IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 12 February 2024, accepted 27 February 2024, date of publication 4 March 2024, date of current version 14 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3373264

SURVEY

Face Recognition for Automatic Border Control: A Systematic Literature Review

FADHIL HIDAYAT, (Member, IEEE), ULVA ELVIANI, GEORGE BRYAN GABRIEL SITUMORANG, MUHAMMAD ZAKY RAMADHAN, FIGO AGIL ALUNJATI, AND REZA FAUZI SUCIPTO

School of Electrical Engineering and Informatics, Bandung Institute of Technology, Bandung, West Java 40132, Indonesia
Smart City and Community Innovation Center, Bandung Institute of Technology, Bandung, West Java 40132, Indonesia

Corresponding author: Fadhil Hidayat (fadhil_hidayat@itb.ac.id)

This research is partially funded by Program Pendanaan Riset dan Inovasi untuk Indonesia Maju (RIIM) under grant Badan Riset dan Inovasi Nasional (BRIN) with funding amount IDR 170.000.000.

ABSTRACT *Context:* Facial recognition is one aspect of research that still has broad potential for research and development, especially as a security system for automatic border control. There is a significant continuous need to understand the characteristics of system development by considering system complexity and implementation environmental conditions. *Objective:* This research aims to provide in-depth insight and assist researchers and practitioners in developing large-scale facial detection systems for automatic border control. It has a high level of complexity that necessitates special attention to several factors such as real-time system, privacy, variations in facial features, quantity of data, model, and implementation environment. *Method:* This study used a systematic literature review as a research methodology by Kitchenham. The analysis was based on studies published between 2019 and 2023 on using facial recognition in autonomous border control. A systematic analysis of research was conducted by examining 112 scientific studies from 7884 papers in scientific databases. *Result:* Based on research questions, 12 types of threats are often encountered in ABC face recognition, which can be seen in section IV. The method most widely used is deep learning, especially for detecting emotional features and morphing attacks. Apart from that, most datasets used are private because they require collaboration with organizations and are related to privacy. Three remaining issues are encountered in this research, including face recognition methodology, privacy, and architecture for large-scale development. *Future directions:* This study suggests two future research topics to enhance achieving desired results in large-scale and complex advancements in a methodical and structured while upholding privacy ethics.

INDEX TERMS Automatic border control, big data, face recognition, large-scale facial detection.

I. INTRODUCTION

Border control is a service a country's government provides that allows persons, animals, and objects to enter and depart its jurisdiction. The primary purpose is to defend the area from subjects that may be harmful once they have crossed the boundary. Border control operates at country borders [1], [2], [3], offices where immigration and visa paperwork are processed, and places of people and commodities transportation centers such as terminals, stations, ports, and airports. Customs control, immigration restrictions, health protection, and biosecurity are part of the border control activities [4]. This paper focuses on border surveillance operations involving persons entering and exiting a country's authority.

Identity and biometric data can be used to monitor persons in border areas. A person can be recognized mainly through the identity documents someone holds and biometrics matching [5]. Facial attributes, in addition to fingerprints, are biometric data used in person recognition. Manual facial recognition by the officers, results in a high risk of detection mistakes. Therefore, a technology-based solution that can aid

The associate editor coordinating the review of this manuscript and approving it for publication was Sangsoon Lim.

in identifying and recognizing facial biometrics in border regions is required.

Facial identification and recognition techniques are widely used in various sectors, such as verifying employee attendance [6], as an authentication mechanism for specific computer applications, a control system for access to buildings and facilities, and automated immigration gate services.

Several nations worldwide have adopted automated immigration gate services based on identification and face recognition. The approach involves comparing faces in the face database, identity documents brought at the time, and real-time facial pictures. Typically, the facial recognition procedure follows the matching of fingerprint data. Anyone can cross the border with the required documents and match them in the database. However, blocklisted people suspected of causing harm to their region of origin or destination are not allowed to cross the border.

Many issues remain in applying face recognition technology [7] for border control, resulting in a list of watchlists that pass the examination. Document matching does not guarantee that the documents provided are authentic. The data on the blocklist also lacks sufficient and up-to-date information about a person's identification. Furthermore, a person's face might alter with age, making identity and recognition difficult [8]. The use of cosmetic products can also cover certain facial features. Plastic surgery can also change a person's appearance. Wearing a headscarf for religious reasons can make identifying someone by his face more difficult in some countries since it disguises certain facial features. These weaknesses lead to the inaccurate identification and recognition of faces in border control. A framework for identifying and recognizing facial features is needed to build an Automatic Border Control (ABC) system based on facial features.

An enormous and comprehensive amount of data is produced during the recognition phase of facial recognition. The facial recognition system is trained using this data to enhance its performance. Naturally, this will entail gathering, storing, processing, and evaluating the face picture data used to ensure that it is very accurate. A massive data set (also known as ''Big data'') in facial recognition essentially refers to using enormous datasets and additional data analysis methods for analyzing and identifying features. Big data contributes to improved security and effectiveness in automatic border control. However, when developing and using big data for facial recognition, it is crucial to consider the legal implications of using facial data and privacy issues.

To address the research questions in Table 2—which are thought to be necessary for determining the state-of-the-art in the design, development, modeling, and implementation of big data—this study conducted a systematic literature review of prior research. This review was done about numerous of the issues mentioned above. In automatic border control, face recognition is beneficial. This study aims to thoroughly understand big data facial recognition to design a framework to improve facial identification and recognition accuracy for border control applications.

TABLE 1. PICOC formulations.

Population	Face recognition system, face recognition application, big data face recognition system, border gate security system.
Intervention	Detection methods, technique, feature analysis, dataset, framework or architecture, and threat analysis.
Comparison	n/a
Outcomes	Architecture for a successful face recognition system.
Context	Studies in public areas, industry, and academia, small and large datasets

II. METHODOLOGY

The primary objective of the Systematic Literature Review (SLR) is to identify and analyze the current state-of-the-art (SOTA) in the development of a facial identification system using big data. The preparation of the systematic literature review involves three distinct processes, as depicted in Figure 1. The initial phase of a systematic literature review holds significant importance in executing a thorough and meticulous study. The review process necessitates the incorporation of certain essential elements to guarantee its efficacy and comprehensibility. The establishment of a precise research topic or purpose is crucial in the context of systematic literature review. This statement aids in determining the central theme and extent of the review. During the planning phase, seeking input from experts or stakeholders to acquire valuable ideas and viewpoints is standard practice. Establishing a well-organized and contemplative planning phase is the basis for a triumphant SLR, guaranteeing that the review remains concentrated, methodical, and follows the research goals.

A. RESEARCH QUESTIONS

Establishing research questions at the outset is crucial for conducting a systematic review [9]. This is because research questions guide data search, collection, extraction, and analysis [10], [11]. The formulation of research questions is mainly guided by the PICOC framework, as outlined by using the PICOC framework proves advantageous in identifying objectives, conducting investigations, making comparisons, establishing effects and outcomes, and assessing the contextual factors surrounding subjects that interest researchers. The formulation of PICOC derived from this research is presented as follows:

The population is defined as the target for the investigation. In this paper, we investigate face recognition. Intervention means specifying the investigative aspects. We invest in face recognition trends, facial attributes, architecture, techniques and methods, and barriers. Comparison is defined as a

TABLE 2. Research questions.

Code	Research Questions	Motivations
RQ1	Threat in facial recognition system used for automatic border control.	To identify the types of threats that often occur in facial verification systems on automatic border control machines.
RQ2	Automatic border control methods utilizing facial recognition.	To identify the most widely used approaches or methods for automatic border control face verification systems.
RQ3	What are the essential facial features used for face recognition-based automatic border control?	To identify features for the facial recognition system in automatic border control.
RQ4	What datasets can be used to construct a facial recognition model for automatic border control?	To identify the datasets used to build facial identification system models for automatic border control.
RQ5	What are the remaining challenges in automatic border control using facial recognition?	To identify research trends in automatic border control facial identification systems.

comparison of the targeted aspect. Outcome means the effect of the intervention. Context means the environment of the investigation. Based on the PICOC structure, the research questions formed are as follows:

The main objective of this research is to identify research trends and challenges for facial identification systems used in automatic border control machines.

B. SEARCH STRATEGY

A search strategy is essential in constructing a systematic literature review to ensure the thoroughness of the research [12]. The search technique employed in this study uses both automatic search and manual inquiry to define strings or keywords that will be utilized to find publications in digital libraries. To gather data that is pertinent to the research questions and objectives, this is done. The string formulation employed in this study is as follows:

("Big Data" **OR**"Massive Data" **OR** "Large-scale") **AND** ("Face" **OR** "Facial" **OR** "Feature" **OR** "Expression") **AND** ("Recognition" **OR** "Identification" **OR** "Detection" **OR** "Validation") **AND** ("Automatic" **OR** "Real-time") **AND** ("Border Control" **OR** "Gate Control") **AND** ("Cyber Security" **OR** "Security **OR** "Threat" **OR** "Vulnerable" **OR** "Fraud" **OR** "Morph")

These keywords are selected according to the SLR that will be made. These keywords are searched for in each digital library with details as shown in table 3. The digital libraries to look for are IEEE, Science Direct, ACM DL, Springer, Hindawi, and MDPI. A total of 7884 literature was obtained, with the highest Springer with 3702. All this literature will be filtered to find truly appropriate literature.

TABLE 3. List of related research findings.

No	Sources	Number of studies
1.	IEEE	218
2.	Science Direct	1103
3.	ACM DL	25
4.	Springer	3702
5.	Hindawi	2475
6.	MDPI	361
TOTAL		7884

TABLE 4. Inclusion and exclusion.

Exclusion	A Paper without solid validation should be removed from consideration. Therefore, this paper uses only articles from magazines and journals.
	Articles that are not open access or not accessible through the author account are removed from the list. This paper only covers articles that can only be viewed and read by authors.
	Articles that are not written in English are removed from the list.
	Duplicate papers are considered as one.
	Articles not related to face recognition for automatic border control are removed from consideration.
Inclusion	The papers published from 2019 to 2023 are related to face recognition and automatic border control.
	Only papers with full text.
	Only consider articles that discuss modelling, techniques, architecture, and security related to face recognition systems for automatic border control.

C. STUDY SELECTION

The alignment of the research domain with the main study applies to two stages. First, papers are filtered by title and abstract manually. We read and choose which literature is appropriate to the SLR topic. Second, applying inclusion and exclusion criteria in screening primary studies. These criteria are listed in Table 4. This criterion serves as a filter in the selection and rejection of literature. This criterion is based on literature content, year of release, ease of full access, and language. The content must be in the realm of research questions about face recognition trends, facial attributes, architecture, techniques and methods, and barriers. Year of release, we look at the last 5 years as ideal. The literature we choose can be accessed in full text. The only language we accept is English literature, as shown in Table 4.

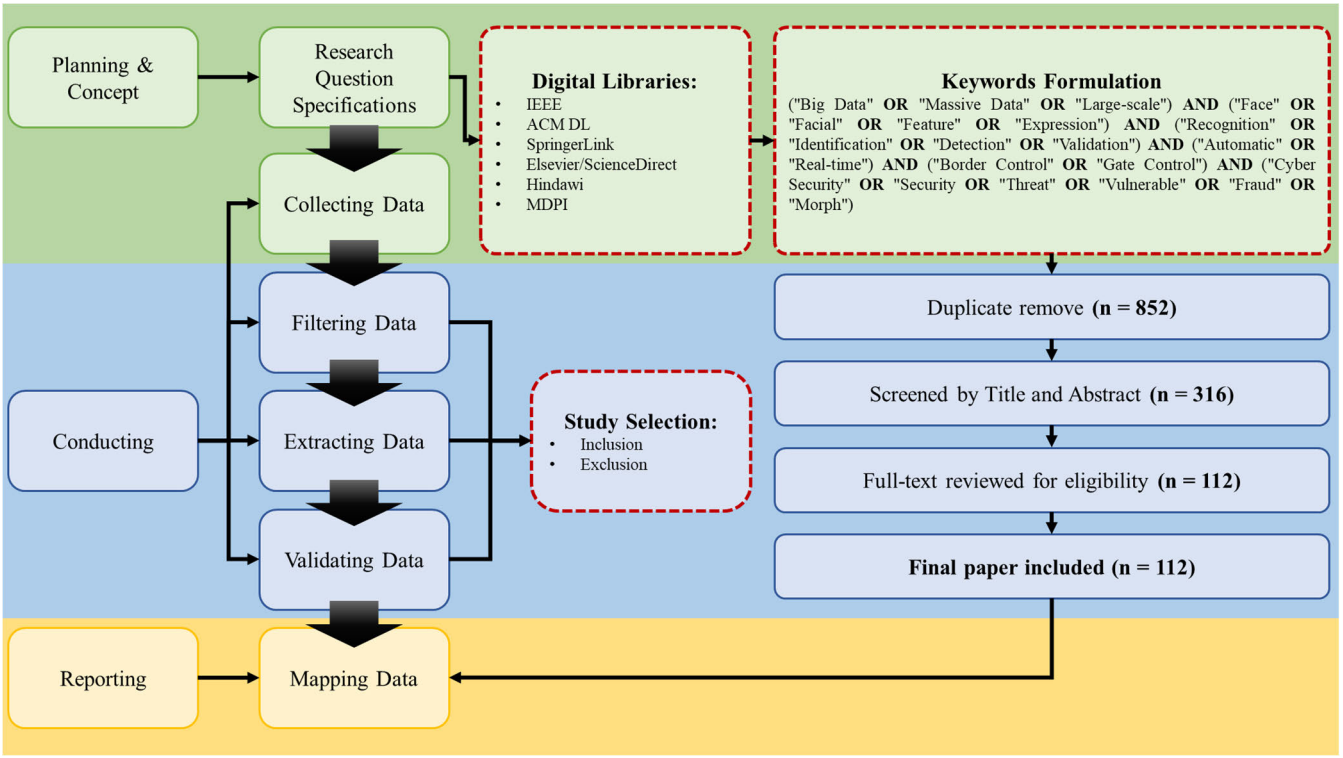

FIGURE 1. Systematic literature review process.

Figure 1. depicts the general flow of the research's systematic literature review approach. SLR is typically carried out in three stages: planning, conducting, and reporting. To ensure that the papers found are consistent with the research targets and objectives, the planning stage includes creating research specifications and gathering data from digital libraries using keyword formulations. The findings of the paper collection completed earlier at the planning stage are filtered, extracted, and validated based on inclusion and exclusion criteria during the conducting stage, which is a part of the research selection process.

This research utilizes a total of 112 papers, as determined by the findings derived from the election study. The literature from IEEE constitutes the most significant proportion, accounting for 36%, followed by Science Direct at 28%. Springer contributes 13% of the literature, while ACM and MDPI have the most minor shares at 8% and 4%, respectively. Hindawi represents 11% of the literature. Based on the findings of the selection study conducted for this research, it is evident that journals represent the predominant medium for scholarly papers, constituting 74% of the total, whereas conferences contribute to a relatively smaller proportion of 25%.

III. DEFINITIONS

A. FACE RECOGNITION

According to a comprehensive study of scholarly literature, variations exist in conceptualizing and interpreting the term "facial recognition." The findings indicate the presence of three distinct categories of definitions, specifically, face detection, face identification, and face verification. The three components mentioned above can be condensed into terminology related to facial recognition. The etymology of this language can be transformed into a systematic approach serving as the foundation for the life cycle of facial recognition advancement. The taxonomy's layout is depicted in Figure 2. To develop a comprehensive face recognition system, it is crucial to thoroughly understand the fundamental concept and precise definition of face recognition. This study aims to enhance the fundamental comprehension of face recognition and get deeper insights into the potential outcomes of implementing face recognition technology. The subsequent passage is a formal elucidation of facial recognition. Specific definitions within this collection have not been paraphrased

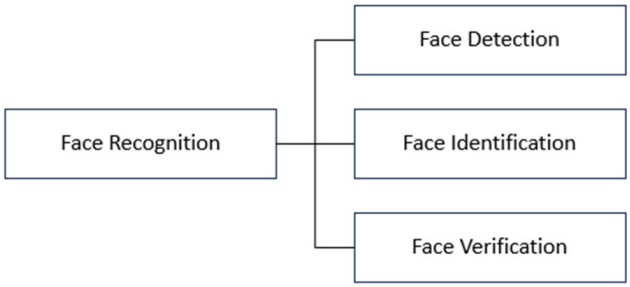

FIGURE 2. Face recognition taxonomy.

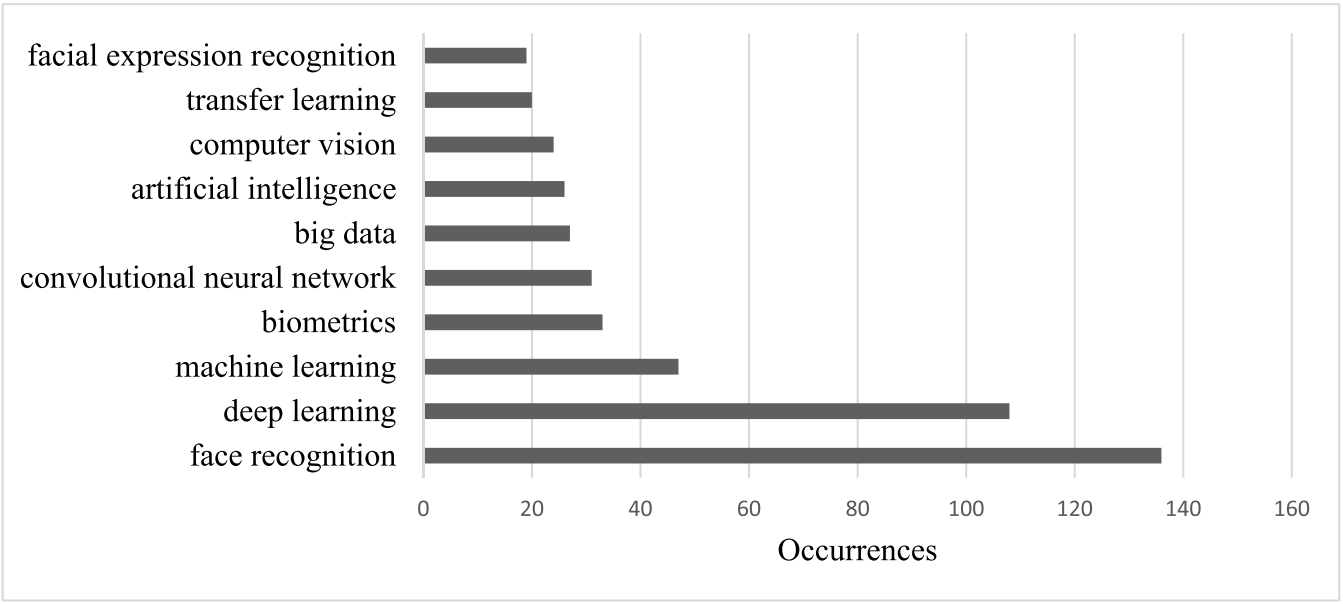

FIGURE 3. Most frequency words.

to preserve the original meaning offered by the respective authors.

1. A face recognition system is a technology to identify and confirm a person from a photo. A three-dimensional face recognition system employs 3D sensors that collect data on a face's shape. A face's surface characteristics, such as the shape of the eye sockets, nose, and chin, may be recognized using this information. The face recognition system is a system that can identify faces with high accuracy based on artificial intelligence technology and deep learning algorithms [13].
2. A face recognition system is a technology that identifies a human face from a digital or video image by comparing the face to a dataset [14].
3. Face recognition is a computer vision technology that analyzes facial feature information for identity identification. In a broad sense, face recognition is divided into face detection and face recognition matching. Face recognition technology is based on the person's facial features and the input face image or video stream. First, determine whether there is a human face. If there is a human face, then further give the position size of each face and the position information of each major facial organ. Based on this information, the identity features contained in each face are further extracted and compared with known faces to identify the identity of each face [15].
4. Face Recognition constitutes visual identification and/or verification of a person using a face picture. Face verification is "a one-to-one mapping of a given face against a known identity (e.g., is this the person?)." [16].
5. Face recognition includes face verification and identification. The former, known as a one-to-one comparison, refers to the authentication of an individual by comparing two face images, and the latter, known as a one-to-N comparison, refers to the identification of a probe face image by comparing it with all faces in the database [17].
6. Face recognition is a subclass of face detection since algorithms first start by detecting a face and then use its features to compare to a set of known faces to recognize the person. Face recognition automatically extracted distinctive facial features, e.g., eyes, mouth, or nose. These features were used to transform the face into a vector, and using statistical pattern recognition techniques, faces were matched [18].
7. Facial recognition is a technology for identifying or verifying a person in images or videos [19].
8. Face recognition includes two sub-tasks: face identification and face verification under the open-set setting [20].
9. Face recognition can be approached as an identification problem or a verification problem [21].
10. Face recognition is an eminent research domain in the computer vision community with ace representation playing the most cardinal role [22].
11. Face recognition is a technique for recognizing individuals through face photographs [23].
12. Facial recognition is a biometric modality that is increasingly used for identification and authentication purposes [24].

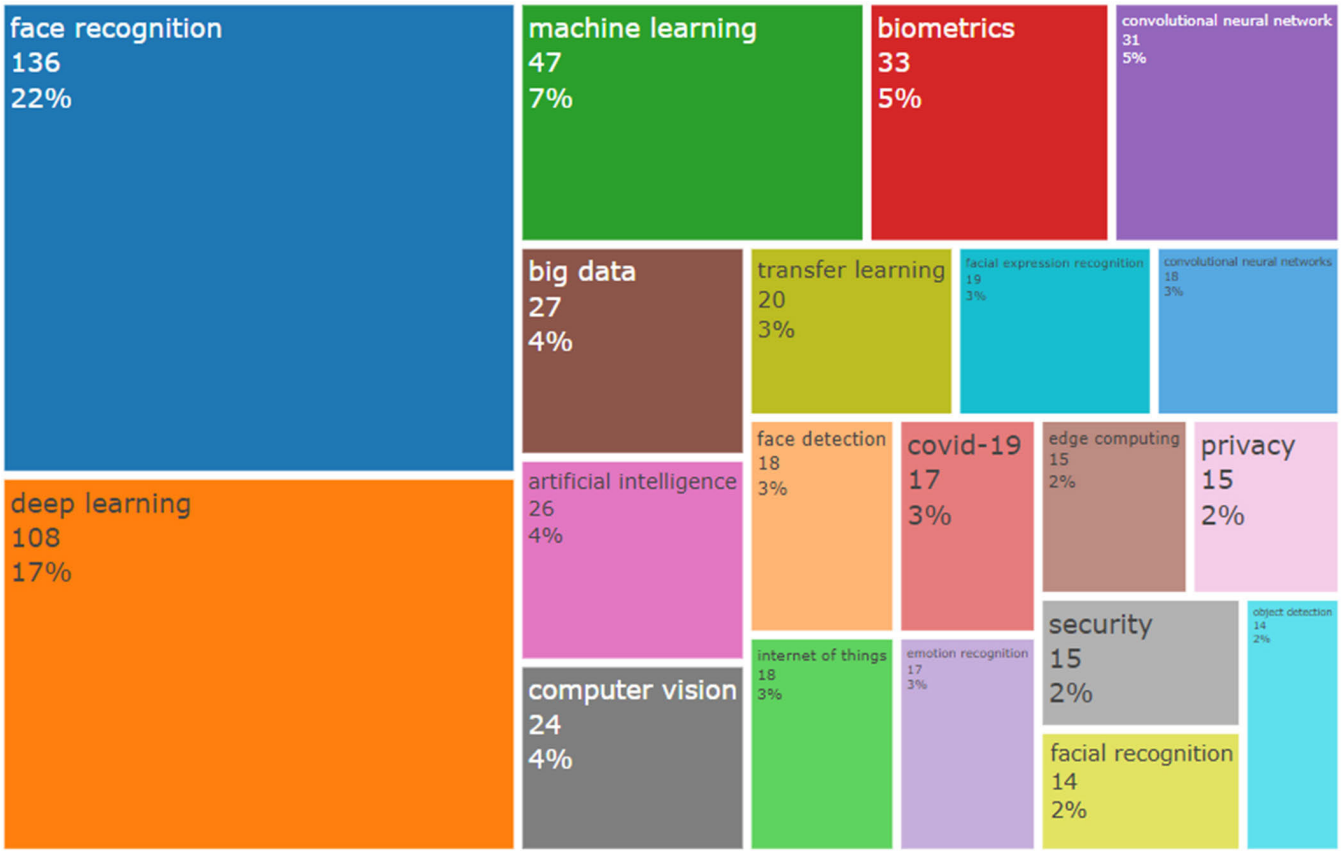

FIGURE 4. Tree map.

13. Face recognition focuses on choosing who this person is in the existing dataset. It is also called one-to-many face identification [25].
14. Face recognition is a perceptual recognition subproblem. For example, people in China constantly identify visual patterns and receive sensory information through their eyes. The brain recognizes these as significant notions. A computer sees an image or a clip as pixels. The computer must figure out what conception each piece of information reflects. It is a graphical modeling recognition problem [26].
15. From a computational viewpoint, the face recognition process is defined as giving still or video images of a scene and identifying one or more people using a stored database of faces. Human face recognition is somehow the same, and the stored database of faces is in our brain, with different degrees of knowledge depending on whether a face belongs to a friend, a famous person, or a person we know by sight [27].

In addition to the identification process, an integral component of the taxonomy pertaining to face recognition encompasses face detection. In the study by [28], face detection is defined as extracting and localizing facial pictures inside video frames. The objective is to ascertain and authenticate a person through specific attributes. The process of detection plays a crucial role within the facial recognition system.

In the context of identity verification, face verification entails comparing facial features to establish a correspondence between an individual's identification and facial references. Reference [29] assert that the verification process involves comparing a presented facial image with a pre-existing facial template, as stated in the study by [3]. The primary objective of the verification process is to establish the authenticity or validity of an individual's identity by utilizing face characteristics as a means of verification. The subsequent passage provides a concise overview of the definition of face verification derived from the findings of a comprehensive survey of scholarly literature.

1. Face verification decides whether two input faces are from the same identity by measuring their similarity in the feature space [20].
2. Face verification is known as the 1:1 matching problem. The identity of the query face is either confirmed or rejected by comparing it with the face data of the claimed identity in the database [21].
3. Face verification is used in authentication based on matching one face image with another (one-to-one) [30].

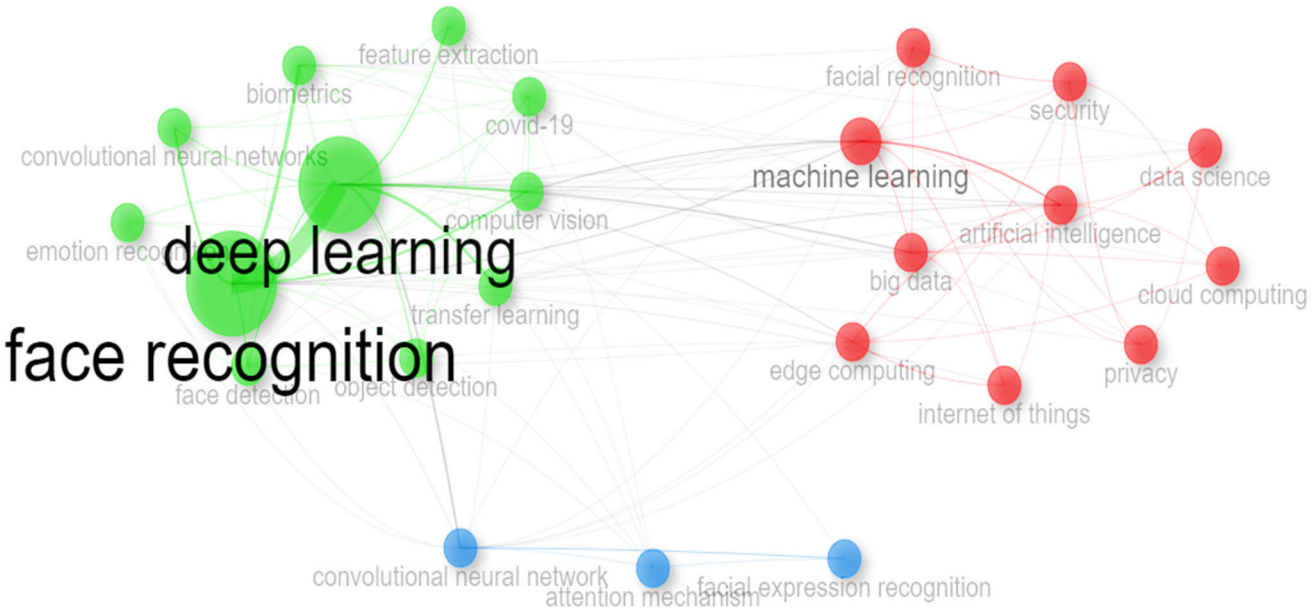

FIGURE 5. Co-occurance network using biblioshiny.

4. Face Verification determines whether a pair of face images or videos belong to the same subject.

B. AUTOMATIC BORDER CONTROL (ABC)

The integration of automatic border control is a component of the existing border security infrastructure found at airports, seaports, and land border crossings. The objective of implementing automatic border control is to enhance the efficiency of border crossing procedures, mitigate congestion and delays, enhance security measures, and optimize the overall functioning of border control operations. Hence, a clear understanding of the precise meaning of automatic border control holds significant importance. Automatic border control refers to a system that utilizes technological advancements to streamline and speed up border crossings. This system employs various automated mechanisms, such as biometric identification and document verification, to authenticate and validate the identity of individuals entering or exiting a country. By reducing the reliance on manual procedures, automatic border control aims to enhance security, efficiency, and accuracy in border management operations.

1. ABC is a fully automated system that performs border checks. The system's essential functions are to authenticate the travel document, establish that the traveler is the rightful holder of the document, query border control records, and, on this basis, automatically verify the entry conditions for Schengen area citizens and Third Country Nationals (TCNs) [1].
2. Automatic identity verification based on stored biometric features with face is selected by the International Civil Aviation Organization (ICAO) as the primary biometric trait for machine-assisted identity confirmation in electronic Machine Readable Travel Documents (eMRTD) [31].
3. ABC systems can have several physical configurations. The most typical ones use electronic gates (e-gates). These devices regulate travelers flow through the border with the use of biometric sensors (e.g., cameras for face recognition and fingerprint reader, travel document readers, scanners, and radio frequency contactless chip readers), as well as physical barriers that let (or not) the traveler to cross the e-gate [5].
4. A system that automatically captures a gate image and computes a similarity score between the gate image and a biometric reference, which is stored in the passenger's electronic Machine Readable Travel Document (eMRTD) chip. If the similarity score exceeds the system's verification threshold, the passenger can cross the ABC gate [32].
5. Border control is comprised of two procedures: an authenticity and integrity check of a travel document and biometric authentication of a traveler based on the biometric record stored in the document. A border guard compares a printed passport photograph with a traveler's face, while an ABC system compares a digital passport photograph with a ''live'' face image using an integrated Automated Face Recognition (AFR) system [33].

As defined earlier, the ABC system is vital in preserving international borders. The ABC system has been specifically developed to carry out three responsibilities outlined by the European Border and Coast Guard Agency [34]. The initial step involves using the ABC system to authenticate travel papers, such as passports and visas [34] [31].

Additionally, the system employs facial biometric data capture to verify the authenticity of the document holder. Subsequently, it assesses the traveler's eligibility to cross the border by considering legal regulations and analyzing the similarity score derived from biometric data analysis [34], [31], [5], [33]. The extensive range of capabilities of the ABC system allows for the independent verification of travelers, encompassing both inhabitants of the Schengen area and TCNs [31].

In addition, the system aligns with the guidelines established by the International Civil Aviation Organization (ICAO) with its emphasis on facial biometrics for machine-assisted verification of identity in electronic Machine Readable Travel Documents (eMRTDs) [5].

In actual applications, ABC systems exhibit diverse physical designs, with electronic gates, sometimes referred to as e-gates, being the predominant form. The e-gates have various biometric sensors, including facial recognition cameras, fingerprint readers, document scanners, and contactless chip readers. According to [32], the effective management of traveler flow at border crossings is achieved by combining these components and implementing physical obstacles. As a result, ABC systems play a crucial role in border control by utilizing biometric technology to verify the authenticity of travel papers and the identity of individuals, consequently strengthening security measures and facilitating the efficiency of border crossings [33].

IV. DATA MAPPING

Data mapping in this study refers to the systematic procedure of identifying and condensing pertinent information from diverse sources relevant to the research subject matter. The primary objective of data mapping is to gather and present data in a manner that allows for a comprehensive understanding of the extent of the literature that has been examined. During this procedure, studies that possess significant qualities will be documented. This study aims to offer a comprehensive assessment of the breadth of material available, aiding researchers in evaluating the significance and caliber of the journal before engaging in a more extensive phase of examination.

Data mapping is crucial in producing a systematic literature review because it establishes a solid foundation for each review phase, including grouping and categorizing literature sources, identifying knowledge gaps, and identifying pertinent trends. Data mapping can effectively mitigate bias during the selection process, enabling researchers to arrive at more precise conclusions regarding the literature studies under review. In addition to its other utility, data mapping facilitates the development of analytical structures that enhance the monitoring of prior research progress. Data mapping is essential in guaranteeing that the review process proceeds in a methodical, unbiased, and all-encompassing manner.

Table 5. provided illustrates the 10 publications that exhibit the highest quantity and relevance to the subject matter under investigation. IEEE Access is the journal that boasts the most articles, precisely 63. Subsequently, the study issue is further explored in Neurocomputing and ACM Computing Surveys, with 34 and 29 publications, respectively. The ACM International Conference Proceedings Series and Pattern Recognition have made substantial contributions, with each publication featuring 26 articles. Furthermore, the research was significantly enhanced by including 23 publications from Procedia Computer Science.

TABLE 5. Top 10 publication and distribution by selected studies.

Sources	Articles
IEEE Access	63
Neurocomputing	34
ACM Computing Surveys	29
ACM International Conference Proceeding Series	26
Pattern Recognition	26
Procedia Computer Science	23
Expert Systems with Applications	18
Proceedings of the ACM On Human-Computer Interaction	18
Image and Vision Computing	15
Journal of Machine Learning Research	14

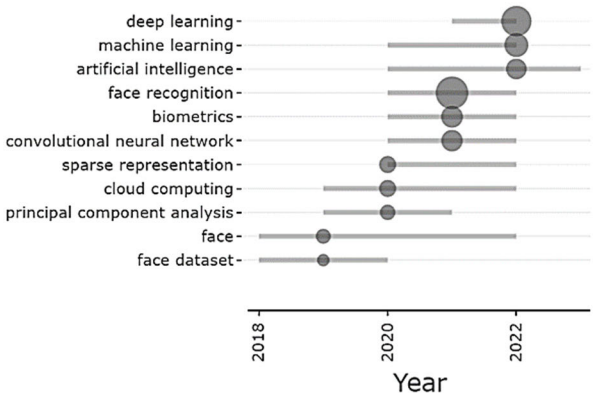

FIGURE 6. Topic trend in automatic border control.

The academic journals Expert Systems with Applications and Proceedings of the ACM on Human-Computer Interaction published 18 articles each. The Journal of Image and Vision Research comprises 14 pieces, whereas the Journal of Machine Learning Research encompasses 15 articles. Table 5 presented herein offers a comprehensive summary of several scholarly works employed to substantiate and examine subsequent investigations.

This study aims to determine the extent of word usage concerning the research issue inside the data mapping procedure. This study aims to assess the degree of pertinence between the title and abstract of prior research and the

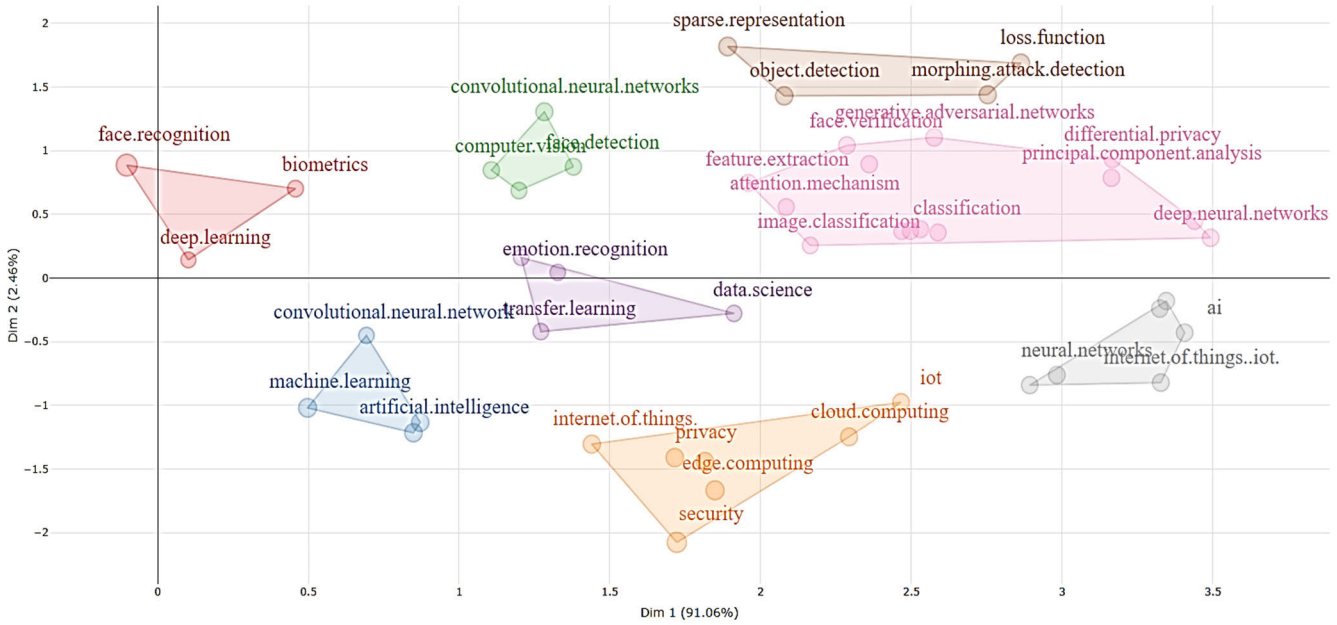

FIGURE 7. Factorial analysis.

conceptual framework of the present study. The visual representation in Figure 3 illustrates the frequency of word usage in each manuscript subjected to evaluation. The application of bibliometric analysis examined the frequency of utilization of these terms. According to the analysis of the provided image, it can be observed that the term ''face recognition'' has been employed approximately 140 times, indicating its prominence as the most frequently utilized word. ''Big data'' currently ranks sixth among the ten most often used words. The findings indicate that there is still room for researching big data in facial detection systems, albeit in limited quantity.

Consequently, there exists significant potential for additional investigation in this area. In addition to this, the present study incorporates data mapping techniques to ascertain the extent of the connection between prior research and the specific research issue under investigation. A tree map visually represents the relevance percentage, as seen in Figure 4.

Face recognition currently comprises the most significant proportion, 22%. Then, machine learning accounts for 7%, and deep learning approaches comprise 17%. Face detection, emotion recognition, the Internet of Things, transfer learning, facial expressions, convolutional neural networks, and COVID-19 all have an average percentage value of 3% on the tree map. On the other hand, security, object detection, privacy, and periphery computing have the most minor importance at 2%. Referring to Figure 6. Facial recognition has emerged as the most prominent study area from 2019 to 2023. This demonstrates the ongoing relevance of research on facial recognition. In addition, deep learning and machine learning are the predominant approaches employed in research establishing automated border control systems.

This research also analyzes data to identify relationships between context elements and data. Based on the Co-occurrence Network analysis using Biblioshiny tools in Figure 5, face recognition, deep learning, and machine learning are the most excellent relationship elements.

The research implementation of factorial analysis is depicted in Figure 7. The objectives are to ascertain the determinants contributing to research outcomes, comprehend the interplay between determinants that mutually affect outcomes, delineate variations, and discern patterns across studies, choose control variables to mitigate bias in meta-analyses, and cluster studies with comparable characteristics to facilitate subsequent analysis.

V. RESULT

A. THREAT IN FACIAL RECOGNITION SYSTEM USED FOR AUTOMATIC BORDER CONTROL

Various types of attacks and challenges have emerged in border security that utilize facial biometric authentication as outlined in Table 6. These encompass presentation attacks, including both biological-based and document-based techniques, such as the morphing attack, which involves the manipulation of images to create a blended representation for verification [35], [36], [31]. Adversarial attacks, on the other hand, involve perturbing images to generate adversarial examples or using patches to create well-designed perturbations [4]. Live spoofing scenarios can mislead recognition algorithms by providing deceptive visual data [37]. Moreover, inconsistencies in matching rates have been observed due to factors like age and nationality [3]. Network availability issues, especially wireless connectivity, have hindered timely matching and verification processes [3]. To further

TABLE 6. List of threats in facial recognition system used for automatic border control.

No	Threats	Description	Author
1.	Presentation Attack	A presentation assault can be characterized as assuming the identity of a particular individual, commonly referred to as the victim, who possesses the necessary authorization. Multiple methodologies exist for executing such assaults, categorized into two main types: biological-based attacks and document-based attacks.	[35]
2.	Morphing Attack	The morphing assault involves manipulating and storing a morphed image within the electronic Machine Readable Travel Document (eMRTD). This morphed image combines the actual owner's ID card (accomplice) with the surrogate or imposter (criminal).	[36]
3.	Morphing attack	The morphing attack is a technique that combines facial photographs from two individuals, resulting in a "morphed" image that can be used to authenticate both individuals involved. However, the biometric data obtained from the morphing image bears enough similarity to the genuine data of both individuals, resulting in a successful identification by the Facial Recognition System (FRS).	[31]
4.	Adversarial attack	Adversarial assaults are performed by introducing perturbations to probing images, resulting in the creation of adversarial examples. Another approach involves strategically using adversarial patches to induce perturbations in certain image sections. Most prior research on adversarial attacks operates assuming that the assailant gains unauthorized access to the system, possessing knowledge of the deep learning model's architecture and parameters.	[4]
5.	Live Spoofing	Live spoofing is a deliberate act in which an individual manipulates or duplicates visual data to trick an activity recognition algorithm. This manipulation leads to the algorithm incorrectly detecting the false data as a legitimately performed action. An instance of misleading or redirecting intelligent systems can occur when a pre-recorded video is played on a smartphone screen within the field of view of a security camera.	[37]
6.	Morphing attack	Facial Morphing Attacks (FMA) undermine the distinctiveness of facial biometric identifiers. The core concept behind FMA involves the creation of a blended image that combines face biometric traits from several individuals.	[2]
7.	Inconsistent matching rate due to certain factors (Passengers under 29 and over 70 years of age had lower match rates and matching of certain nationalities contributed to a low biometric confirmation rate.)	Individuals younger than 29 years old comprised 18 percent of the total number of passengers, although they constituted 36 percent of all passengers whose photographs were erroneously rejected. Similarly, it may be observed that those aged 70 and above constituted 4% of the total passenger population yet accounted for 10% of the passengers whose photographs were erroneously rejected. Numerous photo discrepancies can be attributed to temporal and age disparities between the original photograph kept in the gallery and the live snapshot captured on the day of travel. The temporal disparity can span multiple years, during which alterations in an individual's facial characteristics may have occurred. Additionally, variation in lighting could cause dramatic changes in facial appearance.	[3]
8.	Network availability issues	Technical difficulties were attributed to challenges related to network connectivity and the maintenance of connections with the TVs (traveler verification service). Moreover, the regular interruptions in the system had an adverse impact on the process of taking facial images and the automated exchange of data between the cameras and TVs. Consequently, this led to delays in the prompt matching and verification of responses. The U.S. Customs and	[3]

TABLE 6. *(Continued.)* **List of threats in facial recognition system used for automatic border control.**

		Border Protection (CBP) organization significantly depends on wireless networks, hence attributing the primary factor contributing to suboptimal connectivity. Furthermore, there was a decrease in network performance seen during moments of high demand, coinciding with many passengers being connected to the wireless network. Utilizing a physical connection for stability is crucial, as wireless connectivity is not deemed the optimum alternative for CBP.	
9.	Bypassing the use of facial recognition	Due to the reduced boarding time, CBP has permitted many airlines to bypass biometric processing to expedite the boarding process. Instead, these airlines are allowed to proceed with the usual procedure of scanning boarding cards, a practice that is also preferred by the airlines themselves as it aligns with their goal of ensuring timely departures. Nevertheless, this situation can be difficult as continuously allowing airlines to revert to conventional boarding processes may develop into an ingrained practice.	[3]
10.	Passengers' willingness to use biometrics and the issue of privacy	Photos should be transferred using a template rather than the image itself. The template comprises a series of binary digits, specifically 1's and 0's, that have undergone robust encryption to ensure security. An interviewee emphasized that these encrypted binary digits cannot be deciphered or reconstructed into a picture by reverse-engineering methods. Furthermore, the U.S. CBP asserts that after the departure of an aircraft, the photographic records of individuals are expunged from the database. According to the respondent, travelers often lack awareness of potential mishaps and hazards, leading to dissatisfaction with procedures such as having their photographs taken.	[3]
11.	The need for a human expert and counterproductive MTL implementation	The compliance verification of a single-face image is predominantly conducted through visual inspection by human experts, occasionally with an automated system, due to the substantial number of requirements outlined in the International Standard Organization (ISO) or International Civil Aviation Organization (ICAO) standards, which amounts to over 30. The lack of agility in crucial scenarios, such as international airports, hinders the efficient execution of this work, which is carried out on a massive scale daily. Hence, the complete automation of this work remains a continuous demand, potentially mitigating the necessity for human expertise and expediting the document generation process. Multitask Learning (MTL) can be harmful in certain instances as it disregards a valuable source of knowledge present in several real-world situations, namely the information embedded in other tasks within the same domain.	[38]
12.	Face Morphing	The process of face morphing, which involves combining face images of two or more individuals, can result in creating a composite face image that resembles the facial features of all individuals included in the process. Using a picture as a point of reference within a document is commonly known as a face-morphing attack, as it facilitates the unauthorized dissemination of documents among several users. Previous studies have demonstrated the efficacy of morphing assaults within ABC systems, wherein a wanted criminal can illicitly traverse a border by assuming a deliberately selected (i.e., incorrect) identity.	[39]

TABLE 7. List of automatic border control as a whole system.

No.	ABC Methods	Explanations	References
1.	Illumination Techniques	This study aims to propose a design for an automated border control system that utilizes face recognition technology using several lighting techniques, including halogen light, LED, near-infrared (NIR) lighting, and fluorescent lights. The primary goal of this design is to enhance the performance and efficiency of face identification processes.	[1]
2.	The security assessment of the Border Control system	The Assessment of a biometric program in the form of border control at an airport.	[3]
3.	De-morph	The de-morph-based approach involves capturing chip and Vivo photos for demorphing. Subsequently, the resulting output is utilized for identity verification, explicitly using the Vivo image. The ultimate result will determine the information's authenticity (safety) or falsity (presence of counterfeit threats).	[36]
4.	On-the-fly Presentation	The proposed framework encompasses various components, including a capture module responsible for acquiring photographs or videos in the form of frames, a tracking module for monitoring the movement of subjects, a detection module for identifying potential presentation attacks, a verification module for authenticating the identity of individuals, a presentation attack detection (PAD) module for distinguishing between genuine and fraudulent attempts, and a repository model for storing relevant data.	[5]
5.	Web-based experiment by examining human	This study aims to evaluate the efficacy of identity checks conducted by border control officers within the context of the border control system.	[33]
6.	Comparison of Morphing Attack Detection	The author's examination of Mutual Assured Destruction (MAD) is categorized into multiple sections, which include the comparison between online and offline detection scenarios involving the use of closed-circuit television (CCTV) and electronic Machine Readable Travel Documents (eMRTDs) as input to ascertain the degree of correspondence between individuals. The distinction between deep and non-deep classification pertains to the methodology employed for feature extraction and is a fundamental aspect of nearly all classification tasks following the advent and prevalent adoption of deep convolutional neural networks (DCNN) in recent times. A body of literature on Mutually Assured Destruction (MAD) exists.	[31], [40]
7.	Generative Adversarial Network (GAN)	The implementation of the method comprises various components, including the primary objective of the generator, which is to generate photos that intentionally introduce contradictory visual cues, leading to misclassification by the facial recognition system. The discriminator's objective is to assess the similarity between authentic facial images and the generator's generated facial images using spectacles. A facial recognition system is employed to quantify the degree of resemblance between two facial images.	[4]
8.	Multichannel	The proposed framework comprises four channels: ApparelNet, A-Net, OneDetect, and RSFS. ApparelNet is responsible for verifying both essential and additional equipment. A-Net measures anthropometric light biometrics, while OneDetect predicts global light biometrics. Lastly, RSFS constructs a collection of highly relevant and supportive light biometrics for verification.	[41]
9.	Human Activity Recognition (HAR)	The analysis of human activities can accomplish the identification of live spoofing.	[37]
10.	PERSONA (Privacy, Ethical, Regulatory, and Social No-	This paper examines the difficulties of implementing biometrics-based solutions in a gateless border crossing point scenario. This encompasses the requisite protocols for evaluating social	[42]

TABLE 7. *(Continued.)* **List of automatic border control as a whole system.**

	gate crossing point solutions Acceptance)	acceptability, ethical considerations, privacy concerns, and relevant rules, emphasizing the implications for passengers and border control authorities. Additionally, it considers the potential risks associated with biometric technology concerning fraudulent operations. Various biometric modalities are employed in border control systems, encompassing voice, facial features, signatures, hand geometry, retinal patterns, fingerprints, and iris scans.	

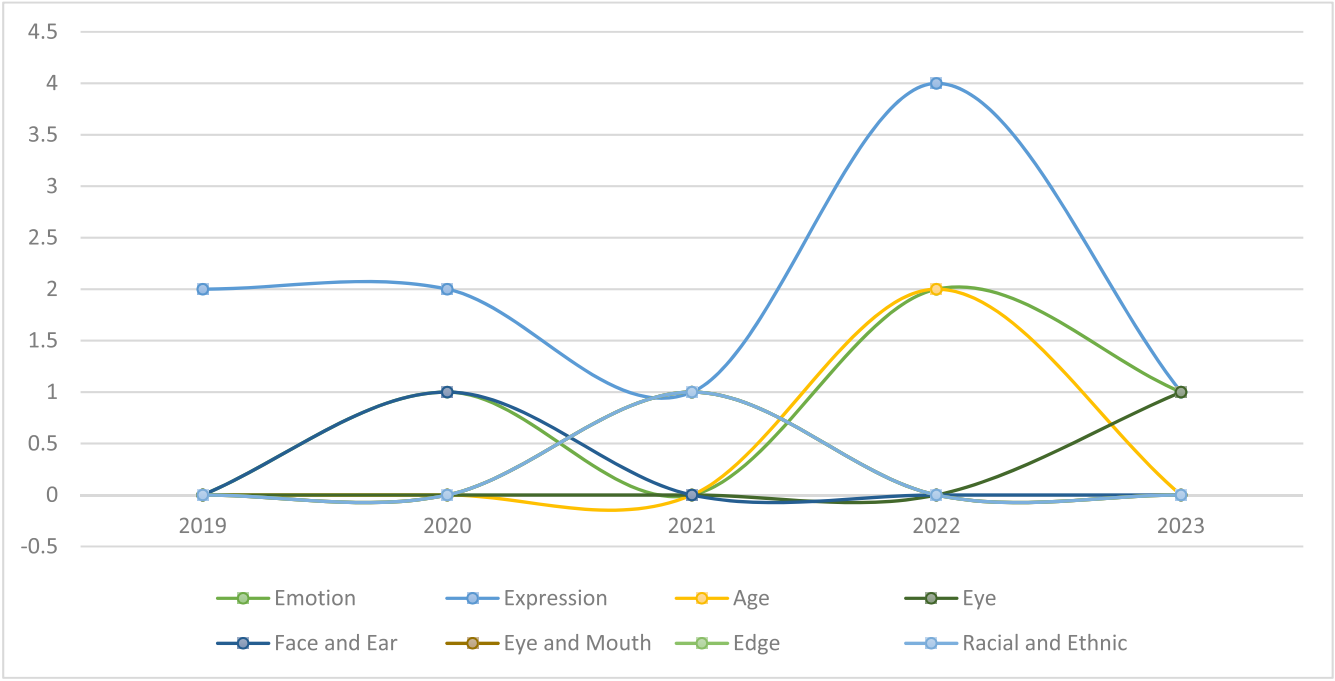

FIGURE 8. Facial figure analysis.

complicate matters, the bypassing of facial recognition by airlines to save time presents a challenge [3]. Passenger willingness to embrace biometrics while addressing privacy concerns remains pivotal [3]. Finally, the need for human experts in compliance verification and the counterproductive implementation of Multitask Learning (MTL) in critical scenarios underscore the ongoing pursuit of automation in the face of evolving threats [38]. In particular, the face-morphing attack has demonstrated its effectiveness in breaching automated border control systems, highlighting the importance of addressing these vulnerabilities to enhance border security and document integrity [39].

B. AUTOMATIC BORDER CONTROL METHODS UTILIZING FACIAL RECOGNITION

The application of facial recognition involves the utilization of diverse methodologies. This study categorizes the collected development methods into two distinct groups: ways for applying face recognition in autonomous border control and methods for developing the face recognition system itself. The categorization examined the similarities and differences among each facial recognition system. Tables 7 and 8 provide a comprehensive description of the methodologies employed in the domain of face recognition.

The facial recognition methods and algorithms utilized in Automatic Border Control are tailored to address the specific challenges encountered in each case study. Deep learning has emerged as a prominent technique in facial recognition due to its ability to achieve high levels of accuracy.

C. WHAT ARE THE ESSENTIAL FACIAL FEATURES USED FOR FACE RECOGNITION BASED AUTOMATIC BORDER CONTROL?

The significance of facial attributes is undoubtedly overstated in the context of face recognition for automated border control. By efficiently discerning and authenticating individuals, this technology enhances the quality of travel experiences and security protocols. As a result, it functions as an invaluable resource for modern border control agencies.

Face recognition for automated border control employs fundamental facial characteristics, including face detection,

TABLE 8. List of algorithmic side-face recognition methods.

No.	Methods	Explanations	References
1.	Deep learning	Deep learning has yielded superior accuracy rates in face recognition tasks by utilizing extensive datasets for model training.	[6], [18], [43], [17], [44], [45], [46],
2.	Convolutional Neural Network (CNN)	CNN has the capability to enhance the performance of facial recognition systems, even when dealing with photos of low quality.	[47], [48]
3.	Dual Generation	This study aims to explore the capability of generating novel samples from noise in images while maintaining two fundamental properties: identity diversity and identity consistency.	[49]
4.	OpenCV	Cascade classifier	[14]
5.	Attention Development Network (AND)	ADN recognizes multiscale faces without detection	[50]
6.	Augmentation	Mitigate the effects of uneven distribution of attributes.	[51], [52]
7.	Multitask Cascade Convolutional Neural Network (MTCNN)	A deep learning-based approach to detect faces and landmarks that has an accuracy rate of above 92% for side faces and 96% for front faces.	[53]
8.	SVM	The individual possesses the capability to categorize and effectively address multi-classification issues independently. Furthermore, they can transform intricate challenges related to facial recognition into high-dimensional space, enabling linear classification inside the state space.	[54], [15]
9.	E3FRM	E3FRM is used to identify the match cases and the value of the acquired picture concerning the match cases.	[55]
10.	Goldstein branching method	Enhance the efficacy of three-dimensional (3D) facial reconstruction.	[56],
11.	GoogLeNet-M	The GoogLeNet-M architecture enhances network efficiency by implementing network simplification techniques and incorporating regularization and migration learning methods, improving precision.	[57]
12.	FaceNet	The proposed method exhibits the capability to substantially enhance the precision of facial identification while effectively addressing challenges such as occlusion, blur, variations in illumination, and diverse angles of head attitude.	[58]
13.	Adaptive Fine-Tuned AdaBoost (AFTA)	AFTA Enhancing facial recognition capabilities within the Hadoop processing framework.	[26]

face alignment, feature extraction, face verification and matching, and liveness detection. Based on a systematic literature review, several features are used in facial recognition, including facial emotion, facial expression, face and ear, eye, and mouth, racial and ethnic, age, eye, and edge. The quantity of papers devoted to the general topic of facial feature utilization in face recognition is illustrated in Figure 8. In comparison to seven other topics, facial expressions have garnered among the most research attention in the past five years, as evidenced by this graph. Since humans possess a wide range of facial expressions, including wrath and smile, the task of distinguishing and comprehending these expressions presents a fascinating challenge. Additionally, the degree of variation in an individual's facial expression will persistently fluctuate over time, thereby exacerbating the challenge associated with facial expression recognition. Facial expressions are carried out to analyze the level of emotion a person shows, for example, the level of sympathy in children [59].

Besides that, developing an emotion parsing module aims to capture inclusion and exclusion characteristics in facial expressions [60]. To detect indications of emotions such

TABLE 9. List of dataset used in automatic border control.

No	Dataset	Detailed	Reference
1	Private	A set of data that is not generally accessible to the public, other researchers, or the general population	[6], [74], [14], [44], [56], [15]
2	CelebA	A massive face attributes dataset with over 200K celebrity photos and 40 attribute annotations per image. Available at: https://www.kaggle.com/datasets/jessicali9530/celeba-dataset	[18], [53], [55], [75]
3	SUN	The extensive Scene UNderstanding (SUN) database is a large-scale scene recognition taken from abbey to zoo. SUN Database are proposed by Xiao et.al in 2010 which contains 899 categories and 130,519 images. Available at: https://spritz.math.unipd.it/projects/BLUFADE/	[18]
4	VGGFace2 2D	VGGFace2 is a dataset developed by Cao et.al in 2018 which contains 3.31 million image data from 9131 subjects, with an average of 362.6 images per subject. Images were downloaded from Google Image Search and have many variations in pose, age, lighting, ethnicity, and profession. This dataset is available at: https://www.kaggle.com/datasets/yuzhangzhang/vggface2	[47], [55], [75], [76]
5	Texas FR3D	The Texas 3D Face Recognition Database (Texas 3DFRD) was developed by Gupta et.al. in 2010. This dataset contains 1149 facial images in both 2 dimensions and 3 dimensions. More information about this database is available at https://live.ece.utexas.edu/research/texas3dfr/	[47], [77]
6	Bosphorus	Bosphorus Database for 3D Face Analysis was developed by Savran et.al. in 2008. This database consists of emotions divided into 6 basic categories, variations in head poses, and various types of facial occlusion. More information about this database is available at https://link.springer.com/chapter/10.1007/978-3-540-89991-4_6	[78]
7	FRGCv2	The Face Recognition Grand Challenge (FRGC) version 2 database is a continuation of the FRGC version 1 database which has been developed since 2004. This database consists of high-resolution 2D images and 3D images of a person. Information regarding this database can be accessed at https://www.nist.gov/programs-projects/face-recognition-grand-challenge-frgc	[79][80]
8	FIFD	Cui et al. developed the FIFD face database in 2019, and it contains ID photographs in addition to pictures from the real-world for a person. The FDID dataset has 100 celebrities' ID images and roughly 1000 stills or live shots. Publications related to this dataset can be accessed via https://www.sciencedirect.com/science/article/abs/pii/S0030399217311143	[46]
9	CASIA NIR-VIS 2.0	CASIA Near infrared vs. Visible light (NIR-VIS) face recognition database was developed by Li et.al. in 2013. This database consists of NIR-VIS images from 725 subjects taken at 4 different times and in different seasons. Each subject has 1 - 22 VIS images and 5 - 50 NIR images. The VIS image format is JPEG and the NIR image format is BMP. Documentation related to this database can be accessed via https://pythonhosted.org/bob.db.cbsr_nir_vis_2/	[81]
10	BUAA-VisNir Face	The BUAA-VisNir database was developed by Huang in 2012 which consists of 150 subjects with 40 images per subject. This database consists of 13 pairs of VIS-NIR images and there are 14 VIS images with different illuminations.	[82][83]
11	IIIT-D Sketch Viewed	The IIIT-D Sketch database is facial sketch image data divided into 3 parts: viewed sketch, semi-forensic sketch, and forensic sketch. In the viewed sketch there are 238 facial sketch image data based on facial images taken from various sources. The semi-forensic sketch has 140 digital images based on the sketch maker's memory. In the forensic sketch database, there are 190 facial sketch data obtained from eyewitness statements. This	[84]

TABLE 9. *(Continued.)* **List of dataset used in automatic border control.**

		database can be accessed via https://iab-rubric.org/index.php/iiit-d-sketch-database	
12	Tufts Face	The Tufts Face Database was developed by Panetta in 2018. This database has more than 10K images of 74 female faces and 38 male faces from 15 different countries. A person's age in this database is between 4 - 70 years. This dataset consists of 7 modalities: visible, near-infrared, thermal, computerized sketch, LYTRO, recorded video, and 3D images. This database can be accessed via https://github.com/kpvisionlab/Tufts-Face-Database	[85]
13	UMDFaces	This database consists of 2 parts, namely still images of 367,888 facial annotations in the form of bounding boxes from 8,277 subjects, and video frames of more than 3.7M facial annotations in the form of bounding boxes from 22,000 files. videos of 3,100 subjects. Information related to this database can be accessed via http://umdfaces.io/	[86], [87]
14	LFW (Labeled Faces in the Wild)[88]	The Labeled Faces in the Wild (LFW) database was developed by the University of Massachusetts, Amherst, and consists of 13,233 images from 5,749 people and is still growing. This database can be accessed via http://vis-www.cs.umass.edu/lfw/	[88]–[91]
15	CPLFW	Contains 5.749 identities with 11.652 images in total.	[88]
16	CALFW	Contains 5.749 identities with 12.174 images in total.	
17	CFP-FP	Contains 500 identities with 7000 images in total.	
18	AgeDB-30	Contains 568 identities with 16.488 images in total.	
19	UCCS (UnConstrained College Students)	Contains more than 14,016 images.	[92]
20	SCface (Surveillance Cameras face)	Database contains 4,160 static images (in visible and infrared spectrum) of 130 subjects.	[93]
21	ORL dataset	Includes 400 pictures from 40 different subjects. Various lighting conditions, facial expressions (open/closed eyes, smiling/not smiling), and facial details (glasses/no glasses) were used when taking pictures of certain subjects at different times. Each picture featured a uniformly dark background and persons standing straight ahead, allowing for slight deviation to either side. Each image has 256 grey levels per pixel and is 92 by 112 pixels.	[94], [95]
22	MegaFace	Contains 530 identities with 1M images in total.	[88]
23	MultiPIE	Consists of face images of 337 subjects taken under different pose, illumination and expressions.	[96]
24	CASIA-WebFace	The CASIA-WebFace dataset is a sizable collection of online facial images. There are 494,414 photos and 10,575 topics in it.	[97]
25	SoF (the Specs on Faces)	Contains 42,592 (2,662×16) images for 112 persons (66 males and 46 females).	[98]
26	M2FPA	The M2FPA dataset involves 397,544 images of 229 subjects with 62 poses (including 13 yaw angles, 5 pitch angles and 44 yaw-pitch angles), 4 attributes and 7 illuminations.	[99]
27	IFRT	Contains 242K identities with 1.6M images in total.	[100]
28	IJB-A	There are 20,412 frames, 11.4 photos, and 4.2 films per topic in the IJB-A database's 5397 images and 2042 videos of 500 different subjects.	[97]
29	IJB-B	An expansion of IJB-A, the IJB-B dataset contains 1845 people, 21.8K still photos (including 11,754 face images and 10,044 non-facial images), and 55K frames from 7, 011 videos.	[97], [88]
30	IJB-C	A further expansion of IJB-B, the IJB-C dataset contains 3531 subjects with 31.3K still images and 117.5K frames from 11,779 videos.	
31	RFW	The Racial Faces in-the-Wild (RFW) dataset [36] is a test database for examining racial bias in face recognition. Caucasian, Asian, Indian, and	[97]

TABLE 9. *(Continued.)* **List of dataset used in automatic border control.**

		African testing subsets are the four created, and each has roughly 3000 people with 6000 image pairs for face verification.	
32	WIDER FACE	The WIDER FACE dataset consists of 393,703 labeled face bounding boxes in 32,203 images (best view in color).	[101]
33	Face-96	Contains 20 images per individual with image resolution 196 x 196 pixels (square format).	[102], [95]
34	Face-95	Contains 20 images per individual with image resolution 180 by 200 pixels (portrait format).	[95]
35	Frontal	Included 475 subjects, each with a frontal and profile image, for a total of 950 face images.	[103]
36	MS-Celeb-1 M	Consists of 100K identities, and each identity has about 100 facial images	[104]
37	YoutubeFace	Contains 3,425 videos of 1,595 different people.	[105]
38	IMDB Wiki Face	Contains more than 500,000 images with all the meta information.	[106]
39	FDDB	Contains a total of 5171 face annotations, where images are also of various resolution, e.g. 363x450 and 229x410.	[29]
40	AFW	contains 203 images with 473 labeled in the various lighting, backgrounds, and facial challenges.	[107]
41	CACD	Contains 163,446 images from 2,000 celebrities collected from the Internet.	[108]
42	MALF	Contains 5,250 images collected from the Internet and ∼12,000 labelled faces.	[109]
43	MAFA	Contains 30, 811 Internet images and 35, 806 masked faces.	[110]
44	4K-Face	Contains 5,102 images with more than 30,000 annotated boxes are acquired in total.	[111]
45	DARK FACE	Contains 6,000 real-world low light images, 9,000 unlabeled low-light images, and 789 paired low-light/normal-light images.	[112]
46	Face Image with Marked Landmark Points	Contains 7049 facial images and up to 15 key points marked.	[113]
47	ImageNet	Contains 14,197,122 annotated images.	[114]
48	CAS-PEAL	Contains 99,594 images of 1040 individuals (595 males and 445 females) with varying Pose, Expression, Accessory, and Lighting (PEAL).	[115]
49	ATR Jaffe database	There are 10 female participants' faces in the ATR Jaffe database total 215 and have a resolution of 256 x 256.	[45]
50	AR database	The 3120 facial photos of 65 men and 55 women in the AR collection were taken throughout two different periods.	[45]
51	GBU	The Good, the Bad, and the Ugly Face Challenge is its entire name. This dataset has three divisions, and each partition has pairs of pictures with varying levels of difficulty based on the results of the top three finishers in the FRVT 2006.	[112]
52	MS1MV2	Contains 5.8M images from 85k celebrities.	[88], [116]

as anger, fear, happiness, sadness, disappointment, surprise, or neutral [61], [62], [63], [64], [65], [66], [67], [68], [69] two methods can be applied such as facial action coding system and emotional expression prototype [62]. Apart from that, Spatiotemporal CNN can also obtain video data information for each frame and the information relationship between frames well [70]. In age detection (age-invariant), age dramatically influences the appearance of a person's face, resulting in variations between faces. What needs to be done to overcome this is to extract features and synthesize faces simultaneously because both provide mutual benefits to each other [8]. The ear in face detection has a fairly good level of stability in the 3D structure and is almost not affected by aging and changing facial expressions [71]. Meanwhile, determining racial and ethnic requires a database containing the characteristics of each racial and ethnic group based on facial features, expressions, gender and so on [72]. Facial recognition attributes such as skin and

eyebrows have stable characteristics but also have security risks [73].

D. WHAT DATASETS CAN BE USED TO CONSTRUCT A FACIAL RECOGNITION MODEL FOR AUTOMATIC BORDER CONTROL?

Datasets are of paramount importance in training and evaluating facial recognition algorithms. The significance of datasets in developing facial recognition systems lies in the necessity of ample data for training machine learning models to effectively identify pertinent facial attributes. Furthermore, including a diverse dataset with several situations and variations can enhance the model's generalization ability, facilitating optimal performance. Datasets are employed to assess and appraise the model's efficacy, ascertaining its accuracy and system performance. Utilizing a more significant number of datasets contributes to enhancing the model's performance during the fine-tuning training procedure. Moreover, face datasets can serve to evaluate the efficacy of security measures and detect potential vulnerabilities or privacy concerns inside facial recognition systems. Table 9 provides a comprehensive overview of the various types of datasets utilized in developing a facial recognition system designed explicitly for Automatic Border Control.

Based on the results of the review, the use of the dataset is adjusted to the needs and research objects. Therefore, most studies choose private datasets because they collaborate with certain institutions. However, private datasets sometimes have incompleteness in representing conditions, so they can cause bias if the system is not managed well.

E. WHAT ARE THE REMAINING CHALLENGES IN AUTOMATIC BORDER CONTROL USING FACIAL RECOGNITION?

The objective of the remaining issues is to identify knowledge deficits that have the capacity to be further investigated. Based on the result of the four research queries, the following gaps required additional investigation:

1. Face Recognition Methodology.

Methodology is a fundamental procedure that is necessary when designing a system. As uncovered in the first research question, the divergent interpretations of the face recognition process indicate that a unified understanding of the system development process is necessary for face recognition. The objective is to offer methodical direction to facilitate a more structured approach to attaining the intended outcomes.

2. Privacy.

Face recognition utilizes facial data as a verification instrument; this, of course, raises numerous privacy and security concerns. Even though facial recognition technology can essentially function as a security system, this can give rise to concerns concerning privacy ethics.

3. Architecture for large-scale development.

Face recognition has considerable potential for implementation on a large scale. Nonetheless, this development necessitates a suitable architectural design to ensure an efficient execution despite environmental variations during implementation. The architecture under consideration incorporates every necessary component in the implementation environment, encompassing data, systems, and auxiliary devices.

VI. FUTURE DIRECTION

Based on the results of the remaining issues in research question 5, this research tries to analyze and develop further the findings described in the remaining issues. Two future works will be carried out in this research: developing a methodology for face recognition and architectural design in developing face recognition on a larger scale. The development scale in question requires integrating and combining technology regarding data, systems, and infrastructure while still considering privacy ethics.

VII. CONCLUSION

This study collects, identifies, and analyzes research in facial recognition. This analysis aims to find state-of-the-art research in facial recognition, mainly applied to automatic border control. The 112 papers presented in this research include definitions, features, datasets, approaches, and algorithms used in face recognition and issues that can be used as material for consideration for further research in the field of face recognition. The results obtained from the literature review provide a detailed description of the implementation of facial recognition in automatic border control and provide a brief overview of solutions to problems found in previous research.

There are discrepancies in the definitions of facial recognition among researchers; the definitions vary depending on the research's goals. Thus, it can be inferred from the researchers' arguments that facial recognition technology uses specific identification methods.

Apart from that, there were 12 threats found, but morphing attacks are a type of threat that is a hot topic for researchers because they have an enormous potential to occur, where this type of threat is used as a means of disguising and falsifying identity so that it can pose quite extensive security risks. Several methods used in facial recognition prove the need to adjust the type of threat and the approach offered to overcome the problems to produce the best solution for each type of threat and need.

Furthermore, the analysis found that expression has been the most researched topic in the last five years. Because the expression feature can monitor and analyze individual behavior patterns. Most of the 53 datasets found in this research used public datasets, that reduces the risk of privacy violations. Even though face recognition is a topic that is still a trend for research, there are still several limitations and challenges that are interesting to research better, such as designing a development methodology for the field of face recognition to equalize perceptions between researchers

and developing face recognition architecture in large-scale development but still considering privacy policy.

REFERENCES

[1] J. Sanchez del Rio, D. Moctezuma, C. Conde, I. M. de Diego, and E. Cabello, "Automated border control e-gates and facial recognition systems," *Comput. Secur.*, vol. 62, pp. 49–72, Sep. 2016, doi: 10.1016/j.cose.2016.07.001.

[2] F. Peng, L. Qin, and M. Long, "Face morphing attack detection and attacker identification based on a watchlist," *Signal Process., Image Commun.*, vol. 107, Sep. 2022, Art. no. 116748, doi: 10.1016/j.image.2022.116748.

[3] N. Khan and M. Efthymiou, "The use of biometric technology at airports: The case of customs and border protection (CBP)," *Int. J. Inf. Manage. Data Insights*, vol. 1, no. 2, Nov. 2021, Art. no. 100049, doi: 10.1016/j.jjimei.2021.100049.

[4] R.-H. Hwang, J.-Y. Lin, S.-Y. Hsieh, H.-Y. Lin, and C.-L. Lin, "Adversarial patch attacks on deep-learning-based face recognition systems using generative adversarial networks," *Sensors*, vol. 23, no. 2, pp. 1–29, Jan. 2023, doi: 10.3390/s23020853.

[5] D. Ortega, A. Fernández-Isabel, I. M. de Diego, C. Consde, and E. Cabello, "Dynamic facial presentation attack detection for automated border control systems," *Comput. Secur.*, vol. 92, May 2020, Art. no. 101744, doi: 10.1016/j.cose.2020.101744.

[6] K. Alhanaee, M. Alhammadi, N. Almenhali, and M. Shatnawi, "Face recognition smart attendance system using deep transfer learning," *Proc. Comput. Sci.*, vol. 192, pp. 4093–4102, Jan. 2021, doi: 10.1016/j.procs.2021.09.184.

[7] M. O. Oloyede, G. P. Hancke, and H. C. Myburgh, "A review on face recognition systems: Recent approaches and challenges," *Multimedia Tools Appl.*, vol. 79, nos. 37–38, pp. 27891–27922, Oct. 2020, doi: 10.1007/s11042-020-09261-2.

[8] J. Zhao, S. Yan, and J. Feng, "Towards age-invariant face recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 44, no. 1, pp. 474–487, Jan. 2022, doi: 10.1109/TPAMI.2020.3011426.

[9] E. Lisova, I. Sljivo, and A. Causevic, "Safety and security co-analyses: A systematic literature review," in *Proc. IEEE 43rd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jul. 2019, vol. 1, p. 833, doi: 10.1109/COMPSAC.2019.00122.

[10] Hanavi and F. Hidayat, "Intelligent video analytic for suspicious object detection: A systematic review," in *Proc. Int. Conf. ICT Smart Soc. (ICISS)*, Nov. 2020, pp. 1–8, doi: 10.1109/ICISS50791.2020.9307600.

[11] U. Elviani and F. Hidayat, "Safe and secure railway station? A systematic review," in *Proc. Int. Conf. ICT Smart Soc. (ICISS)*, Aug. 2022, pp. 1–6.

[12] T. R. D. Saputri and S.-W. Lee, "The application of machine learning in self-adaptive systems: A systematic literature review," *IEEE Access*, vol. 8, pp. 205948–205967, 2020, doi: 10.1109/ACCESS.2020.3036037.

[13] B. A. Mahmood and S. Kurnaz, "An investigational FW-MPM-LSTM approach for face recognition using defective data," *Image Vis. Comput.*, vol. 132, Apr. 2023, Art. no. 104644, doi: 10.1016/j.imavis.2023.104644.

[14] B. Gomathy, K. B. S. Sathya, J. Sathish, S. Santhosh, and S. S. Krishna, "Face recognition based student detail collection using OpenCV," in *Proc. 8th Int. Conf. Smart Struct. Syst. (ICSSS)*, Apr. 2022, pp. 1–4, doi: 10.1109/ICSSS54381.2022.9782211.

[15] H. Yang and X. Han, "Face recognition attendance system based on real-time video processing," *IEEE Access*, vol. 8, pp. 159143–159150, 2020, doi: 10.1109/ACCESS.2020.3007205.

[16] D. Wanyonyi and T. Celik, "Open-source face recognition frameworks: A review of the landscape," *IEEE Access*, vol. 10, pp. 50601–50623, 2022, doi: 10.1109/ACCESS.2022.3170037.

[17] Y.-H. Huang and H. H. Chen, "Deep face recognition for dim images," *Pattern Recognit.*, vol. 126, Jun. 2022, Art. no. 108580, doi: 10.1016/j.patcog.2022.108580.

[18] M. Cardaioli, M. Conti, G. Orazi, P. P. Tricomi, and G. Tsudik, "BLUFADER: Blurred face detection & recognition for privacy-friendly continuous authentication," *Pervas. Mobile Comput.*, vol. 92, May 2023, Art. no. 101801, doi: 10.1016/j.pmcj.2023.101801.

[19] S. P. R. Asaithambi, S. Venkatraman, and R. Venkatraman, "Proposed big data architecture for facial recognition using machine learning," *AIMS Electron. Electr. Eng.*, vol. 5, no. 1, pp. 68–92, 2021, doi: 10.3934/electreng.2021005.

[20] P. Li, S. Tu, and L. Xu, "Deep rival penalized competitive learning for low-resolution face recognition," *Neural Netw.*, vol. 148, pp. 183–193, Apr. 2022, doi: 10.1016/j.neunet.2022.01.009.

[21] M. Taskiran, N. Kahraman, and C. E. Erdem, "Face recognition: Past, present and future (a review)," *Digit. Signal Process.*, vol. 106, Nov. 2020, Art. no. 102809, doi: 10.1016/j.dsp.2020.102809.

[22] S. Bhattacharya, G. S. Nainala, S. Rooj, and A. Routray, "Local force pattern (LFP): Descriptor for heterogeneous face recognition," *Pattern Recognit. Lett.*, vol. 125, pp. 63–70, Jul. 2019, doi: 10.1016/j.patrec.2019.03.028.

[23] K. Sreekala, C. P. D. Cyril, S. Neelakandan, S. Chandrasekaran, R. Walia, and E. O. Martinson, "Capsule network-based deep transfer learning model for face recognition," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–12, Jul. 2022, doi: 10.1155/2022/2086613.

[24] E. Fourati, W. Elloumi, and A. Chetouani, "Anti-spoofing in face recognition-based biometric authentication using image quality assessment," *Multimedia Tools Appl.*, vol. 79, nos. 1–2, pp. 865–889, Jan. 2020, doi: 10.1007/s11042-019-08115-w.

[25] X. Wu, J. Xu, J. Wang, Y. Li, W. Li, and Y. Guo, "Identity authentication on mobile devices using face verification and ID image recognition," *Proc. Comput. Sci.*, vol. 162, pp. 932–939, Jan. 2019, doi: 10.1016/j.procs.2019.12.070.

[26] Y. Zhang, "Hadoop small image processing technology based on big data processing and its application effect in face feature extraction and face recognition system design," *Mobile Inf. Syst.*, vol. 2022, pp. 1–16, Jun. 2022, doi: 10.1155/2022/7493441.

[27] F. Marcolin, E. Vezzetti, and M. G. Monaci, "Face perception foundations for pattern recognition algorithms," *Neurocomputing*, vol. 443, pp. 302–319, Jul. 2021, doi: 10.1016/j.neucom.2021.02.074.

[28] S. Afra and R. Alhajj, "Early warning system: From face recognition by surveillance cameras to social media analysis to detecting suspicious people," *Phys. A, Stat. Mech. Appl.*, vol. 540, Feb. 2020, Art. no. 123151, doi: 10.1016/j.physa.2019.123151.

[29] V. Jain and E. Learned-Miller, "FDDB: A benchmark for face detection in unconstrained settings," UMass Dept. Comput. Sci. Amherst, Amsterdam, The Netherlands, Tech. Rep. UM-CS-2010-009, p. 20, Jan. 2010. [Online]. Available: http://works.bepress.com/erik_learned_miller/55/

[30] H. R. Farhan, M. H. Al-Muifraje, and T. R. Saeed, "A new model for pattern recognition," *Comput. Electr. Eng.*, vol. 83, May 2020, Art. no. 106602, doi: 10.1016/j.compeleceng.2020.106602.

[31] E.-V. Pikoulis, Z.-M. Ioannou, M. Paschou, and E. Sakkopoulos, "Face morphing, a modern threat to border security: Recent advances and open challenges," *Appl. Sci.*, vol. 11, no. 7, p. 3207, Apr. 2021, doi: 10.3390/app11073207.

[32] R. S. S. Kramer, M. O. Mireku, T. R. Flack, and K. L. Ritchie, "Face morphing attacks: Investigating detection with humans and computers," *Cognit. Res., Princ. Implications*, vol. 4, no. 1, Dec. 2019, doi: 10.1186/s41235-019-0181-4.

[33] A. Makrushin, D. Siegel, and J. Dittmann, "Simulation of border control in an ongoing Web-based experiment for estimating morphing detection performance of humans," in *Proc. ACM Workshop Inf. Hiding Multimedia Secur.*, Jun. 2020, pp. 91–96, doi: 10.1145/3369412.3395073.

[34] J. M. G. Sánchez, N. Jörgensen, M. Törngren, R. Inam, A. Berezovskyi, L. Feng, E. Fersman, M. R. Ramli, and K. Tan, "Edge computing for cyber-physical systems: A systematic mapping study emphasizing trustworthiness," *ACM Trans. Cyber-Phys. Syst.*, vol. 6, no. 3, pp. 1–28, Jul. 2022, doi: 10.1145/3539662.

[35] J. C. S. Jacques Junior, Y. Güçlütürk, M. Pérez, U. Güçlü, C. Andujar, X. Baró, H. J. Escalante, I. Guyon, M. A. J. van Gerven, R. van Lier, and S. Escalera, "First impressions: A survey on vision-based apparent personality trait analysis," *IEEE Trans. Affect. Comput.*, vol. 13, no. 1, pp. 75–95, Jan. 2022, doi: 10.1109/TAFFC.2019.2930058.

[36] D. Ortega-Delcampo, C. Conde, D. Palacios-Alonso, and E. Cabello, "Border control morphing attack detection with a convolutional neural network de-morphing approach," *IEEE Access*, vol. 8, pp. 92301–92313, 2020, doi: 10.1109/ACCESS.2020.2994112.

[37] V. D. Huszár and V. K. Adhikarla, "Live spoofing detection for automatic human activity recognition applications," *Sensors*, vol. 21, no. 21, p. 7339, Nov. 2021, doi: 10.3390/s21217339.

[38] A. G. de Andrade e Silva, H. M. Gomes, and L. V. Batista, "A collaborative deep multitask learning network for face image compliance to ISO/IEC 19794-5 standard," *Expert Syst. Appl.*, vol. 198, Jul. 2022, Art. no. 116756, doi: 10.1016/j.eswa.2022.116756.

[39] C. Kraetzer, A. Makrushin, J. Dittmann, and M. Hildebrandt, "Potential advantages and limitations of using information fusion in media forensics—A discussion on the example of detecting face morphing attacks," *EURASIP J. Inf. Secur.*, vol. 2021, no. 1, Dec. 2021, doi: 10.1186/s13635-021-00123-4.

[40] M. Long, X. Zhao, L.-B. Zhang, and F. Peng, "Detection of face morphing attacks based on patch-level features and lightweight networks," *Secur. Commun. Netw.*, vol. 2022, pp. 1–12, Mar. 2022, doi: 10.1155/2022/7460330.

[41] B. Hassan, H. H. R. Sherazi, M. Ali, and A. K. Bashir, "A multi-channel soft biometrics framework for seamless border crossings," *EURASIP J. Adv. Signal Process.*, vol. 2023, no. 1, Jun. 2023, doi: 10.1186/s13634-023-01026-x.

[42] S. Binder, A. Iannone, and C. Leibner, "Biometric technology in 'no-gate border crossing solutions' under consideration of privacy, ethical, regulatory and social acceptance," *Multimedia Tools Appl.*, vol. 80, no. 15, pp. 23665–23678, Jun. 2021, doi: 10.1007/s11042-020-10266-0.

[43] M. He, J. Zhang, S. Shan, M. Kan, and X. Chen, "Deformable face net for pose invariant face recognition," *Pattern Recognit.*, vol. 100, Apr. 2020, Art. no. 107113, doi: 10.1016/j.patcog.2019.107113.

[44] W. Kong, Z. You, and X. Lv, "3D face recognition algorithm based on deep Laplacian pyramid under the normalization of epidemic control," *Comput. Commun.*, vol. 199, pp. 30–41, Feb. 2023, doi: 10.1016/j.comcom.2022.12.011.

[45] Y. Zhu and Y. Jiang, "Optimization of face recognition algorithm based on deep learning multi feature fusion driven by big data," *Image Vis. Comput.*, vol. 104, Dec. 2020, Art. no. 104023, doi: 10.1016/j.imavis.2020.104023.

[46] D. Cui, G. Zhang, K. Hu, W. Han, and G.-B. Huang, "Face recognition using total loss function on face database with ID photos," *Opt. Laser Technol.*, vol. 110, pp. 227–233, Feb. 2019, doi: 10.1016/j.optlastec.2017.10.016.

[47] C.-T. Chiu, Y.-C. Ding, W.-C. Lin, W.-J. Chen, S.-Y. Wu, C.-T. Huang, C.-Y. Lin, C.-Y. Chang, M.-J. Lee, S. Tatsunori, T. Chen, F.-Y. Lin, and Y.-H. Huang, "Chaos LiDAR based RGB-D face classification system with embedded CNN accelerator on FPGAs," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 12, pp. 4847–4859, Dec. 2022, doi: 10.1109/TCSI.2022.3190430.

[48] S. Ge, S. Zhao, C. Li, and J. Li, "Low-resolution face recognition in the wild via selective knowledge distillation," *IEEE Trans. Image Process.*, vol. 28, no. 4, pp. 2051–2062, Apr. 2019, doi: 10.1109/TIP.2018.2883743.

[49] C. Fu, X. Wu, Y. Hu, H. Huang, and R. He, "DVG-face: Dual variational generation for heterogeneous face recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 44, no. 6, pp. 2938–2952, Jun. 2022, doi: 10.1109/TPAMI.2021.3052549.

[50] P. Guo, G. Du, L. Wei, H. Lu, S. Chen, C. Gao, Y. Chen, J. Li, and D. Luo, "Multiscale face recognition in cluttered backgrounds based on visual attention," *Neurocomputing*, vol. 469, pp. 65–80, Jan. 2022, doi: 10.1016/j.neucom.2021.10.071.

[51] M. Luo, J. Cao, X. Ma, X. Zhang, and R. He, "FA-GAN: Face augmentation GAN for deformation-invariant face recognition," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2341–2355, 2021, doi: 10.1109/TIFS.2021.3053460.

[52] P. Wang, F. Su, Z. Zhao, Y. Guo, Y. Zhao, and B. Zhuang, "Deep class-skewed learning for face recognition," *Neurocomputing*, vol. 363, pp. 35–45, Oct. 2019, doi: 10.1016/j.neucom.2019.04.085.

[53] P. P. Oroceo, J.-I. Kim, E. M. F. Caliwag, S.-H. Kim, and W. Lim, "Optimizing face recognition inference with a collaborative edge–cloud network," *Sensors*, vol. 22, no. 21, p. 8371, Nov. 2022, doi: 10.3390/s22218371.

[54] M. Sajjad, M. Nasir, F. U. M. Ullah, K. Muhammad, A. K. Sangaiah, and S. W. Baik, "Raspberry pi assisted facial expression recognition framework for smart security in law-enforcement services," *Inf. Sci.*, vol. 479, pp. 416–431, Apr. 2019, doi: 10.1016/j.ins.2018.07.027.

[55] A. Shah, B. Ali, M. Habib, J. Frnda, I. Ullah, and M. S. Anwar, "An ensemble face recognition mechanism based on three-way decisions," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 35, no. 4, pp. 196–208, Apr. 2023, doi: 10.1016/j.jksuci.2023.03.016.

[56] Z. Wang, X. Zhang, P. Yu, W. Duan, D. Zhu, and N. Cao, "A new face recognition method for intelligent security," *Appl. Sci.*, vol. 10, no. 3, p. 852, Jan. 2020, doi: 10.3390/app10030852.

[57] Z. Yu, Y. Dong, J. Cheng, M. Sun, and F. Su, "Research on face recognition classification based on improved GoogleNet," *Secur. Commun. Netw.*, vol. 2022, pp. 1–6, Jan. 2022, doi: 10.1155/2022/7192306.

[58] H.-C. Li, Z.-Y. Deng, and H.-H. Chiang, "Lightweight and resource-constrained learning network for face recognition with performance optimization," *Sensors*, vol. 20, no. 21, p. 6114, Oct. 2020, doi: 10.3390/s20216114.

[59] J. Chen, C. Guo, R. Xu, K. Zhang, Z. Yang, and H. Liu, "Toward children's empathy ability analysis: Joint facial expression recognition and intensity estimation using label distribution learning," *IEEE Trans. Ind. Informat.*, vol. 18, no. 1, pp. 16–25, Jan. 2022, doi: 10.1109/TII.2021.3075989.

[60] Y. Li, Y. Gao, B. Chen, Z. Zhang, G. Lu, and D. Zhang, "Self-supervised exclusive-inclusive interactive learning for multi-label facial expression recognition in the wild," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 32, no. 5, pp. 3190–3202, May 2022, doi: 10.1109/TCSVT.2021.3103782.

[61] X. Qu, Z. Zou, X. Su, P. Zhou, W. Wei, S. Wen, and D. Wu, "Attend to where and when: Cascaded attention network for facial expression recognition," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 6, no. 3, pp. 580–592, Jun. 2022, doi: 10.1109/TETCI.2021.3070713.

[62] A. A. Pise, M. A. Alqahtani, P. Verma, K. Purushothama, D. A. Karras, S. Prathibha, and A. Halifa, "Methods for facial expression recognition with applications in challenging situations," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–17, May 2022, doi: 10.1155/2022/9261438.

[63] A. V. Savchenko, L. V. Savchenko, and I. Makarov, "Classifying emotions and engagement in online learning based on a single facial expression recognition neural network," *IEEE Trans. Affect. Comput.*, vol. 13, no. 4, pp. 2132–2143, Oct. 2022, doi: 10.1109/TAFFC.2022.3188390.

[64] R. Verma, N. Bhardwaj, A. Bhavsar, and K. Krishan, "Towards facial recognition using likelihood ratio approach to facial landmark indices from images," *Forensic Sci. Int., Rep.*, vol. 5, Jul. 2022, Art. no. 100254, doi: 10.1016/j.fsir.2021.100254.

[65] E. Pei, M. C. Oveneke, Y. Zhao, D. Jiang, and H. Sahli, "Monocular 3D facial expression features for continuous affect recognition," *IEEE Trans. Multimedia*, vol. 23, pp. 3540–3550, 2021, doi: 10.1109/TMM.2020.3026894.

[66] Y. Li, Y. Lu, B. Chen, Z. Zhang, J. Li, G. Lu, and D. Zhang, "Learning informative and discriminative features for facial expression recognition in the wild," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 32, no. 5, pp. 3178–3189, May 2022, doi: 10.1109/TCSVT.2021.3103760.

[67] X. Wang, J. Gong, M. Hu, Y. Gu, and F. Ren, "LAUN improved StarGAN for facial emotion recognition," *IEEE Access*, vol. 8, pp. 161509–161518, 2020, doi: 10.1109/ACCESS.2020.3021531.

[68] C. L. P. Chen, Z. Liu, and S. Feng, "Universal approximation capability of broad learning system and its structural variations," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 30, no. 4, pp. 1191–1204, Apr. 2019, doi: 10.1109/TNNLS.2018.2866622.

[69] M. Shi, L. Xu, and X. Chen, "A novel facial expression intelligent recognition method using improved convolutional neural network," *IEEE Access*, vol. 8, pp. 57606–57614, 2020, doi: 10.1109/ACCESS.2020.2982286.

[70] S. Zhang, X. Pan, Y. Cui, X. Zhao, and L. Liu, "Learning affective video features for facial expression recognition via hybrid deep learning," *IEEE Access*, vol. 7, pp. 32297–32304, 2019, doi: 10.1109/ACCESS.2019.2901521.

[71] Y. Ma, Z. Huang, X. Wang, and K. Huang, "An overview of multimodal biometrics using the face and ear," *Math. Problems Eng.*, vol. 2020, pp. 1–17, Oct. 2020, doi: 10.1155/2020/6802905.

[72] J. Muhammad, Y. Wang, C. Wang, K. Zhang, and Z. Sun, "CASIA-Face-Africa: A large-scale African face image database," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3634–3646, 2021, doi: 10.1109/TIFS.2021.3080496.

[73] Z. Zheng, Q. Wang, C. Wang, M. Zhou, Y. Zhao, Q. Li, and C. Shen, "Where are the dots: Hardening face authentication on smartphones with unforgeable eye movement patterns," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 1295–1308, 2023, doi: 10.1109/TIFS.2022.3232957.

[74] S. Chang and Y. Duan, "Application of face recognition in e-commerce security authentication in the era of big data," *Secur. Commun. Netw.*, vol. 2022, pp. 1–11, Oct. 2022, doi: 10.1155/2022/4246750.

[75] F. Zhao, J. Li, L. Zhang, Z. Li, and S.-G. Na, "Multi-view face recognition using deep neural networks," *Future Gener. Comput. Syst.*, vol. 111, pp. 375–380, Oct. 2020, doi: 10.1016/j.future.2020.05.002.

[76] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman, "VGGFace2: A dataset for recognising faces across pose and age," in *Proc. 13th IEEE Int. Conf. Autom. Face Gesture Recognit. (FG)*, May 2018, pp. 67–74, doi: 10.1109/FG.2018.00020.
[77] S. Gupta, K. R. Castleman, M. K. Markey, and A. C. Bovik, "Texas 3D face recognition database," in *Proc. IEEE Southwest Symp. Image Anal. Interpretation (SSIAI)*, May 2010, pp. 97–100, doi: 10.1109/SSIAI.2010.5483908.
[78] A. Savran, N. Alyüz, H. Dibeklioğlu, O. Çeliktutan, B. Gökberk, B. Sankur, and L. Akarun, "Bosphorus database for 3D face analysis," in *Biometrics and Identity Management* (Lecture Notes in Computer Science, Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 5372, 2008, pp. 47–56, doi: 10.1007/978-3-540-89991-4_6.
[79] P. J. Phillips, P. J. Flynn, T. Scruggs, K. W. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W. Worek, "Overview of the face recognition grand challenge," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. (CVPR05)*, Jun. 2005, pp. 947–954, doi: 10.1109/CVPR.2005.268.
[80] P. J. Phillips, P. J. Flynn, T. Scruggs, K. W. Bowyer, and W. Worek, "Preliminary face recognition grand challenge results," in *Proc. 7th Int. Conf. Autom. Face Gesture Recognit. (FGR)*, Apr. 2006, pp. 15–21, doi: 10.1109/fgr.2006.87.
[81] S. Z. Li, D. Yi, Z. Lei, and S. Liao, "The CASIA NIR-VIS 2.0 face database," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops*, Jun. 2013, pp. 348–353, doi: 10.1109/CVPRW.2013.59.
[82] L. Song, M. Zhang, X. Wu, and R. He, "Adversarial discriminative heterogeneous face recognition," in *Proc. 32nd AAAI Conf. Artif. Intell.*, Sep. 2018, pp. 7355–7362, doi: 10.1609/aaai.v32i1.12291.
[83] X. Wu, H. Huang, V. M. Patel, R. He, and Z. Sun, "Disentangled variational representation for heterogeneous face recognition," in *Proc. 33rd AAAI Conf. Artif. Intell., 31st Innov. Appl. Artif. Intell. Conf., 9th AAAI Symp. Educ. Adv. Artif. Intell.*, 2019, pp. 9005–9012, doi: 10.1609/aaai.v33i01.33019005.
[84] H. S. Bhatt, S. Bharadwaj, R. Singh, and M. Vatsa, "Memetically optimized MCWLD for matching sketches with digital face images," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1522–1535, Oct. 2012, doi: 10.1109/TIFS.2012.2204252.
[85] K. Panetta, Q. Wan, S. Agaian, S. Rajeev, S. Kamath, R. Rajendran, S. P. Rao, A. Kaszowska, H. A. Taylor, A. Samani, and X. Yuan, "A comprehensive database for benchmarking imaging systems," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 42, no. 3, pp. 509–520, Mar. 2020, doi: 10.1109/TPAMI.2018.2884458.
[86] A. Bansal, A. Nanduri, C. D. Castillo, R. Ranjan, and R. Chellappa, "UMDFaces: An annotated face dataset for training deep networks," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Oct. 2017, pp. 464–473, doi: 10.1109/BTAS.2017.8272731.
[87] A. Bansal, C. Castillo, R. Ranjan, and R. Chellappa, "The do's and don'ts for CNN-based face verification," in *Proc. IEEE Int. Conf. Comput. Vis. Workshops (ICCVW)*, Oct. 2017, pp. 2545–2554, doi: 10.1109/ICCVW.2017.299.
[88] X. Lv, C. Yu, H. Jin, and K. Liu, "HQ2CL: A high-quality class center learning system for deep face recognition," *IEEE Trans. Image Process.*, vol. 31, pp. 5359–5370, 2022, doi: 10.1109/TIP.2022.3195638.
[89] G. B. Huang and E. Learned-miller, "Labeled faces in the wild? Updates and new reporting procedures," Univ. Massachusetts Comput. Sci. Dept., Amherst, MA, USA, Tech. Rep. 14-03, 2014. [Online]. Available: https://api.semanticscholar.org/CorpusID:17716267
[90] L. J. Karam and T. Zhu, "Quality labeled faces in the wild (QLFW): A database for studying face recognition in real-world environments," *Proc. SPIE*, vol. 9394, Oct. 2015, Art. no. 93940B, doi: 10.1117/12.2080393.
[91] E. Learned-Miller, G. B. Huang, A. RoyChowdhury, H. Li, and G. Hua, "Labeled faces in the wild: A survey," in *Proc. Adv. Face Detection Facial Image Anal.*, 2016, pp. 189–248.
[92] M. Günther, A. R. Dhamija, and T. E. Boult, "Watchlist adaptation: Protecting the innocent," in *Proc. Lect. Notes Informat. (LNI)*, vol. 306. Bonn, Germany: Gesellschaft fur Informatik (GI), 2020, pp. 21–32.
[93] M. Grgic, K. Delac, and S. Grgic, "SCface—Surveillance cameras face database," *Multimedia Tools Appl.*, vol. 51, no. 3, pp. 863–879, Feb. 2011, doi: 10.1007/s11042-009-0417-2.
[94] H. Azami, M. Malekzadeh, and S. Sanei, "A new neural network approach for face recognition based on conjugate gradient algorithms and principal component analysis," *J. Math. Comput. Sci.*, vol. 6, no. 3, pp. 166–175, Apr. 2013, doi: 10.22436/jmcs.06.03.01.
[95] A. Elmahmudi and H. Ugail, "The biharmonic eigenface," *Signal, Image Video Process.*, vol. 13, no. 8, pp. 1639–1647, Nov. 2019, doi: 10.1007/s11760-019-01514-4.
[96] S. B. Ahmed, S. F. Ali, J. Ahmad, M. Adnan, and M. M. Fraz, "On the frontiers of pose invariant face recognition: A review," *Artif. Intell. Rev.*, vol. 53, no. 4, pp. 2571–2634, Apr. 2020, doi: 10.1007/s10462-019-09742-3.
[97] M. Wang and W. Deng, "Deep face recognition with clustering based domain adaptation," *Neurocomputing*, vol. 393, pp. 1–14, Jun. 2020, doi: 10.1016/j.neucom.2020.02.005.
[98] M. Duan, Y. Wang, L. Jin, and Y. Wu, "SOF: A synthetic occluded face dataset," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2021, pp. 3163–3169, doi: 10.1109/BigData52589.2021.9672029.
[99] P. Li, X. Wu, Y. Hu, R. He, and Z. Sun, "M2FPA: A multi-yaw multi-pitch high-quality dataset and benchmark for facial pose analysis," in *Proc. IEEE/CVF Int. Conf. Comput. Vis. (ICCV)*, Oct. 2019, pp. 10042–10050, doi: 10.1109/ICCV.2019.01014.
[100] X. Deng, T. Mu, Y. Wang, and Y. Xie, "The application of human figure drawing as a supplementary tool for depression screening," *Frontiers Psychol.*, vol. 13, Jun. 2022, Art. no. 865206, doi: 10.3389/fpsyg.2022.865206.
[101] S. Yang, P. Luo, C. C. Loy, and X. Tang, "WIDER FACE: A face detection benchmark," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2016, pp. 5525–5533, doi: 10.1109/CVPR.2016.596.
[102] Q. A. Ahmed and A. Q. H. Al-Neami, "A smart biomedical assisted system for Alzheimer patients," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 881, no. 1, Jul. 2020, Art. no. 012110.
[103] M. Djamaluddin, R. Munir, N. P. Utama, and A. I. Kistijantoro, "Open-set profile-to-frontal face recognition on a very limited dataset," *IEEE Access*, vol. 11, pp. 65787–65797, 2023, doi: 10.1109/ACCESS.2023.3289923.
[104] Y. Zhong, W. Deng, H. Fang, J. Hu, D. Zhao, X. Li, and D. Wen, "Dynamic training data dropout for robust deep face recognition," *IEEE Trans. Multimedia*, vol. 24, pp. 1186–1197, 2022, doi: 10.1109/TMM.2021.3123478.
[105] Z. Deng, H. Chiang, L. Kang, and H. Li, "A lightweight deep learning model for real-time face recognition," *IET Image Process.*, vol. 17, no. 13, pp. 3869–3883, Nov. 2023, doi: 10.1049/ipr2.12903.
[106] O. Agbo-Ajala and S. Viriri, "Deeply learned classifiers for age and gender predictions of unfiltered faces," *Sci. World J.*, vol. 2020, pp. 1–12, Apr. 2020, doi: 10.1155/2020/1289408.
[107] M. D. Putro and K.-H. Jo, "Fast face-CPU: A real-time fast face detector on CPU using deep learning," in *Proc. IEEE 29th Int. Symp. Ind. Electron. (ISIE)*, Jun. 2020, pp. 55–60, doi: 10.1109/ISIE45063.2020.9152400.
[108] B.-C. Chen, C.-S. Chen, and W. H. Hsu, "Face recognition and retrieval using cross-age reference coding with cross-age celebrity dataset," *IEEE Trans. Multimedia*, vol. 17, no. 6, pp. 804–815, Jun. 2015, doi: 10.1109/TMM.2015.2420374.
[109] B. Yang, J. Yan, Z. Lei, and S. Z. Li, "Fine-grained evaluation on face detection in the wild," in *Proc. 11th IEEE Int. Conf. Workshops Autom. Face Gesture Recognit. (FG)*, vol. 1, May 2015, pp. 1–7, doi: 10.1109/FG.2015.7163158.
[110] S. Ge, J. Li, Q. Ye, and Z. Luo, "Detecting masked faces in the wild with LLE-CNNs," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jul. 2017, pp. 426–434, doi: 10.1109/CVPR.2017.53.
[111] S. Dinh Viet and C. Le Tran Bao, "Effective deep multi-source multi-task learning frameworks for smile detection, emotion recognition and gender classification," *Informatica*, vol. 42, no. 3, pp. 345–356, Sep. 2018, doi: 10.31449/inf.v42i3.2301.
[112] W. Wang, X. Wang, W. Yang, and J. Liu, "Unsupervised face detection in the dark," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 45, no. 1, pp. 1250–1266, Jan. 2023, doi: 10.1109/TPAMI.2022.3152562.
[113] M. Jabberi, A. Wali, B. B. Chaudhuri, and A. M. Alimi, "68 landmarks are efficient for 3D face alignment: What about more? 3D face alignment method applied to face recognition," *Multimed. Tools Appl.*, vol. 82, pp. 41435–41469, Apr. 2023, doi: 10.1007/s11042-023-14770-x.
[114] R. Ramya, A. Anandh, K. Muthulakshmi, and S. Venkatesh, "Gender recognition from facial images using multichannel deep learning framework," in *Machine Learning for Biometrics: Concepts, Algorithms and Applications*, P. P. Sarangi, M. Panda, S. Mishra, B. S. P. Mishra, and B. Majhi, Eds. New York, NY, USA: Academic, 2022, pp. 105–128.
[115] W. Gao, B. Cao, S. Shan, X. Chen, D. Zhou, X. Zhang, and D. Zhao, "The CAS-PEAL large-scale Chinese face database and baseline evaluations," *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 38, no. 1, pp. 149–161, Jan. 2008, doi: 10.1109/TSMCA.2007.909557.

[116] Y. Guo, L. Zhang, Y. Hu, X. He, and J. Gao, "MS-Celeb-1M: A dataset and benchmark for large-scale face recognition," in *Computer Vision—ECCV* (Lecture Notes in Computer Science, Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 9907. Amsterdam, The Netherlands: Springer, 2016, pp. 87–102, doi: 10.1007/978-3-319-46487-9_6.

FADHIL HIDAYAT (Member, IEEE) was born in Payakumbuh, in September 1986. He received the master's and Ph.D. degrees from Institut Teknologi Bandung, in 2011 and 2018, respectively. He is currently a Lecturer with Institut Teknologi Bandung and joined the Smart City and Community Innovation Center.

ULVA ELVIANI was born in Bengkalis, in November 1995. She received the bachelor's degree in computer science from Universitas Muhammadiyah Riau, in 2017, and the master's degree from Institut Teknologi Bandung, in 2023. She is currently a Researcher with the Smart City and Community Innovation Center. Her research interests include the Internet of Things, safety and security, complex systems, smart systems, and video analytics.

GEORGE BRYAN GABRIEL SITUMORANG was born in Medan, in July 1999. He received the bachelor's degree in computer science from Diponegoro University, in 2021. He is currently pursuing the master's degree in informatics with the Bandung Institute of Technology. With a passion for technology and a strong academic background, he aspires to make significant contributions to the field of informatics through his studies and future endeavors.

MUHAMMAD ZAKY RAMADHAN was born in 1997. He received the bachelor's degree in computer science from Telkom University, in 2020. He is currently pursuing the master's degree with the School of Electrical Engineering and Informatics, Bandung Institute of Technology (ITB).

FIGO AGIL ALUNJATI was born in Purworejo, in July 2000. He received the bachelor's degree in information systems and technology from Institut Teknologi Bandung, in 2022. His research interests include the world of Internet of Things and video analysis. He hopes that with his ability, he can spread benefits to others through the field of information technology.

REZA FAUZI SUCIPTO was born in Karawang, in June 1989. He received the bachelor's degree in computer engineering from Maranatha University Bandung, in 2010, and the master's degree from Institut Teknologi Bandung, in 2023. He is an Immigration Officer of the Republic of Indonesia.