International Journal of Engineering &Technology, 7 (1.7) (2018) 47-50

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Multibiometric authentication with MATLAB simulation

P Selvarani[1]*, N Malarvizhi[2]

[1]Research Scholar, Department of Computer Science and Engineering, School of Computing,Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai-62, TamilNadu, India
[2]Professor, Department of Computer Science and Engineering, School of Computing,Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,Avadi, Chennai-62, TamilNadu, India
**Corresponding author E-mail: selvarani.meena@gmail.com*

Abstract

Multimodal Biometric Authentication has been used as more security purpose for establishing the user Identification, Authentication and Verification purpose. Multimodal Biometric like Fingerprint and iris are used in this research work for authentication purpose using Matlab simulation. Fingerprint recognition process like Image Enhancement, binarization, Segmentation, thinning, Minutia marking, and Matching are performed with various techniques like Histogram Equalization, Adaptive Binarization, Morphological operations, Minutiae based techniques etc.,Iris recognition process like Segmentation, Normalization, Encoding and Matching are performed with various techniques like Canny edge detection, Daughman's Rubber sheet model, Hamming Distance etc., can be applied for Fingerprint and iris recognition for authentication purpose. Finally Performance the measure of Precision, Recall, F-Score and Accuracy has evaluated in both fingerprint and iris. It can be concluded Iris Accuracy is higher 0.96% compared with fingerprint accuracy 0.81%.

Keywords: *Fingerprint Recognition; Iris Recognition; Precision; Recall; Fscore; Accuracy.*

1. Introduction

Biometric system is more reliable than password based system, becauseit is stable,Permanent, unchanged, not forgotten, stolen, do not share, distribute etc., The main advantage of biometric system is the person should be present at the time of Authentication.Nowadays biometric identification methods are widelyused in various sectors like Military, Government, ATM, working institutions, Banking sectors etc., Biometric system is used for Higher security purpose. [1]. Biometric system worked in identification and verification modes. Biometrics are used to Enhance thehigher Security purpose.

2. Fingerprint process

Capturing Fingerprint Image: Capturing Fingerprint image using fingerprint sensor like capacitance based or optical based sensor and it is stored in system database and derived the input image for further processing. (ii) Image Enhancement: The fingerprint image acquired from sensors or other media's are not assured for perfect quality due to noise. [2] To enhance the quality of the fingerprint image Histogram equalization and FFT technique has been used. Histogram Equalizations a strong technique and widely used for Image Enhancement which improve the quality of images like human viewing , removing noise, increasing contrast between ridges and valleys etc., in the fingerprint images. FFT is used to enhance the intensity of pixels of the fingerprint images and also improve the clarity of the ridges and valleys. FFT is used to divide the image into small processing blocks 32 by 32 pixels. The enhanced image after FFT removes some spurious connections between ridges. (iii) Image Binarization: Binarization is the process of converting a pixel image into a binary image. [3]. A Fingerprint-Image-Binarization transforms an 8-bit gray image to a1-bit binarized image, where 0-value holds for ridges and1-value for Valleys. [3] After the operation ridges are highlighted with black color while valleys are in white color. An adaptive binarization method is achieved to binarized the fingerprint image. (iv) Orientation Flow Estimation: Block direction estimation is used to extract the region of interest. [4].The direction of each block of the fingerprint image with W*W in size (W is 16 pixels by default) is estimated. (v) Region of Interest: ROI is useful to analyze the fingerprint image. Two morphological operations are used in ROI. (i) Open (ii) Close. (i) The Open operation can expand images and remove peaks introduced by background noise. (ii)The Close operation can shrink images and eliminate small cavities in the fingerprint image.[5] (vi) Thinning: The purpose of thinning stage is to gain the skeleton structure of the fingerprint image. Thinning reduces a binary image consisting ridges and valleys into a ridge map of unit width. [6] The thinned ridge map is then filtered by morphological operations to remove H Breaks, isolated points and spikes. (vii) Remove H Breaks and Spikes: The H breaks, isolated points, spikes are removed by morphological operations in the thinned ridge map. H break'-Remove H-connected foreground pixels. 'clean' – Remove isolated foreground pixels. 'spur' Remove spur spikes (viii) Minutia Marking: Minutia points marked on the image.[7] (Ridges, Valleys etc.,)(ix) Save & Match: Save the output of the fingerprint image and Finally Compare the two fingerprint image. If the two Finger print that are having same direction and position are identical should be verified.

Copyright © 2018P Selvarani, N Malarvizhi. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

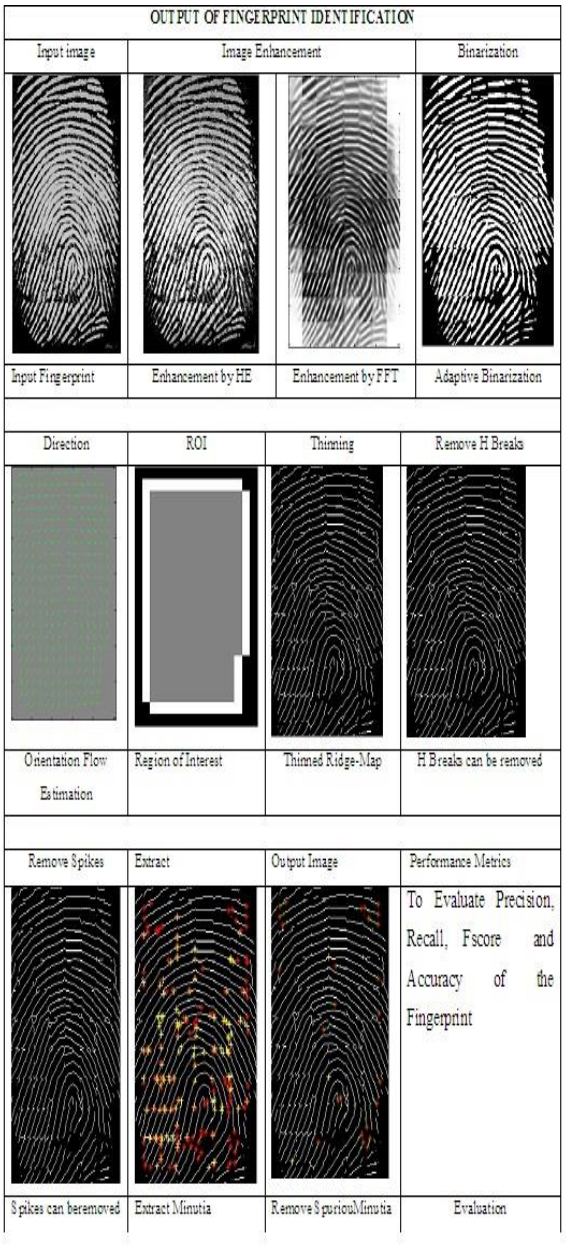
Table 1: Represents Fingerprint Techniques

Capturing Fingerprint image Fingerprint Sensor			
Fingerprint Process	Fingerprint Recognition	Method	Techniques
Pre Processing	Enhancement	Noise Detection	Histogram Equalization & FFT
	Binarization	Convert Binary	Adaptive Binarization
	Direction	Extract ROI	Open and Close Morphological Operation
	ROI	Construct/ Analyse	Morphological Operation
Feature Extraction	Thinning	Skeleton Structure	
	RemoveH Breaks and Spikes	RemoveH Breaks, Isolated Points and Spikes	
	Minutia Marking	Minutia points are marked	crossing Number Approach
Matching	Compared two Template	Verified same Positions are identical	Minutia based Techniques

Performance Metrics: The following parameters are considered for evaluating the performance of Fingerprint True Positive Rate, False Positive Rate, True Negative Rate and False Negative Rate. By calculating PR, FPR, TNR, FNR, to know about the performance of Table represents Precision, Recall, Forehand Accuracy of the Fingerprint.

Table 2: Description

TPR,TNR,FPR,FNR	Description
True positive Rate	A user registered in the database, puts finger on the scanner and a system recognize him
True Negative Rate	A user registered in the database, puts finger on the scanner and a system does not recognize him
False positive Rate	An unregistered in the database, puts finger on the scanner and a system recognize him
False negative Rate	A unregistered in the database, puts finger on the scanner and a system does not recognize him



Fingerprint – Performance Metrics

Evaluated by Precision, Recall, Fscore, Accuracy

Precision = 0.494070833333333 / 0.494070833333333 + 0.025100000000000

Precision = 1.025100000000000

Recall = True Positive / True Positive + False Negative

Recall = 0.494070833333333 / 0.494070833333333 + 0.163675000000000

Recall = 1.163675000000000

Fscore = Precision-recall / Precision + Recall

Fscore = 1.025100000000000 -1.163675000000000 / 1.025100000000000 + 1.163675000000000

Fscore= 1.053593066530094

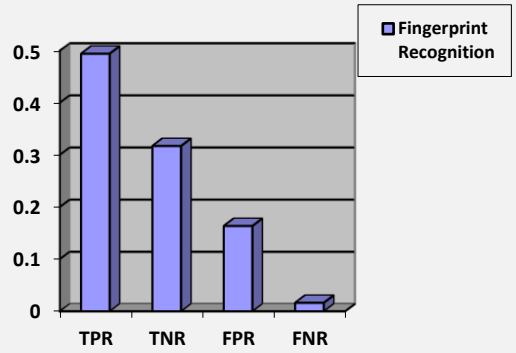
Accuracy = (True Positive + True Negative) / (True Positive + True Negative + False Positive + False Negative)

Accuracy = (0.494070833333333 + 0.317154166666667) / (0.494070833333333 +0.317154166666667 + 25100000000000+ 0.163675000000000)

Accuracy = 0.811225000000000

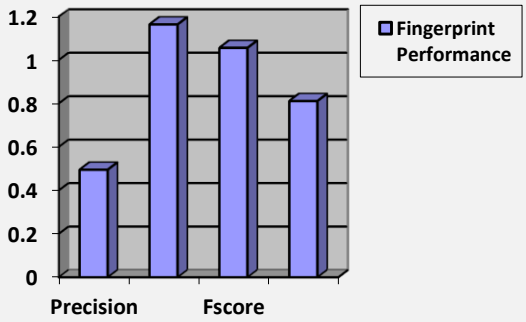
Table 3: Performance of Recall, Precision, Fscore and Accuracy

Fingerprint RecognitionTPR,FPR,TNR,FNR	
True Positive	0.494070833333333
True Negative	0.317154166666667
False Positive	0.025100000000000
False Negative	0.0163675000000000



Fingerprint Performance
Precision, Recall, Fscore, Accuracy

Precision	0.49407083333333
Recall	1.16367500000000
Fscore	1.05593066530094
Accuracy	081122500000000

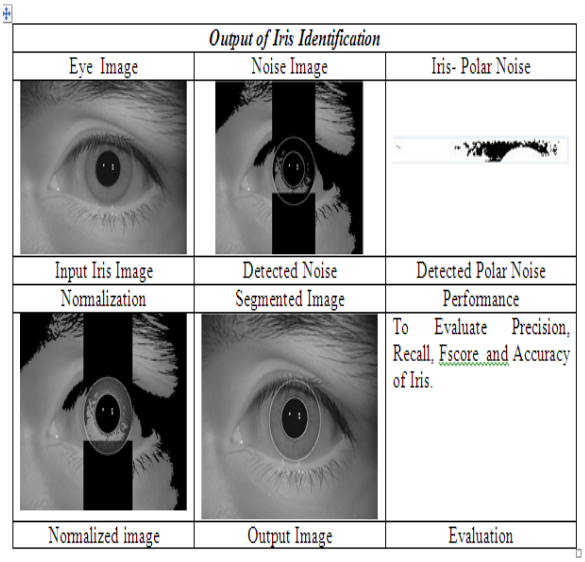


3. Iris process flow

Enrollment: Capturing Iris Image using iris sensor and it is stored in system database and derived the input image for further processing.[8]. the captured iris image include iris, pupil, sclera, eyelid, eyelashes etc., Eyelid eyelashes are the main noise factor on iris image. These noise factors can affect the accuracy of the iris image. To reducing the noise pre-processing techniques can be applied. Pre-processing is an important step in iris recognition. [9]. It consists segmentation. (ii) Segmentation: The information of eye is focused only on iris part and other part can be ignored using canny edge detection technique, for the purpose of iris accuracy.[10] Because of accurate boundaries are needed to normalize and match iris image with the database. (iii) Normalization: The image of iris is gathered by reducing the errors and a rectangular shape of segmented iris is produced.[11]The output of normalization technique is stored into the database into two forms. Pixel values and iris code. It prepares the segmented iris image for the encoding process. (iv) Encoding: Hamming Distance Technique is used for encoding purpose. Digital Iris codes generated and is stored in the database for matching system.[12]. (v)Matching: The matching is carried out by measuring the distance between two images of iris code. The following Table 4 describes Iris Techniques. and Figure 2 describes the output of Iris Key Generation. Table 2 Represents Iris Techniques.

Table 3.0: Iris Acquisition Techniques

Capturing IRIS image using IRIS Sensor			
IRIS Process Flow	Iris Recognition	Method	Techniques
Pre processing	Segmentation	Noise Detection	Canny Edge Detection
Feature Extraction	Normalization	Extract the IRIS Code	Daughman's Rubber Sheet Model
	Encoding	Generating Digital Iris Code	Hamming Distance
Matching	Matching	Match The Previous template	



Iris – Performance Evaluated by Precision, Recall, Fscore, Accuracy

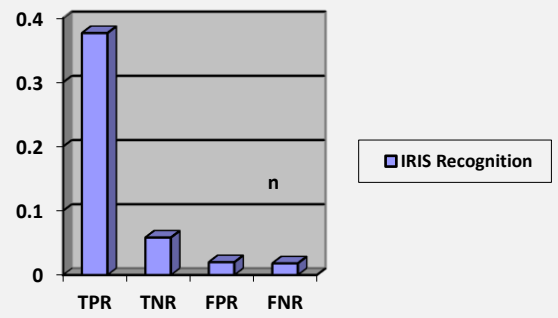
Recall = True Positive / True Positive + False Negative
Recall = 0.376866666666667 / 0.376866666666667 + 0.018216666666667
Recall = 0.953891584053997

Precision = True Positive / True Positive + False Positive
Precision = 0.376866666666667 / 0.376866666666667 + 0.020458333333333
Precision = 0.948509826128904

Fscore = Precision-recall / Precision + Recall
Fscore =0.948509826128904 0.953891584053997 / 0.948509826128904 + 0.953891584053997
Fscore = -0.002828928687861

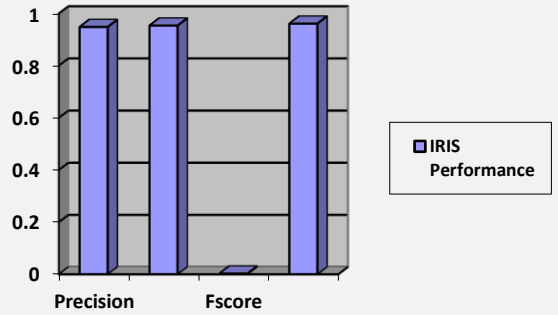
Accuracy = (True Positive + True Negative)/(True Positive + True Negative + False Positive + False Negative)
Accuracy= (0.376866666666667+0.584458333333333)/(0.376866666666667+0.5844583333333333 + 0.020458333333333+ 0.018216666666667)
Accuracy = 0.961325000000000

Iris Recognition TPR,TNR.FPR,FNR	
True Positive Rate	0.376866666666667
True Negative Rate	0.584458333333333
False Positive Rate	0.020458333333333
False Negative Rate	0.018216666666667

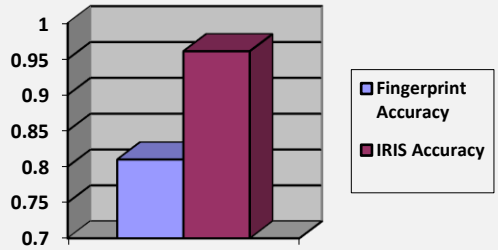


Iris Performance
Precision, Recall, Fscore, Accuracy

Precision	0.948509826128904
Recall	0.953891584053997
Fscore	0.002828928687861
Accuracy	0.961325000000000



Fingerprint Accuracy	0.81
IRIS Accuracy	0.96



4. Performance metrics of iris

The following parameters are considered for evaluating the performance ofIris. True Positive Rate, False Positive Rate, True Negative Rate and False Negative Rate.By calculating TPR, FPR, TNR, FNR, to know about the performance of Precision, Recall, Fscore and Accuracy of the Iris.

5. Conclusion

Multimodal biometric authentication has been used to enhance the ultimate security purpose. To avoid vulnerability, malicious intruder, unauthorized access etc., it is more reliable than current and established authentication methods.
In this research work finally compared the Accuracy of Fingerprint and iris. Iris Accuracy 0.96% is better than compared with fingerprint accuracy 0.81%. It can be work with MATLAB Simulation.

References

[1] A.K. Jain, P. Flynn, and A.A. Ross, eds., Handbook of Biometrics, Springer, 2007. J. Feng, “Combining Minutiae Descriptors for Fingerprint Matching,” Pattern Recognition, Jan. 2008, pp. 342-352.
[2] M. Kaur, J. Kaur, and J. Kaur, “Survey of contrast enhancement techniques based on histogram equalization”, International Journal of Advanced Computer Science and Applications, vol. 2, no. 7, (2011), pp. 137-141.https://doi.org/10.14569/IJACSA.2011.020721.
[3] O. D. Trier and T. Taxt, "Evaluation of Binarization Methods for Document Images," JEEE Transactions on Pattern Analysis and Machine lntelligence, VOL. 17, NO. 3. March 1995.
[4] Jiangyang Zhang, Rongjie Lai and C.-C. Jay Kuo. 2012. Latent Fingerprint Detection and Segmentation with a Directional Total Variation Model. IEEE.https://doi.org/10.1109/ICIP.2012.6467067.
[5] MuktiDubey and SandeepSahu,” Fingerprint Minutiae Extraction and Orientation Detection using ROI (Region of interest) for fingerprint matching, International Journal of Scientific & Engineering Research, Volume 5, Issue 1, January-2014 289 ISSN 2229-5518.
[6] Parul Mishra, Ajit Kumar Shrivastava,AmitSaxena,” Enhanced Thinning Based Finger Print Recognition”, International Journal on Cybernetics & Informatics (IJCI) Vol.2, No.2, April2013.
[7] Minutiae Detection Algorithm for Fingerprint Recognition”, IEEE AESS Systems Magazine, 2002.
[8] John Daugman, How iris recognition works, IEEE Trans. Circuits Syst. Video Techno. 14 (1) (2004), pp. 21–30.
[9] L. Masek, Recognition of Human Iris Patterns for Biometric Identification, University of Western Australia, 2003
[10] Segmentation Techniques for Iris Recognition System, International Journal of Scientific & Engineering Res V volvolume 2, Issue 4, April-2011 , ISSN 2229-5518 IJSER © @ 2011 by Surjeet Singh, .Kulbir Singh.
[11] PrateekVerma , MaheedharDubey , Praveen Verma, SomakBasu,” Daughman"S Algorithm Method For Iris Recognition-A Biometric Approach”, International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 6, June 2012).
[12] Hollingsworth Karen P., Bowyer Kevin W. (Dec. 2011),’ Improved Iris Recognition through Fusion of Hamming Distance and Fragile Bit Distance’, IEEE Transactions vol. 33, no. 12
[13] Powers, David M. W. (2003), Recall and Precision versus the Bookmaker, Proceedings of the International Conference on Cognitive Science (ICSC-2003), Sydney Australia, 2003, pp. 529-534.