ISBN: 978-65-83849-24-3

Aurum EDITORA

CHAPTER 11

COMPUTER VISION FOR FACIAL RECOGNITION: ADVANCES AND RISKS

https://doi.org/10.63330/aurumpub.021-011

Rodrigo Thomé de Moura[1]

ABSTRACT

This work presents a comprehensive analysis of computer vision applied to facial recognition, highlighting its technical advances and the risks associated with the use of this technology in contemporary contexts. The study aimed to explain the foundations of computer vision, describe the technical functioning of facial recognition algorithms, identify the main advances that have expanded the accuracy and dissemination of these systems, and discuss the ethical and social challenges arising from their growing use. The research was developed through a bibliographic review based on relevant works and studies in the fields of artificial intelligence, computer vision, deep learning, and technological ethics. The methodology made it possible to gather, interpret, and compare different theoretical and technical perspectives on the subject, enabling a solid and critical understanding of the phenomenon analyzed. The results showed that facial recognition has evolved rapidly due to the development of deep neural networks, increased computational capacity, and access to large image datasets. The accuracy of these models has increased significantly, leading to the implementation of the technology in mobile devices, access control systems, digital platforms, and security applications. However, the work identified important risks, such as violations of privacy, misuse of biometric data, mass surveillance, algorithmic biases that more intensely affect minority groups, and vulnerabilities associated with digital forgery techniques. The analysis concluded that, although facial recognition represents a significant advance within artificial intelligence, its use requires regulation, transparency, and responsible practices to prevent social harm and ensure the protection of individual rights. The study highlighted the need to balance technological innovation and ethics, pointing to pathways that favor the safe and conscientious application of this tool.

Keywords: Facial recognition; Computer vision; Artificial Intelligence; Privacy; Ethics.

[1] Postgraduate in Dance Therapy
Prisma
E-mail: rodrigofsw@gmail.com

INTRODUCTION

The rapid evolution of Artificial Intelligence has profoundly transformed the way individuals, institutions, and technological systems interact with the digital world. Among these innovations, computer vision stands out as one of the most dynamic areas, as it allows machines to interpret and process visual information in a manner increasingly similar to human capabilities. Within this field, facial recognition has become one of the most widespread applications, present in smartphones, digital platforms, security systems, and mechanisms for automatic authentication. The specialized literature indicates that this technology, driven mainly by advances in convolutional neural networks and deep learning, has reached levels of accuracy previously considered unattainable (Szeliski, 2022; Goodfellow; Bengio; Courville, 2016). However, this accelerated development also raises ethical, social, and technical concerns that require careful analysis.

Thus, the present work focuses on computer vision applied to facial recognition, with an emphasis on its recent advances and the risks associated with its use. This study starts from the understanding that, although extremely useful for biometric authentication, access control, public security, and personalization of digital resources, the technology brings significant challenges related to privacy, the processing of personal data, and the possibility of misuse. The literature consulted reinforces such concerns, highlighting, for example, the high error rates for women, Black people, and minorities (Buolamwini; Gebru, 2018), the risks of mass surveillance (Lyon, 2018), and the increasing sophistication of digital forgeries and deepfakes (Tolosana et al., 2020).

The general objective of this work is to critically analyze the technical advances of facial recognition and discuss the risks and challenges resulting from its expansion. As specific objectives, it seeks to: explain the fundamental concepts of computer vision and image processing; describe the technical functioning of facial recognition and its main algorithms; present the advances that have made this technology more accurate and accessible; and, finally, analyze its ethical, social, and security risks in light of the current literature. The study starts from the hypothesis that, although facial recognition represents a milestone in the development of artificial intelligence, its indiscriminate use without adequate regulation can generate significant negative impacts, especially regarding privacy and social equity.

The justification for this study lies in the contemporary relevance of the topic. In a context in which cameras, sensors, and algorithmic systems become ubiquitous, understanding the functioning and impacts of this technology is essential so that citizens, professionals, and institutions adopt responsible practices aligned with current legislation. Moreover, in light of the growing integration of facial biometrics in public and private spaces, it is urgent to debate limits, risks, and possibilities, contributing to a safer, fairer, and more conscientious use of these tools.

Finally, this work was developed through bibliographic research based on classic and contemporary authors in the areas of computer vision, deep learning, and ethics in artificial intelligence. Throughout the study, fundamental concepts are presented alongside the technical functioning of the systems, their recent advances, and the ethical and social issues arising from their use, enabling a broad, critical, and well-grounded view of the theme..

METHODOLOGY

The work was developed through bibliographic research with a qualitative approach, grounded in the selection, analysis, and interpretation of books, scientific articles, and technical documents related to computer vision, facial recognition, deep learning, and ethics in artificial intelligence. The choice of this method allowed for a broad and critical understanding of technological evolution, the functioning of algorithms, and the social impacts associated with the growing use of this technology. The bibliographic research was conducted based on classic and contemporary authors in the field, making it possible to build a solid and coherent theoretical framework. The methodological process included identifying relevant publications in academic databases, scientific journals, and specialized books, prioritizing materials that discussed in depth the technical aspects, recent advances, and risks involved in facial recognition. After this selection, the content was analyzed and organized into thematic categories, allowing for the structuring of the topics addressed in the development of the work. This procedure made it possible to compare perspectives, synthesize information, and critically discuss the ethical and technological challenges related to the topic. In this way, the methodology adopted ensured theoretical consistency and contributed to a comprehensive analysis, producing a study aligned with academic standards and the purpose of understanding both the advances and the concerns that permeate the use of computer vision applied to facial recognition.

DEVELOPMENT

COMPUTER VISION: BASIC CONCEPTS

Computer vision is one of the most dynamic fields of Artificial Intelligence, as it seeks to enable machines to interpret, analyze, and understand visual information in a manner similar to humans. Broadly speaking, it can be defined as the set of techniques, algorithms, and computational models capable of extracting, processing, and recognizing patterns in images and videos, assigning meaning to this data to perform specific tasks. According to Szeliski (2022), computer vision is based on the capacity to transform raw visual data into structured representations, enabling automated systems to perform tasks ranging from simple activities, such as detecting edges in an image, to complex operations, such as identifying faces, objects, or actions in motion.

Image processing, in turn, is an essential stage within computer vision. It encompasses mathematical and computational procedures aimed at improving, transforming, or analyzing images, enabling the system to extract relevant information for visual recognition. Among the most common techniques are filtering, segmentation, contour detection, and color transformation—fundamental methods for reducing noise, enhancing details, and separating significant elements of the image for later interpretation. According to Gonzalez and Woods (2019), image processing is the foundation upon which more advanced algorithms are built, functioning as a link between the capture of visual information and the automated understanding performed by AI.

In recent years, the most significant advance in the area has occurred with the development of convolutional neural networks (CNNs) and deep learning. CNNs are models deeply inspired by the organization of the human visual cortex and stand out for their ability to identify complex patterns directly from data, without the need to manually extract visual features. LeCun, Bengio, and Hinton (2015) emphasize that this type of network revolutionized the field of computer vision by processing images hierarchically: in the first layers, simple traits such as edges and textures are identified; in deeper layers, abstract representations arise that describe complete objects, faces, or scenes.

Deep learning has further expanded this potential, allowing the training of networks with dozens or hundreds of layers to perform tasks such as facial recognition, image classification, anomaly detection, semantic segmentation, and many other applications. These deep architectures learn autonomously from large volumes of data, which makes their performance highly superior to traditional methods in various visual tasks. As stated by Goodfellow, Bengio, and Courville (2016), deep learning has enabled computer vision to reach levels of accuracy close to—and in some cases surpassing—human performance, especially in controlled environments.

Thus, understanding the basic concepts of computer vision, image processing, and convolutional neural networks is fundamental for studying contemporary applications of machine-based visual recognition. These theoretical foundations support current advances and provide a solid basis for the critical analysis of uses, limitations, and ethical implications of technologies based on artificial vision.

FACIAL RECOGNITION: TECHNICAL FUNCTIONING

Facial recognition, within the field of computer vision, is a complex technical process that involves multiple stages intended to identify or verify the identity of individuals from images or videos. Its modern operation is deeply linked to the use of deep neural networks, which enable precise analysis of visual patterns. For this technology to operate, the system must initially detect and locate a face in the image; then analyze its structural characteristics; and, finally, compare them to a previously registered database. According to Zhao et al. (2003), facial recognition combines techniques of detection, feature

extraction, and classification, forming a pipeline that transforms a face into numerical information capable of representing a person's identity.

The first stage, facial detection, consists of finding the exact region in which the face is present. Classic algorithms such as Viola and Jones's Haar Cascade were widely used for their speed and efficiency. However, modern approaches such as MTCNN (Multi-Task Cascaded Convolutional Networks), SSD, and YOLO offer greater accuracy, being capable of identifying faces under variations in lighting, angle, and expression. After detecting the face, the analysis of facial patterns begins, which involves identifying structural elements such as the position of the eyes, the shape of the nose, the contour of the face, and the distance between specific points. This analysis captures facial geometry, which Bojanowski and Joulin (2017) highlight as essential for representing identity consistently, even in the face of small pose variations.

The next stage, and perhaps the most crucial, is the extraction of facial features. In modern models, this extraction occurs through convolutional neural networks, which transform the face into a high-dimensional numerical vector known as a facial embedding. This embedding functions as a kind of "digital signature" of the face, representing a person's unique patterns in a compact and comparable form. The system then uses similarity metrics—such as Euclidean or cosine distance—to compare the vector of the analyzed face with vectors stored in the database. The smaller the distance between two embeddings, the greater the probability that they refer to the same person. According to Schroff, Kalenichenko, and Philbin (2015), this approach has allowed facial recognition to reach levels of accuracy previously considered impossible. Several algorithms and datasets have contributed significantly to the development of these systems. Labeled Faces in the Wild (LFW), for example, became one of the first highly impactful benchmarks, enabling evaluation of model accuracy in real, uncontrolled conditions. VGGFace, developed by the Visual Geometry Group, further expanded the field by providing a robust dataset and a high-performance pre-trained model. FaceNet, proposed by Schroff et al. (2015), revolutionized facial recognition by introducing the concept of triplet loss, which directly optimizes distances between embeddings, increasing model accuracy in verification and identification tasks. These advances enabled the technology to be incorporated into smartphones, security systems, digital platforms, and authentication tools with increasing precision and efficiency.

As a result, facial recognition has evolved into a technology capable of operating at scale, offering speed and high performance. However, its complex technical functioning requires careful analyses of its social impacts, especially regarding privacy, bias, and ethical use—fundamental aspects for understanding its implications in the contemporary scenario of artificial intelligence.

RECENT ADVANCES

Recent advances in facial recognition reflect the rapid evolution of computer vision driven by deep learning, resulting in systems that are increasingly precise, efficient, and widely disseminated in everyday life. One of the most significant progress points concerns the continuous increase in model accuracy. Thanks to deep neural networks and large datasets, current systems can operate with extremely low error rates, approaching—and in some contexts surpassing—the human ability to identify faces. According to Taigman et al. (2014), the development of more robust architectures, combined with techniques such as data augmentation and contrastive learning, has contributed to building models capable of recognizing individuals even under adverse conditions, such as variations in lighting, different angles, and changes in facial expression.

Another important advance is related to the implementation of these technologies in mobile devices. The popularization of systems such as Face ID, present in Apple smartphones, demonstrates the maturity achieved by the technology by allowing facial authentication to be used safely and quickly on millions of devices. These systems use infrared sensors, depth cameras, and deep learning models integrated with hardware, ensuring high performance even with energy and processing constraints. As Schroff et al. (2015) and Deng et al. (2019) emphasize, advances in facial recognition algorithms, alongside the development of optimized computational architectures, have made real-time processing directly on devices possible, reducing the need to send biometric data to external servers and contributing to greater privacy preservation. This perspective aligns with the critical analyses of Zuboff (2019) and Lyon (2018), which point out how digital surveillance and the use of personal data have become central in contemporary society, reinforcing the importance of technological solutions that reconcile innovation and protection of privacy.

Moreover, the use of facial recognition has expanded significantly across digital platforms. Applications from social networks and video services, such as Instagram, TikTok, and Snapchat, employ computer vision models to apply facial filters, perform expression mapping, and create complex interactive effects. In these contexts, the technology is not merely functional but also part of the aesthetic and entertainment experience, showing how AI has become accessible to the average user. In parallel, access control systems in corporate environments, airports, and public spaces have adopted advanced identification algorithms to replace cards, passwords, and physical documents, improving operational efficiency and security.

Another fundamental point in the area's progress is the emergence and popularization of pre-trained deep learning models. Networks such as VGGFace2, FaceNet, and ArcFace have been trained on millions of images and made available to researchers and developers, democratizing access to cutting-edge technologies. These pre-trained models significantly reduce the time and resources needed to build

facial recognition systems, allowing companies and researchers to adapt architectures to their specific needs without having to train a network from scratch. As Deng et al. (2019) observe, this approach fosters the development of more robust and efficient solutions, contributing to the rapid evolution and dissemination of the technology.

Thus, recent advances in facial recognition demonstrate not only the area's technical maturation but also its growing insertion into everyday life, reinforcing the need for ethical and regulatory debates in the face of its increasingly sophisticated and comprehensive use.

RISKS AND CHALLENGES

The risks and challenges associated with facial recognition accompany the rapid expansion of this technology and reveal ethical, technical, and social issues that cannot be ignored. One of the main problems concerns privacy and the protection of biometric data. Unlike a password or card, the face is a unique and permanent identifier that cannot be "changed" if compromised. According to Zuboff (2019), technologies that capture and analyze sensitive human data significantly expand forms of surveillance and exploitation, making the discussion about consent, security, and limits in the use of biometric information urgent. Brazil's General Data Protection Law (LGPD) classifies biometric data as sensitive, reinforcing that its use requires justification, necessity, and enhanced protection.

Another important risk is mass surveillance and the loss of anonymity in public spaces. Camera systems integrated with facial recognition algorithms make it possible to identify people in crowds, track movements, and reconstruct behavior patterns. Lyon (2018) highlights that such systems, when used without transparency and regulation, expand the surveillance power of state and corporate agents, creating an environment of constant monitoring. This situation can generate harmful effects on democracy, freedom of expression, and the right to come and go, especially when technology is used for social control or political repression. Algorithmic biases represent another serious challenge. Several studies demonstrate that facial recognition systems exhibit significantly higher error rates for women, Black people, and other minorities. The study by Buolamwini and Gebru (2018), conducted at MIT, showed that commercial systems had accuracy above 99% for white men but alarming failure rates when identifying Black women. These results show that the technology can reinforce historical inequalities, generate institutional discrimination, and compromise equity in applications such as policing, border control, or recruitment.

The misuse of technology by governments or companies is also a growing concern. In authoritarian contexts, facial recognition can be used to monitor political opponents, journalists, or vulnerable groups, increasing risks of persecution and repression. In the private sector, its use without consent can fuel abusive practices, such as tracking consumers, covert data collection, or inappropriate

applications in workplace environments. As O'Neil (2016) points out, poorly regulated algorithmic systems tend to operate as "weapons of math destruction," affecting individuals invisibly and without mechanisms for contestation.

Finally, there are technical vulnerabilities that challenge the reliability of these systems. Deepfakes—AI-generated videos capable of faithfully reproducing a person's face—represent a threat to digital security and can be used for fraud, blackmail, manipulation of public opinion, or identity theft. Likewise, spoofing attacks, such as the use of 3D masks, printed photos, or projections, can deceive facial recognition systems, demonstrating that these mechanisms are not always infallible. As reported by Tolosana et al. (2020), facial forgery techniques evolve rapidly, requiring the creation of robust and up-to-date defenses.

Given these risks, it is essential that the development and use of facial recognition technologies be accompanied by clear policies, effective oversight, and ethical reflection. The pursuit of innovation must go hand in hand with the protection of fundamental rights, ensuring that technological advances do not become instruments for violating individual and collective freedoms.

CONCLUSION

The study made it possible to understand that computer vision applied to facial recognition represents one of the most significant advances in contemporary artificial intelligence, bringing together sophisticated deep learning techniques, large datasets, and increasing computational capacity to perform tasks once exclusive to human perception. The analysis showed that, from a technical standpoint, the technology has evolved significantly in recent decades, achieving high accuracy rates and becoming widely used in mobile devices, digital platforms, authentication systems, and surveillance mechanisms. This expansion has been driven by convolutional neural networks capable of extracting facial features with high efficiency, producing robust embeddings that are quickly and reliably comparable across different usage contexts.

Nevertheless, despite its advances, facial recognition has also proven to be a technology marked by significant risks that must be considered critically. Issues related to privacy and the processing of biometric data proved central, since the face is a permanent, sensitive identifier that cannot be replaced in the event of a leak or misuse. The research also evidenced that such systems expand the possibilities for large-scale surveillance and monitoring, threatening fundamental rights such as anonymity and freedom of movement, especially in public environments and in societies with little transparency in the actions of governmental and corporate institutions.

Furthermore, the algorithmic biases identified in the literature underscore the need for caution, as they show that women, Black people, and other minorities continue to face higher error rates in facial

recognition—something that can result in institutional discrimination, injustices in security systems, and inequalities reinforced through automated decisions. It was also found that the technology is subject to technical vulnerabilities, such as deepfakes and spoofing attacks, which can circumvent authentication mechanisms and undermine the reliability of systems that rely exclusively on facial identification.

Accordingly, the work concludes that although facial recognition represents a milestone in the evolution of artificial intelligence and offers numerous benefits in terms of practicality, security, and automation, its use must be accompanied by clear regulations, constant oversight, and policies that ensure transparency, equity, and protection of sensitive data. The analysis showed that the adoption of this technology can only be considered socially responsible when a balance is established between innovation and fundamental rights, preventing technical advances from turning into instruments of abusive surveillance or discrimination. Thus, we highlight the importance of governments, companies, and civil society acting jointly to build ethical guidelines, control mechanisms, and safe development practices, ensuring that facial recognition is applied in a fair, reliable manner aligned with democratic values.

REFERENCES

1. Bojanowski, Piotr; Joulin, Armand. Unsupervised learning by predicting noise. In: International Conference on Machine Learning, 2017. Available at: https://arxiv.org/abs/1704.05310. Accessed on: 15 Nov. 2025.

2. Buolamwini, Joy; Gebru, Timnit. Gender Shades: Intersectional accuracy disparities in commercial gender classification. In: Proceedings of the 1st Conference on Fairness, Accountability and Transparency. PMLR, v. 81, p. 77–91, 2018. Available at: https://proceedings.mlr.press/v81/buolamwini18a.html. Accessed on: 15 Nov. 2025.

3. Deng, Jiankang et al. ArcFace: Additive angular margin loss for deep face recognition. In: IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2019. Available at: https://openaccess.thecvf.com/content_CVPR_2019/html/Deng_ArcFace_Additive_Angular_Margin_Loss_for_Deep_Face_Recognition_CVPR_2019_paper.html. Accessed on: 15 Nov. 2025.

4. Gonzalez, Rafael C.; Woods, Richard E. Digital Image Processing. 4. ed. Pearson, 2019.

5. Goodfellow, Ian; Bengio, Yoshua; Courville, Aaron. Deep Learning. Cambridge: MIT Press, 2016.

6. LeCun, Yann; Bengio, Yoshua; Hinton, Geoffrey. Deep learning. Nature, v. 521, p. 436–444, 2015. Available at: https://www.nature.com/articles/nature14539. Accessed on: 15 Nov. 2025.

7. Lyon, David. The Culture of Surveillance: Watching as a Way of Life. Cambridge: Polity Press, 2018.

8. O'Neil, Cathy. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. New York: Crown, 2016.

9. Schroff, Florian; Kalenichenko, Dmitry; Philbin, James. FaceNet: A unified embedding for face recognition and clustering. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2015. Available at: https://arxiv.org/abs/1503.03832. Accessed on: 15 Nov. 2025.

10. Szeliski, Richard. Computer Vision: Algorithms and Applications. 2. ed. Cham: Springer, 2022.

11. Taigman, Yaniv et al. DeepFace: Closing the gap to human-level performance in face verification. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2014, p. 1701-1708. Available at: https://www.cv-foundation.org/openaccess/content_cvpr_2014/html/Taigman_DeepFace_Closing_the_2014_CVPR_paper.html. Accessed on: 15 Nov. 2025.

12. Tolosana, Ruben et al. DeepFakes and beyond: A survey of face manipulation and fake detection. Information Fusion, 2020. Available at: https://arxiv.org/abs/2001.00179. Accessed on: 15 Nov. 2025.

13. Viola, Paul; Jones, Michael. Rapid object detection using a boosted cascade of simple features. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2001, v. 1, p. I-511–I-518.
Available at: https://www.researchgate.net/publication/3940582_Rapid_Object_Detection_using_a_Boosted_Cascade_of_Simple_Features. Accessed on: 15 Nov. 2025.

14. Zhao, Wenyi et al. Face recognition: A literature survey. ACM Computing Surveys, v. 35, n. 4, p. 399–458, 2003. Available at: https://dl.acm.org/doi/10.1145/954339.954342. Accessed on: 15 Nov. 2025.

15. Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.