Author's version of the accepted version to IEEE CAMAD Oct. 2021

PERFORMANCE OF MULTIMODAL BIOMETRIC SYSTEMS USING FACE AND FINGERPRINTS (SHORT SURVEY)

Mohamed Abdul-Al[*1], George Kumi Kyeremeh[1], Naser Ojaroudi Parchin [1], Raed A Abd-Alhameed[1], Rami Qahwaji[1], and Jonathan Rodriguez[2]

[1] Faculty of Engineering and Informatics, University of Bradford, Bradford BD7 1DP, UK
[2] Instituto de Telecomunicações, Aveiro, Portugal

[*]m.abdul.al@bradford.ac.uk, g.k.kyeremeh@bradford.ac.uk, n.OjaroudiParchin@bradford.ac.uk, r.a.a.abd@bradford.ac.uk, r.s.r.qahwaji@bradford.ac.uk, and jonathan@av.it.pt

Abstract— Biometric authentication is the science and engineering of assessing and evaluating bioinformatics from the human body in order to increase system security by providing reliable and accurate behaviors and classifiers for personal identification and authentication. Its solutions are widely used in industries, governments, and the military. This paper reviews the multimodal biometric systems that integrated both faces and fingerprints as well as shows which one has the best accuracy and hardware complexity with the methods and databases. Several methods have been used in multimodal biometric systems such as KNN (K-Nearest Neighbor), CNN (Convolutional Neural Network), PCA (Principal Component Analysis), and so on. A multimodal biometric system for face and fingerprints that uses an FoM (Figure of Merit) to compare and show between the articles the best accuracy that have used multimodal biometric system face and fingerprints methods. The best performance has been found is 99.43% by using the cascade multimodal method.

Keywords— Multimodal, Biometric, Face, Fingerprint, CNN, KNN, PCA, LDA, Cascade multimodal, accuracy, loss, and FoM

I. INTRODUCTION

The need for a biometric system has grown dramatically in the last two decades. Biometric recognition is necessary to differentiate one person from another by utilizing quantifiable behavioral for instance signature, voice, keyboard, and so on, or morphological for example face, iris, fingerprint, finger vein, and so on traits [1]. These qualities include being less vulnerable to authentication being lost or forgotten. It could It is utilized for personal investigation, immigration and naturalization services, protecting access to systems or private possessions, enabling anonymous interactions, and so on [2].

Because of their uniqueness and invariance to each person, FPs (Fingerprints) have been an important biometric characteristic. Because the obtaining equipment is very tiny, this biometric approach seems to be more widely utilized and accepted by individuals. Furthermore, the accuracy performance is quite good in comparison to several other biometric recognition systems based on the iris, retina, ear shape, and so on [3].
A biometric recognition technique that uses information about human face features to identify or verify people is called FR (Face Recognition). FR methods are sensitive to fluctuations in facial features and accessories, as well as uncontrolled lighting and postures. In this sense, people and machine intelligence performance on facial recognition is a study issue with both broad practical potential and scientific research value [4].
Biometric technologies may be utilized in three various cases, depending on their features and functions:

- Unimodal systems
- Multimodal systems
- Cascade or serial systems

Several security features have previously been created that employ the multimodal fusion approach to improve efficiency and resilience versus spoofing and fraudulent operations.
The fusion is conducted on several distinct characteristics at various stages in all techniques, which has certain drawbacks [5]. All obtainable biometric must be merged, which enhances verification time and improved reliability. As a result, combining cascade with the multimodal system can provide a good balance of efficiency, difficulty, and evaluation time. To address the limitations of a system, focus on a particular biometric modality, a multibiometric system improves resilience

and efficiency versus imposter attacks and environmental changes. This system is divided into multi-modal, multi-sensor, multi-instance, multi-algorithm, and hybrid systems [6].
Multimodal biometric systems are categorized into two categories:

- Parallel multimodal systems
- Serial multimodal systems

A serial multimodal system provides sequential verification, which means that if the previous biometric feature is approved, the next one is verified. A parallel multimodal system, on the other hand, conducts continuous verification, and the degree of correlation is calculated by aggregating all matches of every feature [7].
A recognition accuracy system is made up of four major components that are involved in the identification and verification method [6]:

1. Biometric sensors are utilized to gather real-world users' biometric features and transform them into raw data in digital form.
2. During the registration phase, the extractor sub-part extracts some of the essential discriminating traits to generate succinct representations known as "templates" as distinct biometric features.
3. After that, the biometric template is stored in a data center. This is referred to as the identifying procedure.
4. Even during the operating stage, the system will determine whether a person's condition is unknown or even if the user is fake or real.

To confirm that the individual is a genuine person, the extraction of the features model is validated to the saved template database.

This paper aims to review multimodal biometric systems that integrated both faces and fingerprints as well as to show which one has the best accuracy and hardware complexity with the methods and databases. The paper is arranged as follows: Section 2 will review related work from 2017 to 2021 in brief. All the methods of this paper will be in Section 3. The results and discussion for those methods will be in Section 4, and Section 5 will have limitations and section 6 will have a conclusion.

II. RELATED WORD

In the last 2 decades, there has been a great deal of experimenting in multimodal biometric systems. The creation of an effective fusion strategy, that is required to integrate data provided by different data scientists, is important for successful multimodal biometric systems [8].
In multimodal biometric systems, biometric proof may be merged at many levels. The fusion may be classified into various major groups: - According to identifying fusion, fusion happens before biometric identification. This contains the fusion levels: - feature level fusion and sensor level. Fusing occurs following the fusion of personal features after matching fusion. This comprises the following fusion levels: rank level fusion, match decision level fusion, and score level fusion that can gives good accuracy between 92 and 96%, for more information details you can find it in [9-17].
The Gabor Wigner transform [18] was utilized as a discrete wavelet transform, and an optimization algorithm was used to find the ascending characteristics, leading to a low FAR (False Acceptance Rate) and the accuracy ranges between 90 to 99.4% it depends on the techniques that have been used. Another way for reducing mistake rates utilizing a unique image multimodal biometric methodology [19] offers visibility into facial identification as well as has a good accuracy of around 87%. The SVM (Support Vector Machine) [20] was built with generalization capabilities and machine learning, resulting in better accuracy in facial images. A complete multibiometric database [21] was examined utilizing unmatched equipment and different imaging settings. Nevertheless, with the introduction of the smartphone as an important component, a bimodal identification system [22] was created.
In [23] proposed a multibiometric system with iris, fingerprint, and face recognition that makes use of several streams of modality-specific CNNs (Convolutional Neural Networks). This method has considerable complexity in the multimodal recognition system, which also lowers its acceptance in many domains. Also, it has high accuracy and the ranges of accuracy are between 86 to 99% it depends on the methods the authors used. A multibiometric system is based on finger vein, fingerprint, iris, face, and so on was also explored in [6]. In [24] suggested technique uses a multibiometric detection system that combines facial pictures, fingerprints, and finger-vein with CNNs architectures and algorithms based on RF (Random Forest) Softmax.
In [24] proposed fuse fingerprints and faces and apply a fuzzy approach at the decision level. When compared with previous fusion approaches, this multimodal method offers higher accuracy. In [25] presented a novel multibiometric system that combines facial and fingerprint recognition. Local binary patterns) are utilized to extract facial characteristics, while the C.N. (Crossing Number) approach is utilized to extract fingerprint ridge ends and bifurcations. In [26] investigate several approaches for combining information gathered from diverse biometric characteristics. The work sheds light on alternative system designs associated with the integration of biometric systems, including unimodal and multimodal. Different potential evaluation criteria and benchmarks

are also thoroughly analyzed. When implementing various biometric systems, [27] employ the Ant Colony Optimization method to select parameters which including decision threshold.

The studies indicate below using a variety of feature extraction approaches, including SURF (Speeded up powerful highlights), PCA (Primary Component Analysis), numerous other quantitative features, and SIFT (Scale Invariant Highlight Transform). Other researchers have been used IDMN (Inverse Difference Moment Normalized), LBP (Local Binary Pattern), GLCM (Gray-Level Co-Occurrence Matrix), minutiae feature extraction, and HOG (Histogram of Oriented Gradient).

The majority of the studies [28, 29] have developed a fusion-level method for decision-making at the authentication step for parallel multi-biometric systems. Machine and deep learning has also been effectively employed in the development of fusion-level methods for parallel multibiometric systems [30-33].

To ease the aforementioned issues, this work aims to propose an FoM (Figure of Merit) that can reduce the loss for the multimodal biometric systems for face and fingerprint recognition systems as well as decrease the time.

III. Methodology and Database for multimodal biometric systems for face and fingerprint recognition

To get FP matching scores, the FP recognition software compares the input FP to the FP template contained in the database. FR is in charge of comparing the input FP to the template recorded in the database. In [17], the authors have used SIFT algorithm for FP and FR as well as they used the k-d tree search algorithm serves as the foundation for the BBF (Best Bin First) algorithm. The K-d tree allows for the storage of higher dimensional spaces so that bins in feature space are searched in ascending order from the query point, returning the KNN and PCA and a very close neighbor for a significant proportion of queries.

The FP database was produced from the FVC (Fingerprint Verification Competition) 2004 and is divided into four datasets: DB1, DB2, DB3, and DB4. Each dataset has eight separate photos and ten different individuals, for a total of 400 pictures across all datasets. The dataset was then separated into two categories: testing data and training data [34]. 94 face was used to generate the FP datasets. The datasets were then separated into two categories: testing data and model construction [35].

In [23], the authors comprise several CNN-based modality-dedicated networks and a shared expression level that are collaboratively optimized. The modality-specific images are compared to extract modality-specific characteristics at various abstract layers, and the combined description is taught to evaluate and apply interdependence across multiple methods as well as they look towards combining multi-stream CNN architectures.

Furthermore, this work [23] is used the BioCop database [36]. This dataset is the only one that enables discontinuous multimodal fusion testing and training at different scales. The BioCop database was compiled over four years: 2008, 2009, 2012, and 2013. Voice, hand geometry, face, iris, fingerprint, palm print, and soft biometrics are included in every label for every participant. Moreover, another database that has been used in this work is the BIOMDATA datasets [37] is a difficult dataset to use when some of the picture examples are degraded by shadows, noise, blur, occlusion, and sensor [38]. This dataset includes biometric modalities such as the face, fingerprint, palm print, iris, voice, and hand geometry from people of various ethnicities, genders, and ages.

In [39], the authors are used a DCD-WR (Deep Contourlet Derivative Weighted Rank) framework is created utilizing human face and fingerprint characteristics. The DCD-WR architecture is primarily concerned with the fusion of fingerprint and facial authentication utilizing deep weighted rank level fusion. Also, this work provides a new extracting feature in the sequential region utilizing CNT (Contourlet Transform). However, this CNT creates smooth picture outlines. Moreover, the researchers have been used three different methods as LDTP (Local Derivative Ternary Pattern), DCA (Discriminant Correlation Analysis), LR-JSR (Low-Rank and Joint Sparse Representations) and MDCA (Multiset Discriminant Correlation Analysis) to extract features from face and fingerprint. Furthermore, they have used benchmark/real database as well as CASIA Biometric Ideal Test database.

In [1], the researchers have used six methods at two different levels. In the first level, they were using passed to thinning, Gabor filter, and binarized methods. While in the second level they were using CNN, LBP, and HOG are used to identify and extract feature characteristics from facial pictures. Furthermore, they have used 2 types of databases for face and fingerprint. The AR face database [40] and the FCV-2004 public database [41].

In [42], the researchers have used a hybrid method including three different techniques such as RF (Random Forest), CNN and Softmax considered being a process of multimodal biometric face and fingerprints recognition. Furthermore, the database that has been used is SDUMLA-HMT datasets [43] which contain an actual multimodal biometric database of the face and fingerprint pictures.

In [44], the authors are used a hybrid method integrating cascaded and fusion-based multimodal biometric frameworks employing fingerprint and facial characteristics. Furthermore, this hybrid method is used on a self-created dataset of approximately 450 facial pictures and 450 fingerprints.

Table 1 summarizes all the methods that have been used in multimodal biometric systems for face and fingerprints from 2017 to 2021 with their databases.

Table 1: Summarizes all the methods in multimodal biometric systems for face and fingerprints with database.

References	Methods	Database
[17]	KNN and PCA	FVC-2004
[23]	CNN, KNN, PCA, LDA, DCA, CCA, MDCA and SVM	BioCop database, and BIOMDATA datasets
[39]	DCD-WR, CNT, LDTP, DCA, LR-JSR and MDCA	benchmark/real database, and CASIA Biometric Ideal Test database
[1]	passed to thinning, gabor filter, binarized, CNN, LBP, and HOG	AR face database, and FVC-2004 public database
[42]	RF, CNN, and Softmax	SDUMLA-HMT datasets
[44]	hybrid integrating cascaded and fusion-based multi-biometric	Hybrid is used on a self-created dataset

IV. RESULT AND DISCUSSION

The suggested algorithms are evaluated in comparison to previously published studies in multimodal biometric systems for face and fingerprint. Table 2 represents the accuracy, loss, hardware complexity for all the methods that have been used in the articles that talk about multimodal biometric systems for face and fingerprints. For each parameter, merit was assigned in which the accuracy value is set to 100 percent, and the loss value is set to (loss/accuracy) x 100. For every approach, the average percentage for Figure of Merit (FoM) was determined. The average percentage for FoM of [1] has the best accuracy (99.43%)by using a cascade multimodal algorithm. Moreover, the hardware complexity is low which generates an approvable solution for multimodal biometric systems for face and fingerprints. However, the hardware complexity is high for [23] and [42]. Despite the fact that the given methodology in this study ranks third in terms of the average percentage of merit, it beats the other four strategies in [23] and [42] in terms of loss, accuracy, and hardware complexity, forming an outstanding accuracy with the methods that have been utilized.

Table 2: Summarizes all the methods with the accuracy and hardware complexity in all articles that have been used multimodal biometric systems for face and fingerprints.

Ref	Method	Accuracy	Loss	Average Percentage for Figure of Merit (FoM)	Hardware Complexity
[17]	KNN and PCA	92.5%	7.5%	8.10%	N/A
[23]	SVM-Major	89.27%	10.73 %	12.01%	N/A
[23]	KNN + Serial + PCA	86.28%	13.72 %	15.90%	N/A
[23]	KNN + Serial + LDA	91.28%	8.72%	9.55%	N/A
[23]	KNN + Parallel + PCA	88.12%	11.88 %	13.48%	N/A
[23]	KNN + Parallel + LDA	93.21%	6.79%	7.28%	N/A
[23]	KNN + CCA + PCA	95.27%	4.73%	4.96%	N/A
[23]	KNN + CCA + LDA	95.41%	4.59%	4.81%	N/A
[23]	KNN + MDCA/ DCA	96.36%	3.64%	3.77%	N/A
[23]	CNN-Major	97.70%	2.3%	2.35%	N/A
[23]	CNN-Sum	98.85%	1.15%	1.16%	N/A
[23]	Weighted feature fusion	99.03%	0.97%	**0.97%**	N/A
[23]	Multi-abstract fusion	99.16%	0.84%	**0.84%**	N/A
[39]	LR-JSR	70%	30%	42.85%	N/A
[39]	DCA	79%	21%	26.58%	N/A
[39]	DCD-WR	96%	4%	4.16%	N/A
[1]	Cascade Multimodal	99.43%	0.57%	**0.57%**	**Low**
[1]	Cascade Multimodal and AND Rule	96.28%	3.72%	3.86%	Low
[42]	RF, CNN, and Softmax With Weighted sum	99.30%	0.7%	**0.70%**	**High**
[42]	RF, CNN, and Softmax With Weighted product	99.28%	0.72%	**0.72%**	**High**

[44]	Threshold = 0.48, 0.51, and 0.54	98%	2%	2.04%	Medium

V. Limitations

There are many limitations to the articles that have been presented above. In [17] the authors compared unimodal and multimodal for face and fingerprint recognition using the KNN method with an accuracy of 92.5% which means that the method that has been used is good but it needs more to improve the accuracy better. While in [23] suggested a multi virtual network to address the spatial mismatch issue while sacrificing no quality and reducing network parameters significantly. However, Utilizing real-world data, [39] discovered that multimodal biometric identification framework reduced computing time and complexity when compared to existing biometric recognition approaches. Nevertheless, in [1] multimodal biometrics integrates multiple independent biometric modalities and overcomes the constraints of single-modality systems including intra-class differences, inter-class similarities, spoof attacks, non-universality, and noise in sensed data. Although, in [42] the disadvantages of this method include the inability to merge incompatible feature sets such as minutiae points of fingerprints and Eigen-coefficients of face, the difficulty in predicting the optimum fusion technique given a circumstance. Despite this, several security solutions have previously been created that employ the multimodal fusion approach to improve performance and resilience versus spoofing and fraudulent attacks. The fusion is conducted on several distinct characteristics at different levels in all techniques, which has certain drawbacks [5].

VI. Conclusion

This survey has proposed a multimodal biometric system for face and fingerprints that uses a figure of merit (FoM) to compare between the articles that used multimodal biometric system (Face and Fingerprints) methods, and which one has the minimum loss that means it has the best accuracy as well as representing the hardware complexity. As we found that the best loss has the best accuracy with low hardware complexity by using a cascade multimodal biometric system.

Acknowledgment

This project has received funding from the European Union's Horizon-MSCA-RISE-2019-2023, Marie Skłodowska-Curie, Research and Innovation Staff Exchange (RISE), titled: Secure and Wireless Multimodal Biometric Scanning Device for Passenger Verification Targeting Land and Sea Border Control.

References

[1] R. A. El mehdi Cherrat and H. Bouzahir, "A multimodal biometric identification system based on cascade advanced of fingerprint, fingervein and face images," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 18, no. 1, pp. 1562-1570, 2020.

[2] E. M. Cherrat, R. Alaoui, H. Bouzahir, and W. Jenkal, "High density salt-and-pepper noise suppression using adaptive dual threshold decision based algorithm in fingerprint images," 2017: IEEE, pp. 1-4.

[3] S. R. Borra, G. J. Reddy, and E. S. Reddy, "An Efficient Fingerprint Identification using Neural Network and BAT Algorithm," *International Journal of Electrical & Computer Engineering (2088-8708),* vol. 8, no. 2, 2018.

[4] S. Mane and G. Shah, "Facial recognition, expression recognition, and gender identification," in *Data Management, Analytics and Innovation*: Springer, 2019, pp. 275-290.

[5] G. L. Marcialis, F. Roli, and L. Didaci, "Personal identity verification by serial fusion of fingerprint and face matchers," *Pattern Recognition,* vol. 42, no. 11, pp. 2807-2817, 2009.

[6] G. S. Walia, S. Rishi, R. Asthana, A. Kumar, and A. Gupta, "Secure multimodal biometric system based on diffused graphs and optimal score fusion," *IET Biometrics,* vol. 8, no. 4, pp. 231-242, 2019.

[7] B. Firmanto, A. F. O. Gaffar, B. Suprapty, and A. B. W. Putra, "Multimodal biometric system based on feature source compaction and the proposed VCG (Virtual Center of Gravity) feature," 2021: IEEE, pp. 95-100.

[8] A. A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of multibiometrics*. Springer Science & Business Media, 2006.

[9] M. Ghayoumi, "A review of multimodal biometric systems: Fusion methods and their applications," 2015: IEEE, pp. 131-136.

[10] A. Jain and A. Ross, "Fingerprint mosaicking," 2002, vol. 4: IEEE, pp. IV-4064.

[11] A. Rattani, D. R. Kisku, M. Bicego, and M. Tistarelli, "Feature level fusion of face and fingerprint biometrics," 2007: IEEE, pp. 1-6.

[12] X. Zhou and B. Bhanu, "Feature fusion of face and gait for human recognition at a distance in video," 2006, vol. 4: IEEE, pp. 529-532.

[13] N. Hassan, D. A. Ramli, and S. A. Suandi, "Fusion of face and fingerprint for robust personal verification system," *International journal of machine learning and computing,* vol. 4, no. 4, p. 371, 2014.

[14] T. Kinnunen, V. Hautamäki, and P. Fränti, "Fusion of spectral feature sets for accurate speaker identification," 2004.

[15] L. Hong and A. Jain, "Integrating faces and fingerprints for personal identification," *IEEE transactions on pattern analysis and machine intelligence,* vol. 20, no. 12, pp. 1295-1307, 1998.

[16] D. C. Shubhangi and M. Bali, "Multi-biometric approaches to face and fingerprint biometrics," *International Journal of Engineering Research & Technology,* vol. 1, no. 5, pp. 2278-0181, 2012.

[17] G. W. Mwaura, W. Mwangi, and C. Otieno, "Multimodal Biometric System:-Fusion Of Face And Fingerprint Biometrics At Match Score Fusion Level," *International Journal of Scientific & Technology Research,* vol. 6, no. 4, pp. 41-49, 2017.

[18] N. Saini and A. Sinha, "Face and palmprint multimodal biometric systems using Gabor–Wigner transform as feature extraction," *Pattern Analysis and Applications,* vol. 18, no. 4, pp. 921-932, 2015.

[19] H. Saevanee, N. Clarke, S. Furnell, and V. Biscione, "Continuous user authentication using multi-modal

biometrics," *Computers & Security*, vol. 53, pp. 234-246, 2015.

[20] W.-H. Lin, P. Wang, and C.-F. Tsai, "Face recognition using support vector model classifier for user authentication," *Electronic Commerce Research and Applications*, vol. 18, pp. 71-82, 2016.

[21] J. Ortega-Garcia *et al.*, "The multiscenario multienvironment biosecure multimodal database (bmdb)," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 32, no. 6, pp. 1097-1111, 2009.

[22] E. Khoury, L. El Shafey, C. McCool, M. Günther, and S. Marcel, "Bi-modal biometric authentication on mobile phones in challenging conditions," *Image and Vision Computing*, vol. 32, no. 12, pp. 1147-1160, 2014.

[23] S. Soleymani, A. Dabouei, H. Kazemi, J. Dawson, and N. M. Nasrabadi, "Multi-level feature abstraction from convolutional neural networks for multimodal biometric identification," 2018: IEEE, pp. 3469-3476.

[24] P. Sharma and K. Singh, "Fusion in Multibiometric Using Fuzzy Logic Review," *International Journal*, vol. 6, no. 5, 2016.

[25] W. K. Fatt, A. K. Kushsairy, H. Nasir, S. I. Safie, and N. M. Noor, "Fingerprint and Face Recognition: Application to Multimodal Biometrics System," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 9, no. 2-2, pp. 81-85, 2017.

[26] A. Lumini and L. Nanni, "Overview of the combination of biometric matchers," *Information Fusion*, vol. 33, pp. 71-85, 2017.

[27] A. Kumar and A. Kumar, "Adaptive management of multimodal biometrics fusion using ant colony optimization," *Information Fusion*, vol. 32, pp. 49-63, 2016.

[28] F. Cherifi, K. Amroun, and M. Omar, "Robust multimodal biometric authentication on IoT device through ear shape and arm gesture," *Multimedia Tools and Applications*, vol. 80, no. 10, pp. 14807-14827, 2021.

[29] G. Gavisiddappa, S. Mahadevappa, and C. Patil, "Multimodal Biometric Authentication System Using Modified Relief Feature Selection and Multi Support Vector Machine," *International Journal of Intelligent Engineering and Systems*, vol. 13, pp. 1-12, 2020.

[30] S. S. Sengar, U. Hariharan, and K. Rajkumar, "Multimodal Biometric Authentication System using Deep Learning Method," 2020: IEEE, pp. 309-312.

[31] N. Alay and H. H. Al-Baity, "Deep learning approach for multimodal biometric recognition system based on fusion of iris, face, and finger vein traits," *Sensors*, vol. 20, no. 19, p. 5523, 2020.

[32] S. Keykhaie and S. Pierre, "Mobile match on card active authentication using touchscreen biometric," *IEEE Transactions on Consumer Electronics*, vol. 66, no. 4, pp. 376-385, 2020.

[33] M. Hammad, Y. Liu, and K. Wang, "Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint," *IEEE Access*, vol. 7, pp. 26527-26542, 2018.

[34] N. Ratha and R. Bolle, *Automatic fingerprint recognition systems*. Springer Science & Business Media, 2003.

[35] A. T. L. Cambridge, "The database of faces," *Cambridge University Computer Laboratory*, 2002.

[36] W. V. University. "Biometrics Identification and Innovation Center." https://biic.wvu.edu/ (accessed 19/Augest/2021, 19/Augest/2021).

[37] S. Crihalmeanu, A. Ross, S. Schuckers, and L. Hornak, "A protocol for multibiometric data acquisition, storage and dissemination," in *Technical Report, WVU, Lane Department of Computer Science and Electrical Engineering*, 2007.

[38] M. Haghighat, M. Abdel-Mottaleb, and W. Alhalabi, "Discriminant correlation analysis: Real-time feature level fusion for multimodal biometric recognition," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 1984-1996, 2016.

[39] K. Gunasekaran, J. Raja, and R. Pitchai, "Deep multimodal biometric recognition using contourlet derivative weighted rank fusion with human face, fingerprint and iris images," *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije,* vol. 60, no. 3, pp. 253-265, 2019.

[40] A. Martinez and R. Benavente, "The AR Face Database: CVC Technical Report, 24," 1998.

[41] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2004: Third fingerprint verification competition," 2004: Springer, pp. 1-7.

[42] E. mehdi Cherrat, R. Alaoui, and H. Bouzahir, "Convolutional neural networks approach for multimodal biometric identification system using the fusion of fingerprint, finger-vein and face images," *PeerJ Computer Science*, vol. 6, p. e248, 2020.

[43] Y. Yin, L. Liu, and X. Sun, "SDUMLA-HMT: a multimodal biometric database," 2011: Springer, pp. 260-268.

[44] P. Tomar and R. C. Singh, "Cascade-based Multimodal Biometric Recognition System with Fingerprint and Face," 2021, vol. 397: Wiley Online Library, 1 ed., p. 2000271.