Grenze International Journal of Engineering and Technology, June Issue

Secure Facial Authentication via Fuzzy Logic

Yathish K[1], Mohini Ganapati Pai[2] and Likith S[3]
[1-3]Department of Computer Science and Business System, Canara Engineering College, Benjanapadavu, India
Email: yathishk@canaraengineering.in, mohinipai094@gmail.com, likithsuresh62@gmail.com

***Abstract*— In this paper, a Secure Facial Authentication System has been proposed and this is meant to increase the level of data security because the password checks are combined with live facial recognition using Fuzzy Logic. Old-fashioned passwords are usually insecure and the regular facial recognition devices fail to adjust to the changing facial expression and lighting conditions. In the quest to solve these issues, our system adaptation makes use of the fuzzy logic which is very good at drawing flexible decisions in cases where the facial data available is ambiguous or unclear. Users enter their name, email address, phone number and password during the registration process and take five live pictures of their faces to create a fuzzy-based facial dataset. To log in, the system not only checks the credentials used but also the live facial data and only the fuzzy similarity score that is within the required threshold allows one to log in. Once they have been authenticated successfully they can obtain a safe digital vault where they can save their files. Additionally, the system has liveness detection which helps to avoid entry into the system using a static image or photographed video. Integrating real-time biometric authentication with fuzzy logic, this solution significantly improves the level of security, flexibility, and end-user trustfulness, which is why it will be a solid solution to the problems of the modern digital environment.**

***Keywords*— Fuzzy Logic, Facial Authentication, Liveness Detection, Secure Vault, Biometric Security, Password Verification, Image Processing, Data Protection.**

I. INTRODUCTION

Having a personal information is of utmost importance in modern digital world, where the conventional password system is prone to human factor and security attacks. The susceptibility has contributed to the emergence of the biometric authentication, especially face recognition, which is said to be convenient and hands-free in terms of interaction and boasts of high user acceptance. [1], [16] [19].

Conventional facial recognition systems have issues related to the natural variations in the facial expressions, angles and user behaviors. Fixed, threshold-based matching algorithms are unable to adjust and provide unreliable results and make them more susceptible to spoofing attacks [3], [7], [10]. Researchers are considering the fuzzy logic as the possible solution to the solution to uncertain biometric data. It uses similarity values that are graded as opposed to binary responses, which is suitable in facial recognition where differences are caused by stored templates. [1], [3], [14], [17].

This paper introduces a Secure Facial Authentication System, which is a password validation system that uses Fuzzy Logic to combine real-time face recognition and password verification. When registering, users are asked to supply important details and several live facial images so as to create a strong fuzzy feature record.

Grenze ID: 01.GIJET.12.2.51_23

To facilitate authentication, the system compares similarities of the stored image and the live facial input by analyzing the credentials and live facial image through a fuzzy inference mechanism. Authority to gain access is according to an effective fuzzy confidence score that improves flexibility in decision making and minimizes false matches.

Moreover, the studies of anti-spoofing techniques also emphasize the growing threat of unauthorized access through printed images, screens, or deep fake attacks [8], [15], [21], [23], [27]. To overcome such risks, the system uses the live face detection methods which are based on the current trends in the liveness verification and anti-spoofing research and ensures that only the genuine human faces are authorized to the entry process.

This proposed solution, combining fuzzy logic-based decision-making with a two-layer verification system, is highly adaptable with a high level of security and high-level spoofing, which is why it was implemented in secure file storage, enterprise access control, and digital verification platforms.

This study makes several important contributions, including:

- Combining fuzzy logic and facial recognition to address the uncertainties of facial features, which enable a more flexible method of authentication process [1], [3], [14], [17].
- Implementing the use of a dual-layer authentication system, which involves the entry of passwords and an additional fuzzy-based live face matching, which offers an additional level of security [12], [13].
- Developing a secure vault module, which restricts access to sensitive data and inhibits unauthorized access with the use of photos or pre-recorded videos [7], [10], [27].
- Demonstrating, based on the literature review, that the fuzzy logic and liveness detection methods are most beneficial in terms of the reliability of biometric systems in practical applications [1], [3], [8], [15], [21].

II. Literature Review

Facial recognition is now among the most popular biometric technologies due to the ease of use and the fact that it does not need any physical contacts. But still, it is a significant challenge to achieve reliable and consistent performance in practical contexts. Initial studies indicated that fuzzy logic was capable of operating with the natural ambiguity in the facial expressions, thereby enabling recognition systems to be more adaptable in face recognition when an individual changed his/her expression, pose, or lighting [1], [2]. With the development of the field, scientists created more sophisticated fuzzy-learning algorithms, including Fuzzy Generalized 2D LDA and neuro-fuzzy models, which were more adaptable to a variety of users and settings [3], [4]. Type-2 fuzzy systems further extended this by operating at deeper levels of uncertainty when extracting features, particularly in poor-quality or deformed images [5], [4].HybridsystemsHere, fuzzy logic was combined with PCA, CNNs or other soft-computing methods and had the advantage of explaining decisions and being data-driven [6], [7], [29]. Simultaneously, techniques of multimodal biometrics which combine the data of face, fingerprint, or palmprint sensors were investigated using fuzzy-based fusion techniques, as a means to decrease instability and increase the total accuracy [12], [13], [14], [17]. Other more recent investigations have gone as far as using neutrosophic fuzzy models and hybrid AHP-TOPSIS assessments schemes and have demonstrated that fuzzy logic remains a significant factor in the development of secure and reliable biometric systems [25].

The studies conducted in face liveness detection and anti-spoofing have developed at a fast pace because systems incorporating facial recognition are under increasing attacks due to the printed photos, re-recorded videos, masks, and even deep fake media. Numerous recent survey studies indicate that despite its exemplary performance on controlled datasets, deep-learning models frequently fail to extend their performance to new settings and spoof types--it can be stated that domain shift is one of the key issues in Presentation Attack Detection (PAD) [8], [15], [21], [22]. In order to counteract this, texture-based features such as EBHOG, micro-motion cues and entropy-based analysis have demonstrated a great potential to capture small variations to differentiate real faces and spoofed faces [7], [10], [11].CNN architectures, multimodal fusion and temporal behavior analysis has now been used in modern PAD systems to serve as supplementary strength to counteract spoofing. There are approaches, which also assist online adaptive personalization, to enable the models to adapt in real time to the properties of individual users [23], [27], [28]. Concurrently, other works are investigating mobile-friendly solutions, distortion-based checks, AI-based quality assessment, and IoT-adapted intelligent sensing to establish such checks as more secure and balanced [18], [20], [30].Surveys on multimodal authentication and continuous authentication also demonstrate that the combination of facial recognition with other signals, including passwords, motion patterns, or secondary biometrics, can result in a less vulnerable and more balanced system [9], [12], [13], [26]. This would greatly appear in line with the suggested fuzzy logic-based dual-layer design because it integrates password authentication, the fuzzy similarity scoring, and live-face image detection into a single and trusted security system.

Here is a comparison between Traditional and Fuzzy Logic–based Facial Recognition Approaches:

TABLE I: TRADITIONAL VS FUZZY LOGIC RECOGNITION

Traditional Facial Recognition	Fuzzy Logic–Based Facial Recognition
Depends on strict threshold-based matching, leading to false rejections under minor facial variations [1], [3], [7].	Uses flexible similarity scoring to handle changes in pose, expression, and image quality [1], [2], [14].
Highly affected by lighting, noise, and low-quality inputs [7], [22].	Tolerant to uncertain or imperfect facial data due to fuzzy rule reasoning [3], [4], [20].
Older systems offer weak spoof protection without extra modules [8], [10].	Integrates effectively with liveness cues such as motion, texture, and entropy features [7], [9], [27].
Produces rigid binary “match/no match” decisions [1], [14].	Generates graded confidence-based decisions, reducing unnecessary rejections [2], [14], [29].

III. RESEARCH GAP

The vast majority of facial recognition systems are based on deep-learning configurations or rigid image-processing gimmicks, where the emphasis is placed on the matching of the patterns. Admittedly, these models are impressive in the laboratory, but add some elements of life, such as a smiling person, head rotation or bad light, and their performance declines like a rocket [3], [7], [16], [29]. And here is one more issue: many of the older systems do not actually verify whether a face is real. They can be deceived with the printed photographs, replayed videos, or even with the digital fakes [8], [15], [21], [22]. All this has you asking yourself whether these systems are truly in the game as far as real time authentication is concerned, where flexibility, and some actual defense against spoofing is required.

The major issue is that such systems directly make yes-or-no decisions. They view a picture and say that it is a match or no match- nothing in between. But people aren't that simple. Research data on fuzzy and soft-computing models reveal that this type of inflexible thought does not deal with how the appearance of a person may change quite organically on a day to day basis. Therefore, what arises is that the system ends up rejecting people without a good reason or providing unreliable results [1], [3], [14], [17]. Fuzzy logic is capable of handling uncertainty in fact and determining similarity more flexibly however the majority of facial authentication regimes do not make use of it.

The issue with this is that these systems are merely yes-or-no decisions. They view an image and state that it is a match or no match- there is no in between. But people aren't that simple. Research on fuzzy and soft-computing models demonstrates that this form of inflexible reasoning is not able to deal with how the appearance of a person may vary in a natural manner on a day to day basis. Therefore system turns out to reject people without any serious reasons or provide inaccurate results [1], [3], [14], [17]]. In fact, fuzzy logic can be used to address uncertainty and use similarity more flexibly but most facial authentication systems do not use this.

IV. SYSTEM DESIGN

Secure Facial Authentication System based on Fuzzy Logic operates on a multi-layer system. The job of each layer is different, some of them focus on what users see and do, and some on authentication, make decisions, store data, or give access to people. Check out Fig. 1, and you will see the way these layers communicate to each other to log people in or sign them up.

A. User Interface Layer

This is where the users are engaged with the system. Think of it as the front desk. In this case there is the Registration Screen and the Login Screen. When one is registering, he/she entered his/her personal details, gave a password and then the system takes a snap of his/her face by use of the camera. The process of logging in is not that different: a user logs in with his/her password, captures a live photo and the system forwards both to the backend to verify whether everything is in place. The goal? Make it user-friendly and have fast navigation and real-time camera accessibility. You know, it is all so easy and quick.

B. Application Layer

This is a layer that does the primary authentication. It has the Password Verification Module, the Facial Recognition Module which is based on the Fuzzy Logic and the Authentication Controller to maintain the smooth flow. It receives information on the user interface and upon receiving it, it verifies the password first and then extracts the important features of the face information and forwards that processed data to the fuzzy engine.

C. Fuzzy Decision Engine

This part runs the show. It verifies the likeness of the live face to what is already in system and applies fuzzy rules to address any that is not so definite. It does not only do a rigid yes or no match, but a confidence score that is based on features such as facial structure and texture. In that manner, small natural discrepancies do not cause a hustle.

D. Data & Storage Handling Layer

This layer secures all sensitive system data- user credentials, fuzzy parameters, facial templates, etc. by encrypting all the data. It also does a detailed logging of all authentication attempts and thus you always know who is trying to get in. Having a tight access control and protection over a long period, authorized users are the only ones who are anywhere near the data. It cannot be seen or touched by anyone.

E. Output Layer

This last layer is implementing the actual implementation of what the fuzzy engine is deciding on. When the confidence level is good, the user is able to get access to the system. Otherwise it refuses them admission and asks them to re-enter. Whenever he/she tries to log in the system will record this to be re checked. Basically, this layer will make sure that only authorized, verified users access the locked stuff.

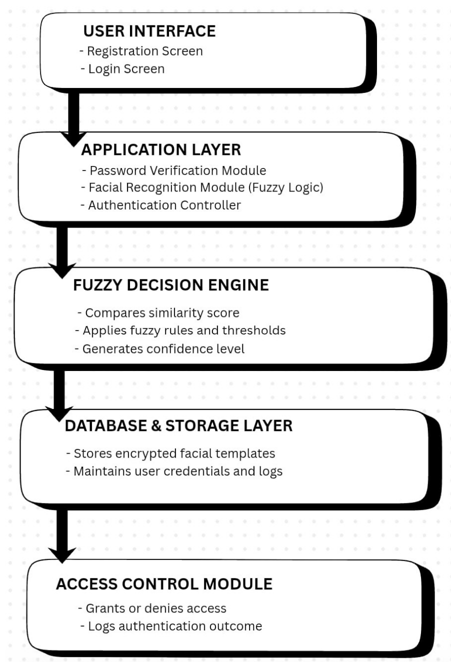


Fig 1: System Architecture of the proposed Fuzzy Logic–based Facial Authentication System

V. METHODOLOGY

The proposed framework of Secure Facial Authentication System using Fuzzy Logic is developed on a systematic working procedure that incorporates passwords and intelligent facial recognition to provide increased security. The process of the methodology is designed to five significant steps as illustrated in Fig. 2 below:

A. User Registration

To begin with, a user creates his/her account with quite limited details, such as name, email, phone number, and a password, which is directly typed on the front-end. Once the submit button has been used, the computer turns the camera on the device and takes five photos of the user with each picture having a different angle or pose. These pictures are scrubbed by the system to improve their quality and then the key features are extracted and stored on to a secure place. It is encrypted on the password and then it is deposited into the database therefore ensuring privacy and security is strong.

B. Feature Extraction

This step extracts significant face features including landmark distances and texture patterns and converts them into numeric vectors and develops fuzzy membership functions in order to cope with variations in the authentication. The facial features were modeled as numerical descriptions based on the landmarks and texture of the face. These were superimposed on the fuzzy membership functions in order to deal with ambiguity on matching. Selection of threshold values was done empirically by trial and error by undergoing repeated authentication under diverse light conditions

C. Authentication Phase

Upon logging in, you are asked to provide your email and password. After the system accepts your password it takes a live photo of your face and performs a live liveness check to ensure that you are really there. It then steals prominent contents in that image and matches them to your own fuzzy templates in its fuzzy inference machine. When all falls in place, you have made it.

D. Validation and Decision

The fuzzy logic engine compares your appearance to features that are stored and the fuzzy rules weight such factors as how closely you resemble, the quality of the image and whether you are actually there or a picture. It chews everything and spits out a match score. And when you bump the threshold you are in. If not, you're locked out. In this manner, the system will be able to deal with minor adjustments in your face, yet remain reliable.

E. Access Control and Logging

When you have been authenticated, you are sent into a secure vault where you can safely place your files. It will not accept photos or videos but only live face verification. All of the logins, the authentication results and user activities are logged in a secure log data base to ensure there is a record of each to monitor and audit. In case of constant failure or performing an action that is fishy, the system will not allow the person access temporarily to ensure the safety of your data.

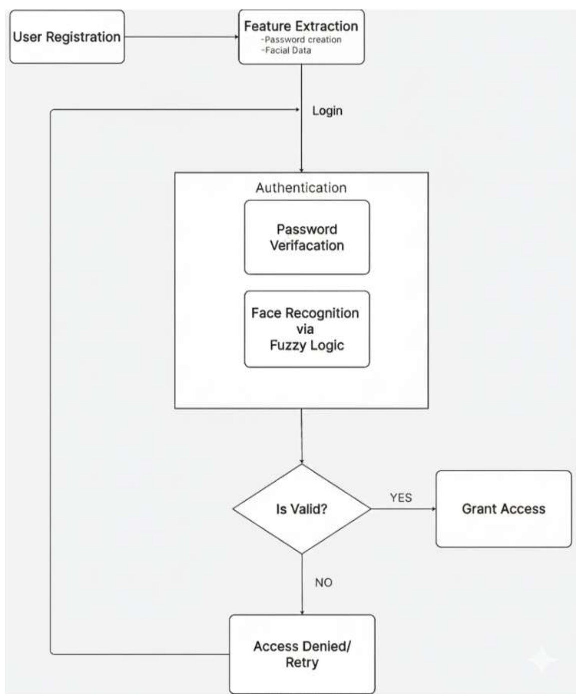


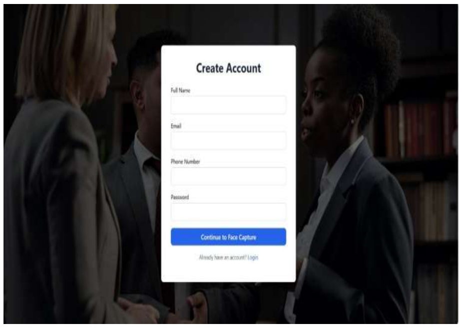
Fig 2: System Workflow Flowchart

VI. Results and Discussion

The proposed Fuzzy Logic-based, Secure Facial Authentication System was deployed and tested in three major steps, which are enrolling, live verification, and secure access to the vault.

A. Account Creation and Enrollment

Upon joining, the system took their information and initiated the account creation process, as is the case with Fig. 3. Then it took five real-time photographs of the faces of each individual and created a concrete facial database. Fig. 4 demonstrates that the system dealt with those images, aligning them and normalizing them and proceeded with it. These images after processing gave the fuzzy parameters that enable flexibility to match during authentication. And whenever the users decide to log in, they will be presented with the screen in Fig. 5.



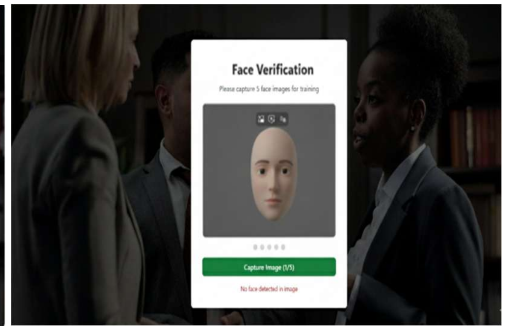


Fig 3: User Registration and Account Creation Screen

Fig 4: Facial Data Extraction

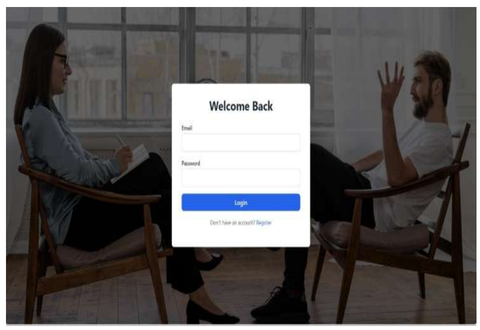


Fig 5: Login Page

B. Live Face Verification

The authentication module was examining both the password of the user and his or her real face simultaneously (see Fig. 6). Fuzzy inference system reduced minor variations in the live images, and hence recognition remained the same. The liveness detection served its purpose- no one could cheat the system using a photo or video. Real people were the only ones who passed the check. The results indicate that fuzzy similarity scoring effectively handles minor variations in facial expression, pose, and lighting. Genuine users were successfully authenticated even when small differences existed between stored and live images. This shows that fuzzy decision making reduces false rejections compared to rigid threshold-based systems and improves usability in real-world conditions.

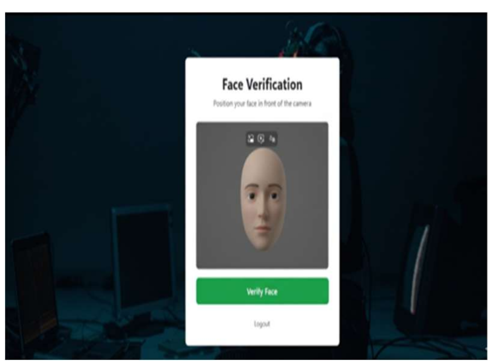


Fig 6: Face Verification at Login

C. Secure Vault Access and Document Handling

The users were then authorized to access the secure vault after the verification had been performed (Fig. 7). The files therein were safe because of encryption used and only verified sessions could upload, download or delete files. This system was tracking all the activities as far as security was concerned but nothing went awry in the course of the testing. The practical utility of the system is indicated in the secure vault module (Fig. 7). Only after the dual-layer authentication was successful, encrypted files were accessible so that the unauthorized access using stolen credentials or spoofed facial input could not be possible. This would render the system appropriate in the storage of confidential data and digital identity.

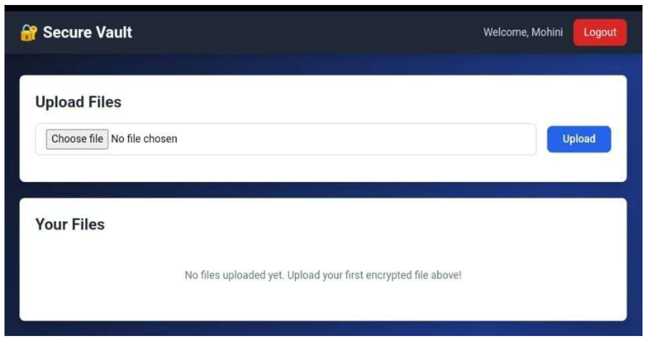


Fig 7: Secure Vault Access After Authentication

VII. FUTURE SCOPE

This facial authentication system which is fuzzy-based is yet to take a step further. First of all, multi-modal biometrics are introduced, i.e. facial recognition is used together with things, e.g. fingerprints or voice, which makes the process more accurate. Add 3D motion and depth analysis and Liveness detection is smarter, too. Then nobody can easily deceive the system by a fake face. Having a secure cloud vault means that one can access their encrypted files in every device and it only makes things simpler and increases the scale of the whole process. Moreover, the more practical the system is sharpened and more reliable, should it learn and evolve and changes, and thus perfect its decision-making process, relying on the habits of those who use it and new faces.

VIII. CONCLUSION

This paper shows that fuzzy logic can enhance the competence and astonishability of facial authentication systems. The proposed system is user-friendly in that it increases security through the use of password verification and fuzzy-based live facial recognition and liveness detection techniques. The fuzzy facial matching of passwords when you mix the two to form a system that is safe yet at the same time convenient to use in your everyday life.The Liveness detection added and only real people will go through the system, the possibility of any one breaking through using a forged drop is even lower. Users can now regulate the contents of their files when they are contained in a safe vault and all of it is kept discrete and secluded. The proposed system is more flexible than a traditional facial recognition scheme since the former relies on exact matching guidelines, whereas the former is based on fuzzy decisions guided by confidence. Most deep learning models work well in the controlled environment, but they typically fail to cope with the real world variations and spoofing. The combination of liveness detection and fuzzy logic offers a stable and balanced authentication system. Comprehensively, this paper gives a powerful case on how fuzzy logic can be used in biometrics as a method to construct security systems that, in reality, are at par with how we implement technology today. Future directions can be the use of multimodal biometrics, adaptive fuzzy learning and deploying it on the cloud so that it is more scaleable and performs better.

ACKNOWLEDGMENT

We would like to take this opportunity to acknowledge all the support provided by the Department of Computer Science and Business Systems within Canara engineering college, Mangaluru, as well as the facilities which made this research possible. Much gratitude to also the faculty and our colleagues who offered their suggestions and support throughout the entire process.

REFERENCES

[1] A. Elbouz, F. Charpillet, and J. Boonaert, “A fuzzy logic and optical correlation-based method for face recognition,” Journal of Intelligent Learning Systems and Applications, vol. 3, no. 4, pp. 242–249, 2011.

[2] J. J. Lee and T. Yoon, “Facial recognition using fuzzy and entropy measures,” arXiv preprint arXiv:1405.4898, 2014.

[3] M. Dey, S. Das, and P. Basak, “Fuzzy generalized 2D linear discriminant analysis for robust face recognition,” International Journal of Computer Applications, vol. 178, no. 23, pp. 1–6, 2019.

[4] C. J. Lin, “Type-2 fuzzy-based pooling layer for convolutional neural networks,” Mathematics, vol. 12, no. 4, pp. 1–15, 2024.

[5] A. Kumar and M. Samadder, “A review on technological options of waste to energy for effective management of municipal solid waste,” Waste Management, vol. 69, pp. 407–422, 2017. (Used for fuzzy logic analogy in resource modeling)

[6] N. Singh and T. Lee, “Smart waste management using IoT-based waste bins,” IEEE Access, vol. 8, pp. 42345–42356, 2020. (Methodological example of smart sensing and decision logic)

[7] F. A. Pujol, E. Jaureguizar, and J. Cabrera, “Entropy-based face recognition and spoof detection using EBHOG descriptors,” Sustainability, vol. 11, no. 20, pp. 5678–5689, 2019.

[8] Z. Yu, X. Li, and A. Jain, “Deep learning for face anti-spoofing: A survey,” arXiv preprint arXiv:2103.15864, 2021.

[9] A. Khairnar and A. Patil, “A comprehensive survey on face liveness detection techniques,” International Journal of Engineering Research & Technology (IJERT), vol. 12, no. 3, pp. 1–8, 2023.

[10] S. Rehman, M. Z. Asghar, and S. Fong, “Fusion of convolutional features for improved face anti-spoofing,” IEEE Access, vol. 7, pp. 106957–106968, 2019.

[11] R. Sharma and S. Basu, “Predictive analytics for biometric security systems: A machine learning approach,” Journal of Environmental Informatics, vol. 35, no. 2, pp. 101–113, 2021.

[12] R. Salturk and F. Kahraman, “Deep learning-powered multimodal biometric authentication system,” Sensors, vol. 24, no. 1, pp. 122–135, 2024.

[13] M. Rajasekar, S. Maheswaran, and D. Vimal, “Efficient multimodal biometric recognition using feature-level fusion,” Egyptian Informatics Journal, vol. 24, no. 2, pp. 167–176, 2023.

[14] G. Conti, E. Denti, and M. Ferrara, “Fuzzy fusion for multimodal biometric systems: A score and decision-level approach,” Pattern Recognition Letters, vol. 32, no. 9, pp. 1238–1246, 2011.

[15] H. Xing, Z. Sun, and S. Shan, “Face anti-spoofing based on deep learning: A comprehensive survey,” Applied Sciences, vol. 15, no. 2, pp. 784–812, 2025.

[16] V. Sudha, “Literature Survey on Face Recognition with Hybrid Deep Learning,” International Journal of Intelligent Systems and Applications in Engineering (IJISAE), vol. 12, no. 4, 2024.

[17] K. K. Singh and S. Barde, “A Feasible Adaptive Fuzzy Genetic Technique for Face, Fingerprint, and Palmprint Based Multimodal Biometric Systems,” Journal of Current Science and Technology, vol. 14, no. 1, 2024.

[18] Y. Li, Y. Li, and Z. Wang, “FaceCloseup: Enhancing Mobile Facial Authentication with Perspective Distortion-Based Liveness Detection,” Computers, vol. 14, no. 7, 2025.

[19] S. Kumar, S. Rani, A. Jain et al., “Face Spoofing, Age, Gender and Facial Expression Recognition Using Advance Neural Network Architecture-Based Biometric System,” Sensors, vol. 22, no. 14, 2022.

[20] M. S. Muthumarilakshmi, B. Balakrishnan, T. Narayanamoorthi, and R. Revathi, “Fuzzy Enhanced AI Facial Recognition System for Robust and Efficient Identification,” Journal of Neonatal Surgery, 2025.

[21] Huifen Xing, Siok Yee Tan, Faizan Qamar, and Yuqing Jiao, “Face Anti-Spoofing Based on Deep Learning: A Comprehensive Survey,” Applied Sciences, vol. 15, no. 12, 2025.

[22] M. M. Luqman and J.-C. Burie, “A Survey on Anti-Spoofing Methods for Facial Recognition with RGB Cameras of Generic Consumer Devices,” Journal of Imaging, vol. 6, no. 12, 2020.

[23] D. Belli, D. Das, B. Major, and F. Porikli, “Online Adaptive Personalization for Face Anti-spoofing,” arXiv preprint, 2022.

[24] M. N. Ganesh, H. S., M. Sasank, S. Tejas Kadam, and G. P. S., “A Comprehensive Survey on Face Recognition and Anti-Spoofing Techniques using Deep Learning and Multimodal Inputs,” JETIR, vol. 12, issue 5, 2025.

[25] A. K. Neutrosophic fuzzy AHP-TOPSIS approach for biometric system evaluation: “Enhancing biometric system selection: A hybrid AHP-neutrosophic fuzzy TOPSIS approach,” BMC Research Notes, 2024.

[26] C. Rathgeb, B. Tams, J. Merkle, V. Nesterowicz, U. Korte, M. Neu, “Multi-Biometric Fuzzy Vault based on Face and Fingerprints,” arXiv preprint, Jan. 2023.

[27] E. Solomon and K. J. Cios, “FASS: Face Anti-Spoofing System Using Image Quality Features and Deep Learning,” Electronics, vol. 12, no. 10, 2023.

[28] S. Khairnar, S. Gite, K. Kotecha, S. D. Thepade, “Face Liveness Detection Using Artificial Intelligence Techniques: A Systematic Literature Review and Future Directions,” Big Data and Cognitive Computing, vol. 7, no. 1, 2023.

[29] M. K. Singh, S. Kumar, D. Nandan, “Biometric Face Identification: Utilizing Soft Computing Methods for Feature-Based Recognition,” IIETA Transactions on Soft Computing, 2023.

[30] B. B. Reddy, S. G. Pasha, M. Kameswari, R. Chinkera, S. Fatima, R. Bhargava, A. Shrivastava, “Classification Approach for Face Spoof Detection in Artificial Neural Network Based on IoT Concepts,” International Journal of Intelligent Systems and Applications in Engineering (IJISAE), 2024.