Enhancing the Security of Biometrics in ATM

N.Geethanjali
MTECH IT, SNS College of Technology, India

K.Thamaraiselvi
Assistant Professor of IT, SNS College of Technology, India

Abstract— Biometrics based authentication provides various advantages over other authentication methods, it has replaced the password based authentication and token based authentication. Biometrics plays a major role in Automated Teller Machine (ATM) system, E-Commerce, Online banking, Passports. The growth in electronic transactions has been increased tremendously; there is a greater demand for fast and accurate user identification and authentication. In distributed system like ATM system the security is a main issue. The security levels have been grown from providing PIN (Personal Identification Number) to Smart Card to Biometrics. Even though the security has been increased, at the same time fraudulent activities have grown to equal level. So to overcome the hacking activities, the proposed work is developed to provide protection to the biometric template and to enhance the security in the ATM system with Multibiometrics, Multimodal biometrics and Two-tier security. Biometrics along with cryptography is used to encrypt the template which is stored in the database. Biometric cryptosystem scheme namely fuzzy vault and fuzzy commitment is used to protect the template which is extracted from the biometrics.

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

1 INTRODUCTION

IN this modern world, many of us are using ATM machine. Fast development of banking technology has various advantages and disadvantages to banking activities and transactions are the advent of automated teller machine (ATM). ATMs are electronic banking machines located in different places and the customers can make basic transactions without the help of bank staffs. With the help of ATM the user can perform several banking activities like money transfer, cash withdrawal, paying various home usage bills like electricity and phone bill. It is a more convenient for users to access their bank accounts and to conduct financial transactions. The account holder will be given the ATM card and private PIN (Personal Identification Number) or password. PIN number or password is an important aspect in ATM system, which is commonly used to secure and protect financial information of customers. PIN number need to be remembered by the card owner and it should not be shared with others to prevent unauthorized access **[1].** Crime which is happening in ATM became a serious issue that affects not only customers but also bank operators.

Security is a serious issue in ATM system. ATM scam involves thieves putting a thin, clear, rigid plastic sleeve into the ATM card slot. By doing like this, when you enter your card, the machine can't read the strip, so it will be keep asking you to re-enter your PIN number **[12].** At that time, the hackers will notice the tap of your number and he can easily guess out the 4-digit PIN number. The thieves then remove the plastic sleeve and use their account. The main solution to this problem is biometrics.

Biometrics is a measure of physical or behavioural characteristic that can be captured and subsequently compared with another instance at that time of verification. Any human physical or behavioural biometrics can be used as a biometric characteristic as long as it satisfies the following requirements **[2]:**

- Universality- Every person should possess the biometric characteristic.
- Distinctiveness- Any two persons should be sufficiently different in terms of the characteristic.
- Permanence- The characteristic should be sufficiently invariant over a period of time.
- Collectability- The biometric characteristic should be measurable with some sensing device.
- Performance- Refers to the level of accuracy and speed of recognition of the system, the resources required to achieve the desired recognition level, as well as the operational and environmental factors that affect the accuracy and speed.
- Acceptability- Indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives.
- Resistance/ Circumvention- Refers to the degree of difficulty required to defeat or bypass the system.

The rest of the paper is organized as follows: The **section 2** presents the existing unimodal biometrics in ATM and **section 3** presents the multibiometrics which overcome the problem of unimodal biometrics. Template protection using biometric cryptosystem is explained in **section 4.** Multimodal biometrics and two tier security is used to enhance the security of ATM in **section 5** and **section 6** presents the various applications of biometrics. In **section 7** conclusion is provided.

2 UNIMODAL BIOMETRICS IN ATM SYSTEM

The term "biometrics" is derived from the Greek words "bio" (life) and "metrics" (to measure). Biometrics refers to automatic system that uses measurable physiological characteristics or behavioural traits to recognize the identity or authenticate the claimed identity of an individual. Biometric systems based on single source of information are called Unimodal systems. The three ways to establish the identity of a person are " something you know" (e.g., password, PIN) which provides first level of security and " something you carry" (e.g., ID card, smart card) and "something you are" (biometrics), these provide second level of security. In smart card, the fingerprint templates are encoded into a smart card memory, to identify a person, his/her fingerprints are compared against the digital templates stored in the card memory. Identity management system is to find the individual's identity. Traditional methods of establishing a person's identity include knowledge-based and token-based mechanisms, which can be easily lost, shared or stolen. To overcome all these problems biometrics was introduced.

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 **[3].**

The oldest and successful technology which is implemented in ATM is fingerprint recognition **[9].**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 **[11].**

2.1 Limitations of Unimodal Biometrics:

Biometric system is essentially pattern recognition system that operates by acquiring biometric data from an individual. Biometric systems are often affected by the following problems **[4]:**

- **Noise in sensed data**- The accuracy play a major role in recognition of biometrics. The accuracy of the biometric system is very sensitive to the quality of the biometric input and the noise present in the data will result in a significant reduction in the accuracy.
- **Non-Universality**- If every individual is able to present the biometric trait for recognition, then the trait is said to be universal. Non-universality leads to Failure to Enroll (FTE) error in a biometric system.
- **Lack of individuality**- Feature extracted from different individuals may be similar. This lack of uniqueness increases the False Accept Rate (FAR) of a biometric system.
- **Intra-class variations**- The data acquired for verification will not match to the data used for generating template during enrollment. For example the face biometric is captured under different angle. Large intra-class variations increase the False Reject Rate (FRR) of a biometric system.
- **Inter-class variations**- It occurs mainly between twins. It refers to the overlap of feature spaces corresponding to multiple individuals. Large inter-class variations increase the False Acceptance Rate (FAR) of a biometric system.
- **Spoofing**- A biometric system may be circumvented by presenting a fake biometric trait to the sensor.

3 MULTIBIOMETRICS IN ATM SYSTEM

Multibiometrics is a combination of one or more biometrics. It can be any physical or behavioral biometrics. Multibiometrics overcomes the problem of unimodal biometrics **[5].** These systems are expected to be more reliable due to the presence of multiple, fairly independent pieces of evidence. This system mainly addresses the problem of non-universality and provides anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple traits of a legitimate user. There are variety of factors that need to be considered while designing the multibiometric system, these include the choice and number of biometric traits; the level in the biometric system at which information provided by multiple traits should be integrated. Based on the multiple sources multibiometric systems are classified as Multi-sensor systems, Multi-algorithm systems, Multi-instance systems and Multi-sample systems. There are various level of fusion like Sensor level fusion, Score level fusion, Matching level fusion and feature level fusion **[13].**

Multibiometrics is mainly used to provide security in the server side. The fingerprint, Iris and Face 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. In figure 2 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, Iris and Face 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.

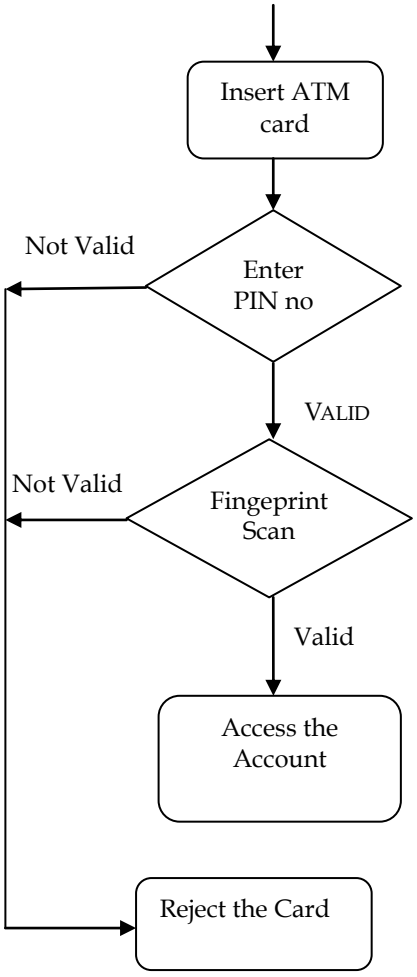


Figure 1: System Flow Diagram for ATM using Unimodal Biometrics

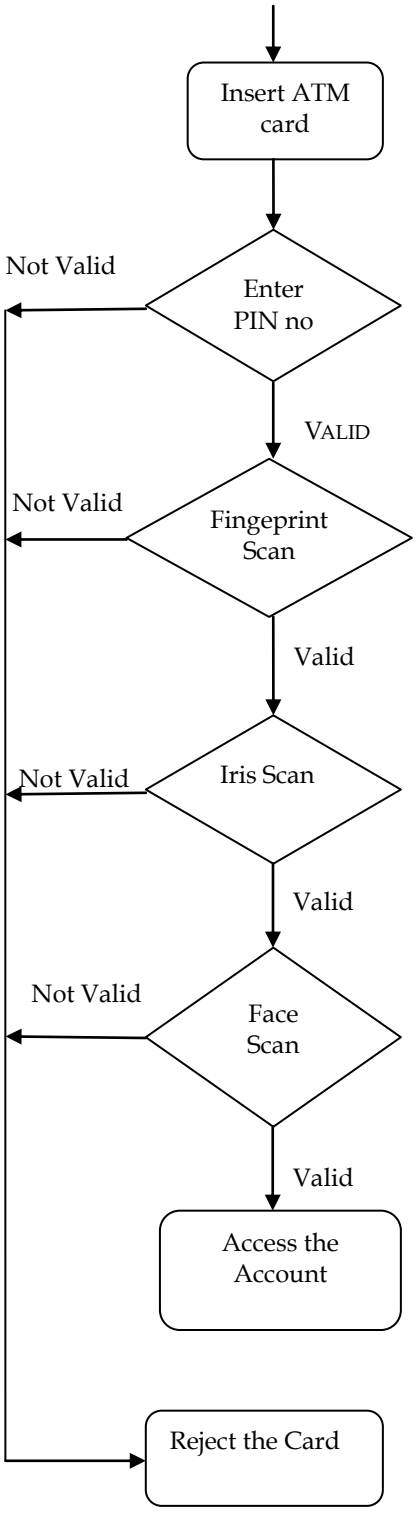


Figure 2: System Flow Diagram for ATM using Multibiometrics

3.1 Advantages and Disadvantages Of Multibiometrics:

The various advantages are of multibiometrics are:

- Increase of reliability and identification quality, while reducing FAR (False Acceptance Rate) error rates.
- A variety of identifiers that can be used together or separately.
- Speeding up the identification procedure.

The limitations of multibiometrics are:

- If one of the biometric fails due to presence of noise in the biometrics, the FRR (False Reject Rate) will be increased.

4 Biometric Cryptosystem

Fuzzy vault and fuzzy commitment build the biometric cryptosystem **[7].** They do not generate revocable templates. In the enrollment phase, the helper data is extracted from the template and combine with secret key to form a secure sketch, In the authentication phase, the biometric query is compared with the template stored in the database and key is obtained to check whether the template is valid or not. Fuzzy Commitment is a biometric system that can be used to secure biometric traits represented in the form of binary vectors and fuzzy vault is represented in the form of point set.

4.1 Fuzzy Vault

In fuzzy vault encoder, the biometric template will be given along with random secret key which is converted to a polynomial degree and polynomial is evaluated in a graph. The set of points is then secured by hiding them with chaff points [6]. The set of genuine points along with polynomial evaluations together with chaff points constitute the sketch or vault.

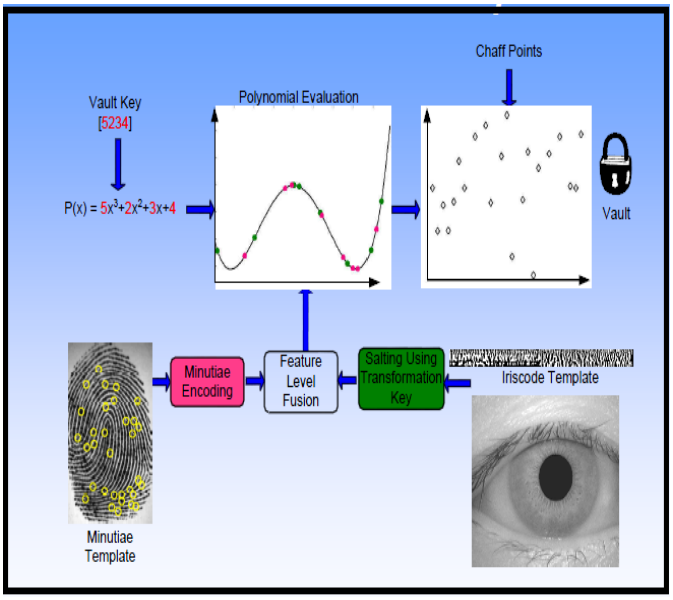


Figure3: Fuzzy Vault

In fuzzy vault decoder, the biometric will be given and then by using the filter the vault points and the query are compared. If the biometric query set is sufficiently close to many genuine points and it can be correctly identified and polynomial is reconstructed successfully and key is generated which is used for validity check. In multibiometric vault the feature level fusion is used to combine the biometrics and then fuzzy vault scheme is addressed.

4.2 Fuzzy Commitment

Fuzzy commitment is represented in the form of binary vectors. The binary string is divided into a number of segments and each segment is separately secured using a fuzzy commitment scheme **[8].** The keys associated with these segment wise fuzzy commitment schemes are then used as additional points in the fuzzy vault constructed using the point-set based features.

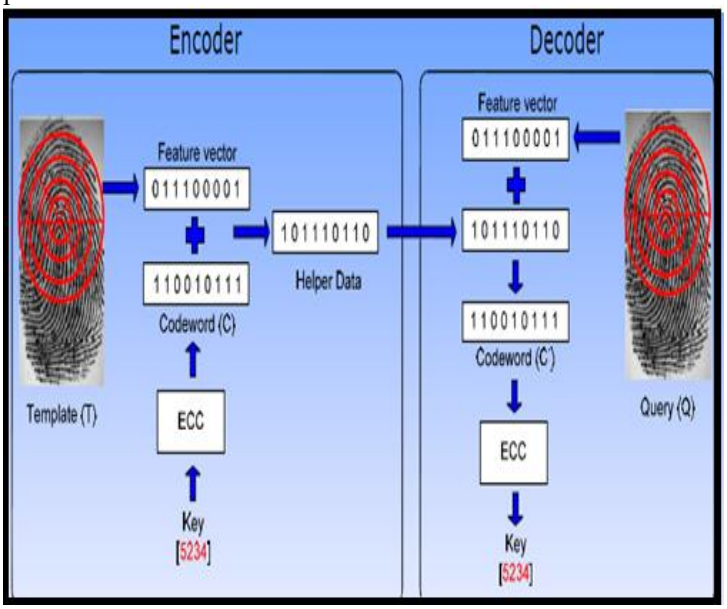
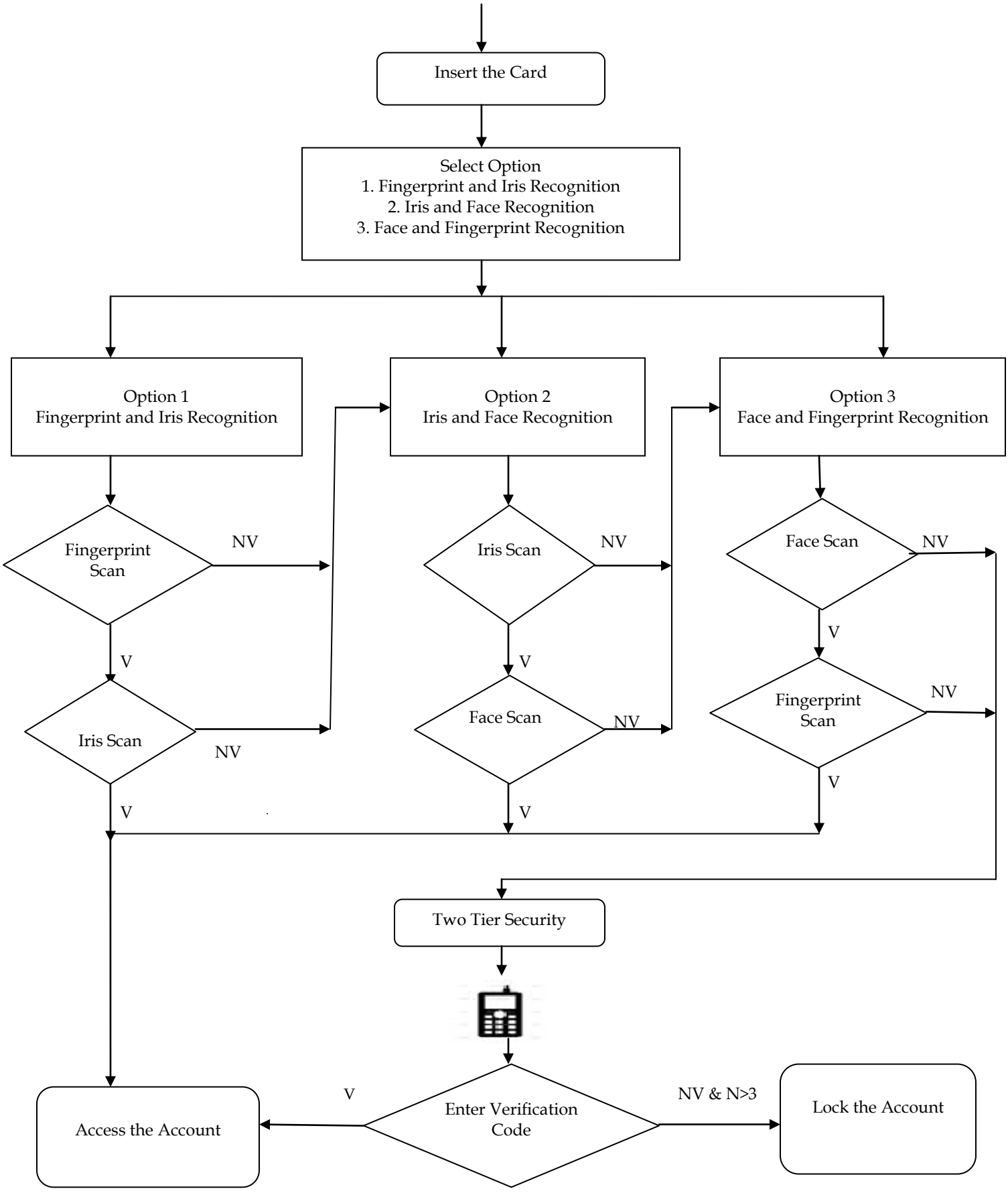


Figure 4: Fuzzy Commitment

5 Multimodal Biometrics And Two-Tier Security

Multimodal biometrics is an integration of various biometric systems **[14],** it can be unimodal biometrics system or multibiometrics system. The integration of two or more types of biometric verification systems helps to meet stringent performance requirements set by security-conscious customers. In proposed system, the multimodal biometrics taken under consideration is fingerprint and iris biometric system, Iris and face biometric system and Face and fingerprint biometric system. Multiple biometrics helps in improving the accuracy of the overall system and it provides a secondary means of enrollment and verification, if sufficient data is not extracted from the given biometric sample. It is mainly used to provide security to the client side. Depending on the traits, sensors and feature set; there are single biometric

Figure 5: Multimodal Biometrics and Two-Tier Security in ATM Sytem



trait- multiple sensors, multiple biometrics, multiple units-single biometric traits, multiple snapshots of single biometric and multiple matching algorithm for the same biometric **[16].** Multimodal biometrics addresses the spoof attacks and the FRR and FAR is 0 %, which is the main problem in Multibiometrics.

Multimodal biometrics is with the combination of face and fingerprint is used to provide security to ATM system [17].It provides a better security than other methods. 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 **[10].** 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 mobile number as sms or call. 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.

6 Applications of Biometrics For Security Purposes

Biometric system is a pattern recognition system that recognizes a person by determining the authenticity of a specific physical or/and behavioural characteristic possesses by the person. The selection of number and choice of biometric modalities, the level at which the evidence is accumulated and the methods used for the integration or fusion of information depends on the system and the level of security needed **[4].** In the last few years it has considerably increased the area of application of biometrics and it's expected that in the near future, we will use biometrics many times in our daily future; we will use biometry many times in our daily activities such as **[15]:**

- **Biometrics home security system-** For accessing the door, the security is provided through fingerprint door locks, voice or face recognition biometrics.
- **Biometrics port security-** For reducing the level of crime and illegal activity at ports and shipyards through the fingerprint or retinal scan biometrics.
- **Biometrics in banking security-** For protecting banking information with fingerprint readers, avoid problems online with biometric signature verification, secure online banking with fingerprint readers, easily use ATM and customer identification with biometric Iris scanners.
- **Computer security biometrics-** It will ensure that only those permitted can access work files with the help of voice, face, iris and fingerprint recognition, which will keep your laptop and mobile devices, PDA and smart phones safe.

7 Conclusion

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.

References

[1] S.S.Das and Debbarma "Designing a Biometric Stradegy fingerprint Measure for enhancing ATM Security in Indian e-banking system",*International Journal of Information and Communication Technology Research*,volume.1,no.5,pp.197-203,2011.

[2] Jain A.K, Ross A. and Prabhakar S. *IEEE Transactions on Circuits and Systems for Video Technology*, 14, 4-20, 2009.

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

[4] A. Ross, K. Nandakumar and A. K. Jain "Handbook of Multibiometrics", New York: Springer, 2006.

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

[6] K. Nandakumar and A. K. Jain "Multibiometric Template Security Using Fuzzy Vault," in Proc. *IEEE 2nd International Conerence of. Biometrics*: Theory, Applications, and Systems, Washington, DC, September,2008.

[7] A. Nagar, K. Nandakumar, and A. K. Jain "Adapting Biometric Representations For Cryptosystems" Department of Computer Science and Engineering, Michigan State University, 2011.

[8] Juels and Wattenberg "A Fuzzy Commitment Scheme", in proc, 6th ACM conference, Computer and Communication Security, 1999.

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

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

[11] 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.

[12] Selina Oko and Jane Oruh "Enhanced ATM Security Using Biometrics", IJCSI, Volume 9, Issue 5, September, 2012.

[13] Karthik Nandakumar "Multibiometric Systems: Fusion Strategies and Template Security", Michigan State University, 2008.

[14] 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.

[15] Refernece site at http://www.biometric-security-devices.com/biometrics-security.html.

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

[17] 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.