International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Special Issue 31(September, 2015), PP. 117-225

M-BANKING VERIFICATION USING OTP AND BIOMETRICS

P. S. Sakhare[1], D. Y. Chirayil[2]
[1]Department of Electronics & Telecommunication, Mumbai University, PHCET, Rasayni.
[2]Professor, Department of Electronics & Telecommunication, Mumbai University, PHCET, Rasayni.
[1]pritisakhare@ymail.com
[2]indiangold1@rediffmail.com

***Abstract*— Due to the fast development of information and communication technology (ICT), the modes of transaction in banking sector has been changed from on-side to remote and upgraded to telephone banking, and quickly entered into the era of online-banking. Currently, it has been moving towards the generation of M-banking (mobile banking).In order to provide the security M-banking has adopted, one-time password (OTP), smart card, user-defined password, as a remedy over the risk of stealing while M-banking is undertaken. The previous technologies used to send OTP's to the personal mobile phone, but now most smart mobile phones can easily perform M-banking. Thus, there is a higher risk to information security due to mobile phone hacking. The personal biometrics (finger, face and iris) have been adopted and combined with the OTP for the verification of M-banking. The server side then generates an client defined OTP message and transmit that to the mobile phone via internet. Now the user is supposed to enter the OTP received via a webpage of the M-banking system for the purpose of verification in order to gain authority to perform further transactions.**

***Keywords*— Multimodal biometrics, M-banking security, indexing schemes, biometric recognition systems with index codes.**

I. INTRODUCTION

With the advancement of large-scale networks (e.g., social networks, e-commerce, e-learning) and the growing concern for identity theft problems, the design of appropriate personal authentication systems is becoming most important. Usually, person authentication for applications like access control to a prohibited area, or for identification in different networks or social services scenarios, is done using biometric systems. A biometric system is defined as “a system which automatically distinguishes and recognizes a person as individual and unique through a combination of hardware and pattern recognition algorithms based on certain physiological or behavioral characteristics that are inherent to that person”[16]. Some of the physiological characteristics that are now used for biometric recognition include face, fingerprint, hand-geometry, ear, iris, retina, DNA, palm print, hand vein etc. Voice, gait, signature, keystroke dynamics defines the behavioral characteristics used in biometric recognition systems. Recently, soft biometric characteristics, such as, gender, weight, height, eye color, ethnicity, age, scar, marks, etc. have been started to be used in person recognition along with some physiological or behavioral characteristics. Any physiological or behavioral attribute can qualify for being a biometric trait unless it satisfies the criteria such as (i) universality : possessed by all humans, (ii) distinctiveness: discriminative amongst the population , (iii) Invariance :the selected biometric attribute must exhibit invariance against time,(iv) collectability: easily collectible in terms of acquisition, digitization and feature extraction from the population , (v) performance: pertains to the availability of resources and imposition of real constraints in terms of data collection and guarantee to achieve high accuracy,(vi) acceptability: willingness of population to submit that attribute to recognition system.

M-banking is next version of Internet banking. M-banking makes use of a mobile terminal to perform banking transactions. It combines currency electronisation and mobility to offer a new kind of banking service and allows people to perform many different kinds of banking service at anytime, anywhere. In adopting M-banking there are some advantages as follows:

- ✓ No restrictions in location: The user can perform banking activities at any time in any place.
- ✓ High penetration: The popular utilization of mobile phones provides a sufficient assurance of the growth and utilization of M-banking.
- ✓ Personalization: Each mobile phone is dedicated to a specified user. Therefore it increases the effectiveness of user authentication.

Existing system

M- banking verification scheme with OTP(one time password) and a single personal biometric trait(image/ video) provides better reliability as well as security. In this scheme, the user (client) can perform any query/browse/money transaction type of operation, simply by registering on the web page with their respective user ID & password [8]. The server then verifies client’s id & for correct id, server sends an OTP on user’s request for the transaction. When OTP is verified by the server, it requests the user to upload his biometrics. Finally the user gets access to start money transaction, if his respective uploaded biometrics are matched with those enrolled in the database. Using multimodal biometrics for M- banking -System can retain a high threshold recognition setting and system administrator can decide the level of security that is needed. Hence by using combination of multiple sources of information, systems improve matching performance, Increase population coverage.

The One-Time Password (OTP) system is a Two-Factor Authentication system in which the password constantly alternates whenever used. Due to which the risk of an unauthorized intruder gaining access to the account reduces to great extent. In OTP Password Generation it uses a hash function for the generation of password. The one-time password system works by starting with an initial seed, then generating passwords as many times as necessary [8]. The table mentioned below gives a comparison of various M-banking schemes along with the factors & functions they provide,

TABLE I
COMPARISON OF VARIOUS M-BANKING SCHEMES ALONG WITH THE FACTORS & FUNCTIONS.

Functions	M-Banking Scheme		
	Traditional OTP verification scheme	OTP and biometric(single biometric)verification scheme	Proposed OTP and multimodal biometrics verification scheme
OTP	Randomly generated	Randomly generated	Randomly generated
Webpage verification	Randomly generated	Randomly generated	Randomly generated
Password transfer via internet	Plain text	Ciphertext	Ciphertext
Biometric verification	No	Yes	Yes
Recognition performance	Poor	Moderate	Better

Indexing is the process of assigning a numerical value to a database entry, in order to facilitate its rapid retrieval. For example while indexing a fingerprint database it helps in reducing the search space and improves the response time of an identification system. In biometric identification systems, the identity of the input data is determined by comparing it with each and every entry of the database. This process increases the response time of the system and, potentially, the rate of identification. A method that narrows the list of potential identities will allow the input data to be matched against a smaller number of identities. We describe a method for indexing large-scale multimodal biometric databases based on the generation of an index code for each enrolled identity. An index code is built by computing match scores between a biometric input image over a fixed set of reference images. Depending upon the similarities between the index code of the input probe image and identities in the database, images are being retrieved.

II. PROPOSED VERIFICATION SCHEMES

A. Proposed work

The project main idea is based on Multi-factor authentication. The project has two main parts; registration and transaction. The registration page has the details like; name, address, phone number and assigning face, iris and finger images. The data is stored. The biometric data is multimodal. The fused matrix can be used for comparison. In translation, user will enter the ID, an OTP is generated. He will enter the OTP. Once OTP is correct, then the biometric identification is required. In this user should select the same images for finger, iris and face, which were assigned during registration [since we are not using hardware; we will select the images from the folder].The biometric data is compared with registered data. If matches, then the user will be allowed for further processing. The various algorithms for image comparisons are mentioned below.

For finger comparison, we are using morphological method. For face comparison, we are using the PCA algorithm and for iris comparison, we are using DCT (discrete cosine transform) based method. The flow of the project can be shown as below.

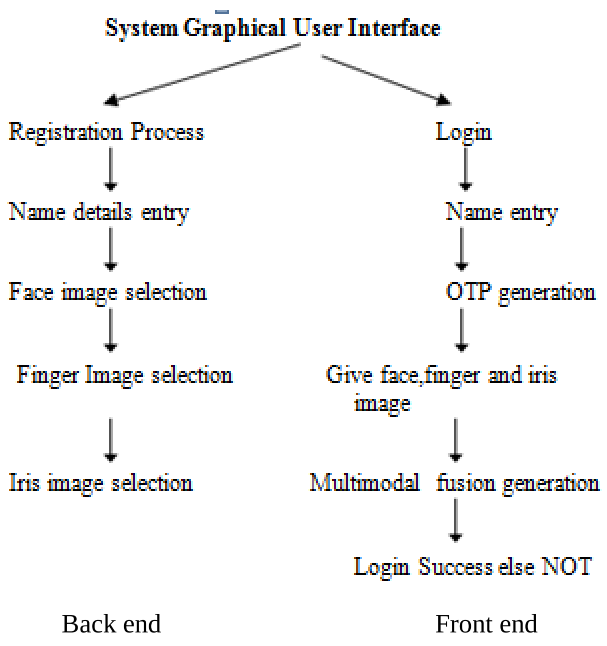


Fig. 1 Proposed system design flow.

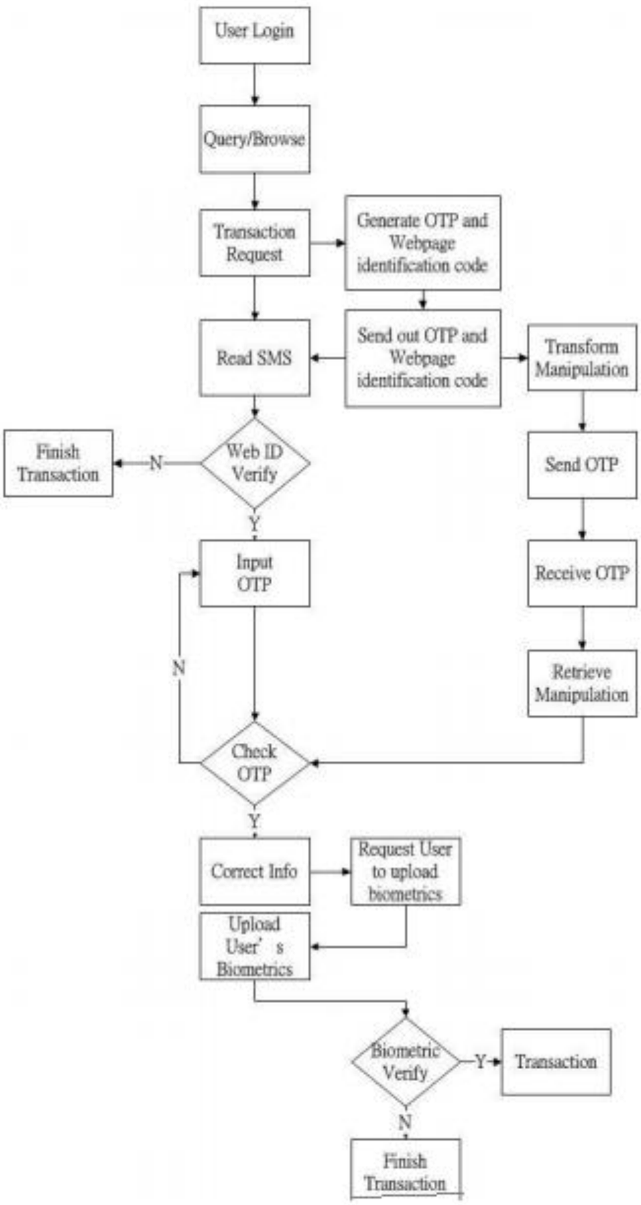


Fig. 2 Flowchart of proposed M-banking Scheme

B. Multimodal biometrics using indexing

We present a method for indexing multimodal biometric databases based on index codes generated by biometric matching algorithms. The indexing mechanism is executed separately for each modality and the results of each modality are combined into a final list of potential candidates[13]. A modality-specific index code is generated by matching an input image against these reference images, resulting in a set of match scores these are nothing but an index code of that image. During identification, the index code of the input image is compared to the index codes of the enrolled identities in order to find a set of potential matches from database.

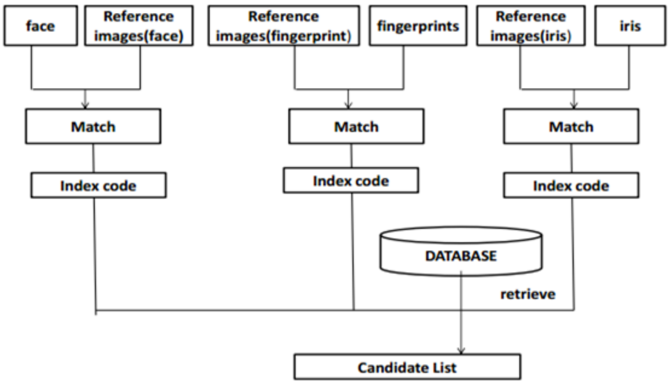


Fig. 3 Indexing three modalities.

1) *Indexing methodology*

The proposed system uses a small set of reference images are = {} That has good representation and dis-criminative power. The representational power ensures that there are a sufficient number of reference fingerprints, while the discriminating power ensures that these prints exhibit sufficient variants amongst themselves.

The index of an arbitrary image x is constructed in two steps. First, a set of match scores is computed by comparing x against the reference, $r_1, r_2, ... r_n$ in a fixed order. The result is the set $S_x(R) = \{s(x,r_1), s(x,r_2) ..... s(x,r_n)\}$ Where S () is the matching function. A discretize-tone function $D_b{:}R^n \rightarrow Z_b^n$ is used to transform S_x to an index code.

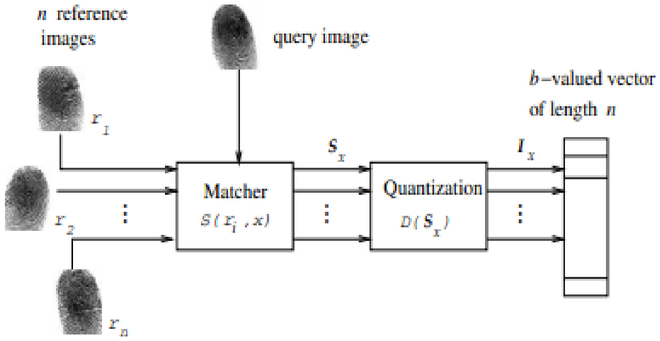


Fig. 4 Indexing scheme

In enrollment stage, the image associated with an identity is processed with the above procedure in order to generate its model index code. The model index code is stored in the database along with the identity of the associated print. During identification, when a query image is presented to the system, a Hamming distance-based search mechanism is invoked to retrieve only those in the database whose model index codes are probable candidates for a match

2) *Selecting reference images*

Images whose impostor match scores exhibit a large variance are selected as reference images. While the entire database of prints may be viewed as a candidate pool for selecting reference images.

3) *Creating Index Codes*

The index code for an arbitrary image x is computed as follows. The vector S_x is computed as $S_x = \{S_1^x, S_2^x \dots . S_n^x\}$ where $S_i^x = \{r_i, x\}$. Next, the index of $I_x = \{I_1^x, I_2^x \dots . I_n^x\}$ If x is generated by using a discretization function $D_b\ (S_x)$. The choice of, denoting the maximum number of output values of the discretization function, depends on the characteristics of the match scores generated by the matcher.

4) *Retrieving image from database*

Match score values may vary significantly depending on the quality of the images taken. The quality is impacted by the photometric and geometric variations in the images. This variation can cause the index code of a query image to be different from its corresponding model index code. However, the quantization function ensures that a majority of the individual elements constituting these two index codes is the same. During identification, when a potential list of candidate matches has to be determined, the Hamming distance can be used to find model index codes located in the neighborhood of the query index code. The size t of the neighborhood depends on the expected error rate between the query and model index cards and is estimated empirically. The following algorithm explains the search process for index codes.

Algorithm –

Let I_q be the index code of the query image and Ix_i be the index code of the image x_i from the database.

Compute the Hamming distances

$d_i = D_h\ (I_q, Ix_i)$ for $i = 1,2 \dots . M$.

Retrieve all x_i Such that $d_i\ <\ t$.

C. *Face recognition using PCA*

PCA is statistically dimensionality reduction method which produces optimal linear least square decompositions of the training set. In PCA based face recognition algorithm, the input is the training set $t1, t2, \dots \dots tN$ of N facial images. In computing the PCA representation, each image is constructed as point in $R^{n \times m}$ where each image is $n \times m$ pixels. PCA is a method of finding the optimal linear least square representation in $(N-1)$ dimensional space. There are total three modules in face recognition system.

1) *Normalization*

The first module normalizes the input image. This module transforms the facial image into a standard format that removes or attenuates variations that affect the recognition performance. Low pass filter (LPF) compresses the original image and removes high frequency noise. An image is compressed to save storage space and reduce transmission time. Geometric normalization places the face in standard geometric position by rotating, scaling, translating the center of eyes to standard locations [11]. This step removes the variation in size, orientation and location of the face, etc. the face, making block mask background pixels, hairs and clothes. The illumination normalization attenuates illumination variations among the images.

2) *Feature extraction*

This module performs PCA decomposition on the training set, which produces eigenvectors and eigenvalues.

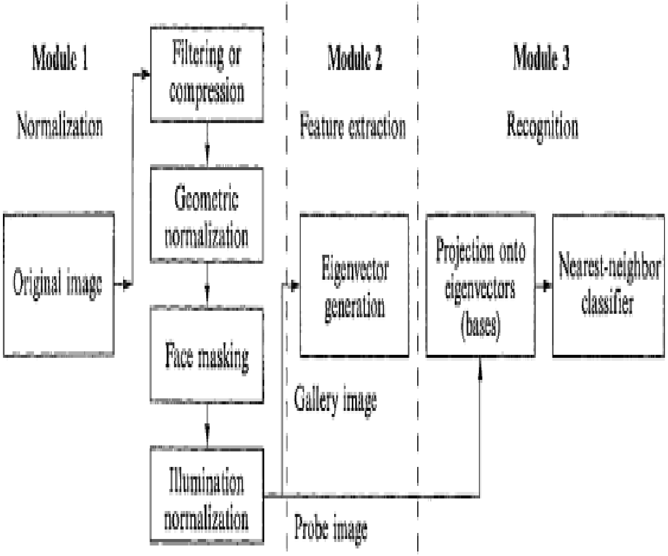


Fig. 5 Block diagram of PCA based face recognition system.

3) Recognition

This module identifies the face in normalized image. The first step projects image into face space while the second step identifies faces with a nearest neighbor classifier.

D. *Iris recognition using DCT*

The DCT is a real valued transform, which calculates a truncated Chebyshev series possessing well-known mini-max properties and can be implemented using the Discrete Fourier Transform (DFT). There are several variants out of which the most commonly used is that operates on a real sequence x_n of length N to produce coefficients C_k ,[14]

$$C_k = \frac{2}{N}\, w(k) \sum_{n=0}^{(N-1)} x_n \cos(\frac{2n+1}{2N}\ \pi k)$$

$$0 \le k \le (N-1)$$

Where, $$x_n = \sum_{k=0}^{(N-1)} w(k) C_k \cos(\frac{2n+1}{2N}\ \pi k)$$

$$0 \le n \le (N-1)$$

$$w(k) = \sqrt{2}$$

$$k = 0$$

$$w(k) = 1$$

$$1\ \le k\ \le (N-1)$$

1) Data collection

With the camera manually lined up and focused, a video sequence of several seconds duration is collected. Suitable images from the video sequence are selected in two stages. First, to evaluate focus and motion blur, the area of the specular reflection within the pupil is measured and images with light-areas greater than an experimentally set cutoff are removed. Specular reflection detection is carried out by searching for the largest positive change over a 5-pixel neighborhood for all rows in the analysis. In the second stage, the remaining images are normalized and tested for sharpness using a kurtosis measure of their 2D Fourier spectrum. The kurtosis is defined as the ratio of the fourth and squared second central moments. The images are sorted according to their kurtosis value in ascending order and 20 are accepted from the highest ranked images for each eye by manual inspection.

2) Image preprocessing

For coding, irises are extracted from the eye images and normalized to a standard format for feature extraction in order to remove variability introduced by pupil dilation, camera-to-eye distance, head tilt, and torsional eye rotation within its socket.

Localization

Location of the pupil and outer iris boundaries requires removal of the bright spot in the pupil caused due to the reflection of the infrared light source. This reduces the influence of high gray-level values of the gray scale distribution. Then, the image is scanned to isolate a region containing the pupil and iris. This is done by a heuristic method by making the assumption that the majority of image rows and columns passing through the pupil has large gray-level variance than those not passing through the pupil[12]. Also it is assumed that the pupil is circular and, because the pupil boundary is a distinct edge feature, a Hough transform is used to find the center and radius of the Pupil. In order to locate the outer boundary of the iris (limbus), a horizontal line through the pupil center is scanned for the jumps in gray level on either side of the pupil.

Normalization & Enhancement

Due to the dilation and constriction of the human pupil, there is variation in the radial size of the iris for different illumination conditions and in response to physiological factors. The resulting deformation of the iris texture is approximated as a linear deformation. Using the iris boundaries, we can map a rectangular image array back to an angular and radial position in the iris. This position will not, in general, map exactly onto a pixel in the source image, so the normalized gray value is obtained by bilinear interpolation from its four nearest neighbors. The gray levels are then adjusted by removing the peak illumination which were caused by light sources reflecting from the eye, estimating and subtracting the slowly varying background illumination, and equalizing the gray-level histogram of the iris image [12]. The final normalized image is of resolution 512 $\times$80, from which we code only the 48 rows nearest the pupil to mitigate the effect of the eyelids.

E. Fingerprint recognition using morphological methods

Fingerprint recognition is the process of comparing a fingerprint against another fingerprint to determine if the impressions are from the same finger. The system uses two types of minutia namely, termination and bifurcation for fingerprint matching. Termination defines the immediate end of a ridge; whereas, the term bifurcation refers to the point on the ridge from which two branches are derived.

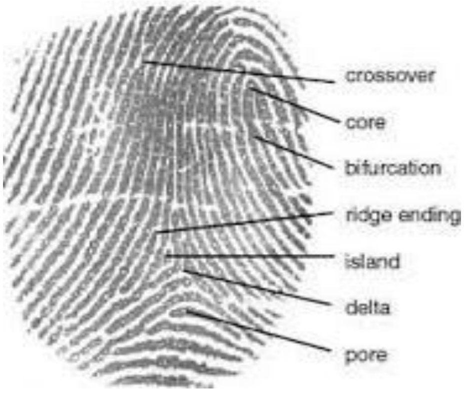


Fig. 6 Key minutia features.

1) Reading and enhancing the fingerprint images

The two fingerprint images to be matched are read and then image enhancement is applied on the two images[15]. Variations in skin can cause corruption of ridges and valleys. Also the other conditions like scars, humidity, dirt and non-uniform contact with the fingerprint capture device, may degrade the image quality. Hence, in order to increase the definition of ridges, the image enhancement technique is used to reduce the noise in the image and enhance the definition of ridges against valleys. For enhancing the fingerprint images, histogram equalization is used. It is a technique of improving the global contrast of an image by adjusting the intensity distribution on a histogram.

2) Fast Fourier Transform of the input images

The enhanced fingerprint image is divided into small processing blocks (32 x 32 pixels) and the Fourier transform is applied as:

$$F(u,v) = \sum_{X=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\exp\{-j2\pi\,(\frac{ux}{M}+\frac{vy}{N})\}$$

In order to enhance any specific block by its dominant frequencies, the FFT of the block is multiplied by its magnitude a set of times, according to the equation:

$$g(x,y) = F^{-1}\{F(u,v) * |F(u,v)|^{k}\}$$

Where $F^{-1}\{F(u,v)$ is inverse Fourier transform and $k = 0.4$.

Higher value of K improves the appearance of the ridges by filling up small holes in ridges. However, a high value of K can also result in false joining of ridges which might lead to a termination and became a bifurcation. The enhanced image after FFT has the improvements as some false broken points on ridges get connected and some spurious connections between ridges get removed. Now the enhanced images are converted into their binary version. Binarization is a process in which the 8-bit Gray image is transformed to a 1-bit image by assigning 0-value for ridges and 1-value for valleys. After the operation, ridges in the fingerprint are highlighted with black color while valleys are white.

3) Minutia marking and extraction

Fingerprint Ridge Thinning: Ridge Thinning is done to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. This is done using the Matlab's built in morphological thinning function. Bwmorph (binary Image,'thin', Inf). The thinned image is then filtered, again using Matlab's three morphological functions to remove some H breaks, isolated points and spikes , using the bump (binaryImage, 'break', k); bwmorph (binaryImage, 'clean', k) and bwmorph (binaryImage, 'spur', k).

Minutiae Marking: After the fingerprint ridge thinning, the next step is to mark minutia points. This can be implemented in three ways: for each 3x3 window, 1) if the central pixel is 1 and has exactly 3 one-value neighbors, then the central pixel is a ridge branch 2) if the central pixel is 1 and has only 1 one-value neighbor, then the central pixel is a ridge ending 3) the special case that a genuine branch is triple counted. Suppose both the uppermost pixel with value 1 and the rightmost pixel with value 1 have another neighbor outside the 3x3 window, so the two pixels will also be marked as branches.

False Minutiae Removal: This stage focuses on removing any false minutia, e.g., any false ridge breaks due to noise. For this purpose, the average inter-ridge width D is estimated at this stage. The average inter-ridge width refers to the average distance between two neighboring ridges and for each row it is given by:

$$\text{inter ridge distance} = \frac{\text{sum all pixel values with 1}}{\text{raw length}}$$

4) Minutiae matching

After minutiae extraction from the two fingerprint images, the next step is to match the Minutiae. For this purpose, an elastic string based iterative ridge alignment algorithm is used. In this algorithm first the minutiae's of two fingerprints are aligned and then the percentage of the matched minutia pairs are computed. In the alignment stage, the two fingerprint images to be matched are taken and any one minutia from each image is chosen. Then the similarity of the two ridges associated with the two referenced minutia points are calculated using the standard cross-correlation formula. If the similarity is larger than a threshold , each set of the minutia is transformed into a new coordination system whose origin is at the referenced point and the x-axis is coincident with the direction of the referenced point.

III. EXPERIMENTAL RESULTS

A. Performance measurements

The performance of the biometric system is considered by the decision made by a biometric system that is either a "genuine individual" type of decision or an "impostor" type of decision.

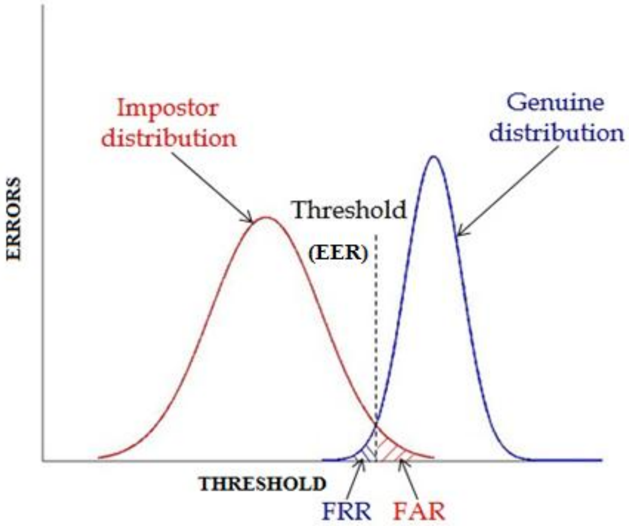


Fig. 7 Graph showing the measurement parameters of biometric systems.

False accept rate – FAR is defined as "the probability of an impostor being accepted as a genuine individual". That is, in a biometric authentication system, the FAR is computed as the rate of number of people is falsely accepted (false people are accepted) over the total number of enrolled people for a predefined threshold.

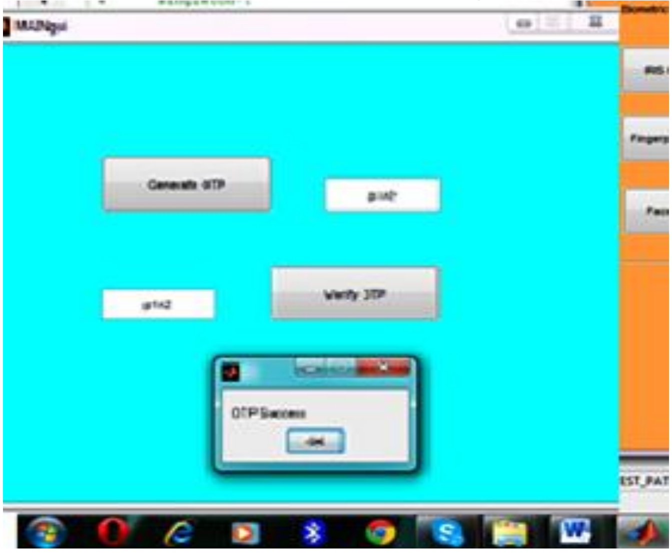
False reject rate - FRR is defined as "the probability of a genuine individual being rejected as an impostor". That is, in a biometric authentication system, the FRR is computed as the rate of number of people is falsely rejected (genuine people are rejected) over the total number of enrolled people for a predefined threshold.

Genuine Accept Rate – GAR is used to measure the accuracy of a biometric system. It is measured as the rate of number of people is genuinely accepted (genuine peoples are accepted) over the total number of enrolled people for a predefined threshold. Two other types of failures are also possible in a practical biometric system.

Failure-to-Enroll Rate - FTER is "the proportion of individuals who cannot be enrolled in the system". This error can occur if an individual cannot interact correctly with the biometric user interface or if the biometric samples of the individual are of very poor quality, thus the sensor or feature extractor may not be able to process these samples. The most commonly used plotting curves is the Receiver Operating Characteristics (ROC) curve, which is used mostly for biometric verification. ROC curves plot FAR against the corresponding FRR for any threshold.

B. OTP Generation

The result evaluation is designed by keeping in mind two objectives: OTP generation and then multi-biometric modalities recognition. The user when initiates these application, he will see the window, showing OTP generation and verification. The user must first send request from his mobile handset, to generate OTP. After receiving the OTP message he must enter that OTP for verification process. If the OTP matches with the received OTP, it shows the message, "OTP Success". Now the user can proceed further for verification of biometric modalities: iris, fingerprint and face.

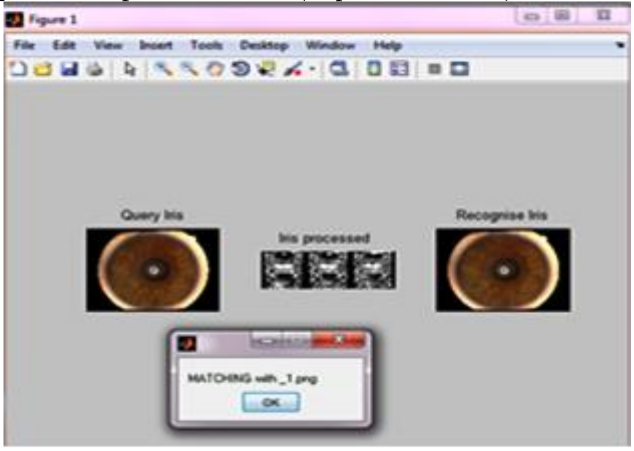


OTP Success

Fig. 7 OTP generation and verification.

C. Iris Recognition

Fig(8) shows, after successful OTP verification, the next window appears, which will allow user to select various biometric modalities(iris, fingerprint and face) from the database. Here for demo purpose, we are using the standard datasets for iris, fingerprint and face biometric modalities. The user must first verify his iris by clicking on "iris biometric modality". If this query image matches with the enrolled iris image of the user, it will proceed. The window will now show various performance parameters like hit rate, penetration rate and computation time for iris recognition process.

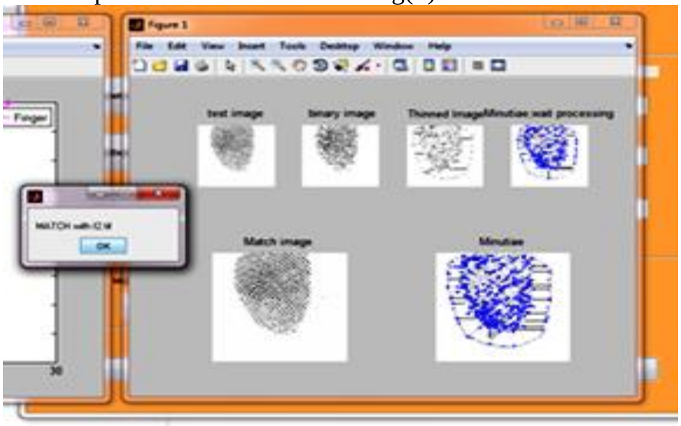


MATCHING with _1.png

Fig. 8 Iris Recognition.

D. Fingerprint Recognition

By clicking on "fingerprint biometric modality", the user is allowed to select the fingerprint query image from database. Then the window appears showing the matching process. Initially the query image(test image) is taken and is converted into binary form. This window shows the thinned image and the minutiae extraction. If the query image matches with the enrolled fingerprint image of the same user, it will show the message, for example as shown in fig(): "MATCH with 02.tif". As like iris recognition, fingerprint recognition performance is also calculated with three parameters: hit rate, penetration rate and computation time hit rate, penetration rate and computation time as shown in fig(9)



MATCH with 02.tif

Fig. 9 Fingerprint Recognition.

E. Face Recognition

In order to proceed, user must click on "face biometric modality". Now the user is supposed to select face query image from database. If the user has already enrolled his face modality, then the window will show message as "Matched image". Finally, all performance parameters will appear with their respective graphs.

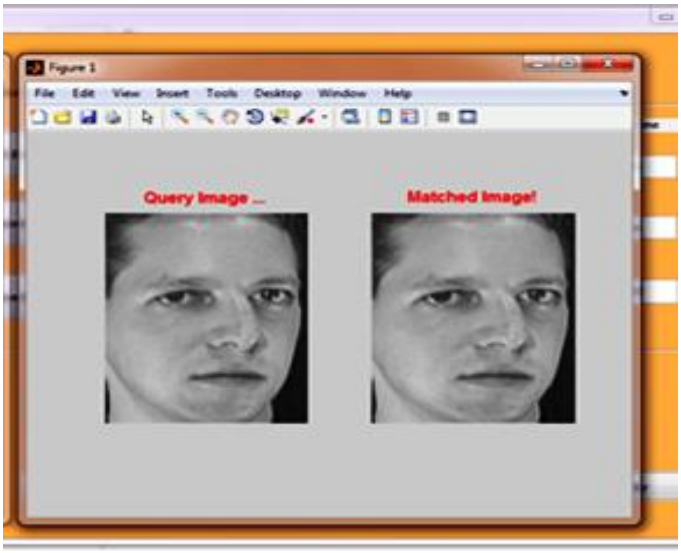
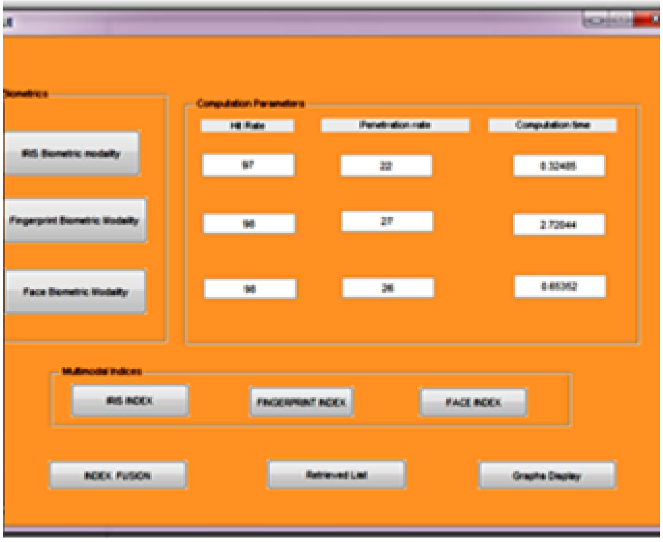


Fig. 10 Face Recognition.

For indexing the biometric modalities, user must click on respective pushbuttons (iris index, fingerprint index, face index).



	Hit Rate	Penetration rate	Computation time
IRIS Biometric modality	97	22	0.32485
Fingerprint Biometric Modality	98	27	2.72044
Face Biometric Modality	98	26	0.65352

Fig. 11 Performance parameters of all three modalities: iris, fingerprint and face.

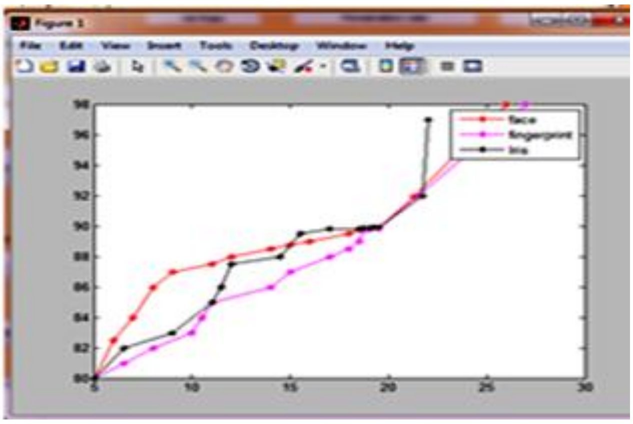


Fig. 12 Graphical display of performance parameters.

On Mat lab's command window, D1 will show iris index, D2 will show fingerprint index, D3 will show face index. Then by clicking on" Index Fusion" all three indices are fused together by using concatenation of iris index code technique. Finally the retrieved list is displayed on command window of matlab.

IV. CONCLUSION

This paper describes the security and Authentication for banking application system by using OTP and Biometrics System. In daily life, use of banking applications is increased gradually. The security of such type of online applications is more important. Current applications provide the security like security card, passwords for authenticating the user but do not provide more security for the users and are also not available for any emergency situations. In order to overcome the disadvantages of security cards, we used OTP and Biometrics for Authentication of finance application system.

REFERENCES

[1] K. Pousttchi, and M. Schurig, Assessment of Today's Mobile Banking Applications from the View of Customer Requirements, MPRA Paper No.2913,pp.1–11,2007,http://mpra.ub.uni muenchen.de/2913/1/MPRA_paper_2913.pdf

[2] J.A . Unar, Woo Chaw Seng, Almas Abbasi, "A review of biometric technology along with trends and prospects" Pattern Recognition 47 (5 February 2014) 2673– 2688

[3] Maria De Marsico, Chiara Galdi, Michele Nappi, Daniel Riccio " FIRME: Face and Iris Recognition for Mobile Engagement" Original Research Article Image and Vision Computing, Volume 32, Issue 12, December 2014, Pages 1161-1172.

[4] P. S. Sanjekar, J. B. Patil "AN OVERVIEW OF MULTIMODAL BIOMETRICS" Signal & Image Processing : An International Journal Vol.4, No.1, February 2013

[5] A. Kahate, Cryptography and Network Security, 2nd Edition, McGraw-Hill, 2008, http://highered.mcgraw-hill.com/sites/0070648239/information_center_view0

[6] RSA Laboratories, "Cryptographic token interface standard," PKCS, vol. 2.3, no. 11, RSA Security Inc., 2009.

[7] J. K. Y. Ng, "Ubiquitous healthcare: Healthcare systems and applications enabled by mobile and wireless technologies," J. Converg., vol. 3, no. 2, pp. 15–20, June 2012.

[8] Chang-Lung Tsai; Chun-Jung Chen; Deng-Jie Zhuang "Secure OTP and Biometric Verification Scheme for Mobile Banking" Mobile, Ubiquitous, and Intelligent Computing (MUSIC), 2012 Third FTRA International Conference on DOI: 10.1109/MUSIC.2012.31 Publication Year: 2012 Page(s): 138 – 141 IEEE Conference Publications.

[9] "A Novel Serial Multimodal Biometrics Framework Based on Semisupervised Learning Techniques"Qing Zhang ; Yilong Yin ; De-Chuan Zhan ; Jingliang Peng .Information Forensics and Security, IEEE Transactions on Volume: 9, Issue: 10 DOI: 10.1109/TIFS.2014.2346703 Year: 2014 , (1681- 1694).

[10] "A coding scheme for indexing multimodal biometric databases " Gyaourova, A. ; Ross, A. Computer Vision and Pattern Recognition Workshops, 2009. CVPR Workshops 2009. IEEE Computer Society Conference on DOI: 10.1109/CVPRW.2009.5204311 Publication Year: 2009 , Page(s): 93- 98 .

[11] Ghinea, G. ; Kannan, R. ; Kannaiyan, S. "Gradient-Orientation-Based PCA Subspace for Novel Face Recognition" Access, IEEE, Volume : 2 DOI: 10.1109/ ACCESS.2014.2348018 Publication Year: 2014 , Page(s): 914- 920.

[12] Donald M. Monro, Soumyadip Rakshit, Dexin Zhang "DCT-Based Iris Recognition" IEEE TRANSACTIONS ON PATTERN ANALYSIS

AND MACHINE INTELLIGENCE, VOL. 29, NO. 4, APRIL 2007. Page(s): 586 – 595

[13] Gyaourova, A.; Ross, A. "Index Codes for Multibiometric Pattern Retrieval" Information Forensics and Security, IEEE Transactions on Volume: 7, Issue:2 DOI: 10.1109/TIFS.2011.2172429 Publication Year: 2012 Page(s): 518-529 Referenced in: Biometrics Compendium, IEEE .

[14] Galbally, J.; Marcel, S.; Fierrez, J. "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition" Image Processing, IEEE Transactions on Volume: 23 , Issue: 2 DOI: 10.1109/TIP.2013.2292332 Publication Year: 2014 Referenced in: Biometrics Compendium, IEEE .

[15] Sankaran, A. ; Vatsa, M. ; Singh, R. "Latent fingerprint matching: A survey" Access, IEEE Volume:2 DOI: 10.1109/ACCESS.2014.2349879 Publication Year: 2014 , Page(s): 982- 1004 Referenced in: Biometrics Compendium, IEEE

[16] Mobile Banking, http://en.wikipedia.org/wiki/Mobile_banking, Accessed on 30 January 2012.