GRD Journals | GRD Journal for Engineering | National Conference on Emerging Research Trend in Electrical and Electronics Engineering (ERTE'19) | May 2019
e-ISSN: 2455-5703

Enchanced Security ATM Transaction using Iris, Fingerprint, OTP Authentication

[1]Melinda Don Seemanthy [2]Aleena Mary Varghese [3]Rakesh T K [4]Aravind Menon [5]Sebin Jose
[1,2,3,4,5]Department of Computer Science Engineering
[1,2,3,4,5]Albertian Institute of Science Technology

Abstract

ATMs, they're a valuable extension of financial institution, and are viewed by customers as an essential part of consumer banking. Always available, always ready to provide a variety of transactions. Criminal acts against ATMs and their customers have always been a top concern. Additional surveillance cameras, electronic locks and other physical controls have been added to make the ATM a secure place for banking transactions. Over the past few years, criminals use skimming of device that captures the magnetic stripe and keypad information from ATM machines, gas pumps and retail and restaurant checkout devices. They are easily accessible skimming technology available off the Internet. This technology tool are hard to spot. Thus to overcome this attack we use the concept of biometric system. The accuracy of biometrics in identification is increasing its usage extensively. The method proposed in this paper focuses on how the money transaction in an ATM machine will be secured by providing personal identification, by analyzing biometrics like fingerprints and iris patterns which are known for their steadiness and diversity. Use of biometrics provides a paperless banking environment along with the smart ATM access. In this system the samples of the fingerprint and iris along with the registered mobile number of the customer needs to be collected and saved in the database by the banker .The actual operation of the system begins when the customer accesses the ATM to make a money transaction. The fingerprint or iris samples will be captured and matched. The system will distinguish between the real legitimate trait and fake self manufactured synthetic or reconstructed samples by comparing it with the samples saved in the database during enrollment. After finding valid samples the system generates a 6 digit code which is received by the customer on his/her registered mobile number.

Keyword- Biometrics, Fingerprint Matching, Image Quality, Iris Recognition

I. INTRODUCTION

In an ATM (Automated Teller Machine) the personal identification using biometrics are preferred over the traditional ATM identification involving passwords and PIN numbers due to its high reliability. Among the various types of biometrics used the fingerprint matching and iris recognition have gained more interest due to high accuracies in verifying an individual's identity. In the proposed system we replace the PIN number identification used in the traditional ATM by fingerprint identification which is done using a fingerprint module, iris recognition and OTP verification.

II. LITERATURE SURVEY

A. Secured ATM Transaction System using Micro- Controller

The ID cards used in the traditional systems may be lost or may be misused so replacing it by the biometric system is essential. Memorizing passwords or PINs and sharing them with our friends could be risky so OTP generation can avoid this overhead and help in achieving better and secured identification. Physiological Biometrics of fingerprint and iris used for authentication secured the transaction system. In many applications which are entrusted with private or secret information like safe locker system or banks, plastic ID cards or PINs used can be easily defeated, in that case a non- invasive and user friendly fool proof biometric system proves to be a convenient and secured option.

B. Enhanced Security for ATM Machine with OTP and Facial Recognition Features

The purpose of this paper is to reinforce security of the conventional ATM model. They have posited a new concept that enhances the overall experience, usability and convenience of the transaction at the ATM. Features like face recognition and One-Time Password (OTP) are used for the enhancement of security of accounts and privacy of users. Face recognition technology helps the machine to identify each and every user uniquely thus making face as a key. This model used principal component analysis for face recognition. This completely eliminates the chances of fraud due to theft and duplicity of the ATM cards. Moreover, the randomly generated OTP frees the user from remembering PINs as it itself acts as a PIN. The flaws in the face recognition technique have focused our attention to other biometrics like fingerprint and iris.

C. Image Quality Assessment for Fake Biometric Detection Application to Iris, Fingerprint and Face recognition

The authors proposed a fake detection method which was purely software based it was applied to multi-biometrics like fingerprint, iris and face to identify accesses which involved deception. This method was simple and could be used in real time. Here a single image was taken into account and features of image quality were calculated.

D. Efficient Biometric Iris Recognition using Hough Transform with Secret Key

The method in this paper which analyzed iris biometrics for identifying an individual proved to be very efficient. False accept and reject rates were used to signify the accuracy of the system. In this method Hough Transform performed feature separation and detection of lines, circles, ellipses etc. for an image.

E. A Secured Approach for Authentication System using Fingerprint and Iris

Proposed an approach which secured the authentication process by performing recognition of iris and fingerprint patterns along with the use of a RFID card reader.

F. ARM7 based Smart ATM Access and Security System using Fingerprint Recognition and GSM Technology

Developed an embedded system which was used for ATM transaction security .Here RFID card was used as input to the microcontroller also a GSM module was used to send messages to the card holder which included three options (yes, no, action). The system used Visual Basic 6.0 software in the Front End and Assembly language in the back end. To ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic is a significant problem in biometric authentication, which requires the development of new protection measures. In this paper, they present a novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts.

III. OVERVIEW OF PROPOSED SYSTEM

A. Problem Statement

To design a web based application for the users to provide enhanced security for ATM transaction.

IV. ARCHITECTURE OF THE PROPOSED SYSTEM

The proposed system consists of three modules:

1) Fingerprint Scanning
2) Iris Scanning
3) OTP Generation

A. Fingerprint Scanning

A fingerprint-based biometric system is essentially a pattern recognition system that recognizes a person by determining the authenticity of her fingerprint. Customer's identity using fingerprints was checked by capturing real time fingerprint images of individuals using the optical sensor of the fingerprint module and storing pixel images in bitmap format as real images during enrolment. During authentication both real and a fake user fingerprints were checked. The experiment was carried out for different users by enrolling their fingerprints and then verifying their identity. An identification system recognizes an individual

By searching the entire template database for a match. It conducts one-to-many comparisons to establish the identity of the individual. Nowadays, most civil and criminal AFIS accept live-scan digital images acquired by directly sensing the finger surface with an electronic fingerprint scanner.

V. LIVE SCAN SENSING

The most important part of a fingerprint scanner is the sensor (or sensing element), which is the component where the fingerprint image is formed.

Optical sensors. Frustrated Total Internal Reflection (FTIR) is the oldest and most used live-scan acquisition technique today. The finger touches the top side of a glass prism, but while the ridges enter in contact with the prism surface, the valleys remain at a certain distance (see Figure 1); the left side of the prism is illuminated through a diffused light. The light entering the prism is reflected at the valleys, and absorbed at the ridges. The lack of reflection allows the ridges to be discriminated from the valleys. The light rays exit from the right side of the prism and are focused through a lens onto a CCD or CMOS image sensor. In spite of a generally better image quality and the possibility of larger sensing areas, FTIR based devices cannot be miniaturized unlike other techniques like optical fibers.

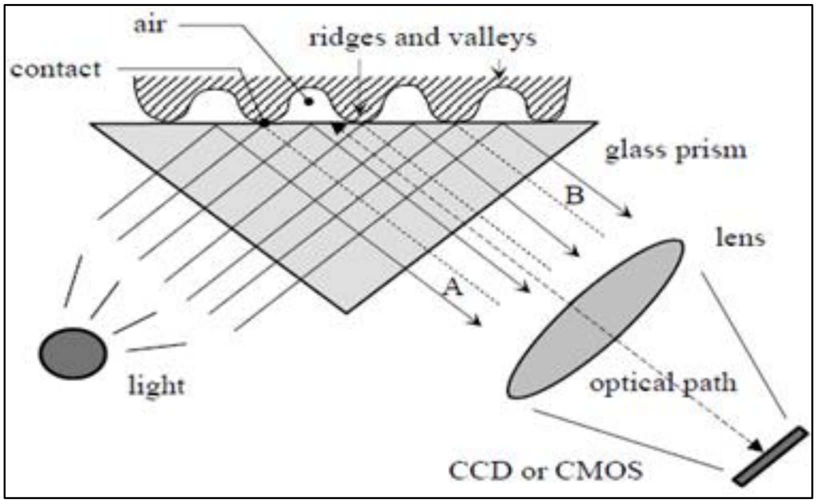

Fig. 1: Fingerprint-based verification system and an identification system

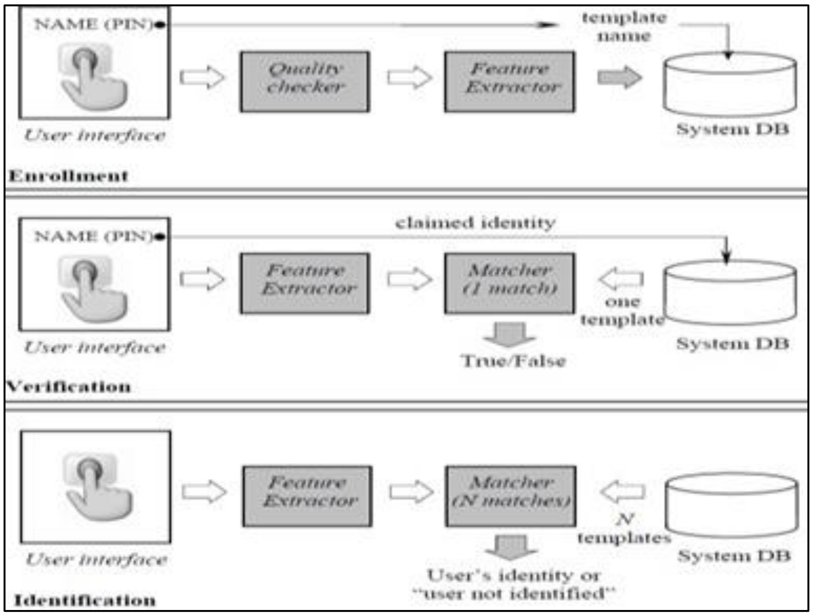

Fig. 2: Block diagrams of enrollment, verification and identification tasks

User enrollment, which is common to both tasks (see Figure 2); is also graphically illustrated. The enrollment module is responsible for registering individuals in the biometric system database (system DB). During the enrollment phase, the fingerprint of an individual is acquired by a fingerprint scanner to produce a raw digital representation. A quality check is generally performed to ensure that the acquired sample can be reliably processed by successive stages. In order to facilitate matching, the raw digital representation is usually further processed by a feature extractor to generate a compact but expressive representation, called a template. The verification task is responsible for verifying individuals at the point of access. During the operation phase, the biometric reader captures the fingerprint of the individual to be recognized and converts it to a digital format, which is further processed by the feature extractor to produce a compact digital representation. The resulting representation is fed to the feature matcher, which compares it against the template of a single user.

In the identification task, no PIN is provided and the system compares the representation of the input biometric against the templates of all the users in the system database; the output is either the identity of an enrolled user or an alert message such as "user not identified."

VI. FEATURE EXTRACTION

The first step in the feature extraction phase is to first place the fingerprint sample onto the device. The major points on the finger is then saved as an image in the device. After which this information is then send to the software, where it is encrypted [SHA 256][14] and stored. For sending the fingerprint sample from the device database to the desired software database a connection is to be setup between the device and the software. A fingerprint is the reproduction of a fingertip epidermis, produced when a finger is pressed against a smooth surface. The most evident structural characteristic of a fingerprint is a pattern of interleaved ridges and valleys (see Figure 3.a); in a fingerprint image, ridges (also called ridge lines) are dark whereas valleys are bright. When analyzed at the global level, the fingerprint pattern exhibits one or more regions where the ridge lines assume distinctive shapes called singularities or singular regions and may be classified into three typologies: loop, delta, and whorl (see Figure 3.b)

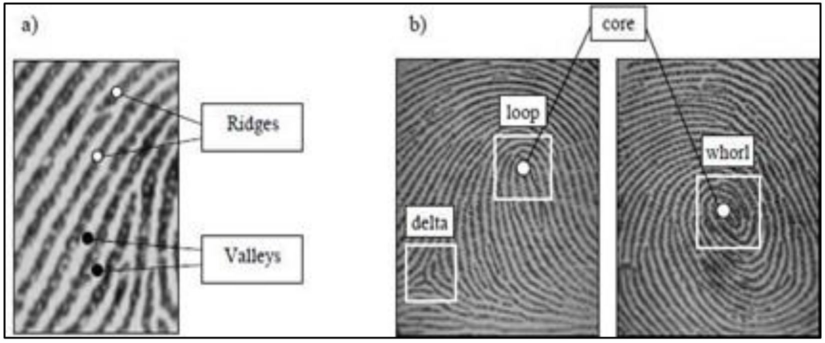

Fig. 3(a): Ridges and valleys on a fingerprint image Fig. 3(b): Singular regions and core points in - fingerprint images

Singular regions are commonly used for fingerprint classification that is, assigning a fingerprint to a class among a set of distinct classes, with the aim of simplifying search and retrieval.

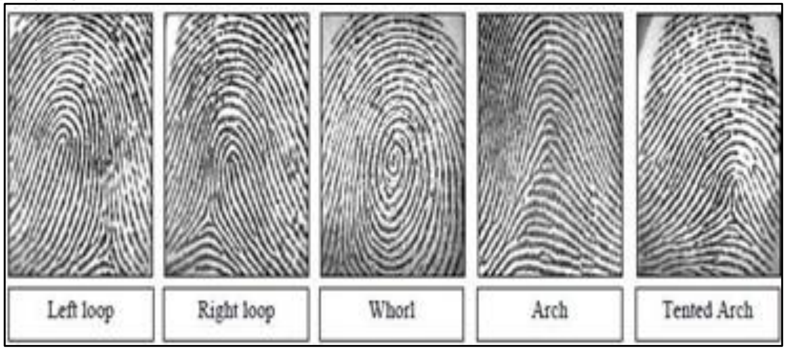

Fig. 4: One fingerprint from each of the five major classes

Most of the fingerprint recognition and classification algorithms require a feature extraction stage for identifying salient features. The features extracted from fingerprint images often have a direct physical counterpart (e.g., singularities or minutiae).

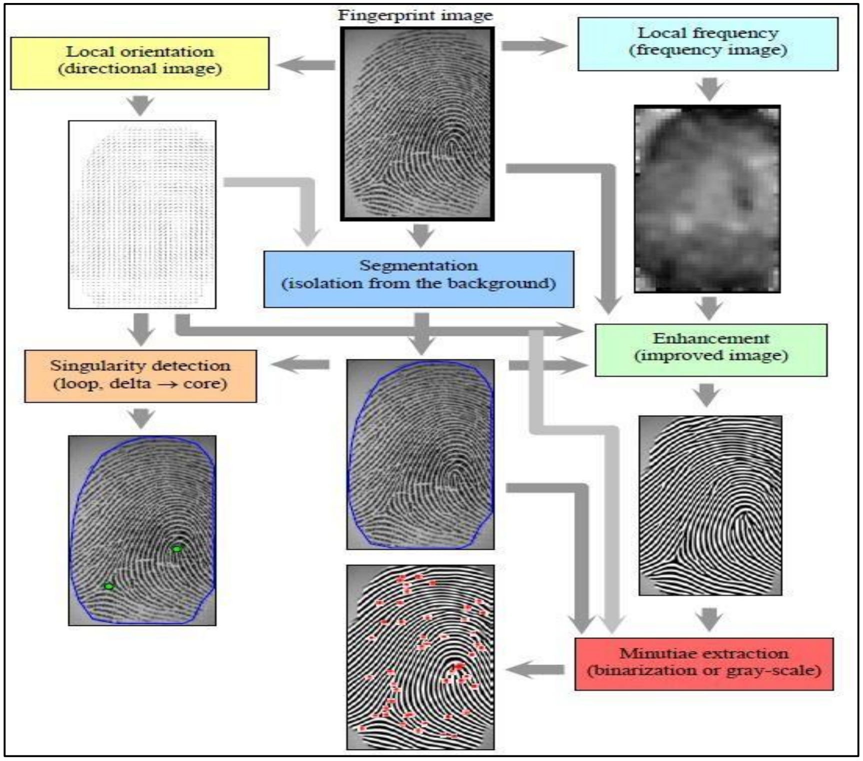
Fingerprint image
Local orientation (directional image)
Local frequency (frequency image)
Segmentation (isolation from the background)
Enhancement (improved image)
Singularity detection (loop, delta → core)
Minutiae extraction (binarization or gray-scale)

Fig. 5: Graphical representation of fingerprint - feature extraction steps and their interrelations

VII. SEGMENTATION

Separating the fingerprint area from the background is useful to avoid extraction of features in noisy areas of the fingerprint and background, uses circular Hough transform.

VIII. ENHANCEMENT AND BINARIZATION

The performance of minutiae extraction algorithms and other fingerprint recognition techniques relies heavily on the quality of the input fingerprint images. In an ideal fingerprint image, ridges and valleys alternate and flow in a locally constant direction. In such situations, the ridges can be easily detected and minutiae can be precisely located in the image.

The goal of an enhancement algorithm is to improve the clarity of the ridge structures in the recoverable regions and mark the unrecoverable regions as too noisy for further processing. Usually, the input of the enhancement algorithm is a gray-scale image. The output may either be a gray-scale or a binary image, depending on the algorithm.

Hong, Wan, and Jain [7] proposed an effective method based on Gabor filters. Gabor filters have both frequency-selective and orientation-selective properties and have optimal joint resolution in both spatial and frequency domains.

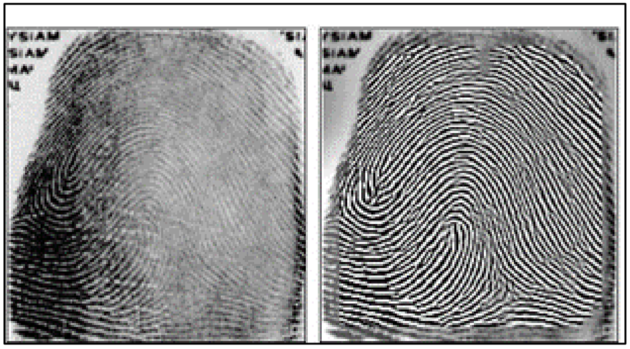

Fig. 6: Graphical representation of a bank of 24 Gabor filters and their application to the enhancement of a noisy image

IX. MINUTIAE EXTRACTION

Although rather different from one another, most of the proposed methods require the fingerprint gray-scale image to be converted into a binary image.The binary images obtained by the binarization process are usually submitted to a thinning stage [8] which allows for the ridge line thickness to be reduced to one pixel. Finally, a simple image scan allows the detection of pixels that correspond to minutiae through the pixel-wise computation of crossing number.

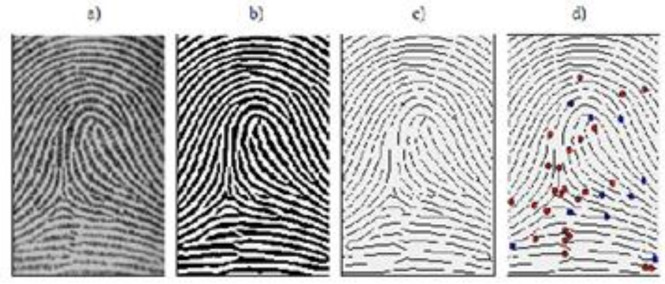

Fig. 14. a) A fingerprint gray-scale image; b) the image obtained after enhancement and binarization; c) the image obtained after thinning; d) termination and bifurcation minutiae detected through the pixel-wise computation of the crossing number.

Fig. 7

X. MATCHING

Matching high quality fingerprints with small intra-class variations is not difficult and every reasonable algorithm can do it. The real challenge is matching samples (sometimes very poor quality) affected by:

- Non-linear distortion.
- High displacement and/or rotation.
- Different pressure and skin condition.
- Feature extraction errors.

A. Iris Scanning

The three main stages of an iris recognition system are image pre-processing, feature extraction and template matching. The iris image needs to be pre-processed to obtain useful iris region. Image pre-processing is divided into three steps: iris localization, iris normalization and image enhancement.

Iris localization detects the inner and outer boundaries of iris. Eyelids and eyelashes that may cover the iris region are detected and removed. Iris normalization converts iris image from Cartesian coordinates to Polar coordinates. The normalized iris image is a rectangle image with angular resolution and radial resolution. The iris image has low contrast and non-uniform illumination caused by the position of the light source. All these factors can be compensated by the image enhancement algorithms.

Feature extraction uses texture analysis method to extract features from the normalized iris image. The significant features of the iris are extracted for accurate identification purpose. Template matching compares the user template with templates from the database using a matching metric. The matching metric will give a measure of similarity between two iris templates. It gives a range of values when comparing templates from the same iris, and another range of values when comparing templates from different irises. Finally, a decision of high confidence level is made to identify whether the user is an authentic or imposter.

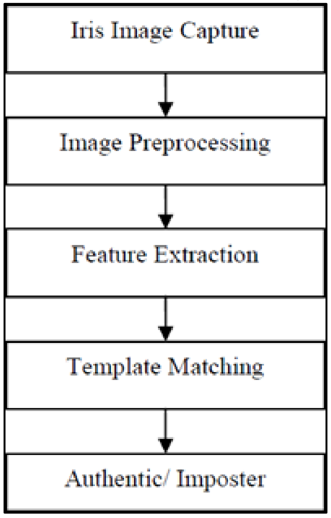

Fig. 8: Stages of Iris recognition algorithm

XI. IMAGE PRE-PROCESSING

Iris image pre-processing is divided into three steps: iris localization, iris normalization and image enhancement.

A. Iris Localization

Iris localization detects the inner and outer boundaries of the iris. Both the inner and outer iris boundaries can be approximately modeled as circles. The center of iris does not necessarily concentric with the center of pupil. Iris localization is important because correct iris region is needed to generate the templates for accurate matching. The method that we use here is Hough transform

1) Hough Transformation

Since the inner and outer boundaries of an iris can be modeled as circles, circular Hough transform is used to localize the iris [9]-[10]. Firstly, edge detector is applied to a gray scale iris image to generate the edge map. The edge map is obtained by calculating the first derivative of intensity values and thresholding the results. Gaussian filter is applied to smooth the image to select the proper scale of edge analysis. The voting procedure is realized using Hough transform in order to search for the desired contour from the edge map. Assuming a circle with center coordinate (xc,yc) and radius r, each edge point on the circle casts a vote in Hough space. The center coordinate and radius of the circle with maximum number of votes is defined as the contour of interest. For eyelids detection, the contour is defined using parabolic curve parameter instead of the circle parameter.

2) Eyelid and Eyelash Detection

Eyelids and eyelashes may cover the iris region. Eyelids can be detected using texture segmentation and Daubechies wavelets method. The eyelashes detection algorithms consist of Gabor filter, variance of intensity and combination of both edge and region information.

B. Iris Normalisation

Iris may be captured in different size with varying imaging distance. Due to illumination variations, the radial size of the pupil may change accordingly. The resulting deformation of the iris texture will affect the performance of subsequent feature extraction and matching stages. Therefore, the iris region needs to be normalized to compensate for these variations.

1) Daugman's Rubber Sheet Model

The centre of the pupil was considered as the reference point, and radial vectors pass through the iris region .A number of data points are selected along each radial line is defined as the radial resolution. The number of radial lines going around the iris region is defined as the angular resolution.

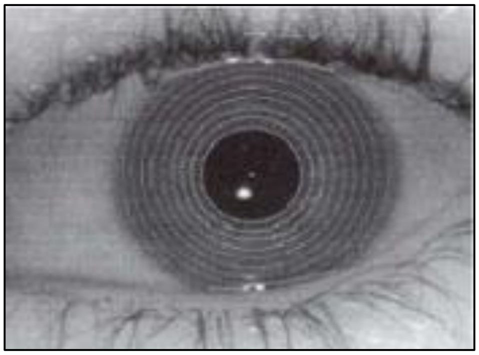

Fig. 9:

Normalisation produces a 2D array with horizontal dimensions of angular resolution and vertical dimensions of radial resolution. Rubber sheet model does not compensate for rotational inconsistencies.

C. Image Enhancement

The normalized iris image has low contrast and non-uniform illumination caused by the light source position. The image needs to be enhanced to compensate for these factors.

Local histogram analysis is applied to the normalized iris image to reduce the effect of non-uniform illumination and obtain well-distributed texture image.

Reflections regions are characterized by high intensity values close to 255. A simple thresholding operation can be used to remove the reflection noise.

XII. FEATURE EXTRACTION

In this stage, texture analysis methods are used to extract the significant features from the normalized iris image. The extracted features will be encoded to generate a biometric template.

A. Gabor Filters

2D Gabor filters are used to extract iris features. Gabor filter's impulse response is defined by a harmonic function multiplied by a Gaussian function. It provides optimum localization in both spatial and frequency domains.

Each pattern is demodulated to extract its phase information using quadrature 2D Gabor wavelets. The phase information is quantized into four quadrants in the complex plane. Each quadrant is represented with two bits phase information. Therefore, each pixel in the normalized image is demodulated into two bits code in the template.

The phase information is extracted because it provides the significant information within the image. It does not depend on extraneous factors, such as imaging contrast, illumination and camera gain. A Log Gabor filter which is Gaussian on a logarithmic scale is proposed by [11]. It has strictly band pass filter to remove the DC components caused by background brightness [12].

B. Template Matching

The templates generated from the feature extraction stage need a corresponding matching metric. The matching metric compares the similarity between the templates. A threshold is set to differentiate between intra-class and inter-class comparisons.

C. Hamming Distance

Hamming distance is defined as the fractional measure of dissimilarity between two binary templates. A value of zero would represent a perfect match. The two templates that are completely independent would give a Hamming distance near to 0.5. A threshold is set to decide the two templates are from the same person or different persons.

The fractional hamming distance is sum of the exclusive- OR between two templates over the total number of bits. Masking templates are used in the calculation to exclude the noise regions. Only those bits in the templates that correspond to '1' bit in the masking template will be used in the calculation.

The advantage of Hamming distance is fast matching speed because the templates are in binary format. The execution time for exclusive-OR comparison of two templates is approximately 10μs [13]. Hamming distance is suitable for comparisons of millions of template in large database.

D. Normlized Correlation

It is defined as the normalized similarity of corresponding points in the iris region. The correlations are performed over small blocks of pixels in four different spatial frequency bands. Normalized correlation accounts for local variations in image intensity. However, normalized correlation method is not computationally effective because images are used for comparisons.

XIII. ONE TIME PASSWORD

The one-time password (OTP) is type of password that is valid for only one use. It is a secure way to provide access to an application or perform a transaction only one time. The password becomes invalid after it has been used and cannot be used again. One Time Password is usually used for increasing security during online transactions. OTPs are widely used these days to increase security. In this project, we use a Random Java Class to generate One Time Passwords. By using Random class we can generate any number of digit of OTPs. The generated OTP is send to the registered mobile number of the user. Bulk SMS defined are of three types, normal SMS service, Transactional SMS service and Promotional SMS service. Normal SMS service has a low speed compared to other SMS services. Accuracy of normal SMS service is also very low. Transactional SMS are used to deliver important information and alert notifications like OTPs. Transactional SMS includes OTP are send within a limited time frame. The accuracy of this SMS service is high compared to normal or promotional SMS services. Promotional SMS includes push messages, advertisements, etc. The API integration is used to send OTP automatically (automation), SMS Gateway API must be simple, strong and easy to integrate.

REFERENCES

[1] Mrs.S.P.Balwir,Ms.K.Katole,Mr.R.D.Thakare,Mr.N.S.Pa nchbudhe,Mr. P.K.Balwir,"Secured ATM transaction system using micro-controller", International Journal of Advanced Research in computer science and software engineering, Vol.4,Issue 4,April 2014.

[2] Mohsin Karovaliya, Saifali Karedia, Sharad Oza, Dr.D.R.Kalbande, "Enhanced Security for ATM machine with OTP and facial recognition features",International Conference on Advanced Computing Technologies and Applications (ICATA-2015).

[3] Javier Galbally, Sebastien Marcel and Julian Fierrez, "Image Quality Assessment for Fake Biometric detection Application to Iris, Fingerprint and Face recognition", IEEE trans.on image processing, vol. 23,No.2 February 2014.

[4] Kriti Sharma, Hinanshu Monga, "Efficient Biometric Iris Recognition Using Hough Transform with Secret Key", International Journal of Advanced Research in Computer Science and Software Engineering.Vol.4,Issue 7, July 2014

[5] D.Shelkar Goud,Ishaq Md,P.J.Saritha, "A Secured Approach for Authentication system using fingerprint and iris", Global journal of Advanced Engineering Technology,Vol,Issue3-2012.

[6] Khatmode Ranjit P, Kulkarni Ramchandra V, "ARM7 Based Smart ATM Acess and Security System Using Fingerprint Recognition and GSM Technology", International Journal of Emerging Technology and Advanced Engineering Vol.4, Issue 2,Feb. 2014.

[7] Hong, L., Wan, Y., Jain, and A.K.: Fingerprint Image Enhancement: Algorithms and Performance Evaluation. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 8 (1998) 777−789.

[8] Lam, L., Lee, S.W., Suen, C.Y.Thinning Methodologies A Comprehensive Survey. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 14, no. 9 (1992) 869−885.

[9] R.P. Wildes (1997). "Iris Recognition: An Emerging Biometric Technology", Proceedings of the IEEE, vol.85, pp.1348-1363

[10] L.Ma, Y. Wang, and T. Tan (2002). "Iris recognition using circular symmetric filters", International Conference on Pattern Recognition, vol.2, pp.414-417.

[11] D. Field (1987). "Relations between the statistics of natural images and the response properties of cortical cells", Journal of the Optical Society of America.

[12] P. Yao, J. Li, X. Ye, Z. Zhuang, and B. Li (2006). "Iris Recognition Algorithm Using Modified Log-Gabor Filters", Proceedings of the 18th International Conference on Pattern Recognition.

[13] J. Daugman (2004). "How iris recognition works", IEEETrans. CSVT, vol. 14, no. 1, pp. 21 – 30.

[14] A.Arul Lawrence Selvakumar, C.Suresh Ganandhas." The Evaluation Report of SHA-256 Crypt Analysis Hash Function"2009 International Conference on Communication Software and Networks.