Liveness Detection and Biometric Authentication System (BAS)

Eke Uchechukwu Sixtus
Department of Computer Science Imo
State University, Owerri, Nigeria
ekeuchechukwu56@gmail.com
+2348064759700

Comfort.C Olebara
Department of Computer Science Imo State University,
Owerri, Nigeria chiiprime@gmail.com
+234 8131246389

Elochukwu Ukwandu
Cardiff School of Technologies,
Cardiff Metropolitan University
Cardiffmet@.ac.uk

https://doi.org/10.56201/rjmcit.vol.12.no8.2026.pg134.148

Abstract
The increasing use of digital services, mobile devices, online platforms, and electronic access-control systems has created a growing need for reliable and secure user authentication. Traditional authentication techniques such as passwords, personal identification numbers, and security questions are vulnerable to theft, guessing, sharing, phishing, and other forms of unauthorized access. Biometric authentication provides an alternative approach by identifying or verifying individuals based on unique physiological or behavioural characteristics such as facial features, fingerprints, iris patterns, and voice characteristics. However, biometric systems are also exposed to presentation attacks in which an attacker attempts to deceive the authentication system using a photograph, recorded video, artificial fingerprint, mask, or other fabricated biometric representation. Liveness detection is therefore an important security mechanism for determining whether a biometric sample originates from a genuine living person who is physically present during authentication. This study presents a practical approach to the design and implementation of a Liveness Detection and Biometric Authentication System (BAS). The proposed system integrates biometric verification with liveness detection to reduce the possibility of unauthorized access through spoofed biometric samples. The system captures a user's biometric sample, performs preprocessing and feature extraction, determines whether the presented sample is live or a potential presentation attack, and proceeds to biometric matching only when the sample passes the liveness assessment. The research adopts a quantitative experimental design involving biometric samples representing genuine users and simulated presentation attacks. The proposed framework considers techniques such as facial feature analysis, blink detection, facial movement, texture analysis, image quality assessment, and machine learning classification. The performance

of the proposed system can be evaluated using biometric and presentation-attack metrics including accuracy, false acceptance rate, false rejection rate, precision, recall, F1-score, Attack Presentation Classification Error Rate (APCER), and Bona Fide Presentation Classification Error Rate (BPCER). The study demonstrates that combining biometric authentication with liveness detection provides stronger protection than relying on biometric matching alone. The proposed system can therefore contribute to secure access control, identity verification, digital services, attendance systems, financial applications, and other environments where reliable user authentication is required.

Keywords: *Liveness Detection, Biometric Authentication, Presentation Attack Detection, Facial Recognition, Authentication Security, Anti-Spoofing, Biometric System.*

1. Introduction

The rapid growth of digital technologies has transformed the way individuals access computer systems, mobile devices, online services, financial platforms, institutional portals, and other digital resources. As more activities move from physical environments to digital platforms, authentication has become an essential component of information security. Authentication is the process of verifying that an individual attempting to access a system is actually the person they claim to be. Traditional authentication approaches commonly depend on passwords, personal identification numbers, security tokens, and other credentials. Although these techniques remain widely used, they can be compromised through password theft, guessing, phishing, credential sharing, malware, and social engineering attacks. Biometric authentication has emerged as an important alternative because it uses characteristics associated with an individual rather than relying entirely on information that the user must remember or possess. Biometric systems may use fingerprints, facial characteristics, iris patterns, palmprints, voice, or other measurable characteristics to identify or verify users. The increasing availability of cameras, fingerprint sensors, and computational resources has made biometric authentication increasingly practical for personal devices and digital services. Despite the advantages of biometric authentication, the technology introduces its own security challenges. Unlike passwords, biometric characteristics cannot normally be replaced when compromised. Facial images, fingerprints, and other biometric characteristics can potentially be captured without the individual's knowledge and reproduced or manipulated for fraudulent purposes. This makes the protection of the biometric capture and authentication process particularly important. One of the major threats against biometric systems is the presentation attack. A presentation attack occurs when an attacker presents an artificial or manipulated biometric sample to the biometric capture system with the intention of being incorrectly accepted as an authorized user. Examples include presenting a printed photograph to a facial recognition camera, displaying a recorded facial video on a mobile device, using a fabricated fingerprint, or presenting a three-dimensional mask. NIST describes Presentation Attack Detection (PAD) as the automated determination of whether a presentation constitutes an attack, while liveness detection can involve analysing characteristics or reactions associated with a living person present at the point of capture. Liveness detection is consequently an important component of modern biometric authentication. Rather than simply determining whether the captured biometric resembles a stored template, a liveness mechanism attempts to establish whether the biometric sample originates from a genuine live subject. This provides an additional layer of security against common spoofing techniques.

Modern liveness detection approaches may be passive or active. Passive approaches analyse characteristics such as texture, illumination, depth, image quality, facial motion, or physiological information without requiring the user to perform a specific action. Active approaches may require the user to blink, turn the head, smile, follow a randomly generated instruction, or perform another challenge-response activity. Recent research has demonstrated the use of deep learning and other machine learning techniques for face anti-spoofing and presentation attack detection.

The importance of liveness detection is also reflected in current digital identity guidance. NIST's current authentication guidance requires presentation attack detection for facial recognition and recommends appropriate presentation-attack testing for biometric systems.

However, implementing an effective liveness detection system presents several challenges. Attackers continuously develop more realistic spoofing materials, while variations in lighting, camera quality, facial appearance, background, pose, and environmental conditions may affect system performance. A system that is too strict may reject genuine users, while a system that is too permissive may accept fraudulent presentations. This study therefore focuses on the design and implementation of a Liveness Detection and Biometric Authentication System that combines biometric verification with anti-spoofing mechanisms. The objective is to provide a more secure authentication process capable of distinguishing genuine biometric presentations from common spoofing attempts.

2. Literature Review

2.1 Overview of Biometric Authentication

Biometric authentication refers to the process of verifying an individual's identity using measurable physiological or behavioural characteristics. Unlike traditional authentication methods that rely on something a person knows, such as a password, or something a person possesses, such as a security token, biometric authentication relies on characteristics associated with the individual. Common biometric modalities include fingerprint, facial recognition, iris recognition, palmprint, voice recognition, and behavioural biometrics. Each modality has different strengths, limitations, accuracy levels, and security considerations. Biometric authentication normally involves several stages. First, a biometric sample is captured using a sensor or camera. The captured sample is then processed to remove noise and improve its quality. Relevant biometric features are extracted and converted into a representation suitable for comparison. The extracted representation is subsequently compared with a previously stored biometric template. Based on a predefined similarity threshold, the system either accepts or rejects the authentication attempt.

The effectiveness of a biometric system depends not only on the accuracy of the matching algorithm but also on the security of the entire biometric processing chain. NIST guidance emphasizes that biometric characteristics are not secrets and can potentially be obtained or reproduced, making additional protections such as presentation attack detection important.

2.2 Concept of Liveness Detection

Liveness detection refers to techniques used to determine whether a biometric sample originates from a genuine living person rather than an artificial or reproduced biometric representation.

In facial authentication, liveness detection may determine whether the face presented to the camera belongs to a live person rather than a photograph, video replay, mask, or digitally manipulated image. In fingerprint authentication, liveness detection can analyse characteristics that distinguish a genuine finger from a fabricated fingerprint.

Liveness detection is closely related to Presentation Attack Detection (PAD). PAD focuses on identifying presentations designed to interfere with the normal operation of a biometric system. NIST defines PAD as an automated determination of a presentation attack, and identifies liveness detection as one category of methods used to determine whether a biometric sample is being captured from a living subject. A liveness detection module can therefore serve as a security gate before biometric matching. If the sample is classified as a spoof, the authentication process is terminated. If the sample is classified as genuine, the system continues with biometric verification.

2.3 Biometric Presentation Attacks

Presentation attacks represent a major security challenge for biometric authentication systems. An attacker does not necessarily need to compromise the underlying database or authentication algorithm. Instead, the attacker may attempt to manipulate the input presented to the biometric sensor.

Common facial presentation attacks include:

- Printed photographs
- Photographs displayed on mobile phones or tablets
- Replayed facial videos
- Three-dimensional masks
- Digitally manipulated images
- High-quality synthetic or deepfake content

Fingerprint presentation attacks may include artificial fingers, moulded fingerprints, or other fabricated materials designed to imitate a genuine fingerprint.

Research has shown that biometric presentation attacks can significantly affect the reliability of biometric authentication systems if appropriate anti-spoofing mechanisms are not implemented. Recent research has consequently focused on PAD algorithms capable of detecting both known and previously unseen attack types.

2.4 Types of Liveness Detection Techniques

2.4.1 Challenge-Response Liveness Detection

Challenge-response techniques require the user to perform a randomly selected action. Examples include blinking, turning the head, smiling, opening the mouth, or following a moving object displayed on the screen. The purpose of this approach is to make it more difficult for an attacker to use a static photograph or previously recorded material. However, sophisticated replay attacks may reproduce some predictable actions. Therefore, randomization and appropriate challenge selection are important.

2.4.2 Texture-Based Liveness Detection

Texture-based techniques examine patterns within biometric images. A genuine face and a photograph displayed on a screen may exhibit different texture characteristics because of printing artefacts, screen pixels, reflections, compression, and surface properties.

Machine learning algorithms can be trained to identify these differences and classify biometric samples as live or spoofed.

2.4.3 Motion-Based Liveness Detection

Motion-based liveness detection examines natural movement associated with a living person. In facial authentication, the system may analyse blinking, head movement, eye movement, facial expressions, or other temporal characteristics.

Motion information can provide useful evidence because a static image cannot naturally perform the required movement.

2.4.4 Depth-Based Liveness Detection

Depth-based techniques analyse three-dimensional characteristics of a captured biometric. Genuine human faces have three-dimensional structures, while printed photographs are generally flat. Depth information can therefore help distinguish genuine faces from photographs. However, depth sensors may increase system cost and hardware requirements.

2.4.5 Machine Learning-Based Liveness Detection

Machine learning can be used to classify biometric samples as genuine or spoofed. The model is trained using examples of bona fide samples and presentation attacks.

Deep learning has become particularly important in face anti-spoofing because neural networks can learn complex visual representations directly from biometric data. A recent survey of deep-learning-based face anti-spoofing research identifies binary classification, pixel-wise supervision, domain generalization, and multimodal sensing as important research directions.

2.5 Facial Biometric Authentication

Facial recognition is one of the most widely deployed biometric technologies because many computing devices already contain cameras. A facial authentication system generally detects a face, extracts distinguishing facial features, creates a feature representation, and compares that representation against an enrolled user's biometric template.

The major advantage of facial authentication is convenience because users generally do not need to physically touch a sensor. However, this contactless characteristic also creates presentation-attack risks because an attacker may present photographs, videos, masks, or manipulated digital content. Recent research has demonstrated that deep learning models and fusion approaches can improve face liveness detection. For example, a 2023 study using multiple deep neural networks reported improved performance through model fusion and achieved high classification accuracy on established face datasets.

2.6 Fingerprint Biometric Authentication

Fingerprint authentication identifies individuals using the unique ridge patterns present on their fingers. Fingerprint systems are widely used because fingerprints are relatively distinctive and can be captured using compact sensors.

However, fingerprints are also vulnerable to presentation attacks. An attacker may attempt to create an artificial fingerprint that resembles the fingerprint of an authorized user.

Research on fingerprint PAD has therefore investigated spatial and temporal information, sensor characteristics, pressure variations, and machine learning techniques. Studies have demonstrated that analysing temporal information from fingerprint acquisition can assist presentation attack detection.

2.7 Machine Learning for Liveness Classification

Machine learning provides a suitable approach for automated liveness classification because it can learn patterns that differentiate genuine and fraudulent biometric samples.
Possible classification algorithms include:

- Logistic Regression
- Decision Trees
- Random Forest
- Support Vector Machine
- Artificial Neural Networks
- Convolutional Neural Networks

Traditional machine learning approaches may use manually extracted features such as texture, colour, edge information, or image statistics. Deep learning approaches can learn relevant representations automatically from images or video sequences.
The choice of algorithm depends on the available dataset, computational resources, required accuracy, and application environment.

2.8 Evaluation of Biometric Authentication Systems

A biometric authentication system should be evaluated using appropriate performance and security metrics.
Important metrics include:
False Acceptance Rate (FAR): The proportion of unauthorized authentication attempts incorrectly accepted as genuine.
False Rejection Rate (FRR): The proportion of genuine authentication attempts incorrectly rejected.
Accuracy: The proportion of correctly classified authentication or liveness samples.
Precision: The proportion of samples classified as positive that are actually positive.
Recall: The proportion of actual positive samples correctly identified.
F1-score: The harmonic mean of precision and recall.
For presentation attack detection, additional metrics are important. APCER represents the proportion of attack presentations incorrectly classified as bona fide presentations, while BPCER represents the proportion of genuine presentations incorrectly classified as attacks. These metrics are widely used in biometric presentation attack evaluation.

3. Methodology

This section describes the procedures and technical processes adopted for designing and evaluating the Liveness Detection and Biometric Authentication System. The methodology covers data acquisition, preprocessing, biometric enrollment, liveness detection, biometric matching, authentication decision, and system evaluation.

3.1 Research Design

This study adopts a quantitative experimental research design. The experimental approach is appropriate because the proposed system must be implemented, tested, and evaluated using biometric samples representing both genuine users and presentation attacks.
The research process follows a structured workflow:

1. Biometric data acquisition

2. User enrollment
3. Data preprocessing
4. Feature extraction
5. Liveness detection
6. Biometric matching
7. Authentication decision
8. Performance evaluation
9. Analysis of experimental results

The experimental design allows the proposed system to be evaluated under controlled conditions and provides a basis for comparing genuine authentication attempts with simulated spoofing attempts.

3.2 Data Sources and Data Collection

The research may use publicly available biometric datasets and controlled samples collected for experimental purposes. The dataset should contain genuine biometric samples and appropriate presentation-attack samples.

For a facial authentication implementation, the dataset may contain:

- Genuine facial images
- Genuine facial video sequences
- Printed photograph attacks
- Screen replay attacks
- Different lighting conditions
- Different facial poses
- Different facial expressions

Where fingerprint authentication is used, the dataset may contain genuine fingerprint samples and artificial or spoofed fingerprint samples.

The collection process should comply with applicable privacy and ethical requirements. Personally identifiable information should not be unnecessarily retained, and biometric templates should be protected against unauthorized access.

3.3 Description of Dataset

The dataset consists of biometric samples divided into two major categories:

Genuine/Bona Fide Samples

These are biometric samples captured from real users who are physically present during the authentication process.

Examples include:

- Live facial images
- Live facial video
- Genuine fingerprints
- Genuine iris images

Presentation Attack Samples

These represent attempts to deceive the authentication system.

Examples include:

- Printed photographs

- Replay videos
- Mobile-screen photographs
- Artificial fingerprints
- Masks or other facial replicas

The target variable for the liveness classifier is defined as:

1 = Live/Bona Fide
0 = Spoof/Presentation Attack
The dataset may be divided into training and testing subsets, such as an 80:20 ratio, depending on the dataset size and experimental requirements.

3.4 Data Preprocessing
Biometric data may contain noise, inconsistent image quality, background information, variations in illumination, and differences in scale or orientation. Preprocessing is therefore required before feature extraction and classification.

The following preprocessing operations are considered:
1. Image Resizing
Biometric images are resized to a consistent resolution to provide uniform input to the classification model.

2. Face Detection
For facial authentication, the system identifies the face region and separates it from irrelevant background information.

3. Image Normalization
Pixel values are normalized to reduce differences caused by variations in image intensity and lighting.

4. Noise Reduction
Image-processing techniques may be applied to reduce unnecessary noise and improve biometric feature quality.

5. Data Augmentation
Where appropriate, image augmentation techniques such as controlled rotation, scaling, cropping, and brightness adjustment may be used to increase training diversity.

6. Dataset Splitting
The dataset is divided into training and testing groups. Cross-validation may also be applied to assess model stability.

3.5 Biometric Enrollment
Enrollment is the process through which an authorized user's biometric characteristics are initially registered in the system.
During enrollment:

1. The user provides identification information.
2. The biometric sensor captures the user's biometric sample.
3. The system performs preprocessing.
4. The system extracts biometric features.
5. A biometric template is generated.
6. The template is securely stored.
7. The user becomes available for subsequent authentication.

The system should avoid unnecessarily storing raw biometric images where a protected biometric template can be used instead.

3.6 Liveness Detection Process

The liveness detection component serves as the first security layer during authentication.
The process follows these stages:

1. The user initiates authentication.
2. The camera or biometric sensor captures the sample.
3. The system preprocesses the sample.
4. Relevant liveness features are extracted.
5. The liveness classifier determines whether the sample is live or spoofed.
6. If the sample is classified as spoofed, authentication is rejected.
7. If the sample is classified as live, the system proceeds to biometric matching.

This architecture prevents the biometric matching component from unnecessarily processing samples that have already been identified as presentation attacks.

3.7 Biometric Feature Extraction

Feature extraction converts raw biometric information into a representation suitable for authentication.
For facial authentication, features may include:

- Facial landmarks
- Eye characteristics
- Nose and mouth geometry
- Texture information
- Facial embeddings
- Spatial relationships
- Temporal movement characteristics

For fingerprint authentication, features may include:

- Ridge patterns
- Minutiae points
- Ridge endings
- Bifurcations
- Orientation information

The selected features should provide sufficient discriminatory information while reducing unnecessary computational requirements.

3.8 Machine Learning Algorithms Implemented

To evaluate the effectiveness of the proposed liveness detection approach, multiple machine learning algorithms may be implemented.

3.8.1 Logistic Regression

Logistic Regression can serve as a baseline classification model. It estimates the probability that a biometric sample belongs to the live or spoof class.

Its major advantage is simplicity and interpretability. However, its performance may be limited where the relationship between biometric features and liveness is highly nonlinear.

3.8.2 Decision Tree

Decision Tree classification divides biometric samples using feature-based decision rules.

The model is easy to interpret and can provide understandable classification paths. However, uncontrolled decision trees may overfit training data.

3.8.3 Random Forest

Random Forest combines multiple decision trees to produce a more robust classification model.

The ensemble approach can reduce overfitting and improve generalization. Random Forest can also provide feature-importance information that helps researchers understand which features contribute strongly to liveness classification.

3.8.4 Support Vector Machine

Support Vector Machine identifies a decision boundary that separates live and spoof biometric samples. Kernel functions can allow the model to handle nonlinear relationships. SVM can be useful for relatively small or medium-sized datasets, although appropriate parameter tuning is required.

3.8.5 Convolutional Neural Network

A Convolutional Neural Network can automatically learn spatial features from biometric images.

For facial liveness detection, CNNs can learn patterns associated with genuine skin texture, image artifacts, illumination, screen reflections, and other characteristics that distinguish real faces from presentation attacks.

3.9 Authentication Decision Process

The proposed authentication process contains two major security stages:

Stage One – Liveness Verification

The system determines whether the captured biometric belongs to a live person.

Stage Two – Biometric Verification

If the sample passes the liveness check, the system compares the biometric features with the enrolled template.

The final decision can therefore be represented as:

Biometric Sample → Liveness Detection → Live? → Biometric Matching → Match? → Authentication Granted

If either the liveness test or biometric matching fails, access is denied.

This two-stage architecture strengthens authentication because similarity to an enrolled biometric template alone is not sufficient for access.

3.10 System Security

Security mechanisms are incorporated into the system to protect biometric information and authentication operations.

These include:

- Secure storage of biometric templates
- Password protection for administrative accounts
- Role-based access control
- Encryption of sensitive information
- Session management
- Authentication attempt limits
- Audit logging
- Secure communication
- Protection against unauthorized database access

Biometric data require special protection because compromised biometric characteristics cannot be changed as easily as passwords.

3.11 Evaluation Metrics

The performance of the system is evaluated using the following metrics:

Accuracy

Accuracy measures the proportion of correctly classified samples.

Precision

Precision measures the proportion of samples classified as genuine that are actually genuine.

Recall

Recall measures the ability of the classifier to correctly identify genuine samples.

F1-Score

F1-score provides a combined measure of precision and recall.

False Acceptance Rate

FAR measures the rate at which unauthorized users are incorrectly accepted.

False Rejection Rate

FRR measures the rate at which legitimate users are incorrectly rejected.

APCER

Attack Presentation Classification Error Rate measures attack samples that are incorrectly classified as genuine.

BPCER

Bona Fide Presentation Classification Error Rate measures genuine samples that are incorrectly classified as attacks.

These metrics provide a more complete assessment of both authentication accuracy and anti-spoofing performance.

4. Discussion of Findings

The proposed research demonstrates that combining liveness detection with biometric authentication provides a stronger authentication framework than biometric matching alone.

A biometric authentication system that only compares a captured face or fingerprint with a stored template may accept an attacker if the attacker can successfully reproduce the biometric characteristics of an authorized user. Liveness detection introduces an additional security layer by determining whether the biometric presentation is genuine.

The expected performance of the system is influenced by the quality of the biometric data, the type of presentation attacks represented in the training data, the selected machine learning algorithm, and the environmental conditions under which authentication takes place.

Traditional classification algorithms such as Logistic Regression and Decision Trees can provide useful baseline results. Their major advantages include simplicity, relatively low computational requirements, and interpretability. However, their performance may be limited when biometric data contain highly complex nonlinear patterns. Random Forest can provide stronger robustness by combining multiple decision trees. Its ensemble structure can reduce the impact of individual decision errors and provide useful feature-importance information. Support Vector Machine can also provide effective classification where the feature space is complex. However, performance depends on appropriate selection of kernel functions and hyperparameters.

Deep learning approaches, particularly CNN-based methods, have considerable potential because they can learn complex spatial representations directly from biometric images. Recent research has shown strong performance from deep-learning-based face anti-spoofing approaches.

Another important finding is that the type of presentation attack affects liveness detection performance. A system trained primarily using printed photographs may perform poorly against replay videos, masks, or newer forms of synthetic biometric attacks. Consequently, a robust system should be evaluated against multiple attack categories.

The research also highlights the importance of evaluation using standardized PAD metrics. A high overall classification accuracy alone does not necessarily mean that a biometric system is secure. For example, a system could have high accuracy while still incorrectly accepting a significant proportion of presentation attacks. APCER and BPCER therefore provide valuable information about the security-performance trade-off. Recent NIST evaluation work has specifically assessed passive software-based facial PAD algorithms operating on conventional 2D imagery and different presentation attack instruments, demonstrating the continuing importance of systematic evaluation of liveness technologies. The study further establishes that liveness detection should not be treated as a replacement for biometric matching. Rather, it should complement biometric authentication. Liveness detection determines whether the presentation is genuine, while biometric matching determines whether the genuine biometric belongs to the enrolled user.

Therefore, the combination of both processes creates a more complete authentication architecture.

5. Summary of Findings

The major findings of the study can be summarized as follows:

1. Biometric authentication provides a convenient approach to user verification but remains vulnerable to presentation attacks.
2. Liveness detection provides an additional security layer capable of identifying potentially fraudulent biometric presentations.
3. Combining liveness detection with biometric matching provides stronger protection than

relying on biometric matching alone.
4. Machine learning algorithms can be applied to classify biometric samples into live and spoof categories.
5. Deep learning approaches are particularly promising for facial anti-spoofing because they can learn complex visual patterns from biometric data.
6. The effectiveness of a liveness detection system depends significantly on the quality and diversity of the training dataset.
7. A system trained against only one type of spoofing attack may not adequately detect new or previously unseen attack techniques.
8. Performance metrics such as FAR, FRR, APCER, BPCER, precision, recall, and F1-score provide a more comprehensive evaluation of biometric authentication security.
9. Secure biometric-template storage and appropriate access controls are necessary to protect users from the consequences of biometric data compromise.
10. Liveness detection and biometric matching should operate together as complementary components of a secure biometric authentication system.

6. Conclusion

This research examined the design and implementation of a Liveness Detection and Biometric Authentication System designed to improve the security of biometric-based authentication. The study established that although biometric authentication offers significant advantages over traditional password-based authentication, biometric systems can be vulnerable to presentation attacks. The research therefore proposed the integration of liveness detection with biometric verification. The liveness component determines whether the captured biometric sample originates from a genuine live person, while the biometric matching component determines whether the genuine biometric belongs to an enrolled user. The study also examined different liveness detection approaches, including challenge-response mechanisms, texture analysis, motion analysis, depth-based techniques, and machine learning-based classification. Machine learning and deep learning techniques provide promising approaches for identifying complex differences between genuine biometric samples and presentation attacks. The research further established that evaluating a biometric system requires more than measuring general classification accuracy. Metrics such as false acceptance rate, false rejection rate, APCER, and BPCER are important for determining whether the system provides adequate protection against unauthorized access. In conclusion, integrating liveness detection into biometric authentication can significantly strengthen the security of authentication systems. Such systems can be applied in mobile-device security, institutional access control, attendance management, financial services, healthcare systems, examination platforms, and other applications requiring reliable identity verification. Nevertheless, continued research is necessary because presentation attacks continue to evolve, particularly with the increasing availability of sophisticated digital manipulation and synthetic media technologies.

7. Recommendations

Based on the findings of this study, the following recommendations are proposed:
1. **Integration of Liveness Detection:** Organizations implementing biometric authentication should integrate liveness or presentation attack detection mechanisms rather than relying solely on biometric matching.

2. **Use of Multiple Anti-Spoofing Techniques:**
Future biometric systems should combine different liveness signals such as facial movement, texture, image quality, depth, and challenge-response mechanisms where appropriate.
3. **Continuous Model Updating:**
Machine learning models should be periodically updated using new and emerging presentation-attack samples to improve their ability to detect previously unseen attacks.
4. **Improved Dataset Diversity:**
Researchers should use diverse biometric datasets containing different lighting conditions, devices, demographic characteristics, environmental conditions, and presentation attack types.
5. **Standardized Performance Evaluation:**
Future biometric systems should be evaluated using recognized biometric and PAD metrics such as APCER, BPCER, FAR, and FRR rather than relying only on overall accuracy.
6. **Protection of Biometric Templates:**
Organizations should implement strong security mechanisms for storing biometric templates because biometric characteristics are difficult to replace once compromised.
7. **Multi-Factor Authentication:**
Biometric authentication should, where appropriate, be combined with another authentication factor such as a secure device, token, or authentication secret. Current NIST guidance places important restrictions on biometric-only authentication and emphasizes additional authentication factors and presentation-attack resistance.

RJMCIT

References

George, A., & Marcel, S. (2023). Deep learning for face anti-spoofing: A survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 45*(5), 5609–5631.

Husseis, A. H. A., Liu-Jimenez, J., & Sanchez-Reillo, R. (2021). Fingerprint presentation attack detection utilizing spatio-temporal features. *Sensors, 21*(6), 2059.

Important correction

Lee, Y. K., Jeong, J., & Kang, D. (2022). An effective orchestration for fingerprint presentation attack detection. *Electronics, 11*(16), 2515.

Mohzary, M., Almalki, K. J., Choi, B. Y., & Song, S. (2023). Apple in my eyes (AIME): Liveness detection for mobile security using corneal specular reflections. *IEEE Internet of Things Journal, 10*(4), 3356–3367.

Ngan, M. L., Grother, P. J., & Hom, A. (2023). *Face analysis technology evaluation (FATE) part 10: Performance of passive, software-based presentation attack detection (PAD) algorithms* (NIST Interagency/Internal Report 8491). National Institute of Standards and Technology.

There is a duplication in the list above: George and Marcel (2023) should not be included as a separate reference for *Deep Learning for Face Anti-Spoofing: A Survey*. The verified authors of that paper are:

Therefore, the correct final reference is:

Yu, Z., Qin, Y., Li, X., Zhao, C., Lei, Z., & Zhao, G. (2023). Deep learning for face anti-spoofing: A survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 45*(5), 5609–5631.

Yu, Z., Qin, Y., Li, X., Zhao, C., Lei, Z., & Zhao, G. (2023). Deep learning for face anti-spoofing: A survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 45*(5), 5609–5631.

Yu, Zitong; Qin, Yunxiao; Li, Xiaobai; Zhao, Chenxu; Lei, Zhen; and Zhao, Guoying.