

State of the Art on Facial Recognition and Liveness Detection Technologies

YAKOUBI Kahina

*Department of Electrical Engineering and
Industrial Computing
National Higher School of Advanced Technologies
Algiers, Algeria
k_yakoubi@ensta.edu.dz*

BOUZEGZEG Amine

*Three S PAY
Algiers, Algeria
amine.bouzegzeg@3s-pay.com*

LABIOD Wissam

*Department of Electrical Engineering and
Industrial Computing
National Higher School of Advanced Technologies
Algiers, Algeria
w_labiod@ensta.edu.dz*

CHOUAF Seloua

*Department of Electrical Engineering and
Industrial Computing
National Higher School of Advanced Technologies
Algiers, Algeria
seloua.chouaf@ensta.edu.dz*

Abstract—Facial recognition has become a crucial technology in biometric authentication systems, but it remains vulnerable to spoofing attempts, such as using fake photos or videos. As a result, liveness detection plays an important role differentiating genuine users from fraudulent ones. This work provides a state-of-the-art review of the main technologies in facial recognition and liveness detection. It first discuss recent deep learning-based advances in facial recognition, particularly those involving angular margin losses and embedding networks. Then, we analyze liveness detection approaches, distinguishing between passive methods (based on image analysis) and active methods (based on user interaction). This study examines their performance, benefits, limitations, and the latest trends and challenges in biometric security.

Index Terms—Facial Recognition, Liveness Detection, Biometric Security, Deep Learning, Artificial Intelligence

I. INTRODUCTION

Recent advancements in biometric authentication systems have positioned facial recognition as one of the most prominent modalities, primarily due to its non-intrusive nature and the convenience it offers to end users. Its integration into applications such as mobile security, border control, and digital identity verification has underscored its practical importance. Nevertheless, despite its widespread adoption, facial recognition systems remain vulnerable to various security threats, particularly spoofing attacks involving the use of photographs, videos, or three-dimensional masks.

To address these threats, liveness detection has become a critical component of modern biometric systems. Liveness detection techniques are designed to ascertain whether the presented biometric sample originates from a live individual physically present at the point of capture, thus preventing the use of fake faces or photos. These techniques can be broadly classified into passive methods, which infer liveness from intrinsic image characteristics, and active methods, which

involve explicit user interaction—for example, asking the user to blink, smile, or turn their head during verification.

This study aims to present a comprehensive review of state-of-the-art technologies in facial recognition and liveness detection. We systematically examine recent methodological advances, analyze the advantages and limitations of prevailing approaches, and identify emerging research trends. Furthermore, we highlight the key challenges that must be addressed to enhance the robustness and reliability of facial biometric systems against sophisticated spoofing attempts.

Unlike existing reviews that often examine facial recognition and liveness detection independently, this work jointly analyzes both domains, emphasizing their interdependencies, comparative challenges, and future integration opportunities.

II. FACIAL RECOGNITION

Facial recognition is a biometric technology that identifies or verifies a person's identity based on its facial features. It works by analyzing an image or a video of a face, extracting key characteristics (like the distance between the eyes, shape of the nose, and contours of the jawline), and comparing them to a stored data for authentication (face verification 1:1) or identification (face identification 1:N). [1].

A. Principles of Facial Recognition

Facial recognition technology has rapidly evolved in recent years due to advances in deep learning and computer vision [2]. Modern facial recognition systems comprise several critical steps—such as face detection, alignment, feature extraction, and matching—that collectively enable accurate identity analysis. This process is illustrated in Figure 1, which outlines the typical pipeline of a facial recognition system, from input image to final verification.

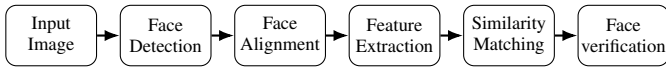


Figure 1. Pipeline of Facial Recognition.

1) **Face Detection:** Face detection is the preliminary step in any facial recognition pipeline. It involves identifying and localizing facial regions within an image or a video frame.

- **Classical Face Detection Algorithms:** Several models have been developed for face detection, including:

- 1) **Local Binary Patterns:** LBP is a texture descriptor that labels pixels of an image by thresholding the neighborhood of each pixel and considering the result as a binary number [3].
- 2) **Viola–Jones Algorithm:** Introduced in 2001, it utilizes Haar-like features and a cascade of classifiers for rapid face detection [4].
- 3) **Histogram of Oriented Gradients (HOG):** This method captures edge or gradient structures that are characteristic of local shape, often combined with Support Vector Machines (SVM) for classification [3].

- **Modern Deep Learning-Based Methods:** Leveraging large datasets and neural networks, these methods have significantly improved face detection accuracy:

- 1) **Multi-task Cascaded Convolutional Neural Networks:** MTCNN is a three-stage deep learning framework that performs face detection and facial landmark alignment simultaneously as shown in the figure below. It processes images in a coarse-to-fine manner, enhancing accuracy and enabling real-time performance even under challenging conditions like varying poses and lighting. [5].
- 2) **RetinaFace:** It is a single-stage face detector that achieves pixel-level face localization by leveraging both extra-supervised and self-supervised multi-task learning. It detects faces across various scales and predicts five facial landmarks, making it robust for real-world applications, as illustrated in the figure 3. [6].
- 3) **You Only Look Once and Variants:** YOLO is a real-time object detection system that treats face detection as a general object detection task. It processes entire images in a single neural network evaluation, enabling high-speed and accurate detections. YOLO's efficiency makes it suitable for applications requiring real-time face detection. [7].

To better contextualize the evolution of face detection techniques, Table I summarizes this methods across different generations, highlighting their main characteristics, years of introduction, and reported performance metrics.

2) **Face Alignment:** Face alignment involves detecting key facial landmarks—such as the eyes, nose, and mouth corners—and applying geometric transformations to align these

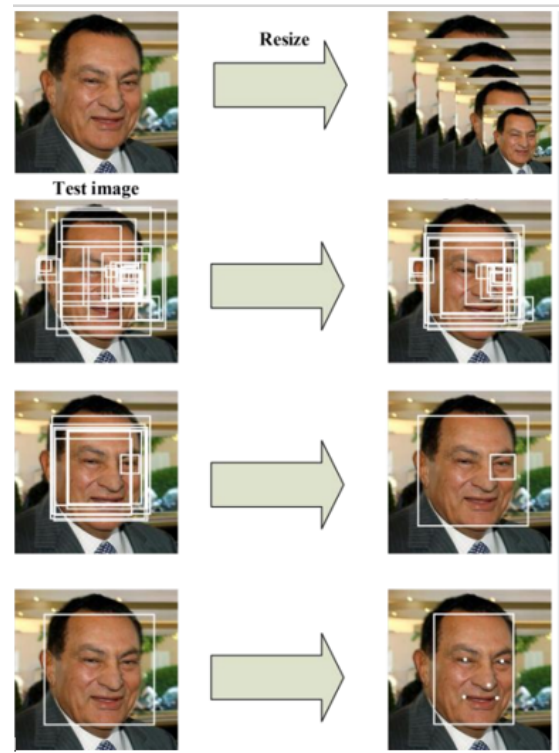


Figure 2. Pipeline of three-stage deep learning framework [5].

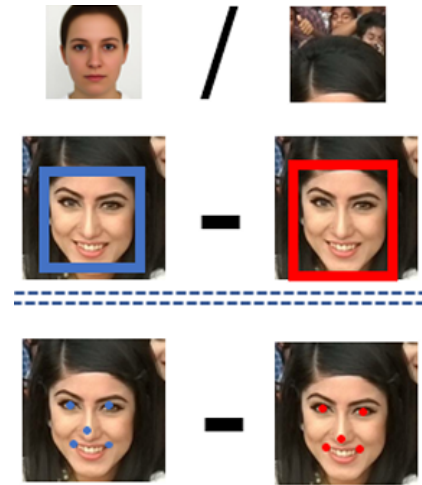


Figure 3. RetinaFace Architecture [6]

features to predefined positions [10]. The primary objectives are to:

- Rotate the face so that the eyes are horizontally aligned [10].
- Scale the face to a standard size [11].
- Translate the face to center it within the frame [11].

Techniques for face alignment have evolved over time, encompassing both classical methods and modern deep learning approaches.

Table I
COMPARATIVE OVERVIEW OF FACE DETECTION TECHNIQUES

Method	Year	Approach	Notable Performance Metrics and Features
LBP	1994	Texture-based	Efficient for texture classification; robust to lighting variations in face detection tasks.
Viola-Jones	2001	Haar features + Cascade	Achieved a detection rate of 95% with a false positive rate of 1 in 14,084 on the MIT+CMU dataset [8].
HOG + SVM	2005	Gradient-based	Effective for pedestrian detection; extended to faces with detection rates of 42% and false positives of 2.9–3.5% on CMU test subsets [9].
MTCNN	2016	Deep Learning	Real-time detection and alignment with high accuracy; suitable for facial landmark localization.
RetinaFace	2019	Deep Learning	Achieved 91.4% Average Precision on the WIDER FACE hard set, surpassing prior methods by 1.1% [6].
YOLO5Face	2021	Deep Learning	Achieved state-of-the-art performance on the WIDER FACE dataset: 96.9% (Easy), 96.0% (Medium), 91.6% (Hard) subsets [7].

- **Classical Face Alignment Techniques:** Classical methods rely on statistical models and handcrafted features to detect and align facial landmarks:

- 1) **Active Shape Models:** ASM are statistical models that fit object shapes to images by aligning key landmarks, constrained by a Point Distribution Model (PDM) learned from training data. Commonly used in traditional applications like photo editing, ASMs help automatically correct facial orientation. [12].
- 2) **Active Appearance Models:** build on ASM by combining shape and texture to better capture facial variations. They align faces by minimizing differences between the model and the input image, making them effective for enhancing recognition accuracy in biometric authentication. [12].
- 3) **Constrained Local Models:** CLM detect facial landmarks by combining local texture detectors with a global shape model that maintains consistency across all landmarks. This method is especially useful in video surveillance for stable, continuous facial landmark tracking [13].

- **Modern Deep Learning-Based Face Alignment Techniques:** Deep learning has revolutionized face alignment, enabling precise and robust facial landmark detection across diverse conditions. Key methodologies include:

- 1) **Convolutional Neural Networks:** CNNs are found

dational in facial landmark detection due to their ability to learn hierarchical feature representations from raw image data. Their layered architecture captures both low-level features (like edges) and high-level abstractions (such as facial structures), ensuring robustness against variations in lighting, pose, and occlusion [14].

Several architectures have been introduced, including:

- **Deep Alignment Network (DAN):** Employs a multi-stage CNN where each stage refines the landmark predictions of the previous one. Unlike methods focusing on local patches, DAN processes entire face images at all stages, enhancing robustness to large pose variations and challenging initializations [15].

- **Stacked Hourglass Networks:** Utilize an encoder-decoder architecture that captures both local and global contextual information. Multiple hourglass modules are stacked to repeatedly process and refine heatmaps, leading to improved accuracy in landmark localization [16].

- 2) **3D Face Alignment:** 3D face alignment techniques reconstruct a three-dimensional facial model, accommodating variations in head pose and facial expressions more effectively than 2D approaches. By capturing the geometry of the face, these methods provide more accurate alignment, particularly in scenarios with significant pose changes [17].

The following models exemplify some approaches to 3D facial alignment:

- **Position Map Regression Network (PRNet):** An end-to-end method that directly regresses the 3D facial structure and dense alignment from a single image, bypassing traditional 3D Morphable Model fitting. [18].

- **DeepFace:** Employs a nine-layer neural network with over 120 million parameters to perform 3D alignment and frontalization, enhancing face recognition accuracy under varying poses [19].

- 3) **Multi-Stage and Cascaded Networks:** These networks progressively refine facial landmark predictions through multiple stages or cascades. Each stage uses the output of the previous one as input, iteratively improving accuracy. This step-wise refinement helps correct initial errors and results in highly precise alignment [20].

Some of the most prominent architectures proposed for this purpose include the following:

- **DeCaFA (Deep Convolutional Cascade for Face Alignment):** An end-to-end deep convolutional cascade architecture that uses fully-convolutional stages to maintain full spatial resolution throughout the cascade. DeCaFA employs chained transfer layers with spatial softmax to

produce landmark-wise attention maps, facilitating progressive refinement [21].

- **Pose-Invariant Face Alignment with a Single CNN:** Introduces a visualization layer that can be integrated into the CNN architecture, enabling joint optimization with different loss functions. This approach allows for end-to-end training and reduces the training time compared to traditional cascaded CNNs [22].

3) **Feature Extraction:** Feature extraction is a pivotal phase in facial recognition systems, aiming to derive meaningful representations from facial images. Early methods predominantly utilized linear techniques:

- **Classical Feature Extraction Techniques**

- 1) **Principal Component Analysis:** PCA is a statistical technique that reduces the dimensionality of facial image data by identifying the directions (principal components) that capture the most variance in the dataset. In face recognition, this approach, known as the Eigenfaces method, simplifies the data while retaining the most critical information, facilitating efficient and accurate recognition. [24].
- 2) **Linear Discriminant Analysis:** LDA, also known as the Fisherfaces method in face recognition, seeks to find the linear combinations of features that best separate different classes (identities). Unlike PCA, which focuses on capturing variance, LDA emphasizes maximizing class separability, making it effective for distinguishing between individuals. [25].

- **Modern Deep Learning-Based Feature Extraction Techniques:** Facial feature extraction has evolved with the adoption of deep learning methods.

- 1) **Deep Metric Learning:** It is a technique in machine learning that focuses on learning an embedding space where semantically similar inputs are mapped close together, and dissimilar ones are positioned far apart. In the context of face recognition, DML enables models to distinguish between different identities by learning such embeddings from facial images [26].
- 2) **Transfer Learning with Pre-trained Models:** Transfer Learning involves leveraging models pre-trained on large datasets, such as ImageNet, to perform feature extraction on new tasks. This approach is particularly beneficial when labeled data is scarce, as it allows for effective feature extraction without extensive training from scratch. [27]. Several well-known deep learning models have been proposed and widely adopted for facial feature extraction, including:

- **VGGFace:** It consists of 16 layers and was trained on a large dataset of over 2 million celebrity images. The model can be fine-tuned for

specific facial recognition applications, leveraging its robust feature extraction capabilities [28].

- **ResNet50:** A deep residual network comprising 50 layers pre-trained on ImageNet, often used for feature extraction and fine-tuning in various image recognition tasks [29].

4) **Similarity matching:** The goal is to compare extracted facial features to determine if two faces belong to the same individual. This process involves measuring the similarity between feature vectors obtained from facial images.

- **Classical Similarity Matching Techniques:** Classical methods primarily rely on mathematical and statistical measures to compare facial features.

- 1) **Euclidean Distance:** Calculates the straight-line distance between two feature vectors. It's simple and effective when features are well-aligned and normalized [30]. It is often used in constrained environments such as employee check-in systems, where pose and lighting variations are minimal.
- 2) **Cosine Similarity:** Measures the cosine of the angle between two vectors, focusing on their orientation rather than magnitude. This method is particularly useful when the magnitude of the vectors is not informative [30]. It is common in mobile device authentication, where lighting and scale may vary, but relative feature orientation remains consistent.

- **Modern Similarity Matching Techniques:** Instead of relying on predefined distance metrics, learned similarity functions train models to determine the similarity between facial features. This is achieved by optimizing the model to output higher similarity scores for matching pairs and lower scores for non-matching pairs [31].

- **Siamese Networks:** These networks consist of twin subnetworks that process two input images to produce comparable feature vectors. The network is trained using contrastive loss, which encourages the feature vectors of similar images to be close and those of dissimilar images to be distant.
- **Triplet Loss:** This method involves training the model on triplets of images: an anchor, a positive example (same identity as the anchor), and a negative example (different identity). The objective is to ensure that the distance between the anchor and positive is less than the distance between the anchor and negative by a specified margin.

5) **Face verification:** It is the process of confirming that a person's claimed identity matches their actual identity by comparing their facial features to a previously stored image or biometric template.

- **Classical Face verification Techniques:** Several traditional machine learning algorithms have been widely used in face recognition before the advent of deep learning methods.

- 1) **Support Vector Machines:** SVMs aim to identify a hyperplane that best separates data points of

different classes by maximizing the margin between them. This approach is particularly effective in high-dimensional spaces, which is common in face recognition due to the complexity of facial features [32].

- 2) **K-Nearest Neighbors(k-NN):** It classifies a facial image by identifying the 'k' closest matches in a feature space and assigning the most common label among them. This method is particularly effective when dealing with well-separated classes and smaller datasets [33].

• Modern Face verification Techniques

- 1) **FaceNet** is a facial recognition system developed by Google that maps face images to a 128-dimensional Euclidean space, where distances directly correspond to face similarity. It uses a deep convolutional neural network trained with a triplet loss function to optimize the embedding space, enabling efficient face verification and clustering [34].
- 2) **ArcFace** is a deep learning-based face recognition model that introduces an additive angular margin loss function to enhance the discriminative power of the network. This approach improves the model's ability to distinguish between different identities by maximizing the angular distance between classes in the feature space [35].
- 3) **AdaFace** introduces an adaptive angular margin loss function, adjusting the margin based on the image quality. This approach enhances the model's ability to distinguish between different identities by emphasizing hard examples in high-quality images and down-weighting unidentifiable low-quality samples. By leveraging feature norms as a proxy for image quality, AdaFace improves recognition performance across datasets with varying image qualities [36].

The following table presents a comparative overview of key face recognition techniques, including both classical and deep learning-based approaches, along with the benchmark datasets they were evaluated on and their reported accuracies.

Table II
FACE RECOGNITION TECHNIQUES AND BENCHMARK PERFORMANCE

Technique	Benchmark Dataset(s)	Reported Accuracy
SVM	FERET	~85–90% (with PCA/LDA) [32]
k-NN	ORL Face Database	~90% (on small datasets) [33]
FaceNet	LFW, YouTube Faces	99.63% (LFW), 95.12% (YTF) [34]
ArcFace	LFW, MegaFace, IJB-B	99.83% (LFW), SOTA on others [35]
AdaFace	LFW, MegaFace, IJB-B	99.80% [36]

B. Limitations of Face Recognition Systems

Despite advancements, face recognition systems are susceptible to several spoofing techniques:

- 1) **Presentation Attacks:** Attackers may use photographs, videos, or masks to impersonate legitimate users [37].
- 2) **Deepfakes:** Sophisticated AI-generated videos can mimic a person's facial movements and expressions, deceiving recognition systems [38].
- 3) **3D Masks:** High-quality 3D masks can replicate facial features, making it challenging for systems to distinguish between real and fake faces [39].

These limitations highlight the need for additional security measures to ensure the authenticity of the user.

III. LIVENESS DETECTION

Liveness detection is a security feature in biometric systems that verifies whether the presented biometric data—such as a facial image—is from a live person physically present at the time of capture, rather than from a fake representation like a photo, video, or mask [40].

A. Principles of Liveness Detection

Liveness detection methods are generally categorized into two types:

- 1) **Active Liveness Detection:** This approach requires user interaction to verify liveness. The system prompts the user to perform specific actions, such as [41]:

- Blinking
- Smiling
- Turning the head
- Speaking certain words

These actions help the system determine that it is interacting with a live person.

- 2) **Passive Liveness Detection:** This method does not require any action from the user. Instead, it analyzes the captured image or video for signs of liveness, such as [41]:

- Skin texture and micro-movements
- Reflections in the eyes
- Depth information

Advanced algorithms assess these factors to determine if the subject is a live person.

The table below presents a comparison between active and passive liveness detection techniques:

- **Classical Liveness Detection Techniques:** Traditional liveness detection techniques primarily focus on observable physical and behavioral cues to distinguish between live subjects and spoofing attempts. These methods include:

- 1) **Texture Analysis:** By examining the fine details of skin texture—like pores, wrinkles, and natural imperfections—systems can differentiate between real skin and synthetic materials or printed images [43]. Commonly used techniques include:

- **Local Phase Quantization (LPQ):** Focuses on capturing fine-grained texture details by analyzing the phase information of local image regions.

Table III
COMPARISON BETWEEN ACTIVE AND PASSIVE LIVENESS DETECTION
[41]

Aspects	Active Liveness Detection	Passive Liveness Detection
User Action	Required (e.g., blink, smile, turn head)	Not required
Verity	High if the user cooperates	High, but can be tricked in some cases
User Experience	Sometimes inconvenient	Seamless and fast
Spoof Attack Resistance	Strong against printed attacks	Strong with advanced models
Deployment Complexity	Moderate	Low
Common Use Cases	High-security banking, KYC	Mobile apps, smooth onboarding

It's often robust to blurring and useful for texture classification [42].

- **Gray-Level Co-occurrence Matrix (GLCM):** Uses statistical approaches by computing how often pairs of pixel intensities (gray levels) occur together at a certain spatial relationship, extracting features like contrast, correlation, energy, and homogeneity [44].

2) **3D Depth Sensing:** Utilizing specialized hardware like structured light or time-of-flight sensors, this method captures depth information to create a three-dimensional map of the subject's face. This depth data helps distinguish between a live person and a flat image or mask [45].

3) **Vital Sign Detection:** Some systems analyze physiological signals such as pulse, blood flow, or pupil dilation in response to light changes [46]. For instance, iris recognition systems may monitor pupil reactions to verify liveness.

• **Modern and Advanced Liveness Detection Techniques:** The integration of deep learning has significantly advanced liveness detection, enabling systems to move beyond hand-crafted features and leverage powerful neural network-based approaches. Modern techniques integrate sophisticated architectures, multi-task learning, and attention mechanisms for robust and real-time spoof detection.

1) **Convolutional Neural Networks:** CNNs have replaced traditional feature engineering by automatically learning hierarchical feature representations from raw input data. These models are trained end-to-end, allowing optimal feature extraction and classification [47].

- **ResNet:** Incorporates residual connections to enable the training of very deep networks by mitigating vanishing gradient issues [48].
- **DenseNet:** Features dense connectivity between layers, promoting feature reuse and improving gradient flow [49].

- **EfficientNet:** Scales network width, depth, and resolution in a balanced way for improved accuracy and efficiency [50].

2) **Auxiliary Supervision Methods:** To enhance discrimination between live and spoofed faces, modern systems often incorporate auxiliary tasks that provide richer supervisory signals during training [51]:

- **Depth Map Estimation:** Predicts facial depth to differentiate between flat 2D presentation attacks and real 3D faces.
- **Binary Mask Generation:** Segments the image into genuine and spoofed regions at the pixel level for fine-grained supervision.
- **Remote Photoplethysmography (rPPG):** Extracts physiological signals such as heart rate from subtle variations in skin tone, which are absent in spoofed media.

3) **Advanced architectures:** Advanced architectures have emerged that integrate domain-specific enhancements and attention mechanisms for superior performance:

- **Central Difference Convolutional Network (CDCN):** Introduces the Central Difference Convolution (CDC) operator, which captures both intensity and gradient-based features, enhancing robustness to common spoofing artifacts [52].
- **CDCN++ with Neural Architecture Search (NAS):** Builds on CDCN by using NAS to automatically discover optimal architectures. Includes a Multiscale Attention Fusion Module (MAFM) for better integration of multi-scale features [52].

B. Limitations of Liveness Detection Systems

Liveness detection is a crucial component in biometric security systems, designed to distinguish between genuine biometric traits and spoofed artifacts. Despite its significance, several limitations and challenges affect its efficacy and widespread adoption.

- 1) **Adaptation to Evolving Spoofing Techniques:** As fraudsters develop more sophisticated methods, such as high-resolution 3D masks and deepfake videos, liveness detection systems must continuously evolve to counter these advanced threats [53].
- 2) **Cross-Dataset Generalization Challenges:** Liveness detection models often struggle to maintain accuracy across different datasets, especially when trained on limited or non-diverse data. This limitation affects the system's robustness in real-world scenarios [54].
- 3) **Susceptibility to Environmental Factors:** External conditions, such as lighting variations and camera quality, can impact the performance of liveness detection systems, leading to inconsistent results [55].

IV. PERFORMANCE ANALYSIS AND REMAINING CHALLENGES

This section analyzes the performance of facial recognition and liveness detection systems, highlighting key metrics and discussing challenges that impact their robustness, fairness, and real-world applicability.

A. Facial Recognition

Facial recognition systems have become integral to modern biometric authentication. This subsection outlines how their performance is evaluated, focusing on commonly used accuracy metrics.

1) **Performance Metrics** : Facial recognition systems are assessed using several key metrics:

- **False Acceptance Rate (FAR):** The probability that the system incorrectly matches an input to a non-matching template in the database [56].
- **False Rejection Rate (FRR):** The probability that the system fails to match an input to a matching template in the database [57].
- **Equal Error Rate (EER):** The point at which FAR and FRR are equal; a lower EER indicates higher accuracy [58].

2) **Ethical Considerations:** The deployment of facial recognition technology raises several ethical concerns:

- **Privacy Invasion:** Unauthorized surveillance and data collection can infringe on individual privacy rights [59].
- **Bias and Discrimination:** Studies have shown that facial recognition systems can exhibit higher error rates for certain demographic groups, leading to potential discrimination [60].
- **Data Security:** Storing and handling biometric data pose significant security risks if not managed properly [61].

B. Liveness Detection

Liveness detection systems play a vital role in differentiating between real users and spoofing attempts. This subsection discusses key evaluation metrics used to assess their effectiveness and explores ethical considerations related to their deployment.

1) **Performance Metrics:** Liveness detection systems, which aim to distinguish between live users and spoofing attempts, utilize specific metrics:

- **Attack Presentation Classification Error Rate (APCER):** The rate at which spoof attempts are incorrectly classified as genuine [62].
- **Bona Fide Presentation Classification Error Rate (BPCER):** The rate at which genuine attempts are incorrectly classified as spoof attempts [62].
- **Average Classification Error Rate (ACER):** The average of APCER and BPCER, providing an overall error rate [63].
- **Spoofing Success Rate (SSR):** The percentage of spoofing attempts that successfully bypass the liveness detection system.

2) **Ethical Considerations:** While liveness detection enhances security, it also presents ethical challenges:

- **User Consent:** Users should be informed and consent to the collection and processing of their biometric data [64].
- **Accessibility:** Ensuring that liveness detection systems are accessible to individuals with disabilities is essential.
- **Potential for Misuse:** Like facial recognition, liveness detection can be misused for unauthorized surveillance or data collection [65].

V. CONCLUSION

Facial recognition and liveness detection technologies have evolved considerably, driven by advances in deep learning architectures, auxiliary task integration, and domain generalization strategies. These systems now demonstrate remarkable accuracy, robustness, and processing speed, enabling their deployment across a wide range of practical applications including security and access control, biometric payment systems, healthcare, and smart surveillance.

However, several persistent challenges remain. Issues such as demographic bias, lack of generalization to unseen scenarios, and vulnerability to presentation and adversarial attacks continue to pose significant risks. Additionally, the limited availability of accessible and diverse benchmark datasets (especially free or affordable ones) hinders the ability of researchers to reliably evaluate and compare new models. This restriction slows down community-wide progress and makes replicability more difficult without significant investment.

Furthermore, the emergence of generative adversarial networks and deepfake technologies introduces new security threats, necessitating the development of sophisticated detection and mitigation strategies.

Future research must prioritize:

- The development of fair and unbiased biometric systems capable of ensuring equitable performance across diverse populations.
- Improved generalization techniques, including advanced domain adaptation and domain generalization frameworks, to enhance robustness in real-world scenarios.
- The design of resilient architectures resistant to adversarial and synthetic attacks, leveraging multi-modal biometrics and advanced liveness detection strategies.
- Strengthening privacy protections through secure data handling, federated learning, and compliance with emerging biometric regulations.

Overall, ensuring the secure, ethical, and responsible deployment of biometric technologies requires continuous innovation, interdisciplinary collaboration, and proactive regulatory engagement.

REFERENCES

- [1] Robert Urpis, *Facial Recognition Technology Explained* Teracom Solutions Pty Ltd, <https://www.teracom-solutions.com/reports/facial-recognition.pdf>.
- [2] X. Wang, J. Peng, S. Zhang, B. Chen, Y. Wang, et Y. Guo, "A Survey of Face Recognition," *arXiv:2212.13038*, pre-publication, december 26, 2022, <https://arxiv.org/abs/2212.13038>.

- [3] Innovetrics, *Face Detection* Innovetrics Glossary, <https://www.innovetrics.com/glossary/face-detection>.
- [4] D. M. Abdulhussien et L. J. Saud, "An evaluation study of face detection by Viola-Jones algorithm," *International Journal of Health Sciences*, vol. 6, no. S8, 2022, pp. 4174–4182.
- [5] K. Zhang, Z. Zhang, Z. Li, et Y. Qiao, *Joint Face Detection and Alignment using Multi-task Cascaded Convolutional Networks*, pre-publication arXiv:1604.02878, april 10, 2016, <https://arxiv.org/abs/1604.02878>.
- [6] J. Deng, J. Guo, Y. Zhou, J. Yu, I. Kotsia et S. Zafeiriou, *RetinaFace: Single-stage Dense Face Localisation in the Wild*, pre-publication arXiv:1905.00641v1, may 2, 2019, <https://arxiv.org/abs/1905.00641>.
- [7] D. Qi, W. Tan, Q. Yao, et J. Liu, *YOLO5Face: Why Reinventing a Face Detector*, pre-publication arXiv:2105.12931v3, january 27, 2022, <https://arxiv.org/abs/2105.12931>.
- [8] P. Viola et M. Jones, "Rapid object detection using a boosted cascade of simple features," in *Proceedings of CVPR*, 2001, pp. 511–518.
- [9] Stanford University, "Study of Viola-Jones Real Time Face Detector," CS231A Course Project Report, 2016.
- [10] E. Onaran, E. Sarıtaş, et H. K. Ekenel, *Impact of Face Alignment on Face Image Quality*, pre-publication arXiv:2412.11779, december 16, 2024, <https://arxiv.org/abs/2412.11779>.
- [11] A. Rosebrock, *Face Alignment with OpenCV and Python*, PyImageSearch blog, <https://www.pyimagesearch.com/2017/04/03/face-alignment-opencv-python/>.
- [12] W. Zhao, R. Chellappa, P. J. Phillips et A. Rosenfeld, *Face Recognition: A Literature Survey*, *ACM Computing Surveys*, vol. 35, no. 4, pp. 399–458, 2003.
- [13] N. Hamzah, F. H. K. Zaman et N. M. Tahir, *A Mini-review of Face Alignment – Classical Method versus Deep Learning Approach*, *Journal of Electrical and Electronic Systems Research*, vol. 19, 2021, p. 7.
- [14] Saiwa, *Facial Landmarks Detection: Unveiling Power Applications*, Saiwa Blog, february 8, 2025, <https://www.saiwa.com/blog/facial-landmarks-detection>.
- [15] M. Kowalski, J. Naruniec et T. Trzcinski, *Deep Alignment Network: A Convolutional Neural Network for Robust Face Alignment*, *CVPR Workshops*, 2017, pp. 2034–2043.
- [16] A. Newell, K. Yang et J. Deng, *Stacked Hourglass Networks for Human Pose Estimation*, pre-publication arXiv:1603.06937, march 22, 2016, <https://arxiv.org/abs/1603.06937>.
- [17] X. Zhu, Z. Lei, X. Liu, H. Shi et S. Z. Li, *Face Alignment Across Large Poses: A 3D Solution*, in *Proceedings of CVPR*, pp. 146–155, 2016.
- [18] Y. Feng, F. Wu, X. Shao, Y. Wang et X. Zhou, *Joint 3D Face Reconstruction and Dense Alignment with Position Map Regression Network*, pre-publication arXiv:1803.07835, march 21, 2018, <https://arxiv.org/abs/1803.07835>.
- [19] GGANBU Marketplace, *DeepFace: Unraveling the Power of Facial Recognition Technology*, GGANBU Marketplace blog, 2025, <https://marketplace.gganbu.com/deepface-power-facial-recognition>.
- [20] A. Author, B. Author, et C. Author, *Face Recognition using PCA and LDA on 3D Facial Images*, *Journal of Physics: Conference Series*, vol. 1237, no. 3, p. 032048, 2019.
- [21] A. Dapogny, K. Bailly et M. Cord, *DeCaFA: Deep Convolutional Cascade for Face Alignment In The Wild*, pre-publication arXiv:1904.02549, april 9, 2019, <https://arxiv.org/abs/1904.02549>.
- [22] A. Jourabloo, M. Ye, X. Liu et L. Ren, *Pose-Invariant Face Alignment with a Single CNN*, pre-publication arXiv:1707.06286, july 20, 2017, <https://arxiv.org/abs/1707.06286>.
- [23] F. Schroff, D. Kalenichenko et J. Philbin, *FaceNet: A Unified Embedding for Face Recognition and Clustering*, pre-publication arXiv:1503.03832, march 26, 2015, <https://arxiv.org/abs/1503.03832>.
- [24] F. Jalled, *Face Recognition Machine Vision System Using Eigenfaces*, pre-publication arXiv:1705.02782, may 8, 2017, <https://arxiv.org/abs/1705.02782>.
- [25] S. Lee, *Exploring Linear Discriminant Analysis (LDA) in Data Science*, Number Analytics Blog, march 13, 2025, <https://numberanalytics.com/exploring-lda/>.
- [26] Z. Fu, Y. Li, Z. Mao et al., "Deep Metric Learning with Self-Supervised Ranking," in *AAAI-21*, 2021.
- [27] Iguazio, *What Is Transfer Learning in Machine Learning?*, Iguazio Glossary, 2025, <https://www.iguazio.com/glossary/transfer-learning/>.
- [28] A. Malhotra, *Working with VGG16 Dataset*, Medium post, january 28, 2024, <https://medium.com/@ashishmalhotra/vgg16-dataset-123456>.
- [29] Nicolas, *ResNet 50: a pre-trained model for image recognition*, Innovatica Blog, august 17, 2024, <https://innovatica.com/resnet-50-pretrained-image-recognition>.
- [30] Michael W., *Similarity Measures in Data Science: Euclidean distance Cosine similarity*, LinkedIn post, 2022, https://www.linkedin.com/posts/michaelw_similarity-measures-data-science.
- [31] N. Chen, *Similarity Learning in Machine Learning*, AI Odyssey (Medium), november 27, 2023, <https://medium.com/ai-odyssey/similarity-learning-abcdef>.
- [32] Bluechip Technologies Asia, *Support Vector Machines (SVM)*, LinkedIn post, may 3, 2024, https://www.linkedin.com/posts/bluechip-tech_svm.
- [33] O. Happiness, *Performing Face Recognition using KNN*, She Code Africa Blog, may 8, 2023, <https://shecodeafrica.org/blog/knn-face-recognition>.
- [34] Anonyme, *FaceNet Key Points*, Scribd document, 2025, <https://www.scribd.com/document/facenet-key-points>.
- [35] J. Deng, J. Guo, N. Xue et S. Zafeiriou, *ArcFace: Additive Angular Margin Loss for Deep Face Recognition*, *CVPR*, 2019, pp. 4690–4699.
- [36] M. Kim, A. K. Jain et X. Liu, *AdaFace: Quality Adaptive Margin for Face Recognition*, *CVPR* 2023.
- [37] Veridas, *Beyond the Deepfake: 14 Types of Presentation Attacks (PA)*, Veridas Blog, 2022, <https://www.veridas.com/blog/presentation-attacks>.
- [38] SEON, *What Is a Deepfake – How Do Deepfakes Work?*, SEON Dictionary, 2025, <https://dictionary.seon.io/deepfake>.
- [39] P. C. Yuen, *3D Mask Face Anti-Spoofing*, presentation, Université baptiste de Hong Kong, 2019.
- [40] Innovetrics, *Liveness Detection* [Glossaire], Innovetrics Glossary, 2025, <https://www.innovetrics.com/glossary/liveness-detection>.
- [41] H. Akiode, *Active vs. Passive Liveness Detection: Guide...*, You-verify Blog, 7 octobre 2024, <https://www.youverify.com/blog/liveness-detection-guide>.
- [42] J. Heikkilä et V. Ojansivu, *Methods for Local Phase Quantization in Blur-Insensitive Image Analysis*, in *Proceedings of ICIAR*, 2009.
- [43] Aware, Inc., *Liveness Detection: Enhancing Security with Biometrics*, blog, septembre 14 2023, <https://aware.com/blog/liveness-detection>.
- [44] E. Gomede, *Gray-Level Co-Occurrence Matrix (GLCM): A Comprehensive Analysis*, Medium post, february 19, 2024, <https://medium.com/aimonks/g lcm-comprehensive-analysis>.
- [45] VIAVI Solutions, *3D Sensing*, business article, 2025, <https://www.viavisolutions.com/en-us/resources/articles/3d-sensing>.
- [46] Recognito, *How Face Recognition Liveness Detection Works*, blog, 2025, <https://recognito.com/blog/face-liveness-detection>.
- [47] S. Suman et N. Salimath, "Face Liveness Detection: A Comprehensive Study on Techniques and Applications," *Journal of Neonatal Surgery*, vol. 14, no. 18s, pp. 939–947, 2025.
- [48] M. Negi, "Residual Connections in Deep Neural Networks," Medium post, 1 décembre 2024, <https://medium.com/@manishnegi/residual-connections-dnn>.
- [49] E. Gomede, "DenseNet: Densely Connected Convolutional Neural Networks," Python in Plain English (Medium), 3 octobre 2023, <https://medium.com/python-in-plain-english/densenet-cn...>
- [50] T. Karmakar, "Introduction to EfficientNet," Kaggle post, 2025, <https://www.kaggle.com/code/tapendu/efficientnet-intro>.
- [51] Y. Liu, A. Jourabloo et X. Liu, "Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision," pre-publication arXiv:1803.11097, 26 mars 2018, <https://arxiv.org/abs/1803.11097>.
- [52] Z. Yu et al., "Searching Central Difference Convolutional Networks for Face Anti-Spoofing," in *Proceedings of the CVPR*, 2020, pp. 5295–5305.
- [53] T. Stankovic, *Liveness Detection: A Complete Guide for Fraud Prevention and Compliance in 2025*, SumsuB Blog, may 21, 2025, <https://sumsub.com/blog/liveness-detection-guide>.
- [54] O. Kuznetsov et al., *Cross-Database Liveness Detection: Insights from Comparative Biometric Analysis*, Actes de l'atelier SCIA 2023, vol. 3608, pp. 250–263, 2023.
- [55] KBY-AI, *Most Powerful Face Liveness Detection – Face Anti-Spoofing Version 1.0*, blog, septembre 17, 2023, <https://kby-ai.com/blog/most-powerful-face-liveness-detection>.
- [56] Facia, *What is the False Acceptance Rate (FAR) in Facial Recognition?*, Facia Knowledge Base, 2025, <https://facia.ai/kb/far-facial-recognition>.
- [57] Recogtech, *FAR and FRR: security level versus ease of use*, Recogtech Insights, 2025, <https://recogtech.com/insights/far-frr-security>.

- [58] Facia, *Knowing the Equal Error Rate (EER) in Biometrics*, Facia Knowledge Base, 2023, <https://facia.ai/kb/eer-biometrics>.
- [59] Flashcards World, *Flashcard Set: f3ad9bb2-dd01-45b5-8414-223bf594f34a*, <https://www.flashcardsworld.com/set/f3ad9bb2-dd01-45b5-8414-223bf594f34a>.
- [60] DataGuard Insights, *The Growing Data Privacy Concerns with AI: What You Need to Know*, DataGuard, 2024, <https://www.dataguardinsights.com/ai-data-privacy>.
- [61] Identity Management Institute, *Biometric Authentication: Benefits and Risks*, <https://www.identitymanagementinstitute.org/biometric-authentication>.
- [62] M. Gomez-Barrero, *Presentation Attack Detection and Unknown Attacks*, presentation IFPC/NIST, 2020.
- [63] ID R&D, *Biometric Authentication: Definitions, FAQs, and Concepts*, <https://idrnd.com/biometrics-faqs>.
- [64] GDPR Register, *Biometric Data and GDPR: Key Considerations*, article réglementaire, 19 janvier 2025, <https://gdprregister.eu/biometric-data-key-considerations>.
- [65] T. Myers, *Ethical Implications of Biometric Face Recognition Systems*, Facia.ai Insights, 2023, <https://facia.ai/blog/ethical-biometric-face-recognition>.