University of Ibadan
Journal of Science and Logics in ICT Research

A Robust Biometric Authentication Framework for Access Control

[1]✉ Achimba T., [2] Okhuoya O. J., [3]Akinyede R. O., [4] Ibrahim A., [5]Alabi P. A., [6]Ateata G.
[1, 4, 5] Department of Computer Science, Mewar International University, Masaka, Nasarawa State, Nigeria.
[2]Computer Science Department, University of Benin, Benin city, Edo State, Nigeria.
[3]Information Systems and Security department, Federal university of technology, Akure, Ondo State.
[6] Office of the Deputy Registrar, Fidei Polytechnic, Gboko, Benue State, Nigeria.
[1]terfaachimba@gmail.com, [2]joseph.okhuoya@uniben.edu, [3]roakinyede@futa.edu.ng, [4]aisha.nsta@miu.edu.ng, [5]akubo.pa@miu.edu.ng, [6]graceateata@gmail.com

Abstract

Unauthorized access poses significant security concerns, jeopardizing the confidentiality, integrity, and availability of critical data and resources. Ensuring authorized access is essential for protecting sensitive systems across diverse fields, including smart buildings, military bases, hospitals, airports, and financial institutions. Biometric authentication has emerged as a reliable solution for access control, leveraging unique human traits for verification. However, traditional feature-based biometric systems are limited by environmental sensitivity, poor generalization, and vulnerability to spoofing, while deep learning-based systems face challenges such as high computational demands, reliance on large datasets, and lack of interpretability. To address these limitations, this research proposes a hybrid biometric authentication framework that combines the strengths of deep learning, specifically Residual Network (ResNet)-a Convolutional Neural Network (CNN), with the Local Binary Pattern (LBP) method. By integrating interpretable, computationally efficient features from LBP with ResNet's ability to learn complex patterns, the framework improves robustness, reduces overfitting, and enhances scalability. This approach offers a balanced, efficient solution for secure biometric authentication, tailored for real-world and resource-constrained environments**.**

Keywords: *Computer Security, Access Control, Biometric Authentication, Deep Learning, Local Binary Pattern*

1. Introduction

The proliferation of Information Technology (IT) has raised significant concerns about risks associated with insecurity, including attacks on and compromises of network systems and services. These risks often jeopardize the confidentiality, integrity, and availability of data due to inadequate IT security measures such as unauthorized access [1]. Ensuring data and individual privacy protection requires robust security practices, among which access control plays a critical role. Access control mechanisms are essential for safeguarding resources and critical infrastructures, including smart buildings, military bases, hospitals, and airports [2].

Without adequate access control, issues like unauthorized access frequently lead to security breaches. User authentication, an essential component of access control, is a widely adopted method for verifying individuals seeking access to sensitive resources. This process prevents unauthorized users from accessing systems like Automated Teller Machines, credit card platforms, and border control systems [3].

Biometric technology has emerged as a promising solution to overcome limitations of traditional authentication systems, which are often susceptible to loss, forgetfulness, and brute force attacks. Biometrics, which leverages unique human traits for authentication, has seen significant advances in recent years [4]. While traditional biometric systems rely on feature-based approaches, they face challenges such as sensitivity to environmental conditions, vulnerability to spoofing attacks, and scalability issues [5].

To address these limitations, researchers have turned to deep learning approaches, which have demonstrated remarkable improvements in biometric authentication. However, these

Achimba T., Okhuoya O. J., Akinyede R.O., Ibrahim A., Alabi P.A. and Ateata G. (2025). A Robust Biometric Authentication Framework for Access Control. *University of Ibadan Journal of Science and Logics in ICT Research (UIJSLICTR),* Vol. 13 No. 1, pp. 239 - 246

methods are highly dependent on large datasets, computationally demanding, and prone to overfitting, particularly with imbalanced data. Furthermore, their "black-box" nature and vulnerability to adversarial attacks present additional challenges [6].

To address these challenges, this research aims to develop a face biometric authentication framework that combines deep learning, specifically the ResNet CNN, with a traditional feature-based method, the Local Binary Pattern (LBP).The LBP method excels in capturing hand-crafted, interpretable features that are computationally efficient and robust in simple scenarios. Conversely, the ResNet CNN architecture can automatically learn intricate, high-level features from data, effectively handling complex patterns and diverse datasets.

By combining these approaches, traditional features complement deep learning features, enhancing robustness and interpretability. This hybrid approach mitigates reliance on large datasets by providing a strong baseline representation through traditional methods while enabling deep learning to refine and adapt these features to complex patterns. Furthermore, this combination reduces overfitting risks, improves generalization, and lowers computational demands by simplifying deep learning models through feature-level fusion. This synergy offers a balanced and efficient solution, addressing the limitations of both traditional and deep learning approaches.

2. Related Works

Iwasokun *et. al.* [7] presented a Fingerprint-Based Authorization Platform for Electronic-Based Examination was presented. This research was motivated by the need to replace the conventional techniques of administering e-exams which poses as a major threat due to its susceptibility to share and transfer.The system is limited with the fact users will have to make contacts with the sensors, standing the risk of contracting diseases

Elmir *et. al.* [8] utilized Raspberry Pi technology to present an improved access control system that is based on biometric recognition. The research was motivated by the need to provide a more secure and reliable means of access control as compared to the traditional methods that are based on keys or passwords. The system has potential challenges in varying lighting conditions and is vulnerable to spoofing attacks.

A Multi-Level Access Control System in Automated Teller Machines was presented by Oladimeji *et. al.* [9]. The research is motivated by the need to eliminate the issues encountered with the traditional authentication systems. The system suffers difficulty in handling complex backgrounds. Venna and Inampudi [10] presented a Multimodal biometric authentication system. This research was motivated by the need to provide security solutions to the vulnerabilities and attacks exploiting mobile devices. The specific objective of this research is to introduce a multimodal biometric authentication based on cryptographic generation system. Fusion is done only at feature level which might result in a feature vector with huge dimensionality, giving rise to the problem of the curse of dimensionality. Users suffer discomforts as they have to pass through many scans in order to provide biometric traits.

Bharathi *et. al.* [11] presented an enhanced security system with multilevel authentication. The system is motivated by the need to eliminate the shortcomings of the previous systems which include low optimization. The system is likely to experience explosive dimensionality issue. Rabiya and Patil [12] proposed a Multilevel Biometric Based Authentication System. The research is motivated by the need to tackle the vulnerabilities of the traditional authentication systems. The system is inflexible to diverse data.

Omotosho *et. al* [13] developed a biometric system based on convolutional neural network. This research was motivated by the need to overcome the limitations of unimodal biometrics system and improve recognition. The system might result in a feature vector with huge dimensionality, giving rise to the problem of the curse of dimensionality. Also, the experiments were done using a smaller number of subjects in the datasets. A Biometrics System using Multilevel fusion and Deep learning Techniques was presented by Arjun and Prakash [14]. The research was motivated by the need to tighten Computer security by using complex security systems. The research methodology involves extracting Histogram of Oriented Gradients features from Fingerprints and Signature Biometric traits and feature fusion applied at two levels. The system might result in a feature vector with huge dimensionality, giving rise to the problem of the curse of dimensionality. Users also stand the risk of contracting diseases.

Choras [15] proposed a Multimodal biometric system for person authentication. This research was motivated by the inability of unimodal systems to effectively identify people. Users of the system experience discomforts as they must pass through many scans to provide biometric traits. The system makes use of Gabor technique with high redundancy of features, which might reduce recognition rates.
Li *et. al.* [16] presented a Face Recognition AI Technology Based on Deep Learning. The research addresses challenges in traditional face recognition, such as time consumption, labor, and issues with illumination, expression, and occlusion. The model experiences reduction in the algorithm execution efficiency.

Alay and Al-Baity [17] presented a Deep Learning Approach for Biometric Recognition System. Variations in lighting, facial expressions, poses, and occlusions (e.g., masks, glasses) can degrade performance. Also, limited access to high-quality iris datasets may restrict model training and evaluation. Arthi *et.al.* [18] presented a Deep Learning Based Multi-Modal Biometric Security System. The research was motivated by the need to strengthen the previous systems characterized by traditional methods. The system experiences lower learning rates and reduced time for training. Also, tuning of hyper parameters and network predictions need to be improved. Singh [19] presented a Multimodal Biometric Authentication System using Machine Learning. The research was motivated by the need to address the challenges encountered with traditional authentication systems. The system might result in a feature vector with huge dimensionality, giving rise to the problem of the curse of dimensionality.

Betrand *et. al.* [20] developed an Authentication System Using Biometric Data for Face Recognition. The research is motivated by the inefficiencies and inaccuracies of traditional attendance systems. These systems are prone to errors, manipulation, and delays, particularly in large educational institutions. The study seeks to address these limitations by leveraging facial recognition technology, which offers non-intrusiveness, usability, and high accuracy, to create a reliable and automated attendance management system. The study uses the Object-Oriented Analysis and Design Methodology (OOADM) to develop the proposed biometric attendance system. A client-server model integrates user interfaces, face recognition modules, and database management. The face Recognition Module employs a pre-trained algorithms to detect and match facial features. The system utilizes Kotlin programming language and TensorFlow for real-time face recognition. The research acknowledges several challenges and limitations which include environmental sensitivity, privacy concerns, reliance on deep learning algorithms and computational resources which might impact scalability in large-scale implementations.

A Biometric Face Authentication System for Secure Smart Office Environments was developed by Siswanto *et. al.* [21]. The paper is motivated by the need for efficient and secure access control systems in smart office environments. Biometric systems, particularly facial recognition, offer a more reliable and user-friendly solution. This research addresses gaps in existing IoT-based smart office systems by designing a cost-effective and efficient facial biometric authentication system to enhance security and user experience. The research uses a Design Research Methodology (DRM), which includes the Creation of a hardware prototype comprising ESP32 CAM for facial image capture and template creation, NodeMCU microcontroller for database storage and access control management. The system's performance may be affected by variations in lighting, facial expressions, and poses. Dependence on low-cost components might limit scalability and durability in larger systems. Limited storage capacity in the NodeMCU microcontroller could restrict the number of registered users.

Alharbi and Alshanbari [22] developed Face-Voice Based Multimodal Biometric Authentication System. The research implements a voice recognition system using Gaussian Mixture Models (GMM) for high accuracy and robustness against noise. FaceNet, a state-of-the-art neural network, is utilized for extracting facial embeddings to improve face recognition accuracy. The system was trained and tested on a limited dataset (700 samples), which might impact generalization to larger populations. Variations in lighting conditions and background noise could affect face and voice recognition performance. Combining GMM and FaceNet might introduce computational complexity, especially for real-time applications. System accuracy relies heavily on the quality of input audio and video samples.

Mon *et. al.* [23] worked on a Periocular Biometric-Based Access Control Systems. The study is driven by the increasing demand for

secure and reliable access control systems. Traditional methods, such as passwords and PINs, are vulnerable to hacking and theft. The aim to develop an access control system using periocular biometrics for secure and reliable authentication. Emgu CV (a .NET wrapper for OpenCV) is used for image processing and feature extraction, Rapid Application Development (RAD) methodology to facilitate iterative prototyping and system customization. Limited dataset is used for testing and development, which may affect generalization to diverse populations. Performance may degrade under varying lighting conditions or with poor-quality images. Lack of a standard protocol for defining the exact periocular region might introduce inconsistencies.

Rahouma and Mahfouz [24] developed a Face Recognition System Based on API Mobile Vision and Normalized Features of Still Images. The research is motivated by the increasing need for efficient and secure biometric authentication systems on mobile devices. Traditional security methods like passwords are prone to hacking and theft, while biometric systems, particularly face recognition, offer enhanced security and convenience. The research aims to design and implement a robust and efficient face recognition system for Android mobile devices using normalized features and correlation-based recognition. Google's Mobile Vision API is used to detect facial landmarks (e.g., eyes, nose, mouth, cheeks).The study extracted 30 geometrical measurements by calculating distances between key facial landmarks. Pearson Correlation Coefficients was used to compare test face features against stored features in the database. The study addresses the limitations of existing mobile-based face recognition systems, such as processing constraints, storage limitations, and accuracy issues, by leveraging advanced techniques like Google's Mobile Vision API and Pearson Correlation. Performance depends on the quality of input images; poorly lit or misaligned images may affect accuracy. The system uses pre-stored images and lacks real-time recognition capabilities. Backgrounds or lighting inconsistencies may influence detection accuracy. The system is optimized for Android devices and as a result, performance on other platforms or low-spec devices may vary.

Rahim and Mohamad [25] developed a Biometric Authentication system that uses Face Recognition Algorithms for a Class Attendance System. The motivation for this research stems from the inefficiencies and vulnerabilities of conventional class attendance systems, which rely on handwritten signatures. These systems are prone to manipulation, such as forging signatures or having peers sign on behalf of absentees. To address this, the paper explores biometric authentication, particularly facial recognition, as a robust and reliable method to ensure accurate attendance tracking. Facial recognition is chosen due to its non-intrusive nature, ease of data collection, and superior performance compared to other biometric modalities. A training database was created using facial images of eight students, with variations in angle, expression, and lighting. Each subject contributed ten images under different conditions: straight faces, angled poses, expressive faces, and low-light settings. LBP, PCA, and HOG were used for feature extraction, while the classifiers involved were SVM for LBP and HOG, and Euclidean distance for PCA. Performance significantly degrades under low illumination conditions, especially for PCA and LBP methods. Limited testing dataset of eight students restricts the generalizability of results to larger populations. System accuracy depends on controlled conditions, such as proper alignment of the face. HOG+SVM achieves the highest accuracy but is slower than PCA, indicating a trade-off between accuracy and processing speed.

Tiong *et. al.* [26] implemented an RGB-Orthogonal Combination-Local Binary Coded Pattern (OCLBCP) Dual-Stream CNN for Periocular recognition. The research is motivated by the need to address the challenges of periocular recognition in the unconstrained environments. The research is limited by the fact that it does not have the ability to recognize subjects wearing sun glasses.

The limitations of the reviewed models above include the following: The use of contact-based systems poses significant health risks due to the potential transmission of diseases, making them unsuitable for environments requiring high hygiene standards. Additionally, these systems are highly sensitive to environmental factors, such as varying lighting conditions, which can degrade their performance. They are also vulnerable to spoofing attacks and suffer from the curse of dimensionality caused by high-dimensional feature vectors. User discomfort arises from the need for multiple scans during authentication, while limited dataset sizes restrict the system's ability to generalize across diverse populations and scenarios. Performance degradation occurs due to poor-quality images, occlusions, or variations in facial expressions

and poses. Scalability issues, privacy concerns, and the computational demands of handling large-scale biometric data further hinder their implementation. Moreover, algorithmic inefficiencies result in struggles with real-time recognition capabilities, and trade-offs between accuracy and processing speed reduce effectiveness, particularly in resource-constrained environments. Collectively, these limitations underscore the urgent need for innovative solutions to enhance the robustness, efficiency, and adaptability of biometric authentication technologies.

3. Methodology

This section focuses on the structural and functional aspects of the face biometric authentication system. It provides an in-depth explanation of the system's architecture, design components, and data flow to help understand how the system works. The system's workflow is shown in Figure 1.

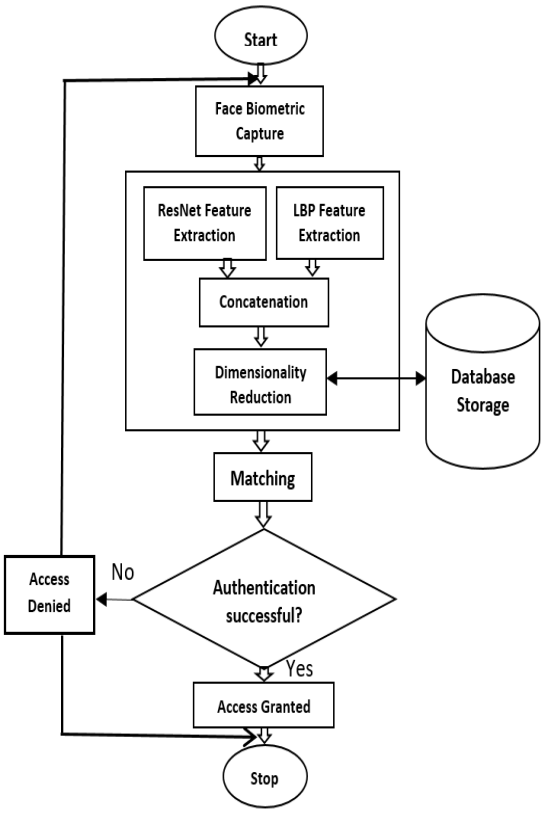

Figure 1 System Work flow

A. Functional Modules of the System

The system is divided into several functional modules, each serving a specific purpose:

1) User Interface Module

This module facilitates user interaction with the system. It allows users to enroll, authenticate, or manage their profiles.

2) Data Acquisition Module

This handles the capture of face images or video frames using cameras. It ensures that image quality and resolution meet system requirements.

3) Preprocessing Module

This performs image normalization, face alignment, and noise reduction. It ensures consistency across captured images under varying conditions.

4) Feature Extraction Module

This module **e**xtracts unique face features using deep learning and traditional feature-based methods.

5} Authentication and Decision Module

This module matches the extracted features with stored templates using the Support Vector Machine (SVM) classifier.

6) Database Module

This module **s**tores user templates securely with encryption. It handles data retrieval during matching.

B. Feature Extraction Techniques

This section provides a detailed description of the feature extraction techniques used in the feature extraction module mentioned earlier.

An approach that combines deep learning and traditional feature-based methods is used, with the following procedure.

1) Deep Learning-Based Approach

The Residual Network (ResNet) CNN architecture is used to extract discriminative features from facial images. For a convolutional layer, the core operation is the convolution of an input image with a set of filters (kernels). The output of this operation is called a feature map.

The equation for a single output pixel (i, j) of the feature map is:

$$F_{i,j} = \sum_{m=0}^{k-1} \sum_{n=0}^{k-1} (I_{i+m,j+n}\ K_{m,n}) + \quad b \qquad (1)$$

Where:
$F_{i,j}$ = is the value of the feature map at position (i, j).

I is the input image.

K is the filter (kernel) with dimensions $k \times k$.

b is the bias term.

m and n are indices that iterate over the spatial dimensions of the convolutional filter (kernel).

The Rectified Linear Unit (ReLU) activation function is applied to introduce non-linearity. The ReLU function is:

$$A_{i,j} = \max(0, F_{i,j}) \quad (2)$$

Where:
$A_{i,j}$ is the activated output at position (i, j).

Pooling is used to reduce the spatial dimensions of the feature map. For max pooling, the output is:

$$P_{i,j} = \max_{(m,n) \in pooling\ window} A_{i+m,j+n} \quad (3)$$

Where:
$P_{i,j}$ is the pooled feature map value at position (i, j).

The pooling window is typically 2×2 or 3×3.

The fully connected (FC) layer is used to combine the features extracted and perform classification. The output y of a fully connected layer is:

$$y = \sigma\left(\sum_{i=1}^{n}(w_i . x_i) + b\right) \quad (4)$$

Where:
w_i are the weights of the connections.

x_i are the inputs from the previous layer.

b is the bias term.

σ is the activation function

2) Traditional Feature-Based Approach

In this approach, the Local Binary Patterns (LBP) is used to extract texture features from the face region. LBP captures local texture information, which is useful under varying lighting conditions.

The biometric feature extraction is done using the following procedure:

For each pixel (i, j) in the face image, a 3×3 neighbor- hood is defined. The LBP value is then calculated using the equation below.

$$LBP(i,j) = \sum_{k=0}^{7} s(l_n - l_c) \times 2^k \quad (5)$$

Where
l_c is the grey value of the center pixel $(i. j)$

l_n is the grey values of the 8 surrounding pixels

k represents the position of the neighbor pixel in the 3×3 neighborhood, where k=0, 1… 7.

s (x) is the thresholding function, defined as:

$$s(x) = \begin{cases} 1, if\ x \geq 0 \\ 0, if\ x < 0 \end{cases} \quad (6)$$

The histogram of the LBP values for the entire face region is then computed. This histogram of LBP values serves as the feature vector.

C) Feature Fusion Strategy

1) Concatenation

The deep learning features are concatenated with the LBP features to form a combined feature vector. This fusion leverages both high-level and texture-specific information.

Feature fusion in a hybrid biometric authentication framework can be represented mathematically as the combination of features extracted from traditional methods and deep learning models. Let the feature vectors obtained from Local Binary Pattern (LBP) and Residual Network (ResNet) be F_{LBP} and F_{ResNet}, respectively. The fused feature vector, F_{fused}, can be expressed as:

$$F_{fused} = \alpha . F_{LBP} + \beta . F_{ResNet} \quad (7)$$

Where:

- α and β are weighting coefficients that determine the contribution of F_{LBP} and F_{ResNet} to the fused feature vector. These weights can be empirically determined or optimized based on the application and dataset.
- $F_{LBP} \in R^m$ is the feature vector extracted using the LBP method, capturing text-based information.
- $F_{ResNet} \in R^n$ is the feature vector extracted using the ResNet model, capturing deep, hierarchical features.
- R^m and R^n denote m-dimensional and n-dimensional spaces of real-valued features, respectively. These spaces provide the domain within which the feature vectors are defined.

2) Dimensionality Reduction

The Principal Component Analysis (PCA) is then applied to reduce the dimensionality of the fused feature vector. PCA helps retain essential information while reducing computational complexity.

D) Authentication and Decision Strategy

A Support Vector Machine (SVM) classifier is used for final decision-making, categorizing whether the presented biometric matches the authorized user or not. **A**uthentication decisions are made based on a predefined threshold (T), as shown below:

$$y = \begin{cases} 1, & if\ F_{fused} \geq T \\ 0, & if\ F_{fused} < T \end{cases} \qquad (8)$$

4. Conclusion

This paper presents a biometric authentication framework that integrates deep learning with traditional feature extraction techniques, combining ResNet CNN and Local Binary Pattern (LBP). By merging interpretable features with the deep learning capabilities of ResNet, the framework provides a scalable and efficient solution for secure authentication. The implementation is currently underway, utilizing Python and OpenCV for system development and training, while MySQL is used for securely storing biometric templates.

The framework holds significant potential for real-world applications across various sectors, including smart buildings, airports, healthcare facilities, and financial institutions. Its modular design enables seamless integration into existing security systems, facilitating widespread adoption. Future research should focus on implementation and performance evaluation across diverse scenarios, addressing challenges such as privacy concerns, evolving spoofing techniques, and adversarial attacks. This work represents a step forward in the advancement of biometric authentication systems, paving the way for more secure, efficient, and interpretable solutions in an era of increasing security demands.

References

[1] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186.

[2] Ali, W., & Arsalan, H. (2024). Ensuring Data Security and Privacy: Strategies for Targeted Data Discovery, Data Management Systems, and Private Data Access in Educational Settings.

[3] Achimba T., Alaaga J., & Kwaghbee S (2021). Multi-modal biometrics systems: Concepts, strengths, challenges and solutions. *International Journal*, *10* (3).

[4] Iwasokun, G. B., Akinyokun, O. C., & Omomule, T. G. (2019). Design of e-invigilation framework using multi-modal biometrics. In *2019 15th International Conference on Electronics, Computer and Computation (ICECCO)* (pp. 1-6). IEEE.

[5] Lien, C. W., & Vhaduri, S. (2023). Challenges and opportunities of biometric user authentication in the age of iot: A survey. *ACM Computing Surveys*, *56*(1), 1-37.

[6] Maiti, D., Basak, M., & Das, D (2024). Fingerprint Bio-metric: Confronting Challenges, Embracing Evolution, and Extending Utility-A Review. *Journal of Engineering Research and Sciences*, 3(9):26-60

[7] Iwasokun, G., Akinyokun, O., Akinyede, R., & Udoh, S. (2016). Fingerprint-based authorization platform for electronic-based examination. *Journal of Scientific Research and Reports*, *12*(6), 1-10.

[8] Elmir, Y., Abdelaziz, A., & Haidas, M. (2023). Design and Implementation of Embedded Biometric-Based Access Control System with Electronic Lock using Raspberry Pi. *J. Ilm. Tek. Elektro Komput. Dan Inform. JITEKI*, *9*(2), 429-443.

[9] Oladimeji, I. W., Olusayo, O. E., Folasade, I. M., & Taiwo, O. A. (2021). Multi-level access control system in automated teller machines. *International Journal of Marketing and Technology*, *11*(6), 1-9.

[10] Venna, S. R., & Inampudi, R. B. (2019).MMBAS-NS: Multimodal Biometric Authentication System and Key Generation Algorithm for Network Security on Mobile Phones. *International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7 Issue-5S2*

[11]Bharathi S, Abarna A, Arun Pandeeswaran RV and Akil G (2023): "enhanced security with multilevel authentication for accessing biometric database", Eur. Chem. Bull. 2023, 12 (Si6), 5434 – 5447

[12]Rabiya S and Patil G .A (2019): "Multilevel Biometric Based Authentication System", Journal of Emerging Technologies and Innovative Research (JETIR), Volume 6, Issue 2.

[13]Omotosho L., Ogundoyin I., Adebayo O & Oyeniyi J. (2021): "An enhanced multimodal biometric system based on convolutional neural

network", journal of engineering studies and research – volume 27 (2021) no. 2.

[14]Arjun, B. C., & Prakash, H. N. (2021). Multimodal biometric recognition system using face and finger vein biometric traits with feature and decision level fusion techniques. *International Journal of Computer Theory and Engineering*, *13*(4), 123-128.

[15]Choras, R. S. (2019). Multimodal biometrics for person authentication. *Security and Privacy From a Legal, Ethical, and Technical Perspective*, 177.

[16] Li, W., Li, J., & Zhou, J. (2022). Deblurring method of face recognition AI technology based on deep learning. *Advances in Multimedia*, *2022*(1), 9146711.

[17] Alay, N., & Al-Baity, H. H. (2020). Deep learning approach for multimodal biometric recognition system based on fusion of iris, face, and finger vein traits. *Sensors*, *20*(19), 5523.

[18] Arthi, R., Manojkumar, D., Abraham, A., Kishan, A. R., & Sattenapalli, A. (2022). Deep Learning Based Multi-Modal Biometric Security System Using Visible Light Communication. *WSEAS Transactions on Systems and Control*, *17*, 34-41.

[19]Singh, D. (2022). Design and analysis of multimodal biometric authentication system using machine learning. *Journal of Algebraic Statistics*, *13*(3), 2911-2919.

[20] Betrand, C. U., Onyema, C. J., Benson-Emenike, M. E., & Kelechi, D. A. (2023). Authentication system using biometric data for face recognition. International Journal of Sustainable Development Research, 9(4), 68–78. https://doi.org/10.11648/j.ijsdr.20230904.12

[21] Siswanto, A., Efendi, A., & Kadir, E. A. (2023). Biometric face authentication system for secure smart office environments. Indonesian Journal of Electrical Engineering and Computer Science, 32(2), 1134–1141. https://doi.org/10.11591/ijeecs.v32.i2.pp1134-1141

[22] Alharbi, B., & Alshanbari, H. S. (2023). Face-voice based multimodal biometric authentication system via FaceNet and GMM. PeerJ Computer Science, 9, e1468. https://doi.org/10.7717/peerj-cs.1468