iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** IV **Month of publication:** April 2021

DOI: https://doi.org/10.22214/ijraset.2021.33479

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IV Apr 2021- Available at www.ijraset.com

Multimodal Biometric Authentication Systems using Deep Learning

R. Aarthy[1], T. Aarthi[2], M. Elavarasi[3], R. Indhumathi[4], V. Karthika[5]
[1]*M. Tech.,* [2, 3, 4, 5]*B.E., CSE, Anna universityUniversity*

Abstract: ***The use of biometrics for identification operations needs that a specific biometric issue is distinctive for each person that it is calculated, which it's invariant over time. Biometrics similar to signatures, photographs, fingerprints, voiceprints, and retinal vas patterns all have noteworthy drawbacks. Though signatures and images are low cost and simple to get and store, they're impossible to spot automatically with assurance and are simply forged. The human iris, on the other hand, is an interior organ of attention and yet protected against the external environment, however, it is easily visible from among one meter of distance makes it an ideal biometric for an identification system with the benefit of speed, responsibility, and automation. In this work, it's planned to implement a face and iris recognition system, wherever unvaried closest purpose formula (ICP) and deep neural network is employed to section the face, eye, and iris region. In this proposal, the system propose a novel and strong approach for periocular recognition and feature extraction. In the approach, the face is detected in real-time face images which are then aligned and normalized. The proposed system utilizes an entire strip containing both the eyes as a periocular surface. For feature extraction, the model computed the magnitude responses of the image filtered with a filter bank of harder Gabor filters. Feature dimensions are reduced by applying the Grassmann algorithm. Hence, the system produces High-level security and the identification accuracy is well-maintained. Also, the real-time camera-based implementation and readability of multiple features at the time are focussed. The results show that the proposed method is effective for multi-modal biometric recognition.***
Keywords: Multi-model Biometrics, Periocular recognition, Grassmann algorithm, Gabor filters, and security.

I. INTRODUCTION

Biometrics is the measurement and statistical analysis (SA) of people's different physical and behavioral operations. The technology is mainly used for identification and access control AC or for defining individuals who are under surveillance. The common premise of biometric authentication is that every person can be finitely identified by their physical or behavioral traits. The name biometrics have functioned from the Greek format bio ‘means life’, and metric means to measure. Indication by biometric verification is attaining increasingly basic incorporate and finite security systems (Fss) consumer electronics and point-of-sale (POS) applications. Additionally, to security, the driving force behind biometric addressing has been attained, as there are no passwords to remember or security tokens to carry. Some biometric techniques, similar to measuring a person's gait, can operate with no official contact with the individual being addressed [1].

Components of biometric devices embrace the following:

A. A reader or scanning device to record the biometric issue being authenticated;
B. Package to convert the scanned biometric information into a uniform digital format and to check match points of the determined data to hold on data; and
C. An info to firmly store biometric information for comparison.

Biometric content could also be controlled in an exceedingly centralized database DB, though modern biometric implementations often rely instead on gathering biometric data locally, then cryptographically hashing it so authentication or verification are attained without direct access to the biometric information itself. Iris recognition is considered the foremost reliable and correct identity verification system available. Iris-recognition is an usual technique of biometric verification that uses mathematical pattern-recognition module on pictures of the irises of an user’s eyes, whose superior random patterns are different. Generally, biometric systems have been employed by surrounding the real-time world and deployed in the past decades. Many Biometric systems and fingerprints can be spoofed by recreating samples to the sensor. Several multi-model and mono-model biometric technology were highlighted previously to incur potential, accurate, and market value prospects. Simultaneously, promising biometrics evolving worldwide is an Electrocardiogram (ECG). To collect ECG fingerprints has been widely used for recognizing biometrics worldwide and for safety purposes. But, fingerprints do not maintain secrecy as a fake finger to spoof the biometric system is being provoked nowadays easily. Also, in ECG there is a major drawback that is ‘irrevocability’ that directly affects the performance.

The fake sensors by using some fake samples which do not need the biometric model. Additionally, sensor rank attacks are in the analog field. In the digital domain, there are cryptography and watermark which are not that useful.

II. RELATED WORKS

In recent times, periocular biometrics has captured a lot of attention from authors and some importance have been presented in the literature survey. The existing paper studies the effect of integrating bio-inspired techniques for dynamic disseminated auto-scaling on container orchestration series. The system focuses on running a self-managed container comparing different configurationoptions for the container. The performance of the models is validated through simulations subjected to synthetic and real-time workloads. Besides, multiple scaling options are assessed to define exceptional cases and enhancement areas [2].

Some of the examples of auto-scaling services are ECS Service Auto-Scaling[3], auto-scaling groups for Google Cloud, or Microsoft-Azure Autoscaling [4]. A rich conceptual metrics of auto-scaling systems is defined in the work by Qu *et al. [5]* And in the method of Al-Dhuraibi *et al.* [6]. Dynamic vertical scaling has also been addressed in the past through the dynamic allocation of memory to Virtual Machines, as described in the work by Moltó *et al.* Even public Cloud providers are starting to provide this functionality to some extent, as is the case of Jelastic [7]. To overcome the vulnerability of the model, 2 improved schemes are planned [8], [9]. However, Liu et al. [10] Noted that they're additionally insecure against familiar plaintext attacks (pas) below their security assumptions, and proposed a replacement privacy-preserving identification scheme utilizing the properties of orthogonal matrices and extra random numbers. In [11] the technique produces the Weighted Finite Element Method (FEM) which Achieves a low dimensional local periocular pattern. But the system restricts periocular region authentication for pose and illumination invariance using geometrical attributes. Further, Chen LC et al., in [12] produced a DeepLabv3 model for encoding and decoding model and proposed a Convolutional neural network algorithm. This algorithm Provides refined segmentation results. But, irrelevant features are extracted at the time of classification and security is not sufficient. Hence, the system suggests an enhanced theory as a proposed system. The proposed paper is segregated as follows. Section 1 involves an Introduction. Section 2 relates work and provides the necessary process. Section 3 gives the design of multi-modal biometrics and presents a secured system. The last section proves the accuracy of the design. Section 4 contains a result analysis and Section 5 concludes the paper.

III. PERIOCULAR RECOGNITION AND MULTI MODEL BIOMETRIC AUTHENTICATION

Multi-modal biometrics is systems, which are ensured of customizing more than one behavioral characteristic for addressing, verification, and identification. The proposed model provides a novel and robust approach for periocular recognition and multimodal authentication. In the model approach initially, the face is detected in real-time face images. Then, the detected face is aligned and normalized. The system utilizes the whole strip containing both the eyes as a periocular surface. For further feature extraction, the model computed the magnitude responses of the image filtered with a filter bank of harder Gabor filters. Feature dimensions are reduced by applying the Grassmann algorithm. The reduced feature vector is classified using Backpropagation neural network. The system demonstrates a promising authentication and identification accuracy; further the robustness of the proposed approach are ascertained by providing a comprehensive comparison with some of the well-known methods.

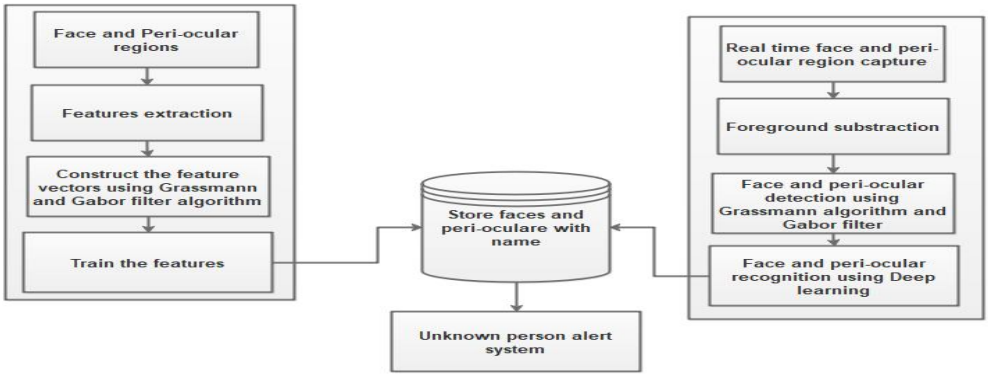


Figure 1. System Architecture of periocular recognition and Deep learning Approach

From figure 1. A framework is constructed where user authentication is done. then, the system undergoes a Face features extraction and Peri-ocular region extraction implementing the Grassmann algorithm and Gabor filter. Deep learning is evacuated and after learning the features are registered and stored. In case if any, unknown person occurs immediately an alert system is triggered.

The system contribution and the models are discussed briefly below:

A. Framework Construction And Face Features Extraction

Multi-modal biometric systems take input from single or multiple biometric devices for the measurement of two or more different biometric characteristics. In this module, the system can implement the framework for person authentication. Basic user details are entered into the system. Further, Facial feature extraction is very much important for the initialization of processing techniques like face tracking, facial expression recognition, or face recognition. Among all facial features, eye localization and detection are essential, from which locations of all other facial features are identified. In this module, basic facial feature points are extracted. These features are extracted using the Grassmann algorithm. Features are constructed as feature vectors.

B. Peri-Ocular Regions Extraction

Periocular related biometrics on reference to the automatic identification or classification of an user based upon features extracted from the area of the face that surrounds the eye. Normally, the facial area utilized extended from the top of the eyebrow to the cheek and indulge the area from the centre of the nose. These features are attained using the Gabor filter algorithm.

C. Face Registration And Classification

In deep learning feature vectors are obtained representing numeric or symbolic operations, named features, of an object in a mathematical, easily analyzable way. They are important for many different areas of deep learning and pattern processing. In this module, user details with face vector and peri-ocular region features are stored in the database. Based on these details, the user can be verified. In this module, implement a Backpropagation neural network algorithm. The Backpropagation algorithm looks for the minimum value of the error function in weight space using a technique called the delta rule or gradient descent. The weights that minimize the error function is then considered to be a solution to the learning problem. Users can log in with the user name, password and Capture the face details and peri-ocular details matching them to the database.

D. Alert System

If the match is found means, automatically recognized as a Known person. If the match is not found means, send an alert about the Unknown person to admin. Security and accuracy are maintained.

IV. RESULT ANALYSIS

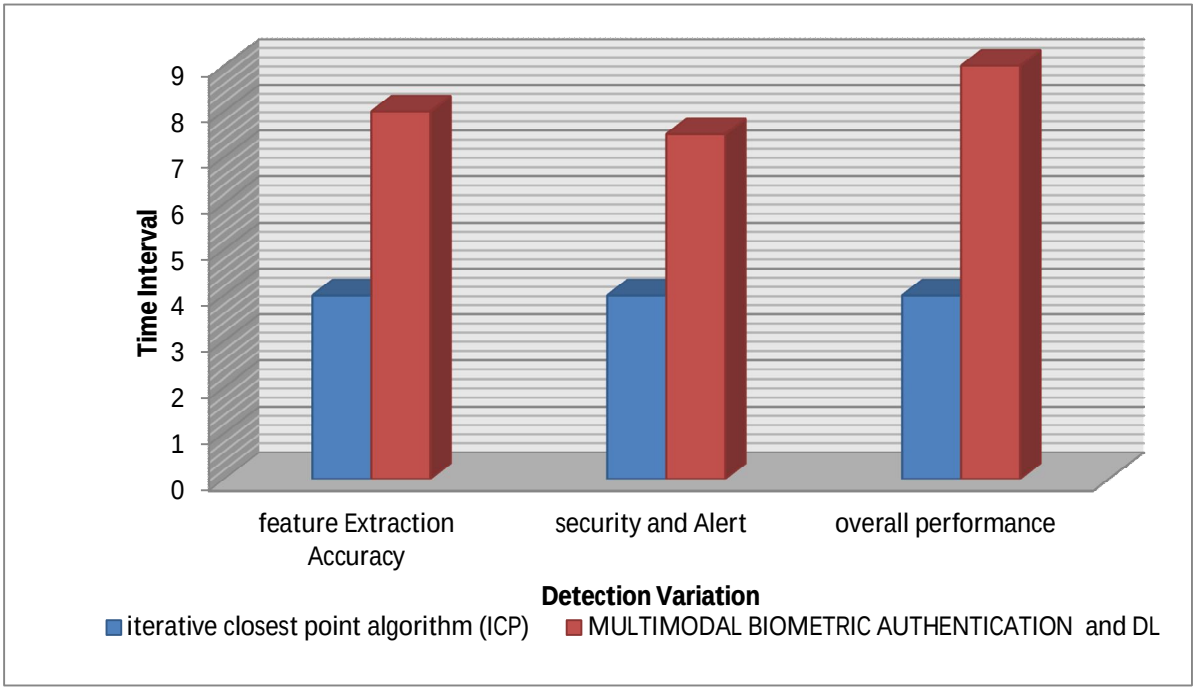


Figure 2. Comparative Analysis with Existing and Proposed System

In Figure 2. The development and performance of each one are noted, analyzed, and shown. From all the discussed terms and techniques the Multimodal biometric Authentication with Deep Learning is considered to be the best one.

V. CONCLUSION

Unimodal biometric systems fail due to a lack of biometric information for a particular feature. Thus, it is robust to use multimodal biometrics for providing greater authentication. This system observed that multimodal biometrics authentication solves the problem in unimodal biometrics systems such as inter-class, noisy data, and non-universality. In multimodal biometric, the biometric identifiers are fused based on feature extraction level, matcher score level, and decision level. In this project, the various existing techniques used for the face and ocular multimodal biometric system have been reviewed.

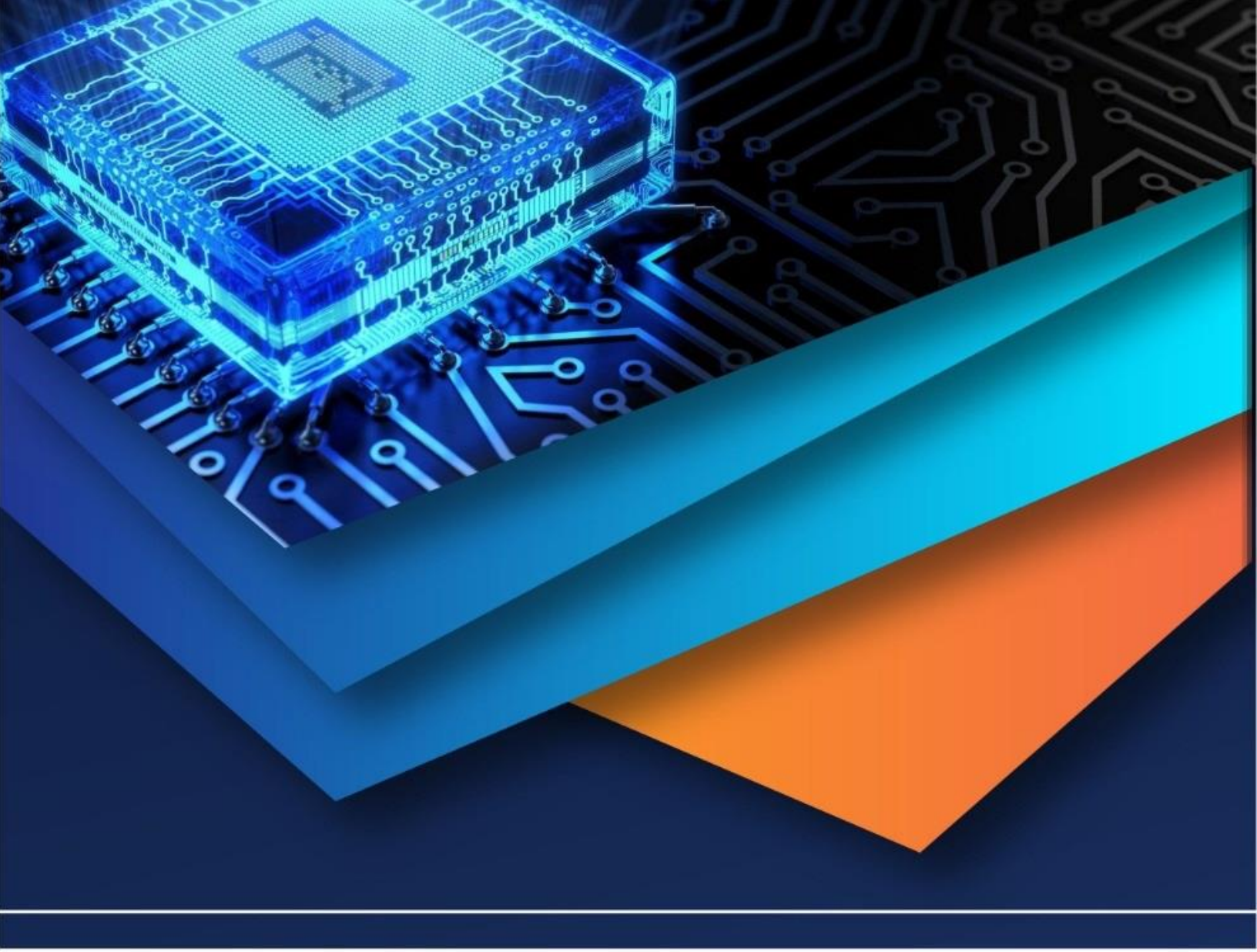
The primary objective of this proposed system is to provide a detailed view of periocular biometrics literature and about their features and feature extraction methods. Considering the fast-growing technological period, the model used for identification and verification of an individual must seek less user involvement.

For that 'periocular biometrics' is a very good option for this problem. The periocular region can be considered as a very promising method both as a single modality and as a supporting factor for face biometric. Further, for feature extraction, the model computed the magnitude responses of the image filtered with a filter bank of harder Gabor filters. Also, the proposal uses the Grassmann algorithm for reducing feature dimensions providing more security.

In future work, the finger vein and an ocular multimodal biometric system with novel feature extraction and matching techniques can be used to offer better accuracy and security.

REFERENCES

[1] Kim and K. S. Kim, "A Statistical Inference Attack on Privacy-Preserving Biometric Identification Scheme," in IEEE Access, vol. 9, pp. 37378-37385, 2021, doi: 10.1109/ACCESS.2021.3063693.
[2] J. Herrera and G. Moltó, "Toward Bio-Inspired Auto-Scaling Algorithms: An Elasticity Approach for Container Orchestration Platforms," in IEEE Access, vol. 8, pp. 52139-52150, 2020, doi: 10.1109/ACCESS.2020.2980852.
[3] Amazon. (2019). ECS Auto-Scaling. Accessed: Jan. 11, 2020. [Online]. Available: https://docs.aws.amazon.com/AmazonECS/latest/ developerguide/service-auto-scaling.html
[4] Google. (2019). Google Auto-Scaling. Accessed: Jan. 11, 2020. [Online]. Available: https://cloud.google.com/compute/docs/autoscaler/
[5] Microsoft. (2019). Azure Autoscale. Accessed: Jan. 11, 2020. [Online]. Available: https://azure.microsoft.com/en-us/features/autoscale/
[6] Y. Al-Dhuraibi, F. Paraiso, N. Djarallah, and P. Merle, ``Elasticity in cloud computing: State of the art and research challenges," IEEE Trans. Services Comput., vol. 11, no. 2, pp. 430_447, Mar. 2018.
[7] Jelastic. (2019). Jelastic Web Page. Accessed: Jan. 11, 2020. [Online]. Available: https://jelastic.com.
[8] L. Zhu, C. Zhang, C. Xu, X. Liu, and C. Huang, ‘‘An efficient and privacypreserving biometric identification scheme in cloud computing,’’ IEEE Access, vol. 6, pp. 19025–19033, 2018
[9] S. Hu, M. Li, Q. Wang, S. S. M. Chow, and M. Du, ‘‘Outsourced biometric identification with privacy,’’ IEEE Trans. Inf. Forensics Security, vol. 13, no. 10, pp. 2448–2463, Oct. 2018.
[10] C. Liu, X. Hu, Q. Zhang, J. Wei, and W. Liu, ‘‘An efficient biometric identification in cloud computing with enhanced privacy security,’’ IEEE Access, vol. 7, pp. 105363–105375, 2019.
[11] U. Park, R. Jillela, A Ross, A.K Jain, Periocular biometrics in the visible spectrum, IEEE transactions on information forensics and security, Vol 6, No. 1, March 2011, 10.1109/TIFS.2010.2096810.
[12] Chen LC., Zhu Y., Papandreou G., Schroff F., Adam H. (2018) Encoder-Decoder with Atrous Separable Convolution for Semantic Image Segmentation. In: Ferrari V., Hebert M., Sminchisescu C., Weiss Y. (eds) Computer Vision – ECCV 2018. ECCV 2018. Lecture Notes in Computer Science, vol 11211. Springer, Cham. https://doi.org/10.1007/978-3-030-01234-2_49.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY