Facial detection for border security

George SUCIU,
Beia Consult International, Bucharest, Romania
george@beia.ro

Răzvan BRĂTULESCU,
Beia Consult International, Bucharest, Romania
razvan.bratulescu@beia.ro

Robert FLORESCU,
Beia Consult International, Bucharest, Romania
robert.florescu@beia.ro

Vlad-Constantin STĂNESCU,
Beia Consult International, Bucharest, Romania
vlad.stanescu@beia.ro

Mari-Anais SACHIAN,
Beia Consult International, Bucharest, Romania
anais.sachian@beia.ro

Teodor-Matei BÎRLEANU,
Beia Consult International, Bucharest, Romania
teodor.matei.birleanu@gmail.com

Abstract
Facial recognition has come a long way, evolving from simple image processing techniques to powerful AI-driven tools. In this article, we take a closer look at how these technologies, both classical and modern, can be used to support something as critical as border security. Our focus is on a practical application we developed, designed to verify a person's identity by comparing their face to a database of known individuals. The system uses a combination of Haar cascade classifiers (a classic approach for face detection) and neural networks based on deep learning to improve accuracy and adaptability. Built with OpenCV, the application follows a straightforward process: a new face is uploaded, analysed, and either matched or flagged as unknown. What makes this work interesting is the balance it strikes between speed and reliability, qualities that are essential in a fast-paced border control setting. We show that even with lightweight tools, solid results can be achieved, and when combined with more advanced AI models, the system becomes even more robust. Our goal wasn't just to explore the tech, but to show how these tools can be applied in real-world scenarios where security really matters. This study adds to the ongoing conversation around biometrics and AI, and we hope it sparks further exploration into how these technologies can help make borders safer and smarter.

Keywords: AI, biometry, database, neural networks.

1. Introduction
Facial recognition technology plays a pivotal role in modern computer vision and artificial intelligence, with far-reaching implications across diverse sectors like security, biometrics, and human-computer interaction. As digital cameras proliferate and technology advances, the automatic identification and tracking of human faces within images and videos have assumed unprecedented importance. The advent of deep learning has revolutionized the field, elevating performance metrics, including accuracy and processing speed, to

unprecedented heights compared to traditional machine learning approaches [1]. Among these deep learning innovations, convolutional neural networks (CNNs) have emerged as powerful tools, proving their mettle in tackling a myriad of image-based challenges, notably in the realm of face detection and recognition.

In this article, we take a closer look at the latest research and innovations that aim to make face detection and recognition more reliable and efficient, with real-world applications in mind. We start by introducing the fascinating field of computer vision, highlighting just how important facial detection and recognition have become. From there, we dive into the world of neural networks, especially convolutional networks, to better understand the technology that powers these systems.

2. Related work - Facial recognition methods

Border control is a government-administered service that regulates the movement of individuals, animals, and goods across a country's boundaries. Its main objective is to protect the region from potential threats that may arise once the border has been crossed.

To monitor individuals in border areas, identity verification and biometric data are commonly utilized. A person's identity is primarily confirmed through official documents and biometric authentication. Facial features serve as a key biometric marker for personal identification. However, manual facial recognition performed by officers carries a significant risk of errors. As a result, an advanced technological solution capable of accurately identifying and verifying facial biometrics in border regions is necessary.

This method entails comparing facial images from a database, identity documents presented at the checkpoint, and real-time captured photos. Individuals are permitted to cross the border as long as they provide the necessary documents, and their facial features match the records in the database [2].

A vast and detailed volume of data is generated during the facial recognition process. This involves collecting, storing, processing, and analysing facial images to achieve high accuracy. In the context of facial recognition, large-scale datasets, often referred to as “Big Data”, are used alongside advanced analytical techniques to detect and identify features [3]. However, when developing and implementing big data solutions for facial recognition, it is essential to address legal considerations and privacy concerns related to the use of facial data.

Face recognition is a subclass of face detection, as the process begins by identifying a face before analysing its features to compare it with a database of known faces for identification. In face recognition, unique facial attributes such as the eyes, mouth, and nose are automatically extracted [3]. These features are then converted into a vector, allowing statistical pattern recognition techniques to be applied for accurate face matching.

In the realm of facial recognition methods, it's essential first to grasp the fundamental concept of image recognition, which forms the backbone of this cutting- edge technology. Image recognition, in essence, is the process through which a computer program is

empowered to identify and label various entities within an image, ranging from objects and buildings to the most intricate element of all – human faces [4]. This is undoubtedly one of the most common and widely recognized computer vision applications, having far-reaching implications in diverse sectors.

In the pursuit of achieving precision and efficiency in image recognition, deep learning stands out as a formidable contender, with convolutional neural networks (CNNs) leading the charge. These sophisticated models are trained on vast datasets consisting of meticulously labelled images. Through this rigorous training process, CNNs acquire the ability to discern intricate patterns and features that correspond to distinct objects or classes within the images. Once trained, the CNN model can seamlessly process new images as input and furnish corresponding labels for the objects it identifies within the image [5].

The versatility of image recognition transcends its ubiquitous presence, extending into critical domains such as self-driving cars, surveillance through security cameras, and the organization of vast photo collections. Beyond these practical applications, image recognition's transformative potential also emerges in advanced use cases, notably in the realms of facial recognition, object detection, and image generation. However, it's important to note that face detection and recognition represent two intimately intertwined yet distinct tasks within the broader landscape of computer vision [5]. Face detection serves as a specialized computer technology designed to pinpoint and locate human faces within digital images and videos. This function is a specific application of object detection, a broader field within computer vision dedicated to identifying instances of semantic objects belonging to various classes, such as humans, cars, buildings, and more.

Face detection algorithms employ diverse techniques to identify facial features within an image. By scrutinizing elements such as edges and textures, these algorithms discern whether the detected features align with the characteristics of a human face. An algorithm typically delineates a bounding box around the recognized face upon successful detection. This bounding box serves as a foundational step for subsequent processes, including but not limited to facial recognition or tracking a face within a video stream [6].

Some techniques that have emerged as a breakthrough in face detection are deep learning (DL) methods, leveraging their capacity to learn intricate features from extensive datasets autonomously. These DL-based models undergo rigorous training on sizable repositories of annotated image data, acquiring the ability to discern intricate patterns and unique facial features. The relentless advancement of deep learning has ushered in significant enhancements in the performance of face detection algorithms.

In contrast, facial recognition is a distinct process focused on identifying individuals from digital images or video frames. This method usually entails comparing facial features against a comprehensive database of known faces, yielding a person's name or identification when a match is established [6]. Facial recognition algorithms rely on the bounding box provided by the preceding face detection step as a starting point, subsequently extracting and scrutinizing facial features for comparison against the known facial profiles.

Facial recognition systems typically follow one of three main approaches: local methods, holistic (or subspace) techniques, and hybrid models, as illustrated in Fig. 1. Local approaches focus on analysing specific facial features and tend to be more sensitive to changes in facial expressions, partial obstructions, and different head positions.

They can be further categorized into two subtypes: local appearance-based techniques and key point-based techniques. The former extracts intricate local features by dissecting the facial image into smaller regions or patches, concentrating on pivotal facial landmarks like the nose, mouth, and eyes. These techniques employ descriptors such as pixel orientations, histograms, geometric attributes, and correlation planes to characterize local features. Conversely, key point-based techniques identify points of interest within the facial image and extract features at these salient points, harnessing them to unveil distinctive features described by a concise set of parameters.

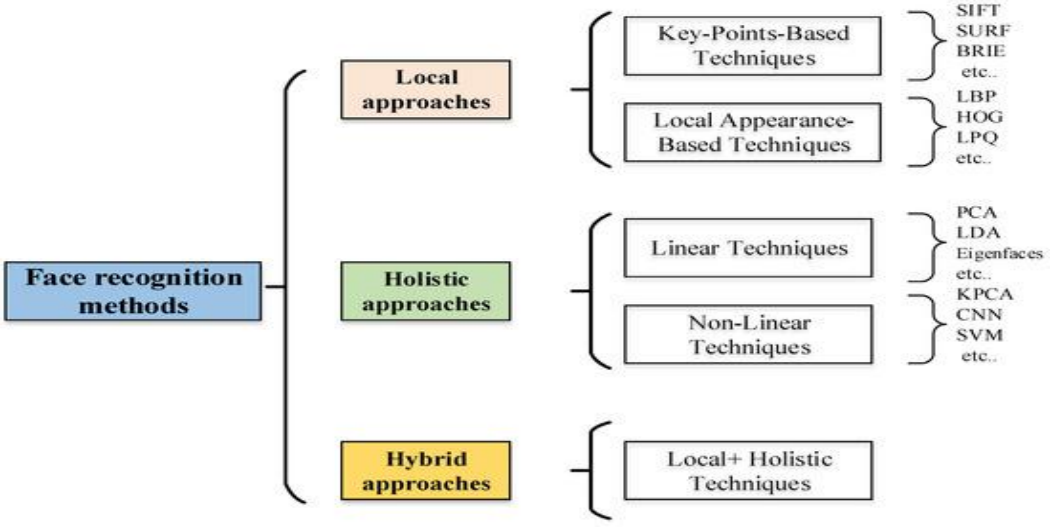

Fig. 1. Face recognition methods.
Source: K. Yassin, J. Maher, A. F. Ayman and A. Mohamed, "Face Recognition Systems: A Survey," Sensors, vol. 20(2), 2020 [7].

In contrast, holistic approaches embrace the entire facial image as input data, projecting it onto a compact subspace or correlation plane. This approach preserves the image as the whole information, homing in on regions or points of significance. Nonetheless, this attribute can be a drawback, as it presupposes that all image pixels are equally relevant, rendering these techniques computationally intensive and demanding a substantial degree of alignment between test and training images. Furthermore, holistic approaches often need to pay more attention to local intricacies, thus rendering them infrequently employed for face identification purposes.

Hybrid approaches represent a synthesis of both local and holistic paradigms, engineered to harness the strengths of each approach. These strategies amalgamate local and global features to extract the collective benefits of both techniques. The choice between these methodologies' hinges on the specific application context, considering factors such as

image size and the nature of the recognition task at hand. For instance, in face recognition systems utilizing diminutive images, methods found on local features may not be the most prudent choice. Hybrid approaches emerge as a valuable strategy to enhance recognition performance and bolster accuracy.

Evaluating these techniques' effectiveness reveals varying recognition accuracy levels across diverse datasets. It's imperative to recognize that the accuracy of face recognition systems hinges on an array of factors, including data quality, dataset size, and algorithmic complexity, underscoring the nuanced nature of this evolving field.

3. Border security

Border security refers to the measures taken by a country or region to monitor and control its borders to prevent unauthorized entry or exit of people, goods, and other items that may pose a threat to national security, public safety, or the economy. This can include the deployment of various security personnel, such as border guards and police, as well as the use of technological tools and infrastructure, such as surveillance cameras, biometric databases, and risk assessment algorithms.

Beyond the utilization of cutting-edge technologies, international collaboration and information exchange across nations can also greatly enhance border security. The effectiveness of border management can be significantly increased by cooperative initiatives, such as joint border patrols, shared intelligence databases, and coordinated responses to security concerns. For example, real-time information exchange on wanted persons, stolen vehicles, and missing persons is facilitated by the Schengen Information System (SIS) used by member states of the European Union. This helps identify and apprehend suspects more efficiently. By working together, nations may successfully address the intricate and international border security issues, resulting in safer and more secure borders around the world.

In recent years, Artificial Intelligence (AI) has emerged as a transformative force in both border security and cybersecurity. AI technologies are increasingly employed to enhance security systems by enabling faster detection and prevention of threats, automated responses to incidents, and more accurate risk assessments [8]. For instance, AI-driven surveillance can analyse real-time data from cameras and sensors to detect suspicious behaviour at border crossings. Additionally, behavioural analysis powered by AI allows systems to identify anomalies in user or network activity, which can indicate a potential security breach.

AI also plays a growing role in cybersecurity; a domain closely linked to border security through the protection of digital infrastructure and sensitive data. AI enhances threat intelligence by quickly analysing vast amounts of data to uncover hidden patterns or attack vectors. However, the relationship between AI and cybersecurity is complex. While AI strengthens defences, it also introduces new vulnerabilities, such as adversarial AI, where malicious actors exploit weaknesses in AI models.

A notable challenge in the cybersecurity field is the skills gap, with a shortage of qualified professionals to manage increasingly sophisticated threats. AI helps bridge this gap by automating routine tasks and supporting human analysts with advanced tools. At the same time, ethical considerations, data protection, and privacy concerns must be addressed to ensure responsible use of AI technologies [9].

Looking ahead, the integration of AI into both border and cybersecurity strategies is expected to expand. Areas such as ethical AI use, human-machine collaboration, and ongoing research and development will be critical to ensuring that AI continues to serve as a force for security while mitigating its inherent risks. In this rapidly evolving landscape, the synergy between AI, cybersecurity, and border management will be essential to maintaining a secure and resilient global environment.

4. Key features of facial detection for border security

Border security involves using a variety of technologies to monitor and protect a country's borders. These technologies are used to detect and prevent illegal border crossings, smuggling and other security threats. Some of the key technologies used for border security include, see Fig. 2:

- High-resolution surveillance cameras equipped with night vision and thermal imaging capabilities are used to monitor border areas around the clock. These cameras can capture and transmit live video images to control centers for real-time monitoring.
- Drones equipped with cameras and sensors are used for aerial surveillance of border regions. They can quickly cover large areas and provide valuable situational awareness to border patrol agents.
- Ground sensors, including seismic, acoustic and magnetic sensors, are deployed along border areas to detect the movement of people or vehicles. These sensors can trigger alarms when unusual activity is detected.
- Physical barriers, such as walls, fences and vehicle barricades, are used to deter and prevent unauthorized border crossings.
- Biometric technology, such as fingerprint and facial recognition systems, is used to identify and verify the identity of individuals at border crossings.
- LPR systems use optical character recognition to read and record license plate numbers of vehicles entering or exiting a border area. This information can be cross-referenced with databases of stolen or suspicious vehicles.
- Radar technology can detect the movement of objects, including boats and aircraft, in border regions. It helps in identifying and tracking potential threats.
- Specialized vehicles equipped with advanced communication systems and surveillance equipment are used by border patrol agents to respond quickly to incidents and maintain a visible presence.
- At border checkpoints and crossings, biometric scanners and document readers are used to verify the authenticity of passports, visas, and other identification documents.

- Satellite imagery provides a broader view of border regions and can be used for monitoring changes in the landscape, identifying unauthorized construction, and tracking large groups of people.
- Advanced communication networks, including secure radio systems and satellite communication, enable real-time information sharing among border security personnel.
- Data analytics and machine learning for border security agencies are used to process and analyse large amounts of data, helping them to more effectively identify patterns and potential threats.
- Unmanned Ground Vehicles (UGVs) or ground-based robots, can be used for patrolling remote or hazardous areas, as well as for tasks like explosive ordnance disposal.
- Underwater Sensors, in border regions with bodies of water, underwater sensors can detect the presence of underwater vehicles or divers attempting to breach the border.
- Biological and Chemical Detection Systems, these systems are used to identify potential threats related to the transportation of hazardous materials or the spread of diseases.
- X-ray technology is used for the inspection and scanning of cargo, vehicles, luggage, and packages. It plays a crucial role in identifying hidden threats, contraband, and illegal goods that may be concealed within these items.

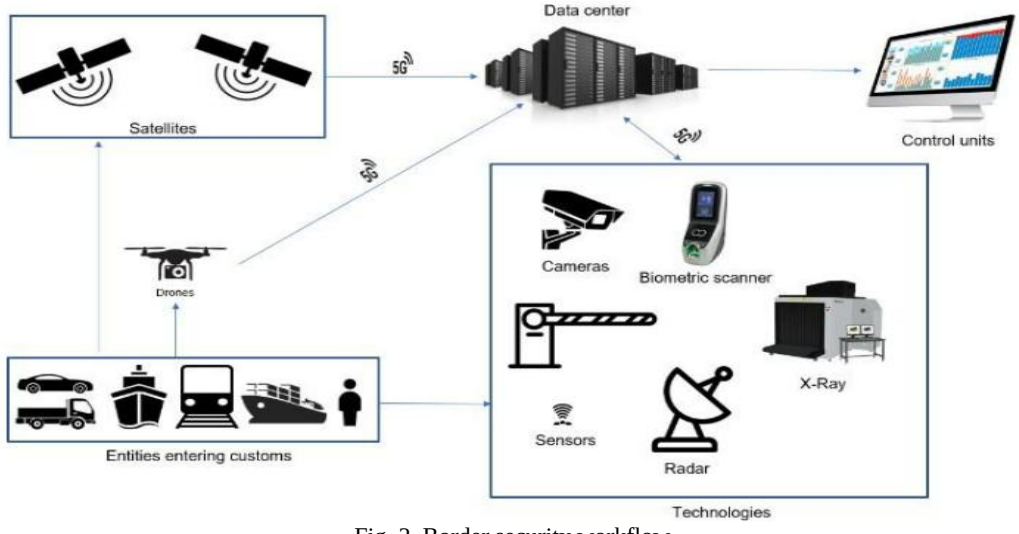

Fig. 2. Border security workflow.
Source: Authors' own work

In today's ever-evolving world, border security stands as one of the paramount concerns for governments globally. To tackle the challenges posed by modern-day threats, facial detection technology has emerged as a game-changer. It offers a unique set of features that has significantly transformed border control strategies.

Rapid Identification: Facial detection technology brings to the table a remarkable ability to swiftly identify individuals, making it a game-changer at border crossings. The U.S. Customs and Border Protection (CBP) agency, for instance, deploys the Traveler Verification Service (TVS) to leverage facial recognition for faster traveler processing. By efficiently comparing travelers' facial features with a vast database of known identities, the system streamlines border crossings, reducing waiting times and enhancing overall efficiency.

To get a better perspective on rapid identification, consider the European Union's Smart Borders initiative. It aims to expedite border crossings for frequent travelers by using facial recognition technology. This initiative shows how facial detection's rapid identification capabilities can significantly improve cross-border movement, making it more efficient and secure for everyone. Modern facial detection systems have reached impressive levels of accuracy, which is pivotal for enhancing security at border checkpoints. Singapore's Changi Airport, one of the world's busiest aviation hubs, incorporates facial recognition technology to bolster security measures while simplifying passenger processing [10]. By meticulously matching passengers with their passport photos and travel documents, the airport sets a global standard for border security, ensuring both precision and efficiency.

Zooming in further, think about the European Union's Entry/Exit System (EES), where facial detection plays a pivotal role in tracking non-EU nationals within the Schengen Area. The high accuracy of these systems enables authorities to maintain an up-to-date and comprehensive traveler profile, significantly elevating border security standards.

Efficient border security necessitates the seamless integration of multiple data sources, and facial detection technology excels in this regard. The European Union's Entry/Exit System (EES) provides a prime example of this integration, where facial detection technology seamlessly integrates with biometric data, visa information, and other pertinent databases to monitor non-EU nationals within the Schengen Area. This comprehensive data integration equips the authorities with a holistic and up-to-date traveler profile, significantly enhancing border security [10].

5. Privacy concerns and ethical considerations

A comparative study of facial recognition technology (FRT) regulation across the European Union, the United States, and China reveals distinct legal philosophies and enforcement models shaped by cultural, ethical, and institutional differences. The EU, anchored in deontological ethics, emphasizes the intrinsic value of privacy and dignity, enforcing strict compliance through frameworks such as the GDPR and the AI Act Proposal. In the Clearview AI case, Italian authorities sanctioned the company for unlawfully collecting and processing biometric data without informed consent, highlighting the EU’s proactive, top-down enforcement model and its commitment to “privacy by design” and “privacy by default” [11].

In contrast, the U.S. response is rooted in consequentialist ethics, focusing on individual injury and procedural breaches. The Facebook case under Illinois' Biometric Information

Privacy Act (BIPA) demonstrated a strong but market-driven legal remedy, with courts awarding substantial financial compensation for non-consensual biometric data processing. However, the U.S. framework remains fragmented, with regulatory efforts mainly at the state level, and enforcement often driven by class action litigation rather than centralized oversight [11].

China, on the other hand, has moved from a fragmented legal landscape—described metaphorically as "nine dragons playing with a pearl"—to a more unified approach through recent laws like the Personal Information Protection Law (PIPL). The Gu v. Chengguan Property case illustrated a utilitarian and pragmatic model, where enforcement relies on concrete harm rather than abstract rights. Chinese courts required deletion of personal data but issued modest fines, reflecting a "learning by doing" governance style in a context of rapid FRT adoption and growing public awareness [11].

Despite their differences, all three jurisdictions converge on certain principles: the need for informed consent, the minimum necessary standard for data processing, and a growing recognition of the risks FRT poses to privacy and autonomy. Yet their enforcement diverges—Europe mandates compliance regardless of harm, the U.S. emphasizes procedural injury and financial penalties, while China seeks a balance between innovation and legal response, often favoring collective benefit over individual autonomy. Together, these regulatory pathways highlight the complexity of governing FRT in a globalized digital ecosystem and point to the need for context-aware, cross-border standards [11].

Facial recognition technologies have been criticized for their difficulty in accurately identifying individuals with certain physical traits, potentially leading to biased outcomes in border control. Studies show that these systems frequently misidentify darker-skinned females, with error rates up to 34% higher compared to lighter-skinned males. Additionally, they are less effective for children, elderly individuals, and non-binary people. Another concern is the lack of transparency regarding data usage and consent. Passengers at border checkpoints often receive minimal information on how to opt out of facial recognition processes.

In Fig. 3, the graph in the Innovatrics report illustrates the improvement in facial recognition accuracy over time. The x-axis represents the years when new algorithms were developed, while the y-axis indicates the accuracy ratio, specifically the False Reject Rate (FRR) and False Accept Rate (FAR). Each vertical line corresponds to the latest algorithm developed at that time. The graph demonstrates that, since 2017, Innovatrics have enhanced their facial recognition accuracy by a factor of four for low-quality images (depicted by the cyan line) and by 33 times for high-quality images (depicted by the yellow line). As the line drops on the X axis, the number of times the system did not recognize a person based on the source of the Visa picture decreases as it approaches the current year and date. Observing the yellow line in 2018, on average, 0.18 cases out of 1 million failed to be correctly detected. Two years later in 2020, the numbers greatly improved to an average of only 0.0054 cases out of 1 million [12].

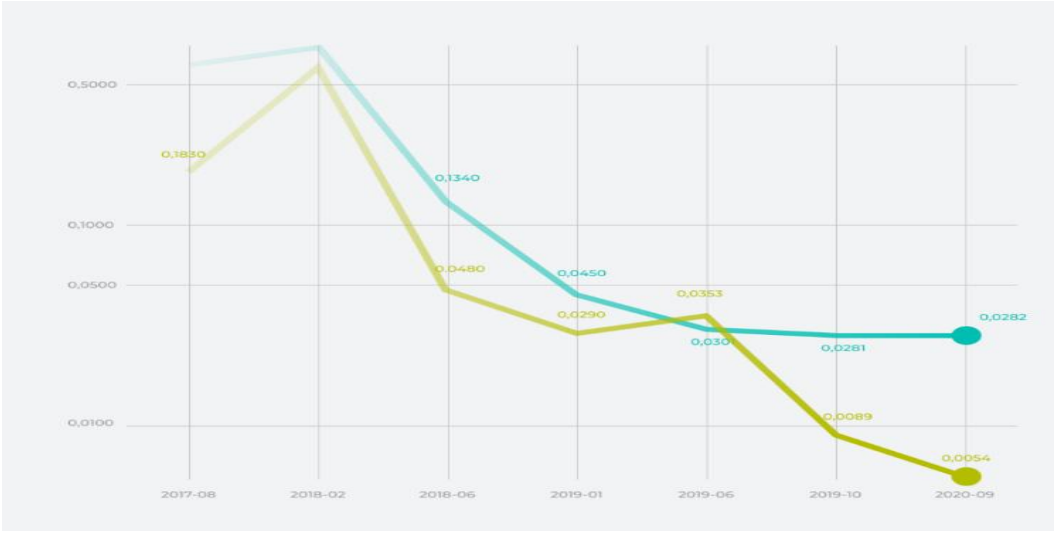

Fig. 3. The accuracy of face recognition algorithm.
Source: https://innovatrics.com/trustreport/how-the-accuracy-of-face-recognition-technology-has-improved-over-time/ [12]

6. Proposed method

The method applied in this article for face recognition is based on the Haar cascade classifier, as described above. This method is widely used due to its computational efficiency, speed, and high accuracy in facial detection. It operates in four key stages: Haar-feature selection, creation of integral images, AdaBoost training, and cascade classification. Haar-like features consist of regions with contrasting light and dark areas, where the algorithm extracts essential features by computing intensity differences [13].

To improve computational efficiency, the algorithm employs integral images, where each pixel represents the sum of all pixels above and to the left, significantly reducing processing time. AdaBoost training selects the most relevant features by combining multiple weak classifiers into a strong classifier, enhancing detection accuracy. Finally, the cascade classifier processes image regions hierarchically, quickly eliminating non-facial regions while focusing on potential face-like areas for optimized detection. OpenCV provides various pre-trained classifiers based on this method, making it a powerful tool for real-time face detection [14].

In this project, the Haar cascade classifier is implemented for face detection, following the method described above. The script begins by loading an image using OpenCV and converting it to grayscale to enhance detection accuracy while reducing computational complexity. The classifier is initialized using OpenCV's pre-trained model (haarcascade_frontalface_default.xml), and the detectMultiScale function scans the image for faces, with adjustable parameters (scaleFactor=1.15, minNeighbors=5) to fine-tune detection accuracy and minimize false positives. When a face is detected, its coordinates are used to crop and save it as an individual image file for further processing. Additionally, the script integrates an instance of the mrz_reader class for Machine Readable Zone (MRZ) processing, a technique commonly used for scanning identity documents such as passports.

Configuration options allow the system to enhance image clarity by removing shadows, reducing skewness, and clearing the background for improved document processing. The implementation of this method ensures efficient and accurate face recognition, leveraging OpenCV's capabilities to optimize detection and processing [15].

A reliable face recognition system typically follows three main steps: (1) face detection, (2) feature extraction, and (3) face recognition, as illustrated in Fig. 4. [7]. First, the system identifies and locates faces within an image during the detection phase. Next, in the feature extraction stage, it generates feature vectors for each detected face. Finally, the recognition step involves comparing these extracted features with those stored in a database of known faces to determine the person's identity.

Based on the requirements of the project, an application was developed using Streamlit. Fig. 5. depicts the interface of the application that has received an image of someone's face. After analysis, the application successfully identifies the person as Adrian, whose biometric information was uploaded earlier in the database.

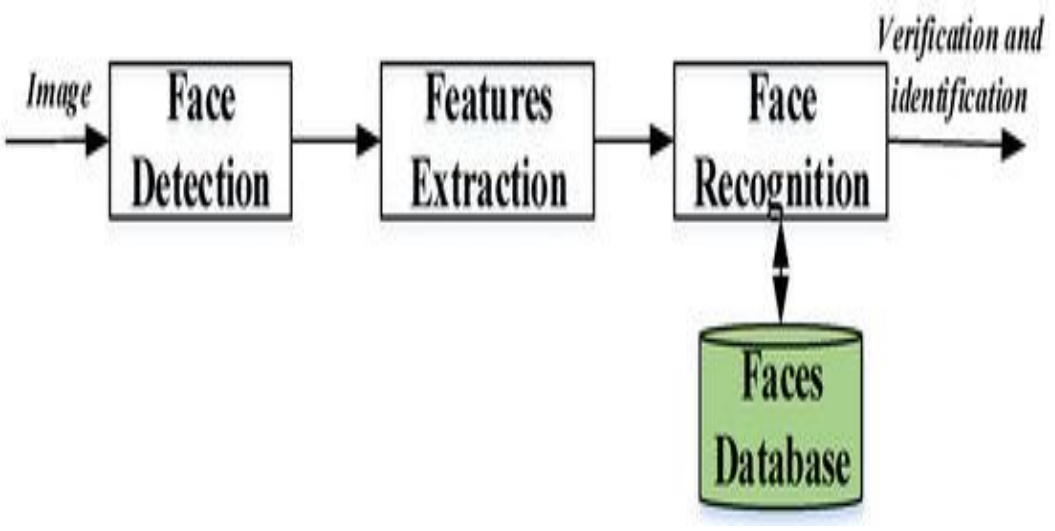

Fig. 4. Face recognition structure.
Source: K. Yassin, J. Maher, A. F. Ayman and A. Mohamed, "Face Recognition Systems: A Survey," Sensors, vol. 20(2), 2020 [7].

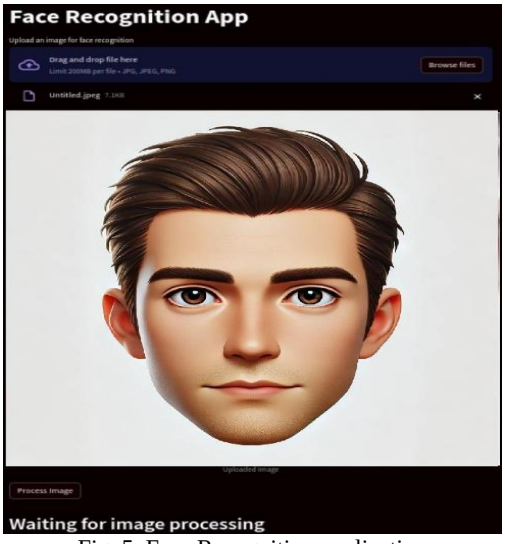

Fig. 5. Face Recognition application
Source: Authors' own work

Similarly, when uploading images of people that aren't registered in the database, the web app will mention that no match was found.

Through the collaboration with the border police, who will provide access to their database of biometric and ID records, this application will make identifying people faster and reduce the number of manual identifications/ searches that must be carried out independently.

7. Conclusion

In the ever-evolving landscape of border security, facial recognition technology emerges as a transformative tool, offering unprecedented precision and efficiency. From its roots in computer vision to its application at border checkpoints worldwide, facial detection and recognition have revolutionized identity verification processes. We've seen how it enables rapid identification, enhances accuracy, and streamlines the flow of legitimate travelers while combating identity fraud.

However, as with any technological advancement, ethical considerations loom large. Privacy concerns and data security risks underscore the need for responsible governance and transparent regulations. As we navigate the intersection of innovation and ethics, it's imperative to strike a balance between security imperatives and individual liberties. By harnessing facial recognition technology judiciously and ethically, we can create safer, more secure borders while upholding fundamental principles of justice and equality.

In essence, facial recognition stands as a testament to the potential of technology to enhance border security. It's not just about safeguarding physical boundaries but also about fostering a world where security coexists with dignity and respect for human rights.

Facial recognition technology is transforming border security, offering unparalleled efficiency in identity verification. By leveraging advanced algorithms, it enables rapid identification, minimizes human error, and accelerates traveler processing while helping to prevent identity fraud. These capabilities make it a powerful tool for modern border management, streamlining security without disrupting the flow of legitimate travelers.

However, its implementation is not without challenges. Privacy concerns, potential biases in recognition algorithms, and risks associated with biometric data storage demand careful oversight. Studies have shown that facial recognition systems can exhibit inaccuracies, particularly for individuals from minority groups, raising questions about fairness and reliability. Additionally, the storage and use of biometric data introduce cybersecurity risks, emphasizing the need for strict data protection measures and transparency in how this information is handled.

To fully realize the benefits of facial recognition while addressing these risks, responsible governance is essential. Clear policies on data usage, ethical algorithm development, and mechanisms for public oversight must be established. The goal should not only be to enhance security but also to ensure that innovation aligns with fundamental rights and freedoms.

Ultimately, facial recognition represents both an opportunity and a responsibility. It is more than just a tool for securing borders; it reflects how technology can be used to protect societies while respecting human dignity. The challenge lies in ensuring that security measures evolve in a way that safeguards both physical boundaries and the ethical principles that define them.

Acknowledgment
The work presented in this paper has received funding from the following projects: S1. The European Research Executive Agency (REA) program, HORIZON-CL3- 2021-BM-01 FLEXI-CROSS project under grant agreement No 101073879.

References

[1] Dlib C++ Library, “Dlib C++ Library,” 27 May 2025. [Online]. Available: http://dlib.net. [Accessed 15 July 2023].

[2] F. Hidayat, U. Elviani, G. B. G. Situmorang, M. Z. Ramadhan, F. A. Alunjati and R. F. Sucipto, “Face Recognition for Automatic Border Control: A Systematic Literature Review,” *IEEE Access,* vol. 12, pp. 37288 - 37309, 2024.

[3] Maheswaran, Gomathi, Rithikhaa, Praveen, Prathiksha and Murugesan, “A Perspective way of designing Intelligent systems with Face Detection and Recognition using Artificial Intelligence for Authentication,” in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Delhi, 2023.

[4] M. S. S. K. Varma, “Human Face Detection and Recognition using Artificial Intelligence,” in *2023 7th International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, 2023.

[5] S. Purohit, N. Mishra, T. Yang, R. Singh, D. Mo and L. Wang, “Real-Time Threat Detection and Response Using Computer Vision in Border Security,” in *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)*, Hassan, 2024.

[6] K. Kumar, “Criminal face identification system using deep learning algorithm multi-task cascade neural network (MTCNN),” *Materials Today: Proceedings*, vol. 80, pp. 2406-2410, 2023.

[7] K. Yassin, J. Maher, A. F. Ayman and A. Mohamed, “Face Recognition Systems: A Survey,” *Sensors*, vol. 20(2), 2020.

[8] O.-A. SARCEA, “AI & Cybersecurity – connection, impacts, way ahead,” in *International Conference on Machine Intelligence & Security for Smart Cities (TRUST)*, Bucharest, 2024.

[9] G. Waizel, “Bridging the AI divide: The evolving arms race between AI- driven cyber attacks and AI-powered cybersecurity defenses.,” in *International Conference on Machine Intelligence & Security for Smart Cities (TRUST)*, Bucharest, 2024.

[10] European Commission, “Entry/Exit System (EES),” 2021.

[11] C. Wenhao and W. Min, “Regulating the use of facial recognition technology across borders: A comparative case analysis of the European Union, the United States, and China,” *Telecommuncations Policy*, 2023.

[12] Innovatrics, “How the accuracy of facial recognition technology has improved over time,” 2020. [Online]. Available: https://innovatrics.com/trustreport/how-the-accuracy-of-face-recognition-technology-has-improved-over-time/.

[13] R. Bratulescu, “BorderProject,” [Online]. Available: https://github.com/razvanbratulescu/BorderProject.

[14] K. S. Ainampudi, S. Kadavakollu, S. P. Kothamasu and B. Vasantha, “An approach for Face Detection and Face Recognition using OpenCV and Face Recognition Libraries in Python,” in *2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, 2023.

[15] “OpenCV Documentation,” [Online]. Available: https://docs.opencv.org/4.x/. [Accessed 15 July 2023].