IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 13, April 2025
Impact Factor: 7.67

User Authentication Based on Face and Periocular Regions Using Deep Learning Algorithm

[1]Mrs. Banuppriya P, [2]Muthu Prakash A, [3]Gokulnath P, [4]Ajay R, [5]Abinesh N
Assistant Professor, Computer Science and Engineering[1]
Students, Computer Science and Engineering[2-5]
Mahendra Institute of Engineering and Technology, Namakkal, India

Abstract: *A specific biometric characteristic must be unique for each person for whom it can be calculated and must be constant throughout time in order to be used for identifying purposes. Biometrics, which include voiceprints, fingerprints, photos, signatures, and retinal blood vessel patterns, all have significant disadvantages. While photos and signatures can be easily falsified and are inexpensive and simple to collect and keep, they cannot be reliably identified mechanically. However, because the human iris is an internal organ of the eye and is both insulated from the outside environment and easily visible up to a distance of one meter, it is an ideal biometric for an automated, fast, and reliable identification system. The most dependable and accurate biometric identification technology currently in use is iris recognition. The automated biometric identification process known as "iris recognition" makes use of mathematical pattern-recognition techniques on photographs of each individual's unique, complicated, random iris patterns. This work proposes to create a face and iris identification system that segments the face, eye, and iris region using the Grassmann algorithm, Gabor filtering, and deep neural network. Using template matching, a template of the observed region is produced. The recognition is predicated on features found in the real-time enrollment system. The outcomes demonstrate the effectiveness of the suggested approach for iris-based biometric identification*

Keywords: Authentication, Biometric system, Deep learning, Face recognition, Iris classification

I. INTRODUCTION

Metrics pertaining to human traits are called biometrics. In computer science, biometrics authentication, also known as realistic authentication, is used for access control and identification. It is also employed for the purpose of identifying members of monitored groups.Individuals are then identified and described by unique, quantifiable traits known as biometric identifiers. Biometric identifiers are frequently classified as behavioral versus physiological traits. The body's form is associated with physiological traits. A few examples are fingerprints, veins in the palm of the hand, face recognition, DNA, palm print, hand geometry, iris identification, retina, and smell or odor. Behavioral traits, such as typing rhythm, gait, and voice, are associated with an individual's pattern of behavior. The latter category of biometrics is known as behavior-metrics, according to some academics. Token-based identity systems, like a passport or driver's license, and knowledge-based identification systems, like a password or personal identifying number, are examples of more conventional methods of access control. The collecting of biometric identifiers raises privacy concerns regarding the final use of this information, however biometric identifiers are more reliable than token and knowledge-based approaches in proving identity because they are unique to each individual. Fig 1 shows the biometric block diagram.

DOI: 10.48175/IJARSCT-26004

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 13, April 2025
Impact Factor: 7.67

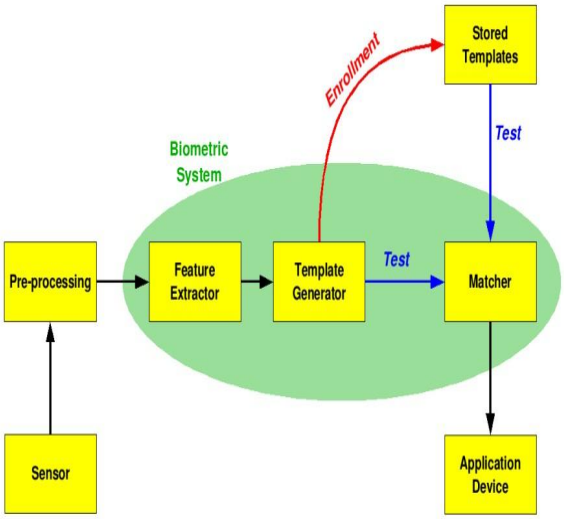

Fig 1: Biometric block diagram

MULTIMODAL BIOMETRIC SYSTEM

To get beyond the drawbacks of unimodal biometric systems, multimodal biometric systems employ several biometrics or sensors. For example, aged irises can compromise iris identification systems, while worn-out or damaged fingerprints can impair finger scanning systems. It is doubtful that many unimodal biometric systems will have the same drawbacks, even though unimodal biometric systems are constrained by the integrity of their identifier. Multimodal biometric systems are capable of acquiring sets of data from distinct biometrics (such as fingerprint scans and spoken passcodes via voice recognition) or from the same marker (such as multiple iris scans or finger scans). These uni-modal systems can be fused sequentially, concurrently, in combination, or in series by multimodal biometric systems; these fusion modalities correspond to sequential, parallel, hierarchical, and serial integration modes, respectively. Different phases of a recognition system may experience biometric information fusion. When feature level fusion occurs, either the data itself or the features that are taken from several biometrics are combined. Through matching-score level fusion, the scores produced by several classifiers related to various modalities are combined. Lastly, decision level fusion combines the outputs of several classifiers using methods like majority voting. The reason for the higher efficacy of feature level fusion over other levels of fusion is because the feature set has more detailed information about the input biometric data than either the matching score or the classifier's output choice. Better recognition outcomes are thus anticipated from feature-level fusion.

II. RELATED WORK

Pawel Drozdowsk, et.al .[1] proposed work protected indexing technique for biometric data is described. A multi-stage search structure is formed by fused features of an intelligently coupled set of templates. The collection of possible candidate identities is gradually pre-filtered during retrieval, which lowers the quantity of template comparisons required for a biometric identification transaction. Homomorphic encryption is used to protect the biometric probing templates, the produced index, and the reference templates that are stored. Using two cutting-edge open-source face recognition systems, the suggested solution is thoroughly tested in closed-set and open-set identification situations using databases that are accessible to the public. The suggested approach allows for a 90% decrease in the computational burden related to a biometric identification transaction without compromising biometric performance when compared to a standard baseline algorithm that uses an exhaustive search-based retrieval algorithm. Moreover, the suggested approach ensures the unlink ability, irreversibility, and renewability of the protected biometric data by enabling a smooth integration of template protection with open-source Homomorphic encryption libraries. This article

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 13, April 2025
Impact Factor: 7.67

presents a computationally efficient method for indexing and retrieving biometric data. The suggested indexing technique is based on feature-level fusion after intelligently matching facial parent templates according to how similar they are (in terms of soft biometrics or non-mated comparison scores). Multi-stage biometric identification retrieval is made easier by the constructed search structure, whereby the retrieved candidate lists are progressively condensed at each step of the cascade.

Dailé Osorio-Roig et.al .[2] suggested a face identification system that protects privacy and indexes and retrieves protected face templates using a Product Quantization-based hash look-up table. These face templates are protected by completely Homomorphic encryption techniques, hence assuring great privacy protection of the enrolled people. The experimental evaluation conducted in both closed-set and open-set conditions demonstrates the viability of the suggested technique for implementation in large-scale facial identification systems for the optimal configuration: Together with a low pre-selection error rate of less than 1%, a workload reduction of 0.1% of a baseline technique carrying out an exhaustive search is achieved. Regarding biometric performance, practical False Positive Identification Rate (FPIR) values on the FEI and FERET face databases yield a False Negative Identification Rate (FNIR) in the range of 0.0% - 0.2%. Furthermore, competitive performance is demonstrated by our concept on unconstrained databases, such as the LFW face database. To the best of the authors' knowledge, this is the first study to propose a workload reduction strategy that is competitive, protects privacy, and executes template comparisons in the encrypted domain.

Quang Nhat Tran et.al .[3] proposed work makes the following contributions to the field's understanding: (1) It offers an innovativeand thorough taxonomy of privacy-preserving biometrics for the classification of the field's body of knowledge and body of literature. (2) It offers a literature survey guided by taxonomy. (3) Future projects and open research issues are discussed. (4) A taxonomy and synopsis of the state-of-the-art biometric matching techniques has also been produced, as the techniques employed in privacy-preserving biometric authentication systems rely on or integrate with generic biometric matching techniques. Researchers in both the biometrics and cryptography communities would benefit from this system-level knowledge organisation by producing great self-contained reference materials. Without it, these researchers would struggle to comprehend the pertinent information from the other group. Following that, this work offers a forecast for field trends based on other recently developing research fields and their possible effects, or where they might be referencing previous studies in this area. This work focuses especially on new developments in mobile devices, cloud computing, and the Internet of Things. Future biometric recognition systems will undoubtedly grow more and more significant; this is practically required given the development of new devices and computer paradigms.

Wencheng Yang et.al .[4] created project offers a thorough analysis of current HE research in relation to biometrics. Various HE methods to biometric security are analysed and discussed in detail based on the categories of distinct biometric features. Additionally, this paper discusses the integration of HE for biometric security with other cutting-edge technologies (such as blockchain and machine/deep learning). Lastly, difficulties and future possibilities for study are presented based on the most recent developments of HE in biometrics. During the verification stage, a similarity score is determined by comparing or matching a query's biometric data with the template, which is handled in the same manner as during the enrolment phase. Matching is successful if this score is higher than a predetermined threshold; if not, matching is failed. This survey article gives a general overview of biometric applications. A discussion was held regarding the availability and specifications of HE libraries that have been or may be utilised for biometrics, as well as specific HE schemes under various, HE categories. Various HE-based methods for face, fingerprint, iris, and other biometric security were presentedin this work. The difficulties and potential paths for future HE researches in biometrics were highlighted, along with the integration of HE with other technologies. Overall, this survey comprehensively assessed the current status for biometric security, which is of benefit to readers specialising in biometrics research.

Tong-Yuen Chai et.al .[5] suggested method is trainable and doesn't call for any additional changes to the secured iris biometric templates. This method uses two techniques to create a confidence matrix that will lessen the iris BTP schemes' performance degradation. While the probability confidence matrix performed better in iris databases with higher image quality, the suggested binary confidence matrix performed better in noisy iris data. Furthermore, the

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 13, April 2025
Impact Factor: 7.67

possible impacts on recognition performance resulting from database-associated noise masking and the variety of biometric data types generated by various iris BTP methods have been taken into account in our suggested scheme. It tried the suggested scheme on a number of publicly available iris research databases, and the results showed a notable improvement. In our studies, the suggested solutions successfully increased the performance of the state-of-the-art BTP by 68.68% under optimal conditions. While the proposed probability-based solution works better with higher quality iris photos collected under more controlled conditions, our proposed binary-based confidence matrix can mitigate the deterioration of noise protected biometric templates.

Rosario Arjona et.al .[6] suggested using Learning Parity With Noise (LPN) commitments in biometrics as a template protection strategy. As far as it is aware, this is the first post-quantum security-oriented solution for biometric template protection based on the LPN problem (i.e., the difficulty of decoding random linear codes). Within the protected domain, biometric features are compared. The qualities of resistance against similarity-based assaults, crosshatching, stolen tokens, and False Acceptance Rate (FAR) are all met, along with the properties of irreversibility, revocability, and unlink ability. Because user-specific secret keys are used and the False Rejection Ratio (FRR) can be modified based on a threshold to maintain the accuracy of the unprotected scheme in the Stolen Token scenario, recognition accuracy with a 0% FAR is obtained. For security levels of at least 80 bits, good performance is achieved in terms ofexecution time, template storage, and operation complexity. To demonstrate how it provides security using authentication and potentially malicious database (cloud) servers, the suggested system is implemented in a dual-factor authentication protocol from the literature. Any biometric trait represented by binary features and any matching score based on Hamming or Jaccard distances can be used with the suggested LPN-based protected system. Specifically, the experimental outcomes of a useful Matlab-based finger vein detection system are shown.

Pawel Drozdowski, et.al .[7] proposed process using two cutting-edge open-source face recognition systems, the created approach is thoroughly tested in closed-set and open-set identification scenarios using databases that are accessible to the public. The suggested approach allows for a 90% decrease in the computational burden related to a biometric identification transaction without compromising biometric performance when compared to a standard baseline algorithm that uses an exhaustive search-based retrieval algorithm. Moreover, the suggested approach ensures the unlink ability, irreversibility, and renewability of the protected biometric data by making it easier to integrate template protection with open-source Homomorphic encryption libraries. The suggested indexing technique is based on feature-level fusion after intelligently matching facial parent templates according to how similar they are (in terms of soft biometrics or non-mated comparison scores). The generated search structure enables a multi-stage retrieval of biometric identification, where the recovered candidate lists are progressively condensed in each cascade phase. Put another way, a tenfold decrease in the computational effort needed for biometric identification is achievable with the suggested method, and this can be done without compromising biometric performance. The suggested approach accomplishes post-quantum security and the biometric template protection goals of unlink ability, irreversibility, and renewability by incorporating Homomorphic encryption.

Quang Nhat Tran, et.al .[8] proposed is a lightweight AI-based biometric identification system based on the binary representation of a biometric instance is shown by the built project. Specifically, the binary strings representing the intraclass and interclass biometric subjects will be used to train a binary classifier. The multi-layerPerceptron Neural Network and Support Vector Machine are selected as the classifiers to assess the authentication capabilities of fingerprint and iris biometrics. The verified biometric text is then passed via a hash function to generate a hash value that will be utilised in a Zero-Knowledge-Proof Protocol to protect privacy. It developed a straightforward but effective method to increase the binary strings' discriminative power in order to improve the classifier's recognition; this method is called Composite Features Retrieval. Using the iris dataset UBIRISv1 and the four publicly accessible fingerprint datasets FVC2002-DB1, FVC2002-DB2, FVC2002-DB3, and FVC2004-DB2, it assessed the suggested approach. The encouraging outcome demonstrates the potential of this approach. It has presented a Composite Feature Retrieval approach and tested its efficacy using several classifiers based on artificial intelligence. The biometric data is extracted with both the classic and the CFR strategy. The bit string is applied with a (n, k) RSC after being verified by a classifier to create an identical hashed string that is utilised in a Zero Knowledge-Proof Protocol.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 13, April 2025
Impact Factor: 7.67

Kamel Aizi, et.al .[9] developed novel multibiometric fusion technique for iris and fingerprint biometric identification is presented in this paper. The individual processing of each modality results in a vector of scores. The score level is where the fusion process is used. It divided the score range into three zones of interest that are pertinent to the suggested identification approach for each modality after conducting a preliminary analysis using the k-means clustering method. Two methods are then used to apply the fusion to the extracted regions. The first method uses a decision tree and weighted sum (BCC) to achieve classification, whereas the second method uses fuzzy logic (BFL). The efficacy of the suggested techniques was assessed by a series of experiments on reference biometric datasets employing four metrics: False Accept Rate, False Reject Rate, Enrolled False Accept Rate, and Recognition Rate. The results show that the suggested fusion techniques perform better than those based on a single modality, which makes them highly intriguing. Furthermore, was demonstrated that the BCC fusion method outperforms the BFL by a small margin. This work's primary goal was to demonstrate the benefits of multimodal identification while also suggesting a novel fusion technique for the two chosen modalities. It selects the fusion at the scorelevel among the several levels of fusion that are currently in use since the scores derived from diverse modalities are highly informative. Furthermore, all multimodal systems can use this level of fusion.

Aniello Castiglione, et.al [10] suggested approach uses the Local Binary Pattern on Three Orthogonal Planes descriptor to model these dynamic facial patterns that are obtained from edge Internet of Things devices. This descriptor successfully recovers the local features of the face as well as its movement at the fog level of the architecture. The collected features are matched to a reference database using a trained and optimised deep feed forward network that is accessible via the cloud. The obtained findings demonstrate the state-of-the-art identification reliability and resilience of the suggested strategy, particularly for demanding IIoT scenarios. Because it is inherently difficult to forge such a time-dependent descriptor, the suggested technique and the associated edge-fog-cloud architecture proven to be highly effective in enhancing the IIoT environment's trustworthiness. Through the use of a specially designed database, the studies produced results that demonstrated state-of-the-art recognition accuracy of 98.7% at rank 1, high robustness to the manner the passphrase is spoken if the subject is authentic and reliable rejection of imposters even at low decision thresholds. Experiments to evaluate the effectiveness of the three-level design in comparison to a more traditional approach focused on local processing will be the focus of future study. The audio portion of the speech samples for building a bimodal biometric system could be included to this article as an extension to increase the suggested method's accuracy and dependability.

III. EXISTING METHODOLOGIES

Recently, there has been an increase in interest in biometric recognition using the periocular region. The secret is to employ all of the textures from the skin surrounding the eye as well as the shape of the eyelid, the eyebrow, and the eyelashes in addition to the discriminating information found inside the iris, which is obtained by acquiring an area identical to that used by iris identification systems. Identity verification by face or ocular traits has been increasingly popular in the last few years. A number of scholarly studies have proposed newfeatures and classification strategies that can be applied to each of these modes to enhance their performance. Nevertheless, in the case of iris identification or face recognition, the majority of these methods operate on the implicit premise that we can either obtain an extremely high-quality iris image or the subject's full face. It would be quite helpful in these situations to look into the feasibility of employing specific facial features exclusively as a biometric. We focus on the periocular area of the face, which has a lot of texture and includes features like the eyelid curves, eyebrows, and eye folds. This could be helpful, for example, if the wearer is wearing a mask that only reveals their eyes, or if extremely bright lighting highlights certain facial characteristics. The past few years have seen remarkable advancements in ocular biometrics, mostly because of the substantial advances made in iris recognition.

IV. PROPOSED METHODOLOGIES

Systems with the ability to use multiple physiological or behavioural traits for enrolment, verification, and identification are known as multi-modal biometrics. Multi-modal biometrics-based human identification is a developing trend, and increasing recognition accuracy is one of the main motivations for combining several modalities. Other

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 13, April 2025
Impact Factor: 7.67

justifications for combining two or more biometrics include the possibility that distinct biometric modalities are better suited for particular deployment circumstances or situations in which security is crucial to safeguarding sensitive data. We start by creating a tangent space from a collection of images that have been perturbed, and we find that this space admits a vector space structure. Second, we use a chordal distance to compare subspaces and embed the approximated tangent spaces on a Grassmann manifold. Using a course to fine strategy speeds up the matching process. Periocular biometrics has garnered significant attention from researchers lately, and some of their efforts have been documented in published works. In this work, we suggest a fresh and reliable method for periocular recognition. Real-time face detection in approach photos is followed by alignment and normalization. We used the whole strip, which included both eyes, as the periocular area. We calculated the magnitude responses of the image filtered via a bank of intricate Gabor filters in order to extract features. The Grassmann algorithm is used to minimize the dimensionality of features. Back propagation neural networkclassification is applied to the decreased feature vector. The experimental results show a promising level of verification and identification accuracy. In addition, a thorough comparison with some of the most well-known state-of-the-art methodologies is provided to determine the robustness of thesuggested strategy. Fig 2 shows the proposed framework which contains face and iris biometric system using machine learning framework.

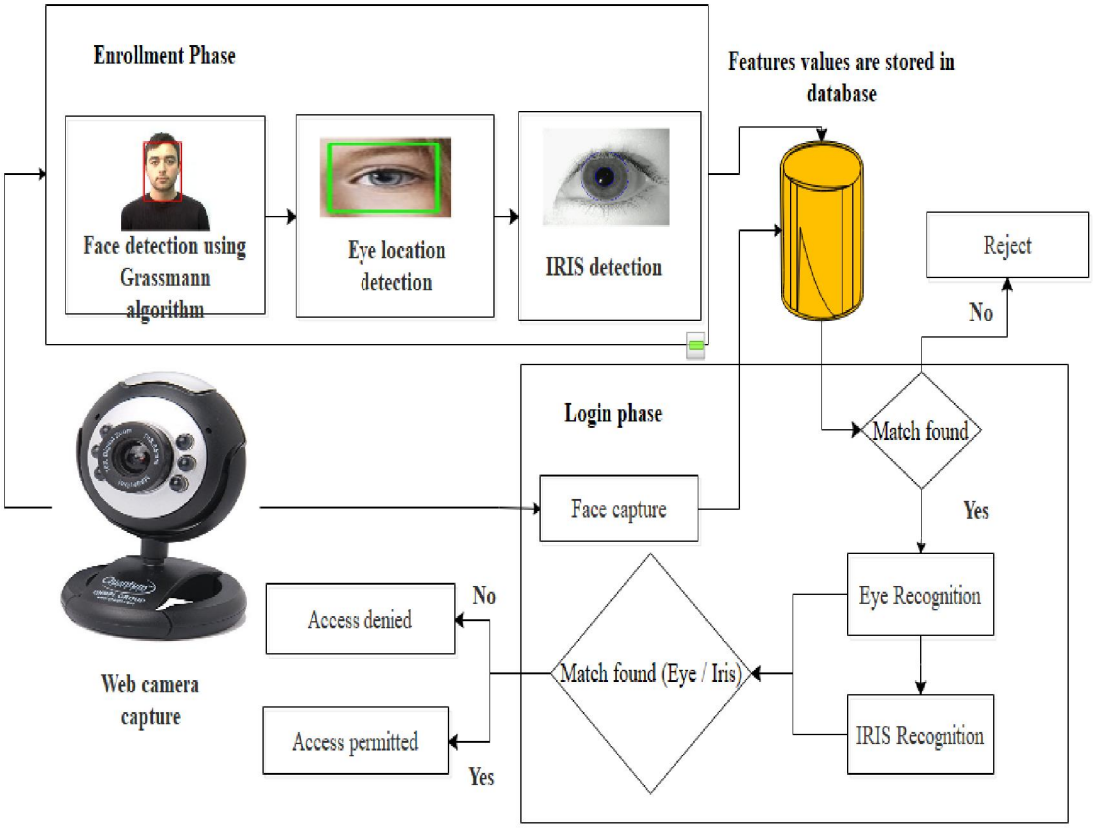

FIG 2: PROPOSED FRAMEWORK

FEATURES EXTRACTION ALGORITHM

A Grassmann manifold $G_{n,p}$is a set of p-dimensional linear subspaces of R^n (p-planes in R^n) for $0 < p \leq n$. This Grassmann manifold has a natural quotient representation $G_{n,p}= V_{n,p}/ O_p$, where Vn,p is a Stiefel manifold (a set of n×p orthonormal matrices) and O_p is the orthogonal group. This representation states that two matrices belong to the same

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 13, April 2025
Impact Factor: 7.67

equivalence class if their columns span the same p dimensional subspace. Hence, the entire equivalence class can be represented as the subspace spanned by the columns of a given matrix Y.

$$[Y] = \{YQ_p : Q_p \in O_p\}$$

In other words, a point on the Grassmann manifold is a linear subspace which may be specified by any arbitrary orthogonal basis.

Use eye coordinates to determine the initial affine registration parameters for each image.

Sample the affine registration manifold by perturbing the affine parameters

Compute the k nearest neighbours from the registration manifold

Apply color equalization and filter features values

Construct the tangent space

Embed the approximated tangent space and compute canonical angles

Compute the subspace distance

V. EXPERIMENTAL RESULTS

The proposed system implemented in PYTHON to provide attendance based on Face, Eye and Iris features. Then using real time facial datasets and calculate the performance in terms of accuracy. False reject rate is an access attempt by an authorized user. A system's FRR typically is stated as the ratio of the number of false rejections divided by the number of identification attempts

FALSE REJECT RATE = FN / (TP+FN)

FN =Genuine Scores Exceeding Threshold

TP+FN = All Genuine Scores

The proposed system can be provided a smaller number of rejection rate than the existing algorithms such as Support Vector Machine, Random Forest, Adaboost classifier and Grassmann algorithm that can be shown in fig 3 and table 1.

ALGORITHM	FRR
RANDOM FOREST	0.42
ADABOOST CLASSIFIER	0.35
SUPPORT VECTOR MACHINE	0.28
GRASSMANN	0.14

Table 1: Performance table

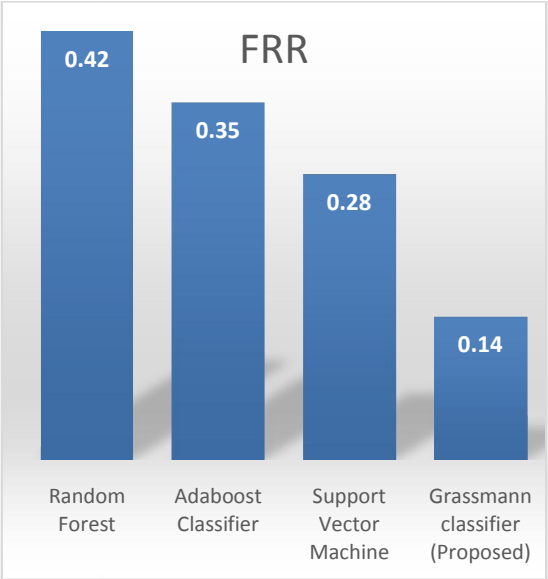

Fig 3: Performance char

DOI: 10.48175/IJARSCT-26004

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 13, April 2025
Impact Factor: 7.67

VI. CONCLUSION

Lack of biometric data for a certain feature causes unimodal biometric systems to malfunction. Therefore, using multimodal biometrics to provide stronger authentication is a solid option. This research found that multimodal biometric authentication addresses the problems associated with unimodal biometric systems, including non-universality, noisy data, and interclass similarities. Biometric identifiers in multimodal biometrics are fused according to decision, matcher score, and feature extraction levels. The several approaches now in use for the facial and ocular multimodal biometric system have been examined in this system.This study's major goal is to present an illuminating overview of the literature on periocular biometrics, including what features, feature extraction techniques, and matching schemes have already been studied and what problems still need to be resolved in this area. Periocular biometrics is an excellent solution to this issue. In the rapidly evolving world of technology, it is imperative that the system used for person identification and verification require minimal human interaction. Periocular area biometrics show great promise as a stand-alone modality and as a complement to face and iris biometrics. In many situations, periocular region outperformed face biometric due to several limitations such as position, variation in illumination, occlusion, and aging effect.

REFERENCES

[1] Drozdowski, Pawel, et al. "Feature fusion methods for indexing and retrieval of biometric data: Application to face recognition with privacy protection." IEEE Access 9 (2021): 139361-139378.
[2] Osorio-Roig, Dailé, et al. "Stable hash generation for efficient privacy-preserving face identification." IEEE Transactions on Biometrics, Behavior, and Identity Science 4.3 (2021): 333-348.
[3] Tran, Quang Nhat, Benjamin P. Turnbull, and Jiankun Hu. "Biometrics and privacy-preservation: How do they evolve?." IEEE Open Journal of the Computer Society 2 (2021): 179-191.
[4] Yang, Wencheng, et al. "A review of homomorphic encryption for privacy-preserving biometrics." Sensors 23.7 (2023): 3566.t
[5] Chai, Tong-Yuen, Bok-Min Goi, and Wun-She Yap. "Towards better performance for protected iris biometric system with confidence matrix." Symmetry 13.5 (2021): 910.
[6] Arjona, Rosario, and Iluminada Baturone. "A post-quantum biometric template protection scheme based on learning parity with noise (LPN) commitments." IEEE Access 8 (2020): 182355-182365.
[7] Drozdowski, Pawel, et al. "Feature fusion methods for indexing and retrieval of biometric data: Application to face recognition with privacy protection." IEEE Access 9 (2021): 139361-139378.
[8] Tran, Quang Nhat, et al. "A privacy-preserving biometric authentication system with binary classification in a zero-knowledge proof protocol." IEEE Open Journal of the Computer Society 3 (2021): 1-10.
[9] Aizi, Kamel, and Mohamed Ouslim. "Score level fusion in multi-biometric identification based on zones of interest." Journal of King Saud University-Computer and Information Sciences 34.1 (2022): 1498-1509.
[10] Castiglione, Aniello, Michele Nappi, and Stefano Ricciardi. "Trustworthy method for person identification in IIoT environments by means of facial dynamics." IEEE Transactions on Industrial Informatics 17.2 (2020): 766-774.
[11] V. Krivokuca Hahn and S. Marcel, "Biometric template protection for neural-network-based face recognition systems: A survey of methods and evaluation techniques," IEEE Trans. Inf. Forensics Security, vol. 18, pp. 639–666, 2022
[12]X. Dong, S. Kim, Z. Jin, J. Y. Hwang, S. Cho, and A. B. J. Teoh, "Open-set face identification with index-of-max hashing by learning," Pattern Recognit., vol. 103, Jul. 2020, Art. no. 107277.
[13]D. Osorio-Roig, C. Rathgeb, H. O. Shahreza, C. Busch, and S. Marcel, "Indexing protecteddeep face templates by frequent binary patterns," in Proc. IEEE Int. Joint Conf. Biometrics (IJCB), Oct. 2022, pp. 1–8.
[14]S. K. Choudhary and A. K. Naik, "Protected biometric identification with multiple finger vein," in Proc. 2nd Asian Conf. Innov. Technol. (ASIANCON), Aug. 2022, pp. 1–6.
[15] A. Sardar, S. Umer, C. Pero, and M. Nappi, "A novel cancelableFaceHashing technique based on non-invertible transformation with encryption and decryption template," IEEE Access, vol. 8, pp. 105263–105277, 2020.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 13, April 2025
Impact Factor: 7.67

[16] P. Drozdowski, N. Buchmann, C. Rathgeb, M. Margraf, and C. Busch, "On the application of homomorphic encryption to face identification," in Proc. Int. Conf. Biometrics Special Interest Group (BIOSIG), Sep. 2019, pp. 1–5
[17]D. Osorio-Roig, C. Rathgeb, P. Drozdowski, and C. Busch, "Stable hash generation for efficient privacy-preserving face identification," IEEE Trans. Biometrics, Behav., Identity Sci., vol. 4, no. 3, pp. 333–348, Jul. 2021.
[18] P. Drozdowski, F. Stockhardt, C. Rathgeb, D. Osorio-Roig, and C. Busch, "Feature fusion methods for indexing and retrieval of biometric data: Application to face recognition with privacy protection," IEEE Access, vol. 9, pp. 139361–139378, 2021.
[19] J. Kolberg, P. Bauspies, M. Gomez-Barrero, C. Rathgeb, M. Durmuth, and C. Busch, "Template protection based on homomorphic encryption: Computationally efficient application to iris-biometric verification and identification," in Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS), Dec. 2019, pp. 1–6
[20] P. Bauspie, J. Kolberg, P. Drozdowski, C. Rathgeb, and C. Busch, "Privacy-preserving preselection for protected biometric identification using public-key encryption with keyword search," IEEE Trans. Ind. Informat., vol. 19, no. 5, pp. 6972–6981, May 2023