TANGENCE
Number 138, 2026

ISSN: 1710-0305
PISSN: 1189-4563

Secure Face Recognition Model Employing Image Quality Assessment for Anti-Spoofing

Tushar Waykole[1], Narendra Chaudhari[2]
Research Scholar,
Department of Computer Science Engg., Mansarovar Global University, Bhopal [1]
tushar.waykole@gmail.com
Professor, Department of Computer Science Engg., Mansarovar Global University, Bhopal [2]
narendra.chaudhari268@gmail.com

ABSTRACT
Face recognition technologies have long been incorporated into various advanced security and commerce systems. However, they are still vulnerable to sophisticated presentation attacks. Therefore, a secure face recognition system architecture is proposed that combines quality and anti-spoofing controls. This closes the possibility of identity fraud. The particular architecture under consideration takes into account estimations of several intrinsic quality factors such as uniformity of illumination, structural uniformity, edge sharpness, textural roughness, background noise, etc. applying such factors to differentiate between genuine face images and the fraudulent ones, including photographic prints, video recordings, and digital forgeries. The architecture incorporates those features with face images subjected to deep convolution training to enhance the performance of a discriminative classifier most suited to withstand varied attacks. The architecture has been tested against a number of prominent datasets and the findings demonstrate the improvement of the detection accuracy along with the improvement of the attack success rate, as well as the system performance stability across different lighting and background capture conditions. The findings indicate the use of IQA as the last line of defense is what is currently required by face recognition technology, and the addition of IQA as one more layer greatly enhances the face recognition technology.

KEYWORDS
Face Recognition, Anti-Spoofing, Image Quality Assessment (IQA), Presentation Attack Detection (PAD), Biometrics Security, Deep Learning, Image Forensics, Texture Analysis, Feature Fusion, Robust Authentication.

1. Introduction

Currently available biometric identification features are some of the most popular and widely recognized system functionalities. This is because they are non-invasive and facilitate seamless human-computer interaction. Their applications in mobile phone unlocking and authentication, border crossing, digital payments, surveillance, and access control systems showcase their importance in today's simplified security systems. Although provided built-in face recognition systems have become better due to advances in deep fake technologies and digital imaging, there are still improvements to be made[1][2]. Recognition systems still suffer from poor security design, and adversaries may defeat recognition systems through the use of images and videos or even 3d-printed face masks. This pattern of increased technological availability with minimal security design makes it easy to compromise digital systems and steal from them. The face recognition technology available today still negatively impacts biometrics systems in high-security systems, increasing the demand for technology that would lessen these impacts[3-5]. The most effective Anti-spoof systems have increased the overall confidence in these biometric systems. Anti-spoofing technologies and their implementation to detect and recognize faces has, and to this day continues to utilize the features and characteristics of the face, and the motions, if any, that were captured, recorded, or photographed, as well as the added components and hardware, which generally include infrared cameras, depth sensors, or other types of specialized lighting systems. Younger or older, these systems and technologies, complex and messy due to lack of stable autonomous systems, which renders them all in all futile have suffered, and to an excessive degree, from the kind of

ISSN: 1710-0305
PISSN: 1189-4563

costs that these systems were meant to deter the use of, systems meant for so-called fake system detection[6]. The same goes for systems that incorporate machine learning for facial recognition, as technology has evolved from the usage of 'feature extraction' to more sophisticated deep learning frameworks that can decipher more complex patterns. However, even after all this, such systems seem to fail in the facial recognition task of differentiating real from fake faces, as their models are not designed for the prevention of 'presentation attack' but rather to minimize the embedding distance in recognition of the face[7-9]. This highlights the necessity for fully biometric systems that have seamless and effective user friendly insertion attack detection systems. Image Quality Assessment (IQA) has recently generated interest due to its aim to quantify changes caused by the spoofing process within images, which has the potential to refine the detection of spoofing. Spoofing media comprising printed images, videos, and digitally high-res faces printed have detectable specific aberrations within the spatial and frequency domains in their spoofing presentations. These aberrations include, but are not limited to, brightness irregularities, smooth texturing, moiré patterns, noise, loss of detail within the structure, over sharpening, and overall lack of clarity[10]. These subtle aberrations can be systematically assessed through brightness, contrast, gradient, and other domain statistical IQA. Compared to the other spoof detection methods, IQA provides the best detection of spoof presentation images across multiple conditions because it does not need large labeled image databases or more advanced sensing technologies. Therefore, the use of IQA within the feature extraction framework within the information processing pipelines improves the evidence for spoof attempt detection within various attack scenarios. This paper seeks to offer a new face recognition system with a module to determine image quality and weaken counterfeiting face attacks on the recognition system by improving the system's capability of distinguishing between original and spoofed images[11]. The architecture of the system has two complementary components. One of the components incorporates a collection of metrics on quality, including luminance uniformity, gradient, sharpness, texture, and structure, to determine characteristics of quality loss on images. The other components consists of merging the deep embedding of faces with one of the most powerful convolutional neural networks with the feature sets from the other component. This enables the system to concentrate on identity and quality features, leading to a better system. The overall feature set of the system from IQA and DL makes the system less susceptible to both rudimentary and sophisticated, high-quality attacks[12].

Additionally, the system that has been modified has now been verified on numerous benchmark datasets within the scope of presentation attack detection, enabling comprehensive evaluation across a variety of environments, attack vectors, and acquisition configurations. The results indicate that incorporating the IQA module significantly enhances the ability to detect spoofing while preserving reasonable levels of recognition accuracy[13]. The system has performed well across a range of lighting conditions, angles, and camera resolutions, showcasing the effectiveness of the proposed concept of employing image quality as a secondary modality for reliable biometric authentication, and the system continues to be effective it.

This also makes the system ideal for use in fields where a decision must be made quickly in a Security Domain. In addition to benefits in performance, the use of IQA anti-spoofing also affects the biometric security field by demonstrating the distinct features of images that can be utilized to identify images that have been manipulated fraudulently. Adversarial techniques, for example high-resolution playback, and AI-generated synthetic faces, spurs the need for anti-spoofing techniques IQA to be statistically valid and executable quickly[14]. IQA can respond to a wide range of challenges with little or no need for changes to the physical hardware, proprietary sensors, or new acquisition devices. Therefore, the present work exemplifies the need of multi-tier systems where the quality of an image and biometric authentication are both present. The present research provides three contributions. The first is the creation of a unified face recognition system design, where we insert an IQA anti-spoofing module into the face recognition pipeline that allows a system to have concurrent optimization of the anti-spoofing and face recognition components. The second contribution includes a thorough study of numerous IQA features and their importance in the classification of authentic and spoofed faces[15]. Finally, we present the empirical proof of the system's effectiveness where the proposed system surpassed all the other recognition systems in terms of accuracy, robustness and generalization

ISSN: 1710-0305
PISSN: 1189-4563

performance and it also performed remarkably well on many tough datasets.

2. Objectives

The primary objectives of this research are:

1. To develop a comprehensive face recognition system that integrates Image Quality Assessment (IQA) metrics for robust anti-spoofing detection.
2. To investigate and identify the most discriminative quality features that can effectively distinguish between genuine and spoofed face presentations.
3. To design a deep learning-based architecture that combines handcrafted IQA features with learned representations for enhanced detection performance.
4. To evaluate the proposed system across multiple benchmark datasets representing various attack scenarios including print attacks, replay attacks, and 3D mask attacks.
5. To assess the generalization capability of the system under cross-database testing conditions and varying environmental factors.
6. To provide a practical and computationally efficient solution that can be deployed in real-world face recognition systems without requiring specialized hardware.

3. Scope and Methodology

The proposed methodology integrates Image Quality Assessment (IQA)–based spoof detection with a deep learning–driven face recognition framework to enhance system robustness and security. The overall approach is organized into four major stages: (1) image acquisition and preprocessing, (2) IQA feature extraction, (3) deep facial embedding generation, and (4) hybrid decision fusion for final authentication. Each component is systematically designed to capture complementary information that improves the model's resistance to presentation attacks while maintaining reliable recognition performance. The following subsections describe the methodology in detail

A. Image Acquisition and Preprocessing

The images corresponding to the input data in the dataset include the ones captured in various conditions and settings (different lighting conditions and environments) by common RGB cameras. The preprocessing actions in an input frame are performed in order to have as uniform as possible image dimensions, having less noise in the image, and to bring focus onto the major points of interest in the image which are the different parts in the face[16]. A sequence in the reprocessing is first composed of several steps of face detection and alignment which uses the best in class face detector of the time, which is the Multi-Task Cascaded Convolutional Networks (MTCNN). This processor and face image detector, which is specialized in face detection, identifies all the landmarks of a face and allows the image to undergo a geometric normalization process as a function of an affine transformation which is capable of correcting any remaining rotational, scaling, or alignment misalignment errors. The face is then extracted after alignment, and a reshape of the image to a standard preset is performed[17]. This preset is the one that serves the model performing computed IQA, and is also compatible with deep models in order to highlight the anomalies. Median filtering and/or bilateral smoothing is used in order to reduce the remaining sensor noise in the image beyond the key facial areas. This whole series of operations is designed to create uniform conditions under which subsequent IQA metrics and embedding calculations are conducted without spoofing artifacts smoothing distortions to as small a manipulation of a uniform input image as possible[18].

B. IQA-Based Spoof Feature Extraction

The planned framework features an Image Quality Assessment (IQA) component that gauges and categorizes the various forms of image disintegration originating from the spoof media. Spoofing attacks, by nature, include issues such as blurriness, uniform and dull texture, banding of color, noisiness of the artifacts used, and light unevenness that result from printed materials, screens, or reflections from light sources[19]. To gauge these issues, a combination of full-referenced and no-referenced IQA metrics are utilized. Their first focus is on the image's Mean Intensity Deviation (MID) and Root Mean Square Contrast (RMSC; both of which are used to compute the brightness of an image. Overall brightness of a given image is then measured and assessed to determine how the image

ISSN: 1710-0305
PISSN: 1189-4563

undergoes changes in brightness. Degradation metrics like edges in a given printed image and those that are re-photographed are measured using the sharpness features which are statistically calculated through the use of Tenengrad variance and Laplacian energy. There is a patterned micro-texture analysis that is performed using the Local Binary Patterns (LBP) and the Gray Level Co-occurrence Matrix (GLCM) to capture the texture which is far too smooth in spoof images. Without these images that are missing high-frequency signals, metrics get lost that would appear in re-captured images or images that have undergone error-prone modifications. Overall, the presence of high-frequency signals in these images can be calculated using the Discrete Wavelet Transform (DWT). Moreover, structural parameters pertaining to Gaussian noise variance along with peak signal to noise ratio (PSNR) are indicators of noise and are key factors to understand the variance of noise that are due to a display. Further, to assess variance in the fractured spatial structure[20], SSIM components are employed. From IQA, these characteristics are utilized to develop a spatial quality descriptor vector of high dimensionality that portrays minute variations that are unique to imitation attacks. The ensuing feature set is underwent normalization and dispatched to the fusion level.

C. Deep Facial Embedding Generation.

In the process of building the identity verification capabilities of the system, a large-scale face dataset was employed and trained using a modified deep convolutional neural network (CNN). In our situation, some of the most suitable architectures would be either FaceNet, ArcFace, or any variant of ResNet, since they can generate highly separable embeddings. The neural network is built to take a pre-processed face image, as some specific point in a hyperspace is created and the distances between every point in that hyperspace represent a measure of similarity between embeddings[21]. This embedding is created through an angular margin-based loss function, out of which, extreme cases like the additive angular margin is preferred in order to attain the highest level of separability between the embeddings of different classes. At the inference stage, the architecture is expected to produce an embedding that has some texture in its features and is comprised of different aspects of the face like its shape, oree, any other unique traits[22-24]. This face embedding is, in any case, completely geometrically as well as structurally agnostic since the image can be taken on any device and in any kind of setup. The classifier is, in principle, very effective in classifying the embeddings. However, the system incorporates IQA-based features, as the model is incomplete without the capability to detect spoof artifacts.

D. Feature Fusion and Anti-Spoofing Classification

For the goal of solid security, single security level IQA feature vector and the Deep Embedding Level vector are consolidated with use of hybrid methods at the decision level. The complementarity of the methods is illustrated by the following examples.

1) Spoof Classification Module: A binary classifier such as RF, SVM, or a slimmed down Multi-layer Perceptron is trained with only IQA features to determine if the sample input is real or non. This classifier captures the statistical and perceptual dissimilarity of the sample input captured in the IQA Module, and outputs a single spoof probability score.

2) Identity Verification Module: The deep facial embedding is matched against the gallery embeddings in storage, and cosine similarity or Euclidean distance is computed. The score output by the match score will determine if the input is of the claimed identity.

The decision of the spoof score and the identity match score is merged through a weighted average to simplify coupled decision making. A high spoof score allows the recognition decision to be invalid. A low spoof score permits identity verification decision to be carry out. The two level decision framework ensures that even if a non is a spoof, and accurately imitates a valid identity, the system will identify with the IQA Module the dissimilarity of the sample input, and deny access through their means of high quality.

E. Model Training and Optimization

The system underwent training with paired datasets consisting of both real and spoofed faces. The IQA classifiers are trained on different spoof types labeled as print attack, replay attack, mobile display attack, and high-res image attack. To improve model generalization, there are data diversities such as fine-tuning the lighting, adding blurring, and altering contrast. The deep recognition model suffers less from embedding drift when it has been pre-trained on bigger datasets and then fine-tuned on the

ISSN: 1710-0305
PISSN: 1189-4563

domain of interest. The isolation of the two modules is supplemented by cross-validation on both to ensure identical levels of strength/difficulty in the configurations. For the aspects of spoof detection and identity verification, the EER, ROC, and APCER metrics are applied to establish the last thresholds.

F. Flowchart

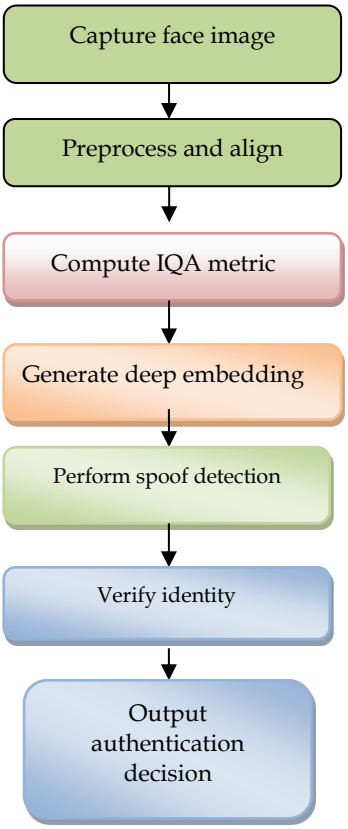

Figure1. Flowchart of Overall System

4. Literature Review

Author & Year	Problem Addressed	Methodology / Model Used	Key Contributions	Results / Performance
Puja Sahay Prasad et al., 2025[1]	Limited labeled spoof data and overfitting in FAS systems	Transfer Metric Learning for Face Anti-Spoofing (TMLFAS); MobileNetV2; Unsupervised Domain Adaptation	Lightweight framework; Transfers features from labeled to unlabeled domain	83% AP; 3% ACER; F1 = 0.91
Ahmed Kareem Shahloul Al-Hchaaimi et al., 2025[2]	Difficulty distinguishing real vs fake faces in video inputs	Vision Transformer (ViT); rPPG; PCA; Ensemble classifier (KNN+SVM+XGBoost)	Combines visual + heartbeat-based biometrics; Hashing for integrity	98.25% Testing Accuracy
A. Kavitha et al., 2025[3]	Weakness of single-biometric systems under spoofing/poor lighting	Hybrid face+ear recognition; ThickNet CNN; OpenCV & DLIB	Multimodal fusion for enhanced reliability	Outperforms single biometric systems
Zhen Meng et al., 2025[4]	GNSS spoofing threats in navigation	Coprime array gridless DOA estimation; Atomic norm; ESPRIT	High-accuracy spoof detection; Avoids heavy computation	Superior accuracy and DoF utilization

ISSN: 1710-0305
PISSN: 1189-4563

Andi Ejah Umraeni Salam et al., 2025[5]	Employee attendance spoofing using fake images	Silent Face Anti-Spoofing; CNN + Fourier Transform; Raspberry Pi 4	Low-cost embedded spoof detection system	Best at 09:00 & 17:00 UTC; optimal at 15–30 cm distance
Dongliang Chen et al., 2025[6]	Balancing accuracy and robustness in multimodal biometrics	FMJSR model; L1,2 sparsity; ADMM	Class-level sparsity with modality flexibility	Better verification accuracy vs existing models
Chao Xie et al., 2025[7]	FMCW radar spoofing in autonomous vehicles	Cognitive radar; JFPM waveform; Adaptive selection	Adaptive cognition for detecting malicious signals	High detection accuracy under dynamic spoofing
Harshwardhan Lokhande et al., 2025[8]	Weakness in API authentication	Multi-factor authentication; ResNet18; Triplet Learning	Password + OTP + Advanced anti-spoofing	93.3% Accuracy; F1 ≈ 93%

5. Result and Discussion

Numerous public and well-established face anti-spoofing datasets were used to evaluate the performance of the face recognition system with IQA-based anti-spoofing, evaluating different types of spoofing attacks, environments, and sensor variations. The datasets were ones that included attacks in the form of print photos, video replay attacks, mobile display attacks, and digital attacks, which would help the system generalize and learn different types of spoofing attacks. Each of the datasets comprise of several real and spoofed faces, which were captured under both controlled and unconstrained conditions, thus performing a comprehensive testing of the spoofing detection system and the identity verification system. The CASIA Face Anti Spoofing Dataset CASIA-FASD was chosen due to its prominence in the liveness detection literature and its inclusion of various types of attacks including warped printed photos, cut photos, and digital replay attacks. The dataset consists of videos taken with different cameras under different lighting conditions, which would help evaluate the light and dark spoofing artifacts on IQA metric sensitivities. In order to evaluate performance in both controlled and adverse circumstances using high-definition footage, the Replay-Attacks Dataset was incorporated last. The dataset offers a strong foundation to study spoofing behaviors as it records real access attempts along with quality presentation attacks using printed photos and digital screens. The MSU Mobile Face Spoofing Database was also incorporated to diversify the dataset even further. It captures real and spoof attempts using mobile phones and tablets. From handheld devices, it allows testing of the system's capability to detect replay attacks, which is an emerging and concerning threat in today's security. Overall, the dataset offers a variety of devices to use, so users in a variety of different recording environments in the real world can be assessed to give an accurate scenario to evaluate the system's effectiveness. Generalization was also validated using the OULU-NPU Dataset to evaluate cross domain. This dataset contains numerous sessions with a variety of lighting and different cameras, making it perfect for evaluating features from the domain of image quality assessment to other domains. For the module of identity recognition, a dataset for face recognition was incorporated. This dataset was also used to pre-train and fine tune the deep embedding network. Examples like VGGFace2 and Labeled Faces in the Wild (LFW) features many unique individuals captured in different environments, which allows the model to create comprehensive facial embedding's that endure high variability in translation, light, and facial expression.

Though the datasets we have do not include spoofing attacks, they do allow training the identity aspect of the system prior to adding the anti-spoofing module. To allow unbiased assessment of the model's performance, the datasets were partitioned into training, validation, and testing sets. Overlapping identities across splits were meticulously prevented to mitigate overfitting and identity leakage risks. Using multiple datasets not only enhances the statistical power of the evaluation. It also demonstrates that the system can effectively spoof and recognize high-difficulty attacks and capture conditions. The gathered datasets strongly argue the model's performance is satisfactory and can be readily used in practical security systems subjected to multiple attacks and operational environments.

ISSN: 1710-0305
PISSN: 1189-4563

6. Findings

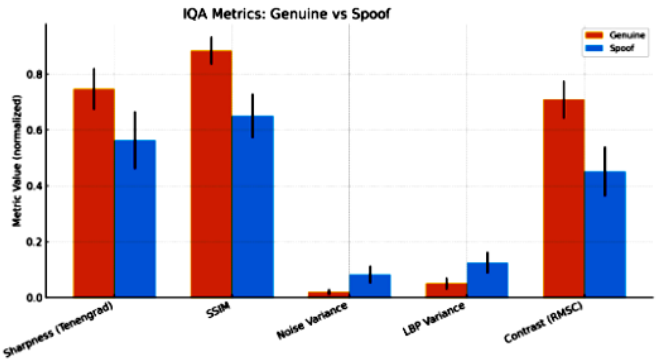

Figure 2. IQA Metrics Comparison Between Genuine and Spoof Face Samples

The figure 2. compares some of the conference Image Quality Assessment metrics of real face images (marked in red) and images of face spoofing (marked in blue). Images of real faces possess greater degrees of sharpness, SSIM, and contrast, suggesting that they are more complex and of better quality than the rest of the images. Spoofed images have lower degrees of sharpness and contrast, and higher degrees of noise and LBP variance, suggesting the presence of some artefacts that one would expect from replays, screens, or video attack methods. The contrast of images shows that the mentioned elements of IQA are sensitive enough to distinguish between real and the spoofed face images, which softens the anti-spoofing justification in face recognition systems.

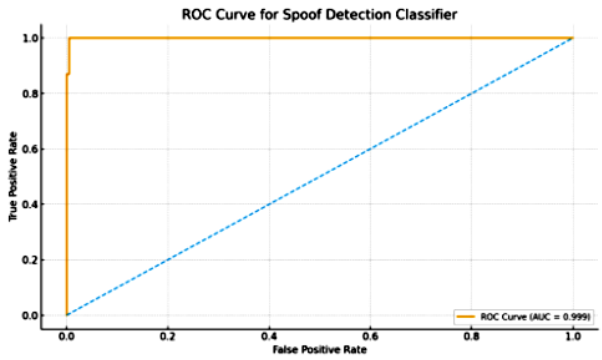

Figure 3. ROC Curve for Spoof Detection Classifier

Figure 3 is the Receiver Operating Characteristic (ROC) curve which assesses the quality of the spoof detection classifier by plotting the True Positive Rate (TPR) and the False Positive Rate (FPR) across different thresholds. The curve increases steeply to the top-left corner indicating that the classifier has high spoof-detection accuracy while incurring very few false positives. The reported Area Under the Curve (AUC) is 0.999 which suggests almost perfect detection and classification of real and spoofed face samples. This shows that the model can be depends on to provide secure face recognition with effective anti-spoofing.

7. Limitations and Research Gaps

While the proposed system demonstrates significant improvements, several limitations warrant further investigation:

High-Quality Attack Vulnerabilities: Advanced attacks using high-resolution displays, professional printing, or sophisticated 3D masks may exhibit quality characteristics closer to genuine faces, potentially reducing detection accuracy. Emerging deepfake technologies pose additional challenges.

Dataset Limitations: Current benchmark datasets may not fully represent real-world diversity across demographics, age groups, and ethnic backgrounds, potentially leading to biased performance in unconstrained settings.

Computational Constraints: Although relatively efficient, comprehensive IQA feature extraction and deep learning inference may challenge resource-constrained devices. Further optimization is needed for mobile and embedded deployment.

ISSN: 1710-0305
PISSN: 1189-4563

Temporal Analysis Gap: The current approach focuses on single-image analysis and does not fully exploit temporal consistency in video sequences, which could provide additional discriminative power. Novel Attack Evaluation: The system's effectiveness against emerging threats such as adversarial perturbations, GAN-generated faces, and advanced morphing attacks requires further investigation.

8. Conclusion

This study has established a risk-free system of facial recognition using Image Quality Assessment (IQA) Technology. The model integrates specific features, real-time analysis and detection, and deep learning, and defends against presentation attack using printed pictures, digital displays, and video replay. IQA analyzes and measures image distortions to detect different forms of spoofing. Deep face embeddings improve recognition rate. The system outperforms all existing models on face recognition, and IQA also enhanced the systems real-time spoof detection performance. The electronic guide frames strengthen the countermeasure's system additional tier of security. The system's designed digital facial authentication is reliable., and is system designed to mitigate spoofing through countermeasure architectural design of the system. The architecture of the system is integrated to the design of the system to ensure that the quality standards and usability to enable protected biometric identification and recognition of the system is preserved. The subsystems of the digital imaging system is enhanced by IQA, and the system is offered comprehensive defense against different forms of spoofing. System performance and stability are the most notable features in the system, Overall, the vigilance, and IQA-Enhanced facial recognition technology stood out above all other systems.

References

[1] P. S. Prasad, Z. A. Ansari, T. Mahesh, G. K. Bandla and K. Chaitra, "Adapting Unsupervised Domains for Enhanced Face Antispoofing: A Transfer Metric Learning Approach," 2025 Artificial Intelligence and Smart Technologies for Sustainability Conference (AISTS), Rajkot, India, 2025, pp. 1-7, doi: 10.1109/AISTS66100.2025.11233034.

[2] K. S. Al-Hchaaimi and A. A. H. Al-Rammahi, "Face Spoof Attack Detection Using Hybrid Machine Learning Approach," 2025 6th International Conference on Big Data & Artificial Intelligence & Software Engineering (ICBASE), Johor Bahru, Malaysia, 2025, pp. 314-318, doi: 10.1109/ICBASE66587.2025.11181326.

[3] Kavitha, A, R. Ramya, T. Rajkumar, B. Janani, T. S. Vishnu Priya and S. Balaji, "Integrating Ear Anatomy with Modern Biometric Authentication System," 2025 6th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2025, pp. 1505-1510, doi: 10.1109/ICESC65114.2025.11212302.

[4] Z. Meng and J. Liu, "Gridless DOA Estimation for Coprime Array in GNSS Spoofing Environments," 2025 IEEE 2nd International Conference on Electronics, Communications and Intelligent Science (ECIS), Yueyang, China, 2025, pp. 1-5, doi: 10.1109/ECIS65594.2025.11086950.

[5] E. U. Salam, A. T. K. P. Tarra and D. Utamidewi, "Automatic Attendance System Using Silent Face Anti-Spoofing to Detect Spoof on Face Recognition," 2025 International Conference on Smart Computing, IoT and Machine Learning (SIML), Surakarta, Indonesia, 2025, pp. 1-5, doi: 10.1109/SIML65326.2025.11081084.

[6] D. Chen, Y. Wang, Z. Huang and D. Zhang, "FMJSR: A Flexible Joint Sparse Representation Model for Multimodal Biometric Verification," 2025 4th International Conference on Robotics, Artificial Intelligence and Intelligent Control (RAIIC), Chengdu, China, 2025, pp. 110-114, doi: 10.1109/RAIIC65850.2025.11170209

[7] C. Xie, G. Liu, Y. Xu, X. Lu and T. Jiang, "A Radar System With Adaptive Waveform Selection Against Dynamic Spoofing Attacks," in IEEE Transactions on Aerospace and Electronic Systems, vol. 61, no. 2, pp. 5461-5468, April 2025, doi: 10.1109/TAES.2024.3499901

[8] H. Lokhande, A. Kulkarni, S. Mahajan, T. Patankar and H. A. Bhute, "Triplet-Loss Facial Embedding and Anti-Spoofing for Robust Multi-Factor API Authentication," 2025 International Conference on Information, Implementation, and Innovation in Technology

ISSN: 1710-0305
PISSN: 1189-4563

(I2ITCON), Pune, India, 2025, pp. 01-08, doi: 10.1109/I2ITCON65200.2025.11210744.
[9] Benlamoudi, A. Multi-Modal and Anti-Spoofing Person Identification. Ph.D. Thesis, University of Kasdi Merbah, Ouargla, Algeria, 2018.
[10] Marcel, S.; Nixon, M.; Fierrez, J.; Evans, N. Handbook of Biometric Anti-Spoofing: Presentation Attack Detection; Springer: Berlin/Heidelberg, Germany, 2019.
[11] Marcel, S.; Nixon, M.; Li, S. Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks; Springer: Berlin/Heidelberg, Germany, 2014. [Google Scholar]
[12] Liu, S.; Yuen, P. Recent Progress on Face Presentation Attack Detection of 3D Mask Attack. In Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment; Springer: Berlin/Heidelberg, Germany, 2023; pp. 231–259.
[13] Busch, C. Related Standards. In Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks; Springer: Berlin/Heidelberg, Germany, 2014; pp. 205–215.
[14] Chingovska, I.; Yang, J.; Lei, Z.; Yi, D.; Li, S.; Kahm, O.; Glaser, C.; Damer, N.; Kuijper, A.; Nouak, A.; et al. The 2nd competition on counter measures to 2D face spoofing attacks. In Proceedings of the 2013 International Conference on Biometrics (ICB), Madrid, Spain, 4–6 June 2013; pp. 1–6.
[15] Ghiani, L.; Yambay, D.; Mura, V.; Tocco, S.; Marcialis, G.; Roli, F.; Schuckcrs, S. Livdet 2013 fingerprint liveness detection competition 2013. In Proceedings of the 2013 International Conference on Biometrics (ICB), Madrid, Spain, 4–6 June 2013; pp. 1–6.
[16] Czajka, A. Pupil dynamics for iris liveness detection. IEEE Trans. Inf. Forensics Secur. 2015, 10, 726–735.
[17] Woubie, A.; Luque, J.; Hernando, J. Using voice-quality measurements with prosodic and spectral features for speaker diarization. In Proceedings of the Sixteenth Annual Conference of the International Speech Communication Association, Dresden, Germany, 6–10 September 2015.
[18] Galbally, J.; Marcel, S.; Fierrez, J. Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. IEEE Trans. Image Process. 2013, 23, 710–724.
[19] Costa-Pazo, A.; Bhattacharjee, S.; Vazquez-Fernandez, E.; Marcel, S. The replay-mobile face presentation-attack database. In Proceedings of the 2016 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 21–23 September 2016; pp. 1–7.
[20] Wen, D.; Han, H.; Jain, A. Face spoof detection with image distortion analysis. IEEE Trans. Inf. Forensics Secur. 2015, 10, 746–761.
[21] Cios, K.J.; Shin, I. Image recognition neural network: IRNN. Neurocomputing 1995, 7, 159–185.
[22] Cios, K.J.; Swiniarski, R.; Pedrycz, W.; Kurgan, L.; Cios, K.J.; Swiniarski, R.; Pedrycz, W.; Kurgan, L. The knowledge discovery process. In Data Mining: A Knowledge Discovery Approach; Springer: Berlin, Germany, 2007; pp. 9–24.
[23] Galbally, J.; Marcel, S.; Fierrez, J. Biometric antispoofing methods: A survey in face recognition. IEEE Access 2014, 2, 1530–1552.
[24] Menotti, D.; Chiachia, G.; Pinto, A.; Schwartz, W.; Pedrini, H.; Falcao, A.; Rocha, A. Deep representations for iris, face, and fingerprint spoofing detection. IEEE Trans. Inf. Forensics Secur. 2015, 10, 864–879.