ISSN (Online): 2455-7838
SJIF Impact Factor (2016): 4.144

EPRA International Journal of

Research & Development

(IJRD)

Monthly Peer Reviewed & Indexed
International Online Journal

Volume:2, Issue:1, January 2017

Published By :
EPRA Journals

SJIF Impact Factor: 4.144 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 2 | Issue: 1 | January | 2017

2-FACTOR AUTHENTICATION FOR AVOIDING FRAUDULENCES IN ATM SERVICES BY MMBS

S.Koteswari[1]
[1]Research Scholar, Department of ECE, Rayalasema University, Kurnool, Andhra Pradesh, India

Dr .P. John Paul[2]
[2] Principal & Professor, Department of ECE, Mallareddy College of Engineering (MRCE), Maisamaguda, Secunderabad, Telangana , India.

ABSTRACT

In a quickly evolving world, observation is no sufficiently longer to put a stop to ATM misrepresentation. Budgetary foundation is progressively at of benignancy of intelligent hostile on their ATM systems. For huge information investigation, in fact needs a progressive approach, so as to win security. Keeping them one basic stride in front of fraudsters, budgetary foundations can now anticipate the early shake indications of misrepresentation. This examination paper researches the similar investigation of highlight level and choice level combination of multimodal biometrics framework and security is enhanced by giving two-calculate validation. Multimodal biometric framework in light of iris and unique mark mean to circuit at least two physical or behavioral qualities to give ideal False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER) in this manner enhancing framework precision and trustworthiness. We have outlined a combination strategy in somewhat extraordinary route to the examination of traditional showing up combination strategies it is connected all in all method for CASIA iris information base and unique mark databases (FVC). Include level combination is performed utilizing DCT-DHT and Apart from that XNOR-AND sort choice combination utilized as a part of a tweaked level to differ the execution parameters. Trial comes about in that capacity Simulation and union outcomes are acquired to known the precision of the framework.

KEYWORDS: *Authentication; Iris; Fingerprint; ATM Security; MMBS; 2FA; DCT-DHT;*

1. INTRODUCTION

1.1 ATM

Scot John Shepherd - Barron imagined ATM (Automated Teller Machine). The world's first ATM was introduced in a branch of Barclaysin the northern London ward of Enfield, Middlesex, in 1967.Without the need of human teller, bank's client can make money withdrawals and can check their record adjust whenever through an electronic gadget ATM, it will likewise permit to store money or checks , furthermore cash exchange among their ledgers. Clients need to verify themselves by utilizing a plastic card with an attractive stripe which is known as "ATM CARD". The client's record number and a numeric secret word which is known as PIN (Personal Identification Number) are encoded on an attractive stripe. The procedure in ATM incorporates, at first the ATM prompts the client to embed the card. At the point when the card is embedded, client's PIN is asked for, as the client inputs his or her PIN , if the card is substantial then it is prepared by the machine, and next then it prompts the client to either pull back, exchange or store money according to the client's prerequisite. The components for the development of ATM are that the exchanges should be possible at whatever time and more than one time in a day and relatively time utilization is less to make an exchange than a teller in banks, which makes convenience for individuals. It is much solid as the banks work stack diminishes, exchange exactness makes strides. Though the issues in ATM are grouped in like manner in view of the issues confronted by clients which incorporates non-getting money while the record charged, Wrong inclusion of the ATM card. This issue is more normal with new ATM clients who are not acquainted with ATM machine furthermore at times they didn't get slip of record adjust [1]. Close to these the cash exchange issue are some time cash stuck in machine at the season of exchange, Some time machine did not acknowledge ATM cards, Time out issue when the client delays for any progression of preparing. In like manner we additionally had Customer's issue when the procedure of bank is change, and when money not accessible. Lastly the issues confronted by the banks are robbery cash from ATM'S, burglary of ATM'S (counting burglary of whole ATM'S),System issue (counting server down),System failure(system crash or the product not work properly),Hack the banks site which impact entire keeping money framework. As appeared in figure 1 beneath , ATM assaults are named – ATM physical assaults, and a basic misrepresentation of attacks are clearly mentioned.

.

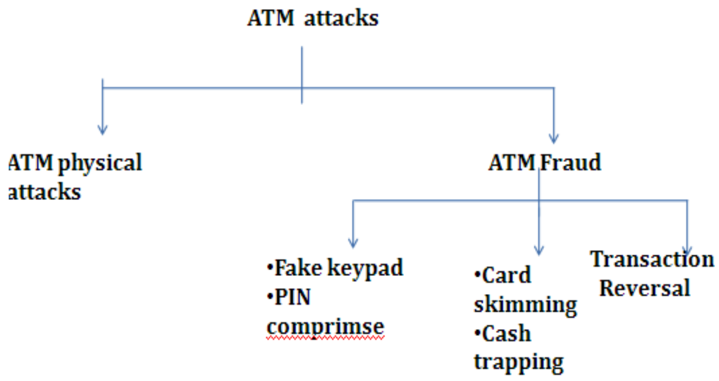

Figure1. Types of ATM attacks

A part of the shirking measures ought to be considered to keep the fraudulences in ATM, for instance, :Wrap-up, means reliably cover your one hand with the other hand while entering in the PIN number. By securing your PIN, offenders don't have passage to your record when card information is compromised (this procedure is significant when executing at an ATM or motivation behind sale).secondly In contact, promise you have in contact impelled on all your esteem based accounts(credit cards ,check cards et cetera) [2]. To ensure that you for the most part know when false activity occurs for you/s. Persistently Stand close to the ATM and use your body as a shield and extra security to guarantee your card and PIN. Do whatever it takes not to recognize help, heading or allow anyone to intrude with your trade as fraudsters here and there stance as bank powers by offering assistance or interfering with your trade. Simply insert the card when the ATM prompts you to do accordingly, it not there is a shot for the fraudsters stick ATM'S to make perplexity with customers.

Biometrics

Biometrics is very convenient, as they are not required to carry anything with a fear of its theft. No need to use human memories for the storage of passwords or PIN's [3] .with a fear of forgetting them and access denied to resources will never be faced by the user. They are for the most part utilized for confirmation, as it gives higher security. As the innovation is becoming quickly, yet in the meantime security splits and fakes in exchanges are likewise expanding world over. For safe and secure future, all agencies who are in need of security and safety have to adopt biometrics .They are reliable and robust, as the biometric identifier is technically more robust than ID cards, signature, PIN numbers, passwords, , etc. and they cannot be stolen, spied, delegated, proxyed, misplaced and therefore cannot be misused. Specially they are easy to maintain and it eliminates the gap for remembering the multiple passwords. As shown in figure 2 ,based on his or her physiological or behavioral characteristics biometrics refers to the automatic identification of a person, it operates in two modes

a. Identification (1: N): In endeavor to recognize an obscure individual it is an one to numerous correlation of the caught biometric against a biometric database confirmation.
b. Verification (1:1): In endeavor to recognize an obscure individual it is a coordinated

correlation of a caught biometric with a put away format to check that the individual is who he claims to be.

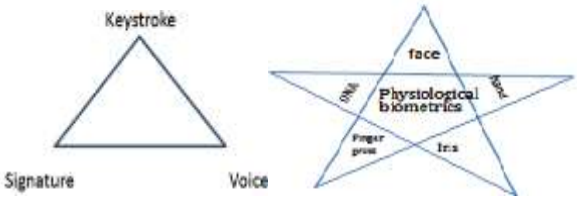

Figure2. Types of Biometrics (behavioral and physiological)

1.3 Multimodal biometrics (MMBS)

MMBS offer high degree of security, but they are far from perfect solution.

1.3.1 Fusion in Biometry. So as to join two or more biometric qualities, a technique called . "combination" is utilized[4] .As shown in figure 3 , the Combination in biometry alludes to the way toward consolidating two or more biometric modalities

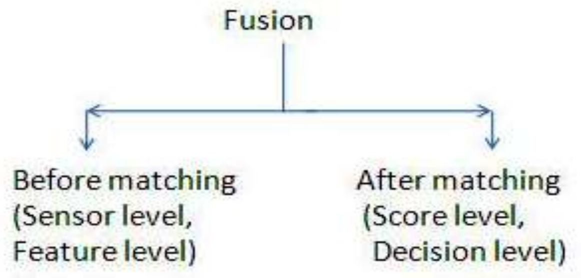
Fusion
Before matching (Sensor level, Feature level)
After matching (Score level, Decision level)

Figure 3. Fusion in MMBS

Fusion before matching: In this combination process is done before the matching process. It can be applied to both feature level and sensor level as per the requirement. In sensor fusion the best captured image can be taken in to account, as more than one sensor are used. In feature fusion, feature extraction is done using various techniques, it is very handful in practice both the methods in fusion before matching provide very impressive results.

Fusion after matching: Here fusion is [performed after the distances are generated. These methods are known as score level fusion and decision level fusions.

1.3.1. Level of Fusion.

There are Five levels of mix in multimodal structures were exhibited in the written work [5] which are the going with.

i) Sensor Level

Multisensory biometric frameworks test a similar instance of a biometric trait with two or more especially assorted sensors. Treatment of the diverse examples ought to be conceivable with one figuring or mix of estimations.

(ii) Feature Level

The highlight level mix is important in portrayal [6]. Particular segment vectors are combined, procured either with different sensors or by applying various component extraction estimations to a similar unrefined data

(iii) Decision Level

With this approach, each biometric subsystem finishes freely the techniques of highlight extraction, planning, and affirmation. Decision systems are for the most part of Boolean limits, where the affirmation yields the lion's share decision among each and every present subsystem [7].

(iv)Rank Level.

As opposed to using the entire design, distributions of the configuration are used. Positions from arrangement fragments are solidified to survey the mix rank for the request [8]. Rank level blend incorporates joining conspicuous verification positions obtained from different unimodal biometrics. It combines a rank that is used for settling on authority conclusion.

(v) Score Level.

It insinuates the mix of planning scores gave by the different systems. The score level mix systems are isolated into two key sets: settled rules (AND, OR, overwhelming part ,most extraordinary, minimum, aggregate, thing and calculating guidelines) and arranged models (weighted aggregate, weighted thing, fisher coordinate isolate, quadratic isolate, strategic backslide ,strengthen vector machine, multilayer perceptrons, and Bayesian classifier

1.3.2 Architecture of MMBS

There are two types.

a. Serial architecture
b. Parallel architecture

Serial design otherwise called course[9] , the handling of the modalities happens successively and the result of one methodology influences the preparing of the consequent modalities Ex: Bank ATMs.

In the parallel outline, diverse modalities work freely and their outcomes [10] are consolidated utilizing a fitting combination plan Ex: In military

2. LITERATURE SURVEY

Previously, the existing system is the most popular methods of keeping information and Accessing money from ATM centers but at present the need arises for the security of ATM cards and User ID/PIN protection. These schemes require the users to authenticate themselves by entering a "secret password" that they had previously created or were assigned. When ATM cards are lost or stolen, these systems are prone to hacking, either from an attempt to crack the password or from passwords which were not unique. A Biometric Identification system is one in which the user's body becomes the password/PIN. Biometric characteristics of an individual are unique and therefore can be used to authenticate a user's access to ATM centers. Previous methods of authentication in ATM centers are Unimodal Biometric methodologies.These Unimodal identification and verification systems are using single biometric characteristic. A new methodologies adding one more characteristic multimodal biometric characteristic is improved for authentication purpose. The table-1 below represents the literature survey of previous research based on multimodal biometrics using different fusion techniques for the purpose of security.

Table 1. Some literature survey of previous research based different fusion in different levels in MMBS.

Year	Modalities fused	Author(s)	Fusion level	Fusion approach	Performance in percentage
2004	Finger print+face	Kalyan et.al	Score+decision	Sum rule	58.33% correlation and sum rule
2005	Face+finger print	Snelick et.al	Match score	AND rule	Not calculated
2011	Face+palm print	Linin Shen[11]	Feature+Decision	FPCODE	FLF:91.52% DLF: 91.63%
2013	Face+Ear	S.M.S Islam[12]	Feature+score	L3DF, Ieterative closest point	FAR-0.001% Recognition:96.8%
2014	Face+Fingerprint+Iris	A.Annis Fathima et.al[13]	Sore+Dynamic decision	Weighterd average Fusion	Recognition: 78.5484 (Iris+face)=85 %

3.FORMATION OF THE PROBLEM AND METHODOLOGY

3.1 Objectives

1. To improve overall performance of the ATM system and achieve accuracy with minimized error rates using multimodal biometrics[12].
2. Multimodal Biometric ATMS solve the issues of multi factor authentication: Card+PIN+MMBS
3. Cardless authentication

3.2 Materials and methods

Database used for system is multimodal database CASIA for iris data base with training image of 756 iris images and testing images are 120. For finger print FVC (2004) testing images are 120. Our implementation is performed using Mat lab 7.0 on PC with 2.00GHz dual processor and 1.00 GB RAM. SYNOPSIS tool for high accuracy.

4. PROPOSED WORK

The proposed work below represents a flowchart in figure 4, which represents the sequence of operations to be performed. In figure 5 , it represents the block diagram of fusion at feature level and decision level.The fusion at feature level is performed using DCT-DHT and decision level fusion is done using XNOR-AND logic.

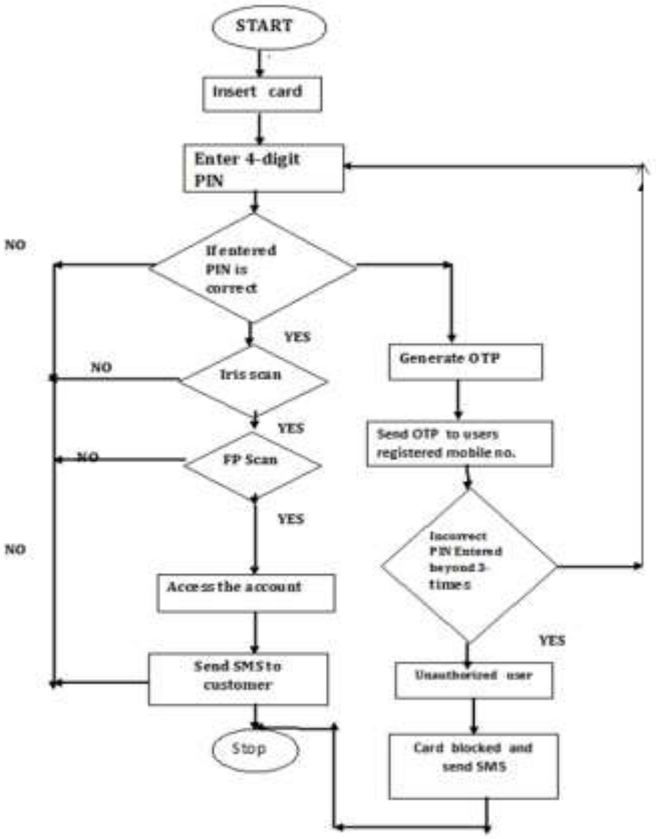

Figure 4. Flowchart of Proposed Work

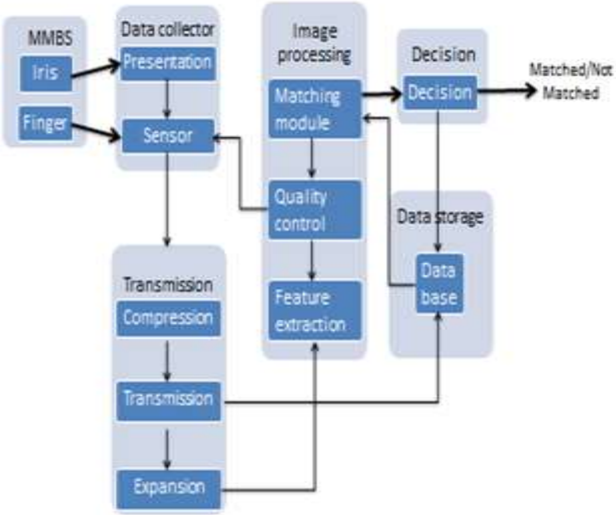

Figure 5.Block diagram of Fusion at feature level and decision level

4.1 Fingerprint recognition system using hybrid transform for ATM banking

1. 1. Picture obtaining is performed by catching the unique finger impression picture from client by a finger impression sensors.

2.Pre-preparing: In this stage the nature of caught picture is surveyed and checked .In the accompanying procedure fundamental attributes are removed. Unique mark pre-preparing states that a few operations are to be performed before extraction of the particulars.

3.Feature extractor: This is a significant stage as one needs to separate the correct elements in ideal way, Image or vector of the numbers with particular properties is utilized for making format. Half breed transform(DCT-DHT) are utilized for the component extraction.

4.Template Generator: Template is combination of related elements removed from source , components of biometric estimations those are not required for examination calculations are expelled in formats for lessening size or document and for ensuring personality of enrolee.

5. Put away Template: while the enrolment happens, layout gets put away in database or on card.

6.Matcher: And while coordinating procedure is performed , procured format gets passed on to person that is coordinating it with existing one, assessing separation between these two utilizing Euclidean Matching project assesses layout with info. This then turns into the yield for indicated reason. Unique mark coordinating is the procedure which depicts coordinating rate/score between two unique finger impression pictures.

4.2 Iris acknowledgment framework utilizing half breed change for ATM managing an account

1. Picture securing is performed by catching the iris picture from client by an iris scanner.

2. Preprocessing in this stage binarisation and finding the supplement of the paired picture is performed.

3. Iris division
    - Outer and inward iris limits confinement utilizing Daugman's integro-differential administrator
    - Occlusions evacuation utilizing Linear Hough Transform and thresholding

4. Iris locale standardization
    - Using Daugman's Rubber Sheet Model to change over iris picture from Cartesian facilitate framework to Polar framework

5. Iris acknowledgment is done through component extraction.
    - Feature extraction utilizing DCT-DHT

6. Coordinating
    - Using the Hamming Distance.

Choice level combination for both unique mark and iris is performed utilizing XNOR-AND.The combination for multimodal biometrics is performed both at highlight level and choice level for the change of security for maintaining a strategic distance from fraudulences in ATM administrations.

4.3 Feature extraction using DCT-DHT.

The 2-D DCT[14] expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. The cosine is more efficient than sine functions, whereas for differential equations the cosines express a particular choice of boundary conditions. DCT is a Fourier related transform similar to the Discrete Fourier Transform (DFT) using only real numbers[15,16].

The DCT eq (4.1) computes the ith and jth entry of the DCT of an image

D(i,j)=

$$1/\sqrt{2}(i)c(j)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}p(x,y)\cos[(2x+1)i\pi/2N]\cos[(2y+1)j\pi/2N] \quad (4.1)$$

$$C(u)=\begin{cases}\frac{1}{\sqrt{2}} & if\ u=0\\ 1 & if\ u>0\end{cases}$$

Discrete Hartley Transform (DHT)

Here we display another approach for picture pressure utilizing the Hartley change (HT) [6]. The Hartley change has the benefit of taking care of the issue of stage wrapping from which the Fourier change endures. The greatness and stage pressure utilizing this change (HT) have demonstrated preferable execution over those of the Fourier Transform. Extent and stage were handled independently. The quantization of recurrence tests in less bits has expanded the pressure proportion. Moreover, the disseminations used to produce the clamor fundamentally impact the outcome. The lossy pressure method utilized appears not to debase the picture quality. A nonlinear channel for smoothing the subsequent picture would be appropriate for picture upgrade. As a rule, the general pressure proportion is worthy it packs to around 82% the extent of the first picture. A lossless pressure strategy could be performed moreover to expand the pressure figure. Equations 4.2 represents the expression for Hartley transform and 4.3 represents the inverse of Hartley transform

$$H(k\ \Omega_v) = \frac{1}{\sqrt{N}}\sum_{n=0}^{N-1} h(nT)cas(k\Omega vnT) \quad (4.2)$$

The inverse DHT is

$$h(n\ T) = \frac{1}{\sqrt{N}}\sum_{n=0}^{N-1} H(k\Omega v)cas(k\Omega vnT) \quad (4.3)$$

The combination of gain based synthesis with Magma's Fixed Timing methodology enables fast implementation and analysis without sacrificing accuracy, and ensures delivery of a high-quality Physical Net list for predictable timing closure. Experiments have been conducted and results are tabulated in Table 2. It is observed from table that DHT+DCT is giving better area results because both individual transforms deal with real coefficients.

Table 2. For the comparison of delay, power, area for various transforms

Transform used	Delay after synthesis	Power Consumption	Area(*10mm^2)
DCT	100.34nsec	1000.44uw	1444
DFT	124.84nsec	1241.35uw	1681
DST	158.14nsec	1429.91uw	1812
DWT	192.16nsec	1863.12uw	2170
DHT	84.3nsec	600.85uw	1100
DHT+DCT	156.12nsec	44.1mw	1714
DHT+DFT	194.78nsec	68.1mw	2185
DHT+DST	243.18nsec	81.21mw	2843
DHT+DWT	309.12nsec	125.21mw	3233

4.4 2-Factor Authentication(2-FA)

The fuse of no less than two sorts of biometric affirmation structures meets obliging execution essentials, which are developed for the security-aware customers. In proposed structure, multimodal biometrics (MMBS) helps in improving the accuracy of the general system. in this paper the multimodal biometrics thought about is extraordinary stamp and iris biometrics of an affirmed individual and it gives a fundamental strategy for selection and check. Here Multimodal biometrics is with the mix of iris and one of a kind check and it is used to offer security to ATM organizations. It gives a prevalent security than other method and it is endorsed that it in like manner can be used for various applications. 2FA means Two Factor affirmation, security it is used to give two level of security. In multimodal system, if the assorted recording something about the body, for instance, biometric structure fails(this situation happens now and again) two level security makes one walk before , in that limit here, the checking for the truth(verification) code will be send to the customer convenient, which acts like a two phase checking truth in Gmail account. By then customer needs to enter the generous code and if the customer enters the honest to goodness code, he/she is allowed to get to the record. In case the PC hooligans endeavor to hack the record by endeavoring differing blend of checking for truth code, the record will be blasted if more than three attempts are made, this makes the system more secure. Furthermore, the multimodal and 2FA is used as a piece of cash machine structure (ATM)to improve the security level of the customer account by reckoning unapproved get to. Also it diminishes the False Reject Rate (FRR). Two Factor securities (2FA) is given, when all the recording something about the body structure misfires. In the 2FA security, the checking for truth code will be send to the customer compact number as sms (short message organization) or call. He needs to enter that checking code precisely to show his as affirmed customer and only three attempts are given and if the PC criminal endeavor to make sense of the code by endeavoring more than three attempts, that record will be darted and he/she can't prepared to get to the structure.

4.5 Performance factors

Performance factors commonly take the form of rates: for each factor, it is important to note that the measured / observed rate noted in any evaluation is distinct from the predicted / expected rate that occurs in biometric system.

Common performance factors include [17,18].

The false acceptance rate or FAR, is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user.

$$\text{FAR} = \frac{\text{Number of False Acceptance}}{\text{Total number of Attempts}}$$

$$\text{FRR} = \frac{\text{Number of False Rejection}}{\text{Total number of Attempts}}$$

The false recognition rate or FRR , is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. Where EER(Equal error rate)is FAR= FRR(equilibrium state)

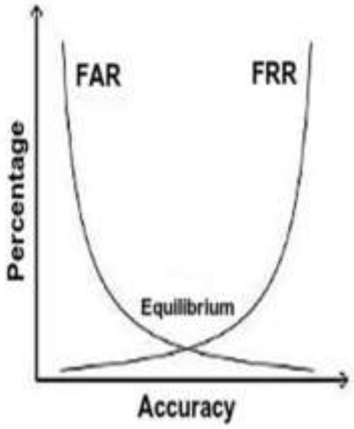

Figure 7. FAR and FRR equilibrium

5. EXPERIMENTAL RESULTS

In the following tables, the summary of the results are shown clearly, table 3 represents the comparison of ATM system with the proposed system. This represents basic difference between the proposed system and already existing system. Personal identification number , finger print processing , iris and one time password are the main features of the proposed system, which ensures the security for the bank customers.

Table 3. Comparison of ATM system

S. No.	Technique	Existing ATM system	Proposed ATM system
1.	PIN(Personal Identification Number)	✓	✓
2.	Fingerprint Processing	NA	✓
3.	Iris Processing	NA	✓
4.	OTP(One Time Password)	NA	✓

VI. CONCLUSION &FUTURE WORK

The experimentation of the work is here performed on various combination approaches and before applying combination, unimodal framework exhibitions are additionally broke down utilizing iris and unique finger impression databases [19,20]. In any multimodal biometrics framework the fundamental parameter to quantify the execution is figuring the FAR and FRR. This kind of verification framework gives security of bank client's cash, despite the fact that the preparing time may increment. Comparative procedure can be outlined by utilizing different other multimodal biometrics, with another technique which can supplant the proposed calculation with a superior calculation and which will give more exact and upgraded comes about. To deliver better outcomes propelled procedures can be utilized and general security can be enhanced up to expansive degree.

REFERENCES

1. *W.W.N.Wan, C.L.Luk, and C.W.C.Chow, "Customers Adoption of Banking Channels in HongKong", International Journal of bank Marketing, vol.23,no.3,pp.255-272,2005.*
2. *S.S, Das and J.Debbarma, "Designing a Biometric Strategy (fingerprint) measure for enhancing ATM security in Indian e-banking system", International Journal of Information and Communication Technology Research, vol.1, no.5, pp 197-203, 2011.*
3. *N.K.Ratha, J.H.Connell, and R.M.Bolle, " Enhancing Security and Privacy in Biometrics-based Authentication Sytems",IBM Sysems Journal,vol,40,no.3,pp.614-634,2001.*
4. *A. K. Jain and A. Ross, "Multibiometric systems," Communications of the ACM, vol. 47, no. 1, pp. 34–40, 2004.*
5. *J. Fierrez-Aguilar, J. Ortega-Garcia, and J. Gonzalez- Rodriguez, "Fusion strategies in multimodal biometric verification," in Proceedings of the IEEE Intetrnational Conference onMultimedia and Expo (ICME '03), pp. 5–8, 2003.*
6. *R. Brunelli and D. Falavigna, "Person identification using Multiple Cues," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 12, pp. 955-966, 1995*
7. *K. Veeramachaneni, L. Osadciw, A. Ross, and N. Srinivas, "Decision-Level Fusion Strategies for Correlated Biometric Classifiers," presented at the*

Computer Vision and Pattern Recognition Workshops, 2008. CVPRW'08. IEEE Computer Society Conference on, Anchorage, AK 2008. pp. 1-6.

8. *N. Radha and A. Kavitha, "Rank level fusion using fingerprint and iris biometrics," Indian Journal of Computer Science and Engineering, vol. 2, no. 6, pp. 917–923, 2012.*
9. *N. D. Kalka, J. Zuo, V. Dorairaj, N. A. Schmid, and B. Cukic, "Image Quality Assessment for Iris Biometric," in SPIE Conference on Biometric Technology for Human Identification III, 2006, pp. 61 020D–1–62 020D–11.*
10. *Snelick, R., Uludag, U., Mink, A., Indovina, M., and Jain, A.K.(2005), "Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems", IEEE Transactions on Pattern Analysis and Machine Intelligence,Vol.27, No. 3,pp450–455.*
11. *L. Shen, L. Bai, and Z. Ji, "FPCODE: An Efficient Approach for Multi-Modal Biometrics," International Journal of Pattern Recognition and Artificial Intelligence, vol. 25, no. 02, pp. 273-286, 2011.*
12. *S. M. Islam, R. Davies, M. Bennamoun, R. A. Owens, and A. S. Mian, "Multibiometric Human Recognition Using 3D Ear and Face Features," Pattern Recognition, vol. 46, no. 3, pp. 613-627, 2013.*
13. *A. A. Fathima, S. Vasuhi, N. N. Babu, V. Vaidehi, and T. M. Treesa, "Fusion Framework for Multimodal Biometric Person Authentication System," IAENG International Journal of Computer Science, vol. 41, no. 1, pp. 1-14, 2014.*
14. *S. Saha, "Image compression—from DCT to wavelets: a review", Crossroads, vol. 6, no. 3,* ***(2000)****, pp. 12-21.*
15. *P.John Paul , P.N.Girija, "A High Performance Novel Image Compression Technique using Hybrid Transform for Multimedia Applications" IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.4, April 2011.pp119-125.*
16. *H. B. Kekre, V. A. Bharadi , "Performance Comparison of DCT, FFT, WHT, Kekre"s Transform & Gabor Filter Based Feature Vectors for On-Line Signature Recognition", Int. Journal of Computer Application (IJCA), Special Issue for ACM Conf. ICWET 2011, February 2011*
17. *K. Sasidhar, V. L. Kakulapati, K. Ramakrishna, and K. K. Rao, "Multimodal biometric systems—study to improve accuracy and performance," International Journal of Computer Science and Engineering Survey, vol. 1, no. 2, pp. 54–60, 2010.*
18. *R. N. Kankrale and S. D. Sapkal, "Template level concatenation of iris and fingerprint in multimodal biometric identification systems," International Journal of Electronics, Communication& Soft Computing Science & Engineering, pp. 29–36, 2012.*
19. *CASIA Iris Image Database", http://www.sinobiomerics.com/Databases.htm,2007 Fingerprint Verification Competition (FVC) 2000, Available: http://bias.csr.unibo.it/fvc2000/databases.asp. [94]*