Int. J. Communications, Network and System Sciences, 2016, 9, 506-518
http://www.scirp.org/journal/ijcns
ISSN Online: 1913-3723
ISSN Print: 1913-3715

Fusion of Iris and Fingerprint Biometric Identifier for ATM Services: An Investigative Study

S. Koteswari[1], P. John Paul[2], Agshare Dheeraj[3], Rajesh Kone[4]

[1]Department of ECE, Chaitanya College of Engineering, Bhimavaram, Andhra Pradesh, India
[2]Department of ECE, Mallareddy College of Engineering (MRCE), Secunderabad, Telangana, India
[3]Department of ECE, RGUKT Basar University, Telangana, India
[4]Department of ECE, Sri Vasavi College of Engineering Tadepalligudem, Andhra Pradesh, India
Email: eshwari.ngr@gmail.com

How to cite this paper: Koteswari, S., Paul, P.J., Dheeraj, A. and Kone, R. (2016) Fusion of Iris and Fingerprint Biometric Identifier for ATM Services: An Investigative Study. *Int. J. Communications, Network and System Sciences,* **9**, 506-518.
http://dx.doi.org/10.4236/ijcns.2016.911040

Received: September 20, 2016
Accepted: November 21, 2016
Published: November 24, 2016

Abstract

Wrongdoing at ATMs has turned into an issue across the country that appearances clients, as well as bank administrators and this money related wrongdoing case rise over and again as of late. A great deal of crooks mess with the ATM terminal and take clients' card points of interest by illicit means. When clients' bank card is lost and the secret key is stolen, the clients' record is helpless against assault. Conventional ATM frameworks confirm for the most part by utilizing a card (credit, charge, or brilliant) and a secret word or PIN which doubtlessly has a few imperfections. The predominant methods of client verification, which includes the utilization of either passwords, and client IDs (identifiers) or recognizable proof cards and PINs (individual distinguishing proof numbers), experience the ill effects of a few confinements. Passwords and PINs can be unlawfully obtained by direct incognito perception. At whatever point credit and ATM cards are lost or stolen, an unapproved customer can every now and again think about the right individual codes. An implanted unique mark and iris combined biometric validation plan for robotized teller machine (ATM) managing an account framework is proposed in this paper. In this plan, a multimodal biometric system is intertwined with the ATM for individual validation to ease the security level. The paper is masterminded as follows: Section 2 gives the back ground and literature survey of ATM security and the requirement for biometrics, and the related work on biometric identifiers. Section 3 depicts the materials and techniques utilized to direct the overview. Section 4 exhibits the outcomes got and the talks on the outcomes. Section 5 winds up with conclusions.

Keywords

ATM, Security, Biometrics, PIN, Fingerprints, Iris

1. Introduction

Quick improvement of saving money innovation has changed the way that keeping money exercises is managed. One saving money innovation that has affected emphatically and adversely to keep money exercises and exchanges is the approach of computerized teller machine (ATM). With an ATM, a client can conduct a few keeping money exercises, for example, money withdrawal, cash exchange, paying telephone and power bills past authority hours and physical collaboration with bank staff. More or less, ATM gives clients a speedy and helpful approach to get to their ledgers and to lead monetary exchanges. Individual recognizable proof number (PIN) or secret key is one essential perspective in ATM security system. PIN or watchword is normally used to secure and shield monetary data of clients from unapproved access [1]. An ATM (referred to by different names, for example, computerized saving money machine, money point, money machine or a gap in the divider) is a mechanical framework that has its underlying foundations inserted in the records and records of a deal with a record association [2]. It is a modernized machine intended to apportion money to bank clients without need of human connection; it can exchange cash between ledgers and give other essential budgetary administrations, for example, parity enquiries, scaled down proclamation, withdrawal and quick money among others [3].

To consider the conceivable fakeness benefits in ATM.

To audit the current fraudulences arrangements and to discover holes in the current administrations.

To propose the answer for evading the crevices.

Traditional techniques for recognizable proof in view of ownership of ID cards or selective information like a government disability number or a watchword are not all together solid. ID cards can be lost, ignored or lost; passwords can be overlooked or contained; yet ones' biometric is obviously associated with its proprietor. It can't be obtained, stolen or effectively overlooked. Automatic teller machines have turned into a develop innovation which gives money related administrations to an expanding portion of the populace in numerous nations. Biometrics, especially unique finger impression filtering, keeps on picking up acknowledgment as a solid type of securing access through recognizable proof and confirmation forms. This proposal distinguishes that an abnormal state shows for the adjustment of existing ATM frameworks utilizing both security conventions as PIN and biometric unique mark and iris system. We have possessed the capacity to build up a multimodal instrument as a biometric measure to improve the security components of the ATM for powerful saving money exchange for Indian keeping money framework.

The model of the created application has been discovered promising on the record of its affectability to the acknowledgment of the clients, multimodal biometric (combination of unique finger impression, iris) as contained in the database. This framework when completely conveyed will definitely lessen the rate of false exercises on the ATM machines with the end goal that only the enrolled proprietor of a card has access to the bank account. In the greater part of the current multimodal biometric procedures, one

and only change is utilized. Thus, it is turning into an extraordinary trouble in light of the fact that the picture pressure standard is function (or change) particular. Rather than utilizing stand out change, the proposition investigates of utilizing cross breed change. The analysis results are extremely reassuring.

2. Background and Literature Survey

2.1. ATM (Automated Teller Machine)

There is little doubt that fast development of banking technology has modified the approach in addressing banking activities. One in all the examples is ATM machine (ATM). Using ATM, a client can conduct many banking activities as money withdrawal, cash transfer, paying phone and electricity bills on the far side official hours and physical interaction with bank workers. In short, ATM provides customers fast and convenient thanks to access their bank accounts and to conduct monetary transactions. Personal positive identification (PIN) is one in all necessary aspects in ATM security that is usually accustomed secure and shield monetary data of shoppers from unauthorized access. They compare the code against a keep list of approved passwords and users. PIN usually in a rather four digit combination of numbers that entered through ATM panel. If the code is legitimate, the system permits the access at the safety level approved for the owner of the account. In general, PIN is decent to safeguard against fraud and effectively eliminating almost typical makes a try to realize unauthorized access. The four digits PIN is additionally simple to hit the books and can be written quickly with few errors and is something as tough to be cracked if it is managed properly. the foremost recent programs to steal ATM holder's cash terribly simple, some public that sleep in today's high school society that area unit bombarded everyday by such a many ranges as Social Security number, laptop Arcanum, MasterCard range. Sometimes each one is confusing, tough to be recalled in a right away will result in a heavy drawback. Generally it is written down on little piece of paper or on ATM card so do not expect such event. The strength of PIN as a security is weakened since the probability of the code unworthy to others enhanced. A private positive identification (PIN) is employed in many equivalent as a Arcanum. It is numerical in format and sort of a acronym that ought to be unbroken secret. The foremost common use of the PIN is in ATM machine (ATM). "Most usually PIN's area unit 4-digit numbers within the vary 0000 - 9999 leading to 10,000 attainable numbers, in order that a wrongdoer would want to guess a median of 5000 times to urge the proper PIN". Statistics may be a apace evolving technology that's being wide employed in forensics, as criminal identification and jail security, that has the potential to be employed in an over-sized vary of civilian application areas. Statistics is accustomed stop unauthorized access to ATMs, cellular phones, good cards, desktop PCs, workstations and laptop networks.

2.2. Biometrics

Biometrics can be characterized as a quantifiable physiological and behavioral trademark that can be caught and in this way contrasted and another example at the season

of check. It is computerized strategies for perceiving a man taking into account a physiological or behavioral trademark [4]. It is a measure of an individual's novel physical or behavioral attributes to perceive or confirm its personality [5]. Common physical biometrics qualities incorporate unique mark, hand or palm geometry, retina, iris and face while mainstream behavioral attributes are mark and voice. Biometrics innovations are a protected method for validation since biometrics information are novel, can't be shared, can't be duplicated and can't be lost.

Biometrics is a measure of physical or behavioral trademark that can be caught and in this way contrasted and another occasion around then of confirmation. Any human physical or behavioral biometrics can be utilized as a biometric trademark the length of it fulfills the accompanying necessities.

- Universality—Every individual ought to have the biometric trademark.
- Distinctiveness—Any two people ought to be adequately unique as far as the trademark.
- Permanence—The trademark ought to be adequately invariant over a timeframe.
- Collectability—The biometric trademark ought to be quantifiable with some detecting gadget.
- Performance—Refers to the level of precision and speed of acknowledgment of the framework, the assets required to accomplish the coveted acknowledgment level, and the operational and natural components that influence the exactness and speed.
- Acceptability—Indicates the degree to which individuals will acknowledge the utilization of a specific biometric identifier (trademark) in their everyday lives.
- Resistance/Circumvention-Refers to the level of trouble required to thrashing or sidesteps the framework.

Unimodal biometrics in ATM system:

The expression "biometrics" is gotten from the Greek words "bio" (life) and "measurements" (to quantify). Biometrics alludes to programmed framework that utilizations quantifiable physiological attributes or behavioral characteristics to perceive the personality or confirm the guaranteed character of a person. Biometric frameworks in light of single wellspring of data are called Unimodal frameworks. The three approaches to build up the personality of a man are "something you know" (e.g., secret key, PIN) which gives first level of security and "something you convey" (e.g., ID card, keen card) and "something you are" (biometrics), these give second level of security. In savvy card, the unique finger impression layouts are encoded into a brilliant card memory, to recognize a man, his/her fingerprints are looked at against the computerized formats put away in the card memory. Personality administration framework is to locate the individual's character. Customary techniques for setting up a man's character incorporate information based and token-based instruments, which can be effectively lost, shared or stolen. To conquer every one of these issues biometrics was presented.

Physical biometrics is a static biometrics and the information is gotten from the estimation of an activity performed by a person. It joins one of a kind finger impression, Iris, Retina, Hand geometry; Palm print, Face affirmation, DNA and Vascular Pattern

Recognition. Behavioral biometrics is a dynamic biometrics and the data is gotten from the estimation of an action performed by an individual and the parameter considered here is time; the measures action has a beginning, focus and end it incorporates signature, keystroke, Handwriting, Voice acknowledgment and Gait. Delicate biometrics otherwise called concoction biometrics is a human trademark that gives some data about the person. It incorporates stature, weight and shade of hair [5].

The most established and fruitful innovation which is executed in ATM is unique mark acknowledgment [6]. The calculations utilized for unique finger impression acknowledgment is particulars extraction and solitary point identification. After the client embeds the card in the ATM framework and enters the PIN number, if the PIN number is substantial, then the client needs to print his/her unique mark for verification reason. In the event that the unique finger impression layout matches with the format which is put away in the database amid enlistment, then the client is verified and he/she can get to their record which is appeared in **Figure 1**. The purpose for the ubiquity of finger impression based acknowledgment among the biometric-based security frameworks is the un-changeability of fingerprints amid the human life expectancy and their uniqueness. This kind of framework gives the essential level of security and the blunder rates is high [6].

Impediments of Unimodal Biometrics:

Biometric framework is basically design acknowledgment framework that works by gaining biometric information from a person. Biometric frameworks are regularly influenced by the accompanying issues.

Noise in detected information the precision assumes a noteworthy part in acknowledgment of biometrics. The exactness of the biometric framework is extremely touchy to the nature of the biometric input and the commotion show in the information will bring about a critical diminishment in the precision.

Non-Universality—If each individual can show the biometric characteristic for acknowledgment, then the quality is said to be general. Non-comprehensiveness prompts Failure to Enroll (FTE) blunder in a biometric framework.

Lack of distinction—Feature separated from various people might be comparable. This absence of uniqueness expands the False Accept Rate (FAR) of a biometric framework.

Intra-class varieties the information gained for check won't match to the information utilized for creating format amid enlistment. For instance the face biometric is caught under various points. Expansive intra-class varieties increment the False Reject Rate (FRR) of a biometric framework [7].

Inter-class varieties—It happens essentially between twins. It alludes to the cover of highlight spaces relating to various people. Substantial between class varieties increment the False Acceptance Rate (FAR) of a biometric framework.

Spoofing—A biometric framework might be evaded by displaying a fake biometric quality to the sensor.

Multi-biometrics in ATM system:

Multi-biometrics is a combination of one or more biometrics. It can be any physical or behavioral biometrics. Multi-biometrics overcomes the problem of unimodal biometrics [8]. These frameworks are required to be more dependable because of the nearness of numerous, genuinely autonomous bits of proof. This framework basically addresses the issue of non-all inclusiveness and gives hostile to parodying measures by making it troublesome for an interloper to at the same time parody the various characteristics of a honest to goodness client. There are assortment of components that should be considered while planning the multi-biometric framework, these incorporate the decision and number of biometric characteristics; the level in the biometric framework at which data gave by numerous qualities ought to be coordinated. In view of the different sources multi-biometric frameworks are delegated Multi-sensor frameworks, Multi-calculation frameworks, Multi-occasion frameworks and Multi-test frameworks. There is different level of combination like Sensor level combination, Score level combination, coordinating level combination and highlight level combination [9]. Multi-biometrics is predominantly used to give security in the server side. The unique finger impression, Iris and Face acknowledgment is utilized to give security. The elements are separated from biometrics utilizing highlight level combination and the elements are joined into single biometric and biometric cryptosystem. The different points of interest are:

- Increase of unwavering quality and distinguishing proof quality, while lessening FAR (False Acceptance Rate) mistake rates.
- A assortment of identifiers that can be utilized together or independently.
- Speeding up the recognizable proof technique.
- The restrictions of multi-biometrics are:
- If one of the biometric comes up short because of nearness of clamor in the biometrics, the FRR (False Reject Rate) will be expanded.

Abhijeet S. Kale *et al.* the foremost point of the portrayed proposition is to ad lib the security of ATM framework utilizing Aadhaar card and unique finger impression and diminishing the dependability on attractive card pursuer [10]. Utilizing ARM 7 microcontroller a model is proposed in the script an extra module for unique mark scanner and Aadhaar card recognizer, this model is organized by GSM which is connected with security division of bank. This proposed model closes to tackle the security issues up to a level. K. Lavanya *et al.* gone for multimodal biometrics for check token to anticipate security breech on ATM clients [11]. At first the check of an individual is finished by PIN and unimodal biometric. Be that as it may, the exploration proposed the extent of multimodal biometrics and confinements of unimodal over it. A multimodal biometric framework whole up the assortment of biometric data of people to gives a superior and effective method for going. A few existing techniques are utilized for ATM security. Asst. Prof. Sanjay S. Ghodke *et al.* proposed venture utilizes palm print system for biometric recognizable proof; closed examination on palm print distinguishing proof had high precision and proficiency rate, the utilized calculation for palm print acknowledgment speed up the working procedure and fathoming the security issues [12]. Kande Archana *et al.* proposed to improve the security utilizing multimodal biometrics

as a part of ATMs, paper looks at the constraints of unimodal biometrics and level of security gave by the multimodal biometrics. By utilizing multimodal biometrics with two level securities, the mistake rates has been decreased. The security level likewise expanded by utilizing multimodal biometrics which maintains a strategic distance from the programmers for any breech into the framework since the multimodal biometrics gives a superior fluffy rationales to the framework's security.

Sheik and rabaiotti [13] analyzed the unified kingdom identify scoundrel plan. Their investigation drew nearer the scheme from the point of view of high volume open arrangement and depicted an exchange off triangle model. They inferred a few qualities, for example, exactness, protection and adaptability in biometric based character administration framework, where accentuation on one undermines the other. Amurthy and reddy [14] developed an inserted unique mark framework, which is utilized for ATM security applications. In their framework, investors gather clients fingerprints and versatile numbers while opening records, then clients just get to ATM machine. The working of the ATM machine is to such an extent that when a client place a finger on the unique finger impression module, it consequently produced every time diverse 4-digit code as a message to the portable of the approved client through GSM modem associated with the microcontroller. The code got by the client is gone into the ATM machine by squeezing the keys on the touch screen. After entering it checks whether it is a legitimate one or not and permits the client further get to.

3. Materials and Methods

The objective populace of this study was understudies and representative of some business establishments in Andhra Pradesh. The clients and understudies were arbitrarily chosen.

Table 1. Profile of participants.

No	Profile	Description
1.	Age	20 - 55 years old
2.	Gender (male:female)	87:80
3.	Bank account and ATM card	The respondents over differing kinds of accounts in numerous banks, bank product and styles of services rendered.

The instrument utilized for this study was a 16-thing survey created by the specialists. The things in the poll were gotten from broad review of important writing and oral meeting the instrument has three segments the main segment manages members' profile the second manages members use and unwavering quality of ATM the third area manages dependability of unique mark biometric normal for the 200 duplicates of the survey controlled 167 usable duplicates were returned. This spoke to 84 percent return rate. This study was completed over a time of three months. The things in the instrument were investigated utilizing illustrative measurable techniques [14]. The auxiliary wellsprings of information were gotten from diaries, the web and course readings.

Master judgments were utilized to determine the legitimacy of the things in the survey. Two specialists face-accepted every one of the things in the survey. The wordings of things were likewise checked for clarity. Two things in the survey were erased for immateriality while three vaguely worded things were rebuilt to reflect clarity. After the remedies, the two specialists observed the things to be appropriate for organization on the subjects.

Table 2. Use and reliability of ATM (1).

No	Question	Responses		Total	Percentage (%)	
		Yes	No		Yes	No
1.	Did you ever use ATM?	147	20	167	88	12
2.	Do you feel that you password (or) pin is secured while using ATM?	50	117	167	31	69
3.	Since how many years you are using ATM? a)Less than a year b)Greater than one year, less than 3 years c) More than 3 years	20 47 100	--- -- --	167	12 28 60	88 72 40
4	Since how many years you are using ATM? a)Personally b)Media c) Friends	167 20 44 103	0 --- -- --	167 167	 12 26 58	 88 74 42

Table 3. Use and reliability of ATM.

No	Question	Responses		Total	Percentage (%)	
		Yes	No		Yes	No
5.	Does any measure have been taken regarding ATM fraud?	110	57	167	66	34
6.	Do you feel ATM transactions are risky?	157	10	167	94	06
7.	Does security concerns will make you to stop using ATM?	160	7	167	95	05
8.	Do you prefer a higher security for ATM?	167	0	167	100	00
9	Do you know that the biometrics is a means of authentication?	140	27	167	84	16
10.	Do you feel biometric is a gold standard for ATM security	167	0	167	100	00

4. Results and Discussion

The synopsis of the outcomes acquired is displayed (Tables 1-3). Table 1 demonstrates the profile of members. The scope of period of members was 20 - 55 years. 87 guys and 80 females partook in the study. Each of the members own no less than one kind of financial balance this reliant on the bank, the items offered and benefits gave by the bank. This came about to the presentation of ATM and the administrations it gives. Table 2 demonstrates the utilization and unwavering quality of ATM. 147 respondents speaking to a few clients and staff of a few banks, speaking to 88 percent of the populace utilize the ATM while 12 percent of the populace is yet to utilize the machine. This 12 percent of the populace is still distrustful about utilizing ATM as a result of the issues

acquainted with it. Such issues as failure of the machine to give back a client's card after exchange which may take days to redress, charging a client's bookkeeping in an exchange much part client is not paid and money not apportioned, and "out of administration" normally showed by the machine which more often than not is baffling and disappointing among others. 100 percent of the populace knows about one type of ATM misrepresentation or another. 89 percent of the populace imagines that ATM exchanges are turning out to be excessively hazardous this required 93 percent of the populace avowing that there will proceed with the utilization of ATM in light of security issues connected with the machine. Hence, 100 percent of the populace favored third verification aside the utilization of ATM card and PIN this populace trusted that with the imbuement of biometrics qualities to existing ATM card and PIN, ATM security will be enhanced radically [15].

Table 4. Reliability of biometrics characteristics.

S. No.	Question	Biometric classification	Responses	Percentage (%)
1.	Characteristic of statistics that you detected off?	a) Finger-print	106	63
		b) Iris	18	11
		c) Face-recognition	08	05
		d) Signature	10	06
		e) DNA	06	04
		f) Retina	11	06
		g) Voice	08	05
		Total	**167**	**100**

Table 4 demonstrates the unwavering quality and fame of unique mark and iris biometric character. 63 percent of the populace is acquainted with unique mark biometric and 11 percent of the populace is acquainted with iris biometric. 54 percent of the populace emphatically trusted that with the joining of unique finger impression to the current ATM card and PIN, will gave better security to the ATM, and 19 percent of the populace accepted with the fuse of iris for better security to ATM.

Table 5 demonstrates the biometric clasification and its responses which represent the reliability of biometric characteristics along with their percentages.

Table 5. Reliability of biometrics characteristics based on security.

S. No.	Question	Biometric classification	Responses	Percentage (%)
1.	What are the Characteristic of statistics, would offer higher security?	a) Finger-print	90	54
		b) Iris	31	19
		c) Face-recognition	17	10
		d) Signature	10	06
		e) DNA	02	01
		f) Retina	10	06
		g) Voice	07	04
		Total	**167**	**100**

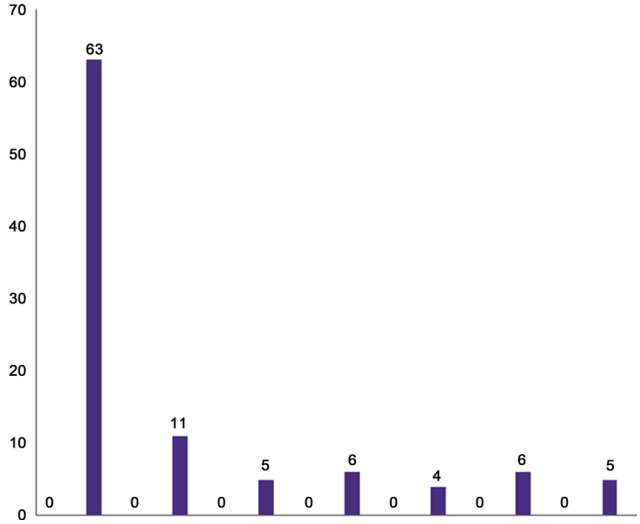

Figure 1. Comparative survey of other biometrics.

4.1. Fingerprint Biometrics

Unique mark designs stay unaltered all through the whole grown-up life and are effortlessly delivered for distinguishing proof. On the off chance that a finger is harmed, different fingers that are beforehand selected into the framework can likewise be utilized for distinguishing proof. Genuinely little storage room is required for the biometric layout, diminishing the span of the database required. Every last unique finger impressions including every one of the fingers are interesting, even the indistinguishable twins have diverse fingerprints. Sound potential for scientific use as the vast majority of the nations have existing unique mark databases. Generally reasonable and offers abnormal state of precision. A unique mark is an example of edges and wrinkles situated on the tip of every finger. Fingerprints were utilized for individual distinguishing proof for a long time and the coordinating precision is satisfactory. Before, examples were separated by making a connected impression of the fingertip on paper. Today, minimal sensors give computerized pictures of these examples. The acknowledgment procedure begins by catching the finger picture by direct contact with a pursuer gadget, which can likewise play out some approval systems to stay away from fake measures (check of temperature and heartbeat). The uniqueness of a finger impression can be controlled by the example of edges and wrinkles and additionally by the details focuses. The coordinating procedure includes looking at the two-dimensional particulars test and format designs. Among the principle points of interest for the utilization of fingerprints are the larger amount of worthiness and their convenience, also the way that it is a developed innovation with quite a while of demonstrated viability. Additionally, the way that its innovation is lawfully acknowledged and that a great many enlisted fingerprints exist, are essential. As hindrances, it is viewed as defenseless against clamor and contortion brought on by soil and bends. Additionally, since physical contact between the finger and checking gadget is required, the surface can turn out to be sleek and overcast after rehashed utilize and decrease the affectability. Hygienic contemplations must be considered as well.

4.2. Iris Recognition

In 1987 the creators acquired a patent for a unimplemented calculated configuration of an iris biometric framework. Iris acknowledgment is a standout amongst the most blasting biometric modalities. It has been come to in the most recent 20 years because of its novel character as a biometric highlight, which makes iris recognizable proof and confirmation frameworks a standout amongst the most exact biometric methodology Iris is remotely obvious, shading ring around the student, the extravagant example is one of a kind for every person, the privilege and left eye of any given individual, have disconnected iris designs. They are steady all through life and fulfill arbitrariness. Their configuration recommended very controlled conditions, headrest, target picture to coordinate the subject's look, manual administrator, student development and compression was controlled by changing the enlightenment to constrain the understudy to a foreordained size. Discovery of the understudy is done through edge based methodology. Extraction of iris descriptors is performed through example acknowledgment instruments, edge discovery calculations, Hough change. Iris elements could be put away on a charge cards or distinguishing proof card to bolster a confirmation undertaking.

4.3. Multimodal Biometrics and Multi-Biometrics

Biometrics framework can be characterized as an acknowledgment framework which is equipped for distinguishing a man in view of their natural properties. The expression "multimodal biometric" alludes to different biometric attributes utilized together at a particular level of combination to perceive people. The "multi-biometrics" incorporates either the utilization of various calculations, likewise called classifiers at enrolment or coordinating stages [16] for the same biometric attribute, or the utilization of numerous sensors of the same biometric quality like utilizing distinctive instruments to catch the biometric subtle elements, or utilizing different cases of the same biometric characteristic like the utilization of fingerprints of three fingers, or at long last utilizing rehashed occurrences like rehashed impressions of one finger. The proposed model for multimodal biometrics is shown in Figure 2, which provides encouraging results and improves security for ATM banking.

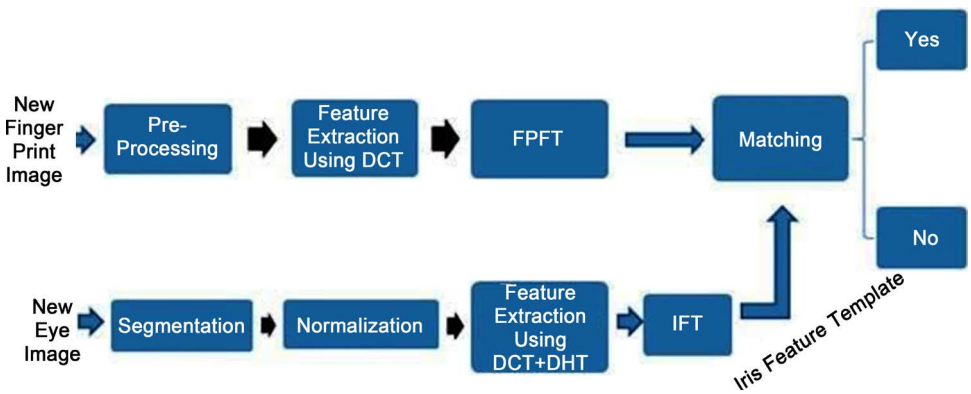

Figure 2. Proposed model for multimodal biometrics for ATM banking.

5. Conclusion

Routine system for perceiving confirmation that considers obligation regarding cards or selects information like a governing body managed reserve funds number or a watchword is not all together reliable. ID cards can be lost, overlooked or lost: passwords can be forgotten or comprised, but ones' biometric is undeniably connected to its owner. It cannot be borrowed, stolen or easily forgotten. Automatic teller machines have become a mature technology which provides financial services to an increasing segment of the population in many countries. Biometrics, in particular fingerprint scanning, continues to gain acceptance as a reliable form of securing access through identification and verification processes. This paper identifies a high level model for the modification of existing ATM systems using both security protocols as PIN and biometric fingerprint and iris strategy. We have been able to develop a multimodal mechanism as a biometric measure to enhance the security features of the ATM for effective banking transaction for Indian banking system. The prototype of the developed application has been found promising on the account of its sensitivity to the recognition of the customers, multimodal biometric (fusion of fingerprint, iris) as contained in the database. This system when fully deployed will definably reduce the rate of fraudulent activities on the ATM machines such that only the registered owner of a card has the access to the bank account. Late instances of data fraud have increased the requirement for techniques to demonstrate that someone is really who he/she claims to be. Biometric verification innovation utilizing multi-modular biometrics (fingerprint and iris) may take care of numerous issues since a man's biometric information is undeniably associated its owner, and is non transferable and special for each person. Biometrics is an astonishing case investigating certification issues and also, if painstakingly utilized, could be a drawing developed with the probability to make our general populace more secure, diminish trickery and incite client comfort by comprehensively giving the running with three functionalities: (a) positive recognizable proof, (b) huge scale recognizable proof and (c) screening.

References

[1] Wan, W.W.N., Luk, C.L. and Chow, C.W.C. (2005) Customers Adoption of Banking Channels in Hong Kong. *International Journal of Bank Marketing*, **23**, 255-272. http://dx.doi.org/10.1108/02652320510591711

[2] Das, S.S. and Debbarma, J. (2011) Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian e-Banaking System. *International Journal of Information and Communication Technology Research*, **1**, 197-203.

[3] Roberts, C. (2005) Biometrics. http://www.ccip.govt.nz/newzroom/informationnotes/2005/biometrics.pdf

[4] Oyeka, C.A. (1990) An Introduction to Applied Statistical Methods. Modern Avocation Publishing Company, Enugu, 4, 36, 56.

[5] Zuwaylif, F.H. (1999) General Applied Statistics. 3rd Edition, Addison Wesley Publishing Company, California.

[6] Wikipedia (2012) Biometrics. http://en.wikipedia.org/wiki/Biometrics

[7] Eze, J.I., Obiegbu, M.E. and Jude-Eze, E.N. (2005) Statistics and Qualitative Methods for Construction and Business Managers. The Nigerian Institute of Building, Lagos.

[8] Gupta, P., Rattani, A., Mehrotra, H. and Kaushik, A.K. (2006) Multimodal Biometrics System for Efficient Human Recognition. *International Society of Optical Engineering*, **6202**, 62020Y.

[9] Jain, A.K., Ross, A. and Prabhakar, S. (2004) An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, **14**, 4-20. http://dx.doi.org/10.1109/TCSVT.2003.818349

[10] Kale, A.S. and Nanda, S.K. (2014) A Review Paper on Design of Highly Secured Automatic Teller Machine System by Using Aadhaar Card and Fingerprint. *International Journal of Advance Research in Computer Science and Management Studies*, **2**. www.ijarcsms.com

[11] Lavanya, K. and Naga Raju, C. (2013) A Comparative Study on ATM Security with Multimodal Biometric System. *International Journal of Computer Science & Engineering Technology*, **4**.

[12] O'Gorman, L. (1998) Overview of Fingerprint Verification Technologies. *Elsevier Information Security Technical Report*, **3**.

[13] Shaikh, S.A. and Rabaiotti, J.R. (2010) Characteristic Trade-Offs in Designing Large-Scale Biometric Based Identity Management Systems. *Journal of Network and Computer Applications*, **33**, 342-351. http://dx.doi.org/10.1016/j.jnca.2009.12.015

[14] Ratha, N.K., Connell, J.H. and Bolle, R.M. (2001) Enhancing Security and Privacy in Biometrics-Based Authentication Sytems. *IBM Systems Journal*, **40**, 614-634. http://dx.doi.org/10.1147/sj.403.0614

[15] Ghodke, S.S., Kolhe, H., Chaudhari, S., Deshpande, K. and Athavle, S. (2014) ATM Transaction Security System Using Biometric Palm Print Recognition and Transaction Confirmation System. *International Journal of Engineering and Computer Science*, **3**. www.ijecs.in

[16] Paul, P.J. and Girija, P.N. (2011) A High Performance Novel Image Compression Technique Using Hybrid Transform for Multimedia Applications. *International Journal of Computer Science and Network Security*, **11**, 119-125.