IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, February 2026
Impact Factor: 8.2

Border Surveillance System Using Dual Biometric Authentication

Vishwajeet Sasulkar[1], Ashwinder Singh Hanspal[2], Harpreet Kaur Sandhu[3], Tanishka Babar[4], Prof. Ms. Rashmi Howal[5]
Diploma Students, Department of Computer Engineering[1-4]
Guide, Department of Computer Engineering[5]
Pimpri Chinchwad Polytechnic, Pune, India
vishwajeetsasulkar5515@gmail.com, ashwinderhanspal515@gmail.com,
sandhuharpreetkaur553@gmail.com, tanishkababar10@gmail.com

Abstract: *Border security is a critical concern for national safety, requiring advanced technological solutions to prevent illegal infiltration, identity fraud, and unauthorized access. Traditional border surveillance systems largely depend on manual verification methods and physical monitoring, which are time-consuming, error-prone, and inefficient. To overcome these limitations, this research paper presents a Border Surveillance System based on biometric authentication, utilizing face recognition and fingerprint recognition techniques. The proposed system integrates biometric technologies to provide a secure, reliable, and automated identity verification mechanism at border checkpoints. Face recognition is employed for non- intrusive real-time identification, while fingerprint recognition ensures highly accurate personal authentication. The dual-biometric approach enhances security by reducing false acceptance and rejection rates. This system is designed to assist border authorities by enabling rapid identity verification, real-time monitoring, and secure data management.*

The proposed model demonstrates improved accuracy, scalability, and efficiency over conventional surveillance methods. This research highlights the implementation details, system architecture, working methodology, and future scope of biometric-based border surveillance systems.

Keywords: Border Surveillance, Biometrics, Face Recognition, Fingerprint Recognition, Authentication, Security Systems

I. INTRODUCTION

Border surveillance is an important part of national security because it helps keep people from crossing international borders illegally and stops crimes like smuggling, terrorism, and identity theft. As more people travel and move around the world, border control officials have a harder time making sure they are who they say they are while still keeping things safe and efficient. Manual checks of identity documents and physical monitoring by security personnel are a big part of traditional border surveillance systems. These methods are often slow, require a lot of work, and are prone to mistakes.

There are significant security risks associated with the forging, theft, or misuse of traditional identification methods like passports, visas, and identity cards. When a lot of travellers need to be processed fast during peak hours, manual verification also becomes ineffective. These drawbacks emphasise the necessity of an automated, dependable, and secure identification system that can improve border security and lessen reliance on human intervention.

These issues have been effectively addressed by biometric authentication systems, which identify people by their distinct physiological traits. Because biometric characteristics are hard to duplicate, they are ideal for applications that require high security. Face recognition and fingerprint recognition are the most popular biometric technologies because of their high accuracy, ease of use, and universality.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, February 2026
Impact Factor: 8.2

Face recognition is a contactless, non-intrusive technique that uses camera-captured facial features to enable real-time identification. Because of this, it is especially appropriate for surveillance settings where convenience and speed are crucial. However, elements like pose variations, facial expressions, and lighting can have an impact on face recognition systems. Conversely, one of the earliest and most trustworthy biometric methods is fingerprint recognition. Because fingerprint patterns are distinct and stable over time, they offer extremely reliable authentication. However, a sensor's usefulness as a stand-alone solution may occasionally be limited by the need for physical contact.

Recent studies have concentrated on multimodal biometric authentication, which combines two or more biometric characteristics to increase accuracy and security, in order to get around the drawbacks of single biometric systems. The shortcomings of one modality can be offset by the advantages of the other by combining fingerprint and face recognition. By drastically lowering false acceptance and rejection rates, this combined strategy improves system reliability.

This study suggests a multimodal biometric authentication system for border surveillance that uses fingerprint and face recognition. At border checkpoints, the suggested system seeks to offer safe, automated, and effective identity verification. The system improves overall border security and provides a workable answer to contemporary surveillance needs by reducing human intervention and improving authentication accuracy.

II. LITERATURE SURVEY

Because of the growing problems with illegal immigration, cross-border crimes, terrorism, and identity fraud, border surveillance and security systems have become increasingly important in recent years. Conventional border control methods primarily depend on security personnel's physical surveillance and manual examination of identity documents like passports and visas. Despite being in use for decades, these techniques are frequently laborious, ineffective, and susceptible to document forgery and human error. These restrictions have spurred researchers to investigate technologically advanced and automated security solutions.

Systems for biometric authentication have become a dependable substitute for traditional identification techniques. The identification of people using distinctive physiological traits that are hard to duplicate or steal is known as biometrics. For security applications, researchers have thoroughly examined a variety of biometric characteristics, including face, fingerprint, iris, voice, and palm print. Because of their uniqueness, stability, and ease of data collection, face recognition and fingerprint recognition are the most extensively studied and used of these.

Applications for face recognition technology in law enforcement, access control, and surveillance systems are numerous. Face recognition-based systems that identify people using image processing and pattern recognition techniques have been proposed in a number of studies. Face recognition's primary benefit is its non-contact and user-friendly nature, which makes it appropriate for real-time surveillance settings like border checkpoints. However, studies have revealed that face recognition systems may have issues with image quality, pose changes, facial expressions, and lighting variations. When face recognition is employed as a stand-alone authentication technique, these factors may lower accuracy.

One of the most dependable biometric identification methods for a long time has been fingerprint recognition. Numerous studies demonstrate that each person's fingerprint pattern is distinct and doesn't change over time. In general, fingerprint-based authentication systems offer low false acceptance rates and high accuracy. Fingerprint recognition has been successfully used by researchers in access control systems, forensic investigations, and security systems. Fingerprint recognition systems may encounter difficulties like sensor noise, dry or damaged fingers, and the need for physical contact, which can occasionally impair user convenience, despite their high reliability.

To overcome the limitations of unimodal biometric systems, researchers have proposed multimodal biometric authentication systems that combine two or more biometric traits. Multimodal systems improve security by reducing dependency on a single biometric feature and increasing resistance to spoofing and impersonation attacks. Research studies demonstrate that integrating face and fingerprint recognition significantly enhances authentication accuracy and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, February 2026 Impact Factor: 8.2

system robustness. Even if one biometric modality fails due to environmental or sensor-related issues, the other modality ensures reliable verification.

Recent studies in border security applications emphasize the importance of multimodal biometric systems for high-security environments. Researchers have shown that such systems reduce false acceptance and false rejection rates while improving overall system reliability. However, many existing systems focus on complex architectures and expensive hardware, which may not be suitable for student-level or cost-effective implementations.

Based on the reviewed literature, it is evident that a multimodal biometric-based border surveillance system can effectively address the limitations of traditional and unimodal systems. This research builds upon existing studies by proposing a practical, efficient, and cost-effective border surveillance system using face and fingerprint biometric recognition, suitable for real-world deployment as well as academic research.

III. PROPOSED SYSTEM

The proposed Border Surveillance System is designed to enhance border security by implementing an automated and reliable identity verification mechanism using multimodal biometric authentication. The system integrates face recognition and fingerprint recognition technologies to accurately identify individuals attempting to cross border checkpoints. This approach aims to reduce manual intervention, minimize human error, and prevent unauthorized access.

In the proposed system, biometric data of authorized individuals is collected during the registration phase and securely stored in a centralized database. The facial images are captured using a camera, while fingerprint data is obtained through a biometric sensor. These biometric traits are chosen due to their uniqueness, permanence, and widespread acceptance in security applications.

During the verification process, the system captures real-time facial images and fingerprints of individuals at the border checkpoint. The captured data undergoes preprocessing to enhance quality and remove noise. Facial features and fingerprint characteristics are then extracted and compared with the stored biometric templates in the database.

Authentication is granted only when both face recognition and fingerprint recognition results are successfully matched. This dual-verification mechanism significantly reduces the chances of identity fraud, impersonation, and false authentication. If either of the biometric traits fails to match, access is denied and the system alerts the authorities for further verification.

The proposed system operates in real time and provides instant authentication results, making it suitable for high-traffic border surveillance environments. By combining two biometric modalities, the system improves accuracy, reliability, and security compared to traditional document-based and single-biometric systems

IV. METHODOLOGY

The methodology of the proposed Border Surveillance System focuses on providing a secure, reliable, and automated mechanism for identity verification using multimodal biometric authentication. The system is designed to minimize human intervention while ensuring high accuracy and efficiency in border surveillance operations. It follows a structured workflow that includes biometric data acquisition, preprocessing, feature extraction, matching, and decision-making.

Initially, biometric data of authorized individuals is collected and stored in the system database during the enrollment process. Facial images are captured using a camera under controlled conditions to ensure clarity and consistency, while fingerprint samples are obtained through a biometric fingerprint sensor. The captured biometric data undergoes preprocessing to enhance image quality, remove noise, and standardize the input format. This step is essential to improve the reliability of the feature extraction and matching processes.

From the preprocessed facial images, distinctive facial features are extracted using face recognition techniques. These features represent unique characteristics of an individual's face and are used for identification purposes. Similarly,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, February 2026
Impact Factor: 8.2

fingerprint images are processed to extract unique fingerprint features such as ridge patterns and minutiae points. The extracted features from both biometric modalities are securely stored in the database along with the individual's identification information.

During real-time system operation, facial images and fingerprint samples of individuals attempting to cross the border are captured. The newly acquired biometric data is subjected to the same preprocessing and feature extraction steps to maintain consistency. The extracted facial and fingerprint features are then compared with the corresponding stored biometric templates in the database using matching algorithms.

Authentication is granted only when both biometric comparisons result in a successful match. This dual-authentication mechanism significantly reduces the chances of unauthorized access, identity fraud, and impersonation. In case of any mismatch or failure in verification, the system immediately denies access and notifies the authorities for further inspection and manual verification if required.

The system provides instant authentication results, enabling smooth and efficient border surveillance without causing delays. By integrating face recognition and fingerprint recognition into a single framework, the proposed methodology enhances overall system reliability, accuracy, and security. This approach makes the system suitable for real-world border surveillance applications where high security and operational efficiency are essential.

V. RESULTS AND DISCUSSION

The proposed Border Surveillance System using face and fingerprint biometric recognition was implemented and tested to evaluate its effectiveness in terms of authentication accuracy, system reliability, response time, and overall security performance. The system was tested under controlled conditions that simulate real-world border checkpoint scenarios involving authorized and unauthorized individuals.

During testing, the system successfully captured facial images and fingerprint data and performed biometric authentication in real time. The face recognition module provided quick and contactless identification, making it suitable for surveillance environments where speed and convenience are important. The fingerprint recognition module demonstrated high accuracy due to the uniqueness and permanence of fingerprint patterns, contributing significantly to secure identity verification.

When both biometric modalities were used together, the system showed a noticeable improvement in authentication accuracy compared to using a single biometric trait. The combined biometric approach reduced false acceptance cases, where unauthorized individuals are mistakenly granted access, and false rejection cases, where authorized individuals are incorrectly denied access. This confirms that multimodal biometric authentication enhances system reliability and security.

The response time of the system was found to be acceptable for practical border surveillance applications. Although the combined authentication process required slightly more processing time than individual biometric methods, the delay was minimal and did not affect system usability. The trade-off between response time and improved security was considered acceptable for high-security environments such as border checkpoints.

The results also indicate that the system effectively reduces dependency on manual document verification and human decision-making. Automated biometric authentication minimizes the chances of identity fraud, impersonation, and human error. In cases where biometric mismatch occurred, the system correctly denied access and generated alerts for further inspection, ensuring an additional layer of security.

Overall, the experimental results demonstrate that the proposed system provides a secure, efficient, and reliable solution for border surveillance. The integration of face and fingerprint recognition strengthens authentication accuracy and enhances resistance to unauthorized access. The discussion confirms that the proposed system is suitable for real-world implementation and aligns with the objectives of improving border security through advanced biometric technologies.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, February 2026
Impact Factor: 8.2

VI. APPLICATIONS

The proposed Border Surveillance System using face and fingerprint biometric recognition can be applied in various security-sensitive and real-world environments where accurate identity verification is required. Some of the major applications of the proposed system are as follows:

1. Border Checkpoints and Immigration Control

The system can be deployed at international borders, immigration counters, and check posts to verify the identity of travelers. It helps in preventing illegal entry and identity fraud by ensuring that only authorized individuals are allowed to cross the border.

2. Airports and Seaports

Airports and seaports require high-level security due to heavy passenger movement. The proposed biometric system can be used for passenger verification, reducing manual document checks and improving security efficiency.

3. Defense and Military Zones

The system can be used to control access to restricted defense and military areas. Multimodal biometric authentication ensures that only authorized personnel are permitted to enter sensitive zones.

4. Government Security Facilities

Government buildings and sensitive administrative offices can use the system to enhance access control and prevent unauthorized entry.

5. High-Security Checkpoints

The system is suitable for deployment at high-security checkpoints such as research centers, nuclear facilities, and critical infrastructure locations.

6. Criminal Identification and Monitoring

The biometric system can assist law enforcement agencies in identifying suspects and monitoring individuals with restricted access permissions.

7. Smart Surveillance Systems

The proposed system can be integrated with smart surveillance infrastructure to provide automated and intelligent security solutions.

VII. CONCLUSION AND FUTURE SCOPE

This research work presented the design and implementation of a Border Surveillance System using face and fingerprint biometric recognition with the objective of improving security, accuracy, and efficiency at border checkpoints. Traditional border surveillance methods primarily rely on manual document verification and human monitoring, which are often time-consuming and vulnerable to errors, impersonation, and identity fraud. The proposed system addresses these challenges by introducing an automated biometric authentication mechanism that enhances reliability while reducing human intervention.

The system utilizes a multimodal biometric approach by combining face recognition and fingerprint recognition. Face recognition enables quick and contactless identification, making it suitable for real-time surveillance environments, while fingerprint recognition provides high accuracy due to the uniqueness and permanence of fingerprint patterns. The integration of these two biometric modalities strengthens authentication by compensating for the limitations of individual techniques. The experimental results demonstrate that the proposed system achieves higher accuracy, lower false acceptance rates, and improved reliability when compared to single biometric systems.

The implementation of the proposed system also shows that biometric-based authentication significantly reduces dependency on physical identity documents and manual inspection. Automated verification minimizes operational delays and enhances the overall efficiency of border surveillance operations. In addition, the system is capable of providing instant authentication results, making it suitable for high-traffic border checkpoints and security-sensitive environments. The results confirm that the proposed solution is practical, secure, and effective for real-world border surveillance applications.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, February 2026 Impact Factor: 8.2

In terms of future scope, the proposed system offers several possibilities for further enhancement and expansion. Advanced biometric techniques such as iris recognition, voice recognition, or behavioral biometrics can be integrated to further strengthen system security. The application of artificial intelligence and deep learning algorithms can improve face recognition accuracy under challenging conditions such as poor lighting, occlusion, and pose variations.

Future implementations can also include cloud-based data storage and centralized databases to enable real-time data sharing across multiple border checkpoints. Integration with national or international identity databases can further enhance authentication reliability and tracking capabilities. Additionally, the system can be extended with real-time alert mechanisms, intelligent analytics, and reporting tools to assist authorities in detecting suspicious activities and making informed security decisions.

With continuous advancements in biometric and surveillance technologies, the proposed system has the potential to evolve into a comprehensive and intelligent border surveillance solution. Such enhancements will enable the system to effectively address future security challenges while ensuring safer and more efficient border management.

VIII. ACKNOLEDGMENT

I would like to express my sincere gratitude to all those who contributed to the successful completion of this research work titled “Border Surveillance System Using Face and Fingerprint Biometric Recognition.”

First and foremost, I am deeply thankful to my project guide for their valuable guidance, constant support, and constructive suggestions throughout the development of this project. Their encouragement and technical insights played a crucial role in shaping this research work.

I would also like to thank the Head of the Department, Computer Science, and all the faculty members of Pimpri-Chinchwad Polytechnic for providing the necessary resources, academic support, and a conducive learning environment during the course of this project.

I extend my heartfelt appreciation to my friends and classmates for their cooperation, motivation, and assistance during various stages of the project. Their support and discussions greatly contributed to the successful implementation of the system.

Finally, I would like to express my sincere gratitude to my parents and family members for their continuous encouragement, moral support, and patience throughout my academic journey. Without their support, this work would not have been possible.

REFERENCES

[1]. Jain, A. K., Ross, A., and Prabhakar, S., “An Introduction to Biometric Recognition,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, 2004.

[2]. Gonzalez, R. C., and Woods, R. E., Digital Image Processing, 3rd ed., Pearson Education, 2008.

[3]. Maltoni, D., Maio, D., Jain, A. K., and Prabhakar, S., Handbook of Fingerprint Recognition, 2nd ed., Springer, 2009.

[4]. Zhao, W., Chellappa, R., Phillips, P. J., and Rosenfeld, A., “Face Recognition: A Literature Survey,” ACM Computing Surveys, vol. 35, no. 4, pp. 399–458, 2003.

[5]. Li, S. Z., and Jain, A. K., Encyclopedia of Biometrics, Springer, 2015.