Feature Level Fusion of Multimodal Biometrics and Two Tier Security in ATM System

N.Geethanjali
PG Student,
Department of IT,
SNS College of Technology,
Coimbatore

K.Thamaraiselvi
Assistant Professor, Department of IT,
SNS College of Technology, Coimbatore

ABSTRACT

Unimodal biometrics uses a single source of biometric system for personal identification. It has a variety of problems such as noise in the sense data, Intra-class variations, Inter-class similarities and spoof attacks. Multibiometrics is a combination of one or more biometrics. In multibiometrics the noise in any one of the biometrics will lead to high false reject rate (FRR) while identification. All these problems are addressed by Multimodal biometrics. Multimodal biometrics is the integration of two or more types of biometrics system (e.g. Fingerprint and Face, Face and Iris, Iris and Fingerprint). It provides a secondary means of identification in case sufficient data is not extracted from a given biometric sample. The main objective is to provide a higher level security to the distributed system and to protect the biometric template by making use of biometric cryptosystem. In the existing approaches multibiometrics which is a combination of one or more biometrics is used to provide security along with feature level fusion to combine the biometric template. The failure of one of the biometrics in multibiometrics system leads to the serious issue. The proposed work is to enhance the security in ATM system with multimodal biometrics along with email verification code which provides two level security to the system.

General Terms

Biometric Cryptosystem, Security, Biometrics, Template Protection

Keywords

ATM (Automated Teller Machine), Biometric Cryptosystem, Biometrics, Face recognition, Fingerprint recognition, Iris recognition, Multibiometrics, Multimodal biometrics, Template Protection, Two-tier security

1. INTRODUCTION

The term “biometrics” is derived from the Greek words “bio” (life) and “metrics” (to measure). Biometrics refers to the physiological or behavioural characteristics of a person to authenticate his/her identity [1]. Biometric systems based on single source of information are called Unimodal systems. Multimodal biometrics is an integration of two or more types of biometric system and it provides a secondary means of identification. The integration of two or more types of biometric verification systems helps to meet stringent performance requirements set by security conscious customers. The biometric system is a combination of various unimodal biometrics; it aims to fuse two or more physical or behavioural traits. After determining which biometric sources are to be integrated, then the next step is to build the system architecture. Multimodal biometric systems can operate in three different modes [2] [3]:

- **Serial Mode –** In serial mode, each modality is examined before the next modality is investigated. It is not necessary to capture all the biometric traits at the same time. The overall recognition duration can be decreased. This mode is sometimes known as cascade mode.
- **Parallel Mode –** In parallel mode, the information from multiple modalities are processed together to perform recognition. Then the results are combined to make final decision.
- **Hierarchical Mode –** In hierarchical operational mode, individual classifiers are combined in a treelike structure. This mode is preferred when a large number of classifiers are expected.

Multimodal biometric systems are designed to operate in one of the five integration scenarios as below:

- **Multiple Sensors –** The information obtained from different sensors for the same biometric are combined.
- **Multiple Biometric –** Multiple characteristics such as fingerprint and face are combined. These systems will contain more than one sensor with each sensor sensing different biometric characteristics.
- **Multiple Units of the Same Biometric –** Fingerprints from two or more fingers of a person may be combined or one image each of the same person may be combined.
- **Multiple Snapshots of the Same Biometric -** More than one instance of the same biometric is used for the enrollment and recognition, which includes multiple impression of the same finger, multiple samples of a voice can be combined.
- **Multiple Representations and Matching Algorithms for the Same biometrics –** Combining different approaches to feature extraction and matching of the biometric characteristics.

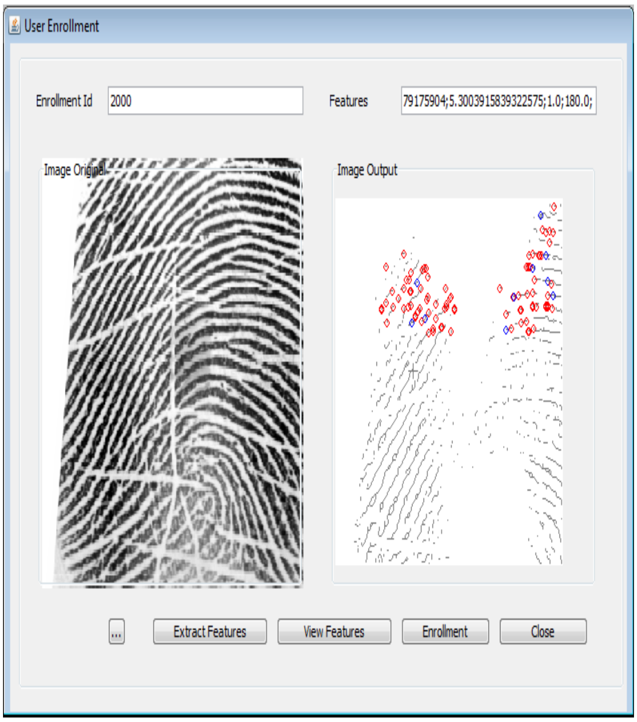
The rest of the paper is organized as follows: The **section 2** presents the existing unimodal biometrics in ATM and Multibiometrics biometrics in ATM which overcomes the problem of unimodal biometrics. Multimodal biometrics and two tier security is used to enhance the security of ATM in **section 3** and **section 4.** In **section 5** conclusion and future work has been presented.

2. UNIMODAL AND MULTIBIOMETRICS IN ATM SYTEM

Physical biometrics is a static biometrics and the data is derived from the measurement of an action performed by an individual. It includes fingerprint, Iris, Retina, Hand geometry, Palm print, Face recognition, DNA and Vascular Pattern Recognition. Behavioural biometrics is a dynamic biometrics and the data is derived from the measurement of an action performed by an individual and the parameter considered over here is time; the measures action has a beginning, middle and end. It includes signature, keystroke, Handwriting, Voice recognition and Gait. Soft biometrics also known as chemical biometrics is a human characteristic that provide some information about the individual. It includes height, weight and color of hair [4].

2.1 UNIMODAL BIOMETRICS

The oldest and successful technology which is implemented in ATM is fingerprint recognition [5].The algorithms used for fingerprint recognition are minutiae extraction and singular point detection. After the user inserts the card in the ATM system and enters the PIN number, if the PIN number is valid, then the user needs to print his/her fingerprint for authentication purpose. If the fingerprint template matches with the template which is stored in the database during enrollment, then the user is authenticated and he/she can access their account which is shown in figure1. The reason behind the popularity of fingerprint-based recognition among the biometric-based security systems is the unchangeability of fingerprints during the human life span and their uniqueness. This type of system provides the basic level of security and the error rates is high [6].



User Enrollment

Enrollment Id: 2000

Features: 79175904;5.3003915839322575;1.0;180.0;

Figure 1: Unimodal biometrics implemented in ATM

2.2 MULTIBIOMETRICS IN ATM SYSTEM

Human users find difficult to remember long cryptographic keys. Therefore, researchers, for a long time period, have been investigating ways to use biometric features of the user rather than memorable password or passphrase, in an attempt to produce tough and repeatable cryptographic keys [7]. In the existing approaches the passwords has been replaced by biometrics and it is no longer need to be remembered as it remains as a part of the body. Our goal is to integrate the volatility of the user's biometric features into the generated key, so as to construct the key unpredictable to a hacker who is deficient of important knowledge about the user's biometrics.

The biometric cryptosystem approach for multi biometric template protection is for two reasons. Well-known biometric cryptosystems such as fuzzy vault and fuzzy commitment are available for securing different types of biometric features and it is relatively easy to analyze the security (non invariability) of a secure sketch by leveraging on the characteristics of error correcting codes. Multibiometrics is a combination of one or more biometrics is implemented in ATM. Feature level fusion makes use of embedding algorithms to convert different biometrics into common representation [8] [9].

Embedding algorithm converts binary strings to point-sets, point-sets to binary strings and fixed-length real-valued vectors to binary strings. Biometric cryptosystems have been designed only for specific biometric feature representations. The fuzzy commitment scheme assumes a binary string representation, where the dissimilarity between template and query is measured in terms of the Hamming distance.

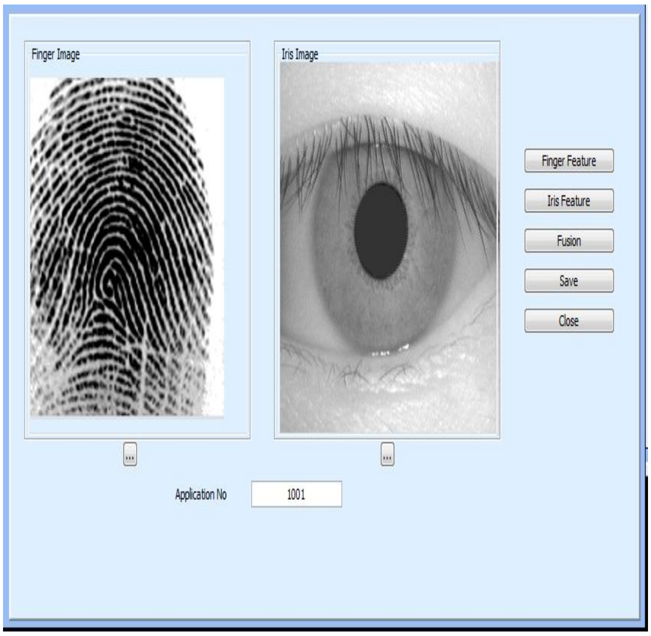
Matching performance of a biometric system is measured with the help of false accept rate (FAR), false reject rate (FRR) and the genuine accept rate (GAR). The false reject rate (FRR) error rate is more in multibiometrics due to the presence of noise and the user will be identified as imposter as the biometrics does not match. This will make the genuine user to get into trouble and he/she have no other choice to prove him as an authorized person and he cannot able to access his account.

Multibiometrics is mainly used to provide security in the server side. The fingerprint and iris recognition is used to provide security. The features are extracted from biometrics using feature level fusion and the features are combined into single biometric and biometric cryptosystem scheme is used to protect the template. The system flows like the person needs to insert the ATM card and enter the PIN number. If it is valid, it undergoes the fingerprint and iris scan and all the biometrics are verified. If all the template query matches with the template stored in the database during enrollment, the user will be authenticated as authorized person and he will be able to access his/her account.

2.3. LIMITATIONS OF MULTIBIOMETRICS SYSTEM

- The accuracy of the biometric enrollment and biometric identification need to be improved.

- Noise in the biometrics like scratches in the fingerprint and lens mark in iris will lead to false rejection rate (FRR).
- In multibiometrics, failure of one biometrics will make the whole system to fail.



Application No 1001

Figure 2: Multibiometrics Security in ATM System

3. MULTIMODAL BIOMETRICS IN ATM SYTEM

The proposed work is to enhance the security of biometrics in ATM system [10][11][12]. From the past work, it has been highlighted that even though the security has been improved, the error rates has to consider for improvement of the performance of system. By considering all those drawbacks, the higher level of security can be provided by implementing multimodal biometrics and two level security in ATM system. In multimodal biometrics, different biometrics like Fingerprint, Iris and Face is considered. The biometric systems are designed in the way as integration of different biometrics. The three different biometric systems are Fingerprint and Iris, Iris and Face, Face and Fingerprint. Based on the user choice, the biometric system is selected. The choice of user depends on the biometrics he needs to enroll for verification and it should not be affected by external factors and it should prove him as an authenticated person. In case of unavoided failure, the user can undergo secondary means of verification by making other two biometric systems. Due to these reasons, the error rates will FAR and FRR will be decreased, which will improve the performance of the system and also enhance the security.

3.1 FEATURE EXTRACTION FROM FINGERPRINT BIOMETRICS

Fingerprint recognition includes fingerprint identification system and fingerprint verification system. In case of both the fingerprint identification and fingerprint verification systems, the task is broken into two stages [6][13]. In *offline phase*, several fingerprint images of the fingerprint of a person to be verified are first captured and processed by a feature extraction module; the extracted features are stored as templates in the database for later use. In *online phase*, the individual to be verified gives his/her identity (in case of verification) and places his/her finger minutia points are extracted from the captured fingerprint image. These minutiae are then fed to a matching module, when matches them against templates in the database. The various steps involved in fingerprint recognition are [14]:

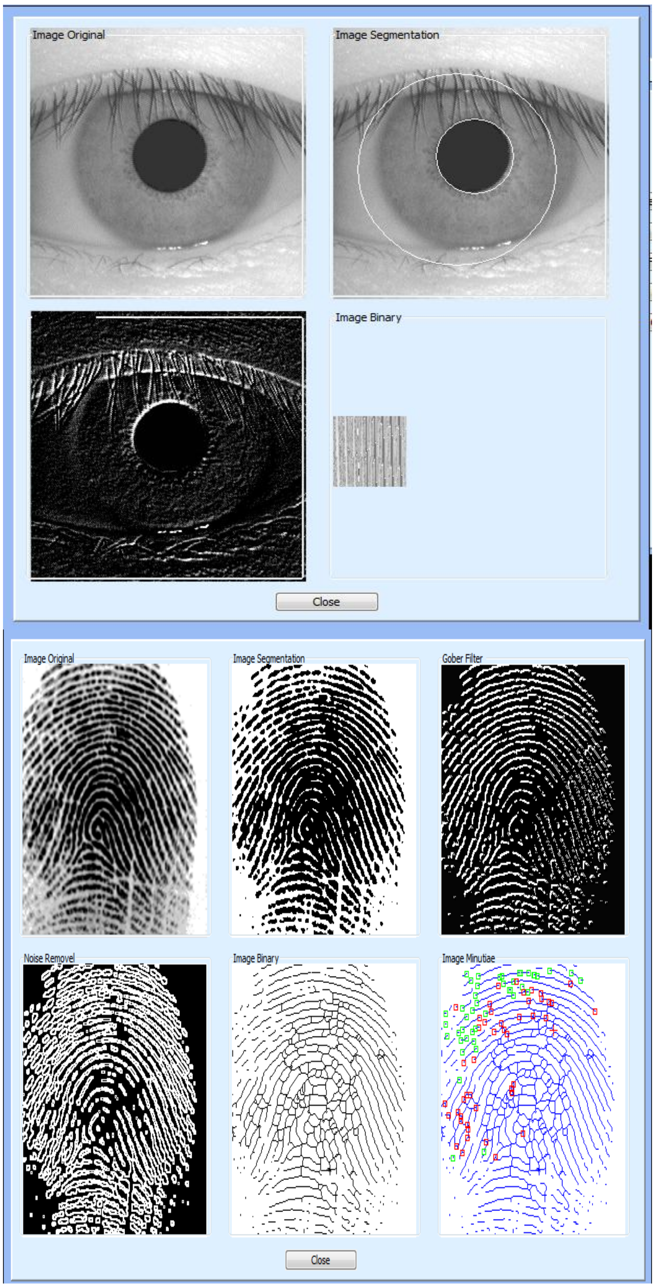


Figure 3: Feature Extraction from Fingerprint and Iris

- In **Image Acquisition**, the image is captured using the scanner and the features are extracted in the form of machine-readable format.
- In **Normalization**, an input image is normalized so that the ridges and valleys are easily distinguished. Normalization is used to enhance the contrast of image by transforming the values in the fingerprint image.

- **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. W is equal to 16.
- **Gabor filter** is used to remove the noise and preserve true ridge and valley structures. Gabor filters have both frequency-selective and orientation selective properties and have both resolution in spatial and frequency domains.
- **Thinning algorithm** is used to remove the pixels from ridges until the ridges are one pixel wide. It is to thin the processed binary image using the morphological thinning operation.
- **Binarization** converts a 256 gray level image to a binary image (black and white) using a threshold value and to classify all pixels with values above this threshold as white and all other pixels as black.
- **Minutiae Extraction** is performed with ridge endings and bifurcations. In minutiae extraction, it is to count the number of ridge pixels, every ridge pixel on the thinned image is surrounded by and depending on the rule and we can assign the minutiae points to pixels. In minutiae matching, it is to match the minutiae obtained from two sample fingerprint images and test whether they are from the same fingerprint or not.

3.2 FEATURE EXTRACTION FROM IRIS BIOMETRICS

The iris images are taken from the database provided by CASIA (Chinese Academy Of Sciences Institute Of Automation) [15] [16] [17]. The steps involved in recognising the iris biometric systems are:

- **Iris localization** is used to locate the boundaries of iris and pupil. By knowing the iris location, it is easy to extract the iris pattern. Iris localization is done by using Hough transform. It is a technique which is used to isolate features of a particular shape within an image. Advantage of using Hough transform is that it is tolerant of gaps in feature boundary descriptions and is unaffected by image noise. If localization is not done properly it will result in resultant noise leading to poor performance.
- **Unwrapping** is done to derive the information signal which is used to create template of iris into binary form. **Sampling** of unwrapped iris is made by applying Haar wavelets to decompose the data in the iris region into different frequency resolutions. Haar wavelet breaks the image into four sub-sampled images i.e. High pass filter and low pass filter. From Haar transform different frequency dimensions are formed. Each dimension has a magnitude between -1 and 1. After sampling signal is transformed into binary form. So it is found that positive part of vector is 1 and negative part is 0. Under perfect conditions the iris template can have 2048 bit length.
- **Binarization** is a process of converting gray level vector signal into a black and white vector signal, which is done with the help of threshold value. Threshold value is set by us. If the values are greater than threshold then it is set to 1. If the values are lesser than threshold then it is set to 0.
- **Matching** of iris is done without considering the iris image size and position. The criteria used to decide whether the iris code matches or not are based on Hamming distance. XOR detect the disagreement between two iris codes AND is to ensure that both pair of bits is uncorrupted by eyelashes and lids on iris. Hamming distance is calculated where code A is first iris code and code B is the iris code which is stored in the database. 0 in the mask bits corresponds to a bad bit in that position in iris code.

$$\mathrm{HD} = \frac{\left\| (codeA \otimes codeB) \bigcap maskA \bigcap maskB \right\|}{\left\| maskA \bigcap maskB \right\|}$$

If the HD is zero then the irises are same and if the HD is one then the irises are different.

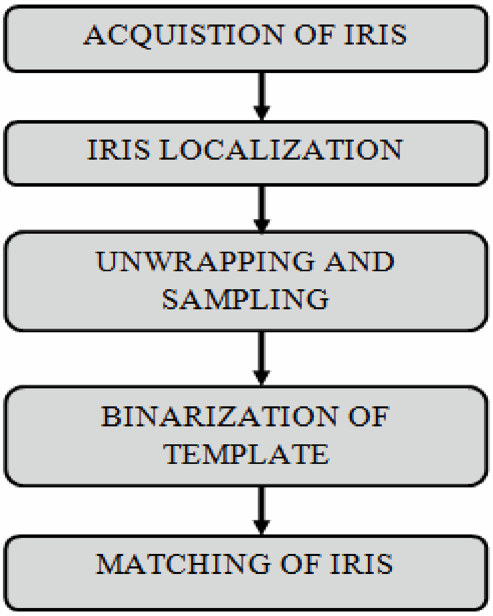


Figure 4: Steps Involved in Iris Recognition System

3.3 FEATURE EXTRACTION FROM FACE BIOMETRICS

The process involved in developing a computational modal of face recognition is quite difficult because faces are complex and multi-dimensional. Two basic methods are involved in face recognition. The first method is based on extracting feature vectors from the basic parts of a face such as eyes, nose, mouth and chin with the help of deformable templates [18]. The key information id got from the basic parts of face and it is gathered and converted into a feature vector. Another method is based on the information theory concepts like principal component analysis. In this method, the information is derived from the entire face. The approach that transforms face images into a small set of characteristic feature images is called Eigen faces. Once the Eigen face is created, identification becomes a pattern recognition task.

The steps involved in face recognition are:

- Acquire the face images and calculate the eigenfaces, which define the face spaces.
- When a new face image is encountered, calculate a set of weights based on the input image.
- Determine if the image is a face at all (whether it is known or unknown) by checking to see if the image is sufficiently close to face space.

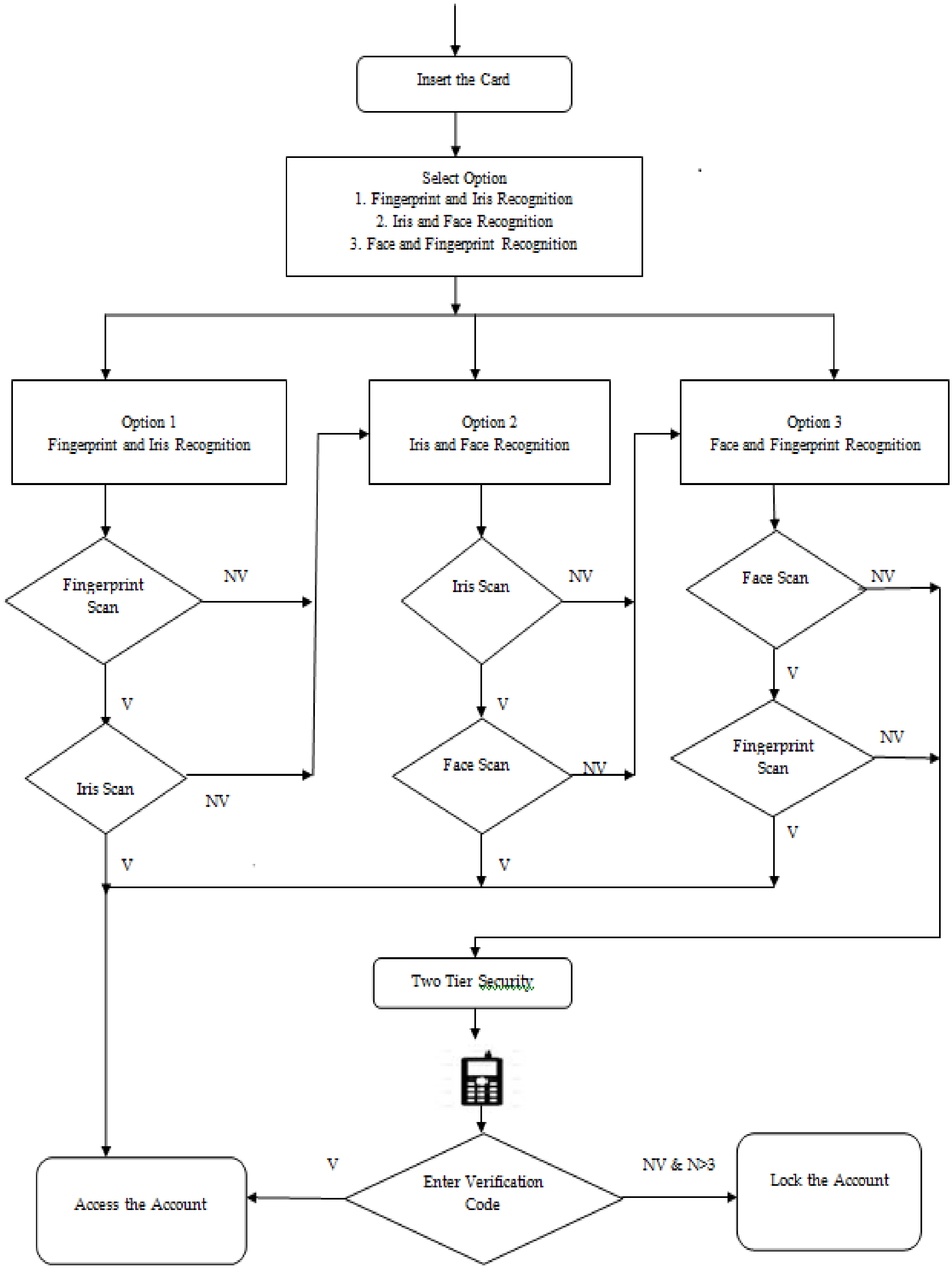


Figure 5: System Flow Diagram for Multimodal Biometrics and Two-Tier Security in ATM System

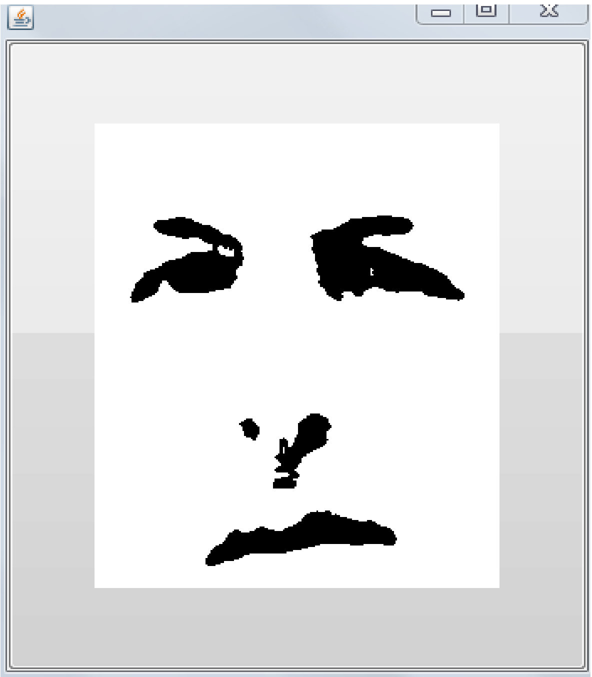


Figure 6: Feature Extraction of Face

4. TWO TIER SECURITY IN ATM SYSTEM

If due to unavoidable reason the user was not able to prove him as a genuine person with the help of multimodal biometrics, he cannot able to access his account. But this situation happen soo rarely. In that situation, if and only if he prove him as authorized person the ATM system will allow user to access his account to avoid hacking activities. Even though the security has been increased at the same time fraudulent activities have grown to equal level, so the security in ATM is an essential one and the two level security has been introduced.

With two level security, the user will be able to prove him as an authorized person with the verification code send through mail to his/her mail id or by sending a message to his/her phone number and access his account at that time which provides higher level of security in ATM. It is recommended that it also can be used for other applications. Two-tier security is used to provide two level of security. In multimodal system, if the different biometric system fails (this situation happens very rarely) two level security takes the advantage [19]. In two tier security, the verification code will be send to the user mobile, which acts like a two step verification in Gmail account. If the user enters the valid code, he/she is allowed to access the account. If the hackers try to hack the account by trying different combination of verification code, the bank account will be locked if more than three attempts are made. This makes the system more secure. Likewise, the multimodal and two-tier security is implemented in ATM system to enhance the security level of the user account by preventing unauthorized access.

Figure 5 explains the proposed concept system flow diagram of multimodal biometrics system and Two-tier security in ATM system. The user needs to insert the card in the ATM system and enter the PIN number; if it is valid the options will be displayed. The user needs to select the biometric system which he needs. In case if he has wound in the finger, he can select option 2 to prove he is an authenticated user. In case of environmental factors, if the user is not identified as authenticated person, he can make use of other biometric system and make a secondary enrollment by selecting other biometric system. Likewise it reduces the False Reject Rate. Two tier security is provided, when all the biometric system fails. In the two-tier security, the verification code will be send to the user email id. He needs to enter that verification code correctly to prove him as authenticated user and only three attempts are provided and if the hacker try to guess out the code by trying more than 3 attempts, that account will be locked and he cannot able to access the system.

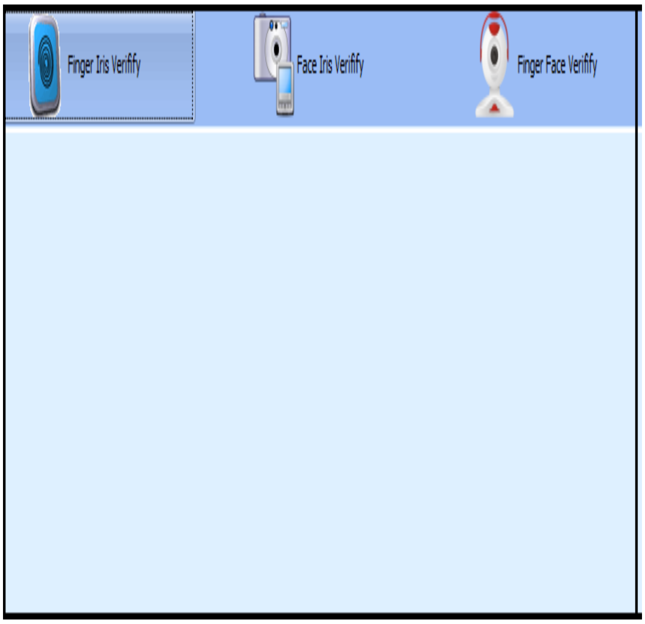


Figure 7: Implementation of Multimodal biometrics in ATM System

5. CONCLUSION AND FUTURE WORK

Multimodal biometrics along with two-tier security provides a higher level of security. The error rates like FAR (False Acceptance Rate) and FRR (False Reject Rate) has been reduced, which avoids the various types of attacks in ATM system and fraudulent activities are reduced. The chance given for hackers to make use of fake biometrics to act as an authorized user is strictly avoided, which makes the ATM system more secure. But the cost spend to design and implement this type of system is higher when compared to the existing ATM system. The future work includes designing the system with latest biometric technologies and implementing multimodal biometrics in other distributed system, which will provide more security.

6. REFERENCES

[1] A. Ross, K. Nandakumar, and A. K. Jain,*"*Handbook of Multibiometrics" NewYork: Springer,2006.

[2] Waheeda Almayyan, "Performance Analysis of Multimodal Biometric Fusion", PhD Thesis, De Montfort University, February, England, 2012.

[3] Karthik Nandakumar, "Integration of Multiple Cues in Biometric Systems", Thesis for Master of Science in Michigan State University. 2005.

[4] Harbi AlMahafzah and Maen Zaid AlRwashdeh "A Survey of Multibiometric Systems", International Journal of Computer Applications, Volume 43, no.15, 2012.

[5] Moses Okechukwu Onyesolu and Ignatius Majesty Ezeani "ATM Security Using Fingerprint Biometric Identifier: An Investigate Study", IJACSA, Volume.3, no.4, 2012.

[6] Roli Bansal, Priti Sehgal and Punam Bedi "Effective Morphological Extraction of True Fingerprint Minutiae based on the Hit or Miss Transform", IJBB, Volume 4, Issue 2, 2010.

[7] Abhishek Nagar, Karthik Nandakumar and AnilK. Jain, "Multibiometric Cryptosystems Based on Feature-Level Fusion", IEEE transactions on information forensics and security, vol. 7, no. 1255-268, February, 2012.

[8] B. Yanikoglu and Kholmatov, "Combining multiple biometrics to protect privacy", in Proc. ICPR-BCTP Workshop, Cambridge, August, England.

[9] A. Nagar and A. K. Jain, "On the security of non-invertible fingerprint template transforms," in Proc. IEEE Workshop Information Forensics and Security, London, U.K., December, 2009.

[10] Santhi.B and Ramkumar.K "Novel Hybrid Technology in ATM Security Using Biometrics*",* JATIT, Volume.37, no 2, 2012.

[11] S.R. Agarwal, D.R. Kokadwar, Zareen Kauser and Gouri Apte "Multimodal Biometrics System-Applications, Challenges and Research Areas", BIOINFO Human-Computer Interaction, Volume 1, Issue 1, 2011.

[12]S. Pravinthraja and K. Umamaheswari"Multimodal Biometrics for Improving Automatic Teller Machine Security*", Bonfring International Journal of Advances in Image Processing,* Volume 1, December, 2011.

[13] Identification Flats: A Revolution In Fingerprint Biometrics, AWARE, White paper

[14] Chirag Dadlani, Arun Kumar Passi, Herman Sahota and Mitin Krishan Kumar, "Fingerprint Recognition Using Minutiae-Based Features",EE85I: Biometrics, Indian Institute of Technology, Delhi.

[15] Michael Boyd, Dragos Carmaciu, Francis Giannaros, Thomas Payne and William Snell,"Iris Recognition", Imperial College London, MSc Computing Science Group Project, March 19, 2010.

[16]Vanaja Roselin.E.Chirch, Dr.L.M.Waghmare and E.R.Chirchi, "Iris Biometric Recognition For Person Identification In Security Systems", International Journal of Computer Applications,Volume 24– No.9, June 2011.

[17] Libor Masek, "Recognition of Human Iris Patterns for Biometric Identification", Bachelor of Engineering degree of the School of Computer Science and Software Engineering, The University of Western Australia, 2003.

[18] Mayank Agarwal, Nikunj Jain, Manish Kumar and Himanshu Agarwal, "International Journal of Computer Theory and Engineering", Volume 2, No.4, August 2010.

[19] Shanthini.B and Swamynathan.S "A Novel Multimodal Biometric Fusion Technique For Security*",* International Conference On Information And Knowledge Management, IPCSIT, Volume 45, 2012.