IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12476

A SECURE MULTIMODAL BIOMETRIC SYSTEM

Dr. M. Ezhilarasan [1],

Mr. Srinivasan.P[2] , Mr. Sujit Swain[3], Mr. Thiruvikram.V[4], Mr.Vishal.SK[5]

Professor, Information Technology, Puducherry Technological University, Puducherry, India[1]

B. Tech Student, Information Technology, Puducherry Technological University, Puducherry, India[2-5]

Abstract: Biometrics has developed to be one of the most relevant technologies used in Information Technology (IT) security. Uni - Biometric systems have issues such as noisy data, non-universality, spoof attacks and unacceptable error rate. These issues can be solved by making use of multimodal biometric systems. Multimodal biometric systems utilize two or more individual traits, like face, iris, retina and fingerprint. It has higher recognition accuracy than uni-modal methods. In this system, two uni-modal biometrics, fingerprint and face are used as multi-biometrics. Decision-level fusion of these two modalities can enhance the overall performance of biometric systems. In this context, the aim of this paper is to provide a comprehensive review of the state-of-the-art methods and techniques for face and fingerprint decision-level fusion. The paper discusses the challenges and benefits of fusing these two modalities, along with a critical analysis of the existing methods. Various decision-level fusion approaches, including score-level fusion, feature-level fusion, and classifier-level fusion, are described in detail. The paper also discusses the performance evaluation of face and fingerprint decision-level fusion systems and provides insights into the future research directions in this area. The findings of this review suggest that decision-level fusion of face and fingerprint biometric modalities is a promising approach for enhancing the overall performance of biometric systems.

Keywords: Fingerprint-recognition, Face-recognition, Multimodal Biometrics, Python, OpenCV

I. INTRODUCTION

Biometric system uses the psychological characteristics and behavioural characteristics such as finger print, face, palm print, palm print and iris for person identification and verification. Multimodal Biometric system uses multiple physical or behavioural characteristics for person's identification. Multimodal Biometric uses different levels of fusion. The advantage of decision level fusion in face and fingerprint fusion is that it can reduce the error rates associated with each individual biometric modality, as well as reduce the effects of variations in environmental conditions, such as lighting and angle of capture. This is because the combination of multiple biometric modalities provides a more robust and reliable identification system.

II. MOTIVATION

- The motivation behind face and fingerprint fusion using decision level fusion is to address the limitations of individual biometric modalities and improve the accuracy and reliability of biometric identification systems.

- Facial recognition and fingerprint recognition systems have both been widely used in various applications, including law enforcement, access control, and financial transactions. However, they each have limitations that can affect their accuracy and reliability, such as variations in lighting and pose for facial recognition, and damage or contamination of fingerprints.

- By combining the strengths of both modalities, face and fingerprint fusion using decision level fusion can provide a more robust and reliable identification system that is less susceptible to errors and variations in environmental conditions. Decision level fusion allows for the combination of multiple sources of information to arrive at a final decision, which can improve the accuracy and confidence of identification decisions.

III. LITERATURE SURVEY

[1] Journal on Face and Fingerprint recognizing multimodal biometrics system, IEEE-2022: Improving authentication and Secure access

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023
DOI: 10.17148/IJARCCE.2023.12476

[2] Performance of Multimodal Biometric Systems Using Face and Fingerprints, IEEE-2022: Identity management

[3] journal on Multi-modal Biometric System for Face and Fingerprint using Convolutional Neural Network, IEEE-2021: Biometric data registration by facial recognition in the check-in process

[4] Online Smart Voting System Using Biometrics Based Facial and Fingerprint Detection on Image Processing and CNN, IEEE - 2021: Improved authentication using CNN

IV. LIMITATIONS IN EXISTING SYSTEM

1. Fingerprint:

- *Variability in fingerprint patterns:* Fingerprint patterns can vary significantly across individuals, and even across different fingers of the same individual.

- *False negatives:* Fingerprint recognition systems can also produce false negatives, i.e., not identifying someone correctly.

2. **Face Recognition:**

- Diversity in faces: Face recognition systems can have difficulty recognizing individuals with non-standard facial features, such as those with darker skin tones, or facial hair.

- Accuracy: Face recognition systems may not always be accurate, particularly if the system has not been properly trained or calibrated.

- Different Face Angles Can Throw Off Facial Recognition's Reliability

V. PROPOSED SYSTEM

In this section, we propose a multimodal biometric system of Face and fingerprint by integrating the information at decision level fusion technique. Initially, features are extracted from both face and fingerprint of a person and are individually studied for their identification accuracies. Later, the fusion of the biometric traits is recommended at decision level fusion.

Fingerprint Recognition:

i.Database:

Fingerprint comparison is a biometric authentication method that uses unique characteristics of an individual's fingerprints to verify their identity. The FVC2004 database is a benchmark database for evaluating fingerprint verification algorithms, consisting of four different datasets: DB1A, DB1B, DB2A, and DB2B. DB2A and DB2B contain fingerprint images from 100 different individuals, with 8 images per finger, and were collected using a high-quality optical scanner.

The FVC2004 database is widely used in research and development of fingerprint recognition algorithms due to its large size, variety of fingerprint images, and well-defined evaluation protocols. The performance of fingerprint comparison algorithms is typically measured using metrics such as the false acceptance rate (FAR), false rejection rate (FRR), and receiver operating characteristic (ROC) curves.

ii.Fingerprint Matching:

The fingerprint recognition system uses minutiae-based matching. This approach is based on the idea that the unique features of a fingerprint can be represented by the location and orientation of minutiae points, which are the locations where the ridges of the fingerprint end or bifurcate.

The novelty lies in its implementation of the minutiae-based matching approach. The system uses several image processing techniques, such as Gaussian blurring, Canny edge detection, and contour analysis, to extract the minutiae points from the fingerprint images. It then computes a similarity score between the reference fingerprint and other fingerprints in a given folder, based on the number of matching minutiae points.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12476

Face Recognition:

i.Database:

Face recognition is a technology that uses computer algorithms to identify and verify the identity of a person based on their facial features. It has various applications, such as security systems, access control, and personalized advertising.

When it comes to a college student photo database, face recognition technology can be used to streamline processes such as attendance taking and campus security. By using a database of student photos, the technology can identify and verify the identity of students as they enter various campus facilities or attend classes.

ii.Face Recognition:

The face recognition system uses a combination of algorithms for face detection and recognition. The face recognition library is used for face detection and recognition, which itself uses deep learning algorithms to extract facial features and compare them with the known faces to recognize the person. Specifically, the face recognition library uses a pre-trained Convolutional Neural Network (CNN) to extract 128-d facial embeddings from the input images, and then compares these embeddings with the embeddings of known faces using Euclidean distance or other distance metrics to recognize the person.

For face detection, the face recognition library uses Histogram of Oriented Gradients (HOG) features and a linear classifier to detect faces in the input image. It also uses a pre-trained deep learning model called Single Shot Detector (SSD) to detect faces in some cases.

Decision-Level Fusion:

Decision-level fusion is a simple averaging fusion rule for fingerprint and face biometric data. This approach is novel in the sense that it can significantly improve the accuracy and robustness of biometric systems.

Integration of multiple biometric modalities: By combining the matching scores from two different biometric modalities (i.e., face and fingerprint), the decision-level fusion approach can provide better accuracy and robustness compared to using a single biometric modality. This is particularly useful for applications where computational complexity and speed are important factors.

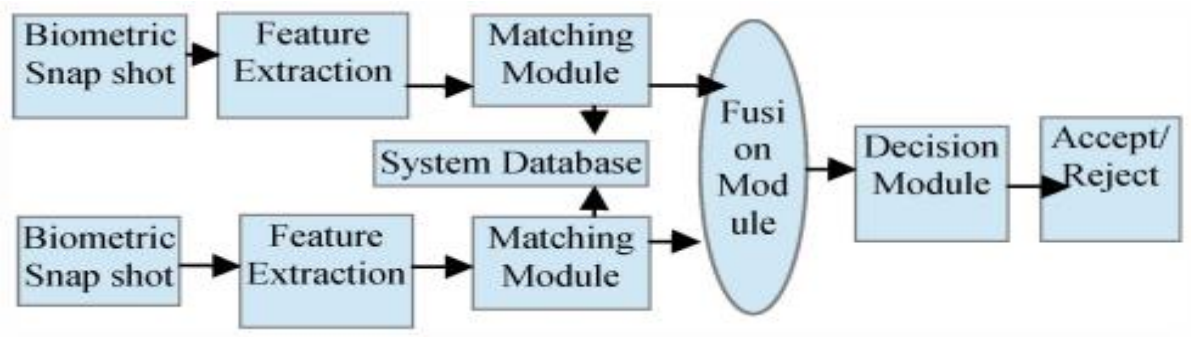

Fig:1 Decision-level fusion model

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12476

VI. DESIGN DIAGRAM FOR PROPOSED SYSTEM

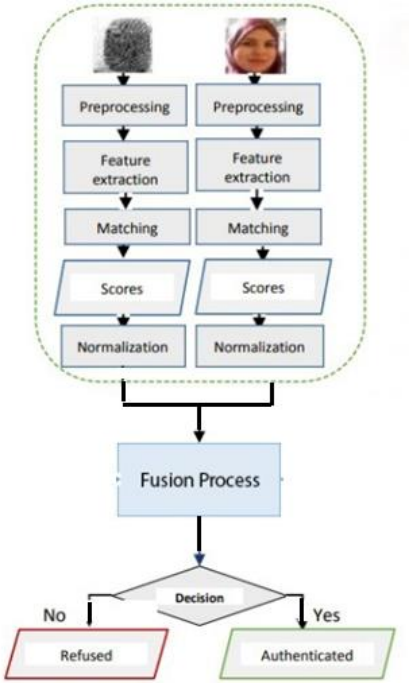

Fig:2 Proposed fusion model

VII. EXPERIMENTAL RESULTS:

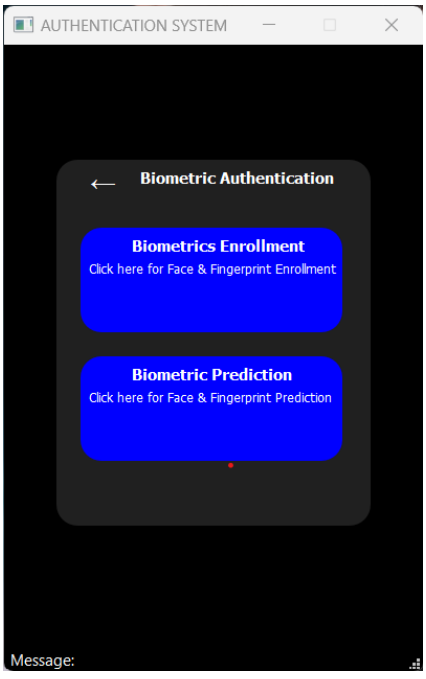

Fig:3 Enrolment and Prediction

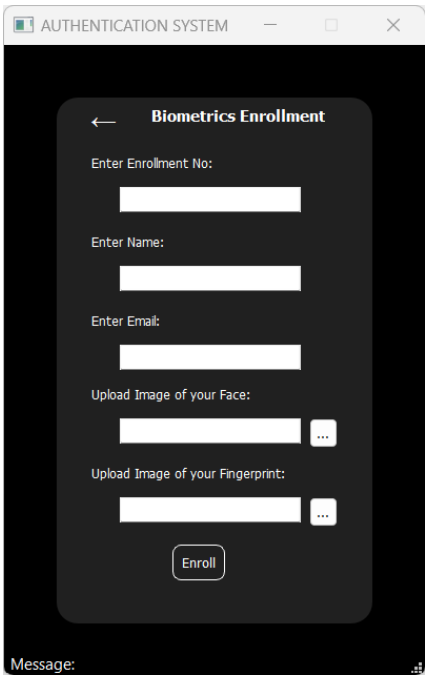

Fig:4 Get details from the user

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12476

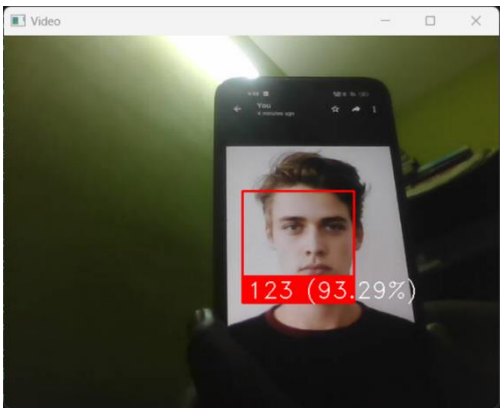

Fig:5 Face recognition with accuracy

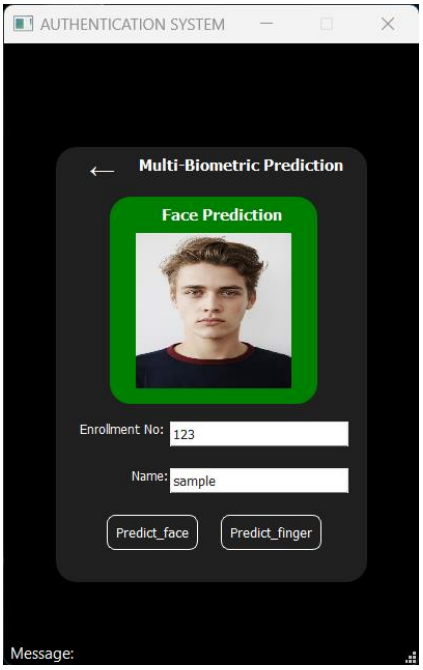

Fig:6 Result of face recognition

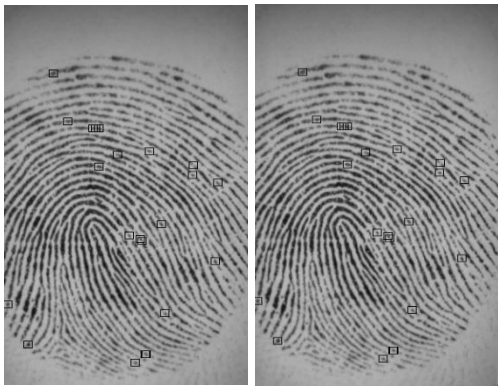

Fig:7 Fingerprint matching with match-points

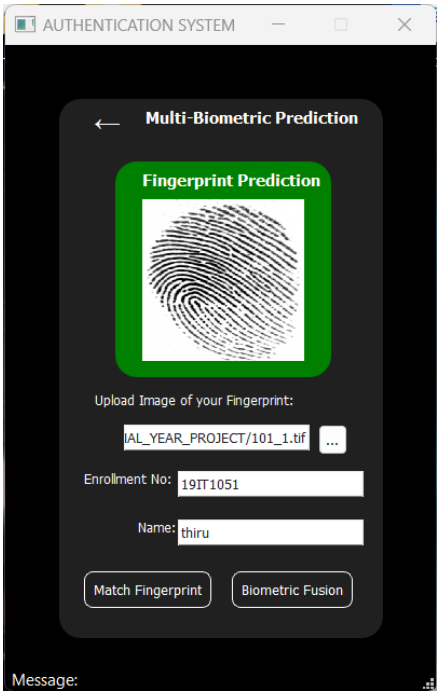

Fig:8 Result of fingerprint recognition

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12476

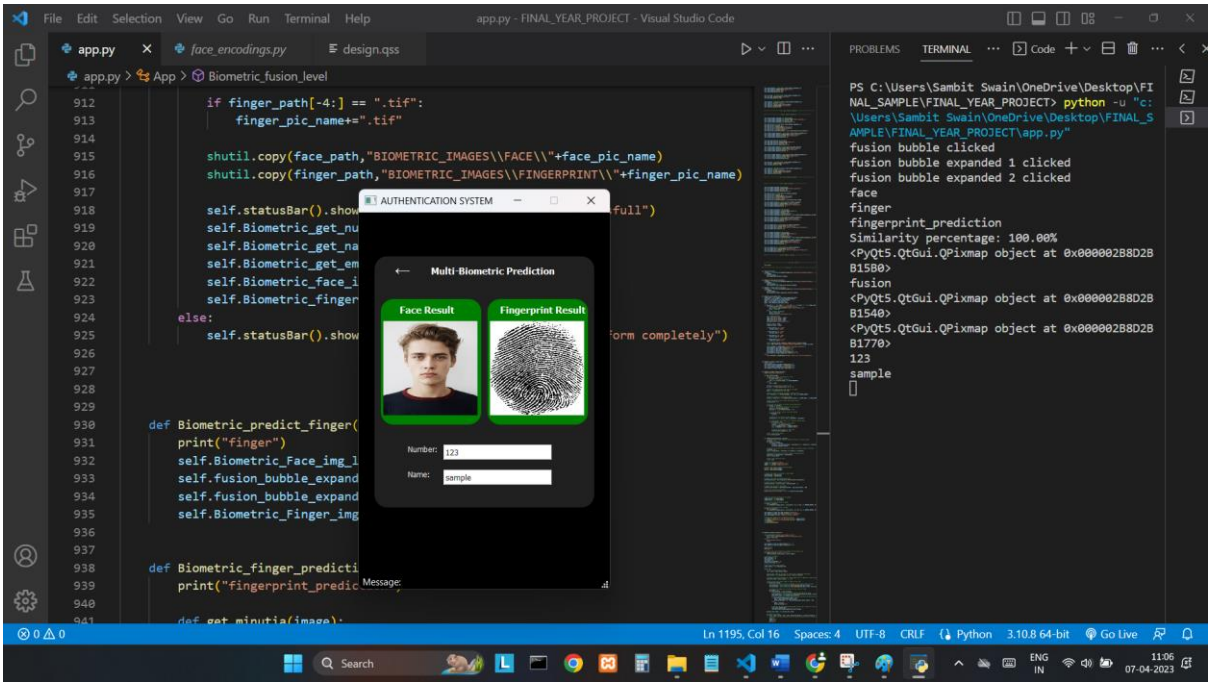

Fig:9 Final result of the prediction

VIII. CONCLUSION

Face and fingerprint fusion using decision level fusion is a promising approach for improving the accuracy and reliability of biometric identification systems. By combining the strengths of both facial and fingerprint recognition technologies, decision level fusion can provide a more robust and secure system that is less susceptible to errors and variations in environmental conditions. Decision level fusion allows for the integration of multiple sources of information to make a final decision, which can improve the accuracy and confidence of identification decisions. This approach can also provide a higher level of security, as it is more difficult for an unauthorized person to spoof or manipulate both facial and fingerprint features simultaneously. However, there are also challenges associated with decision level fusion, such as the need to ensure that the decision rules are well-defined and appropriately weighted, and the potential for increased complexity and processing time. Therefore, it is important to carefully evaluate the performance and feasibility of face and fingerprint fusion using decision level fusion, and to ensure that it meets the required accuracy, speed, and security standards for various applications and industries. Overall, face and fingerprint fusion using decision level fusion has the potential to revolutionize biometric identification systems and provide a more secure and reliable way to verify an individual's identity.

REFERENCES

[1] Jain A. K., Ross A., & Pankanti S., “Biometrics: A tool for information security”. IEEE Transactions on Information Forensics and Security, 2022, 125-143.

[2] Boucetta Aldjia, Boussaad Leila, “Sensor Level Fusion for Multi-modal Biometric Identification using Deep Learning”. Institute of Electrical and Electronics Engineers (IEEE). September, 2021

[3] G. Parziale and A. Niel. “A fingerprint matching using minutiae triangulation”. Proceedings of ICBA, pp. 241–248, 2021.

[4] A. Meraoumia, S. Citroub and A. Bouridane, “Multimodal biometric person recognition system based on fingerprint and finger knuckle print using Correlation filter classifier”, IEEE International conference on communications, pp. 820-824, 2022.

[5] Md. Maruf Monwar & Marina, L. Gavrilova, (2021). Multimodal biometric system using score-level fusion approach. IEEE Transactions on Systems, Man, and Cybernetics—Part B: Cybernetics, Vol. 39, No. 4, pp. 867- 878.

[6] Conti V. Militello. C. Sorbello, F. & vitabile S., “A frequency-based appro based approach for features fusion in fingerprint and iris multimodal biometric identification systems IEEE Transactions on Systems, Man, and Cybernetics—Part C: Applications and Reviews, Vol. 40, No. 4, pp. 384-395.

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.12476

[7] Zewail, R., Elsafi, A., Saeb, M. and Hamdy, N., 2020, July. "Soft and hard biometrics fusion for improved identity verification". In The 47th Midwest Symposium on Circuits and Systems. MWSCAS'04. (Vol. 1, pp. I-225). IEEE.

[8] Abhimanyu Kumar.,Lalita Verma.,Tarushi Singh.,2022, "Introduction to Multimodal Biometrics using OpenCV "2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), IEEE