

# Multimodal Biometric Authentication using ECG and Fingerprint

Manjunathswamy B E  
Department of Computer  
Science and Engineering,  
University Visvesvaraya  
College of Engineering,  
Bangalore, India

Appaji M Abhishek  
Department of Computer  
Science and Engineering,  
University Visvesvaraya  
College of Engineering,  
Bangalore, India

Thriveni J  
Department of Computer  
Science and Engineering,  
University Visvesvaraya  
College of Engineering,  
Bangalore, India

Venugopal K R  
Department of Computer Science and  
Engineering,  
University Visvesvaraya College of Engineering,  
Bangalore, India

L M Patnaik  
Honorary Professor,  
Indian Institute of Science,  
Bangalore, India

## ABSTRACT

Biometric system is a very important recognition system which is used for individual verification and identification. Various types of biometric traits are used in today's world, in which some are used for commercial purpose and few used for verification purpose. Existing authentication techniques are suffer from different errors like mismatch image, spoofing, falsification in the data, to solve this errors the combination of Electrocardiography(ECG) and fingerprint multimodal is introduced. This proposed modal produces effective recognition system when compared to individual recognition system. The proposed multimodal recognition system provides optimum results compared to the individual recognition system which yields better results for authentication compared to the Existing system.

## Keywords

Electrocardiogram (ECG), Fingerprint, Authentication, Multimodal.

## 1. INTRODUCTION

### 1.1 Biometrics

Biometrics is meant a science and technology used to measure & analyze biological data. In information technology, biometrics refers to technology that measures and analyzes the characteristics of a human body such as DNA, Fingerprints, IRIS, Voice patterns, facial patterns and hand measurements for authentication. Biometric verification system used for authentication purpose is becoming very common in corporate security systems, public security systems, consumer electronics and point of sale (POS) applications. In addition to security, the driving force behind biometric verification has been convenience. Biometric devices, such as fingerprint scanners consists of a reader or scanning device, a software that converts the scanned image into digital form and compares with the match points and a database that stores the biometric data for comparison.

In order to prevent the identity theft, gathered biometric data is usually stored in a encrypted format. A software/set of statements is used to convert the biometric input data and to identify the find the common match points. The match points found in the database are processed through an algorithm that translates information into numeric/digital value. The final

database value is compared with the user's biometric input and authentication is either approved or denied[1].

### 1.2 Electrocardiogram (ECG)

An electrical conductivity and the cardio vascular changes in a heart can be measured by using ECG. Each heartbeat generates an electrical signal(wave) which can be used in the detection mechanism. whenever a signal is generated, it passes through the heart muscles and squeezes the muscles. this squeezing helps the heart to pump the blood. The left and right atria or the upper chambers generates first electrical signal(wave) called a "(P-Wave)" followed by a straight line when the electrical signal flows from top chambers to lower chambers. The next wave called "QRS Complex" that is generated by the left and right bottom chambers or ventricles. the last and final wave represents electrical recovery or return to a relaxed state for the ventricles which is called a "T Wave". A normal heartbeat on ECG shows the timing of the top and lower chambers. An ECG gives two major kinds of information. firstly, a doctor determines how long the electrical wave takes to pass through the heart beat by measuring the time intervals on the ECG. Finding out the time taken by wave to travel from one part of the heart to other parts of the body shows if electrical activity is normal or slow or fast or irregular. secondly a cardiologist will be able to find out the parts of the heart are too large or overworked by measuring the amount of electrical activity passing through the heart muscle. Figure 1 shows the typical electrocardiogram.

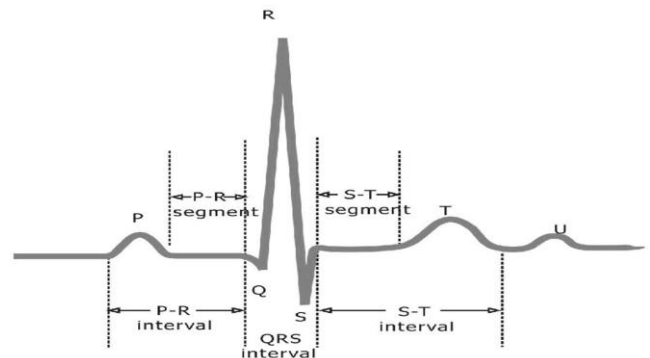


Fig 1:. A typical Electrocardiogram

### 1.3 Fingerprint

Fingerprint identification method is most commonly used identification system in the government or public sectors. This identification system is found by the impressions made by an individuals fingertips which has a minute ridge patterns and the patterns on the fingertips of each individuals remains unchanged throughout the life. Other personal characteristics of an individual may change or vary but the finger prints do not. Fingerprints offer an reliable or error-free means of personal identification. Fingerprints can be recorded or scanned on a standard identification card or can be recorded digitally on the system and transmitted electronically to the FBI (Federal Bureau of Investigation) for comparison. Fingerprints are compared with the fingerprints of the suspected person captured at the spot of crime can provide a absolute proof of the presence or identity of a person [1].

## 2. LITERATURE SURVEY

The studies in the recent past have shown the possibility of the ECG signal as a candidate of biometric for individual authentication. Most of the literatures implements the respective algorithm for the data acquired from MIT - BIH database.

Ming Li et al., used the features like Hermite Polynomial Expansion, Cepstral Feature Extraction with HLDA and modeled using SVM with Linear Kernel and GMM Super vector Modeling. The Score Level Fusion got 98.3% as Accuracy with 0.5% error rate [2]. The algorithm needs to be validated over larger subjects.

Nahid et al., used Physikalisch-Technische Bundesanstalt (PTB) database. The AR Coefficients, PSD, Lyapunov Exponent, approximation entropy, Higuchi fractal dimension and Shanon entropy are used as features and applied to MLP (Multi Layer Perception), PNN (Probabilistic Neural Network) and KNN classifier. The accuracy achieved was 98.58% for 12 subjects using AR coefficients to KNN classifier. By adding PSD, 100 % accuracy combination of fractal dimension lead to better results rather than just one fractal based feature type. The best combination includes ApEN, Shanon Entropy and Lyapunov Entropy [3]. A single Lead ECG obtained from 19 subjects was used in Zir-Merhav (ZM) cross parsing algorithm. The Dictionary is static and buffer slides over it and had got 100% accuracy for more number of subjects [4]. The Single lead ECG was recorded using BIOPAC machine from 269 subjects. The Short term frequency method with robust feature selection was used and 79.9% accuracy rank-1 recognition, 93.5% in rank -15 recognition, when training and testing heart beats are from different days. 99% recognition for same days 5.52% EER in verification and 0.37% EER for same days was obtained [5]. Using MIT – BIH Arrhythmia database of single lead data, 13 subjects, Extended Kalman Filter (EKF) was implemented and it worked on non-linear ECG dynamic signals with Accuracy of 87.5% [6]. The Fusion of ECG with unobtrusive biometrics has led to efficient output. The ECG signals from Physionet were used. Biometric information of face and fingerprint are acquired from NIST in the form of match scores. The genuine acceptance rate of the proposed system has achieved to 100% for the FT-EER fusion technique & 97% for the FT-MSD fusion technique. The EER of 0.22% for proposed Multimodal Biometric. EER of 10.80%, 4.52% and 2.12%, respectively for the ECG signal, face and fingerprint biometrics is obtained [7].

The CVD Patient data from MIT-BIH was taken and a shortened feature character set that represent a person was generated. Generation of individual features from their compressed ECG. Calculation & sorting of the character frequency was done. The Compressed ECG inherently has the benefit of faster and effective transmission. If by any chance the compressed ECG falls into the wrong hand (by spoof attack), the attacker only gets compressed and encrypted ECG messages without the patient's name. There is faster matching and reduced template storage [8]. 150 Fingerprint Images from 50 individuals are taken and Histogram equalization, extraction & modification of ridge direction, dynamic thresholding, ridge thinning, feature extraction (small windows are used), structural matching (local features like relative angle & ridge count) was done. Good accuracy, reliability & execution speed for translated, rotated & stretched fingerprints are obtained. Automated fingerprint recognition system has got FRR as 1%, FAR nearly 0% [9].

**Table I. Comparison among various biometric identification systems**

System	Security	Cost & Complexity	Unique Identity	Environmental Impact
Iris	Moderate	More	More	Less
Fingerprint	Moderate	Moderate	More	Moderate
Palm print	Moderate	Moderate	More	Moderate
Electro Car diagram	Moderate	Less	Moderate	Less
Face Recognition	Less	Moderate	Less	More
Voice Recognition	Less	Less	Less	More
DNA	More	More	More	Less

In this paper, finger print and electrocardiogram (ECG) has been discussed. Biometric have different techniques like IRIS recognition, Palm Print, DNA, Face & Voice recognition systems etc. In authentication system, people are using different Biometric systems. Biometric aim is to secure the different systems like banking systems, military systems and Research and development centers. In authentication system, computer is required to store many passwords which may be stolen or sometimes either forgotten and is also very disastrous for the user in many situations[1].

The comparison of various biometric identification systems is tabulated in Table 1. The primary element used in the table is the security system considered for identification. The biometric of human body can be duplicated easily which is one of the important fact in the biometric system. In the DNA system, the duplication in the existing biometric system is very difficult. The security in the DNA system is more where as in the IRIS and palm print is moderate and in face and voice recognition, security is very less.

The second element considered in the above Table 1 is the cost & complexity. There is more complexity in the DNA and IRIS system where as the complexity is moderate in palm print and face recognition but it is very less in case of voice recognition. The third element considered in the above Table 1

is its uniqueness in identity. Iris is known as an uniqueness biometric system. Different individuals have different Iris so it has more uniqueness properties like palm print and DNA system. But the uniqueness is very less in case of face and voice recognition.

The last and the final element considered in the table 1 is the environmental impact with the changing environment where the biometrics keeps changing. As an example, whenever the finger or palm got hurt, the palm print and the finger print would also be changed as an environmental impact. In various changes, face and voice recognition will have more environmental impact where the IRIS & DNA will have less environmental impact [10].

The cardio vascular condition effect on ECG Biometrics is investigated by Tsu-Wang Shen et al., Lead I and Lead II ECG signals from 23 peritoneal dialysis patients monitored under IRS regulation at Tzu- Chi general hospital. The famous Pan Tompkins method to find R-R interval is adapted. Other peaks are determined based on the time period they are away from R peak. The derivative of ECG and Zero crossing method used to detect PQST points. 17 features selected. Two methods of evaluation are used. First, Correlation coefficient of template matching and the other Statistical t-test with significance level with  $p < 0.05$ . Dialysis has no significant effect on biometrics in short term. ECG is still able to identify individuals even after correlation coefficient decreased from 0.985 to 0.877 after 2 years [11].

Konstantinos et al., used PTB database for ECG conditioning and finding Autocorrelation (AC), Discrete cosine transform (DCT), Performance Evaluation (Normalized Euclidean distance, Normalized Gaussian log likelihood, False negative (FN) and false positive (FP) Performance), Classification Performance. It is possible to perform ECG biometric recognition without the use of PQRST fiducial detection. There is high Recognition Rate and very low false negative rates resulting from the AC/DCT method. This suggests that this method could be applied to biometric recognition scenarios with high FN costs. This Technique can also be applied for acoustic signals [12].

Anil K Jain et al., have used NIST-4 database with 4,000 fingerprint images of image size 512 X 480 from 2,000 fingers. The Main steps are Locate a registration point, decompose the input image into a set of component images, compute the standard deviation, generate the feature vector (Finger Code), use two stage classifier which uses a K-nearest neighbor classifier in 1st & a set of neural network classifiers in its 2nd stage to classify a feature vector into one of the 5 fingerprint classes. The Classification was into five categories: whorl, right loop, left loop, arch, and tented arch. The multichannel filter-based classification algorithm which gives better accuracy and is robust to noise which is reflected in the classification accuracy. Performance (90% for the 5-class classification problem and 94.8% for the 4-class (A & T merged) classification problem with 1.8% rejection during the feature extraction phase) [13].

### 3. PROPOSED ARCHITECTURE

The ECG signal is acquired using Biopac MP35 for different subjects. The signal recorded is used for feature extraction[1]. The signal is pre-processed for baseline wandering and noise removal. The features extracted include amplitude features, angle features and interval features. Finally the similarity scores are generated using the following formula

$$\text{Similarity Score} = \frac{\text{MaximumScore} - \text{IndividualScore}}{\text{MaximumScore} - \text{MinimumScore}}$$

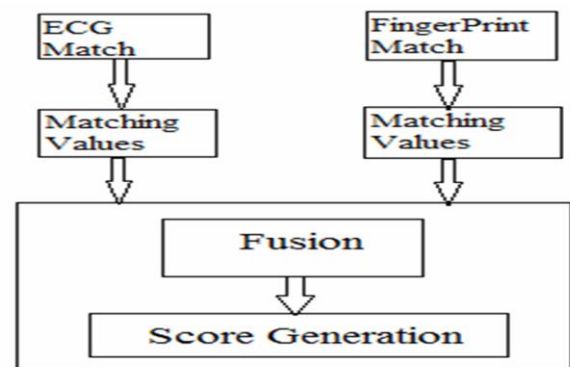
The fingerprint is acquired using fingerprint scanner. The image is then used for feature extraction. The fingerprint image pre-processing is accomplished by Histogram Equalization and Fast Fourier Transform, these operations enhance the Image. The adaptive thresholding is used and the Image is binarized. In Segmentation process, the direction of the ridges is estimated and Region of Interest is extracted.

The Binarized Image is again considered. It is Thinned, then the H-breaks and spikes in the thinned Image are removed. The Minutia Extraction is accomplished by detecting all Minutiae (Bifurcations and Terminations). False Minutiae are removed by using little algorithmic estimation. The removal of False Minutiae enhances the visibility of true minutiae on the thinned Image. The Image is stored in database for further comparison with other minutiae detected Image. The matching is done based on matching the ridges and their location in Image. The steps involved in the ECG recognition and fingerprint recognition is as tabulated in Table 2.

**Table II. Steps involved in ECG and Fingerprint recognition**

ECG Recognition	Fingerprint Recognition
Acquisition	
Pre-processing	Minutiae Extraction & Image Segmentation
Feature Extraction	Pre-processing & post Processing
Score Generation	
Performance Analysis	

The Figure 2 shows the architecture of Multimodal biometrics using finger print and ECG. The fused value is given the scores.



**Fig 2: Architecture of ECG and finger print processing**

#### 4. IMPLEMENTATION

**Step1:** The ECG signal acquired is taken and the wavelet decomposed of the signal is performed. A certain time period window is considered and the highest peak in the window is determined. Since R peak is the maximum amplitude in the ECG signal, this maximum value is assigned as the R peak. The corresponding location of R peak is also recorded and stored as Rloc (location of R peak). The same is repeated for all the cycles of the ECG sample. The R peak and Rloc values are stored for the signal. The P peak is found in the time period region of 50-200ms before R peak, a window is used and the peaks are analyzed in this time interval. The maximum peak in this region is determined to be P peak. The corresponding location of P peak is stored as Ploc (location of P peak). In the way all P peaks and Plocs are determined for the signal. Similarly for Q, R, S and T is extracted on the same grounds. The waves extracted from the ECG are marked on the ECG signal. The angle subtended at the peaks in ECG signal can also be used for biometric recognition. We use 3 angle features here, namely, angle PQR, angle QRS and angle RST. The angles are determined using the mathematical concept of finding angle between two lines. The Interval features are another set of features for Biometric recognition. The interval features in the ECG are many. The features used are majorly peak to peak intervals, namely, RP, RQ, RS, RT and RR intervals. The Score for the features is estimated using the equation

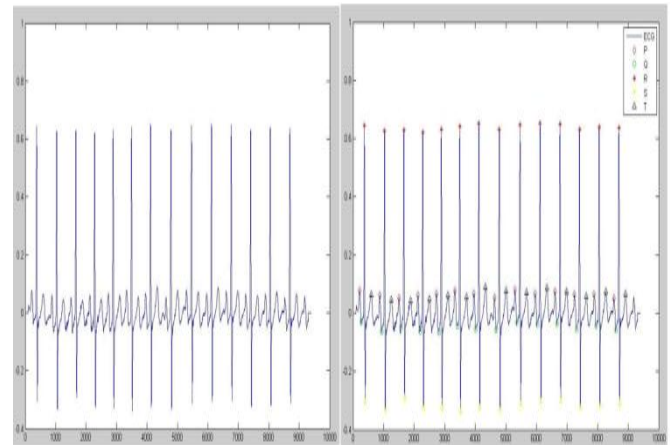
$$\text{Similarity Score} = \frac{\text{MaximumScore} - \text{IndividualScore}}{\text{MaximumScore} - \text{MinimumScore}}$$

**Step2:** Fingerprint pre-processing is done by Image enhancement. This makes the image clearer for further operations. Further, Histogram manipulation helps in Image Enhancement. The Histogram Equalized image is divided into small processing blocks (32 by 32 pixels). The Fourier transform is performed on every block of the Image. The Fingerprint Image is made of Gray levels, there foreit has to be converted into binary format which is achieved by Adaptive binarization. Separating the Region of Interest from the background (unwanted part of image) is called Segmentation of Image. The Minutiae of the finger print is extracted from the image after performing thinning of the ridges.

**Step3:** The fusion of the 2 Biometric techniques is possible as their databases are acquired from same individual. The algorithms are tested. The decision depends on both the outputs. In ECG, totally12 features are considered. In fingerprint 2 features namely, bifurcations and terminations are considered. In fusion the final decision is taken when the individual is tested authenticate by at least 11 out of 14 features. The threshold is set to 75%. ECG and fingerprint fusion results are shown in Table 6.

#### 5. PERFORMANCE ANALYSIS

Figure 3 shows the acquired ECG after processing and the waves and peaks detected signals. Table 3 show the features extracted from the signal and Table 4 shows the matching score percentage.



**Fig 3: Acquired ECG and PQRST detected ECG**

**Table III. ECG features extracted from the signal**

Angle Features	1	2	3	4	5
Angle_PQR	25.24	29.38	48.90	67.54	67.54
Angle_QRS	55.51	58.56	60.53	62.87	62.88
Angle_RST	17.95	11.05	9.23	13.02	13.01

##### Amplitude

RP_amp	0.58	0.59	0.56	0.56	0.56
RQ_amp	0.70	0.72	0.69	0.68	0.68
RS_amp	0.97	0.96	0.94	0.95	0.95
RT_amp	0.58	0.57	0.56	0.59	0.59

##### Interval

RP_interval	159	158	154	168	169
RQ_interval	90	91	100	100	100
RS_interval	-25	-24	-24	-26	-25
RT_interval	219	224	227	212	211
RR_interval	159	158	154	168	169

**Table IV. Match rate for ECG**

Template					
Sample Image	S1	S2	S3	S4	S5
Match Rate(%)	50.42	56.38	44.04	58.71	69



**Fig 4: Original Image, Enhanced Image, Region of Interest and Minutiae extracted image**

**Table V. Match percentage of the finger print**

Template 3_1					
Sample Image	3_2	3_3	3_4	3_5	3_6
Match Rate(%)	83.33	88.89	88.89	66.67	66.67

Here only few results are shown. The threshold for match rate is set to 75%. If the matching rate is greater then 75%, the person is said to be authentic.

**Table VI. Results of fusion of ECG and fingerprint**

Template					
Sample Image	T1	T2	T3	T4	T5
Match Rate(%)	78.57	71.4	78.51	92.8	85.71

**Binarization:** Finger print image is transformed through a 8-bit grey image to a 1-bit image with value 0 for ridges and with value 1 for furrows using Binarization method. On completion of operation, ridges in the finger print are highlighted black in color while the furrows are highlighted white in color.

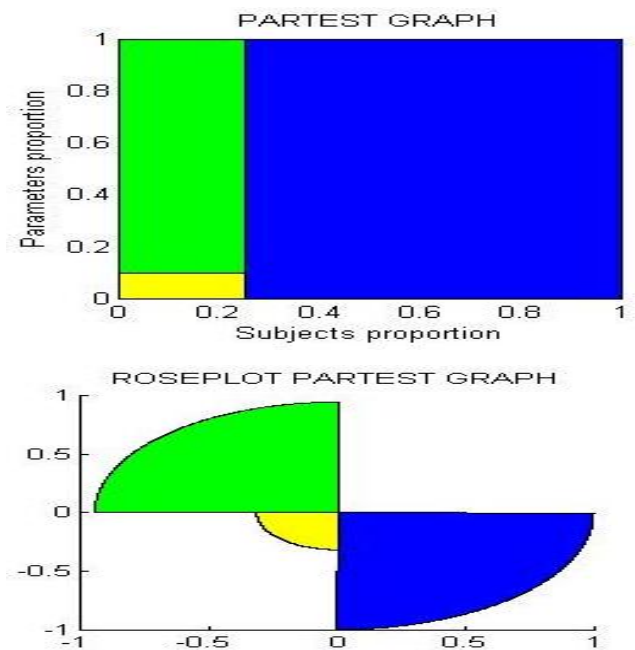
**Direction:** The direction method gives the information of minutiae which needs to be considered for authentication purpose. The orientation information is obtained by converting the ridges and furrows flowing in curves through a pointed direction. Finally minutia is detected using both the ridges and furrows.

**Region of Interest:** To find the region of interest, two morphological operations called OPEN and CLOSE is used. The OPEN operation expands the image and removes the peaks introduced by background noise. The CLOSE operation shrinks the image and eliminates small cavities within the image. The closed area is subtracted from the opened area to get the bounded and the inner area. Then the algorithm throws the 4 blocks out of the bounded area to get the tightly bounded region i.e., leftmost, rightmost, uppermost and the bottom most area. Figure 4 shows the original image, enhanced image, region of interest and minutiae extracted image where as fingerprint matching percentage has been shown in Table 5.

The Table 7 represents the False measure rates for ECG, Fingerprint & fusion of ECG and FP recognition system.

**Table VII. FRR and FAR for the ECG and Fingerprint Recognition System**

	FALSE MEASURE RATES (%)	
BIOMETRIC	FRR	FAR
ECG	9.52	2.38
FINGER PRINT	5.55	7.77
FUSION OF ECG & FINGERPRINT	0	2.5



**Fig 5: Plots for Fusion of ECG and Fingerprint**

Figure 5 shows the Partest Graph and Roseplot Partest Graph for Fusion of ECG and Fingerprint biometrics. The Partest and Roseplot graph shows the graphical representation of the efficiency in biometrics algorithms.

**Table VIII: Results for ECG, Fingerprint and Fusion**

PARAMETERS	ECG	FP	FUSION OF ECG & FINGERPRINT
Prevalence	29.40%	46.30%	25.00%
Sensitivity	80.00%	93.30%	90.00%
False negative proportions	20.00%	6.70%	10.00%
False discovery rates	33.30%	9.10%	0.00%



<b>Specificity</b>	83.30%	92.00%	100.00%
<b>False positive proportions</b>	16.70%	8.00%	0.00%
<b>False omission rate</b>	9.10%	5.90%	3.20%
<b>Youden's Index and Number</b>	0.6333	0.8529	90.00%
<b>Positive predictivity</b>	66.70%	90.90%	100.00%
<b>Positive Likelihood Ratio</b>	4.8	11.6	NIL
<b>Negative predictivity</b>	90.90%	94.10%	96.80%
<b>Negative Likelihood Ratio</b>	0.24	0.0725	10.00%
<b>Predictive Summary Index (PSI)</b>	0.5758	0.8503	96.77%
<b>Test Accuracy or Potency</b>	82.40%	92.60%	97.50%
<b>Mis-classification Rate</b>	17.60%	7.40%	2.50%
<b>F-Measure</b>	72.70%	92.10%	94.70%
<b>Test bias</b>	1.2	1.0267	90.00%
<b>Error odds ratio</b>	0.8	1.225	0.00%
<b>Diagnostic odds ratio</b>	20	160	NIL
<b>Discriminant Power</b>	1.7	2.8	NIL

Table VIII shows the performance results of the ECG, Fingerprint and Fusion of both Biometric Algorithms. The above table shows the values of performance parameters of the ECG and finger print images acquired from different acquisition system.

Prevalence is the proportion of a population found to have a condition. It is arrived by comparing the number of test cases found to have the condition with the total number of test cases studied and is usually expressed as a fraction, percentage or as the number of cases per 10,000 or 100,000 test cases.

Sensitivity measures the proportion of actual positives which are correctly identified as such and is complementary to the false negative rate. or  $\text{Sensitivity} = \text{TP} / (\text{TP} + \text{FN})$

False negative proportions is the proportion of negative tests among test cases with positive conditions. It is typically expressed as a conditional probability or a percentage.

The False Discovery Rate (FDR) of a set of predictions is the expected percent of false predictions in the set of predictions. or  $\text{FDR} = 1 - \text{PPV}$

Specificity measures the proportion of negatives which are correctly identified as such and is complementary to the false positive rate[14]. or  $\text{Specificity} = \text{TN} / (\text{FP} + \text{TN})$

False positive proportions refers to the false positive divided with false positive and true negative

False Omission Rate(FOR)=1-Negative Predictive Value

Youden's index=(Sensitivity Value + Specificity Value) – 1.

The positive and negative predictive values (PPV and NPV respectively) are the proportions of positive and negative results in statistics and diagnostic tests that are true positive and true negative results. or  $\text{PPV} = \text{TP} / (\text{TP} + \text{FP})$  and  $\text{NPV} = \text{TN} / (\text{FN} + \text{TN})$ . Positive likelihood ratio is the probability of a test case which has the condition testing positive divided by the probability of a test cases which does not have the condition testing positive. or  $\text{Positive Likelihood Ratio} = \text{True Positive Rate} / \text{False Positive Rate}$ . Negative likelihood ratio is the probability of a test case which has the condition testing negative divided by the probability of a test cases which does not have the condition testing negative. or  $\text{Negative Likelihood Ratio} = \text{FNR} / \text{FNR Accuracy} = \text{Number of TP} + \text{Number of TN}$  is divided with  $\text{Number of TP} + \text{FP} + \text{FN} + \text{TN}$ .

Misclassification rate says number of negative classification is divided with total number of classifications F-measure (or F1-score) is the measure of a Test's accuracy says 2 multiplied with true positive divided with 2 multiplied true positive and false positive, false negative.

## 6. CONCLUSION

The fusion of the acquired database of ECG and Fingerprint are performed. The FAR and FRR values are much better when compared to those of the separately analyzed databases. **This justifies that the fusion leads to better authentication with less error.** The proposed algorithm is developed for Biometric recognition using ECG and Fingerprint. **The samples for ECG and Fingerprint were acquired from different equipments. However, standalone equipment which can acquire both ECG and fingerprint would be helpful for easy acquisition. The future development could be the fusion of more Biometrics.** This becomes possible only when we acquire modalities from the same individual. Also the proposed algorithm can be developed by investigation of new features for ECG for comparison, making it more accurate.

**The future of the work presented in this paper is consideration of few more biometric traits and more biometric trait combinations for building robust and reliable recognition systems for individual identification Systems.**

## 7. REFERENCES

- [1] Manjunathswamy B E, Appaji M Abhishek, Thriveni J, K. R. Venugopal, L. M. Patnaik, "Multimodel Biometrics Using ECG and Fingerprint", International Conference on Advances in Communication Network and Computing-CNC, at Chennai, India, February 21-22, 2014.
- [2] Ming Li, Shrikanth Narayanan, "Robust ECG Biometrics by Fusing Temporal and Cepstral Information", International Conference on Pattern Recognition, 1051-4651/10 © 2010 IEEE.
- [3] Nahid Ghofrani, Reza Bostani, "Reliable Features for an ECG-based Biometric System", Proceedings of the 17th Iranian Conference of Biomedical Engineering

- (ICBME2010), 3-4 November 2010, 978-1-4244-7484-4/10 ©2010 IEEE.
- [4] David Pereira Coutinho, Ana L. N. Fred and M´ario A. T. Figueiredo, “One-Lead ECG-Based Personal Identification Using Ziv Merhav Cross Parsing”, 2010 International Conference on Pattern Recognition, 1051-4651/10 © 2010 IEEE.
  - [5] Ikenna Odinaka, Po-Hsiang Lai, Alan D. Kaplan, Joseph A. O’Sullivan, Erik J. Sirevaag, Sean D. Kristjansson, Amanda K. Sheffield and John W. Rohrbaugh, “ECG Biometrics: a robust short-time frequency analysis”, 978-1- 4244-9080-6/10 c 2009 IEEE.
  - [6] Chee-Ming Ting and Sh-Hussain Salleh, “ECG based personal identification using Extended Kalman Filter”, 10th International Conference on Information Science, Signal Processing and their Applications (ISSPA 2010), 978-1- 4244-7167-6/10 © IEEE, 2010.
  - [7] Yogendra Narain Singh, Sanjay Kumar Singh, Phalguni Gupta, “Fusion of electrocardiogram with unobtrusive biometrics: An efficient individual authentication system”, Pattern Recognition Letter, 2012.
  - [8] Fahim Sufi, Ibrahim Khalil and Abdun Mahmood, “Compressed ECG Biometric: A Fast, Secured and Efficient Method for Identification of CVD Patient”, J Med Syst (2011) 35:1349–1358, © Springer Science & Business Media, LLC 2009.
  - [9] A Wahib, S H Chin, E C Tan, “Novel Approach to Automated Fingerprint Recognition”, IEE Processing-Vis. Image Signal Processing, Vol. 145, No. 3, June 1998.
  - [10] FuFu Zeng, Kuo-Kun Tseng, Ming Zhao, Jeng-Shyang Pan, Huang-Nan Huang, Chih-Yu Hsu, Shuo-Tsung Chen, “Biometric Electrocardiogram Card for Access Control System”, Fifth International Conference on Genetic and Evolutionary Computing, IEEE, 2011.
  - [11] Tsu-Wang Shen, Shan-Chun Chang, Chih-Hsien Wang and Te-Chao Fang, “A Longitudinal and Cross-section Investigation on Peritoneal Dialysis Patients: Does the Cardiovascular Conditions Affect on ECG Biometrics?” 37: pp-497–500, Computing in Cardiology, 2010.
  - [12] Konstantinos N. Plataniotis, Dimitrios Hatzinakos and Jimmy K. M. Lee, “ECG Biometric Recognition Without Fiducial Detection”, IEEE Biometrics Symposium, 1 - 4244-0487-8/06, 2006.
  - [13] Anil K. Jain, Salil Prabhakar and Lin Hong, “A Multichannel Approach to Fingerprint Classification” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 21, no. 4, April 1999.
  - [14] <http://en.wikipedia.org/wiki?curid=30688232>