DOI: https://doi.org/10.33103/uot.ijccce.24.4.2

Multi-Biometric Systems: A Review

Zahraa Naji R[1], Abdul Monem S. Rahma[2] , Raheem Ogla[3]
[1, 3]*Computer Science Department, University of Technology, Baghdad, Iraq*
[2]*Computer Science Department, Al-Maarif University College, Anbar, Iraq*
[1]*cs.21.10@grad.uotechnology.edu.iq*, [2]*monem.rahma@uoa.edu.iq*, [3]*raheem.a.ogla@uotechnology.edu.iq*

Abstract— *Traditional authentication methods such as passwords are susceptible to easy hacking, and as technology progresses, the demand is on the rise for more reliable and secure recognition systems, which can be used in surveillance and biometrics applications etc. A biometric recognition system of individuals is established on the unique features of the individual. Multi modal biometric systems represent a significant research field with widespread applications of recognition systems. Unimodal biometric systems have a variety of issues, including nonuniversality and noisy data. Certain limitations and difficulties can be partially addressed with the use of multi modal biometric systems. In this paper, a survey on multi-biometric systems is presented to highlight the challenges, strengths and weaknesses of some of the research discussed in this study which contributes to enhancing the understanding and development of robust and reliable biometric authentication solutions, essential for ensuring security in various domains as well as suggest directions for future work.*

Index Terms— *biometric recognition, multimodal biometric, biometric system, fusion techniques, multi-biometric system.*

I. INTRODUCTION

The security system's functioning has become more and more dependent on biometric systems recently. In many technologies, including the military, e-commerce, communication, etc., natural characteristics are utilized for unique identification. This is known as biometrics, and it is the quantifiable study of these qualities [1] [2]. One aspect that sets biometrics apart from other features is their non-repudiation ability. Biometry is frequently used to improve the overall security of systems that use biometric cryptosystems or authentication systems [3].

Uni-biometric systems are those that primarily depend on one biometric trait to verify an individual's identity, unlike most other biometric systems now in use. The increasing prevalence of biometric-based solutions in law enforcement and civilian contexts makes it imperative to fully understand the limitations and susceptibilities of such systems [4]. Difficulties come from a variety of sources, such as the possibility of noise contaminating biometric data because of subpar acquisition conditions or minute changes in the biometric itself [5]. Furthermore, problems like non-universality could occur, in which case the biometric system is unable to obtain relevant data from specific people. Moreover, behavioral characteristics such as voice and signature are vulnerable to spoof attacks, in which impostors try to replicate characteristics belonging to people who have actually been enrolled. Furthermore, it is not possible to constantly improve the matching performance regarding uni-biometric systems by fine-tuning the matching as well as feature extraction modules [6] [7].

Biometric recognition system consists five main steps: image capture, pre-processing, feature extraction, storage and matching process [8] [9], *Fig. 1*, shows the main steps of biometric recognition systems.

Received 09/May/2024; Accepted 12/August/2024
 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.24.4.2

A. *Image Acquisition*: the first step is acquisitioning the biometric image using suitable imaging hardware systems like cameras, sensors etc.
B. *Pre-processing*: prepare and enhance the biometric image, where the image captured from pervious step may be poor quality and noise.
C. *Features Extraction*: this step works to extract interest and important features that represent the pattern. The main role of the recognition systems dependent on this step due the resulting used as an input in a recognition process.
D. *Storage: the feature* vector that extracted from previous step will be store in the database for the next step.
E. *Matching Process:* finally, the input feature vector will be match with the features vectors that stored in the database in order to recognize the personal identity.

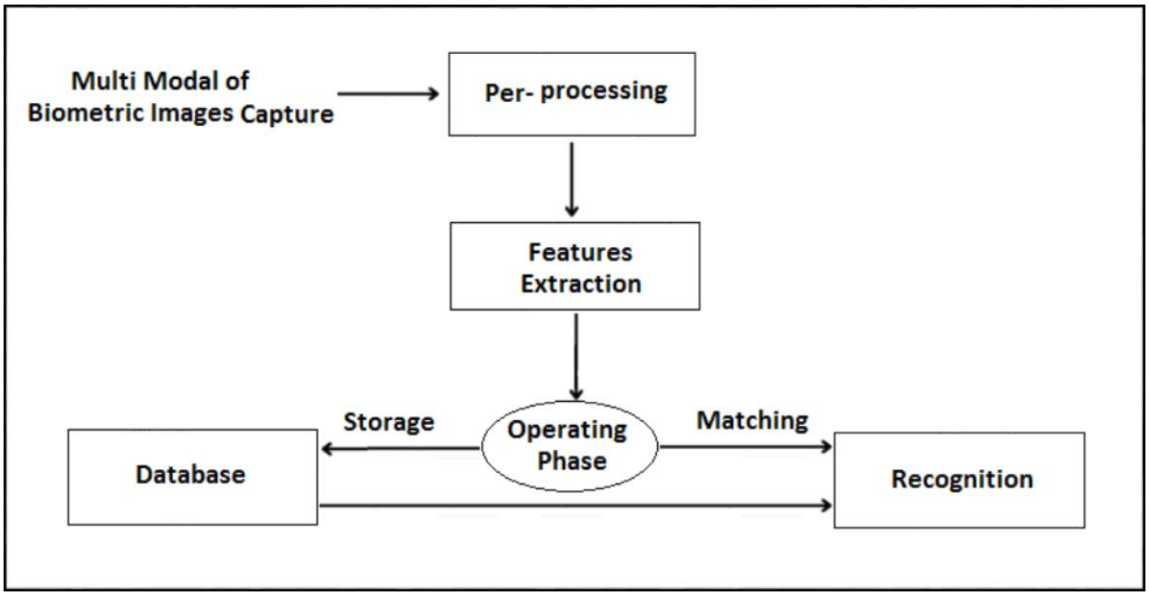

FIG. 1. THE BLOCK DIAGRAM OF BIOMETRIC RECOGNITION SYSTEM [10].

II. TYPES OF MULTIMODAL SYSTEMS

A multi-biometric system makes use of proof from many biometric data sources. Multi-biometric systems could be divided into six different categories based on the properties of such sources [11] [12][13]:

A. Multi-sensor systems: Those systems use several sensors to collect an individual's biometric characteristic.
B. Multi-algorithm systems: Those systems try to improve matching performance through using different feature extraction and/or matching algorithms on the same biometric data.
C. Multi-instance systems: Those systems, which use many instances of the same bodily trait, are also referred to as multi-unit systems. The index fingers on the left and right, for example, could be used.
D. Multi-sample systems: These systems correct for changes within a characteristic by using a single sensor to gather several samples of the same biometric trait.
E. Multimodal systems: In multimodal systems, identity verification is achieved by merging data from several biometric features, like face and voice.
F. Hybrid systems: This term is utilized for describing systems which integrate elements from a subset of the aforementioned scenarios.

Received 09/May/2024; Accepted 12/August/2024

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.4.2

III. PERFORMANCE MEASURES

There are several metrics to evaluate the performance of biometric systems [11] [14], the most commonly used metrics are:

A. False Acceptance Rate (FAR) can be defined as the percentage of fraudster attempts that are accepted by the system [15], FAR given by Eq.1:

$$\text{FAR} = \frac{\text{No. of False Acceptances}}{\text{Total No. of Impostor Identification Attempts}} \times 100\% \quad \ldots (1)$$

B. False Rejection Rate (FRR) can be defined as the percentage of genuine attempts that are rejected by the system [15], FRR given by Eq.2:

$$\text{FRR} = \frac{\text{No. of False Rejections}}{\text{Total No. of Genuine Identification Attempts}} \times 100\% \ldots (2)$$

C. Equal Error Rate (EER) is the point where the FAR and FRR are equal, this refers to a lower EER value, thus, indicating high performance of a biometric system [16].

D. Correct Recognition Rate (CRR) is defined as the percentage of people who correctly identified out of the total number of attempts [17]. CRR is given by Eq.3:

$$\text{CRR} = \frac{\text{Number of samples being correctly classified}}{\text{Total number of tested samples}} \times 100\% \ldots (3)$$

E. Accuracy is a measure of how well a biometric system works overall. It's calculated by looking at the number of correct matches out of all the attempts. High accuracy is important because it means the system is dependable [18].

F. Sensitivity, or True Positive Rate (TPR), shows how good the system is at correctly recognizing genuine users. If the system has high sensitivity, it means that real users are rarely wrongly rejected, which is crucial for making sure the system is user-friendly and reliable [19].

G. Specificity, or True Negative Rate (TNR), measures how well the system can correctly identify and reject impostors. It shows the system's ability to keep unauthorized users out. High specificity is important for the system's security, making sure that impostors aren't mistakenly allowed access [20].

IV. LITERATURES REVIEW

Safaa and Maryam [21] presented a serial multi-modal biometric identification system based on iris and fingerprint. A modified Delaney triangulation system was used to extract fingerprint features, where only the surrounding triangles around each minutia were compared between the template and the stored samples. While for iris feature extraction, the correlation filter is applied to the lower part of the iris region.

Veeru et al. [22] presented a secure multibiometric system that uses facial and iris recognition. The DNN technique is combined with error-correction coding in this system. From the facial and iris biometrics, we can extract domain-specific features using special CNNs. These make it easier to convert them into a shared feature space. The combined features are put together in a joint representation layer, which could be either bilinear or fully connected layer. By selecting characteristics, the size of resulting mixed characteristic vector is reduced through procedure for creating multi-biometric cancelable template. The cancelable template is shown as a binary vector, and it goes through an error-correcting

Received 09/May/2024; Accepted 12/August/2024
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.4.2

decoder to find the nearest codeword. The outcome codeword is then hashed for getting final secure template.

Abdullah et al. in 2017 [23] proposed a model based on three types of biometric traits face, iris, and fingerprint. The Singular Value Decomposition (SVD) technique was used to achieve the features extraction of the face, iris and fingerprint images. The three features are fused by using a simple concatenation method and used as an input for the neural network, where wavelet decomposition produced a compressed feature vector which in turn helped decrease the number of inputs for the neural network (NN) for pattern recognition and identification purposes.

Navdeep and Surinder in 2017 [24] proposed an approach that combines face recognition and the Palm-print method and then merged these images into one gray-scale image using fusion techniques this work uses wavelet decomposition and then further processing will extract their features by converting images into binary for the matching process. The last step is to classify and recognize using combined NN and SVM techniques to increase the accuracy, security, and performance.

Yang et al., in 2018 [25], presented a system that combines fingerprint with finger vein recognition. In this work, feature vectors for both finger-vein and fingerprint are transformed into binary strings or binary vectors. The binary vectors and their variations serve as inputs to the improved partial discrete Fourier transform (EP-DFT) transformation function, giving non-invertibility and revocability to the inputs. This system had utilized feature-level fusion method, and it had provided three methods for fusing together. In the first one of the methods, prior to when the finger vein and finger-print feature vectors are inputted into the EP-DFT, they're concatenated for the purpose of creating a new feature vector. The second approach includes the combination of those vectors after the processing with the P-DFT (Partial Discrete Fourier Transform) and WT (Wavelet Transform). The 3rd approach utilizes the XOR operator; it combines feature vectors (bp) of the finger-vein and finger-print. A binary-valued feature vector that is made from this approach must be changed with the use of the WT prior to putting it into the P-DFT based non-invertible transform. The study tested finger-vein data-base FV-HMTD and finger-print data-bases FVC-2004 DB-2 as well as FVC-2002 DB2 for testing and evaluation.

Shubhleen & Dinnesh in 2019 [26] have brought a multi-biometric recognition system that combines finger-print and speech acquisition. The method for extracting fingerprint features uses minutiae, while for extracting speech features it relies on Mel-Frequency Cepstral Coefficients (MFCC). In this research, classification is done with Feed Forward Neural Network (FFNN). The authors performed testing with the CASIA-V5 dataset for fingerprint images and a dedicated dataset for voice patterns.

Duha et al. in 2020 [27] show a system for multi-biometric that uses the ear and eye to make key, which will be used in encryption process. The images of ear and eye go through preprocessing and we detect region of interest (ROI) from it. For feature extraction in this work, Linear Discriminated Analysis (LDA) method is used on these two types of pictures; then Meerkat swarm algorithm generates the key needed for encryption afterwards.

Abderrahmane [28] proposed a multi-biometric system based on fusion at the feature of fingerprint and palmprint. This system employs the Local Phase Quantization, Local Ternary Patterns, and Binary Similarity Feature for texture feature extraction. two types of classifiers were used for the recognition process: triangular norms and support vector machine. The performance of the system is tested over PolyU and IIT-Delhi datasets to obtain fingerprint and palmprint images, respectively.

Basma et al. [29] presented a multi-modal biometric identification system for the face and iris. Iris features are extracted using a multi-resolution 2D Log-Gabor filter. While the singular spectrum analysis is associated with wavelet transform to extract the facial features. The fusion of features is performed using score and decision fusion methods. Different databases are used to evaluate This system.

Received 09/May/2024; Accepted 12/August/2024

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.4.2

Khodadoust et al. [30] in 2021, presents an approach that combines three different patterns of finger (fingerprint, finger-vein, and finger-knuckle-print), the images captured by using three cameras to obtain the required biometric data. The feature extraction from 2D and 3D space thus, the system was able to cope with the problem of finger rotation. the authors collected their dataset for the research.

Huda et al. [31] 2021 proposed a multi-biometric system based on right and left irises. The CNN and transfer learning are utilized for feature extraction. The training process involves the use of the back-propagation technique with Adam's optimization approach to adjust weights and learning rates. The system utilizes a deep learning model for processing images of a right and left person's irises. The system is evaluated on two public datasets, IITD and CASIA-Iris-V3 Interval, to assess its performance in different conditions.

Mohammad et al. in 2022 [32] put forward a hybrid multimodal biometric system that combines face, iris and thumbprint traits. In this method, Kernel Linear Discriminant Analysis (KLDA) is employed for extracting features of the face while Hough Transform and Daugman algorithm are used to extract characteristics from both irises; the Gabor filter bank is applied to obtain attributes from right as well as left thumbprints. It was tested on seven databases, secure against spoof attacks and can be used for searching large databases.

A multi-biometric system that was presented by Nidaa et al. in 2023 [33] employs facial and fingerprint images to produce a random key which is suitable for electronic numbers, passport identification, civil identification cards as well as seeds for pseudo-random number generators. Every biometric image goes through segmentation into four parts where the segment having most density is used to get different and random identification numbers. After this, the parts go through XOR operations. In addition to that, permutation and thresholding techniques are applied on these parts for a diffusion process.

Iman et al. in 2023 [34] proposed a system for biometric security. This system utilizes the auto-encoder (AE) network for face, fingerprint, and iris feature extraction, which is used to generate two random chaos matrices. The first random chaos matrix is used to permute the pixels of biometric images. while the second random matrix is used to further cipher and confuse the resulting permuted biometric pixels using a two-dimensional (2D) chaotic logistic map (CLM) algorithm. The Feed-Forward Back-Propagation (FFBP) algorithm is used for secret key generation. The training process of the stacked AE network involves the use of the soft-max activation function, cross-entropy error function, and stochastic gradient optimization algorithm.

S. Sai and et. al [35] presented a multi-biometric method using face and iris features called Gradient Neural Network (Gen-NN). The ResNet-101 model is used to extract features from face images, while the WaveNet, which combines Gabor filters and DWT wavelets, are used to extract features from iris images. this system was tested using accuracy, sensitivity, and specificity metrics.

V. CHALLENGES IN MULTI-BIOMETRIC RECOGNITION

A- **Standardization**: absence of standardized methods for representing, testing, and contrasting biometric algorithms and devices. For example, when merging a gait recognition algorithm with a fingerprint recognition algorithm. Locating compatible gait and fingerprint data generated from similar devices becomes exceedingly arduous. Consequently, using whatever data is accessible to evaluate the algorithms, precludes a fair comparison with other algorithms assessed using dissimilar datasets [36] [37].

B- **Performance**: The performance of multi-biometric systems is contingent upon factors such as the characteristics of the matching algorithms employed, the number of biometric traits integrated, and the precision of the biometric data utilized. Notwithstanding the substantial body of research and

Received 09/May/2024; Accepted 12/August/2024

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.4.2

technological advancements in this domain, certain factors persist that hinder the comprehensive realization and utilization of multi-biometric systems [38] [39].

C- **Security and privacy**: When an individual utilize a biometric system for identification or verification, their personal biometric information is captured and stored within the system. Template security becomes a concern particularly when biometric data is centralized in a database. In the event of a breach, all stored biometric data becomes vulnerable [40] [41].

VI. RESULTS AND DISCUSSION

Before discussing the results see Table I that comparison of the techniques and classifiers of each work, as well as datasets used for evaluation:

TABLE I. COMPARISON TECHNIQUE, CLASSIFIER AND DATASET

Ref. Year	Biometric	Method	Classifier	Dataset
[22] 2017	face and iris	DNN	---	Casia-Webfac, CASIA-Iris-Thousand and ND-Iris-0405
[23] 2017	face, iris, and fingerprint	SVD	ANN	AT&T, CASIA-IrisV1and CASIA-FingerprintV5
[24] 2017	face and Palm-print	wavelet decomposition	NN-SVM	Special dataset
[25] 2018	fingerprint and finger-vein	EP-DFT	---	FVC2004 DB2, FVC2002 DB2 FV-HMTD
[26] 2019	Fingerprint and Speech	Minutiae and MFCC	FFNN	CASIA-FingerprintV5 and Special dataset for voice
[27] 2020	ear and eye	LDA	---	Special dataset
[28] 2020	fingerprint and palmprint	LPQ, LTP, BSIF	triangular norms and SVM	PolyU and IIT-Delhi
[29]	Face and iris	Log-Gabor filter, SSA, and WT		ORL and CASIA V3
[30] 2021	fingerprints,finger-veins, and finger-knuckle-prints		---	Special dataset
[31] 2021	Right & Left irises	CNN	SoftMax classifier	IITD and CASIA- Iris-V3 Interval
[32] 2022	face, iris, and thumbprint	KLDA, Daugman and Gabor filter	basis function NN and probabilistic NN classifiers, k-NN classifier, kernel (KSVM) classifier, and Gaussian classifier	seven databases
[33] 2023	facial and fingerprint	Take the highest density	---	Essex Faces 95 and SDUMLA- HMT Datasets
[34] 2023	Face, iris, and fingerprint	auto-encoder (AE) networks	---	six datasets
[35] 2024	Face and Iris	Gen-NN	Gradient Neural Network	VISA

As seen in Table I, many techniques can be used for feature extraction and classification, to face the challenges of multi-biometric systems, where the performance still varies according to the characteristics of datasets, the number of images used to train the system and other parameters that are used for each system. Table II shows the comparison of main strengths and weakness points of each work.

Received 09/May/2024; Accepted 12/August/2024

DOI: https://doi.org/10.33103/uot.ijccce.24.4.2

TABLE II. COMPARISON THE STRENGTH AND WEAKNESS POINTS

Ref. Year	Strength	Weakness
[22] 2017	• Accuracy is 99.7%. • The system employs error-correction coding, which provide security and privacy guarantees. • Utilizes DNN for feature extraction, which can capture complex patterns and improve recognition accuracy.	The paper does not discuss the potential limitations or challenges of implementing the proposed multibiometric secure system.
[23] 2017	• Accuracy is 95%. • Utilizes ANN which can effectively identify individuals based on their biometric characteristics. • Use three sources enhances the system's accuracy and reliability.	• Performance could exhibit a decrease in real-world situations and varied conditions.
[24] 2017	• The MSE equals 0.0414. • Use of NN and SVM techniques in the authentication and recognition process can improve accuracy and performance. • The fusion technique using Inverse DWT is established as the most suitable for a multi-model biometric system.	• The fusion technique may be impact on the overall system performance.
[25] 2018	• Lower EER 0.12%. • The system involves a feature-level fusion strategy offering three options, providing flexibility to select the most appropriate fusion method based on the specific needs of the application. • The EP-DFT based non-invertible transformation strengthens the security of the system.	• There is potential limitation in the understanding and implementation of cancelable multi-biometric systems. • The research lacks exploration and evaluation where the important performance metrics may not have been considered.
[26] 2019	• Accuracy 98.2%. • The use of score level fusion in the proposed system helps to reduce system error rates and improve the accuracy of the system.	• Noise or variations in speech data have an impact of performance.
[27] 2020	• Use LDA for feature extraction helps in accurately identifying the ROI and extracting relevant features. • Use MCA for generating keys, adds an additional layer of security to the system.	• The paper does not provide a comprehensive evaluation of the system's performance in terms of accuracy, robustness, or efficiency.
[28] 2020	• Present a contactless approach for a multi-biometric system that provides hygiene and security.	• Integrating multiple biometrics with many feature extraction techniques led to an increase in the complexity and time of implementation.
[29] 2020	• Achieve high accuracy of more than 99.33%. • Improving the performance of biometric systems by using multi-resolution 2D Log-Gabor filters and SSA with WT for feature extraction.	• Performance could exhibit a decrease in real-world situations and varied conditions depending on the quality of data.
[30] 2021	• Uses three cameras to capture contactless images of all three biometric modalities, making it convenient for users. • Use of 2D and 3D images for each biometric modality, contributed to the satisfactory results obtained by the system.	• The challenges and considerations for the identification mode are not extensively addressed. • Does not use of a specific public database, which may limit the generalizability of the results.
[31] 2021	• Accuracy is 99% for the IITD iris datasets and 94% and 93% when use the CASIA-iris-V3 interval datasets for the left and right iris respectively. • The use of deep learning models and optimization techniques enhances the performance of the system. • The paper utilizes established libraries like OpenCV, Keras, and sci-kit learn, adding credibility to the	• Does not good for real-time applications or large-scale deployments because of the computational requirements. • The generalizability of the proposed system across different demographic groups or variations in iris images is not addressed.

Received 09/May/2024; Accepted 12/August/2024
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.4.2

	implementation.	
[32] 2022	• Overcomes limitations like non-universality, noisy sensor data, and large intra-user variations. • Feature-level fusion is more effective than other levels of fusion. • Can increase the accuracy of a hybrid multimodal biometric system to 100% with only 15 features.	• Challenges in integrating and synchronizing multiple biometric modalities effectively.
[33] 2023	• Can be used for various applications such as electronic numbers, passport identification, and civil identification cards. • Provides a solution to the problem of compromised biometric templates.	• The system partitions the images into four parts for processing. If the partitioning is not done accurately, it may lead to incorrect key generation. • The system's effectiveness may vary depending on the diversity of the biometric data used. If the system is not trained on a wide range of facial and fingerprint images, it may struggle to accurately generate random keys for all individuals.
[34] 2023	• Present a secure biometric system. • Accuracy rate is 99.97% with a lower error rate is 0.00137.	• Using many algorithms may increase the complexity of the implementation.
[35] 2024	• This technique can get a high accuracy rate of up to 93.77%. • Reduce the noise and enhance the image by employing the ResNet-101 for feature extraction.	• Isn't suitable for real-time applications due to the multi-processing steps that increase the time-consuming. • Requires many computational resources and large datasets for training.

VII. CONCLUSIONS AND FUTURE WORKS

This paper presented a literature survey of various methods used for human recognition based on a multi-biometric pattern. The systems combined with multimodal biometrics, such as fingerprints, facial recognition, iris scanning, voice recognition, and others, are generally more reliable, whereas the multi-modal is narrow the disparities present in uni-biometric systems by surmounting some challenges to enhance the effectiveness and accuracy of the people recognition process. Each biometric technology holds significance contingent upon the diverse applications in which it is used. Multi-biometric systems enhance recognition rates by amalgamating the strengths of various patterns, and by capturing more information from individuals, which are critical in applications where precise identification or verification is essential, such as security systems, identity verification, and access control systems. For future work, use cloud computing, since the multi-biometric systems have large extensive datasets and intricate queries, necessitating the implementation of effective search techniques to attain satisfactory performance levels.

REFERENCES

[1] R. Alrawili, A. Abdullah S. AlQahtani and M. Khurram Khan "COMPREHENSIVE SURVEY: BIOMETRIC USER AUTHENTICATION APPLICATION, EVALUATION, AND DISCUSSION," vol. 3, no. 6, pp. 149–160, 2023.

[2] G. R. Sinha and S. B. Patil, "Biometrics : Concepts and Applications Biometrics : Concepts and Applications Authors ' Biography," no. December, 2015.

[3] H. Ahmed and M. Taha, "A Brief Survey on Modern Iris Feature Extraction Methods," *Eng. Technol. J.*, vol. 39, no. 1A, pp. 123–129, 2021, doi: 10.30684/etj.v39i1a.1680.

[4] D. Maltoni, D. Maio, A. K. Jain, and J. Feng, *Handbook of fingerprint recognition: Third edition*. 2022. doi: 10.1007/978-3-030-83624-5.

[5] A. R. and N. Poh, "Multibiometric Systems: Overview, Case Studies and Open Issues," in *Handbook of Remote Biometrics: for Surveillance and Security. London: Springer London*, 2009, pp. 273–292. doi: 10.1109/ICASSP.2010.5495466.

[6] A. Ross, A. K. Jain, and J. Z. Qian, "Information fusion in biometrics," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 2091 LNCS, pp. 354–359, 2001, doi: 10.1007/3-540-45344-x_52.

Received 09/May/2024; Accepted 12/August/2024
 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.24.4.2

[7] A. M. and A. A. Souhail Guennouni and Abstract, "Biometric Systems and Their Applications," *IntechOpen*, p. 15, 2020, [Online]. Available: https://www.intechopen.com/books/advanced-biometric-technologies/liveness-detection-in-biometrics

[8] K. W. Bowyer and M. J. Burge, *Introduction to the Handbook of Iris Recognition*. 2013. doi: 10.1007/978-1-4471-4402-1_1.

[9] K. Anil Jain and A. Kumar, *Chapter 3 Biometric Recognition: An Overview*. 2012. doi: 10.1007/978-94-007-3892-8_3.

[10] Y. Ali and Z. Razuqi, "Palm vein recognition based on centerline," *Iraqi J Sci*, vol. 58, no. 2A, pp. 726–734, 2017.

[11] P. Anil , K. Jain And A. A. Ross, *Handbook of Biometrics*. 2008.

[12] V. Gaikawad and S. Kini, "A Survey of Multi-Biometric Cryptographic Security System," *Int. J. Sci. Res.*, vol. 4, no. 12, pp. 1090–1094, 2015, doi: 10.21275/v4i12.nov152138.

[13] C. Singla, "A Review of Multibiometric System with Recognition Technologies and Fusion Strategies," no. Icaet, pp. 4–9, 2015.

[14] S. Bahgat, S. Ghoniemy, and M. Alotaibi, "Proposed Multi-Modal Palm Veins-Face Biometric Authentication," *Int. J. Adv. Comput. Sci. Appl.*, vol. 4, no. 6, 2013, doi: 10.14569/ijacsa.2013.040612.

[15] S. Bharathi, R. Sudhakar, and V. E. Balas, "Hand vein-based multimodal biometric recognition," *Acta Polytech. Hungarica*, vol. 12, no. 6, pp. 213–229, 2015, doi: 10.12700/APH.12.6.2015.6.13.

[16] Z.. Razoqi, "Palm Vein Recognition Using Centerline Extraction," 2017.

[17] D. Petrovska-Delacrétaz, G. Chollet, and B. Dorizzi, "Guide to biometric reference systems and performance evaluation," *Guid. to Biometric Ref. Syst. Perform. Eval.*, no. January, pp. 1–382, 2009, doi: 10.1007/978-1-84800-292-0.

[18] D. Fronitasari and D. Gunawan, "Palm vein recognition by using modified of local binary pattern (LBP) for extraction feature," *QiR 2017 - 2017 15th Int. Conf. Qual. Res. Int. Symp. Electr. Comput. Eng.*, vol. 2017-December, pp. 18–22, 2017, doi: 10.1109/QIR.2017.8168444.

[19] A. Agha and L. George, "Palm Veins Recognition and Verification System: Design and Implementation," 2014.

[20] I. Muraina and S Abam, "Data Analytics Evaluation Metrics Essentials : Measuring Model," no. August, 2023, [Online]. Available: https://www.researchgate.net/publication/372883214_DATA_ANALYTICS_EVALUATION_METRICS_ESSENTIALS_MEASURING_MODEL_PERFORMANCE_IN_CLASSIFICATION_AND_REGRESSION

[21] S. S.Omran and M. Abdulmunem Salih, "Design and Implementation of Multi-model Biometric Identification System," *Int. J. Comput. Appl.*, vol. 99, no. 15, pp. 14–21, 2014, doi: 10.5120/17448-8255.

[22] V. Talreja, M. Valenti, and N. M. Nasrabadi, "Multibiometric secure system based on deep learning," *2017 IEEE Glob. Conf. Signal Inf. Process. Glob. 2017 - Proc.*, vol. 2018-Janua, pp. 298–302, 2018, doi: 10.1109/GlobalSIP.2017.8308652.

[23] R Hussein, H. Jeiad, and M. N. Abdullah, "Multibiometric Identification System based on SVD and Wavelet Decomposition," *Eng. Technol. J.*, vol. 35, no. 1Engineering, pp. 61–67, 2017, doi: 10.30684/etj.2017.127311.

[24] I. Journal, L. Trends, and T. Vol, "A novel multi-model biometric fusion approach using palm-print & face biometric," *Int. J. Latest Trends Eng. Technol.*, vol. 8, no. 3, pp. 240–247, 2017, doi: 10.21172/1.83.036.

[25] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "A fingerprint and finger-vein based cancelable multi-biometric system," *Pattern Recognit.*, vol. 78, pp. 242–251, 2018, doi: 10.1016/j.patcog.2018.01.026.

[26] S. Sharma and D. Kumar, "Enhance the classification and Score level Fusion Multi-model Biometric System Based on Fingerprint and Speech Recognition," *Int. J. Comput. Sci. Eng.*, vol. 7, no. 6, pp. 956–962, 2019, doi: 10.26438/ijcse/v7i6.956962.

[27] S. Azeez, and A. Hossen, "Key Generation from Multibiometric System Using Meerkat Algorithm," *Eng. Technol. J.*, vol. 38, no. 3B, pp. 115–127, 2020, doi: 10.30684/etj.v38i3b.652.

[28] A. Herbadji, N. Guermat, L. Ziet, Z. Akhtar, M. Cheniti, and D. Herbadji, "Contactless multi-biometric system using fingerprint and palmprint selfies," *Trait. du Signal*, vol. 37, no. 6, pp. 889–897, 2020, doi: 10.18280/TS.370602.

[29] B. Ammour, L. Boubchir, T. Bouden, and M. Ramdani, "Face–iris multimodal biometric identification system," *Electron.*, vol. 9, no. 1, 2020, doi: 10.3390/electronics9010085.

[30] J. Khodadoust, M. A. Medina-Pérez, R. Monroy, A. M. Khodadoust, and S. Mirkamali, "A multibiometric system based on the fusion of fingerprint, finger-vein, and finger-knuckle-print," *Expert Syst. Appl.*, vol. 176, no. December 2020, pp. 0–3, 2021, doi: 10.1016/j.eswa.2021.114687.

[31] H. Therar, A. Mohammed, and J. Ali, "Multibiometric System for Iris Recognition Based Convolutional Neural Network and Transfer Learning," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 1105, no. 1, p. 012032, 2021, doi: 10.1088/1757-899x/1105/1/012032.

[32] M. H. Safavipour, M. A. Doostari, and H. Sadjedi, "A hybrid approach to multimodal biometric recognition based on feature-level fusion of face, two irises, and both thumbprints," *J. Med. Signals Sens.*, vol. 12, no. 3, pp. 177–191, 2022, doi: 10.4103/jmss.jmss_103_21.

Received 09/May/2024; Accepted 12/August/2024
 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.24.4.2

[33] R. Azeez, A. Jamil, A. Al-Adhami, and N Hassan, "Multibiometric System with Runs Bits Permutation for Creating Cryptographic key Generation Technique," *Iraqi J. Sci.*, vol. 64, no. 1, pp. 452–468, 2023, doi: 10.24996/ijs.2023.64.1.40.

[34] I. Almomani, W. El-Shafai, A. AlKhayer, A. Alsumayt, S. S. Aljameel, and K. Alissa, "Proposed Biometric Security System Based on Deep Learning and Chaos Algorithms," *Comput. Mater. Contin.*, vol. 74, no. 2, pp. 3515–3537, 2023, doi: 10.32604/cmc.2023.033765.

[35] S. Sai Satyanarayana Reddy, H. Bommala, G. R. Sakthidharan, and N. Ivanovich Vatin, "Multi-Modal Biometric Recognition for Face and Iris using Gradient Neural Network (Gen-NN)," *MATEC Web Conf.*, vol. 392, p. 01078, 2024, doi: 10.1051/matecconf/202439201078.

[36] P. Phillips *et al.*, "Overview of the multiple biometrics grand challenge," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5558 LNCS, no. June, pp. 705–714, 2009, doi: 10.1007/978-3-642-01793-3_72.

[37] J. Pato, L. I. Millett, and W. Biometrics, *Biometric Recognition challenges and opportunities*, vol. 4, no. 8. 2010. doi: 10.1097/00006324-192708000-00009.

[38] S.. Modak and V. K. Jha, "Multibiometric fusion strategy and its applications: A review," *Inf. Fusion*, vol. 49, pp. 174–204, 2019, doi: 10.1016/j.inffus.2018.11.018.

[39] W. Yang, S. Wang, G. Zheng, and C. Valli, "Impact of feature proportion on matching performance of multi-biometric systems," *ICT Express*, vol. 5, no. 1, pp. 37–40, 2019, doi: 10.1016/j.icte.2018.03.001.

[40] C. Rathgeb and C. Busch, "Multi-Biometric Template Protection: Issues and Challenges," *New Trends Dev. Biometrics*, 2012, doi: 10.5772/52152.

[41] H. Wechsler, "Biometric Security and Privacy Using Smart Identity Management and Interoperability: Validation and ropr_538 63..89 Vulnerabilities of Various Techniques," *Rev. Policy Res.*, vol. 30, no. 1, pp. 63–89, 2012, doi: 10.1111/ropr.12008.

Received 09/May/2024; Accepted 12/August/2024
 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*