ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Cloud Based Online Website Login Using Fingerprint and OTP

Mitali Ganu[1], Sana Momin[2], Mohini Doke[3], Ms. B.R.Thawali[4],

Student, Dept. of Electronics and Telecommunication, Rajarshi Shahu College of Engineering, Tathawade, Savitribai Phule Pune University, Pune, India[123]

Prof. Dept. of Electronics and Telecommunication, Rajarshi Shahu College of Engineering, Tathawade, Savitribai Phule Pune University, Pune, India[4]

ABSTRACT: 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 preceded 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.

KEYWORDS: Security and Protection, Biometrics, Secure Internet Banking, secure transactions, Finger print recognition, Fingerprint matching, Minutiae, Binarization, Thinning, Ridges, Bifurcation, Thresholding.

I. INTRODUCTION

Nowadays, the banking and financial systems have been totally changed due to the environment and globalization changes. People are making use of Internet Banking widely. But there are many security problems such as fake e-mails for bank accounts, hacking the username and password, hacking personal bank accounts etc. This project aims at creation of a secure Internet banking system by making use of Fingerprint Biometric. The users can access their accounts with username, password and using the biometric of fingerprint for getting access. If one of these not get matched then user will not be able to get access and make further processing.On the basis of security trends and developments of the last decade, where vulnerabilities and incidents reported have increased significantly and attacks are constantly getting more sophisticated while requiring less intruder knowledge [5], innovative threat evaluation techniques for systems and software are needed. In the last few years, several innovative approaches to threat modeling have emerged. Online banking has been adopted more regularly to support and enhance the performance of the banking industry operations and management. Online banking systems provide us with easy access to banking services. Via a more sophisticated and user-friendly interface, a browser or a dedicated standalone application, people can use the Internet to connect to the bank's computer system. This increasing trend has meant that security issues of confidentiality, integrity, and privacy have become progressively more serious in online banking systems to both the banks and customers. Study on risk evaluation and threat mining of online banking system have received widespread attention [1, 2, 6].

This paper discusses the security of today's online banking systems. We present a system threat analysis method which

DOI: 10.15680/IJIRCCE.2016. 0402268

combines the STRIDE threat model and threat tree analysis. Through applying this threat analysis method to the online banking system threats analysis, we construct the online banking system threat model. Firstly, we analyze the key business online banking system data flow diagram, and then by constructing STRIDE threat model to identify the threats, and through the establishment of threat tree reducing gradually the complexity of threat analysis of online banking system. It is of important significance to the security analysis and risk evaluation of online banking system, and to deeply mining vulnerabilities and risks of online banking system.

II. MOTIVATION

The motivation for this project was lack of security while doing online transaction using previous authentication techniques. Online banking is not much secure in todays world because anyone can easily hack username and password and make transfer of money or any other malicious activity. So it is necessary to provide strong security for online banking. And using Biometrics is one of the way to do it.By making use of Biometrics we can provide security as every person has the different biometric factors and they cannot be stole easily. Making use of biometrics is one of the way to provide security.

III. LITERATURE SURVEY

In an increasingly digital world, reliable personal authentication has become an important human computer interface activity. National security, e-commerce, and access to computer networks are some examples where establishing a person's identity is vital. [5] Existing security measures rely on knowledge-based approaches like passwords or token-based approaches such as swipe cards and passports to control access to physical and virtual spaces. Though ubiquitous, such methods are not very secure. Tokens such as badges and access cards may be shared or stolen. Passwords and PIN numbers may be stolen electronically. Furthermore, they cannot differentiate between authorized user and a person having access to the tokens or
knowledge. Biometrics such as fingerprint, face and voice print offers means of reliable personal authentication that can address these problems and is gaining citizen and government acceptance.Biometrics is the science of verifying the identity of an individual through physiological measurements or behavioral traits. [6] Since biometric identifiers are associated permanently with the user they are more reliable than token or knowledge based authentication methods. Biometrics offers several advantages over traditional security measures. These include
1. Non-repudiation: With token and password based approaches, the perpetrator can always deny committing the crime pleading that his/her password or ID was stolen or compromised even when confronted with an electronic audit trail. There is no way in which his claim can be verified effectively. This is known as the problem of deniability or of 'repudiation'. However, biometrics is indefinitely associated with a user and hence it cannot be lent or stolen making such repudiation infeasible. [2, 5, 7]
2. Accuracy and Security: Password based systems are prone to dictionary and brute force attacks. Furthermore, such systems are as vulnerable as their weakest password. On the other hand, biometric **5**authenticationsrequire the physical presence of the user and therefore cannot be circumvented through a dictionary or brute force style attack. Biometrics has also been shown to possess a higher bit strength compared to password based systems and are therefore inherently secure. [3]
3. Screening: In screening applications, we are interested in preventing the users from assuming multiple identities (e.g. a terrorist using multiple passports to enter a foreign country). This requires that we ensure a person has not already enrolled under another assumed identity before adding his new record into the database. Such screening is not possible using traditional authentication mechanisms and biometrics provides the only available solution.[4]

IV. ARCHITECTURE

It shows the basic architecture of the biometric system. It has many advantages as Passwords can be forgotten, shared, or observed. Moreover, today's fast-paced electronic world means people are asked to remember a multitude of passwords and personal identification numbers (PINs) for computer accounts, bank ATMs, e-mail accounts, wireless phones, web sites and so forth. Biometrics holds the promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for a variety of applications. Another key aspect is how "user-friendly" a system is. The process should be quick and easy, such as having a picture taken by a video camera, speaking into a microphone, or touching a

DOI: 10.15680/IJIRCCE.2016. 0402268

fingerprint scanner. As biometric technologies mature and come into wide-scale commercial use, dealing with multiple levels of authentication or multiple instances of authentication will become less of a burden for users.

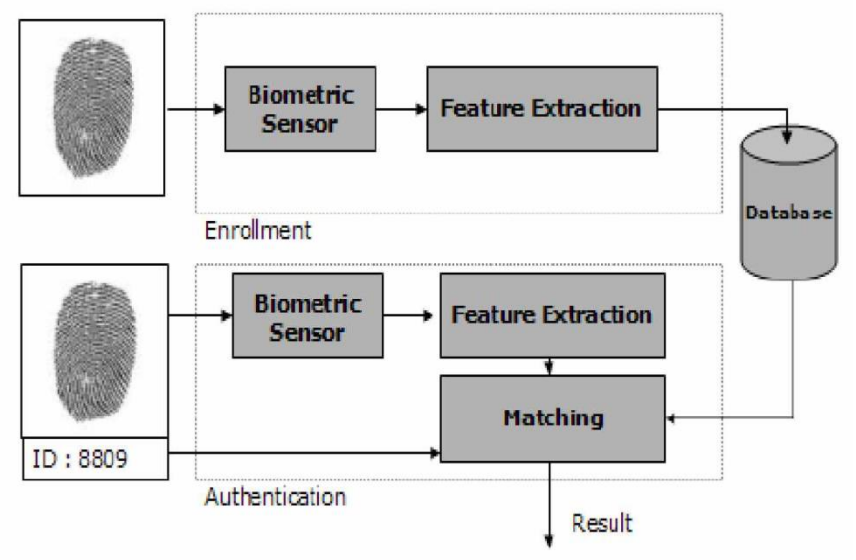


Figure
1: General architecture of biometric system

EXPLANATION-

1. **Performance Verification**

Unlike passwords and cryptographic keys, biometric templates have high uncertainty. There is considerable variation between biometric samples of the same user taken at different instances of time. Therefore the match is always done probabilistically. This is in contrast to exact match required by password and token based approaches. The inexact matching leads to two forms of errors.

1.1 False Accept - An impostor may sometime be accepted as a genuine user, if the similarity with his template falls within the intra-user variation of the genuine user.

1.2 False Reject - When the acquired biometric signal is of poor quality, even a genuine user may be rejected during authentication. This form of error is labeled as a ’false reject’.

The system may also have other less frequent forms of errors such as :-

1.3 Failure to enroll (FTE) - It is estimated that nearly 4% of the population have illegible fingerprints. This consists of senior population, laborers who use their hands a lot and injured individuals. Due to the poor ridge structure present in such individuals, such users cannot be enrolled into the database and therefore cannot be subsequently authenticated. Such individuals are termed as ’goats’. A biometric system should have exception handling mechanism in place to deal with such scenarios.

1.4 Failure to authenticate (FTA) - This error occurs when the system is unable to extract features during verification even though the biometric was legible during enrollment. In case of fingerprints this may be caused due to excessive sweating, recent injury etc. In case of speech, this may be caused due to cold, sore throat etc. It should be noted that this error is distinct from False Reject where the rejection occurs during the matching phase. In FTA, the rejection occurs in the feature extraction stage itself.

2. **Sensors**

Optical sensors capture a digital image of fingerprint. The light reflected from finger
passes through a phosphor layer to an array of pixels which captures a visual image of the fingerprint. Ultrasonic sensors use very high frequency sound waves to penetrate the epidermal coating of skin. The sound waves are generated using piezoelectric transducers. The reflected wave measurements can be used to form an image of the fingerprint. Electrical charges are created between surface of finger and each of the silicon plates when a finger is

placed on chip. The magnitude of these electrical charges depends on distance between fingerprint surface and capacitance plates. Thus fingerprint ridges and valleys result in different capacitance patterns across the plates

V. COMPONENT OF THE SYSTEM

Our system mainly works in three steps as:

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

1. **Image Pre-processing**

The performance of a fingerprint image-matching algorithm depends heavily on the quality of the input fingerprint images. It is very important to acquire good quality images but in practice a significant percentage of acquired images is of poor quality due to some environmental factors or user's body condition. The poor quality images cause two problems: (1) many spurious minutiae may be created and (2) many genuine minutiae may be ignored. Therefore, an image preprocessing is necessary to increase the performance of the minutiae extraction algorithm. The steps to do preprocessing on fingerprint are as explained below:

1. *Image Enhancement:*Since the fingerprint images acquired from sensors are not ensured with perfect quality, so to make the image clearer for easy further operations some image enhancement techniques are applied on image. According to, about 10 percent of all fingerprint images captured are of poor quality. Method adopted in our system for enhancing the fingerprint is Histogram Equalization. Histogram Equalization (HE) is one of the most commonly used algorithms to perform contrast enhancement due to its simplicity and effectiveness. Also it should be mentioned that histogram based techniques is much less expensive comparing 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. A locally adaptive binarization method is used to binaries 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. After binarization, ridges in the fingerprint are highlighted with black color while furrows are white.

3. *Image Segmentation:*In general, for doing any further operation only a Region of Interest (ROI) of fingerprint image is considered. For this, fingerprint segmentation is necessary to eliminate the undesired noisy background and reduce the size of the input data. The image area without ridges and furrows is first discarded since it only holds background information. Then the bound of the remaining effective area i.e. ROI is sketched out. To extract the ROI, following two-step method is used. The first step is block direction computation while the second is intrigued from some morphological methods.

4. Image Thinning:The final step in pre-processing is thinning before the extraction of minutiae. Thinning is a morphological operation that successively erodes away the foreground pixels until they are one pixel wide. A standard thinning algorithm is used, which performs the thinning operation using two sub iterations. The application of the thinning algorithm to a fingerprint image preserves the connectivity of the ridge structures while forming a skeletonized version of the **8** binary image. This skeleton image is then used in the subsequent extraction of minutiae. After thinning there will be some spikes present in the binary image. These spikes are removed using directional smoothing.

2. **Minutiae Extraction**

1) Minutiae

Minutiae consist of different types as shown in the figure 3.2.

- Cores
- Crossovers
- Bifurcation
- Ridge ending
- island
- delta
- pore

But we mainly concentrate on the ridge ending and bifurcation as they form the major part of the finger.

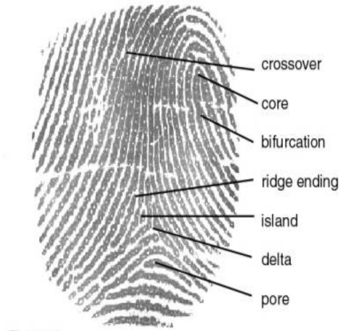


Figure 1

The first difference between fingerprints is created design and template of fingerprint lines (it called "pattern" and it be categorized as "classification"). Following figure 3.3 is showing three different patterns. These patterns are dividing into 4 major categories, including:

• Whorl;
• Left Loop (LL);
• Right Loop (RL);
• Arch;

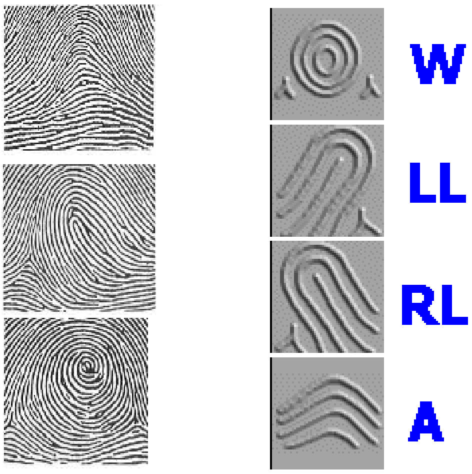


Figure 3 : Different types of patterns

2) Algorithm for minutiae extraction

The Crossing Number (CN) method is used to perform minutiae extraction. This method extracts the ridge endings and bifurcations from the skeleton image by examining the local neighbourhood of each ridge pixel using a 3×3 window. The CN for a ridge pixel P is given by:

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

where P $_i$ is the pixel value in the neighbourhood of P. For a pixel P, its eight neighbouring pixels are scanned in an anti-clockwise direction as follows:

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

After the CN for a ridge pixel has been computed, the pixel can then be classified according to the property of its CN value. As shown in Figure 3.3, a ridge pixel with a CN of one corresponds to a ridge ending, and a CN of three corresponds to a bifurcation. For each extracted minutiae point, the following information is recorded:
• x and y coordinates,
• orientation of the associated ridge segment, and
• type of minutiae (ridge ending or bifurcation).

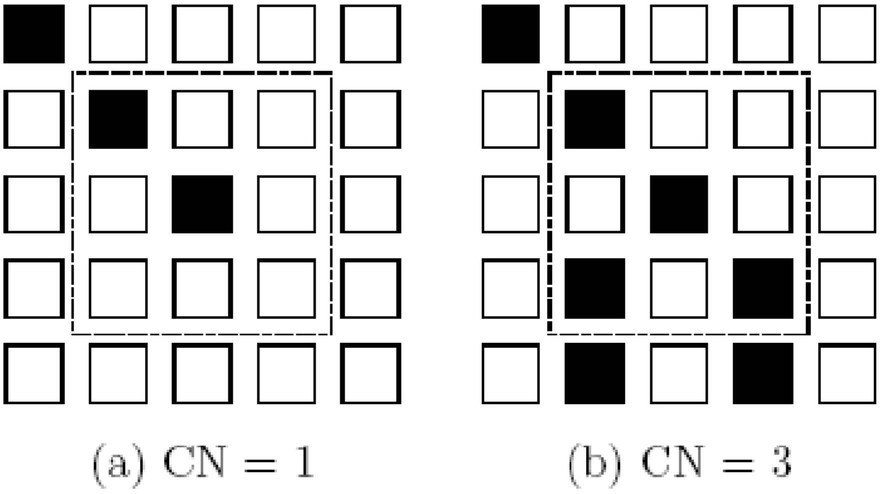


Figure 4: Examples of a ridge ending and bifurcation pixel

3. **Minutiae Matching**

Finding Common Points – Phase 1

The prime purpose of this phase is to find the number of common minutiae points available in a pair of fingerprint images. Given two fingerprint images with 'N1' and 'N2' identified minutiae points respectively (where N1 need not be equal to N2), this phase outputs the 'M' common minutiae points, which would be available in both the images. Effectively, if N1 represents the set of minutiae points in image 1 and N2 represents the set of minutiae points in image 2, M would be the intersection of N1 and N2 (M = N1 ∩ N2). We define a new term called the 'M (i) – tuple' to represent information about a minutiae that would identify it uniquely among the set of all minutiae. The M (i) – tuples of a pair of minutiae can be **10** compared/matched to find if they both are the same or not. The method followed to arrive at M follows in the next sub-section. When two images with identified minutiae points are given as input, the algorithm considers one image to be the base image (BM) and the other image to be the input image (IM). Either of them can be BM or IM and vice versa. Figure 4 shows the ideal output after phase 1.

- **M(I) – Tuples in base image (BM)**

The base image has 'N1' number of minutiae points and N (BM) is the set of all minutiae in the base image. Now, the M (i) – tuple (i = 1 to N1) for each minutiae point is calculated as follows:

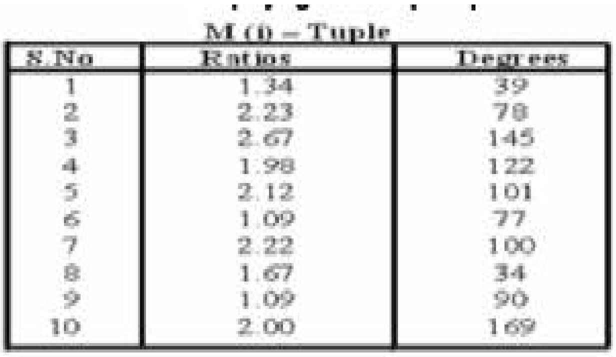
DOI: 10.15680/IJIRCCE.2016. 0402268

Step 1: For each minutiae i = 1 to N1, the 5 nearest minutiae points are found. This is done by calculating the Euclidean Distances from the 'i'th minutiae point to all the other minutiae points in the set N (BM) and noting down the 5 nearest minutiae points with respect to Euclidean Distances.

Step 2: If i1, i2, i3, i4 and i5 are the 5 nearest minutiae points of i, then we calculate M (i) – tuple in the following way:
(a) Calculate distances i – i1, i – i2, i – i3, i – i4, and i – i5. Note that distance 'i – iN' means the Euclidean Distance between the points i and iN. So here, distance i – i1 means the Euclidean distance between minutiae point i and i1 and so on.
(b) Find the following 10 ratios (i - i1): (i - i2), (i - i1): (i –i3), (i - i1): (i – i4), (i - i1): (i – i5) , (i – i2) : (i – i3), (i – i2) : (i –i4), (i – i2) : (i – i5), (i – i3) : (i – i4), (i – i3) : (i – i5), (i – i4) : (i – i5) according to the following equation : (a – b): (a – c) =Max {(a-b), (a-c)} / Min {(a-b), (a-c)}.
While finding the ratio (i – i1): (i – i2), the angle between them can be found by the following way. 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 just an extension. The remaining 180 degrees is split up by 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). So always this angle would never be greater than 180 degrees. Table 3.2 displays how M(i)– tuple of each minutiae would look like. This is how the tuple for each minutia in the set N (BM) is constructed.

- **M(I) – Tuples in Input image (IM)**

Steps that were followed for the Base Image apply to the Input image also. If N2 represents the number of minutiae in the input image and if N (IM) represents the set of all minutiae in the input image, run Step 1 and 2. Now we have the tuples of all the minutiae points in the input image as well. Now, for all the M (i) – tuples in the input image, where i = 1 to N2, compare with all the tuples of the base image.



M (i) – Tuple

S.No	Ratios	Degrees
1	1.34	39
2	2.23	78
3	2.67	145
4	1.98	122
5	2.12	101
6	1.09	77
7	2.22	100
8	1.67	34
9	1.09	90
10	2.00	169

Table 3.3 : M(i) - Tuple

Matching phase

The matching phase of the algorithm does two functions.
(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.

- **Finding confirmed common points list**

From N (BM), which is the set of minutiae points in the base image, the algorithm considers only those points that feature in the Candidate Common Point List to create the tree. The remaining points in the set N(BM) are listed in the set N'(BM). After those points are considered, a tree like structure is drawn from bottom up. Similarly from N(IM), algorithm considers points that feature in the Candidate Common Point List to create the tree and the remaining points are listed in the set N'(IM). The Candidate Common Points in the Base and the Input image are ordered as follows. 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 that are above this point are ordered with respect to their Y values (lower the Y value, lower the order, so the origin point is order 0, the next is order 1 and so on), and when two points happen to have the same Y value, the point with the lower X value is given the lower order. Effectively the order increases bottom up in the image. After ordering all the Candidate Common Points, they are connected from bottom up with respect to their order in both the images.M(i) – tuples are created. These tuples are matched to find any new Candidate Common Point. If any such points are found, they are added to the tree and the matching procedure by comparing edges and removing spurious points is once again followed till no edges can further be removed. Now, essentially what the algorithm has resulted in is a tree whose vertices feature in the Confirmed Common Points List, which in turn indicates the common minutiae points in both the images. If C (N) is the 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 this is true, then the two images are said to be the same, else a negative score is displayed

VI. CONCLUSIONS

The document mainly deals with the requirements for the system for authentication using fingerprint biometrics. It describes in brief about the enhancement, extraction and matching of fingerprint images. It contains the details of types of biometrics, its advantages over password/key authentication. It also contains the advantages of finger-print biometric. It briefs about the image preprocessing techniques.The Crossing Number method has been used for feature extraction of minutiae. This method is able to detect accurately all valid bifurcations and ridge endings from the thinned image.For matching purpose an alignment-based matching algorithm is studied. In this, input minutiae are aligned with the template by estimating the parameters between an input and a template. The input which satisfies the matching score is declared as a matched fingerprint with the template.The document gives detailed architecture of the system along with its data objects, relationships, mathematical formulation, etc. It gives details of the software, hardware and user resources required for the system. Necessary diagrams are also described. Therefore, we have done detailed requirement documentation for our Online banking system. We have also identified the data objects, relationships between them, activity flow, system architecture, etc. We will implement a system for providing strong authentication for online banking transactions.

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, 2012.

[3] AbinandhanChandrasekaran and Dr.BhavaniThuraisingham,”Fingerprint Matching Algorithm Based on Tree Comparison using Ratios of Relational Distances”,Second International Conference on Availability, Reliability and Security.

[4] HosseinJadidoleslamy, “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 HowidaYoussryNafaa, “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, SabyasachiPattnaik, “Hybrid Fingerprint Matching using Block Filter and Strength Factors”, 2010 Second International Conference on Computer Engineering and Applications.

[7] Om PreetiChaurasia, “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] Bellamkondasivaiah, TalasilaVamsidhar, KothaHariChandana, “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, SandeepDhariwal, “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).