Vol.3, No.6, Page 1452- 1459, 2025 https://doi.org/10.59628/jast.v3i6.2286 ISSN 2958-9568 JAST

SUN PUBLISHER

مجلة جامعة صنعاء للعلوم التطبيقية والتكنولوجيا

Sana'a University Journal of Applied Sciences and Technology

https://journals.su.edu.ye/index.php/jast/

From Algorithms to Applications: A Review of AI-Based Face Recognition and Identity Verification

Rusul Hussein Hasan [1]*, Rasha Majid Hassoon[2] and Inaam Salman Aboud[3]

[1]**College of Law, University of Baghdad, Baghdad, Iraq,**
[2]**College of Physical Education and Sports Sciences for Women, University of Baghdad, Baghdad, Iraq,**
[3]**College of Education, Al- Mustansiriya University, Baghdad, Iraq**

*Corresponding author: russl@colaw.uobaghdad.edu.iq

Abstract

Face recognition and identity verification are now critical components of current security and verification technology. The main objective of this review is to identify the most important deep learning techniques that have contributed to the improvement in the accuracy and reliability of facial recognition systems, as well as highlighting existing problems and potential future research areas.

An extensive literature review was conducted with the assistance of leading scientific databases such as IEEE Xplore, ScienceDirect, and SpringerLink and covered studies from the period 2015 to 2024. The studies of interest were related to the application of deep neural networks, i.e., CNN, Siamese, and Transformer-based models, in face recognition and identity verification systems.

Deep learning-based approaches have been shown through cross-sectional studies to improve recognition accuracy under diverse environmental and demographic conditions. Anti-counterfeiting (Anti-Spoofing) and real presence detection features integrated into systems have likewise enhanced system security against advanced attacks such as 3D masks, false images and videos, and Deepfake technology.

Future trends point to the need to develop deep, multi-sensory and interpretable learning models, and adopt learning strategies based on limited data, while adhering to legal and ethical frameworks to ensure fairness and transparency.

Article Info

Keywords:
Face Recognition, , Identity Verification, Deep Learning, Anti-Spoofing, Biometric Authentication.

Article History:
Received: 26-September-2025,
Revised: 24-October-2025,
Accepted: 5-November-2025,
Available online: 28 December 2025.

1. INTRODUCTION

In recent decades, the world has witnessed rapid development in facial recognition and identification verification technologies to the extent that they are currently among the most important and widespread applications of artificial intelligence in various industries. Facial recognition refers to the identification or differentiation of an individual's identity from facial features, whereas identity verification refers to the comparison of the current facial image with a stored image in the past to confirm the personality of the individual. Face recognition and identity verification have been part of verification and security systems in the last few years. This review aims to analyze and combine the development of artificial intelligence technologies, deep learning methods, and their groundbreaking impact on face identification and identity authentication procedures [1, 2].

The major objective of this review is to identify the leading deep learning-based approaches that have achieved remarkable work towards improving the accuracy and robustness of facial recognition systems and highlight ongoing trends and research directions.

A systematic review of the scientific literature was carried out in major science databases such as IEEE Xplore, ScienceDirect, and SpringerLink, and research conducted between 2015 and 2024 was considered. The research works chosen were those that involved apply-

ing deep neural networks such as CNN, Siamese, and Transformer-based networks for face recognition and identity verification mechanisms.[3]

Cross-sectional research has shown that deep-learning-based approaches have significantly improved recognition performance under different environmental and demographic conditions. The addition of anti-counterfeiting (anti-spoofing) and real presence detection (Liveness Detection) techniques has also increased the security of systems against advanced attacks such as 3D masks, synthetic images and videos, and Deepfake technology. Changes in appearance, demographic bias, privacy protection, and practicability in daily applications remain challenges. [4, 5]

Directions for the future show the need to create detailed, multi-modal, and explainable learning models, and adopt learning procedures based on small datasets, all of which are in accordance with legal and ethical standards towards promoting fairness and explainability. Ongoing R&D in this field is a major step towards attaining more secure, trustworthy, and efficient systems in real time, with immense application areas in the fields of digital services, banking systems, and access control systems. [6, 7]

2. LITERATURE REVIEW

These systems use algorithms to analyze facial traits and create a facial template for comparison with a database of known faces. Advances in machine learning and computer vision have improved the accuracy of face recognition technology. [1]

This paper underscores the pressing need for comprehensive regulation and responsible use of this system. The emergence of AI-generated faces and their increasing realism present new challenges, particularly for identity verification processes. The societal implications of these developments are beneficial and risky. [8]

This article summarizes the application of deep learning technology in the field of face recognition over the past decade and introduces the technologies and their development involved in the above four modules. [9].

This study delves into the challenges of accurately identifying faces under various conditions and disguises, emphasizing its significance in security systems and sensitive sectors such as banking. [10]

This study focuses on the recognition of human faces. One stage of recognizing a face is to determine how the eyes, nose, and mouth are placed in the facial structure [6].

This paper presents the results of a thorough comparison between previously established systems, noting caveats in their pathways and underlining the new data types (diversity) yields in terms of recognition performance. [11]

3. ARTIFICIAL INTELLIGENCE TECHNOLOGIES USED

Artificial intelligence technologies, specifically deep learning, hold secret for the qualitative transformation of facial recognition and identity verification systems. Based on a thorough review of previous literature, the most common and widespread techniques were selected based on two straightforward criteria: [12]

(1) Level of accreditation in research and practical applications in recent years
(2) Achieving a balance between accuracy and speed under various conditions.

3.1. Machine Learning Techniques

Before deep learning, face recognition systems used traditional machine learning methods, such as key component analysis, linear discrimination analysis, and vector machine support. Principal Component Analysis: Was method is used to extract facial image discriminant features and project them onto low-dimensional space to improve computational efficiency. Linear Discriminant Analysis: Enables discrimination between classes to be improved by maximizing the variance among different faces and minimizing the variance within a single class. Support vector machine: Effective for classification of small or low-light faces. Although these methods are simple, their use is limited to complex data and nonlinear variables such as changing light, angles, or expressions. [13]

3.2. Deep Learning Techniques

Deep learning is the main driver of the modern generation of facial recognition systems. The following are the most prominent models and structures used, justifying their selection.

- **Deep Neural Networks** They (DNNs) represent the basis of most modern systems because of their ability to extract high-level features directly from raw images, without the need for manual feature design. [14]
- **Bypass Networks** It widely used because of their ability to process spatial patterns in images. It is used in many advanced systems such as VGG-Face, ResNet and FaceNet which have shown high accuracy in huge databases. [15]
- **Twin Networks** It relies on comparing two images to calculate their similarity, and is commonly used to verify binary identity (Pairwise Matching [16]
- **Transformer-based Models** It brought about a paradigm shift due to the self-attention mechanism (Self-Attention) that enables contextual relationships between facial parts to be represented more accurately, such as the ViT-Face and Face Transformer [17].

- **Advanced Models** Angle margin losses (Angular Margin Losses) are used to increase class discrimination and have become the gold standard in many recent studies [18].

3.3. Learning Algorithms and Loss Functions

- Softmax Loss.
- Angular Margin Loss (ArcFace, CosFace).
- Contrastive Loss. [13]

3.4. Facial Preprocessing

Because of its importance in improving the accuracy and stability of systems, pre-processing is an essential stage in any facial recognition system. Includes:

- Detection: Determine facial position using algorithms such as MTCNN or RetinaFace.
- Data Expansion: Generate additional samples by rotating, changing lighting, or adding noise to improve the model generalization.
- Alignment: Rotate and adjust the face according to the location of the eyes or keypoints to reduce the effect of the angles.
- Normalization: Standardize size, lighting, and pixel distribution to ensure consistency.

This phase is important for enhancing the performance of systems. [19]

4. METHODOLOGY

This study adopted a structured methodological approach and a rigorous methodological approach to ensure comprehensive and unbiased coverage of the scientific literature related to facial recognition and identity verification techniques using artificial intelligence. The review was carried out in four main stages: identification, sorting, validity verification, and inclusion. As shown in Figure 1

4.1. Research design

A systematic literature review (Systematic Literature Review – SLR) approach was taken with the aim of providing an objective scientific view of the development of deep learning techniques used in facial recognition and identity verification systems. The methodology focused on achieving transparency, repeatability, and academic rigor in analyzing studies published from 2015 to 2024 and identifying key research trends and challenges.

4.2. Data sources

A comprehensive search was conducted in reliable scientific databases including IEEE Xplore, ScienceDirect, SpringerLink, and MDPI. Secondary sources were also used from conferences, universities, and journals specializing in artificial intelligence, computer vision, and biometric systems for identity verification.

4.3. Research strategy

A combination of precise keywords with logical operators (AND and OR) was used to narrow the search and ensure the comprehensiveness of the results. The most prominent words used were as follows.

"Face Recognition," "Identity Verification," "Deep Learning," "CNN," "Transformer," "Siamese Network," "Anti-Spoofing," "Biometric Authentication."

4.4. Inclusion and exclusion criteria

A set of criteria for selecting appropriate studies has been identified as follows:

Inclusion criteria:

1. Peer-reviewed research published in scientific journals or conferences has addressed the use of deep learning in facial recognition and identity verification systems.
2. Studies that included experimental evaluations or comparisons using approved data sets and measurement criteria.
3. Publications issued between 2015–2024 and written in English.

Exclusion criteria:

1. Studies that are not peer-reviewed or published in languages other than English.
2. Research that focused on other biometric methods (such as fingerprint or iris).
3. Studies that are duplicate or lack sufficient experimental data.

4.5. Data extraction and analysis

Each selected study was analyzed according to a set of standardized criteria that included:

Model structure and techniques used (e.g., CNN, Transformer, Siamese), type of datasets or benchmarks used (e.g., LFW, VGGFace2, IJB-C), and evaluation metrics, such as accuracy (accuracy), false acceptance rate (FAR), false rejection rate (FRR), and equal error rate (EER).

5. EXPERIMENTAL STANDARDS AND ENVIRONMENTS

The utility of facial recognition and identity verification systems is not a function of databases or benchmarks but is highly a function of a set of actual and scientifi-

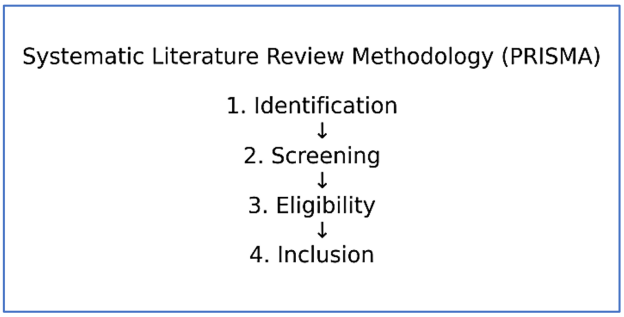

Figure 1. Methodology

cally accepted measures of testing, which are used to determine how well a system verifies identity based on different conditions.

Databases and Benchmarks are aid tools designed to validate models in harmonized environments to enable a fair comparison among competing systems. By combining performance measures with standard experimental environments, a general appraisal can be obtained, covering three prevailing axes: experiment methodology, data quality, and output accuracy. [20]

5.1. Standard Databases

Databases are one of the cornerstones for developing and evaluating facial recognition systems, as the quality and diversity of data directly affect the efficiency of trained models. Databases are divided into three main categories:

- Training databases: Similar to CASIA-WebFace and VGGFace2, it is used to train deep networks on millions of images that are diverse in terms of illumination, age, and capture angle.
- Test databases, Such as IJB-C and MegaFace, are standard references for evaluating a system's ability to recognize difficult conditions, such as different positions or the presence of imperfect lighting.
- Anti-counterfeiting databases, Such as CASIA-FASD and Replay-Attack, are used to evaluate the ability of models to distinguish between real and fake faces via printed images or 3D masks [8, 9].

These rules are chosen based on their diversity and realistic representation, allowing fair testing of model performance in real-world situations and reducing data bias, which is one of the most prominent challenges of contemporary systems.

5.2. Evaluation Protocols and Experiments

The evaluation process was based on standard experimental protocols that ensured an accurate comparison between the models. The most important of these protocols are as follows:

Verification: Testing the system's ability to determine whether two photos belong to the same person.

- Identification: Testing the system's ability to identify an individual within a large group and is divided into two types:
  - The closed domain: where all identities are located within the database.
  - Open domain: where previously unknown identities may appear.
- Anti-counterfeiting tests: Special protocols are used to evaluate the system's ability to detect fake images or videos before they are accepted as valid identities.

These experiments were performed in standardized environments using standard datasets to ensure a fair comparison between different algorithms. [20, 21]

5.3. Evaluation Metrics

To measure performance, a set of statistical measures adopted in the research community was used, most notably:

- Accuracy: The ratio of correctly classified samples to total samples.
- False Acceptance Rate: The percentage of cases in which a system accepts a fake identity.
- False Reject Rate: The percentage of cases in which the system rejected the correct identity.
- Equal Error Rate: The point at which the FAR and FRR ratios are equal and is a general measure of system quality. [22]

5.4. Practical Applications

Face recognition and identity verification technologies have been the most noticeable achievements of digital transformation as they have been widely integrated into daily services and smart infrastructure. Among the most apparent modern applications are

- Unlocked smart devices: This technology allows phones, computers, and payment transactions to be locked without the use of conventional passwords, offering greater security and convenience for consumers.
- Electronic Identity Verification in Banking: Facial technologies in banking are applied in streamlining account opening procedures and establishing electronic payments as well as reducing fraud and improving customer experience without the necessity of visiting branches.

5.5. Access Control Systems

Facial recognition technologies have been adopted as a hygienic alternative to access cards or passwords in

institutions, airports, government buildings, and even prisons and labs because they are contactless (contactless), which is healthier and more effective, especially post-COVID-19 pandemic. It can also be combined with other technologies, such as fingerprinting or voice recognition, for added security with multi-factor authentication [23].

5.6. Internet Services and Digital Verification

Facial identity verification has been one of the most prominent digital authentication solutions since the expansion of electronic services. For example, users can authenticate themselves when registering on government websites, when conducting business transactions online, or even on social media to avoid fake accounts. Video or file authentication is increasingly being used as a secure and immediate way to remotely confirm an identity. [24]

6. ANTI-SPOOFING AND LIVE ATTENDANCE VERIFICATION

As facial recognition systems have evolved and spread into sensitive security and commercial applications, new challenges have emerged in the form of spoofing attacks (Spoofing Attacks), where an attacker attempts to trick the system using alternative media to the face of a legitimate person. For this reason, the importance of live presence verification (Liveness Detection) techniques that aim to distinguish between a real face and fake media has emerged.

6.1. Types of Counterfeiting Attacks

- Static Images: Display a paper or digital photo of the account holder in front of the camera.
- Replay Attacks: Play a pre-recorded video on a screen in front of the system.
- 3D Masks: Use a mask that resembles real facial features to trick the system.
- Mannequins / Dolls: trying to simulate the face by physical means.
- Advanced Replay: Merge digitally modified images or clips to hide traces of counterfeiting.

6.2. Counterfeit Detection Techniques

- Motion Analysis: The study of patterns of movement of the head or eyes, where real facial movements differ from the images or videos shown.
- Head Pose & Tilt: Test the facial response to changing angles and gestures.
- Perspective Distortion: Analysis of visual distortions resulting from the projection of images or videos onto a two-dimensional surface.
- Depth Cues: Depth cameras or 3D technologies for detecting the presence of a true dimension of the face.
- Deep Learning-based Anti-Spoofing: Training CNN and Transformer networks to distinguish between real and fake images using subtle attributes, such as skin texture or light reflections.

7. ISSUES AND CHALLENGES

Despite significant advances in, AI-based facial recognition and identity verification are vital applications that are widely used in smartphones, banking, security, and digital services. However, challenges such as appearance change, bias, counterfeiting, and privacy remain. Future trends include multimodal sensing, low data learning, explainable AI, and ethical compliance. [17, 25–27]

7.1. Variations in Appearance

Changes in appearance are one of the most difficult challenges facing facial recognition systems and include the following:

- Various facial expressions like, smiling, frowning, or sudden expressions.
- Age and age, as aging greatly affects facial features.
- Hairstyles and accessories, such as glasses or hijabs, may hide parts of the face.
- Lighting and environmental conditions, where changing lighting or shadows causes the representation of the face in the image to differ.
- Capture angles (Pose), capturing the face from different angles, reduce the recognition accuracy.
- Noise and distortion (noise) in images are caused by the camera or data compression.

7.2. Demographic Bias

- Studies have shown that the performance of facial recognition systems varies depending on demographic characteristics, such as race, gender, and skin color, which may lead to the following:
- Higher accuracy in some categories compared to others.
- Frequent errors in identifying people from certain population groups raise ethical and legal concerns.

7.3. Privacy and Security

- Protection of facial biometric data is necessary, as its leak or breach would be an invasion of the privacy of users.
- ivacy laws, restricts the collection, storage, and use of facial data.
- The biggest challenge is finding a balance between system effectiveness and commitment to privacy, es-

pecially in the implementation of these technologies in public spaces or on the internet.

7.4. Challenges to Real-World Deployment

- Bad or cut the Internet in some places reduces the effectiveness of systems that rely on cloud processing.
- The quality of the cameras and sensors directly affects the recognition accuracy.
- The expense of computing and processing, particularly in the case of millions of images or videos in real-time.
- Real-time response of the system is required by applications such as security and surveillance, and this is another challenge for big and complicated systems.

7.5. Deepfake and Spoofing Attacks

- The development of deep fake technology has created a challenge in identifying real and fake photos and videos.
- Constant evolution of counterfeiting equipment renders anti-counterfeiting progressively more difficult, requiring more sophisticated anti-spoofing methods and increasingly advanced Liveness Detection models.

8. RECENT REVIEWS AND STUDIES

Facial recognition and identification verification using artificial intelligence has been a subject of global interest in research over the last decade, with the majority of studies focusing on model development, metrics, challenges, and real-life applications. The following are the most impactful studies and reviews in this field. By reviewing the recent studies presented in this paper, a clear discrepancy can be observed in the objectives, methods, and experimental environments used in facial recognition and identity verification systems.

Wang and Deng's study [28] focused on the deep theoretical aspects of deep learning models, particularly the development of angular loss functions (Angular Margin Losses) such as ArcFace and CosFace to improve class discrimination, raising the level of accuracy in different lighting conditions. As for the study of Ahlawat et al. [15] it focused on the applied aspect, demonstrating the effectiveness of bypass networks (CNNs) in building an automated recognition system based on facial characteristics only without the need for manually designed features.

On the other hand, the study by Kortli et al. [29] A comprehensive comparison between traditional and deep recognition systems showed that deep learning systems outperform, especially when using large datasets such as VGGFace2 and LFW, but they pointed out the problem of performance bias based on gender or skin color, which was later confirmed by Fola-Rose et al. [8], who focused on the ethical dimensions of these systems and the need to adopt standards of transparency and interpretation of decisions (Explainable AI).

As for the study of Abdul-Al et al. [10] It was distinguished by highlighting multimedia systems that combine face and sound, with the use of generative networks (GANs) to detect fake or digitally modified faces, which represents an advanced step in the fight against deepfakes (Deepfake).

In comparison, the study by Das et al. focused on. [6] On classical models such as front-fed neural networks (GFFANN) have shortcomings in the face of complex data and lighting changes, which justifies the gradual shift towards deep models and modern structures such as Transformer-based Models addressed by Yu et al. [14] in a study that focused on improving identity verification through deep learning-based programs.

The study by Chen et al. is also discussed. [18] The performance of deep networks in conditions of camouflage or angle change has shown that modern models excel in resisting these factors because of the ability of the self-attention mechanism (Self-Attention) to analyze the spatial context of the face.

Finally, Kajotra and Kaur [11] indicated that the results of the systems vary significantly depending on the type of data used and evaluation methods, which underscores the need to adopt standardized testing environments to ensure fair comparison between different models.

It is clear from this comparison that previous studies are divided between technical trends aimed at improving accuracy and performance and security and ethical trends that focus on resisting counterfeiting and ensuring privacy.

1. Deep Face Recognition: A Survey – Wang & Deng. The study considers central developments in Deep Neural Networks (deep neural networks) and cutting-edge loss function technologies such as Triplet Loss and Angular Margin Loss. The study highlights problems with respect to varying scene conditions, such as lighting, facial expressions, capture angles, age, and how to improve spatial representations of the face by means of deep learning. [28]
2. A Survey of Face Recognition Techniques with Deep Learning – Darsee & Roy Press–a recent survey correlates face recognition methods with various industrial uses, including smartphones, banking, security, and surveillance. The study indicates the difference between traditional architectures, such as CNNs, and the novel Transformer and Siamese Network-based architectures. Liveness Detection and anti-counterfeiting are key aspects for ensuring the security of real-world applications. [15, 30]
3. Face Recognition Systems: A Survey – MDPI: This study considers real-world working face recognition

systems with a focus on the advantages and limitations of operating environments. This study depicts the impacts of appearance and demographic variations on system accuracy, privacy, and security concerns. The discussion provides comparative data across different datasets, such as LFW, IJB-C, and VGGFace, and performance metrics, such as FAR, FRR, and EER. [29]

4. Elements of End-to-end Deep Face Recognition: A Survey of Recent Advances, It focused on end-to-end systems and deals with three major phases: detection, alignment, and representation.

This study surveys recent developments in facial preprocessing techniques and deep learning approaches, including state-of-the-art neural networks. [6]

9. FUTURE DIRECTIONS

As facial recognition and identity verification technology continues to advance, exciting trends have the potential to chart the direction of this field technologically, ethically, and organizationally.

9.1. Improve Resistance to Counterfeiting and Difficult Environments

We focus on developing advanced anti-spoofing models that can handle fake images and videos, 3D masks, and cut or hidden faces.

Improve the ability to perform in true-world scenarios, such as non-uniform illumination, complex backgrounds, and rapid facial movement.

9.2. Explainable AI

There is a need to build models whose decisions are explainable, that is, the means of knowing why a particular identity is accepted or rejected.

9.3. Bare minimum data Learning and Unsupervised Learning

Existing research is trending towards few-shot learning and self-supervised/unsupervised learning to reduce reliance on large datasets that can be expensive or difficult to obtain. Such models facilitate rapid learning of new faces and better performance in low-data or diverse setups.

10. CONCLUSION

Facial recognition and AI-powered identity authentication programs are likely the most far-reaching and influential applications of the digital age, showing their worth in many fields, from phones and the financial world to surveillance security, to virtual documentation on the Internet. Underpinned by deep learning (Deep Learning) and advanced neural networks, it is now possible to improve the accuracy of systems far beyond many of the challenges of traditional methods.

Even with such developments, there remain serious issues regarding the appearance and alteration of the environment, demographic imbalance, forgery and manipulation at the heart, privacy, and security risks that must be settled by means of appropriate technical and ethical solutions. Recent surveys have also indicated that immunity against advanced attacks, growing data, and explainable models need to be improved to provide more transparency and trust in system-made decisions.

Guidelines for the future suggest that multi-sensory sensing, low-data learning, and self-learning should be integrated into the legal and ethical realms to ensure safe and fair use. As research continues in these domains, more consistent, secure, and operational systems can be established in real-world settings to achieve a balance between technological excellence and protecting citizens' rights.

Finally, the field is open to innovation, as new technologies create spaces for innovation in digital services and security but need to ensure integrity and privacy standards, and it is thus necessary to carry out ongoing research to advance these systems to address current as well as future challenges.

Funding: No funding was received for conducting this study. Data Availability: The data that support the findings of this study are available from the corresponding author upon reasonable request Competing Interests: The author declares no competing interests.

Author Contributions: RHH, RMH and ISH contributed to the design and implementation of the research

REFERENCES

[1] S. Kolekar, P. Patil, P. Barge, and T. Kosare, "A comprehensive study on artificial intelligence-based face recognition technologies," in *Springer International Publishing*, 2023, pp. 249–263. DOI: 10.1007/978-981-99-6586-1_17.

[2] M. Ramaswamy, "Ai-enhanced secure identity verification for financial services," *Int. J. Multidiscip. Res.*, vol. 6, no. 6, 2024. DOI: 10.36948/ijfmr.2024.v06i06.26589.

[3] P. Khare and S. Arora, "Artificial intelligence-based biometric authentication systems for facial recognition and identification," in *Proceedings of the ICEECT*, 2024, pp. 1–7. DOI: 10.1109/ICEECT61758.2024.10738912.

[4] W. Mo, "Method and device for identity verification based on face recognition," 2018.

[5] M. K. Pasupuleti, "Ai-enabled multimodal biometrics: Advancing security with facial, voice, and behavioral integration," pp. 1–9, 2025. DOI: 10.62311/nesx/77579.

[6] K. Das, H. Bordoloi, and K. K. Sarma, "Face recognition based verification with reinforced decision support," in *Proceedings of the International Conference on Computer and Communication Technology*, 2010, pp. 759–763. DOI: 10.1109/ICCCT.2010.5640440.

[7] T. Sethukarasi, S. Bharath, K. Sujatha, G. B. Bharathi, and S. Saravanakumar, "A smart face biometric verification oriented attendance handling system using artificial intelligence," in *Proceedings of the ICSES*, 2023, pp. 1–6. DOI: 10.1109/ICSES60034.2023.10465453.

[8] A. Fola-Rose, E. Solomon, K. Bryant, and A. Woubie, "A systematic review of facial recognition methods: Advancements, applications, and ethical dilemmas," 2024, pp. 314–319. DOI: 10.1109/IRI62200.2024.00070.

[9] C. Deng, "A review of face recognition technologies based on deep learning," *Appl. Comput. Eng.*, vol. 46, no. 1, pp. 297–303, 2024. DOI: 10.54254/2755-2721/46/20241638.

[10] M. Abdul Al, G. K. Kyeremeh, R. Qahwaji, N. Ali, and R. A. Abd Alhameed, "The evolution of biometric authentication: A deep dive into multi-modal facial recognition: A review case study," *IEEE Access*, 2024. DOI: 10.1109/ACCESS.2024.3486552.

[11] S. Kajotra and H. Kaur, "Assessing the performance of modern face recognition systems: A comparative exploration," 2025, pp. 1–8. DOI: 10.1109/CONIT65521.2025.11167827.

[12] A. Pandit, R. Nikalje, N. Vishwakarma, V. Vishwasrao, and T. Khose, "Face authentication using mtcnn and facenet," *Int. J. Res. Appl. Sci. Eng. Technol.*, 2023. DOI: 10.22214/ijraset.2023.56679.

[13] H.-C. Wang and J. Wu, *A machine learning-based secure face verification scheme and its applications to digital surveillance*, arXiv preprint, 2024. DOI: 10.48550/arxiv.2410.21993.

[14] R. Yu, X. Zhang, Y. Zhang, J. Song, K. Liu, and Q. Miao, "Design and implementation of identity verification software based on deep learning," *Int. J. Digit. Crime Forensics*, vol. 14, no. 3, pp. 1–15, 2022. DOI: 10.4018/ijdcf.315796.

[15] P. Ahlawat, N. Kaur, C. Kaur, S. Kumar, and H. K. Sharma, "Deep learning based face recognition system for automated identification," in *Springer Science+Business Media*, 2023, pp. 60–72. DOI: 10.1007/978-3-031-48781-1_6.

[16] W. Nie and M. Li, "Deep learning-based face recognition and face verification supervised learning method," 2018.

[17] M. Thalor and O. Gaikwad, "Facial recognition attendance monitoring system using deep learning techniques," *Int. J. Integr. Sci. Technol.*, vol. 2, no. 1, pp. 45–52, 2024. DOI: 10.59890/ijist.v2i1.1290.

[18] B. Chen, X. Liao, H. Zhu, Z. Gong, and Y. Li, "A survey of face recognition methods based on deep learning," *Highlights Sci. Eng. Technol.*, vol. 24, pp. 191–197, 2022. DOI: 10.54097/hset.v24i.3921.

[19] *Facial recognition for kyc solutions*, Vention, Accessed: Sep. 26, 2025, 2025. [Online]. Available: https://ventionteams.com/solutions/computer-vision/facial-recognition-kyc.

[20] *Biometrics and financial crime prevention*, SymphonyAI, Accessed: Sep. 26, 2025, 2025. [Online]. Available: https://www.symphonyai.com/resources/blog/financial-services/biometrics-financial-crime-prevention-regulators.

[21] *Top 5 advantages of using facial recognition in ekyc*, Finextra, Accessed: Sep. 26, 2025, 2025. [Online]. Available: https://www.finextra.com/blogposting/27606/top-5-advantages-of-using-facial-recognition-in-ekyc.

[22] R. Ravindran, S. Udayakumar, Y. Revanth, and K. Namitha, "Enhancing access control: A biometric approach with facial recognition and near-field communication integration," 2024, pp. 263–268. DOI: 10.1109/ICICI62254.2024.00051.

[23] V. Gujar, "Integrating facial recognition technology in indoai app with ekyc case study & future of ai cameras in banking," *Int. J. Sci. Res.*, 2023. DOI: 10.21275/sr231108193207.

[24] R. K. V. Satish et al., "Futuristic authentication: Development of an artificial intelligence based enhanced face detection and recognition system," 2024. DOI: 10.1109/ICICT60155.2024.10544692.

[25] X. You, X. Zhao, and J. Lu, "Identity security verification method and system based on identity documents and face recognition," 2018.

[26] A. Okumura, S. Handa, T. Hoshino, N. Tokunaga, and M. Kanda, "Identity verification using face recognition improved by managing check-in behavior of event attendees," in *Springer*, Cham, 2019, pp. 291–304. DOI: 10.1007/978-3-030-39878-1_26.

[27] "Privacy threats in facial recognition-based identity verification," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 569–572, 2023. DOI: 10.48175/ijarsct-11686.

[28] M. Wang and W. Deng, "Deep face recognition: A survey," *Neurocomputing*, vol. 429, pp. 215–244, 2021. DOI: 10.1016/j.neucom.2020.10.081.

[29] Y. Kortli, M. Jridi, A. Al Falou, and M. Atri, "Face recognition systems: A survey," *Sensors*, vol. 20, no. 2, p. 342, 2020. DOI: 10.3390/s20020342.

[30] T.-K. Wang, Y.-H. Lin, and K.-P. Li, "Application of ai face recognition technology in swipe card attendance systems for hospitals," *Proc. Eng. Technol. Innov.*, vol. 21, pp. 1–9, 2022. DOI: 10.46604/peti.2022.8984.

©2025 JAST