E-Voting System using Multimode Bio-Metric Analysis for Authentication

Tejasvee Pawar
M.Tech Student, Computer Engineering Department
MPSTME, SVKM's NMIMS University
Mumbai, India

Alpa Reshamwala
Assistance Professor, Computer Engineering Department
MPSTME, SVKM's NMIMS University
Mumbai, India

ABSTRACT

In many countries like India Voting takes places in the form of electronic voting and paper based voting. The proposed system is an extension of the Electronic voting. It has major advantage by using multimode biometric analysis to identify a correct individual. As there are many problems related to unimodal biometric system, such as noisy sensor data, non-universality, lack of individuality, non-availability of invariant representations. To solve this problems we will use multimode biometric system. For this purpose, multimode biometric system will take input of two biometric trait and fuse together the biometric sample. There are many possible combinations for fusion such as Hand Geometry and IRIS pattern, fusion hand geometry and palm print, fusion of face and palm print, etc. In this paper we are taking fusion of hand geometry and iris pattern by considering the problem of non-universality. .

General Terms

E-voting system. Biometric authorization, Fusion of multiple biometric traits

Keywords

SMARESIM, Fusion, unimodal biometric system, Multimode biometric system

1. INTRODUCTION

In many countries like India voting takes place manually where voters cast their votes and select a candidate of their choice. In this process there are many limitations such as counting mistakes of votes, also as the verification of voter is done manually there are a lot of possibilities of illegal voting. In villages where most of the people are uneducated are being misused by the others who do bogus voting in their name. So to avoid this illegal voting here we are making use biometric authentication system, by using which we can have legal, efficient, simple voting. The authors of paper [1] and [2] have introduced existing biometric e-voting system.

In an Electronic Voting System the main components of the process include [2]:

I .The Electronic Voter Register; a comprehensive database of eligible voters.

II. Authentication- which is done before to balloting. This is based on the use of a secure biometric identification algorithms and schemes.

III. Voting, Collation and Transmission- the election results directly from each of the polling Stations are sent to designated collation centres in real time.

But both the authors M. Khasawneh et al. [1] and V.C. Ossai et al. [2] have used unimodal biometric system i.e. only a single biometric input is considered such as palm print, hand geometry, iris pattern, and thumb impression, face recognition etc. As there are many problems related to unimodal biometric system, such as noisy sensor data, non-universality, lack of individuality, non-availability of invariant representations, etc., [4]. But here we will use multimode biometric system that will take a fusion of hand geometry and iris pattern as proposed in paper [3]. There are many more combinations of biometric input for fusion such as face and palm print [3], hand geometry and palm print[4], fusion in fingerprint and pattern recognition [5], voice etc.

2. LITERATURE REVIEW

2.1. **E**-voting system that uses biometric technique for authentication of voter to cast a vote was implemented by M. Khasawneh et al. and V.C. Ossai et al.

In [1] voter has to go to polling booths and have to verify self-identity as follows

I. Person has to insert his/her official id card in card reader

II. If person has already enrolled his vote then he/she is rejected but if that person has giving first time then system ask for his/her fingerprint.

III. If fingerprint matches with the existing fingerprint that is already stored in database then Person is authenticated for voting.

The whole process of e-voting in [1] is as follows.
While doing user verification input data i.e. finger print impression is read from sensor devices and sent to the central or local hosting a biometric database through network. Then the system will try to match the input of user being tested with existing enrolled records. If match found then user is authenticated for voting otherwise not. The following figure 1 shows how will be the data flow.

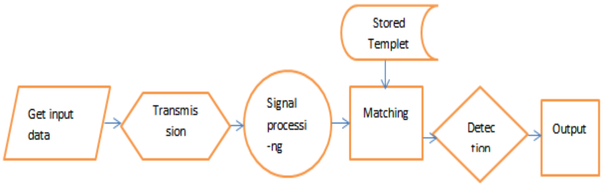


Figure 1 Biometric System data flow [1]

The Proposed e-voting System [1]: In an electronic voting system voters trusts on computer software, hardware and network infrastructure and cast his/her vote [1]. So author [1] has proposed two-sided solution that system will prints two hard copy of vote cast by voter, voter verifies the accuracy of his/her vote . Voters retain one copy and another copy will save in secure box.

For preventing more than one vote from same voter author [1] has used "voting flag"

This flag is set to false initially, whenever voter identity is verified this flag is set to true in data base.

So that whenever voter tries to cast his vote second time system will first check status flag. If this flag is false then voter can give the vote if it is true then it is rejected there only. If two people carrying the same ID card (one is real while the other is counterfeit) attempt to vote at the same time, the first one to access the record will set the flag to TRUE, load the record and prevent the other one from accessing the record[1]. Of course if the one with the counterfeit card obtains the record, the vote cast will fail at the next authentication step [1]. The flowchart of the whole process is as shown in figure 2. Voter has to first his/her official id card into card reader. Once card reader reads the official ID card it will try to search the record from local database. If record found then it will retrieve the voter's record from local database and set the status flag as true otherwise it will try search in central database set the status flag in central database. Now system will ask the voter to insert his/her finger print. Now it will compare finger print with the existing one. If match is found then it will display the pictures of candidate that belong to the same voting circuit then voter will select one. Now system will commit the transaction and set the status flag to false and vote flag to true.

2.1.1. Issues in this method are as follows

I. It is vulnerable interruption, delay, denial of receipt or denial of service; in such cases the assets and information are made unavailable.

II.It is also vulnerable to interception or snooping; in this case, an unauthorized party will be able, by browsing through files, eavesdropping, or reading communications, to gain access to private/sensitive information.

III. Modification or alteration in this information is changed or stored for later access by an unauthorized party.

IV. Fabrication or Spoofing in this refers an attacker may inject spurious information into the system and make it look like it had originated from a legitimate entity.

V. Repudiation of origin, in this is a fake denial that an entity did (send/create) something.

VI. It is also vulnerable to replay attacks, denial-of-service and session hi-jack.

VII. Counting of votes has to be done manually.

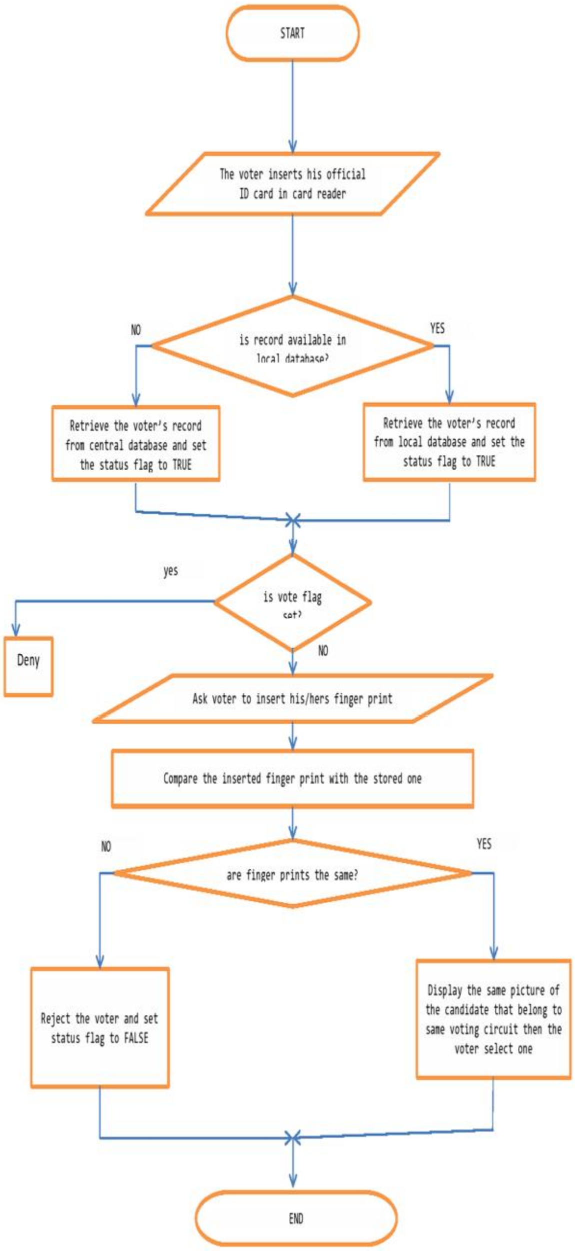
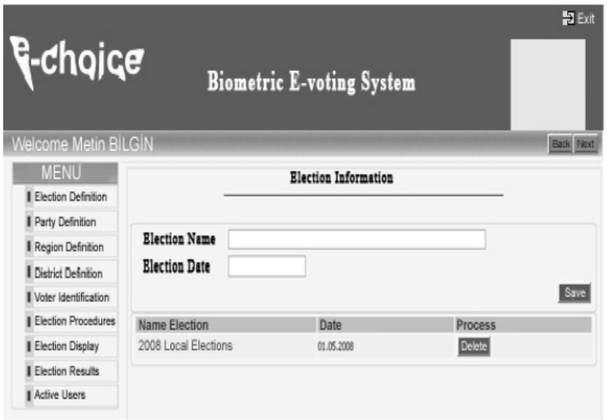

START
The voter inserts his official ID card in card reader
NO
YES
is record available in local database?
Retrieve the voter's record from central database and set the status flag to TRUE
Retrieve the voter's record from local database and set the status flag to TRUE
yes
is vote flag set?
Deny
NO
Ask voter to insert his/hers finger print
Compare the inserted finger print with the stored one
NO
YES
are finger prints the same?
Reject the voter and set status flag to FALSE
Display the same picture of the candidate that belong to same voting circuit then the voter select one
END

Figure 2 User login screen & election defining screen [1]

2.2. Self-Monitoring and Reporting Electronic Voting simulation Model (SMARESIM).[2]

According to the author V.C. Ossai et al. [2] above issues can be solve using Self-Monitoring and Reporting Electronic Voting simulation Model (SMARESIM). The biometric logon of this model is as shown in figure 3a, figure 3b, and figure 3c. This is the web application which is a webpage with program logic running behind it, for data collection and a web service for verification. The e-voting web application is allowed to interface with the physical biometric device but not the database containing the enrolled user data, while the web service can do the exact opposite [2]. As shown in figure 3a is the home page visible to voter at very first time, person has to log in the system using his/her unique log-in id and password. Once person logged into the system page shown in figure 3b is open. Voter has to fill up all the details and then person has to give fingerprint impression that will show in figure 3c page. This web application is to physical biometric device but not the database that contains data of enrolled user.

Figure 3a.User login screen & election defining screen [2]



Name Election	Date	Process
2008 Local Elections	01.05.2008	Delete

Figure 3b. Election defining System screen [2]

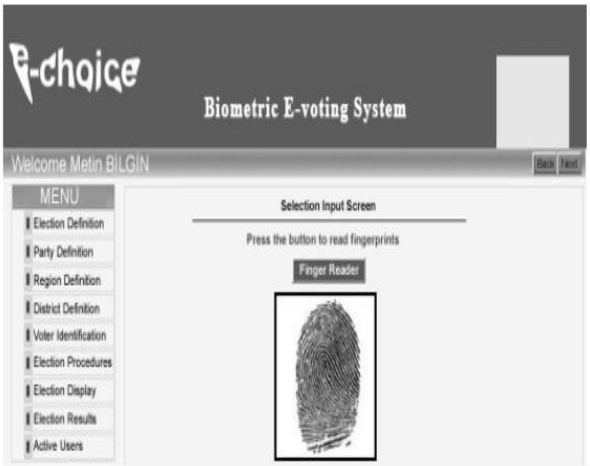


Figure 3c. Fingerprint information is scanned and stored in the database [2]

Applying texture-based feature extraction techniques to fingerprint authentication is very vulnerable. In this case, its security properties considering biometric integration is very vulnerable as attackers, Trojan horses, etc. Biometric technologies may add a new level of authentication and identification to applications, but are not, however, without their risks and challenges. There are important technological challenges such as accuracy, reliability, data security, user acceptance, and cost. Here author V.C. Ossai et al. has proposed Biometric Encryption in which key is bonded to biometric securely or extracted such that neither the key nor the biometric can be retrieved from the helper data[2]. The key is created using fuzzy process because of natural variability biometric samples. It is a group of emerging technologies that securely bind a digital key to a biometric or generate a digital key from the biometric, so that no biometric image or template is stored. What the original image from the encrypted template is impossible [2].

2.2.1. Multi-Protocol Label Switch -Open Virtual Private Network (MPLS-OVPN)

To solve problem of security threats surrounding of a public network, it uses the VPN that Provides secure network connection between sender and receiver by converting public network into a secure private network and provides a way to transmit data between two networked devices by creating tunnel, on top of a protocol such as shown in figure 4 and figure 5. Tunneling is mechanism for encapsulating one protocol in another protocol [2]. VPN also makes use of encryption and digital signature to ensure data cannot be modified without detection.

Essentially, an Open VPN performs the following viz:[2]
I. Receives packets of data (votes) from the polling booths using VNI (Virtual Network Interface).

II. After receiving the packets, it compresses the packets.

III. After compression, it encrypts the packets making use of the AES-128.

IV. It tunnels the packet using the TCP (Transmission Control Protocol) to the other end.

V. On receiving the encrypted traffic, the Open VPN performs the reverse of cryptographic operations to verify integrity and authenticity.

VI. After completing the reverse cryptographic operations, it decompresses the packets.

VII. The decompressed data (recovered votes) is passed by the VNI to the user interface. Figure 8 depicts the model of an Open VPN Tunnel for two remote sites.

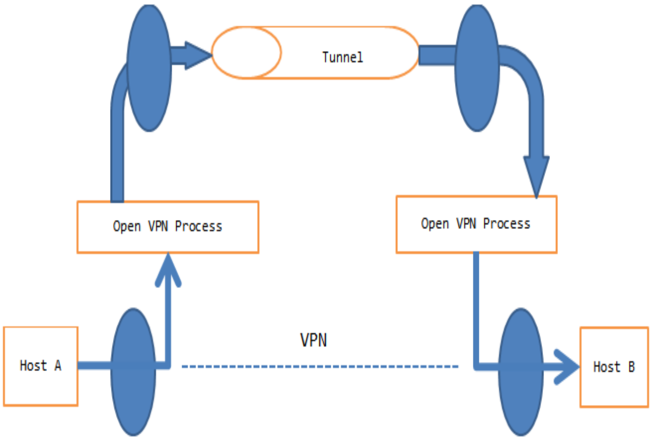


Figure 4. A Model of Open VPN Tunnel between two end points A and B [2]

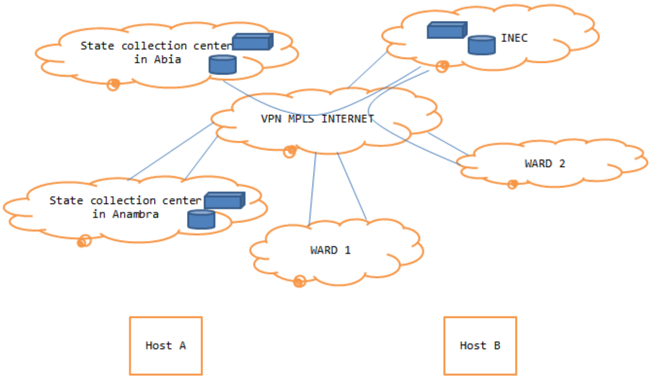


Figure 5 Flow diagram of MPLS -VPN backbone for the proposed SMARESIM [2]

The figure 6 shows the flowchart Biometric Encryption based on biometric key Binding. At Enrollment stage biometric sample is converted to biometric encrypted template using key binding algorithm that uses key created by key generator. At verification biometric sample of user being tested is compared with enrolled user biometric sample. If the match is found allow to vote otherwise deny. After casting a vote encrypt vote with key. After this data is sent using tunnel. At the State and National collection centers it gets decrypted and vote is counted.

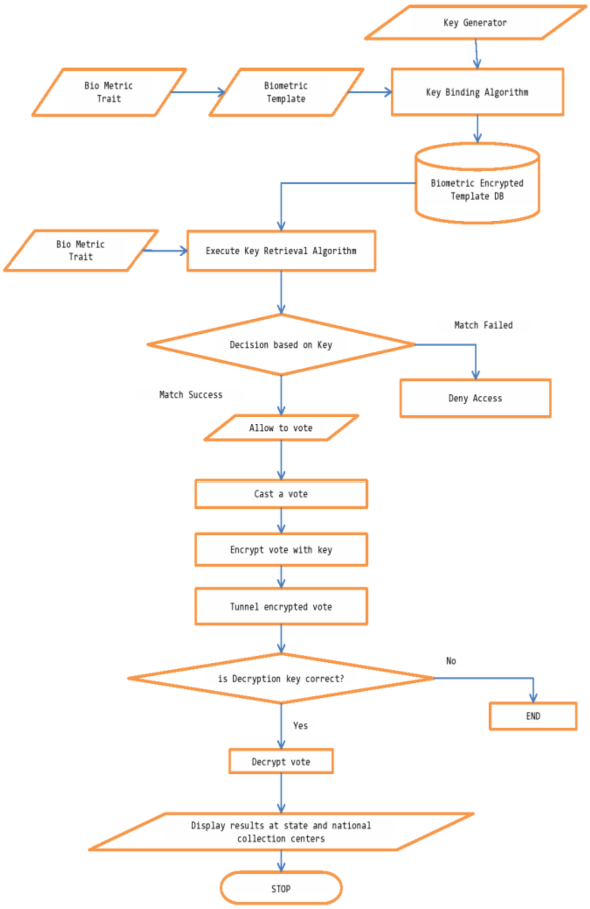


Figure 6 Flowchart of Biometric Encryption

Figure 7 below is a flow chart that briefly summarizes the authentication and voting process. The fresh fingerprint samples collected is combined with the biometrically encrypted template i.e. Bioscrypt which is stored in the database. If any of the of biometrically encrypted templates releases a digital cryptographic key, it means that the voter is a genuine voter who has not voted previous. The voter is granted access to vote for the political party of his choice else the voter is denied access to the E-voting system. The biometrically encrypted template/ Bioscrypt are deleted from the database (so that even if the voter represents himself, he is denied access to vote). The vote is then split into packets, encapsulated and tunnelled via a virtual tunnel to the state and national collection centre where the votes would be decrypted and election results would be tallied at both state and national level [2]

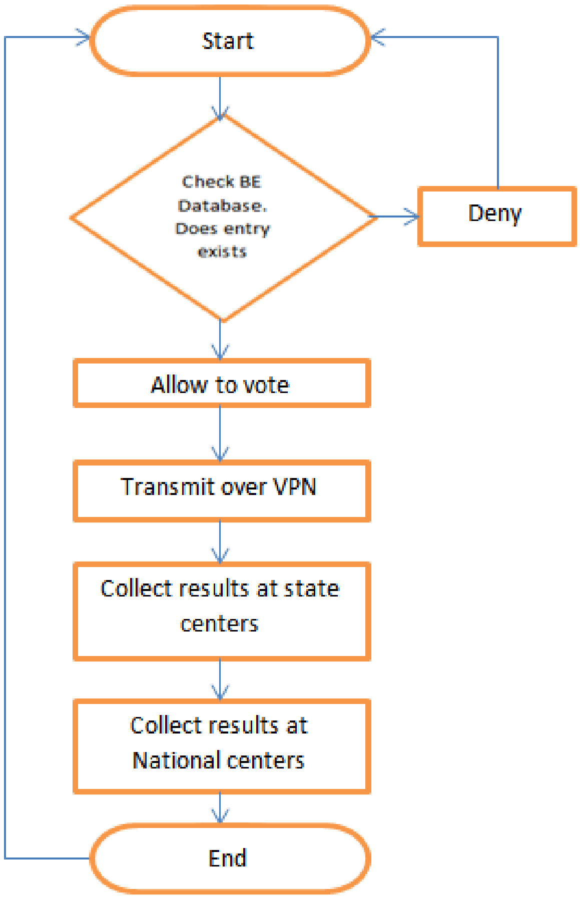

Start
Check BE Database. Does entry exists
Deny
Allow to vote
Transmit over VPN
Collect results at state centers
Collect results at National centers
End

Figure 7 Flowchart for e-voting Process. [2]

2.3. Problems in Unimodal Biometric System:

Both of these existing system [1] and [2] used unimodal biometric system that is analysing one biometric trait at a time. But there are many problems in Unimodal as follows.

1) Noise in sensed data: due to imperfect acquisition conditions, the captured biometric traits might be noisy or distorted. Such variations in biometric information might produce false matches in the database, i.e., an enrolled user of the system might be incorrectly rejected, or otherwise, an impostor might be incorrectly accepted. In face technologies, illumination conditions might affect the quality of the captured face images. In fingerprint applications, acquired fingerprints from crime scenes might just have a portion of a fingerprint, being thus difficult to identify an individual.

2) Non-universality: even though biometric trait is unique among every individual of a given population, it is highly possible that an individual might not be able to provide his/her biometric. For e.g. due to pathological condition of an eye, IRIS images will not be taken. It is difficult to get proper fingerprint structure of an individual working in environments having lot of manual activities leading to failure in getting the fingerprint scan.

3) Upper bound on identification accuracy: the accuracy of biometric system can be improved by developing more robust techniques. There is always a trade-off on system's accuracy. The upper bound mainly depends on quantity and quality of distinct patterns that can be modelled using a given template. The distinct feature of a template can be constrained by two factors; i.e. Intra-class and Inner-class variation amongst individual. The former refers to variation amongst sets belonging to same individuals. The latter refers to different individuals. There can be possibility where there exists a high intra-class variation, i.e. biometric feature of same individual vary to greater extent, similarly low inter-class variations denotes biometric features of different individual have similar feature. Accuracy of biometric systems is affected by High intra-class variations and low inter-class variations.

4) Spoof attacks: spoofing is the most common problem in biometric system, spoofing can be controlled by combining different types of biometric traits and merging into a single application hence curbing the success rate of spoof attacks. Biometric traits such as voice or signature are prone to such attacks.

3. MULTIMODE BIOMETRIC SYSTEM

These problem leads to poor system performance, these limitations can be overcome by using multimode biometric system. In any multimode biometric authentication system the image has to undergo through following stages

- Image Sensing: Image acquisition by using specific camera is called as image sensing .
- Feature Extraction: Extracting the features from acquired biometric trait.
- Matching: Finding a correlation between existing and current biometric samples.
- Decision Level: Weather biometric traits of user being tested and biometric traits of enrolled user are matched or not.

Fusion of biometric samples can be done at any of these above stages

3.1. Fusion of human face and palm print

Author Yinghua Lu et al. of [4] has proposed fusion of Human face and Palm Print. Feature extraction level. The following figure (8) is the system flowchart that Yinghua Lu et al. in [3] have introduced

.

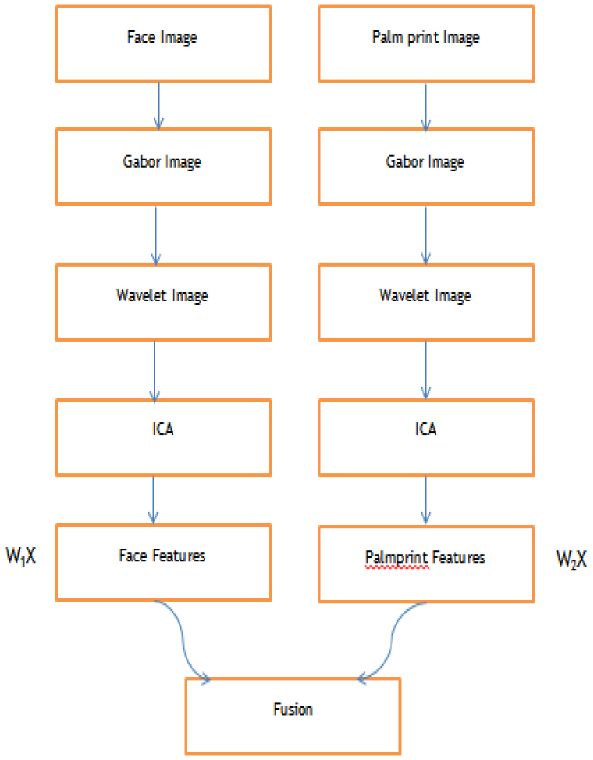


Figure 8 Flowchart of the system [3]

3.1.1. Feature Extraction

3.1.1.1. Gabor Transform: It captures important and multi scale and multi directional space frequency features and enlarge the grey variety of microscope. Gabor Transform is given in equation (1) of [3]

$$G(x,y,\theta,\mu,\sigma) = \frac{1}{2\pi*\pi} e^{-\frac{x*x+y*y}{2*\sigma*\sigma}} e^{(2\pi i(\mu x \cos\theta + \mu y \sin\theta))} \qquad (1)$$

i = √ (-1), μ -frequency, σ -standard deviation

3.1.1.2. Wavelet Transform: Wavelet analysis is a time-frequency localization method whose window size is fixed but shape can optionally change. . After wavelet transformation the image becomes 1/4 of the Gabor transform image.

3.1.1.3.Independent Component analysis:

Independent component analysis is a new feature extraction method recent years whose meaning is decomposing multi-channel observation signals into a number of independent components (Independent Component, IC) through the optimization algorithm. For details refer [6].

3.1.2.Fusion:

As face and palm print features have large difference normalization is needed before fusion. The author has given equation (2) of [3] to normalized score.

$$Xnor = \frac{X - \mu}{\sigma} \qquad (2)$$

X – Face or palm print features extracted by IRIS
μ - mean value
σ - standard deviation

Weighting rules: The weight sum of face and palm sprint should be 1 and they vary in the range [0.1, 0.9] given in equation (3) of [3]

$$W1 + W2 = 1; W1, W2 = 0.1, 0.2, 0.3 \ldots\ldots 0.9 \qquad (3)$$

W1 represents palm print weight and W2 represents face weight. When palm print weight changing from 0.1 to 0.9, face weight changes from 0.9 to 0.1. By the dynamic weighting rule, the largest weight which can get the highest recognition rate is selected
In [4], Nongluk Covavisaruch et al. have introduced fusion of hand geometry and iris pattern as follows.

3.2. Fusion of Hand geometry and Iris pattern

Hand geometry biometric system: In this firstly image is captured through ccd digital camera then noise is removed using median filter, image is converted to the binary image using thresholding, border of the hand silhouette is smoothed by morphological opening and closing.

3.2.1. Feature Extraction: Firstly left most pixel and right most pixel are found and then mid of S1 (left most pixel) and E1 (right most pixel) are found and then mid of S1 and E1 are located. Using this mid pixel valley points and contour point are calculated by using Euclidean distances. After that the length of fingertips are calculated from reference point at distance of 1/3, 1/2 and 2/3 heights. Finger tips and valley points are as shown in figure 9.a and figure 9.b shows hand geometry

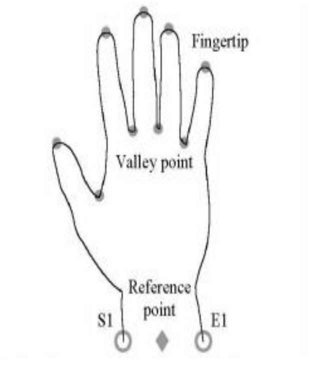


Figure 9a. Finger tips and Valley points of a hand [4]

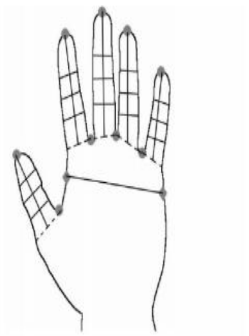


Figure 9b. Hand Geometry features [4]

Now for matching process [3], S1 is selected for matching the features with these of enrolled users.
Minimum distance, or matching is given in equation (4) of [4], is the closet match

$$D_{s1} = 1/n \sum_1^d \ (\min(Yi, fi) / \max(Y, f)) \qquad (4)$$

Yi=ith element of the feature vector of a user being tested
fi= ith element of the feature vector of an enrolled user in a Iris

Biometric System: As steps applied for hand geometry those are also applied for iris pattern i.e. noise removal threshold; dd for converting into binary image, smoothing the edges. After this circular Hough transform is applied to locate the pupil. Iris is located using integro-differential education given in equation (5) of [4] follows, shown in figure 10 database.

$$(r_i, x_i, y_i) = \mathrm{argmax}_{(ri,\ xi,\ yi)} \mid G\sigma(r) * \frac{\partial}{\partial r} \oint \frac{I(xi,yi)ds}{2\pi r} \qquad (5)$$

I (x_i, y_i) – Grey level at (x, y)

Gσ(r) – Smoothing function with standard deviation equals to σ

r_i, x_i & y_i – radius and center of iris

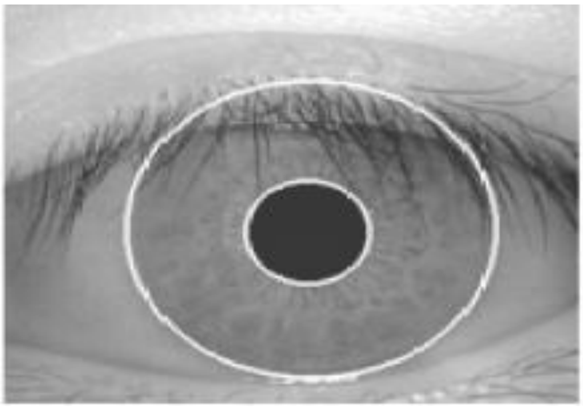


Figure 10. Result of localization of iris and pupil [4]

In this left and right segments of iris are used for feature extraction as it is found that eyelashes and eyelids partially cover in many images Nongluk Covavisaruch et al. has taken only left and right segment of iris. After that polar co-ordinates are converted to Cartesian co-ordinates. As the intensities of the image in dataset is not normalized then intensities of images are normalized using following equation (6) of [4]

$$I^{I}_{(x,\ y)} = \phi_d + \lambda; \qquad \text{if } I_{(x,\ y)} > \phi \qquad (6)$$

$$= \phi_d - \lambda; \qquad \text{otherwise}$$

Where $\lambda = \sqrt{\frac{Pd\ (I(x,y)-\phi)*(I(x,y)-\phi)}{P}}$

ϕ_d – mean of result image

P_d – variance of result image

ϕ – mean of original image

P – variance of original image

Matching is done using following equation (7) of [4]

$$D_a = \sum |Y_i - f_i| \text{ where } i = 1 \text{ to } d \qquad (7)$$

Y_i - ith element of feature vector of user being asked

f_i - ith element of an enrolled user in database

3.2.1.2. Fusion: Fusion can be done at several levels i.e.

- Sensor Level
    - But here two inputs i.e. Hand geometry and iris cannot be taken from same input system. So fusion cannot be done here
- Feature Extraction
    - Here if fusion is done the it can cause series of dimensionality problem that causes poor system performance
- Decision Level
    - Impossible because of insufficient information to classify the user
- Matching
    - Here author has proposed that fusion should be done at matching level

There are 4 different methods author has proposed for normalization

1) Min Max matching score: uses equation (8) of[4]

$$MM = \frac{S - \min(s)}{\max(s) - \min(s)} \qquad (8)$$

2) Z Score matching score: uses equation (9) of [4]

$$Zs = \frac{S - mean(s)}{std(s)} \qquad (9)$$

mean(S) = mean of our matching score

std(S) = is the standard deviation of our matching score.

3) Possible Min-Max matching score : uses equation (10)

Of [4]

$$PMM = \frac{S - P\min(S)}{P\max(S) - P\min(S)}$$

(10)

Possible min-max matching score: It is the method adapted from min-max method. This Normalization score is the minimum score selected

Author has selected Possible min-max matching score method for taking matching score of hand geometry and in's pattern, and has taken the minimum value

Now normalized matching score author has combined it by using weighted sun method as equation (11) of [4]

$$Score_{multi}=W_H*Score_H+ W_I*Score_I \qquad (11)$$

WH & WI – Weights applied to the matching score from hand geometry and iris system.

4. INFERENCES

4.1Advantages:

- No bogus votes possible since it requires biometric or finger print
- No manual intervention required to authenticate
- In [2] there is no overhead of counting votes manually
- In [2] security is maintained by using VPN network.
- As both [1] and [2] uses unimodal biometric system the problems such as Noise in sensed data, Non-universality, Upper bound on identification accuracy, Spoof attacks can be resolved by using multimode biometric system.
- If there is a problem of **Non-universality** then we are having a solution of multimode biometric system as proposed in [3] and [4] so that everyone can vote.

4.2 Disadvantages:

- System [1] was vulnerable to attacks
- Biometrics is an expensive security solution
- Fingerprints of those people working in chemical industry are often affected.
- So use of unimodal biometric is insufficient
- V.C. Ossai et al. [2] has introduced Biometric key binding algorithm, but not yet implemented.

5. CONCLUSION

Thus in this literature review we have studied two existing e-voting system based on biometric authentication.[1] has many issues related to security. Those security issues are solved by using biometric encryption and MPLS-OVPN methods proposed in [2].But still both this existing system uses unimodal biometric system which have many limitations regarding noise in sensed data, non-universality, upper bound on identification accuracy and Spoof attacks. Those limitations can be solved by multimode system as fusion of hand geometry and iris pattern OR fusion of human face and palm print.

6. REFERENCES

[1] Mohammed Khasawneh, Omar Al-Jarrah, Laith Barakat, Thaier S. Hayajneh, and Munzer S. Ebaid, " A Biometric-Secure e-Voting System for Election Processes", Proceeding of the 5th International Symposium on Mechatronics and its Applications (ISMA08), Amman, Jordan, May 27-29, 2008.

[2] V.C. Ossai, K.C. Okafor, H.C. Inyama , A.O. Agbonghae., "SMARESiM: an improved model of e-voting system based on biometric key binding, smaresim: an improved model of e-voting system based on biometric key binding" Volume 2 Issue 6 June, 2013 Page No. 1704-1726

[3] Yinghua Lu , Yao Fu,, Jinsong Li1, Xiaolu Li1, Jun Kong, "A Multi-modal Authentication Method Based on Human Face and Palm print" 2008 Second International Conference on Future Generation Communication and Networking.

[4] Nongluk Covavisaruch, Pipat Prateepamornkul," Personal Identification System using Hand Geometry and Iris Pattern Fusion", Electro/information Technology, 2006 IEEE International Conference .

[5] S. Prabhakar,,. K. Jain, "Decision-level fusion in fingerprint verification, *Pattern Recognition* " (2002) 861-874.

[6] A. Hyvarinen, E. Oja ,"Independent Component Analysis: algorithms and applications", *Neural Networks* 13 (2000) 411-430

[7] Afzel Noore, Richa Singh, Mayank Vatsa, "Robust memory-efficient data level information fusion of multi modal bio-metric images", Information Fusion 8 (2007) 337-346.

[8] www.google.com

[9] www.ieee,org

[10] www.yahoo.com

[11] www.griaulebiometrics.com