ISSN No. 0976-5697

Volume 2, No. 6, Nov-Dec 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

ATM Card Authentication with Hardened Retina Based Fuzzy Vault for Highest Level of Security

R. Sheethal*
MS-Software Engineering
Vellore Institute of Technology (VIT)
Vellore, Tamil Nadu, India
sizzlingsheethal@gmail.com

Abstract: ATM cards are globally being used as a form of Personal Identification and authentication. At Present, ATM cards are primarily restricted only to Personal Identification Number (PIN NO) for authentication.PIN NO are very easy enough for others to steal and misuse it. This has promoted interest in biometric authentication**.** Biometric templates are vulnerable to variety of attacks due to their inherent nature. Biometric Crypto systems blend the idea of cryptography and biometrics. Fuzzy vault is a proven crypto biometric construct which is used to secure the biometric templates. But, fuzzy vault suffer from certain limitations like non-revocability and cross matching. Security level of the fuzzy vault is affected by the non-uniform nature of the biometric data. Fuzzy vault when hardened with password overcomes non-recoverability and cross matching. Password provides an additional layer of security. It also enhances user privacy and security. This paper proposes a method to integrate Retinal recognition with the ATM card to develop a highly secured access environment. A Retinal Recognition system along with ATM machine and smart card programming circuit with its software is developed. Template on card (TOC) is also designed. Hence, the extracted Retinal features stored in ATM card are compared against the data acquired from a Retinal Scanner or database for authentication. The proposed algorithm has superior performance in terms of security, efficiency, reliability, accuracy, user Friendly and consistency compared with other existing technology.

Keywords: ATM Card, Retinal Recognition, Biometric Template, Fuzzy vault, Crypto Biometric Systems.

I. INTRODUCTION

The Five Characteristics of the Ideal Biometrics are Distinctiveness, Robustness, availability, acceptability, accessibility. The biometric cryptography system utilizes the advantages of both biometrics and cryptography for ensuring high security [1]. In biometric based key generation method, biometrics and cryptography are combined together at a much higher level. In this method the secret key is extracted from the combined key and biometric template. The fuzzy vault is a biometric based key generation cryptographic construct[1].

A. ATM Cards:

Traditional security systems like Passwords or Personal Identification Numbers (PIN) and key devices like Smart cards cannot provide security and reliability in all the Scenarios[3]. A user gains access to a ATM card if he/she enters the right PIN. Experience shows that PINs are weak secrets in the sense that they are often poorly chosen and easy to lose.[4] A simple Trojan on the host could easily sniff the PIN and store it for future usage. In general, three strategies of biometric authentication can be identified[5]:

a. ***Template on Card (TOC).*** The biometric template is stored on a hardware security module. It must be retrieved and transmitted to a different system that matches it to the live template acquired by special scanners from the user [2].

b. ***Match on Card (MOC)***. The biometric template is stored on a hardware security module, which also performs the matching with the live template. Therefore, a microprocessor smartcard is necessary, which must be endowed with an operating system running suitable match applications [2].

c. ***System on Card (SOC)***. This is a combination of the previous two technologies. The biometric template is stored on a hardware security module, which also performs the matching with the live template, and hosts the biometric scanner to acquire, select and process the live template [2].

B. ATM Card Issues:

a. ***Removal of Security Lock on ATM memory chip:*** All datas and PIN NO on a ATM card are stored in the EEPROM and it can be erased or modified by an unusual voltage supply. They can also remove the security lock by heating the controller to a high temperature or focusing the UV light on the EEPROM.

Figure 1:Removal of Security Lock on ATM memory chip

b. ***Differential Power Analysis (DPA)***:It is a statistical attack on a cryptographic algorithm and is often capable of extracting an encryption key from a ATM card. Invasive physical attacks are the most destructive when the card is cut and processor removed. Then the layout of the chip can be reverse engineered.

Many of us have devised special ways to keep track of the PIN NO. The need for more convenient, secure systems has become imperative [6]:

c. ***Network Security*** - A separate study of 533 IT managers reported that unauthorized use of computer systems in their companies grew to 49% in 1997 from 42% in 1996, and losses to the companies involved totaled more than $100 million each year[6].

d. ***Credit Card Fraud*** - Credit card fraud is currently at a level of four to six billion dollars a year, and it grows every year.

e. ***Physical Entry Fraud*** - The inconvenience to employees is matched by the lack of security to building owners as users share cards, use temporary card because of failure to bring their regular card, and otherwise 'fool' a pass card system that is annoying to use[6].

f. ***Internet Fraud*** - All companies that deliver content over the Internet are looking for ways to make that content more secure, from try-and-buy software sites to high end content providers, to push technology sites, to retail sites which depend on credit cards.

g. ***Intranet Fraud*** - Companies are increasingly depending on their corporate Intranet as a means of handling electronic transactions with employees, from sending contracts to filling out forms for health benefits. It is imperative that the Intranet be secure and that different users have selective, secure access to specific company information. Yet systems based on passwords and PIN codes are inherently insecure[6]

h. ***Identification System Fraud*** -- The State of Connecticut, which has been a leader in adopting a fingerprint identification system, estimates that it has saved over $7.5 million in fraudulent welfare claims with this system each year. Los Angeles County saw savings of almost $100 million in a biometric test it ran for public aid recipients.

i. ***Electronic Transaction Fraud*** -- Increasing numbers of people are purchasing goods[6] and services electronically with no physical contact between buyer and seller. BCC, Inc. in Norwalk, CT indicates that during 1996 consumer electronic commerce expenditures were $254 billion and that this number is expected to grow to $1 trillion in 2001.5 The potential for increased fraud in such a setting with increased transactions, no physical contact and security systems based on password and PIN numbers, is obvious. Virtually all companies involved in electronic commerce are investigating new ways to identify and verify the identity of their customers

C. Retinal Biometrics:

The Retinal biometric characteristic is used in this paper. Retinal scan captures the pattern of eye‟ s blood vessels [3]. Retina as a biometric has certain advantages when compared to other biometrics. It is very secure and uses a stable physiological feature. Retina is very difficult to spoof. Retinal patterns are different for right and left eye. They are unique even for identical twins. Moreover, retinal patterns do not change with age[3]. Unlike other biometric behavior, the image will not fall on the retina for dead person. As retina is present deep within a person‟ s eyes it is extremely unlikely to be distorted by any environmental or temporal conditions. Therefore retina is a significant biometric feature for high security systems [3]

Parameters	Retinal Scan
UNIVERSALITY	HIGH
UNIQUENESS	HIGH
PERMANANCE	HIGH
COLLECTABILITY	MEDIUM
PERFORMANCE	HIGH
ACCEPTABILITY	HIGH
CIRCUMVENTION	HIGH

D. Construction of Fuzzy Vault:

Fuzzy vault is a cryptographic construct proposed by Juels and Sudan [7]. This construct is more suitable for applications where biometric authentication and cryptography are combined together[1]. Fuzzy vault framework thus utilizes the advantages of both cryptography and biometrics. Fuzzy vault eliminates the key management problem as compared to other practical cryptosystems[1]. In fuzzy vault framework, the secret key S is locked by G, where G is an unordered set from the biometric sample. A polynomial P is constructed by encoding the secret S. This polynomial is evaluated by all the elements of the unordered set G. A vault V is constructed by the union of unordered set G and chaff point set **C** which is not in G[1]**.**

$$V = G \cup C$$

The union of the chaff point set hides the genuine point set from the attacker. Hiding the genuine point set secures the secret data S and user biometric template T[1].

The vault is unlocked with the query template T'**.** T' is represented by another unordered set U'. The user has to separate sufficient number of points from the vault V by comparing U' with V. [1] By using error correction method the polynomial P can be successfully reconstructed if U' overlaps with U and secret S gets decoded**.** If there is not substantial overlapping between U and U' secret key S is not decoded. [1] This construct is called fuzzy because the vault will get decoded even for very near values of U and U' and the secret key S can be retrieved. Therefore, fuzzy vault construct becomes more suitable for biometric data which show inherent fuzziness and hence the name fuzzy vault as proposed by Sudan [7].

The security of the fuzzy vault depends on the infeasibility of the polynomial reconstruction problem. The vault performance can be improved by adding more number of chaff points C to the vault. [1]

E. Limitation of Fuzzy Vault Scheme:

Fuzzy vault being a proven scheme has its own limitations [8].

a. If the vault is compromised, the same biometric data cannot be used to construct a new vault. Fuzzy vault cannot be revoked. Fuzzy vault is prone to crossmatching of templates across various systems.

b. Due to the non-uniform nature of the biometric features it is easy for an attacker to develop attacks based on statistical analysis of the points in the vault. [1]

c. The vault contains more chaff points than the genuine points. This facilitates the attacker to substitute few points from his own biometric

feature. Therefore the vault authenticates both the genuine user and the imposter using the same biometric identity.

d. Original template of the genuine user is temporarily exposed. During this exposure the attacker can glean the template. [1]

To overcome the limitations of fuzzy vault, password is used an additional authentication factor. The proposed retinal based fuzzy vault is hardened by password. This enhances the user-privacy.

F. Hardening of *Fuzzy Vault:*

Biometrics templates are not revocable when compromised like passwords [9]. A template represents a set of salient features that summarizes the biometric data of an individual. A compromised template would mean the loss of a user's identity [10,11]. A potential abuse of biometric identifiers is cross-matching [12]. Therefore, biometric template security is very crucial to protect user privacy. The hardened fuzzy vault overcomes the limitations of non revocability and cross matching by introducing an additional layer of security by password. [1] If the password is compromised the basic security and privacy provided by the fuzzy vault is not affected. However, a compromised password makes the security same as that of a fuzzy vault. Therefore security of the password is crucial. It is difficult for an attacker to compromise password and biometric template at the same time. Figure 2 show the steps involved in hardening process.

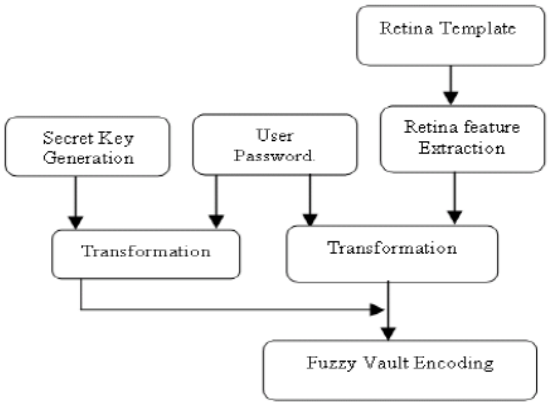


Figure 2: Password Hardening of Retina Based Fuzzy Vault[1]

a. Steps in hardening scheme:

i. A random transformation function is derived the user password.

ii. The password transformed function is applied to the biometric template.

iii. Fuzzy vault frame work is constructed to secure the transformed template.

iv. The key derived from the same password is used to encrypt the vault.

II. HARDENING OF RETINA BASED FUZZY VAULT

The proposed work constructs the password hardened retinal fuzzy vault in three steps[1].

In the first step, the retinal biometric template is subjected random transformation using password. This process enhances the user privacy and facilitates the generation of revocable templates and resists cross matching. This transformation reduces the similarity between the original and transformed template[1].

In the second step, fuzzy vault is constructed to secure the transformed template. The key used in fuzzy vault construction is randomly generated and transformed using the same password. The key can also be generated from the retinal structure for better security[1].

In the third step, the vault is encrypted by the key derived from the password. In this vault, password acts as an additional layer of security.

A. Extraction of Bifurcation Feature point from Retina:

Thinning and joining morphological operation is performed on the Retinal texture. The proposed work uses the idea of Li Chen [13] for extracting the bifurcation structure from retina. These operations highlight the retinal vascular patterns. Then the bifurcation feature points are extracted from the vascular patterns[1]. The (x, y) co-ordinates of the feature points act as lock/unlock data for the vault. Fig 3(a) shows the retina image. Fig 3(b) shows the retinal vascular tree and Fig.3(c) shows the vascular pattern after thinning and joining operation. Fig.3 (d) highlights the retinal template with bifurcation points.

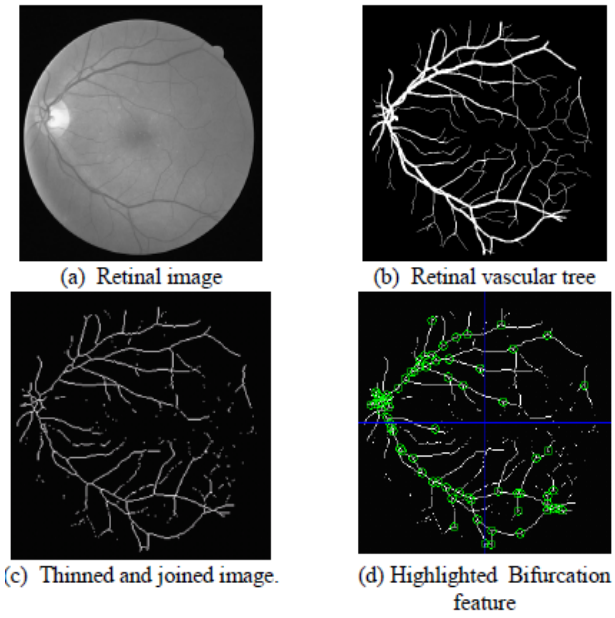


Figure 3: Feature Extraction[1]

B. Implementation of password hardened retina fuzzy vault:

The proposed system is implemented in Matlab 7.0. Retinal samples are taken from DRIVE database. [1]The retinal images taken from the DRIVE data base are resized to the standard 256 x 256 format. This implementation identifies the lock/unlock data by highlighting the retinal bifurcation structures [1]. The (u, v) attributes, of the bifurcation structure, where 'u' and 'v' represents the row and column indices of the image are found out. Permutation and Translation operations are applied on the bifurcation feature points by using the password[1]. The transformed feature points are protected in the fuzzy vault. In this implementation 128 bit random key is generated. The key can also be generated from the retinal structure [1]. This key

is transformed by the 64 bit user password and is used to encrypt the vault.

a. Bifurcation point Transformation:

The retinal vascular tree containing the highlighted bifurcation feature points is subjected to simple permutation and translation. This results in the original bifurcation points being transformed into new points[1].The user password is restricted to the size of 8 characters. Therefore, the length of the password is 64 bits. These 64 bits are divided into 4 blocks of each 16 bits in length.[1]

The feature points highlighted in retinal vascular tree are divided into 4 quadrants. One password block is assigned to each quadrant Permutation is applied in such a way that the relative position of the bifurcation point does not change[1]. Each 16 bit password block is split into two components Tu of 7 bits and Tv of 9 bits in length. Tu and Tv represent the amount of translation in the horizontal and vertical directions, respectively. The new feature points are obtained by the following transformation.[1]

$$X'_u = (X_u + T_u) \bmod (2\text{^}7)$$

$$Y'_v = (Y_v + T_v) \bmod (2\text{^}9)$$

Where Xu and **X'u** are the horizontal distance before and after transformation respectively. Similarly **Yv** and **Y' v** is the vertical distance before and after transformation respectively.

b. Encoding:

The transformed bifurcation features are encoded in the vault as discussed in the earlier section[1]. This password based encryption acts an additional layer of security. It resists an imposter from modifying the vault with the knowledge of the user password.

c. Decoding:

In the authentication phase, the encrypted vault and bifurcation feature point are decrypted by the user password[1]. Password based transformation is applied to the query feature points and the vault is unlocked.

d. Parameters used in implementation:

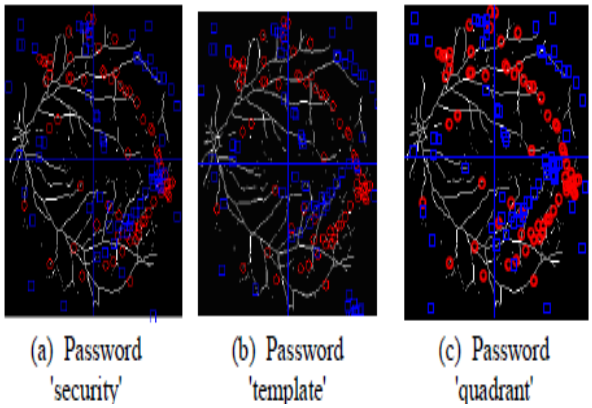
The parameters used in this implementation are shown in Table.I. Chaff points hide the genuine points from the attacker [1]. More chaff points makes the attacker to take much time to compromise the vault with additional computation time. The chaff points added are 10 times in number that of the genuine points.

Table 1: Parameters For Retinal Fuzzy Vault Implementation

Parameter	Size
No. of. Genuine points(r)	30
No. of Chaff points(c)	300
Total no. of points (t = r + c)	330

C. Experimental Results And Security Analysis:

The vertical and horizontal distances of the retinal bifurcation features are used for the polynomial projections.[1] The retinal template is transformed for three different user passwords to check for revocability. The Table II shows the sample bifurcation points from four quadrants after transformation using three different user passwords



(a) Password 'security' (b) Password 'template' (c) Password 'quadrant'

Figure 4:Transformed Retinal Features(Blue – Transformed, Red-Original points)

Consider a 8 character user password 'security', whose ASCII value is given by (115, 111, 99, 117, 114, 105,116,121) or 64 bits[1]. These 64 bits are divided into four blocks of 16 bits each and are further divided into 7 bits and 9 bits for transformation in horizontal and vertical direction. The feature point transformation is done with other two user passwords namely 'template' and 'quadrant' whose ASCII codes are (116, 101, 109, 112, 108, 97, 116 101) and (113, 117, 97, 100, 114, 97, 110, 116) respectively[1]. For the same original template different transformed templates are obtained when password is changed. Fig .4(a), Fig .4(b) andFig .4(c) shows the transformed feature points for three different passwords.

This property of hardened fuzzy vault[1] facilitates revocability. Different password can be utilized for different applications to avoid cross matching. Sample feature points from four quadrants of the same original templates and their transformed equivalent are tabulated in Table II.

The proposed method the security of the fuzzy vault is measured by min-entropy which is expressed in terms of security bits. According to NandaKumar [14] the minentropy of the feature template MT given the vault V can be calculated as[1]

$$H_\infty(M^T \mid V) = -\log_2 \left(\frac{\binom{r}{n+1}}{\binom{r+c}{n+1}} \right) \quad \ldots\ldots\ldots\ldots (1)$$

Where

r = number of genuine points in the vault

c = number of chaff points in the vault

t = the total number of points in the vault (r + c). The security of the proposed vault comes out to be 32 bits[1]s. In order to decode a polynomial of degree d, (d+1) points are required. If the number of feature points is less than (d+1) then Failure to Capture occurs. To overcome this multiple biometric traits [15] [16] can be considered.

Table II. Bifurcation Feature Points After Transformation [1]

Quadrant and Password	Feature points before transformation		Transformation code from password		Feature point after transformation	
	Horizontal Distance (Xu)	*Vertical Distance (Yv)*	*Tu*	*Tv*	*Horizontal Distance (Xu)*	*Vertical Distance (Yv)*
I 'security' 'template' 'quadrant'	122	12	57 58 56	357 101 373	51 52 50	113 113 1
II 'security' 'template' 'quadrant'	159	29	49 54 48	373 368 356	208 213 207	18 13 1
III 'security' 'template' 'quadrant'	110	149	57 54 57	210 97 194	39 36 39	231 215 215
IV 'security' 'template' 'quadrant'	181	227	116 58 110	121 101 116	169 169 163	220 200 215

In modern biometrics, bifurcation points of retinal image can be captured, analyzed, and compared electronically, with relationship drawn between an original and a reference sample[3], as with other biometric approaches. There are two requirements for registration using retina. The user should get the biometric feature of the retina using suitable image processing techniques. The second is that the obtained feature should be encrypted with AES 128[3] bit symmetric cipher and is then transmitted to the server for storage in the database. Therefore, an outside attacker cannot detect the biometric feature by an exhaustive search either at the server side or by meet in the middle attack.[3]

Table III: False Rejection Rate (FRR) (%) Comparison[3]

Degree of Polynomial	Without Hardening	Proposed
4	82.2	78.5
5	85.3	81.8
6	89.1	85.2
7	91.5	87.6
8	92.9	89.2
9	93.8	91.6

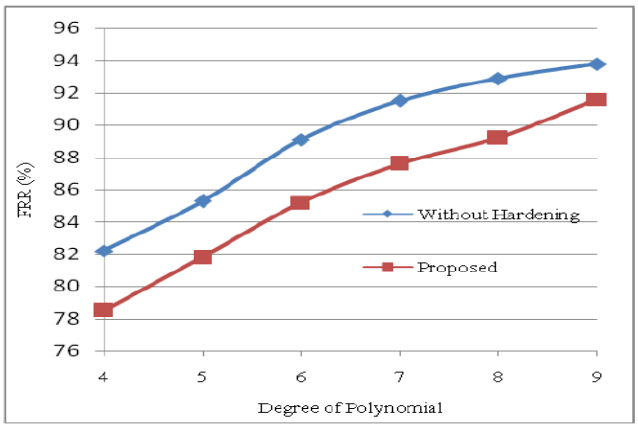


Fig 5: Resulted False Acceptance Rate [3]

Table IV: False Acceptance Rate (FAR) (%) Comparison[3]

Degree of Polynomial	Without Hardening	Proposed
4	0.31	0
5	0.26	0
6	0.17	0
7	0.11	0
8	0.06	0
9	0.02	0

Table III and Fig 5 shows the resulted False Rejection Rate (FRR) for the proposed and existing technique[3]. From the result, it can be observed that the proposed technique results in lesser False Rejection Rate when compared to the existing technique. Table 3 shows the resulted False Acceptance Rate (FAR) for the proposed and existing technique. From the result, it can be observed that the proposed technique results in False Acceptance Rate of 0 for all the Degree of
Polynomial, whereas the existing techniques results with some percentage of False Acceptance Rate[3]. From all the results obtained, it can be said that the proposed technique results in better security than the existing technique.

III. PROPOSED WORK BIOMETRIC SMART CARD

Biometric technologies are defined as automated methods of identifying or authenticating the identity of a living person based on unique physiological or behavioral characteristics[2]. ATM cards have the unique ability to store large amounts of biometric and other data, carry out their own on-card functions, and interact intelligently with a smart card reader[2].

A. Employed Smart Card:

A well known type of smart cards is the ATM Card. The ATM card belongs to microprocessor-contact smart card [2]. It consists of the AT90S8515 microcontroller which is a

low-power CMOS 8-bit microcontroller and the AT24C64 EEPROM which provides 65,536 bits (8KB) of serial electrically erasable and programmable read only memory [17].

B. Smart Card Programmer:

The smart card programmer has been designed to enable read/write from/to the smart card. The programmer is connected to the PC using the parallel port, due to its higher speed compared with serial port and the ability to generate multiple signals at the same time[2]. The block diagram shown in Fig. 6 consists of four parts which are: signal selection circuit, voltage interfacing circuit, connection pins to the parallel port, and connection pins to the smart card. Where C1-C8 are the pins of the smart card and S0-S2 are the selecting Signals [2]

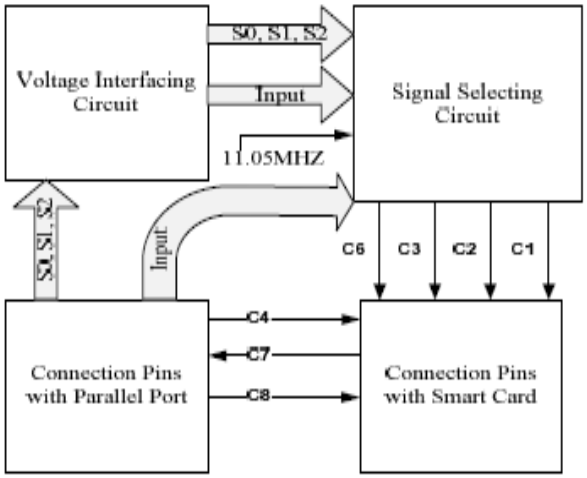


Figure 6. The block diagram of designed programmer

Table V shows the function of each pin in the used smart card.

Pin No.	Name	Function	Direction
C1	Vcc	Power supply 5 VDC	In
C2	Reset	CPU Reset line	In
C3	XTAL	Main clock up to 11 MHz	In
C4	MOSI	SPI master input	In
C5	Vss	Power Ground	In
C6	Nc	Not Connected	--
C7	MISO	SPI Master output	Out
C8	SCK	SPI serial clock	In

C. Integrating Retinal Features with Password hardened Fuzzy Vault with ATM card:

After extracting data from Retina, it is saved in the smart card's flash memory using the smart card programmer. Extracted iris features stored in ATM card are compared against the acquired data from the camera or the database to confirm that a person is authenticated or not. In order to protect the data against manipulation, a signature of the data has been generated using the MD5 hash function [18], which produces 18 bytes signature, and then saved in the smart card. Hence, in the identification process, the system generates the biometric template and its signature from the acquired data and compare them against the ATM card contents. In case of finding any difference between the generated and the saved template or signature, the identification is rejected. Fig. 7 shows the Saving Retinal Features to ATM card and Fig 8 shows Verification of ATM card with Retinal Features.

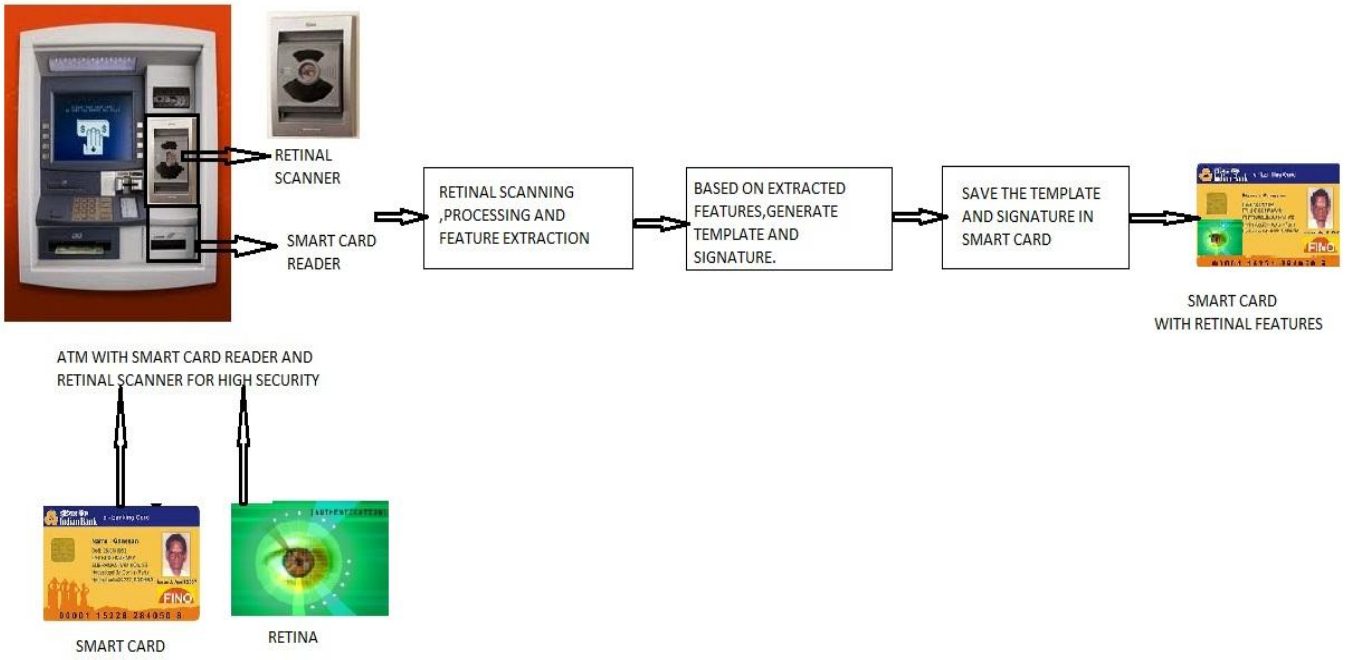


Figure 7:Saving Retinal Features to ATM Card

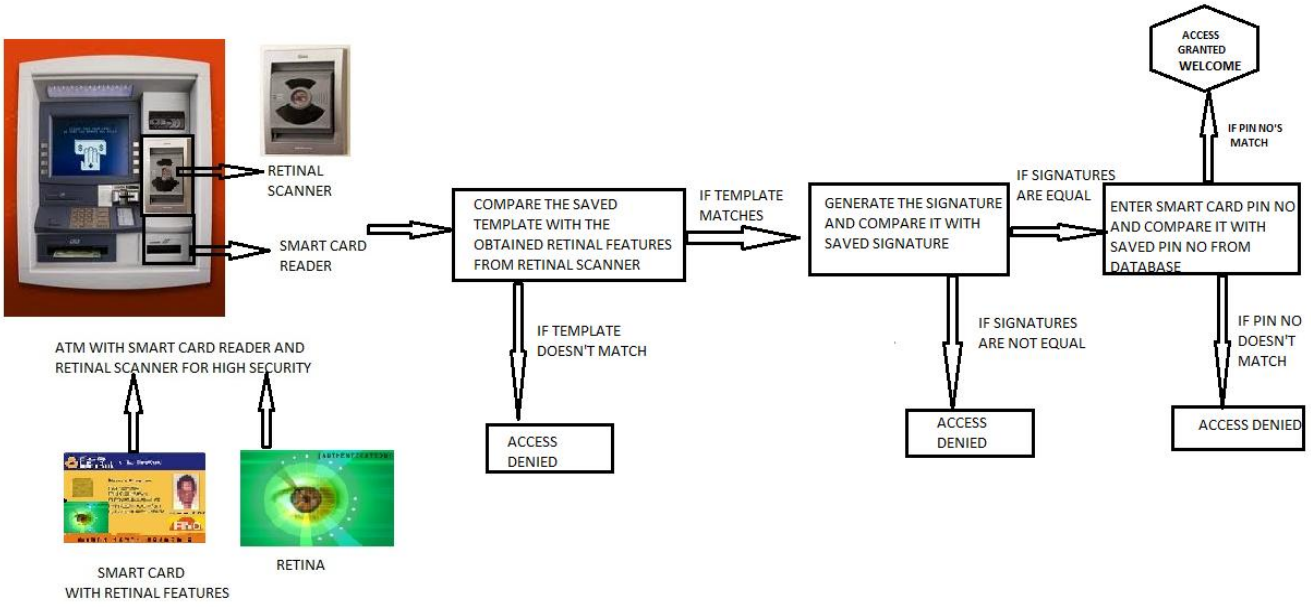


Figure 8:Verification of ATM card with Retinal Features

IV. CONCLUSION

Although fingerprinting was the first generally accepted biometric that was tested, technology has come a long way in creating many other and more precise methods of analysis. Retina is a more unique biometric than the iris.The retina is an extremely stable biometric because it is "hidden" and not subject to wear, other than aging and disease. The retina is not visible and cannot be faked easily.By hardening the retina based fuzzy vault two layers of security namely password and biometrics is introduced. Even if the attacker gains the password he/she may not be able to access the genuine feature points. It is computational very hard for an attacker to identify the genuine feature points[1]. If the attacker generates a brute force attack, the vault has 330 points, therefore there are a total of C(330, 9) = 1.1457 x 10 17 combinations with 9 elements. Only C(30,9) = 1.14307 x 10 9 of these combinations are used to decode the vault. Therefore it takes C(330,9) / C(30,9) = 8.0079 x 109 evaluations for an attacker to decode the vault[1]. The performance of the vault can be improved by application of non-invertible transformations and multiple biometric traits.

V. FUTURE WORK

The inherent simplicity of the RI means that in mass production the cost of the entire unit could come below, say, $100. This is still considerably more expensive than some competing technologies which have a much cheaper scan component (such as fingerprint chips). The trade off is accuracy. If accuracy is important to the ID application, perhaps the additional cost of RI can be justified. With the proliferation of e-commerce applications, RI might reach a critical mass. Because of the RI's accuracy and small signature size it fits more naturally with the encryption that is needed for e-commerce security than competing biometric ID technologies.

VI. REFERENCES

[1]. Security Analysis of Hardened Retina Based Fuzzy Vault V. S. Meenakshi, (Autonomous), Coimbatore, India. e-mail: meenasri70@yahoo.com Dr. G. Padmavathi, ,Coimbatore, India.e-mail: mail_padma@yahoo.com 2009 International Conference on Advances in Recent Technologies in Communication and Computing.

[2]. Smart card with iris recognition for high security access environment. 978-1-4244-7000-6/11/$26.00 ©2011 IEEE .Mohammed A. M. Abdullah F. H. A. Al-Dulaimi, Computer Engineering Department,University of Mosul, Mosul, Iraq,m.am_86@yahoo.com. Waleed Al-Nuaimy Ali Al-Ataby, Department of Electrical Engineering and Electronics, University of Liverpool. Liverpool, L69 3GJ, UK wax@liv.ac.uk

[3]. Retinal Biometrics based Authentication and Key Exchange System. International Journal of Computer Applications (0975 – 8887) Volume 19– No.1, April 2011

[4]. G. Bella, S. Bistarelli, and F. Martinelli, "Biometrics to Enhance Smartcard Security". Lecture Notes in Computer Science, vol. 3364, 2005.

[5]. L. Bechelli, S. Bistarelli, and A. Vaccarelli, "Biometrics authentication with smartcard". Technical Report, CNR, Istituto di Informaticae Telematica, Pisa, 2002.

[6]. Lawrence Aragon, "Facing Up to Security Technology," PC Week (January 12, 1988): p.88.

[7]. A. Juels and M.Sudan, "A fuzzy vault scheme", Proceedings of IEEE International symposium Information Theory, pp. 408, 2002.

[8]. Karthik Nandakumar, Abhishek Nagar and Anil K.Jain, "Hardening Fingerprint Fuzzy Vault Using Password", International conference on Biometrics, pp. 927 – 938, 2007.

[9]. Ratha, N.K., J.H. Connell, and R.M. Bolle, "Enhancing security andprivacy in biometrics-based authentication systems", IBM Systems Journal, vol. 40, no. 3, pp. 614 – 634, 2001.

[10]. A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125–143, June 2006.

[11]. A. K. Jain, A. Ross, and U. Uludag, "Biometric Template Security:Challenges and Solutions," in Proceedings of European Signal Processing Conference (EUSIPCO), Antalya, Turkey, September 2005.

[12]. Anil K.Jain, Karthik Nanda Kumar and Abhishek Nagar, "Biometric Template Security" EURASIP Journal on Advance in Signal Processing, special issue on Biometrics, January 2008.

[13]. Joes Staal, Associate Member, IEEE, Michael D. Abràmoff,Member,IEEE, Meindert Niemeijer, Max A. Viergever, Member,IEEE, and Bram van Ginneken, Associate Member, IEEE, "Ridge-Based Vessel Segmentation in Color Images of the Retina",IEEE transactions On medical imaging, vol. 23, no. 4, April 2004

[14]. K.NandaKumar, "Multibiometric Systems: Fusion Strategies andTemplate Security", PhD Thesis, Department of Computer Scienceand Engineering, Michigan State University, January 2008.

[15]. Jain, Anil K. Jain and Arun Ross, "Multibiometric systems,"Communications of the ACM," January 2004, Volume 47, Number 1(2004).

[16]. A.K. Jain and A. Ross, "Learning User-specific parameters in a Multibiometric System", Proc. IEEE International Conference on Image Processing(ICIP), Rochester, New York, pp. 57 – 60, September 22 – 25, 2002.

[17]. Atmel Cooperation, AT90S8515 Microcontroller Datasheet. Available online: http://www.atmel.com/ dyn/resources/ prod_documents/doc0841.pdf

[18]. The MD5 Message-Digest Algorithm. RFC 1321, section 3.4, "Step 4.Process Message in 16-Word Blocks", page 5.

Short Bio Data for the Author

Miss. R. Sheethal is currently doing MS-Software Engineering (5 years Integrated) pre-final year in Vellore Institute of Technology, Vellore. She is working as a Faculty (Part Time) for .NET in NIIT-Vellore. She is also Certified for "DB2 9 Fundamentals" from IBM, "Network Fundamentals" from CISCO, Microsoft Certified Technical Specialist (MCTS) for both SQL Server 2008 and .NET Windows Application 2.0, Microsoft Certified IT Professional (MCITP) for Designing Database Solutions and Data Access Using Microsoft SQL.