ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940
www.ijasem.org
Vol 18, Issue 3, 2024

Hybrid Biometric Recognition System Using Fingerprint, Iris and Palmprint Biometric Traits with Feature Extraction Technique

Arvind K. Panpatte[1], Dr. S. D. Khamitkar[2], and Dr. H. S. Fadewar[3]

[1] Research Scholar,
[2] Professor, [3] Assistant Professor,
School of Computational Sciences, SRTM University, Nanded-M.H., India

Abstract. The growing demand for high-security and dependable authentication techniques prompted the creation of the unimodal biometric system, which gave rise to the hybrid or multimodal biometric system. For identification and security purposes, the hybrid or multimodal biometric system will employ more than one biometric attribute of a person.

In biometric systems, several fusion approaches are employed. When compared to other fusion approaches, feature extraction & score level fusion is the most often used. This paper discussed a hybrid model designed using hybrid or multimodal biometric. This model considered three biometric traits as like fingerprint, iris and palmprint with feature extraction technique extracted features of these biometric traits. And also, the compression techniques, feature extraction, probability density function, and feature level fusion for recognition of traits. Then the performance of our proposed system is evaluated by some performance metrices as like FAR, FRR & EER. In order to implement our proposed system, we have used the MATLAB platform. Finally, this paper is beneficial for giving security to the digital transactions and executing more than one human physiological features in the platform's security.

Keywords: Hybrid Biometric System, Fingerprint, Iris, Palmprint, Feature Extraction, Fusion

1 Introduction

Biometrics is the practice of recognizing individuals based on their behavioral or physical characteristics. Biometric technologies are used to identify individual (human) physiological or behavioral attributes such as a fingerprint, voice, signature, retina, face, iris, finger vein, hand or palm, and its vein pattern. There is no need to carry any document ID while using biometric identification, as biometric technology employs unique bodily qualities to identify people. The biometric technology identifies the "live sample" rather than the standard PIN (Personal Identification Number), ID cards, passwords, or any other document.

As a result, biometric credentials cannot be anticipated, misplaced, forgotten, or easily copied. Preprocessing is the process of entering data into a biometric system, such as a video, picture, or signal, and then the biometric identification system performs diagnosis or recognizing, which involves extracting the method of interest from the input. Preprocessing includes the elimination of noise, correct data alignment, and data refining.

Some aspects are extracted from previously processed data and examined for biometric recognition systems. The biometric recognition system performs identification using input data or verification using input data pertaining to the same identity. Biometric systems are often unimodal, manipulating a single biometric signal and hence may encounter issues owing to missing information or poor data quality. Multiple biometric features are used in this manner to increase the accuracy of the recognition system.

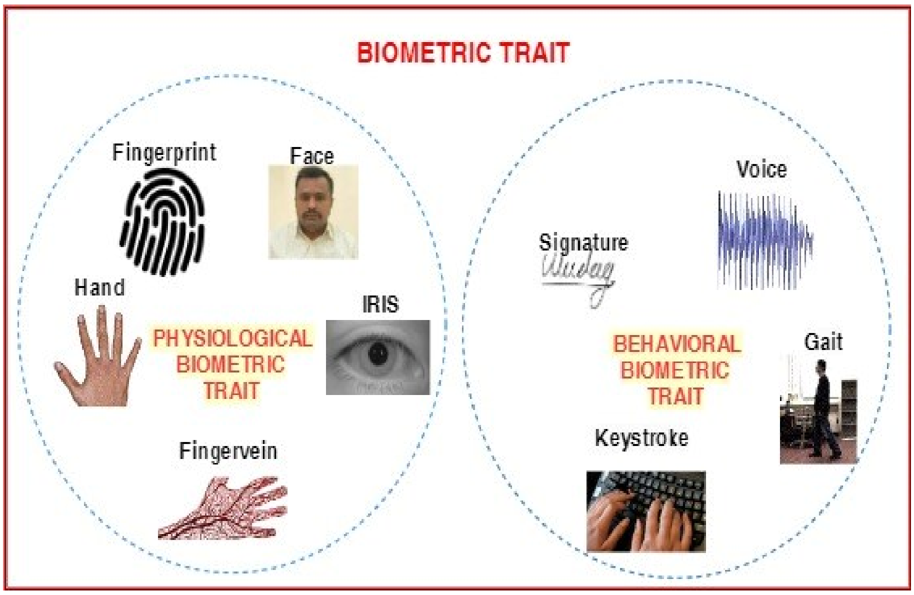


Fig. 1. Biometric Trait [1]

2 Literature Review

Madasu Hanmandlu et al. [2] the suggested t-norm based score level fusion method can also handle any number of modalities and datasets.

Anil Jain et al. [3] used three different biometric traits and imitate the operational environment on a small dataset and explored different fusion levels.

R. Alvarez Marino et al [4] they introduced a crypto-biometric approach for hiding and recovering a secret that makes use of a user's iris template and a fuzzy extractor. Also utilized many parameters sets to investigate and determine which one delivers the best outcomes in terms of inter- and intra-user variability.

Wencheng Yang et al [5] presented an alignment-free bio-cryptosystem based on modified VNSs. By employing rotation- and translation-invariant feature representations generated from modified VNSs, the proposed technique eliminates the need for fingerprint pre-alignment.

B. Prasanalakshmi et al [6] three biometric traits of a person, with the concept that if one fails, the other trait can be used for verification or identity. Furthermore, a cryptosystem notion is included, in which one of the biometric qualities - the palm vein itself - functions as a key to access the stored template database.

Punam Bedi et.al [7] this work presents an effective multimodal biometric image watermarking strategy based on Particle Swarm Optimization (PSO) for concealing a fingerprint picture along with certain demographic data in the associated face image.

Vishi, K. et al [8] primarily interested in the combination of iris and fingerprint biometrics and their possible application as biometric IDs. Three score normalization procedures are used to integrate the individual comparison scores received from the iris and fingerprints at the score level.

According to the above literature review, utilizing different levels of fusion biometric recognition rates can be raised, and there isn't much work done in multilevel fusion using the combination of fingerprint, iris, and palmprint for standard data sets.

Table 1. Survey on existing Biometric methods

Author's	Used Biometric traits	Used Techniques & Algorithms	Dataset	Methods & Classification Accuracy
A. Jain, L. Hong, Y. Kulkarni (1999)	Face, Fingerprint & Speech	Minutia, Eigen Face, HMM & LPC	Created own dataset	Decision level fusion

Madasu Hanmandlu, Jyotsana Grover, Ankit Gureja, H.M. Gupta (2011)	Palmprint, Hand vein & Hand geometry	Frant t-norm	IITD PolyU XM@VTS	Score level
R. Alvarez Marino et.al (2012)	Iris	Fuzzy extractor	CASIA Iris Database	FAR=4.42%, FRR=9.67%, GAR=90.33%
Wencheng Yang et.al (2014)	Fingerprint	A Delunay Quadrangle authentication method and a Unique Topology code	FVC2000, FVC2002, FVC2004	FAR=0.1%, FRR=2%, EER=1.07%
S. Veluchamy, L.R. Karlmarx (2017)	Finger vein & Finger knuckle	Repeated line tracking, Multi-SVM with FFF Optimization	IIT Delhi, SDUMAL-HMT	FAR=5%, FRR=5%, EER=0.35%, Accuracy=95%
Padma Polash Paul et.al., (2013)	Face, Signature & Ear	Social Network Analysis & FLDA (Fisher Linear Discriminant Analysis)	FERET, VIDTIMIT, AT&T, USTB I, USTB II	FAR=5%
Padma Polash Paul et.al., (2014)	Face & Ear	Random Projection Matrix Feature Fusion,	FERET, VIDTIMIT, AT&T, USTB I, USTB II	Accuracy=96%
B. Prasanalakshmi, A. Kannammal (2012)	Face, Fingerprint & Palm vein	Feature Extraction, Key generation	FVC2000	EER: 25%, FAR:25%, FRR:25%, GAR:75%
Punam Bedi et.al, (2012)	Face & Fingerprint	Particle Swarm Optimization	FVC 2004 DB1, Indian Face Database	PSNR (Peak Signal Noise Ratio), NC (Normalized Correlation) & SSIM (Structural Similarity Index)
Vishi, K., & Yayilgan, S. Y. (2013)	Fingerprint & Iris	Score level fusion	CASIA-Iris Lamp, SDUMLA-HMT	EER = 3.30%

3 Databases

Datasets of a fingerprint used are FVC2004 DB1 standard database. The DB1 database is 120 fingers broad and has 12 samples for each finger. The samples of FVC2004 database is in ".tif" format. Data sets of iris used are Multimedia University (MMU) Iris standard database. Five iris images of left & right side with different position of each individual are considered. A total of 80 samples are used.

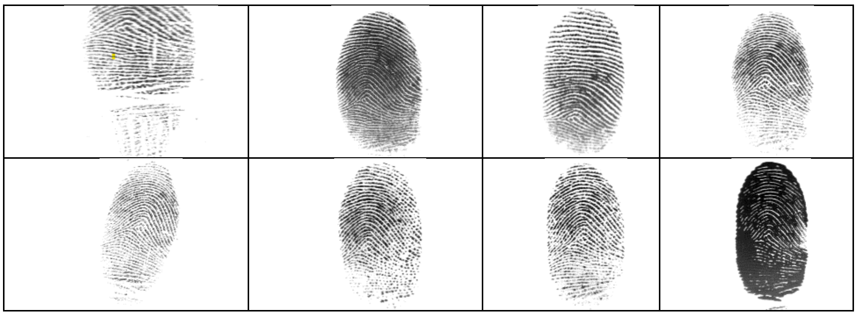


Fig. 2. FVC2004 DB1 Standard Fingerprint databases samples

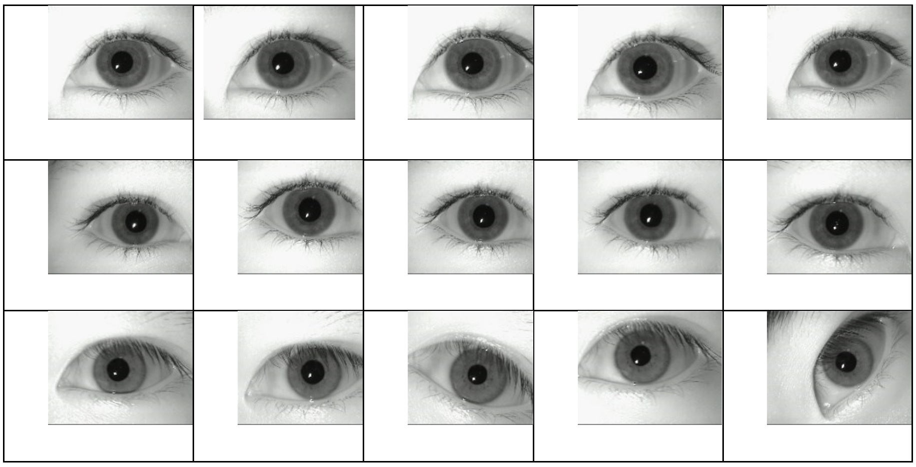


Fig. 3. MMU standard iris database samples

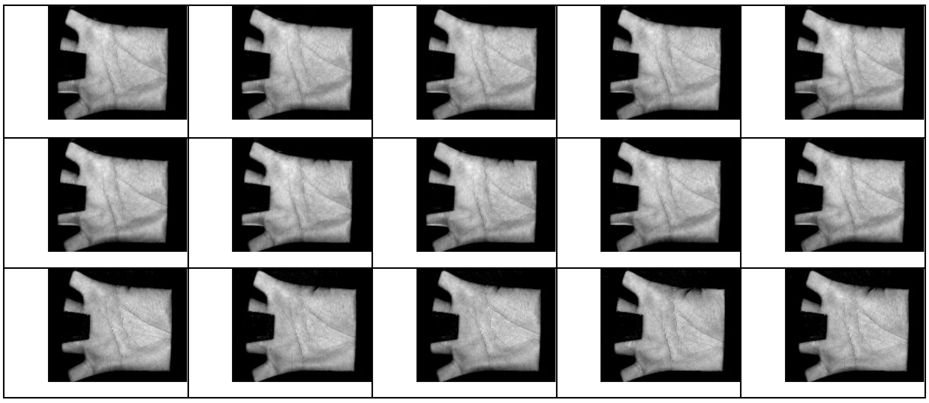


Fig. 4. PloyU standard palmprint database samples

Data sets of palmprint used are PolyU Palmprint standard database. A total of 100 samples are used. Data sets images are in ".bmp" format shown in figure 3 and 4.

4 Proposed Methodology

In this research work fingerprint, iris and palmprint, Biometric standard data sets are used. The challenges of a unimodal biometric system, such as reduced accuracy and user acceptability, are recognized by hybrid biometric systems. In this context, a feature-transition-based coding technique is presented for addressing the under-explored problem of developing a biometric-based authentication system that integrates the fingerprint, iris, and palmprint modalities. The approach is based on capturing binary transitions of symmetric and asymmetric Gabor filtered images at all pixel places [13]. Feature-level fusion is utilized to combine the individual fingerprint, iris, and palmprint performances.

The FVC, CASIA, and POLYU databases are used as benchmarks for fingerprint, iris, and palmprint experiments. To evaluate performance, Receiver operator characteristics (ROC) curves and other measurements such as equal error rate (EER) and area under ROC curves (AUC) are utilized.

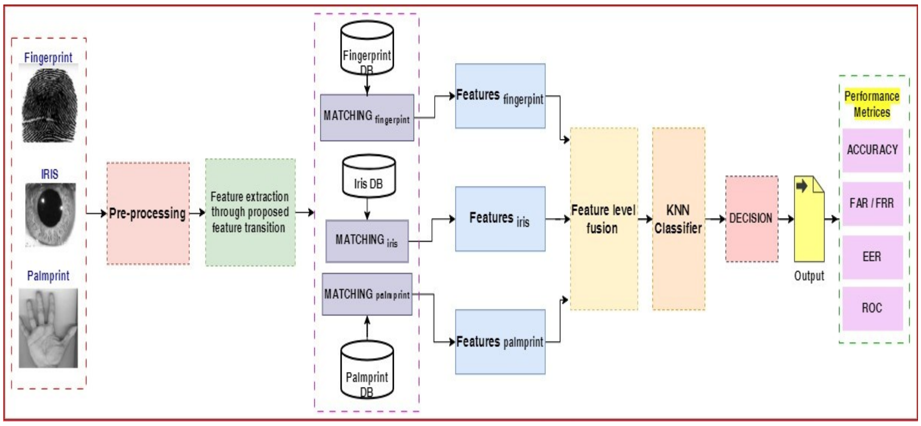


Fig. 5. Block Diagram of Hybrid Biometric System

A comprehensive comparison with numerous state-of-the-art methodologies is provided to validate the utility of the proposed strategy. A hybrid biometric system is being developed by providing an efficient feature representation technique capable of extracting important properties from fingerprint, iris, and palmprint images. The overall block diagram for the concerned hybrid biometric system is depicted in Figure 5. This example shows how to use a single feature extraction strategy for fingerprint, iris, and palmprint identification. This approach utilizes the complementary information of real and imaginary Gabor responses by concatenating the zero-crossings of these answers into a single vector.

Following that, for each pixel point, a binary string is scanned throughout the dimension of concatenation, and all 0-1 and 1-0 transitions are counted and stored in a bit-transition matrix. The feature-transition codes are then created by encoding matrix elements. The matching procedure is used to calculate the genuine and imposter scores after creating the corresponding codes for the fingerprint, iris, and palmprint databases. The below shows the proposed algorithm of hybrid biometric system.

- STEP I: The fingerprint, iris and palmprint images are acquired as the input from the stored database of concerned biometric trait.
- STEP II: After acquisition of biometric trait images, the pre-processing is performed on that image as like binarization, thinning, enhancement, edging etc. of image is performed.
- STEP III: After that Feature Extraction through proposed feature transition is performed on concerned biometric traits to obtain minutiae point, ridges end points, the canny, Laplacian of gaussian, Prewitt and thresholding to produce an edge map.
- STEP IV: Each biometric trait is matching with their preloaded template in biometric trait database. Then the feature value is generated of individual biometric trait.
- STEP V: In this step the feature level fusion through product rule is performed of all given biometric trait as like fingerprint, iris & palmprint. Then after KNN classifier is used for classification of fusion feature value and perform the decision.
- STEP VI: Finally, the system measures the performance metrics as like accuracy, FAR/FRR, EER and ROC.

5 Experimental Results

The ROC Curve of fingerprint, iris and palmprint are shown in figure 6, where experiments are observed using feature extraction and score level fusion techniques.

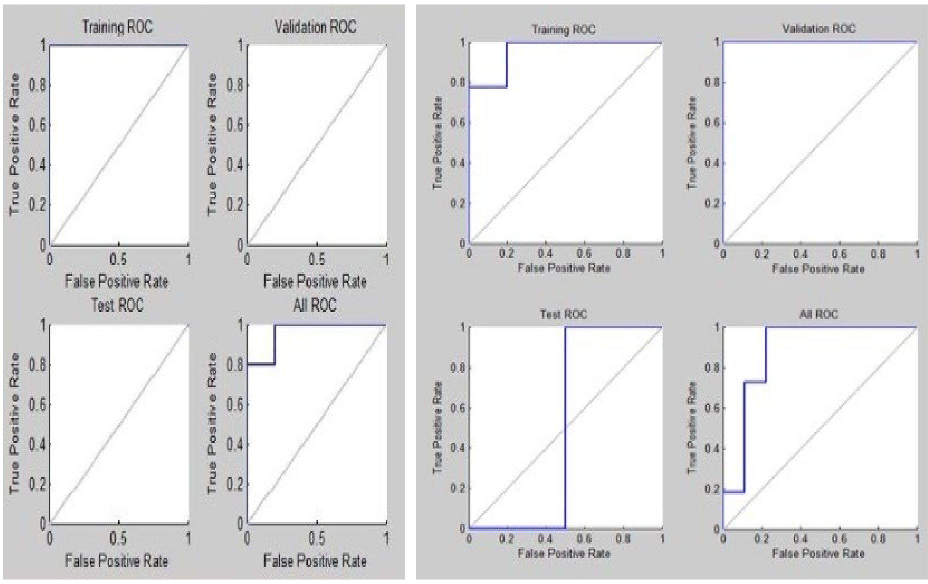


Fig. 6. ROC Curve of Fingerprint, Iris and Palmprint

The three models were designed and explored, in first model only fingerprint biometric is used, for minutiae extraction performed using classification with neural network technique. The model second and third used iris and palmprint recognition respectively, they observed feature extraction with boundary contour vector, MSE (Mean Square Erro) & PSNR (Peak Signal to Noise Ratio) with neural network and finally the classification of these hybrid recognition system is performed and observed the results.

From the Table 2, it has been observed that recognition accuracy with the unimodal experiments with applying feature extraction & score level fusion technique.

Table 2. Recognition Accuracy

Sr.No.	Biometric Trait	FAR%	FRR%
1	Fingerprint	1.12	5.02
2	Iris	1.08	5.2
3	Palmprint	1.28	5.04
4	Hybrid System	0.3	0.5

From the figure 7, we can observe that the analysis of recognition accuracy with the unimodal and hybrid system.

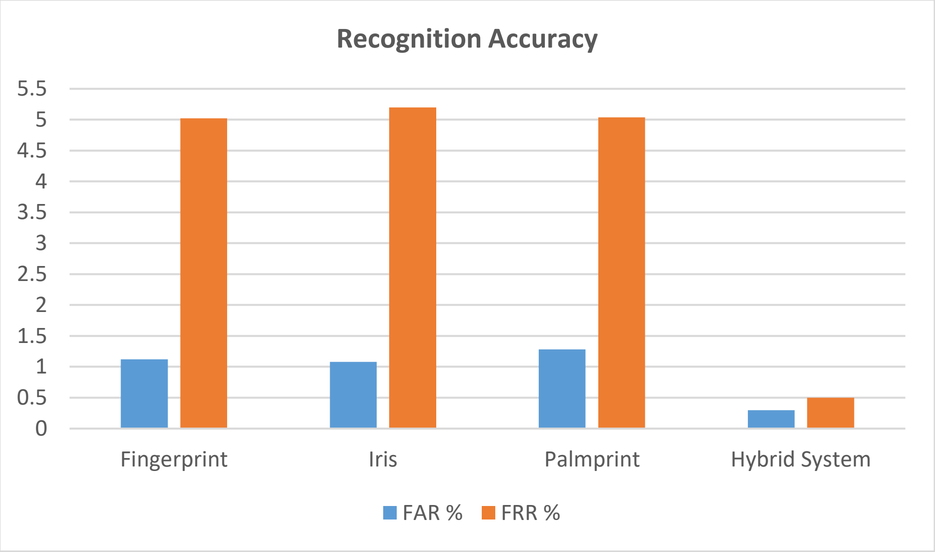
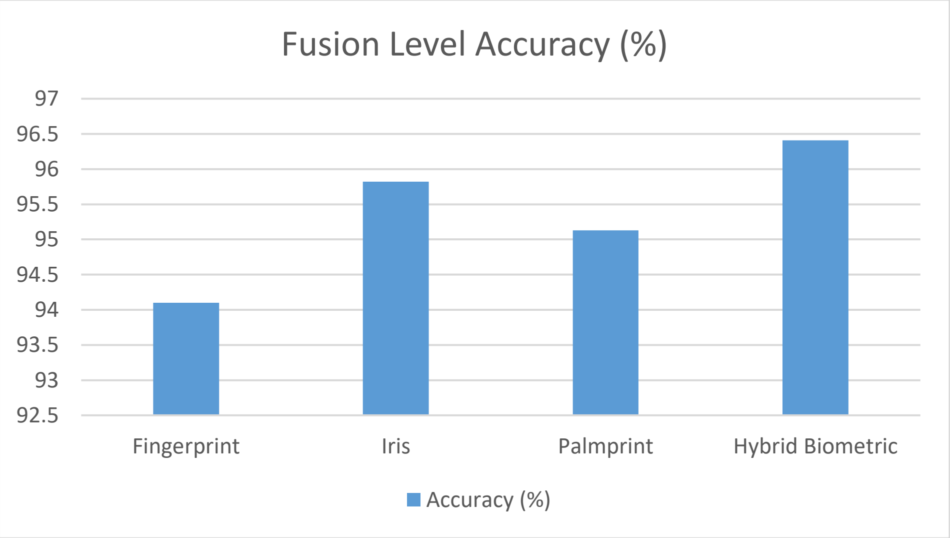


Fig. 7. Analysis of Recognition Accuracy

The Table 3, shows the experiments results of hybrid biometric with the fusion level accuracy.

Table 3. The Accuracy of Fusion level is tested in experiments

Sr.No.	Biometric Trait	Algorithm	Database	Accuracy %
1	Fingerprint	Minutiae Extraction with Neural Network	FVC2002, FVC2004 & LOCALDB	94.10
2	Iris	Feature Extraction with boundary contour vector, MSC & PNSR	CASIA & MMU	95.82



		with Neural Network		
3	Palmprint	Feature Extraction and classification with Neural Network	CASIA & PolyU	95.13
4	Hybrid Biometric (Fingerprint+Iris+ Palmprint)	Minutiae Extraction + Haar Wavelet + Feature Extraction with Neural Network	FVC+CASIA+PolyU	96.41

Fig. 8. Analysis of Accuracy Fusion level is tested in experiments

As a result, before matching, the fingerprint image must be pre-processed. This method's purpose is to provide a more accurate and enhanced fingerprint image. The goal of automated fingerprint matching is to safely extract the minutiae from binary fingerprint images gathered. There are various methods for collecting fingerprint minutiae. Using a neural network, the proposed system achieved 94.10% accuracy for fingerprint identification system rate. In the subject of biometrics for human identification, iris recognition is becoming increasingly significant.

The accuracy of the iris recognition system is 95.82%, with FAR and FRR of 3.9% and 4.9%, respectively. Following that, the rate of palmprint recognition system using neural network is 95.13%, with FAR and FRR of 1.28% and 5.04%, respectively. The Haar Wavelet Coefficient, according to the data, gives excellent accuracy and competence.

6 Conclusion

In this work, three biometric traits are used, named as fingerprint, iris and palmprint. All these biometric traits are considered from the standard databases, fingerprint data sets from FVC2004, iris data sets from MMU and palmprint data sets from PolyU. In this work, the hybrid biometric identification system based on fusion has grown into a weakness in determining the system's genuine security. Several options have been proposed to integrate a variety of approaches in a unique system termed Biometric Fusion in order to partially or completely address these problems.

The identification rate of hybrid biometric approaches based on fingerprint, iris, and palmprint is 96.41%, with FAR and FRR of 0.3% and 0.5%, respectively. This method is also based on score level fusion with a neural network methodology.

References

1. I. M. Alsaadi.: Physiological Biometric Authentication System Advantages, Disadvantages & future development: A review. International Journal of Scientific & Technology Research, vol.4, pp. 285-289(2015).
2. Madasu Hanmandlu, Jyotsana Grover, Ankit Gureja, H.M. Gupta.: Score level fusion of multimodal biometrics using triangular norms. Pattern Recognition Letters, 32(14), 1843-1850 (2011).
3. Jain, Anil K., Lin Hong, and Yatin Kulkarni.: A multimodal biometric system using fingerprint, face and speech. 2nd Int'l Conf. AVBPA. Vol. 10 (1999).
4. R. Alvarez Marino, F. Hernandez Alvarez, L. Hernandez Encinas.: A crypto-biometric scheme based on iris-templates with fuzzy extractor. Information Sciences, 195, 91-102 (2012).
5. Wencheng Yang, Jiankun Hu, Song Wang, Milos Stojmenovic.: An alignment-free fingerprint bio-cryptosystem based on modified Voronoi neighbor structures. Pattern Recognition 47, 1309-1320 (2014).

6. B. Prasanalakshmi, A. Kannammal, B. Gomathi, K. Deepa, R. Sridevi.: Biometric Cryptosystem Involving Two Traits And Palm Vein As Key. International Conference on Communication Technology and System Design, Procedia Eng. 30, 303-310 (2012).
7. Punam Bedi, Roli Bansal, Priti Sehgal.: Multimodal Biometric Authentication using PSO based Watermarking. Procedia Technology 4, 612-618 (2012).
8. Vishi, K., & Yayilgan, S.Y.: Multimodal Biometric Authentication using Fingerprint and Iris Recognition in Identity Management. 2013 Ninth International Conference on Intelligent Informatiion Hiding and Multimedia Signal Processing, 334-341. 10.1109/IIH-MSP.2013.91 (2013).
9. S. Veluchamy, L.R. Karmarx.: System for multimodal biometric recognition based finger knuckle and finger vein using feature-level fusion and k-support vector machine classifier. The Institution of Engineering and Technology, vol.6 Iss. 3, pp. 232-242. 10.1049/iet-bmt.2016.0112 (2017).
10. Padma P. Paul, Marina L. Gavrilova.: Cancelable Fusion of Face and Ear for Secure Multi-Biometric Template. 80 International Journal of Cognitive Informatics and Natural Intelligence, 7(3), 80-94. 10.4018/ijcini.2013070105(2013).
11. Padma P. Paul, Marina L. Gavrilova.: Cancelable Biometric Using Cancelable Feature Fusion. 2014 International Conference on Cyberworlds, 279-284. 10.1109/CW.2014.4 (2014).
12. D. Bhattacharyya R. Ranjan, F.A. a, and M. Choi.: “Biometric Authentication: A Review”, Int. J. Serv. Sci. Technol., vol.2, no.3, pp. 13-28 (2009).
13. Zhang D, Kong W. K., You J., Wong M.: Online Palmprint Identification. IEEE Trans Pattern And Mach Intell, 25(9), 1041-1050 (2003).
14. Feifei CUI, Gongping YANG.: Score Level Fusion of Fingerprint and Finger Vein Recognition. Journal of Computational Information Systems 7(16), 5723-5731 (2011).
15. Sanjekar. P. S and Patil. J. B. An Overview of Multimodal Biometrics. Signal & Image Processing: An International Journal (SIPIJ), 4(1), 57-64. 10.5121/sipij.2013.4105 (2013).
16. Anil K. Jain, Arun Ross.: Multibiometric systems. Communications of ACM, 47(1), 34-40 (2004).
17. Arun Ross and Anil Jain.: Information Fusion in Biometrics. Elsevier: Pattern Recognition Letters, 24, 2115-2125 (2003).
18. Anil K. Jain, Arun Ross, and Salil Prabhakar.: An Introduction to Biometric Recognition. IEEE Transactions on circuits and systems for video technology,14(1), 4-20 (2004).
19. Anne M.P. Canuto, Fernando Pintro, Joao C. Xavier-Junior.: Investigating fusion approaches in multi-biometric cancellable recognition. Elsevier Journal on Expert Systems with Applications, 40, 1971-1980 (2013).
20. Anil K. Jain, Karthik Nandakumar and Abhishek Nagar.: Biometric Template Security. EURASIP Journal on Advances in Signal Processing,2008. 10.1155/2008/579416.