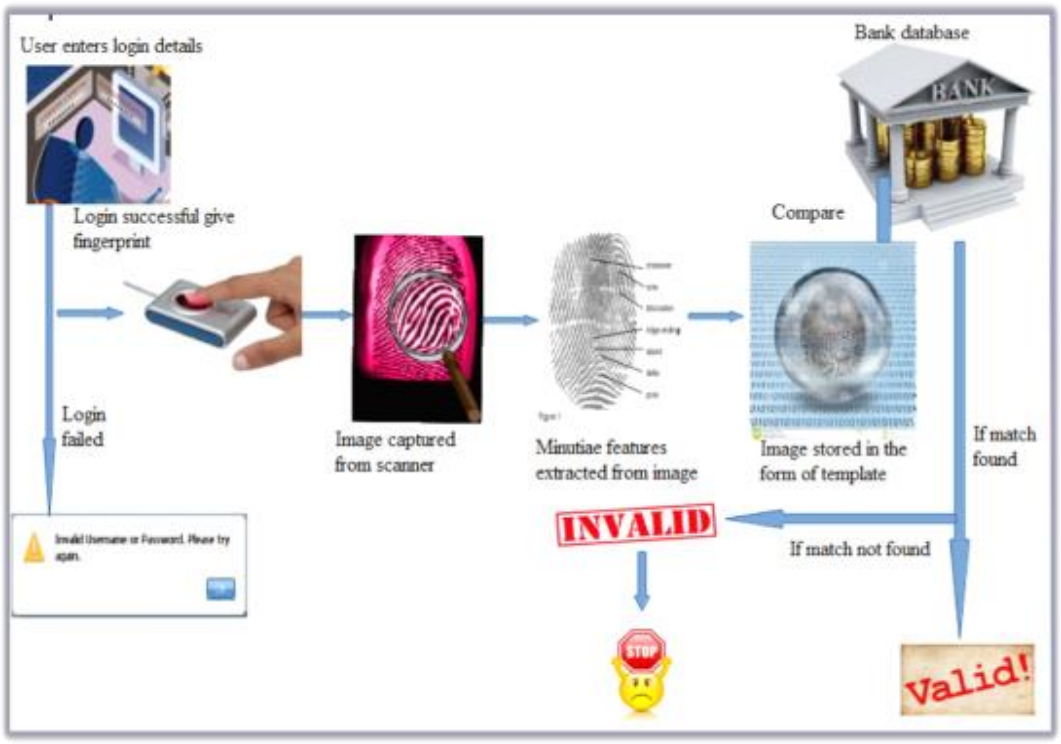

Figure 2 – Fingerprint biometric system.

The above shown Figure 2 represents the system for making online banking transaction using a fingerprint biometric. The system first takes Username and password from the user and checks if they are correct. After successful login the system asks for the fingerprint of the user. After scanning the fingerprint the minutiae features are extracted from it and stored in form of template and matching is done further. The process contains four main steps as follows :

1. Image Acquisition.
2. Image Preprocessing.
3. Minutiae extraction.
4. Minutiae Matching.

1. IMAGE ACQUISITION:

Image acquisition is first step in our system. Based on the type of image acquisition, a fingerprint image can be divided into two types as off-line or live-scan.

An off-line image is obtained by smearing ink on the fingertip and creating an inked impression of fingertip on the paper. A live-scan image, is acquired by sensing tip of finger directly, using a sensor. Live-scan is done with the help of sensors here are three types of sensors used. They are optical sensors, ultrasonic sensors and capacitance sensors. Our system uses Optical sesnsor (Fingerprint sensor mouse).

2. IMAGE PREPROCESSING:

1) Image Enhancement:

*A*s the fingerprint images are acquired from the sensors, it is not ensured that they are with a perfect quality. Therefore, we need to make the image clearer so that the further operations become easy. Probably 10 percent of all fingerprint images which are captured are of poor quality. The Method used in our system for enhancing the fingerprint is Histogram Equalization. It is most commonly used algorithms to perform contrast enhancement because of its simplicity and effectiveness. Histogram based techniques is much less expensive as compared to the other methods.

2) Image Binarization :

Fingerprint Image binarization is to transform the 8-bit gray fingerprint image to a 1-bit image in which 0-value is for ridges and 1-value is for non ridge areas also called as furrows. Algorithmic steps are as follows :

1. Divide the image into 4*4 regions.
2. Calculate the average of pixel values in the first 4*4 region.
3. Threshold the leftmost region of 4*2 by using average pixel values calculated in stage2.
4. Move the 4*4 operation window by 2 pixels to the right. If right edge of the image is reached, then move the window 4 pixels up and return to the left edge.
5. Repeat stage 2 to stage 4 until the entire image is processed by RAT (Regional average thresholding).

3) Image Segmentation :

*F*or doing any further processing on the image only a specific Region of Interest (ROI) of fingerprint image is considered. For doing this, fingerprint segmentation is used to eliminate the undesired noisy background in the image and reduce the size of the input data. The image area which is without ridges and furrows is first discarded since it only contains the background information. Then the remaining effective area i.e. ROI is sketched out. To extract this ROI, following two-step method is used. The first step is block direction computation while the second is intrigued from some morphological methods.

4) Thinning:

Thinning is the process to reduce the pixel value to 1 pixel width. It follows the following steps :

1. The image is read from bottom left to the right side line by line and the algorithm always tries to find any of black pixels in the original image . Because it is obvious that any of black pixels may be constituent of ridge.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (268-275), Month: October - December 2015, Available at: www.researchpublish.com

2. The algorithm finds out (x,y) location of the first black pixel which is not processed yet in the original binary image.

3. A black pixel is inserted into thinned image at (x,y) location (gray pixels) and the black pixel is removed from the original binary image at the location.

3. MINUTIAE EXTRACTION:

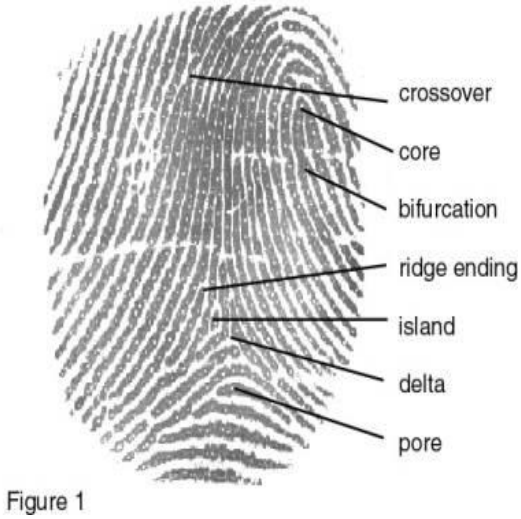

Figure 1

Figure 3: Minutiae points

Minutiae are of various types as follows:

- Ridge ending
- Core
- Crossovers
- Islands
- Delta
- Pore
- Bifurcation

Our system mainly focuses on the ridges and bifurcations.

Ridges are of different types as :

- Whorl (W) – Whorl is a pattern in which fingerprint lines create concentric circles in the center of the finger.
- Left Loop (LL) - Left Loop is a pattern in which a ridge starts from left side of a finger go towards right and forming a rotation or curvature returns to the left direction.
- Right Loop (RL) - Right Loop is a pattern in which a ridge starts from right side of a finger go towards left and forming a rotation or curvature returns to the rightt direction.
- Arch (A) – Arch is a pattern in which ridge goes in the upward direction makes a arc an returns in the downward direction.
- Bifurcation (B) – Bifurcation is a pattern in which a single ridge splits into two different ridges.
- Short Ridges (S) – Ridge which represents a single dot.

1. Pattern recognition algorithm:

The steps followed are :

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (268-275), Month: October - December 2015, Available at: www.researchpublish.com

1. Let (x,y) denote a pixel on the ridge for which we need to check values.
2. N0, N1, ….....,N7 denote its neighbours.
3. Then the pixel (x,y) is a **ridge Ending** if :

$$\sum_{i=0}^{7} N_i = 1$$

4. **Ridge Bifurcation** if :

$$\sum_{i=0}^{7} N_i > 2$$

2. Crossing Number method:

Crossing Number is calculated by checking the 8-neighbours of each central pixel (p) in order to determine the count of all the crossover occurrences in the image.

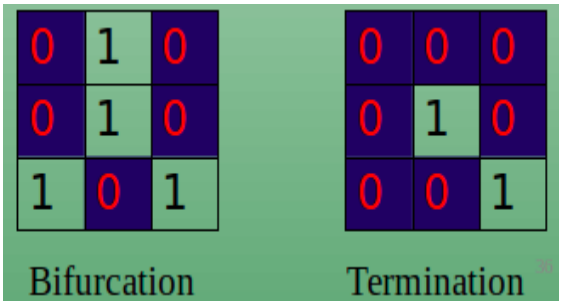

Figure 4: CN Method

For a 3x3 window:

1. If **p=1** and has only **1** one-value neighbor, then the central pixel is considered as a ridge ending.
2. If **p=1** and has exactly **3** one-value neighbors, then the central pixel is a ridge branch i.e. for a pixel P, if Cn(P) = = 1 it's a ridge end and if Cn(P) = = 3 it's a ridge bifurcation.

(Cn being the number of 1-valued neighboring pixels)

4. MINUTIAE MATCHING:

Minutiae matching is required to check whether the input image is same as that stored in the bank database. Minutiae matching can be done using different techniques as follows :

i. Point matching:

In this method the matching is done by comparing pixel by pixel. One pixel from the input image is taken and compared with one pixel from the reference image.

ii. Segment Creation:

The minutiae points extracted from the stage II are connected with each other using segments. The distance between each segment is calculated for both query and reference images. Take two minutiae points at a time. Mark a ray from both these points. Calculate angle from upper ray to the left of segment, this angle is α and calculate angle from lower ray to right of segmrnt, this angle is β. Both images match if :

$| L_r - L_q | < T$ (Tolerance of length)

$| \alpha_r - \alpha_q | < T_\alpha$ (Tolerance of upper angle)

$| \beta_r - \beta_q | < T_\beta$ (Tolerance of lower angle)

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (268-275), Month: October - December 2015, Available at: www.researchpublish.com

iii. Tree based Matching:

Two phases in order to produce a matching score:

Phase 1 - Finding common minutiae point set.

N_1 and N_2 are two images. N_1 is the Base image stored in the database and N_2 is the current input image given by the user. M is common minutiae points from both the images. 'M(i)-tuple' to represent information about minutiae is calculated. Two types of Images having two types of minutiae Base Minutiae(BM) and Input Minutiae(IM).

1. M(i)- tuple for BM

N_1 minutiae points in set N of minutiae points.

M(i)-tuple [i= 1 to N_i] is calculated as follows :

Step 1 - 5 nearest points are found using Euclidean distance

formula from i^{th} point to other.

Step 2 - If i1, i2, i3, i4 & i5 are the points then :

Calculate (i-i1), (i-i2), (i-i3), (i-i4) & (i-i5).

Find 10 ratios as (i-i1):(i-i2), (i-i1):(i-i3).....so on.

Using formula :(a-b):(a-c)=Max{(a-b),(a-c)}/Min{(a-b),(a-c)}

Step 3- Calculate Angle between 'bac' or 'cab' at a.

Extend any one of the edges (i – i1) or (i – i2)

beyond point 'i'. Here, the extended edge is (i – i1).

The angle formed by (i1 – i –extended line) will be 180 degrees always, since it is only an extension. The remaining 180 degrees is split into two angles, Angle 2 which is (Extended line – i –i2), while the other angle is the one that we want which is angle (i1 - i - i2) or (i2 - i – i1).

2. M(i)- tuple for IM

Same calculations are done for the Input image given by the user. Here N_2 represents the input image having N minutiae points.

Table 2 : M(i)-tuple

Sr. No	Ratios	Degrees
1	1.24	35
2	2.36	72
3	2.59	140
4	1.98	121
5	2.10	72

Phase 2 – Matching phase

The matching phase of this algorithm has two functions as follows.

(1) Separates the Candidate Common Points List into two lists, (a) Confirmed Common Points List and

(b) Spurious / Unconfirmed Point List.

(2) Uses the Confirmed Common Points List to generate a

Matching Score between the Base and the Input image.

5. FINDING CONFIRMED COMMON POINTS LIST

From the set N (Base Minutiae), algorithm takes only the points which feature the Candidate Common Point List to create the final tree to compare. The remaining points in this set N are listed in the set N'(BM). After considering those points, a structure like tree is drawn from bottom up. Similarly the tree is drawn from the Input image(IM). The lowest common point in both the images is considered to be the origin of an X –Y co-ordinate system. All the other points which are above this point are ordered with respect to their Y values (if Y vakue is lower, the order is lower, the origin point is order 0, the next is order 1) and when two points have the same Y value, the point with the lower X value is given the lower order.

If C (N) is the given number of points in the Confirmed Common Points List and N is the Maximum Number of points in the base, input images, then C (N) >= (N/2). If it is true, then the two images are said to be the same, else a negative score is displayed.

6. APPLICATIONS

- Can be used to make online transaction for banking applications.
- Can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks.

REFERENCES

[1] Catalin LUPU, Vasile - Gheorghita GAITAN and Valeriu LUPU, "Security enhancement of internet banking applications by using multimodal biometrics", IEEE 13th International Symposium on Applied Machine Intelligence and Informatics, January 22-24, 2015.

[2] Verginia Espinosa, "Minutiae detection algorithm for fingerprint recognition", IEEE AESS Systems Magazine, 2002.

[3] Abinandhan Chandrasekaran and Dr. Bhavani Thuraisingham,"Fingerprint Matching Algorithm Based on Tree Comparison using Ratios of Relational Distances", Second International Conference on Availability, Reliability and Security.

[4] Hossein Jadidoleslamy, "DESIGNING A NOVEL APPROACH FOR FINGERPRINT BIOMETRIC DETECTION : BASED ON MINUTIAE EXTRACTION", International Journal on Bioinformatics & Biosciences (IJBB) Vol.2, No.4, December 2012.

[5] Aliaa A.A. Youssif, Morshed U. Chowdhury , Sid Ray and Howida Youssry Nafaa, "Fingerprint Recognition System Using Hybrid Matching Techniques", 6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2012).

[6] Shashi Kumar D R, Kiran Kumar K, K B Raja, R. K Chhotaray, Sabyasachi Pattnaik, "Hybrid Fingerprint Matching using Block Filter and Strength Factors", 2010 Second International Conference on Computer Engineering and Applications.

[7] Om Preeti Chaurasia, "An Approach to Fingerprint Image Preprocessing", I.J. Image, Graphics and Signal Processing, 2012, 6, 29-35, Published Online July 2012 in MECS (http://www.mecs-press.org/), DOI: 10.5815/ijigsp.2012.06.05.

[8] R. Priya, V. Tamilselvi, G.P. Rameshkumar, "A Novel algorithm for Secure Internet Banking with finger print recognition", International Conference on Embedded Systems - (ICES 2014).

[9] Bellamkonda sivaiah, Talasila Vamsidhar, Kotha Hari Chandana, "An Efficient Approach for Fingerprint Recognition by Matching Minutiae Pairings", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 2, February 2015, ISSN:2277 128X.

[10] Ankita Mehta, Sandeep Dhariwal, "Design & Implementation of Features based Fingerprint Image Matching System", International Journal of Multidisciplinary and Current Research, Accepted 15 Dec 2014, Available online 20 Dec 2014, Vol.2 (Nov/Dec 2014 issue).