https://doi.org/10.47460/minerva.v4i10.91

New technologies for border control and security

Ayala Henry
https://orcid.org/0000-0002-4918-4395
leon_artillery@hotmail.com
Ejército Ecuatoriano
Grupo de Artillería Lanzadores Nro. 80 "Calderón"
Quito-Ecuador

Yange Willians
https://orcid.org/0000-0002-2711-1398
williansyangeenriquez@gmail.com
Ejército Ecuatoriano
Grupo de Artillería Lanzadores Nro. 80 "Calderón"
Quito-Ecuador

Enríquez Carolina
https://orcid.org/0000-0002-4832-1386
isis_30_m90@hotmail.com
Ejército Ecuatoriano
Comando de Apoyo Logístico N°9
Quito-Ecuador

Tamayo Heidy
https://orcid.org/0000-0002-3538-3748
heidyantonela@hotmail.com
Ejército Ecuatoriano
Batallón de Infantería Nº2 "Imbabura".
Ibarra-Ecuador

Recibido(16/04/2022), Aceptado(15/05/2022)

Abstract. - This document describes the advances and new technologies developed for border security control and military use. A systematic review was conducted, considering scientific articles on technological advances from which information was obtained on new techniques, applications, algorithms, surveillance devices, and biometric systems that use artificial intelligence and machine learning to support border security and control of persons, weapons, products, and objects that are not allowed under the current regulations of nations. Technological advances worldwide enable the continuous development of new alternatives to counter the new and improved fraudulent techniques for illegal border crossing of people and objects.

Palabras clave: Technologies, border control, border security, artificial intelligence.

Nuevas tecnologías para el control y seguridad fronteriza

Resumen. - En este documento se presenta una descripción de los avances y nuevas tecnologías desarrolladas para el control de la seguridad fronteriza y de uso militar. Se realizó una revisión sistemática considerando artículos científicos de bases relacionadas con avances tecnológicos de donde se obtuvo información referente a nuevas técnicas, aplicativos, algoritmos, dispositivos para el monitoreo y sistemas biométricos que operan con inteligencia artificial, aprendizaje de máquina para dar soporte a la seguridad y control en el paso fronterizo de personas, armamento, productos y objetos no permitidos por las reglamentaciones vigentes de las naciones. El avance tecnológico alrededor del mundo permite el constante desarrollo de nuevas alternativas que se contraponen a las nuevas y mejoras en las técnicas fraudulentas para el paso de personas y objetos de manera ilegal.

Keywords: Tecnologías, control fronterizo, seguridad fronteriza, inteligencia artificial.

I. INTRODUCTION

Borders are a critical part of a country's security, protecting citizens and keeping them safe from individuals and groups that threaten security on multiple levels. In addition, border patrol teams are essential in maintaining peace in the region and keeping invaders and malicious individuals out of the country.

Many technologies, such as surveillance cameras, biometric scanners, and thermal imaging systems, can be used to protect borders. These technologies have advanced significantly over the years. For example, facial recognition software is an essential technological advancement in border control, which can easily and quickly identify individuals. This software can gather information about who enters or exits a region by scanning their faces at borders or airports.

Modern border control is a complex system. It has multiple layers of security, and more than one country manages the border. Border control has evolved from being a physical barrier to the digital world, developing various technologies for this purpose, classified into two groups: (1) Technologies for the detection and prevention of illegal activities and (2) Technologies for the identification and verification of travelers.

This work describes multiple cases of land border security control technologies that have been effectively applied in various countries of the world, as well as those in development, in the development section. The methodology section specifies the process of obtaining reference information for this work. The results section explains and discusses some findings, approaches, and dilemmas. Finally, the conclusions are presented.

DEVELOPMENT

Currently, multiple operational technologies for land border control are shown in Figure 1 (Fig. 1). Wireless devices, mobile security units, fiber optics for communications, and fixed and mobile monitoring stations exist.

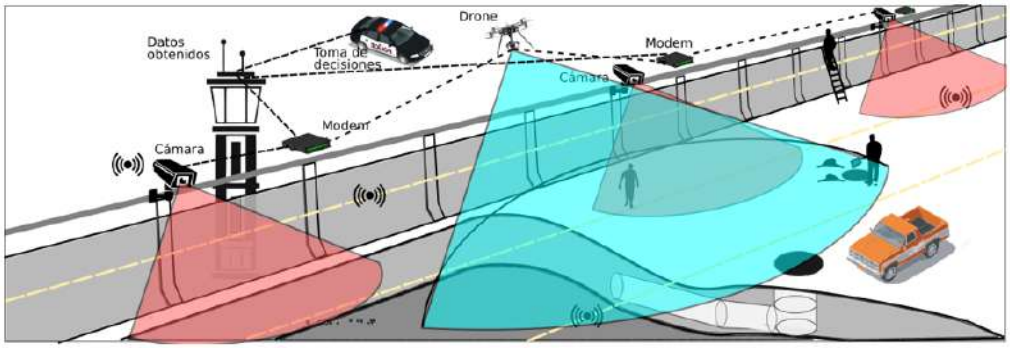

Fig. 1. Technologies used in land border security control systems

The security of fiber optic communication is a technology that was developed to provide more secure communication. It has become the most popular technology for border control, being used in the United States since the 1990s.

The use of fiber optic communication security has been implemented for decades in the military and government sectors. The technology has been developed to its current state through decades of research and development. The use of fiber optic communication security has made it possible for border control agencies to detect intruders and track their movements, as well as provide protection for their employees against terrorist attacks.

The use of fiber optic technology for border control has been around for some time. Countries like the United States, Canada, Mexico, and Australia have used this technology for decades to keep their borders safe and secure.

Multiple technologies can be used for border control. Some technologies used in border control systems are presented in Table 1, along with their application, scope, and technical characteristics.

Table 1. Technologies used in land border security control systems.

Technology	Application	Technical characteristics and scope
Biometric systems	Identity verification	Capture and analysis of physical or behavioral traits, such as fingerprints, iris scans, or facial recognition. These systems are used to authenticate the identity of travelers at airports and land borders. They are also used in visa processing and law enforcement operations. Biometric systems must adhere to strict privacy and data protection regulations.
Automated passport control kiosks	Identity verification	It uses biometric technology to verify passport information and automate the customs process. Automated passport control kiosks are used at airports and can speed up the processing of travelers.
Facial recognition	Identity verification	It uses facial recognition technology to identify individuals. Facial recognition can be combined with other biometric technologies, such as fingerprint scanning, and is used by law enforcement agencies to identify suspects and monitor crowds.
Iris recognition	Identity verification	It uses iris scanning technology to identify individuals. Iris recognition is considered more accurate than other biometric technologies, such as fingerprint scanning, and is used by border control agencies and law enforcement.
Video analytics	Behavioral analysis	It uses artificial intelligence and machine learning algorithms to analyze video footage and identify suspicious behavior, such as someone climbing a fence or entering a restricted area. Video analytics combines other surveillance technologies, such as CCTV cameras and UAVs.
Biometric boarding gates	Identity verification	It uses biometric technology to verify the identity of travelers at boarding gates. Biometric boarding gates can speed up the boarding process and enhance security. They are commonly used at airports.

Table 2 presents technologies used in border systems for detecting objects (weapons, drugs, etc.) on people's bodies, as well as tracking vehicles passing through restricted areas. The technologies in Table 2 employ multiple technologies such as radiofrequency, X-ray, gamma-ray, radar, thermal cameras, and image analysis.

The advantage of the technologies described in Table 2 is to provide visualization through organic tissue, solid objects, and gaseous substances and even detect hot zones such as engines, people, and firearms in areas of poor visibility without affecting the people to whom these technologies are applied.

Currently, surveillance drones are used at border crossings to detect and track objects, people, and vehicles with the advantage that these activities can be controlled from fixed posts, eliminating the need for helicopters and the need to approach safely without risking the safety of border control personnel.

Table 2. Some technologies are used in border control systems for object tracking and detection.

Technology	Application	Technical characteristics and scope
Radio Frequency Identification (RFID)	Tracking and identification of goods	It uses electromagnetic fields to identify and track tags attached to objects, such as cargo or luggage. RFID tags can be read remotely and used to track the location and movement of goods. They are often used in logistics and supply chain management.
X-ray scanners	Detection of concealed objects	It uses X-rays to create images of objects in luggage or on people. These images can reveal the presence of weapons, explosives, or other contraband. X-ray scanners are commonly used at airports and land borders.
Gamma-ray imaging systems	Detection of concealed objects	It uses gamma rays to create images of objects in cargo containers. Gamma-ray imaging is typically used at seaports and land borders to detect contraband, including drugs and weapons.
Unmanned Aerial Vehicles (UAVs)	Surveillance and reconnaissance	It uses remote-controlled aircraft to monitor and patrol borders. UAVs can provide real-time imagery and video and can be equipped with sensors such as thermal cameras to detect heat signatures.
Ground surveillance radar	Detection of illegal crossings	It uses radar to detect the movement of people or vehicles. Ground surveillance radar can cover large areas and detect movement even in adverse weather conditions. They are often used at land borders.
License plate recognition	Identification of vehicles	It uses optical character recognition technology to read license plates and identify vehicles. License plate recognition can monitor traffic and identify vehicles of interest. They are commonly used at land borders and ports.
Thermal cameras	Detection of heat signatures	It uses thermal imaging technology to detect the heat signatures of people or objects. Thermal cameras c to detect people hiding in vehicles or other concealed areas. They are often combined with other surveillance technologies, such as UAVs and ground surveillance radar.

Robots have become widespread as an instrument for detecting intruders at the borders and sending information to the control center. In hostile environments, robots show excellent performance. Automated vehicles with monitoring systems based on facial recognition and detection algorithms have been developed. The presence of human beings is verified through the system, which then executes the facial recognition algorithm to compare them with known soldier data and identify intruders. The HAAR algorithm has been employed for face detection, and the CNN algorithm has been used for facial recognition in these developments [1]. It is anticipated that in the future, there will be more regular use of robots, radar networks, and cameras for these tasks due to the vast borders for which more patrol personnel and vehicles will be required [2].

The introduction of electronic passports containing chips and RFID technology has been proposed to achieve more intelligent and safer control. Greater security is considered because the chip information is locked and cannot be modified or tampered with, including the stored photo. So, if there is a duplicate, this will trigger alarms [3]. Despite the benefits, some people view biometric technologies as evoking fears of privacy and public liberties violations.

The European Union has made advancements in managing its migratory flows, for which it has increased its reliance on technology in border management. Developments have been implemented primarily in two areas: using unmanned aerial vehicles or drones and improving information and surveillance technologies [4].

The techniques employed for border control in Turkey have seen the urgent need for increased use of technology. However, in addition to detecting, filtering, and preventing "illegal" border crossings, smuggling, and terrorism, the humanitarian aspect of saving the lives of migrants has also been considered [5].

The Indian border guard has installed and adopted new technologies such as cameras, night vision devices, and radars. The need for the Internet of Things (IoT) has become evident for better information management, which has already been adopted on a small scale and in limited areas. The fast-decision-making process provides reliability and appropriate responses to secure dangerous border areas, even in extreme weather conditions, diverse terrain, riverine terrains, dense forest areas, and inaccessible areas that are complicated to monitor by personnel. The project "Smart Border Security System using Internet of Things" proposes a low-cost solution using Passive Infrared Sensors (PIR) and the OV7670 camera module to detect the movement of any object within a range and capture images of intruders, respectively, [6].

The algorithm used for object detection in video based on machine learning in this research is the Viola-Jones algorithm. This algorithm requires a training set of positive and negative images. A collection of positive and negative images was used to train the algorithm for objects such as humans, vehicles, and guns. A threat level classifier and an alert warning system were also added to classify and annotate the videos in real-time for each frame. The threat level classifier categorizes the real-time video into safe, low, medium, and high (dangerous). The alert system specifies the type of warning based on the type of intrusion (human, vehicular, or gun) detected. For the algorithm proposed in this work, the accuracy for human detection is an average of 94.93%, the accuracy for vehicle detection is an average of 95.2%, and the accuracy for gun detection is an average of 97.67%. The accuracy of the proposed method (97%) was much higher than that of the previously published compared method (64%) for object detection [7].

Quad-copter drones enable some borders to communicate constantly with the base to detect and track targets effectively. The system has functionalities to send real-time alerts when intruders have been detected so that nearby patrols can act. Good results have been shown in applying these technologies with the use of GPS to direct vehicles, image analysis, machine intelligence with aerial visualization, and target detection [8].

It has been proposed to include a contactless identification system that uses advanced mobile devices for border control, focusing on usability and integrating new technologies. The device is based on the MobilePass device and allows for identification using 4 fingerprints instead of just one, as in conventional systems. The robustness and contributions to the border security system are still being evaluated [9].

Maritime borders where groups of migrants arrive to enter another nation have a particular problem regarding verifying information due to the presence of ships, weather conditions, and extensive monitoring areas. Therefore, maritime surveillance has focused not only on the rescue and recovery of migrants but also on taking subsequent actions to ensure the well-being of individuals [10].

Since the 9/11 incident in Manhattan, the United States, borders have been viewed as one of the main security filters for national security. Many countries have seen the need to improve their automated border control systems to respond to these challenges (Heiskanen, 2014). A new research approach for automated border control (ABC) systems have been proposed. Various security technologies are used for these complex ABC solutions, including biometrics, surveillance, certificate exchange, data protection, secure user interaction, and information security. The FastPass project proposes a stakeholder-driven approach providing a better understanding of security technologies to estimate the automated approach's risks, challenges, and opportunities [11].

"To enhance border security, wireless sensor networks (WSN) powered by solar energy have been developed, allowing for automated monitoring, target tracking, and intrusion detection. These systems have been noted for their features regarding the classification of detection environments, their ability to survive in adverse weather conditions, and their efficient collection of solar energy.", [12].

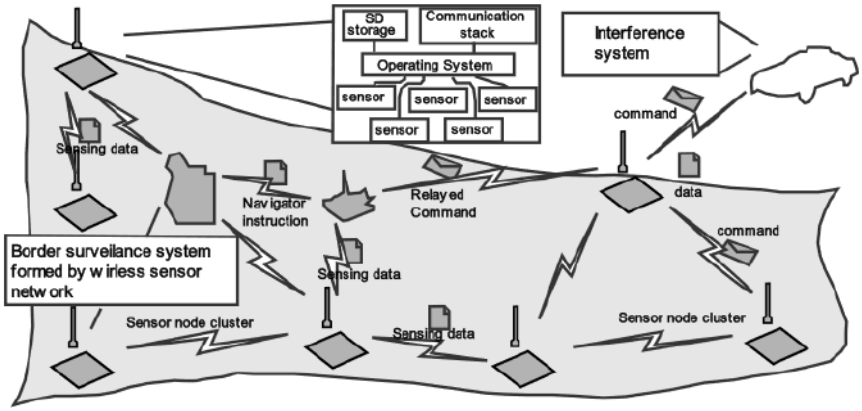

Fig. 2. WSN architecture with the use of wireless nodes.

Fig 2 shows the network architecture of our solar-powered ad-hoc WSN for border surveillance. The wireless sensor nodes are interconnected to build a surveillance system for border security. The gateway base station or sink node receives and aggregates the detection data from the sensors located in a distributed manner and transmits or broadcasts commands to the sensor nodes, such as suspension and activation commands, to manage the sensor nodes. Remote service is also integrated, the gateway transmits the detection data to the operations center, and an inference system processes the data. The sensor nodes can automatically form sensor clusters and work collaboratively. Our network architecture is flexible and imposes no limits on the size of the sensor network and the number of sensors [12]. In addition, sensor networks such as "PACHENDRIYA" from India have also been developed, which incorporate sensors of various types such as geophones, hydrophones, microphones, infrared sensors, and camera sensors to achieve effective surveillance and detection of human intrusions in border scenarios.

Ground Surveillance Radar (GSR) operations allow for securing an area and provide operators and agents with much more time to evaluate, prioritize and stop intruders than a traditional fence system. Additional response time is one of the critical characteristics of the wide-area surveillance concept, along with additional benefits for both operators and response teams. Two leading GSR technologies exist Frequency-Modulated Continuous Wave (FMCW) and Pulse Doppler. Most pulse Doppler radars are derived from legacy military battlefield radar technology applied to wide-area surveillance. In contrast, a new generation of FMCW radar technology has been developed for this new type of surveillance, applied to the security of high-value sites, airports, military bases, ports, and borders [13].

With proper control over X-ray exposure to the human body (Fig. 3), various technical configurations such as transmission imaging (fluoroscopy), backscatter imaging, computed tomography, and other combinations are used in border controls. In this way, the inside of the human body, it's surface, clothing, and luggage is inspected to detect weapons, explosives, and drugs.

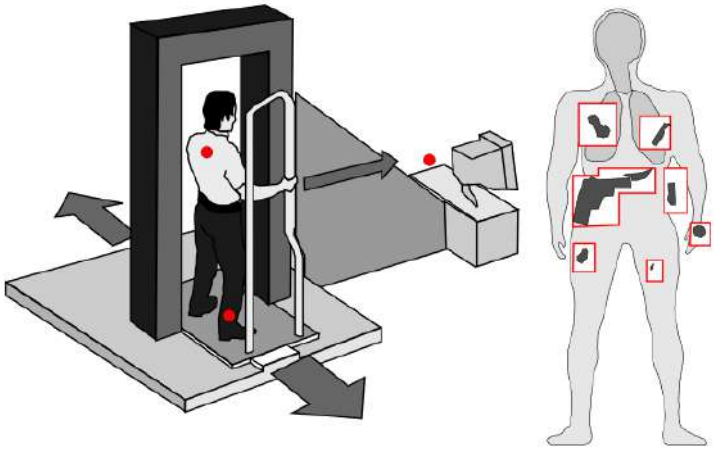

Fig 3. Transmission imaging (fluoroscopy). The image results of a scan: The person slides back and forth (1) for seconds. A pencil beam (2) scans the person. This beam is adjusted to a line of detectors. The digitized image appears on a screen (3).

In Table 3, the most common functional requirements that border security scanning systems must have been shown. Multiple technologies are specified for specific tasks that detect and recognize risk elements.

Table 3. Most common functional requirements needed for border security scanning systems.

Functional requirement	Description
Image capture	The system must be able to capture clear and crisp images of the people or vehicles undergoing the scan, allowing accurate identification of facial details or vehicle features.
Threat detection	The system must be able to detect and alert about possible threats, such as weapons, explosives, drugs, etc., in the objects or people scanned.
Pattern recognition	The system must recognize suspicious patterns in the scanned images, such as strange or unusual behavior, rapid or erratic movements, or hidden packets in the scanned objects.
Database integration	The system should be able to integrate with databases of criminal records, terrorism information, watch lists, and other relevant data to enable the identification of potential threats and informed decision-making.
Processing speed	The system must process the scanned images in real time, allowing a quick and effective response to possible threats.
Accessibility and usability	The system must be accessible and easy to use by the personnel in charge of its operation without requiring complex technical skills.
Data Security	The system must guarantee the security of the stored data, ensuring confidentiality and protection against possible attacks or threats.

Table 3 outlines essential requirements for effective border security scanning systems, including clear and crisp image capture, threat detection, pattern recognition, and integration with relevant databases to identify potential threats. The table emphasizes the need for accessible, user-friendly systems ensuring information security.

To improve the clarity and concision of the second paragraph, it could be revised as follows: There are proposals to enhance border processes by employing a multi-tool approach incorporating increased scanning, controls, and nearly simultaneous passenger queries. This approach could address several common problems, including limitations in traditional information systems for immigration and port security, carrier reservations, economic and demographic statistics, and police and counterterrorism agencies [14].

The OptaSense® Distributed Acoustic Sensing (DAS) system is an innovative technology that utilizes fiber optic communication cables as sensors to detect surface crossings and tunnel construction for border security purposes. This low-cost, high-reliability system has been field-proven in over one hundred locations worldwide and can work with existing border surveillance technologies. OptaSense's ability to detect, classify, and locate activity over hundreds of kilometers in a precise and actionable manner has proven it to be a cost-effective solution for long-border monitoring, with the system scaling to cover up to 1500 km and be controlled by a single central monitoring station in pipeline applications [15].

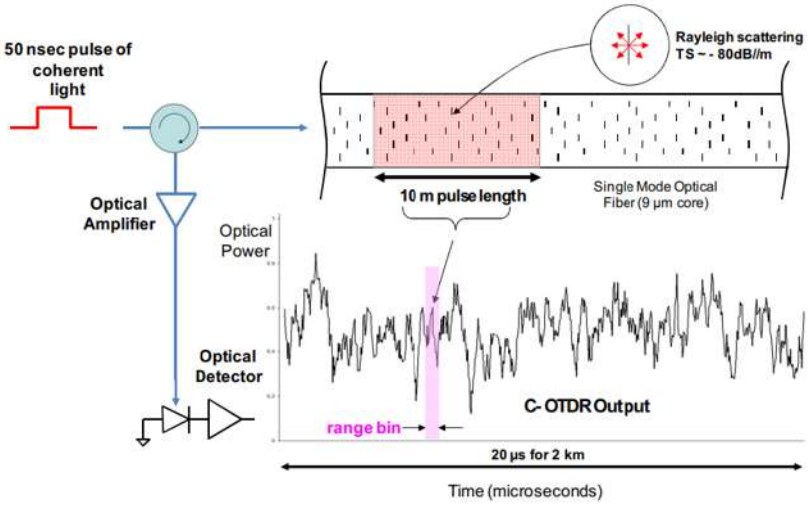

Fig 3. Principle of operation of the OptaSense DAS System.

Figure 4 presents a representation of the operating principle of the current generation DAS OptaSense system. Each range container is sampled 2000 times/second (50 km of fiber) at 20000 cycles/sec (5 km of fiber) and provides the output of the "virtual" strain sensor. A simple system that can provide 4000 programmable channels spaced at 5, 10, or 12.5 meters. The system can detect variations in decibels from 2 microns to 2 km, which can be determined in pulses of 10-meter length, generating an optical signal that is amplified and transmitted to the control station, providing the position of the location where it has crossed near the cable, generating an increase in the noise of the signal.

III. METHODOLOGY

Scientific articles were searched in repositories such as ScienceDirect, Scopus, Taylor & Francis, Web of Sciences, and IEEE Xplore. Duplicate articles were removed, and the remaining works were screened according to their titles. Subsequently, the abstracts were reviewed, and the contents were verified to obtain 15 articles with relevant information, which served as the basis for this document. Figure 5 shows the review process workflow, considering the PRISMA methodology guidelines.

The search keywords used were technologies, control, security, and borders. All articles that addressed the topic without describing the principle of operation of the applied technologies were excluded.

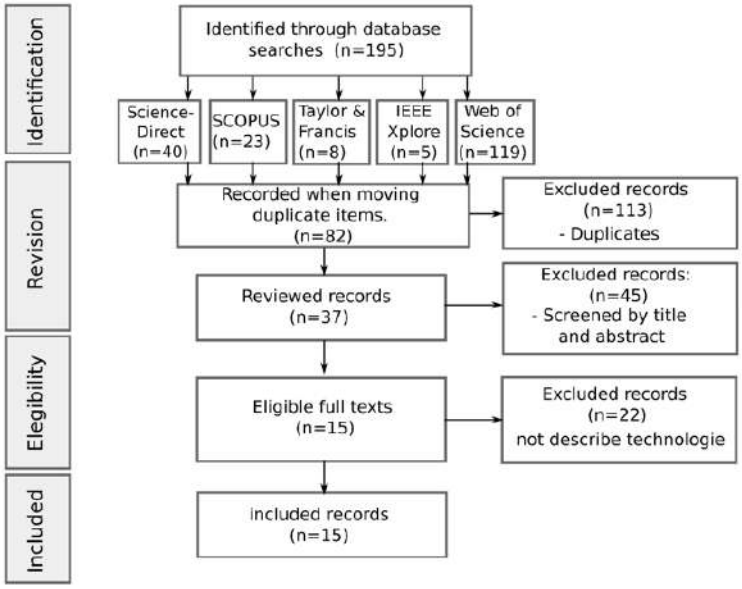

Fig 5. Systematic review conducted, keywords: "Technologies AND control AND border".

IV. RESULTS

Border control is critical to ensure the security and protection of a country's borders. They have developed several technologies to improve their effectiveness. Some of the technologies identified for these security-related tasks are described below.

Video surveillance systems allow surveillance of border areas using cameras that transmit images in real-time to a control center. The technology allows detection patterns and alerts operators if anything unusual is observed within the field of vision.

Movement sensors detect and send information about the presence of people, vehicles, or other objects in specific border areas and alert operators. The sensors can also detect the presence of tunnels and other smuggling devices.

Intrusion detection systems allow alerting about the presence of people or vehicles that cross the border without permission and irregularly. Intrusion detection systems can use multiple technologies, such as video cameras, motion sensors, radars, thermographic detectors, and multispectral image analysis.

Frequent use of biometric identification has been identified. These systems allow the identification of people through unique physical characteristics, such as fingerprints, iris scans, and facial recognition, among others. Biometric identification systems are used to verify the identity of people crossing the border and to detect people wanted by the law.

Baggage and cargo scanning systems provide information on detecting dangerous or illegal objects in baggage and cargo of vehicles crossing the border. These scanning systems use X-ray technology and other scanning methods to identify objects by detecting them through other solids and making them more accessible for control personnel to visualize.

CONCLUSIONS

Advanced technologies are being used to strengthen border security: Border control technologies have evolved tremendously in recent decades. Advanced technologies such as high-resolution cameras, radar systems, and drones are used to monitor borders and detect potential threats. In addition, data analysis and facial recognition techniques are being used to identify suspicious persons and prevent unauthorized persons from crossing.

Border control technologies impact privacy and human rights: As advanced technologies strengthen border security, there are also legitimate concerns about privacy and human rights impacts. In some cases, these technologies can be invasive and result in the collection and use of personal data without the consent of individuals, which can have severe consequences in terms of civil liberties.

Implementing border control technologies is a contentious issue: The performance of border control technologies is controversial in many parts of the world—some support using these technologies to strengthen border security and prevent illegal immigration and cross-border crime. In contrast, others argue that these technologies are costly, invasive, and not consistently effective. It is essential to consider these diverse views when considering implementing border control technologies and working to find solutions that balance security and human rights.

REFERENCES

[1] A. Hanaa Mohsin y S. E. Haider, «WITHDRAWN: Survey of an intelligent surveillance system for monitoring international border security,» Materials Today: Proceedings, pp. 2214-7853, 2021.
[2] P. Marks, «Sensors and robots aim to bolster border security,» New Scientworldwide enable0-21, 2010.
[3] «Border control gets smarter – and safer,» Card Technology Today, vol. 19, nº 11, pp. 12-13, 2007.
[4] B. O. Martins y M. G. Jumbert, «EU Border technologies and the co-production of security 'problems' and 'solutions'» Journal of Ethnic and Migration Studies, vol. 48, nº 6, pp. 1430-1447, 2022.
[5] B. T. Koca, «Bordering processes through the use of technology: the Turkish case,» Journal of Ethnic and Migration Studies, vol. 48, nº 8, pp. 1909-1926, 2022.
[6] M. Bhattacharya y A. Roy, «Smart Border Security System Using Internet of Things,» pp. 268-279, 2020.
[7] A. Goyal y e. al, «Automatic Border Surveillance Using Machine Learning in Remote Video Surveillance Systems,» 2020, pp. 751-760.
[8] S. Darwante y e. al, «Border Surveillance Monitoring Application,» de 2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA), Pune, India, 2019.
[9] A. Weissenfeld y e. al, «Towards Mobile Contactless 4-Fingerprint Authentication for Border Control,» de 2018 European Intelligence and Security Informatics Conference (EISIC), Karlskrona, Suecia, 2018.
[10] M. G. Jumbert, «¿Control o rescate en el mar? Objetivos y límites de las tecnologías de vigilancia de fronteras en el mar Mediterráneo,» Desastres, vol. 42, nº 4, pp. 674-696, 2018.
[11] M. Clabian, «FastPass: automated border control as a challenging combination of various security technologies,» 2014.

[12] J. He, R. Norwood, M. Fallahi y N. Peyghambarian, «Solar-powered ad-hoc wireless sensor network for border surveillance,» Proceedings of SPIE - The International Society for Optical Engineering, vol. 8377, 2012.
[13] W. Butler, «Design Considerations for Intrusion Detection Wide Area Surveillance Radars for Perimeters and Borders,» de 2008 IEEE Conference on Technologies for Homeland Security, Waltham, MA, Estados Unidos, 2008.
[14] C. Hurrey, «The 'Swiss Army Knife' Approach to Border Control: Multitasking in a Multi-threat World,» de The 'Swiss Army Knife' Approach to Border Control: Multitasking in a Multi-threat World, Uppsala, Suecia, 2013.
[15] A. Owen, G. Duckworth y J. Worsley, «OptaSense: Fibre Optic Distributed Acoustic Sensing for Border Monitoring,» de 2012 European Intelligence and Security Informatics Conference, Odense, Dinamarca, 2012.

THE AUTHORS

Henry Ayala, Artillery Captain in the Ecuadorian Army, Artillery Group Multiple Launchers No. 80 "CALDERON." 80 "CALDERON," Bachelor in Military Sciences Escuela Superior Militar Eloy Alfaro, Knowledge in Human International Law (FAE War Academy), Law Student UTPL (Ecuador), Human Talent Officer of GA7 "CABO MINACHO" 2017-2019, Logistics Officer GAAA5 "MAYOR VALENCIA" 2020-2021, Human Talent Officer GA5 "ATAHUALPA" and GALM80 "CALDERON" 2021-2023.

Willians Yange, Artillery Captain in the Ecuadorian Army, Multiple Launcher Artillery Group No. 80 "CALDERON," Bachelor in Military Sciences at the Escuela Superior Militar Eloy Alfaro. Knowledge in chart digitalization, accident investigation, air defense planning, international humanitarian law and military technology, and human resources. Instructor of the Artillery School of the Ecuadorian Army 2015-2017.

Carolina Enríquez, Transport Captain in the Ecuadorian Army, Logistic Support Command N°9, Bachelor in Military Sciences at the Eloy Alfaro Military School (Ecuador). Knowledge in management, maintenance, and supply of logistic resources. Commander of the Supply Platoon in CL74 "HUANCAVILCA 2012-2014. Commander of light and medium vehicles platoon in CL75 "AUCA" 2014-2016. Logistics platoon commander of the CL72 "SHYRIS" 2017-2020. Platoon Commander support of CAL9 2021.military communications systems, pedagogy, languages, and human resources.

Heidy Tamayo, Second Lieutenant of Communications in the Ecuadorian Army, Infantry Battalion No. 2 "Imbabura," Bachelor of Military Sciences at the Escuela Superior Militar "Eloy Alfaro". Instructor at the Conscripts Instruction Center at the Artillery Brigade N°27 "PORTETE". Knowledge in human rights.