I J C T A, 9(34) 2016, pp. 551-563

An Enhanced Secured ATM System

B. Padhmavathi[1], P. Nirmal Kumar[2] and Sungkrityayan Khan[3*]

ABSTRACT

Generally, the ATM customer's identification systems depend only on debit and credit cards, pin numbers, and the identity validation methods in which calculations are not precisely accurate and incorporate individual procedures. For figuring out the glitches of conventionally existing ones, a novel ATM terminal apprehension system is designed to verify the fingerprint of the account holder . Finger Print Recognition System are used to verify the account number. The Face and IRIS are used for the input of amount and One-time password Generation . The propounded algorithm related to the fingerprint images, which has been improved and enhanced, increases the security during the usage of ATM machine. It increases the security during the usage of ATM Machine. The use of Face and IRIS for the purpose of customer verification is an entirely new approach.

***Keywords*:** Minutiae Extraction, Trivia, Biometrics, Iris Recognition, Fingerprint Substantiation, Recognition, Automated Teller Machine terminal, Thinning.

1. INTRODUCTION

Nowadays the financial crime rate has been increased frequently by illegal access of cards (such as debit/ credit). The financial crimers grab pin numbers by placing a duplicate keypad paper on top of the panel so that the user's pin numbers are easily grabbed/accessed by the crimers. Primarily, the current financial circle is solely focused on the customer, so as to identify the financial losses lead by ATM machine transaction. Security facility can be increased to safeguard the easy access to the ATM machines from the hands of the financial crimers. So, with the aim of fulfilling the objective of safeguarding the access, Fingerprint verification schemes, Recognition schemes and Biometrics, have been effectuated[1]. In the case of biometrics, the personality of any obscure persons can be resolved and rectified in the accompanying ways .i.e. though verification(or substantiation) and identification. Out of the two processes mentioned above, fingerprint verification plays an essential part in the forensic applications, criminal's examination, in distinguishing the terrorists, or any other security reasons. So, fingerprint verification has well established the fact, that it is a standout amongst the most dependable personal identification schemes. Biometrics refers to the process of accurately identifying an individual solely depending on his/her classifiable physiological (for example, retina, Fingerprint pattern, face etc.) or behavioral (e.g. pace, writing style, ATM, signature) characteristics. The techniques that have been incorporated into fingerprint substantiation stratagem includes minutiae-based approach and image-based stratagem[4]. Certainly, the methodology of the verification of fingerprints is inevitably dependent on this methodology, so additionally with hybridization, it is likewise helpful to the methodology of the verification of fingerprints, as because fingerprint identification adverts to the robotized or the automated strategy of confirming a match amongst two human fingerprints[5] . For example, let us assume the twins are using the same account, but even though they utilize the same account. their fingerprints (or the thumb impressions) will be different and unique in nature. In spite of that, the financial crimer inevitably tries to create a chaos or a mess with the ATM terminal in one or the other

[1] Asst. Prof., HoD, Department of CSE, SRM University, Chennai-26, India, *E-mail: padmas9169@yahoo.co.in*

[2] Assoc. Prof, Department of ECE, College of Engineering,Anna University, Chennai-25, India, *E-mail: nirmal2100@yahoo.co.in*

[3*] PG Student, SRM B-School, SRM University, Chennai-26, India, *E-mail: sungkrityayankhan@gmail.com*

way, i.e., by stealing user's credit or debit cards and their relevant passwords by illegal means. Let us assume if by mistake one's debit or credit card is misplaced and the password was stealthily procured by illicit means, so, eventually, the criminal will be able to transfer all the cash to their account in the most limited time[9] .

The prime concern of the current financial circle is concerned with as to how the valid identity can be related to the customer. So as a result, it becomes the essential concern in respect of biometric thumb impressions, which actually provides the essential recognizable evidence for any obscure individual. Therefore, hybridizing strategies in collaboration with fingerprint verification methodology, for ATM security are used[10]. Fingerprint has got unique characteristic elements, which doesn't get altered or modified in the entire life and varies from person to person. At the same time, they are very easy to utilize, implement and are available at a cheaper cost. In this way, fingerprint identification or verification is an efficacious way of personal verification strategy, which has been most generically employed as a meronym of correlation accompanied by the additionally available authentication or biometric datas[4]. In this specific paper, these two methods have been implemented. Sometimes if we only use the fingerprint recognition pattern in ATM Machine it leads to some drawbacks. Financial crimers capture the photo of your fingerprint, which is scanned using a scanner when your finger is kept on the glass surface. If an advertising box is placed over ATM Machine, which has a camera inside in it to observe the pin number. Eventually, the pin numbers of the numerous users accessing the atm can be easily encapsulated in a gadget with the assistance of the camera. So that the financial crimers can make duplicate cards, to access the ATM Machine. The Skimming device is capable of recording card details whereas the camera is used to record only the pin number. During the transaction process, sometimes the machine can hang, that is the control gets shifted to the financial crimers which help them to withdraw the user's amount, to their account. Recently, an unscrupulous attack happened at an ATM unscrupulous attack in which thieves utilized a particular type of a gadget to physically embed noxious programming into the machine, which might be a forewarning of more complex scams to come. The men utilized an electronic gadget, that was associated with a portable PC and embedded the gadget into the card acceptable slot on the ATMs. The electronic gadget appears to be an inflexible green circuit board that is more or less 4 or 5 times equivalent the length of ATM card[7].

Whenever a person enters a bank to access the bank account, which is registered in his/her name, through the help of ATM facilities installed in the bank, so it becomes inevitable to provide his/her pollex indentation because of the sake of protection , which plays an essential role. Under the minutiae-based methodology, fastest verification of fingerprints, as well as its execution, is also possible even in the case of two fingermark indentations having the same minutia, whereas they may not exactly possess the same ridgelines also. As because enough minutiae are not extracted, it may result in narrowing the fingerprint image range, which is why it results in decreasing the verification confidence. So as a result, even if the size of a fingerprint image, which is provided as input is minuscule in nature, more precise identification is conceivable[14]. The image of the fingerprint, that has to be provided as an input for the verification process is, basically a gray image having a lightness of 256. Whenever an image of a fingerprint (which is binary in nature), is procured from a gray image through the implementation of the binarization process, which in turn helps to maintain the reliable lightness of the ridges as well as the valley of the fingerprints including the ridges too, which gets ceased because of the result of finger pressure, wrinkles and sweat pores, getting connected[4].

Perhaps, the most advanced methodology of all the biometric advancements is the fingerprint validation technique, which has been exhaustively verified by different applications. Nevertheless, fingerprints are totally one of a kind to a sole person and remain perpetual and everlasting[6]. Hence as a reason, this particular methodology is considered reasonable for pollex impact on biometric at the whatsoever point of time deploying the ATM's. This selectiveness exhibits that fingerprint substantiation is to a greater extent exact and adept when compared with different stratagems, which are available for the purpose of

substantiation or verification. As of, fingerprints are presently being deployed as an invulnerable and captivating substantiation technique in numerous disciplines, incorporating budgetary or financial, sanative and whatever additionally entry controlled applications[2]. So, it can be easily inferred that fingerprints which are unique, are the most extensively implemented biometric characteristics for distinctively distinguishing and confirming in the domain of biometric validating proof. Fingerprints have two fundamental sorts of components i.e., ridge and minutiae, which are being utilized for automatically validating fingerprints.

In an existing typical biometric validation anatomy, the biometric layout is generally stored on the centralized server amidst enlistment, and once the customer's biometric pattern structure is scanned and encapsulated via the biometric gadget, then it is directed to the server, where the matching and processing strides are performed. This condition is the same like, upon entering the pin of the credit or the debit card to the ATM machine, the machine asks for the fingerprint of the respective individual, who has entered the pin of the relevant card. Whenever the details provided by the individual is validated correctly, then the machine displays a positive result else it displays a regret message as 'please attempt once more' or 'please try again'. Utilizing this framework, the unique fingerprint impressions are stored in a database whenever they open up a bank account[15]. As the fingerprints are discerned with the help of biometric machine by taking into consideration the False Rejection Rates (FRR), the fingerprints database test is coordinated in anticipation to the outstanding specimens of the same finger to reckon the False Acknowledgment Rate(FAR) and the False Rejection Rate (FRR). In order to reckon the False Acceptance Rate or FAR, each finger's first sample stored in the index or database, is equated or compared with the initial specimen of the left out fingers, so by utilizing all the above-mentioned processes we can restrict or restrain or stop the criminal activity, by which upon entering the duplicate code, will reject the request of drawing all the available currency in the ATM[11]. When the former case is considered, a person who needs to get himself identified or validated by the machine, proffers a claim , which is in turn, either taken up or declined by the machine. In the later case , an individual gets himself wrongly validated without an individual asserting to be validated or identified[8]. In general, human identification can be defined as the association or relationship of an identity with an individual. Conventionally, ATM pins, passwords, and identity cards are utilized for the purpose of identification to confine the access to these secured frameworks, yet these techniques can be easily infracted or breached, as because an ATM pin or a password can be easily speculated and identity cards can be very easily stolen , hence rendering them unreliable[2]. There is one important thing, which everyone has to ponder upon, is that the fingerprint recognition set-ups can be utilized and implemented solely for grown-ups or adults since the fingerprints of the infants cannot be efficaciously recognized[3]. The prevalent fingerprint recognition set-ups are acceptable for grown-ups solely (owing to the domain and resoluteness of the fingerprint detectors etc.)[2][8].

2. PROPOSED METHOD

It has been expounded precisely to empower individuals to dispatch packets substantial in comparison to a cell. The ATM interface segregates these sort of substantial packets, which in turn transmit the cells individually and reassembles them at another end. This specific layer is denoted by the term AAL whose expanded form stands for ATM adaptation layer. The additional secondary layer of the physical layer is entitled as the TC or Transmission Convergence secondary layer. When the cells are relayed, the TC secondary layers dispatches them as a streak of bits to the PMD layer. In this propounded approach of ATM paradigm, this two layers functionality with performance is present in the physical layer. The AAL layer is divaricated into an SAR, also known as Segmentation and reassembly secondary layer and a CS (also entitled as convergence) secondary layer. The nether the layer residing below the PMD layer divides the packets in the form of cells on the transference side and posits them back simultaneously at the destination. The top secondary layer engenders it plausible for ATM system to proffer distinctive services to the divergent

applications. The above points explain the interlink between machine and the main network server of the particular account details. The proposal for the propounded approach goes as follows:

2.1. Finger Print Recognition

Fingerprint uses biometrics where the biometric points residing in the finger is captured and is processed. Unique finger impression depends on details extractor for acknowledgment that depends on three essential strides:-

2.1. Image Pre-processing

In this specific juncture, the extraction and segmentation of fingerprint are executed. Additionally, the background noise is removed and performance of feature extraction is enhanced. Smoothing takes place. The limit is applied to the picture in a way by doling out the edge pixels which are indicated by "1" and all the left out pixels as "0", so the succeeding parallel picture is appropriate for procurement of highlights. The following steps are involved :-

2.1.1. Histogram Equalization

It starts with expansion of pixel value to increase the efficiency of the viewed information from the image.

2.1 2. Fast Fourier Transform

Fast Fourier Transformation just filters the ridges and furrows orientation frequency and enhances the image for binarization.

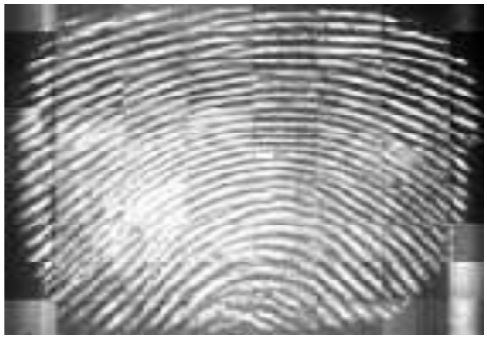

Figure 1: FFT Enhanced Image

2.1.3. Adaptive Binary Conversion

Image Binarization represents the 1-byte Gray image using binary format where 0 's assigned for ridges and 1's for furrows.

Figure 2: Binary Image

By the information attained from the binarization values, a two-dimensional array [X,Y] is formed. It also thins the ridges using the neighboring points.

2.2. Extraction of Minutiae

The withdrawal process or the process of procurement is executed by reducing the edges with the aim of meeting the objective that they are precisely single pixel wide. Henceforth, discovering minutia from the diminished picture becomes easy by reckoning up on neighbors at a juncture of interest in a (3*3) window. The Region of Interest(ROI) that is sequestered seems to be useful for each novel fingerprint image. Firstly, the area of the image lacking efficacious edges and crease or furrows are discarded, is disposed of as it just holds the basic foundation data (see Figure 3). Eventually, the remaining effective area's bound is outlined, as because the trivia in the effective region are very much perplexing with those feigned trivia that are engendered when the ridgelines are out of the detectors. So, for meeting the objectives of extracting or sequestering the ROI, the block direction approximation methodology have been implemented.

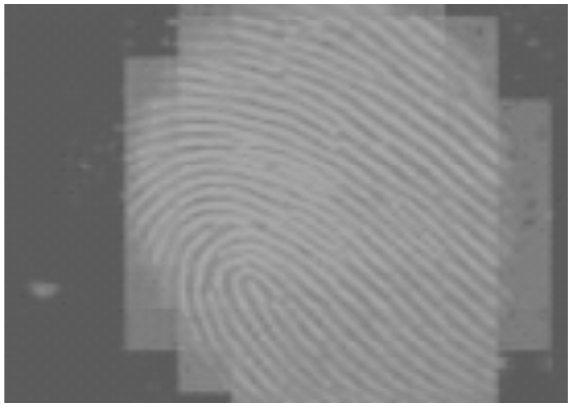

Figure 3: ROI Extracted Image

Trivia or Minutiae are nothing but the culminations and diverging point of the unique mark pictures. The Crossing Number, which is denoted as CN is the predominantly apprehended approach implemented by the majority, for particulars sequestration which incorporates the usage of the skeleton picture where the pattern of the flow of the ridge lines is eight-connected. Hence, by skimming the nearby locale of every edge pel in the ROI sequestered picture utilizing a 3x3window, the minutiae or the trivia are extricated (see Figure 4). At that point, the CN value is reckoned and registered, which is nothing but the summation of the contrast between the pairs of the proximate pixels existing in the eight-neighborhood. The pixels of the ridges can hence be relegated as edge completion, as well as bifurcation or non-bifurcation juncture by the attributes of the Crossing Number. For instance, a ridge pel accompanied by a Crossing Number having a value of one relates to a ridgeline closing, and a CN having a value of three relates to a bifurcation, whilst the assessed value of the CN equals to two then it represents the customary pixel of ridges.

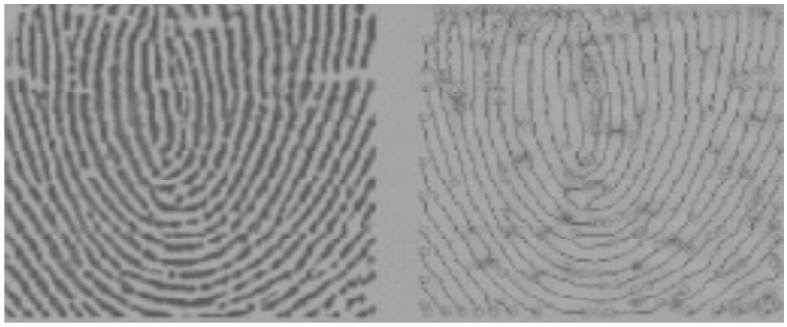

Figure 4: Minutia Extraction

Thinning can be defined as the process by which the thickness of each line of patterns can be reduced so that its width becomes to be a single pixel. It can also be defined as a structural operation that accumulatively splinters the contiguous pixels until and unless they are single pel wide. A customary thinning methodology accompanied by an algorithm has been implemented in this propounded approach, which executes the process of thinning incorporating two sub-iterations. The application of the above algorithm to a fingerprint image helps in maintaining or upholding the network of the ridgeline anatomies whilst imprinting a framework rendition of the twofold picture (see Figure 5). Eventually, this skeleton image is utilized for minutiae extraction.

The false minutia needs to be removed from the image when the preprocessing stage is over. For instance, false edge splinters due to the result of the deficiency in the assessment of ink and edge traverse inking are not completely wiped out. At the prior stages, some artifacts are rarely introduced, which eventually results in false minutia, which in turn will influence the precision of verification (see Figure 6). So the removal of false minutia from the image is crucial and essential to keep the fingerprint validation framework powerful.

Figure 5: Thinned Image

Minutiae are considered to be the ramifications and endings of the fingerprint images. The Crossing Number proposition is the widely accepted technique for the purpose of sequestration of minutiae which incorporates the implementation of the skeleton image where the pattern of the flow of the ridgelines is eight-associated. Hence, by examining the adjacent locale of each and every ridge pixel present in the picture by the implementation of a 3 x3window, the trivia are drawn out (see Figure 4). Subsequently, the CN value is estimated, which can be characterized as a large portion of the whole of the contrasts betwixt sets of locale pixels in the eight-neighborhood. The ridge pel or the pixels can eventually be delegated an edge closure, bifurcation or non-particulars juncture by the attributes of the CN. Let us consider for an instance, a ridge pixel, whose CN value is equal to one is equivalent to a ridge finishing, and a Crossing Number with a value of three relates to ramification or bifurcation, and whenever the CN is estimated to be two, subsequently it compares to a typical ridge pixel.

Thinning can be defined as the approach of lessening the depth of each and every line of arrangements or sequences to become a single pixel width. The approach of thinning can also be defined as a structural operation that in turn wears away the frontal area pixels, until and unless they become one pixel wide. The thinning algorithm executes the thinning manoeuvre utilizing dual sub-iterations. Whenever a thinning algorithm is applied to the image of a fingerprint, it helps in preserving the relatedness of the ridge frameworks whilst marshaling a skeleton variant of the binary image (see Figure 5). This skeleton image is utilized for eventual minutiae extraction. At the same time, false minutia also needs to be removed, when the preprocessing stage comes to a completion. For instance, false edge breaks because of an inadequate measure

of ink and edge traverse inking are not completely disposed of. At the prior stages, some artifacts are rarely introduced, which eventually results in false minutia, which in turn will influence the precision of verification (see Figure 6). So the removal of false minutia from the image is crucial and essential to keep the fingerprint validation framework powerful.

Figure 6: Remove H breaks and Remove spike

2.3. Steps to Remove False Minutia

1. Whenever the stretch betwixt one ramification or bifurcation and one conclusion is lesser in comparison to D and the two trivia happens to exist on the same ridge, then it is suggested to dispatch both of the minutiae. (D is the mean inter-ridge width amongst two collateral adjacent ridges).
2. Whenever the separation betwixt two ramifications or bifurcations is not as much as D or less than D and they are on the same ridge, then it is suggested to dispatch both of the ramifications or bifurcations.
3. If the two 'conclusions' or 'terminations' are happening to exist within the distance D and their guidelines are concomitant with a minimum variation in angle. In addition, they meet the problem in a way such that no other termination or conclusion is situated betwixt the two terminations. So as a result, the two terminations are considered to be fallacious minutia or trivia produced from a damaged or shattered ridge and hence, are disposed of.
4. If the two terminations are positioned in a brief ridge accompanied by a span significantly less than D, then two terminations are disposed of. (see Figure 7).

Figure 7: False Minutia Removal

2.4. Post Processing

It dispenses with spurious element focuses taking into account the basic and spatial connections of the details. At that point, accept the details focuses. So countless particulars get erased. This technique seems

to recognize the majority of genuine element focuses. What's more, the post-handling stage sifts through the undesired component focuses in light of their basic qualities. Among the most stunning qualities of unique mark acknowledgment, we can watch that: it has an abnormal state exactness, minimal effort in view of little size securing gadgets which make it generally utilized furthermore the less demanding method for distinguishing proof. Be that as it may, their shortcomings which may influence the acknowledgment of the unique finger impression: its relationship with criminological or criminal applications. Variables, for example, finger wounds or manual working can bring about positive clients being not able to utilize a unique finger impression based acknowledgment framework, either briefly or forever. Little range sensors may bring about fewer data accessible from a unique finger impression and/or inconsiderable cover betwixt various procurements.

The iris is an exclusive structure which endures being firm and steady until the end of matured life or adult life, which renders it to be extremely important as a biometric validation technique for figuring out individuals. The initial and a distinctive iris structure can probably be procured from a template image of the eye. The template image of the optical vision helps to easily procure the initial iris pattern from it. This biometric template incorporates a rendition of the initial facts preserved in the iris that could be contrasted accompanied by disparate templates. Image control or handling modus operandi are utilized to remodel iris paradigm to a distinctive code that can be preserved in a repository as well as it empowers juxtaposition betwixt the templates. Unique finger impression check is a brisk and proper strategy for setting up an idiosyncratic character amongst all the biometric procedures. Attributing to the many-sided quality of coordinating fingerprints and the gigantic measure of prevailing fingerprints customarily, unique fingerprint acceptance anatomy were customarily deployed as a part of scientific sciences, yet these days the notoriety of finger impression acceptance anatomy is very much predominant, just because of the regular citizen applications, namely, administering physical ingress to offices, administering legitimate ingress to programming, and administering voters amid races. An indispensable fragment in a unique fingerprint acceptance anatomy is the idiosyncratic finger impression coordinating estimation [6]. The natural properties of unique mark arrangement are surely known and fingerprints have been deployed for distinguishing proof impetus for an appreciable period of time.

The most critical stride in coordinating unique finger impression is to consequently extricate particulars from the information unique mark pictures. Be that as it may, the execution of a details extraction calculation depends profoundly on the nature of the info pictures. So as to guarantee that the execution of a programmed unique mark distinguishing proof/confirmation framework would be powerful as for the nature of the unique mark pictures we need to incorporate a unique finger impression upgrade calculation in the details extraction module. Fingerprint validation or identification arrangements were largely employed in forensic sciences, but, at the present scenario, the level of attractiveness of the fingerprint identification arrangements is principally anticipated to civilian applications such as managing or handling tangible usage of provisions, administering reasonable and rational usage of software, and also, managing voters during elections. An essential component in the fingerprint identification or validation arrangements is the fingerprint matching algorithm[6]. The natural characteristics of the fingerprint development are effectively comprehended and fingerprints have been employed for recognition impetuses for years and years.

The main stride in matching the fingerprint is to spontaneously draw out the trivia or minutiae of the fingerprint images that have been provided as an input. Nevertheless, the execution or the functioning of a minutiae deracination algorithm anticipates fully on the basis of the grade of the input images deeply. There is a need for inclusion of the fingerprint augmentation algorithm in the minutiae deracination module so as to ensure the robustness of the fingerprint validation system in relation to the fingerprint images.

2.4.1. Matching

The coordinating stage takes a list of capabilities and enlistment format as information and figures the closeness between them as far as a coordinating score. On the off chance that the coordinating score is higher when compared to the edge, then the choice is coordinated and the individual is perceived as certifiable. The coordinating procedure is finished as the particulars are matched.

2.4.1.1. Displaying the User Account Details: Once the fingerprint is recognized and is matched to the particular user, the system verifies it with the training patterns of the particular user. If the given pattern matches with the training pattern then the system displays the user account details. If the pattern recognition does not match then it just rejects the customer using the ATM system.

3. FACE RECOGNITION

One of the principal concern of face recognition system is feature extraction. Of the many feasible solutions available for the problem, the remarkably outstanding ones are those techniques which are mainly appearance-based, and usually, operates directly on the images or facial objects appearance and operates the image as 2D figures. Feature extraction is concerned with dimensionality reduction i.e. when the input data to be processed is very large and is assumed to be in surplus then it can be transmuted into a reduced feature set (feature vector) meeting certain attributes. The reduced features are assumed to hold pertinent information from the inputs provided. Discrete Curvelet and PCA8 are the broadly utilized systems which are being used for diminution of data and feature extraction in the appearance-based methodologies.

Feature extraction is a basic stride foremost to facial acknowledgment. Feature set extraction significantly improves the execution of facial acknowledgment framework. As the dimensionality of the pictures is unlimited, the quick utilization of pixel qualities like elements is outlandish.

During face recognition, it goes as follows:

1. Training: In the training phase, using discrete curvelet the input face is represented in the form of vector representation. in the vector representation, it generates an eigenvalue and is represented using eigen vectors.the value is stored in the database for the future reference.
2. Testing: During the testing phase,it involves accuracy rate and eigen values. the eigen values are compared with the accuracy rate and using PCA classifier the accurate image is recognized.

GIVING THE INPUT AMOUNT VALUE

Once the accuracy rate of face recognition is reached successfully, it redirects to the amount details wherein the user gives the required amount he needs to withdraw from the ATM.

4. IRIS RECOGNITION

The general procedure for procuring and putting away iris highlights with iris pictures can be recorded as take after :

1. Picture procurement: bring the photograph of iris with great determination and quality.
2. Division: handle the gaining picture for partition of iris from eye picture.
3. Standardization.
4. Highlighting deracination and highlighting the encoding process,
5. Touring separated ciphers in the database as well as contrasting obtaining iris pictures and ciphers in the database.

The creation of iris occurs in the 3rd month of the initial birth stage and distinctive shapes are marshaled throughout the first 12 months of existence. These specific patterns are randomly occurring and don't rely on genetic or hereditary aspect and the sole feature that would depend on genetics is the process of pigmentation. Iris arrangements possess a very low False Accept Rate (FAR) in comparison to additional biometric attributes or features}; the False Reject Rate (FRR) of the arrangements can be alternatively high. Iris identification analyzes attribute such as freckles, rings, and furrows which are in existence, in the colored tissue encircling the pupil. To transform iris patterns to a distinctive code, image processing techniques can be easily implemented. These converted codes can be stored in a repository, which will allow further comparisons between the templates.

4.1. Iris Pre-processing

The input image is given from the database. the image then undergoes a basic preprocessing step such as grayscale conversion where the given input image is converted into a single plane for easy processing.

4.2. IRIS Localization

Circle location calculation is utilized to expand the general rate of the framework (see Figure 8). Circle location is utilized in light of the accompanying:

1. It has great acknowledgment execution and pace.
2. The calculation can precisely recognize even mostly blocked circles.
3. The calculation needs a little measure of memory.

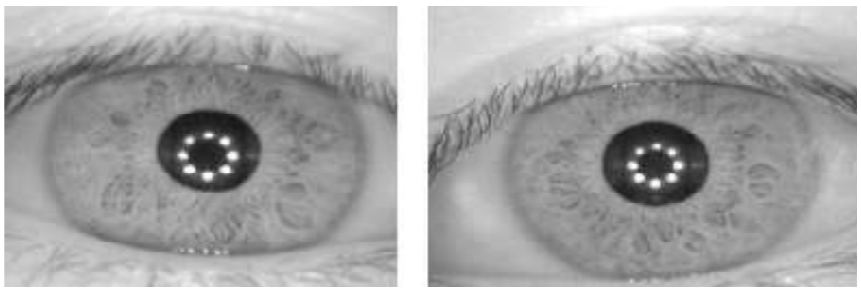

Figure 8: Iris Localization

4.3. Testing

4.3.1. IRIS Segmentation

In this process, firstly it involves utilization of the Canny Edge Detection methodology to create an edge map (see Figure 9). Subsequently, the image or the picture is processed so that the iris can be detached from the eye image.

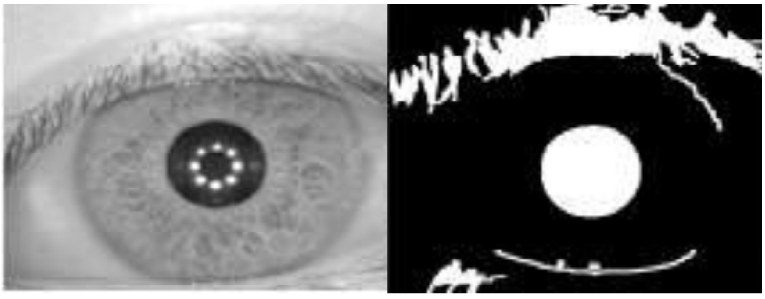

Figure 9: Iris Segmentation

4.3.2. IRIS Normalization

After the efficacious extraction of the iris part from the eye image, and by keeping in mind the end goal to permit correlations between various irises, change the separated iris locale with the goal that it has an altered measurement, and thus expelling the dimensional irregularities between eye pictures because of the extending of the iris brought on by the understudy enlargement from fluctuating levels of enlightenment. Along these lines, this standardization procedure will deliver irises with exactly similar altered measurements, so two photos for the same iris under various lighting ambience will have the same trademark highlights.

4.3.3. IRIS Feature Extraction and Matching

This is conceived as the uttermost essential part of an iris acknowledgment framework as well as it decides the framework's execution to an expansive degree. Iris acknowledgment creates the right culmination by removing components from the information pictures and coordinating these elements with familiar examples in the element database. Components are nothing but the credits removed to procure the one of a kind attributes from the picture. Highlights from the iris picture are extricated utilizing hamming separation calculation.

ONE TIME PASSWORD

Time-based One-time Password Algorithm (TOTP) is a technique that uses shared secret key at the particular time . It generates a 7 long bit code in the audio form.

5. RESULTS

The propounded approach has been implemented experimentally on the fingerprint images , each containing a size of 256*256 pixels, face recognition images of size 256*256 and iris database image having a size of 128*128 . The database incorporates data related to 20 people, of which each person has given 10 images of their finger ,10 images of their face, and 10 images of the iris. When each person is considered, 5 images have been employed in the training phase and 5 images have been utilized in the testing juncture. The experiment was executed in two levels, where, the initial level was executed using the fingerprints , face, and iris individually. The performance was evaluated on the following three things: false acceptance rate or else known as FAR, false rejection rate or else known as FRR, as well as accuracy.

FAR is the likelihood of invalid inputs which are mistakenly acknowledged. Whilst, False Rejection Rate is the likelihood for legitimate inputs which are inaccurately dismissed. Accuracy is the segment of genuine outcomes.

$$\text{FRR} = \frac{Number\ of\ \ falsely\ rejected\ images}{Total\ number\ of\ \ persons\ in\ the\ database}$$

$$\text{FAR} = \frac{Number\ of\ \ falsely\ accepted\ images}{Total\ number\ of\ \ persons\ out\ of\ \ the\ database}$$

$$\text{Accuracy} = \frac{Number\ of\ true\ positive + no.of\ \ true\ negative}{\begin{array}{c}Number\ of\ true\ positive + no\ of\ \ false\ positive + \\ no.of\ \ false\ negative + no.of\ \ true\ negative\end{array}}$$

Table I
Accuracy Results

	FAR (in %)	*FRR (in %)*	*Accuracy (in %)*
Fingerprint	4.38	12.95	91.31
Face	5.68	8.67	92.71
Iris	5.38	6.46	96.68
Proposed Model	0	2.8	98.89

6. CONCLUSION

The Biometrics is an exceptionally encouraging innovation, but difficulties are moderating or slowing down its improvement and usage. Unique fingerprint images, iris images, and facial images are chosen because of their prodigious or outstanding features. Presently, in substantiation and identification techniques, the blend for ownership (cards) and learning (pins) to have full ingress to Automated Teller Machines are being supplanted accompanied solely by biometrics. The three propounded biometric frameworks with and without implementing threshold rendered a precision of 98.89% which incorporates 0% FAR, as well as 2.8% FRR, and the completion time achieved are 20 as well as 30 seconds, separately. By these strides, an effective and safe validation framework which incorporates entirely the elements of ID and confirmation in Automated Teller Machines is brought out.

7. FUTURE ENHANCEMENTS

For the future enhancement during swiping the ATM cards, fingerprints can be included for increased security. During the Account creation process in the bank, the Account holder's fingerprint may be collected. This fingerprint can go through an Visual Cryptographic engine where this fingerprint is divided into Secret Shares by using Random Grid based Visual Cryptographic technique. One of these Secret shares can be embedded into the ATM Card and the other share can be saved in the Account holder's database. Later whenever User swipes the ATM card for money withdrawal, he may be prompted to give his Fingerprint biometric for Authentication. Thus swiped fingerprint again goes through Visual cryptographic engine and is verified. Hence the Authentic account holder is directed to the next phase of money transaction. During these phases too, the Face recognition and the Iris matching can very well be verified with the same Visual cryptographic engine efficiently.

REFERENCES

[1] R. Vinothkanna, A. Wahi, 2012. A Novel Approach for Extracting Fingerprint Features from Blurred Images

[2] Z.A.Jhat, A. H. Mir, S. Rubab, 2011. Personal Verification using Fingerprint Texture Feature

[3] M. Ezhilarasan, D. S.Kumar, S. Santhanakrishnan, S. Dhanabalan, A.Vinod, 2010. Person Identification Using Fingerprint by Hybridizing Core Point and Minutiae Features

[4] J.K. Kim, S.H. Chae, S. J. Lim, S. B. Pan A Study on the Performance Analysis of Hybrid Fingerprint Matching Methods [5].Rakesh Verma, Anuj Goel, 2011, Wavelet Application in Fingerprint Recognition

[5] M. VLAD, A.ANISIE, M. S. VLAD, 2012. Automatic identification technologies

[6] C. Kant, R. Nath Reducing Process-Time for Fingerprint Identification System

[7] J. P. Chaudhari, P.M. Patil, Y.P.Kosta, 2012. Singularity Points Detection in Fingerprint Images

[8] P.KRISHNAMURTHY, MR. M. M REDDDY, 2012. Implementation of ATM Security by Using Fingerprint Recognition and GSM

[9] M. Drahansky, E.Brezinova, D.Hejtmankova, F.Orsag, 2010. Fingerprint Recognition Influenced by Skin Diseases

[10] S. Bana, Dr. D. Kaur Fingerprint Recognition using Image Segmentation

[11] P. Lamon1, I. Nourbakhsh, B. Jensen, R. Siegwart Deriving and matching image fingerprint sequences for mobile robot localization.

[12] M. Dolezel, D.Hejtmankova, C. Busch, M.Drahansky, 2010. Segmentation Procedure for Fingerprint Area Detection in Image Based on Enhanced Gabor Filtering.

[13] A. Ross, J. Reisman, A.Jain, 2002. Fingerprint Matching Using Feature Space Correlation.

[14] M. Lourde R, D. Khosla, 2010. Fingerprint Identification in Biometric Security Systems.