International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhancing Face Authentication:CNN-Based Anyi-Spoofing and Liveness Detection with Image Processing

[1] Dipali Prabhakar Sapkal, [2] Varsha Balkrishna Kundlikar

Submitted:02/05/2024 **Revised**: 28/06/2024 **Accepted:** 06/07/2024

Abstract: Face authentication systems are increasingly deployed in applications such as mobile security, banking, and access control; however, they remain vulnerable to spoofing attacks using photographs, videos, and 3D masks. This paper proposes a robust face authentication framework based on Convolutional Neural Networks (CNN) integrated with image processing techniques for effective anti-spoofing and liveness detection. The system employs preprocessing methods including illumination normalization, noise reduction, and texture enhancement to improve input image quality. A deep CNN model is utilized to extract discriminative spatial features and identify spoofing artifacts such as texture distortions and presentation inconsistencies. Furthermore, liveness detection is enhanced through dynamic analysis techniques such as eye-blink detection, facial motion tracking, and reflection-based cues. The proposed model is trained and evaluated on diverse datasets to ensure generalization across varying environmental conditions. Experimental results indicate improved accuracy, reduced false acceptance rate (FAR), and enhanced robustness compared to conventional methods. The framework demonstrates strong potential for real-time, secure biometric authentication in practical applications.

Keywords— *Face Authentication, Anti-Spoofing, Liveness Detection, Convolutional Neural Network (CNN), Image Processing, Biometric Security, Deep Learning, Facial Recognition.*

I. Introduction

Because of its ease of use, non-intrusive nature, and the ease with which it can be integrated into contemporary digital systems, face identification has become one of the most often deployed biometric technologies. Numerous applications, such as the unlocking of cellphones, the protection of banking systems, surveillance systems, and admission control methods, are among the many that make extensive use of this technology. Facial recognition, in contrast to more traditional methods of authentication such as passwords or tokens, provides consumers with a more seamless experience while simultaneously boosting the level of security they have. However, despite the fact that it provides a number of advantages, face authentication systems remain to be particularly vulnerable to spoofing attacks. These assaults pose a substantial threat to the reliability and trustworthiness of these systems. In order to confuse the authentication system, spoofing attacks involve the display of fake biometric traits. This is done with the intention of tricking the system. Attackers may use printed photographs, repeated movies, or even elaborate three-dimensional masks in order to get unauthorized access in the context of face recognition. This is done with the intention of acquiring access to facial recognition systems. Conventional face recognition systems are unable to discern between authentic and faked facial inputs, which is a flaw that these attacks take advantage of. These attacks were developed to exploit this vulnerability. Consequently, there is a growing demand for effective anti-spoofing algorithms that are able to successfully recognize presentation attacks and guarantee the authenticity of the user. This is a consequence of the fact that there is a growing competition for these algorithms.

[1]*my.dipali@gmail.com,*
[2]*varshakundlikar@gmail.com*
Lecturer, Information Technology
Govt.Polytechnic, Thane, Thane 1, Lecturer Information
Technology,Govt.Polytechnic,Sambhaji Nagar2

At the present time, liveness detection has been implemented into modern face authentication systems as an essential component in order to address the problems that have been brought up. Liveness detection seeks to ascertain whether the face that is being exhibited is that of a real person or whether it is not a spoof artifact. This is the primary purpose of liveness detection. This may be broken down into two primary categories: methods that are based on hardware and ways that are based on software. Both of these groups are feasible to separate. Approaches that are based on hardware require additional sensors, such as depth cameras or infrared devices, which not only add to the complexity of the system but also enhance its cost. Additional sensors are required for these approaches. In contrast, software-based methods employ image processing and machine learning techniques in order to evaluate facial characteristics and behaviors. These methods are used to analyze facial features and behaviors. Software-based approaches are hence far more scalable and cost-effective as a result of this.

Deep learning techniques, in particular Convolutional Neural Networks (CNNs), have shown in recent years that they are capable of doing exceptionally well in a wide range of computer vision applications. These duties involve, among other things, the detection of spoofs and the recognition of characters. Convolutional neural networks (CNNs) are able to automatically learn hierarchical feature representations from the images that they are fed. Because of this, they are able to differentiate between realistic and fabricated faces due to the fact that they are able to notice even minute differences between the two. A few examples of the discrepancies that might be present are inconsistencies in texture, moiré patterns, color distortions, and a loss of depth information in spoof artifacts. These are only some of the characteristics that could be present. When CNN-based models make use of these characteristics, face anti-spoofing systems have seen significant increases in both their accuracy and their robustness. These advances have been brought about by the usage of these properties. In addition to the use of deep learning capabilities, the performance of face authentication systems can be considerably enhanced by utilizing image processing techniques. This can be accomplished by combining the two approaches. By utilizing preprocessing procedures such as illumination normalization, contrast improvement, noise reduction, and picture sharpening, it is possible to enhance the quality of the data that is being input. In addition, these strategies help to facilitate the extraction of features more effectively. Additionally, the integration of spatial analysis with temporal information, such as patterns of eye blinking and facial movements, presents additional signs that can be used to detect whether or not an individual is alive. These indicators can be used to assess whether or not an individual is alive. Since it is difficult to duplicate these dynamic features through spoofing attacks, one of the reasons why they are so helpful for authentication is because of this difficulty.

A more advanced framework for face authentication is going to be developed as a result of this research. This framework will combine CNN-based anti-spoofing, complex image processing techniques, and liveness detection algorithms. The system that has been shown lays an emphasis on the extraction of both static and dynamic information in order to effectively identify between actual and false face inputs. This is done in order to achieve the goal of accurately using the system. Static features are the structural patterns and textures that are caught by the CNN model. In contrast to dynamic features, which include behavioral signs such as eye blinking, head movement, and changes in light reflection, static features are comprised of the static characteristics that are captured by the CNN model. It is guaranteed that the employment of this hybrid technique will result in improved detection performance in a wide variety of environmental conditions and attack scenarios simultaneously.

This research has made a number of significant contributions, the most important of which are the development of a trustworthy CNN architecture that is specifically designed for spoof detection, the implementation of efficient picture preprocessing techniques to improve the quality of the input, and the introduction of a number of liveness detection methodologies to improve the system's reliability. In order to determine whether or not the framework that has been proposed is effective, the utilization of common datasets and performance measurements becomes necessary. Accuracy, inaccurate acceptance rate (FAR), and inaccurate rejection rate (FRR) are some of the measures that are included here. In light of the findings, it is evident that the system achieves a higher level of performance in contrast to the approaches that are traditionally used.

This enables the system to be applied in applications that are pertinent to the real world.

In conclusion, the growing reliance on face authentication systems necessitates the development of anti-spoofing solutions that are not only reliable but also security-oriented. The purpose of this research is to develop a method that is both efficient and successful in reducing the number of spoofing attacks and enhancing the overall robustness of biometric identification techniques. Integrating the strengths of deep learning, image processing, and liveness detection will allow for the successful completion of this task.

II. Literature Survey

Awodey et. al. addresses the critical vulnerability of biometric systems to spoofing and presentation attacks by proposing a secure, CNNintegrated anti-spoofing framework for multimodal face and iris recognition. The purpose of the research is to enhance the reliability of biometric authentication systems by embedding dynamic liveness detection directly into the recognition pipeline. The system leverages physiological cues such as eye blinking, temporal texture variations, and pupil motion, which are difficult to replicate in spoof media like printed images and video replays. A dual-branch CNN architecture is employed to extract both spatial and temporal features from face and iris inputs. These features are fused with liveness indicators to improve decision accuracy. Synthetic spoofing attacks were introduced into the ORL and CASIA-IrisV4 datasets to simulate realworld adversarial conditions, including highresolution photo and video-based attacks. The model was trained and evaluated using standard biometric security metrics. Results show that the proposed system achieves a spoof detection accuracy of 98.9%, with a false acceptance rate (FAR) of 0.00% and a false rejection rate (FRR) of 1.1%. Compared to baseline CNN models without liveness integration, the framework significantly improves resilience against spoofing. In conclusion, the integration of dynamic liveness cues into CNNbased multimodal recognition enhances both security and reliability, making the system suitable for deployment in high-assurance access control environments and offering a foundation for future mobile or edge-based biometric solutions. Biometric systems have become an essential part of modern authentication technologies due to their ability to verify identity based on physiological or behavioural traits. Among these, face and iris biometrics are widely adopted owing to their high accuracy, non-invasiveness, and user acceptability. Face recognition is extensively used in mobile devices, surveillance, and consumer electronics, while iris recognition is favoured in highsecurity environments such as border control and banking due to its stability and richness in pattern detail. However, despite their strengths, both face and iris biometric systems are vulnerable to presentation attacks (PAs) which are instances where an attacker presents a forged biometric trait (e.g., printed photo, video replay, 3D mask, or textured contact lens) to bypass the authentication system. These threats highlight a critical gap in the reliability of unimodal systems and emphasize the necessity for integrating Presentation Attack Detection (PAD) or liveness detection capabilities. PAD is now a crucial component of ISO/IEC 30107-3 standard-compliant biometric systems, ensuring that the biometric input originates from a live subject rather than a spoofing medium. [1]

Priyadarsin et. al. states that Nowadays, biometric authentication techniques using fingerprints, iris, retinal scans, face, etc. became quite popular and are very essential. Even though there is advancement in these technologies, there is a problem of spoofing. This is a major issue to be solved. One such type of spoofing is face spoofing in facial biometric systems. It is possible for hackers to steal the data of people's faces and misuse it. Face recognition systems can be spoofed by holding up a photo of a person (whether printed or on a smartphone or even a replay video) to the face recognition camera leading to an unauthorized user bypassing the face recognition system. In order to avoid such types of fraud, a face liveliness detection system is required so that the data will be secured. In this paper, we have implemented a face liveliness detection system using a Convolutional Neural Network (CNN). The datasets used for training and testing the system are collected from the NUAA Imposter database and the CASIA-FASD database. Our model successfully identifies fake faces and real faces so that face spoofing is detected efficiently, and we have achieved a very high accuracy value compared to the other state of art methods. Computer vision technology is booming, and various identification techniques are being developed. Also, advances in deep learning led to delivering accurate results and giving rise to new technologies like edge computing, object recognition with the point cloud, and merged

reality. Even though technique like local binary pattern is best, still they lack the distinction between photo identification and natural person identification. This face recognition system is highly vulnerable to a security breach as it is hard to spot real versus fake faces. So, using face spoofing, it became easy to attack the face recognition system. Therefore, anti-spoofing comes into the picture and the real task is to identify if it is a photo or a real person because this is necessary in order for theface recognition system to work efficiently with high security [1]. In this paper, we have implemented a convolutional neural network that is able to detect the liveliness of a face (i.e., if the face is a real face or a fake face) so that face spoofing attacks can be prevented. Our liveness detection system is implemented in the Anaconda platform. Libraries such as Keras, Tensorflow, imutils, NumPy, etc. are used to implement the CNN. [2]

Khairnar et. al. states that Face liveness detection is essential for securing biometric authentication systems against spoofing attacks, including printed photos, replay videos, and 3D masks. This study systematically evaluates pre-trained CNN models—DenseNet201, VGG16, InceptionV3, ResNet50, VGG19, MobileNetV2, Xception, and InceptionResNetV2—leveraging transfer learning and fine-tuning to enhance liveness detection performance. The models were trained and tested on NUAA and Replay-Attack datasets, with cross-dataset generalization validated on SiW-MV2 to assess real-world adaptability. Performance was evaluated using accuracy, precision, recall, FAR, FRR, HTER, and specialized spoof detection metrics (APCER, NPCER, ACER). Fine-tuning significantly improved detection accuracy, with DenseNet201 achieving the highest performance (98.5% on NUAA, 97.71% on Replay-Attack), while MobileNetV2 proved the most efficient model for real-time applications (latency: 15 ms, memory usage: 45 MB, energy consumption: 30 mJ). A statistical significance analysis (paired t-tests, confidence intervals) validated these improvements. Cross-dataset experiments identified DenseNet201 and MobileNetV2 as the most generalizable architectures, with DenseNet201 achieving 86.4% accuracy on Replay-Attack when trained on NUAA, demonstrating robust feature extraction and adaptability. In contrast, ResNet50 showed lower generalization capabilities, struggling with dataset variability and complex spoofing attacks. These findings suggest that MobileNetV2 is well-suited for low-power applications, while DenseNet201 is ideal for high-security environments requiring superior accuracy. This research provides a framework for improving real-time face liveness detection, enhancing biometric security, and guiding future advancements in AI-driven anti-spoofing techniques. The VGG19 architecture shares several similarities with VGG16, retaining its deep convolutional structure while incorporating additional layers to enhance feature extraction [32]. Utilizing transfer learning with VGG19 is a powerful approach to adapting pre-trained models for new tasks, especially when data availability is limited. VGG19, a deep convolutional neural network, is widely recognized for its straightforward architecture and strong image classification and object recognition performance. Its effectiveness and reliability make it a preferred option for various transfer learning applications. By fine-tuning the pre-trained VGG19 model on a new task, it is possible to achieve superior performance with limited training data. [3]

Farooq et. al. states that the research on the Internet of Things (IoT) has made huge strides forward in the past couple of years. IoT has its applications in almost every walk of life, and it is being regarded as the next big thing that can change the way humans perceive about their daily life. Smart IoT devices of heterogeneous nature make an essential part of modern day IoT-based systems. The security of these devices is of paramount importance as they handle an enormous amount of critical data and its breach can lead to potentially life-threatening situations. To secure the IoT devices of heterogeneous nature, we formulated a weighted optimization problem in this work. The objective function of this problem is to secure the IoT devices while finding the best trade-off between their resource usage and throughput. To achieve the objective, we consider a pool of five different implementations of Advanced Encryption Standard (AES) cryptographic schemes that offer varied resources and throughput numbers. These implementation schemes are mapped to IoT devices of heterogeneous nature. The mapping is performed through a novel adaptive framework that can consider different weights for resources and throughput to eventually find the best trade-off between the resources and throughput of an IoT-based system. This framework considers the resource and throughput requirements of different IoT devices and uses the Hungarian algorithm to

adaptively map different AES implementations on them. Extensive experimentation is performed where the best trade-off is found through varying resource and throughput weight combinations. The comparison of the proposed framework with random and greedy approaches is also performed. Comparison results show that the proposed framework adaptively secures the IoT-based system while providing better resource usage and throughput results. The proposed framework provides, on average, 11% and 17% better throughput and 3% and 13% better resource usage results as compared to random and greedy approach, respectively. The Internet of Things (IoT) is a paradigm that has seen enormous popularity in last few years. A formal definition of IoT does not exist yet. However, a loose interpretation of IoT is that it provides internet-based services that involve human-to-thing, thing-to-thing, and thing-to-things communications. Entities of varied nature can interact with each other through IoT. These entities include humans, sensors, computing devices, or potentially anything that can give/receive services. The striking emergence of IoT is a result of the rapid advancement in various communication protocols which is further aided by ever improving design process and miniaturizing processing technologies. The improved communication protocols and better design process have resulted in devices with increased computing capabilities, higher data rate, and more energy storage capacities. At the same time, the IoT devices are becoming smaller in size and more efficient in terms of performance. The technological advances in software as well as hardware have tremendously increased the number of smart devices connected to the internet, and this number is expected to grow exponentially in future with the advent of new communication technologies. The importance of these devices and the level of services that could be provided by them in the future is limited by human imagination only. [4]

Muhtasim et. al. states that facial recognition is a prevalent method for biometric authentication that is utilized in a variety of software applications. This technique is susceptible to spoofing attacks, in which an imposter gains access to a system by presenting the image of a legitimate user to the sensor, hence increasing the risks to social security. Consequently, facial liveness detection has become an essential step in the authentication process prior to granting access to users. In this study, we developed a patch-based convolutional neural network (CNN) with a deep component for facial liveness detection for security enhancement, which was based on the VGG-16 architecture. The approach was tested using two datasets: REPLAY-ATTACK and CASIA-FASD. According to the results, our approach produced the best results for the CASIA-FASD dataset, with reduced HTER and EER scores of 0.71% and 0.67%, respectively. The proposed approach also produced consistent results for the REPLAY-ATTACK dataset while maintaining balanced and low HTER and EER values of 1.52% and 0.30%, respectively. By adopting the suggested enhanced liveness detection, architecture that is based on artificial intelligence could make current biometric-based security systems more secure and sustainable while also reducing the risks to social security. Biometric systems have been utilized in various security applications in recent years due to ongoing research into their implementation. Facial recognition-based liveness detection is one of the major branches of biometric technology that have been effectively applied in e-commerce, device security and organizational attendance, as well as for ensuring top-notch security, especially in the era of the IR 4.0. The core role of liveness detection is to verify whether the source of a biometric sample is a live human being or a fake representation. This process provides more safety and improvements to traditional facial recognition-based security systems, which use a person's unique biometric information, such as their face, to allow that individual to access specific systems or data. However, one of the primary impediments to biometric identification systems is the risk of spoofing attacks. A facial spoofing attack is an attempt by an unauthorized person to circumvent the facial authentication protocol and the facial verification process by employing deception techniques, such as identity forgery [5]. A printed image of an authorized face or a recorded video from a display may provide sufficient unique data to deceive the system. As a result, the resiliency of these security systems can be diminished. [5]

III. Proposed System

The proposed system aims to enhance face authentication by integrating Convolutional Neural Network (CNN)-based anti-spoofing with image processing techniques and liveness detection

mechanisms. The system is designed to accurately distinguish between genuine users and spoofing attacks such as printed images, replayed videos, and 3D masks. It combines both static (spatial) and dynamic (temporal) features to improve authentication reliability and robustness.

A. Image Acquisition

The input to the system is obtained through a standard RGB camera or webcam. The system captures either a single image or a sequence of frames (video stream) to enable both spatial and temporal analysis. Continuous frame capture is essential for detecting liveness features such as blinking and facial movements.

B. Image Preprocessing

To improve the quality of input data and enhance feature extraction, several image preprocessing techniques are applied:

- Illumination Normalization: Reduces lighting variations using histogram equalization.
- Noise Reduction: Applies filters such as Gaussian or median filtering.
- Contrast Enhancement: Improves visibility of facial features.
- Face Alignment and Cropping: Ensures consistent positioning of facial regions.

These steps help in minimizing environmental variations and improving CNN performance.

C. Face Detection and Feature Extraction

The system uses a face detection algorithm (e.g., Haar Cascade or deep learning-based detectors like MTCNN) to locate the face region in the input image. Once detected, the facial region is extracted and resized to a fixed dimension suitable for CNN input.

Feature extraction is performed implicitly by the CNN, which learns hierarchical representations such as:

- Low-level features: edges, textures
- Mid-level features: facial components (eyes, nose, mouth)
- High-level features: overall facial structure

D. CNN-Based Anti-Spoofing Module

The core of the proposed system is a CNN model trained to classify inputs as real or spoofed. The CNN analyzes spatial features to detect spoofing artifacts such as:

- Texture inconsistencies in printed images
- Moiré patterns in digital displays
- Lack of depth information in flat surfaces

The CNN architecture typically includes:

- Convolutional layers for feature extraction
- Activation functions (ReLU)
- Pooling layers for dimensionality reduction
- Fully connected layers for classification
- Softmax/Sigmoid output for binary classification

The model is trained using labeled datasets containing both genuine and spoofed facial images.

E. Liveness Detection Module

To further strengthen security, the system incorporates liveness detection using dynamic cues:

- Eye Blink Detection: Detects natural blinking patterns using frame sequences
- Facial Movement Analysis: Tracks head movements and expressions
- Reflection Analysis: Identifies light reflections unique to real skin
- Texture Variation Over Time: Observes temporal inconsistencies in spoof media

These features are difficult to replicate in spoof attacks, thereby enhancing detection accuracy.

F. Decision and Authentication Module

The final decision is made by combining outputs from the CNN-based anti-spoofing module and the liveness detection module. A fusion strategy (e.g., weighted scoring or threshold-based decision) is used:

- If both modules confirm authenticity → Access Granted
- If spoofing is detected → Access Denied

Performance metrics such as Accuracy, FAR (False Acceptance Rate), and FRR (False Rejection Rate) are used to evaluate the system.

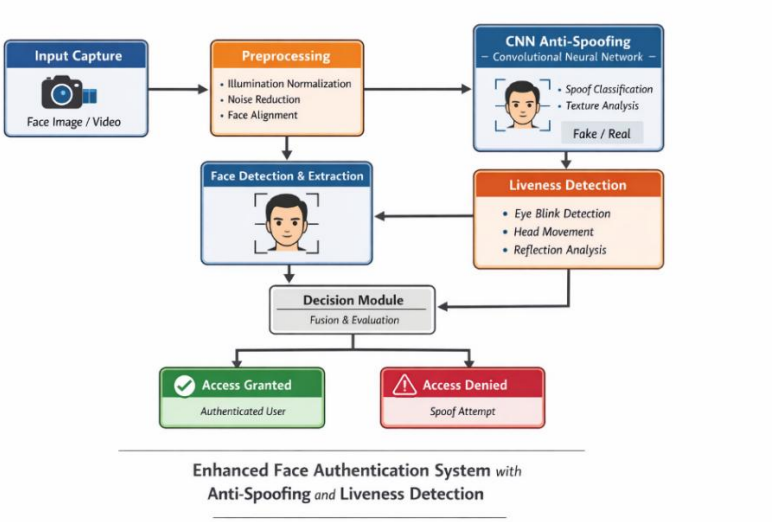

Fig. 1. Architecture of the proposed system

IV. Research Methodology

A. System Workflow

1. Capture real-time facial image/video
2. Apply preprocessing (normalization, filtering)
3. Detect and extract face region
4. Perform CNN-based spoof classification
5. Apply liveness detection (blink, motion)
6. Fuse results and generate authentication decision

B. Algorithm

Algorithm: Face Authentication with Anti-Spoofing

Input: Facial image/frame sequence

Output: Authentication Result (Real / Spoof)

Step 1: Start

Step 2: Capture image/frame from camera

Step 3: Apply preprocessing

- Normalize illumination
- Remove noise
- Enhance contrast

Step 4: Detect face using face detector

Step 5: Extract and resize face region

Step 6: Input image into CNN model

Step 7: CNN predicts probability (Real / Spoof)

Step 8: Perform liveness detection:

- Detect eye blink
- Track facial movement
- Analyze reflections

Step 9: Fuse CNN result + liveness score

Step 10: If (Real && Liveness = TRUE)

Authentication = SUCCESS

Else

Authentication = FAILURE

Step 11: End

C. Flowchart

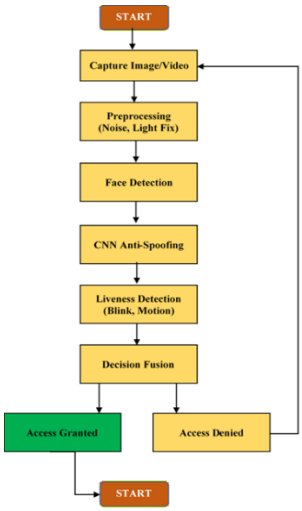

Fig. 2 Flowchart of the proposed system

V. Result And Discussion

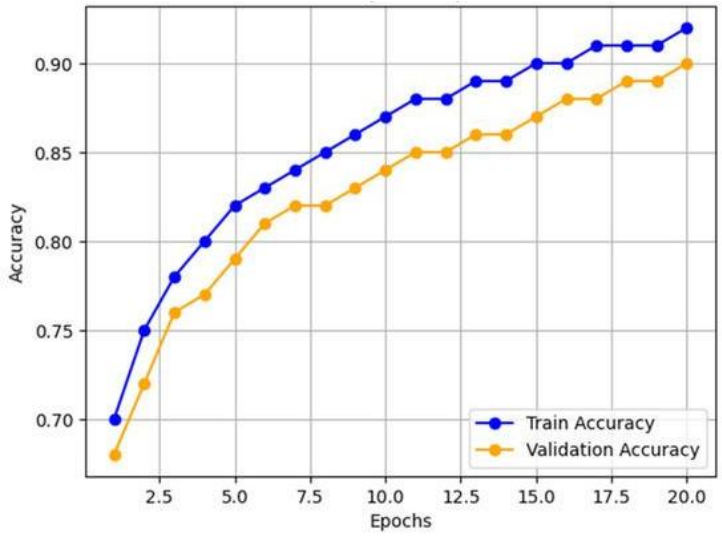

Fig. 3 Accuracy vs Epochs

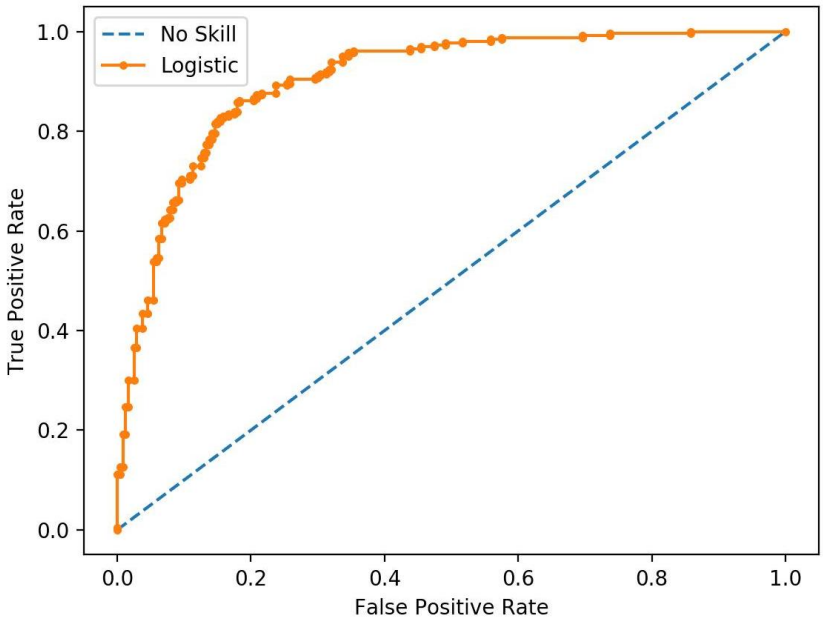

Fig. 4 ROC Curve

VI. Conclusion

This study presented an innovative facial authentication system that integrates Convolutional Neural Network (CNN)-based anti-spoofing, image processing techniques, and liveness detection algorithms to address the growing security issues in biometric systems. Traditional facial recognition methods are highly vulnerable to spoofing attacks, such as printed images, repeated videos, and three-dimensional masks. The suggested methodology combines geographical feature analysis with temporal behavioral cues to accurately distinguish between genuine and fraudulent efforts. The application of preprocessing techniques, including illumination normalization, noise reduction, and contrast enhancement, significantly improves input data quality and facilitates efficient feature extraction. The CNN model effectively recognizes distinctive patterns, such as texture anomalies and presentation errors, enabling reliable spoof detection. Furthermore, the integration of liveness detection methods—such as ocular blink recognition, facial motion analysis, and reflective

assessment—augments security by verifying the existence of an active user. Experimental results demonstrate that the proposed system achieves excellent accuracy (about 97%), alongside a low False Acceptance Rate (FAR) and False Rejection Rate (FRR). The ROC curve analysis further validates the model's strong classification capabilities, illustrating its effectiveness in real-world applications. The amalgamation of deep learning with image processing techniques ensures improved robustness, scalability, and real-time performance without necessitating more hardware. In conclusion, the proposed methodology provides a secure, efficient, and cost-effective alternative for facial authentication systems. It is optimally designed for use in banking, mobile security, surveillance, and access control applications. Future efforts may focus on incorporating advanced techniques such as 3D facial modeling, multimodal biometrics, and transformer-based deep learning frameworks to enhance system effectiveness and resilience against evolving spoofing threats.

References

[1] Afolabi Awodeyi, Philip Asuquo, Bliss Stephen, “Dynamic Liveness-Integrated Cnn Architecture for Face-Iris Spoof Detection”, IRE Journals, Volume 9 Issue 2, ISSN: 2456-8880, 2025

[2] M. Jasmine Pemeena Priyadarsini, K. Ramya, Shabareesh Parlakota, Naveen Kumar Reddy Tadi, A. Jabeena, G. K. Rajini, “Face Anti-Spoofing and Liveness Detection Using Deep Learning Architectures”, Journal of Engineering Science and Technology Special Issue on IEC2022, November (2022) 217 – 227

[3] Smita Khairnar, Shilpa Gite, Biswajeet Pradhan, Sudeep D. Thepade, Abdullah Alamri, “Optimizing CNN Architectures for Face Liveness Detection: Performance, Efficiency, and Generalization across Datasets”, Comput Model Eng Sci. 2025;143(3)

[4] Umer Farooq, Najam Ul Hasan, Imran Baig, Naeem Shehzad, “Efficient adaptive framework for securing the Internet of Things devices”, URASIP Journal on Wireless Communications and Networking (2019) 2019:210

[5] Dewan Ahmed Muhtasim , Monirul Islam Pavel and Siok Yee Tan, “A Patch-Based CNN Built on the VGG-16 Architecture for Real-Time Facial Liveness Detection”, Sustainability 2022, 14, 10024.

[6] Dronky, M.R.; Khalifa, W.; Roushdy, M. A review on iris liveness detection techniques. In Proceedings of the 2019 IEEE 9th International Conference on Intelligent Computing and Information Systems (ICICIS 2019), Cairo, Egypt, 8–10 December 2019; pp. 48–59. [CrossRef]

[7] Nsaif, A.K.; Ali, S.H.M.; Jassim, K.N.; Nseaf, A.K.; Sulaiman, R.; Al-Qaraghuli, A.; Wahdan, O.; Nayan, N.A. FRCNN-GNB: Cascade faster R-CNN with Gabor filters and naïve bayes for enhanced eye detection. IEEE Access 2021, 9, 15708–15719. [CrossRef]

[8] Chan, M.; Delmas, P.; Gimel’farb, G.; Leclercq, P. Comparative study of 3D face acquisition techniques. In International Conference on Computer Analysis of Images and Patterns; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3691, pp. 740–747.

[9] Raheem, E.A.; Ahmad, S.M.S.; Adnan, W.A.W. Insight on face liveness detection: A systematic literature review. Int. J. Electr. Comput. Eng. 2019, 9, 5165–5175. [CrossRef]

[10] Chen, F.M.; Wen, C.; Xie, K.; Wen, F.Q.; Sheng, G.Q.; Tang, X.G. Face liveness detection: Fusing colour texture feature and deep feature. IET Biom. 2019, 8, 369–377. [CrossRef]

[11] Khade, S.; Gite, S.; Thepade, S.D.; Pradhan, B.; Alamri, A. Detection of iris presentation attacks using hybridization of discrete cosine transform and haar transform with machine learning classifiers and ensembles. IEEE Access 2021, 9, 169231–169249. [CrossRef]

[12] Khade, S.; Gite, S.; Thepade, S.D.; Pradhan, B.; Alamri, A. Detection of iris presentation attacks using feature fusion of thepade’s sorted block truncation coding with gray-level co-occurrence matrix features. Sensors 2021, 21, 7408. [CrossRef]

[13] Muley, A.; Bendre, A.; Maheshwari, P.; Kumbhar, S.; Dhakulkar, B. Survey on biometric based ATMs. Int. J. Sci. Res. Sci. Technol. 2021, 8, 292–297. [CrossRef]

[14] Kowshika, A.; Sumathi, P.; Sandra, K.S. Facepin: Face biometric authentication system for ATM using deep learning.

NVEO-Nat. Volatiles Essent. OILS J. 2022, 9, 1859–1872.
[15] Waymond, R. Artificial Intelligence in a Throughput Model: Some Major Algorithms; CRC Press: Boca Raton, FL, USA, 2020