

AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM: A CRITICAL REVIEW OF TECHNOLOGY, ACCURACY, AND FORENSIC APPLICATIONS

Dr Nadia Aslam¹, Malaika Jamil^{*2}, Muhammad Faisal³, Aqsa Ikram⁴,
Zainab Noor⁵, Saifullah Memon⁶

^{1, *2,3,4,5,6}Department of Forensic Medicine and Toxicology, Liaquat University of Medical and Health Sciences (LUMHS), Jamshoro

¹drnadiaaslam77@gmail.com, ²akialamkz@gmail.com, ³abbasifaisalali730@gmail.com,
⁴aqsaawan322@gmail.com, ⁵zainabnoor438@gmail.com, ⁶saifullahmemon865@gmail.com

DOI: <https://doi.org/10.5281/zenodo.19412752>

Keywords

Forensic science, automated fingerprint identification system (AFIS), biometric, fingerprint identification, criminal investigation.

Article History

Received: 01 February 2026

Accepted: 17 March 2026

Published: 31 March 2026

Copyright @Author

Corresponding Author: *

Malaika Jamil

Abstract

Background: Fingerprint identification is a dependable and widely used tool in forensic science because friction ridge patterns are unique and permanent. Traditional manual fingerprint inspection is time-consuming and requires significant human effort, particularly when comparing fingerprints across large criminal databases. The Automated Fingerprint Identification System (AFIS) has greatly enhanced forensic identification by allowing for the automated storage, processing, and comparison of fingerprints.

Objective:

The purpose of this review is to objectively investigate the Automated Fingerprint Identification System (AFIS)'s creation and operational principles, as well as to assess its forensic applications, benefits, limitations, and emerging technological breakthroughs in fingerprint identification.

Methods:

This review draws on previously published research articles, review papers, and forensic science studies about fingerprint identification and AFIS technology. Relevant literature was gathered from scholarly databases and peer-reviewed journals to evaluate the technological processes and forensic applications of automated fingerprint recognition systems.

Results:

According to the studied research, AFIS considerably enhances the speed, accuracy, and efficiency of fingerprint identification. It allows for the quick comparison of latent fingerprints to massive digital databases, which aids law enforcement in suspect identification, forensic intelligence, and cold-case investigations. Poor-quality fingerprints, expensive implementation costs, and the necessity for expert verification can all have an impact on system performance.

Conclusion:

AFIS has become an indispensable instrument in modern forensic investigations. Ongoing improvements in artificial intelligence, machine learning, and advanced imaging technologies are projected to increase the accuracy, reliability, and efficiency of automated fingerprint identification systems in future forensic applications.

INTRODUCTION:

In modern criminal investigations, forensic evidence plays a critical role in guaranteeing precise identification and the administration of justice. Despite advances in technology, fingerprint identification remains one of the most dependable and popular forensic techniques. Fingerprints are an effective method of linking people to crime scenes because of the distinctiveness and durability of friction ridge patterns [1] (Fig. 1). In forensic science, dactyloscopy—also known as fingerprint identification—is widely used for personal identification. Investigators can use this method to compare latent prints taken from crime scenes with known records that have been gathered from suspects or kept in databases. Fingerprints are a reliable biometric identifier as their unique characteristics remain unchanged over the course of a person's life [2]. In the past, fingerprints were even employed as signatures on clay seals in ancient China to confirm their legitimacy [1]. Traditional fingerprint recognition techniques, however, have several limitations. It takes a lot of time and highly qualified examiners to manually compare latent prints; they may need to check hundreds or thousands of records. Millions of fingerprints are stored in contemporary databases, making manual searching practically impractical and ineffective [3]. The Automated Fingerprint Identification System (AFIS) was created in the 1960s to overcome these issues, and it has since experienced substantial improvements. To improve speed and accuracy, modern AFIS uses sophisticated algorithms, machine learning, and automated procedures. It is a vital tool for law enforcement organizations across the globe because of its extensive use in applications including criminal investigations, border control, and civil identity systems [4]. Digital photographs of friction ridge patterns, such as fingerprints, palmprints, and footprints, are stored and processed by AFIS, a biometric system. It enables quick comparison and matching of prints in large databases, ensuring effective record management and the speedy

retrieval of pertinent data [5]. Ten-print searches (rolling and slap impressions) and latent print searches are the two types of searches that the system usually does. Ten-print identification has become widely used because of technological developments that have greatly increased its automation and accuracy [6]. Despite its benefits, AFIS performance is impacted by several factors, including organizational elements (like data security and accessibility), system configuration (like workflow and algorithms), and human factors (like examiner stress levels and competence) [5]. Although fingerprint identification has been transformed by technology, human practices have not yet fully embraced these developments [7]. Additionally, forensic capabilities have been greatly enhanced by the integration and sharing of fingerprint databases between various jurisdictions. This has made it possible for law enforcement to cross-reference data to identify missing persons, connect cross-border crimes, and resolve long-standing cold cases [8]. As a result, the goal of this review is to offer a thorough assessment of AFIS technology, taking into account its essential components, technological developments, and historical evolution. It also looks at existing constraints, like how to handle incomplete or low-quality fingerprints and difficulties integrating with other biometric systems. In order to enhance AFIS's dependability, security, and forensic applications, the study also examines current advancements and potential future research avenues. Despite the widespread use of Automated Fingerprint Identification Systems (AFIS), challenges such as low-quality latent fingerprints, database interoperability, algorithm transparency, and system reliability in real-world forensic conditions remain significant concerns. Therefore, a comprehensive review of AFIS technology, its operational framework, advantages, limitations, and recent technological advancements is necessary to understand its role in modern forensic science and future development.

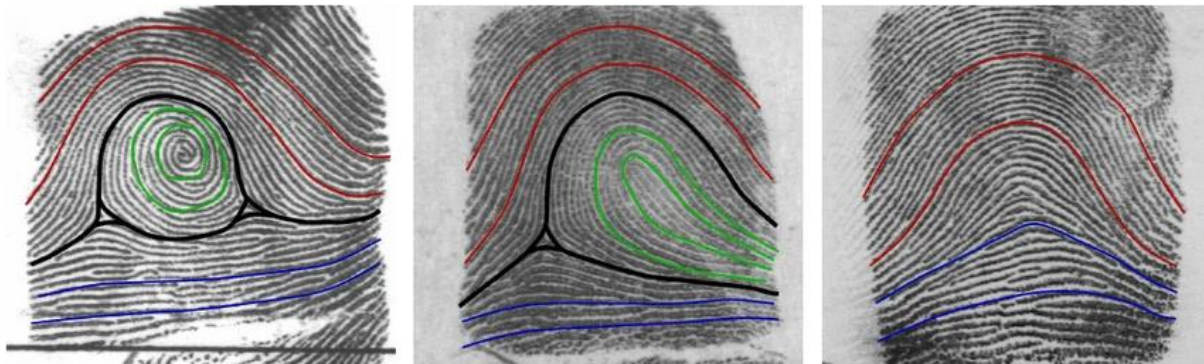


Figure 1: Basic fingerprint patterns, including a. whorl, b. loop, and c. arches (Feng, Jianjiang & Jain, Anil & Ross, Arun. (2009). Fingerprint Alteration. depicts the three basic fingerprint pattern types: whorl, loop, and arch. These patterns serve as the foundation for fingerprint classification systems and are utilized in AFIS databases to effectively index and search fingerprint records

Literature Review

Automated Fingerprint Identification Systems (AFIS) are becoming increasingly important in contemporary forensic science, according to recent studies. One of the most dependable and popular techniques for identifying people is still fingerprint analysis, which is essential to criminal investigations. The efficiency of fingerprint-based biometric systems in guaranteeing safe access control and safeguarding private information is highlighted by Kirvel (2020) [9]. Although the reliability and applicability of fingerprint recognition are strongly supported by this study, it mainly concentrates on ideal conditions and offers little insight into how well the system performs when handling partial, distorted, or low-quality fingerprint impressions.

The primary focus of later studies has shifted to assessing the security and resilience of fingerprint recognition systems. Specifically, research on the creation of artificial fingerprint patterns seeks to evaluate system performance in controlled testing conditions. These studies are important for finding flaws in biometric systems and strengthening their resilience. They do, however, also highlight serious flaws like spoofing and presentation attacks, which were not adequately covered in previous research. In contrast to Kirvel (2020) [10], these studies offer a more critical assessment by emphasizing both system limitations and performance enhancements.

Li et al. [11] demonstrated that deep convolutional neural networks (CNNs) are highly effective in enhancing latent fingerprint quality, particularly in cases involving poor or

incomplete impressions, thereby improving overall matching accuracy in automated fingerprint identification systems. AI-driven systems perform better and are more flexible than traditional approaches. Herke [3] supports the use of hybrid approaches that combine AI and human expertise, but he also points out that fully automated systems may still have reliability problems. This is in contrast to previous research that mainly focused on automation without critically examining practical constraints.

Research Gap:

Despite these developments, there are still a number of significant gaps in the literature. First, the majority of studies only look at one aspect of AFIS, such as accuracy, security testing, or AI integration, without offering a thorough comparison of these methods within a single framework. Second, standard evaluation criteria for evaluating AFIS performance under various forensic conditions are lacking, especially in real-world scenarios where fingerprints are partial, noisy, or degraded. Third, there is little empirical data supporting the efficacy of hybrid human-AI systems in operational forensic settings, despite the fact that they are suggested as more dependable solutions.

In order to guarantee the practical dependability of hybrid systems in forensic investigations, there is an obvious need for integrated comparative studies that assess conventional, security-focused, and AI-based AFIS approaches collectively.

METHODOLOGY:

Research Design

This study uses a structured narrative review supported by a PRISMA-based approach to ensure transparency in the selection and review of relevant literature. Although this methodology is not a comprehensive systematic review, it adheres to the Preferred Reporting Items for Major Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to improve rigor and reproducibility.

Information Sources

A comprehensive literature search was conducted using major academic databases, including Google Scholar, PubMed, Scopus, and ScienceDirect. These databases were selected to ensure broad coverage of peer-reviewed forensic and biometric research. Additionally, a manual search of the reference lists of relevant articles was performed to identify additional studies.

Search Methodology

A systematic search strategy was employed using the following combinations of keywords:

"Automatic Fingerprint Identification System (AFIS)"

"Latent fingerprint identification"

"Fingerprint image enhancement."

"Biometric authentication"

"Feature extraction"

"Forensic Fingerprint Identification"

Boolean operators (AND, OR) were used to narrow down the search results and increase their relevance.

To ensure that AFIS included recent technological advances, the search was limited to studies published between 2015 and 2025.

Criteria for Inclusion

Inclusion criteria:

Peer-reviewed journal articles

Studies focused on AFIS technology

Research on latent fingerprint analysis

Studies covering forensic applications

Research on the analysis and enhancement of latent fingerprints

Articles covering forensic applications of fingerprint identification

Exclusion criteria:

Research not directly related to AFIS

Articles lacking methodological clarity

Non-peer-reviewed sources

Studies with insufficient or irrelevant data.

Application of fingerprint authentication

Selection of Articles

The study selection process took place in several stages after being selected based on PRISMA.

Identification:

A total of 135 records were identified through database searches and additional sources.

Screening:

After removing duplicates, 110 records remained, which were screened based on title and abstract.

Of these, 70 studies were excluded due to a lack of relevance or attention to forensic fingerprint systems.

Eligibility:

Forty full-text articles were assessed for eligibility. Of these, 16 articles were excluded for the following reasons:

Not AFIS oriented (n=6)

Lack of methodological clarity (n = 5)

No peer review (n=5)

Inclusion:

A total of 24 studies were included in the final qualitative synthesis.

The study selection process is illustrated in the PRISMA flowchart

Limitations of the methodology

Although we strive to be rigorous, this review has certain limitations.

This study is based on a limited number of selected papers, which may result in selection bias.

Additionally, differences in study designs and assessment measures in the included literature may affect the comparability of results. The lack of quantitative meta-analysis further limits the generalizability of the results

Analysis of Data:

This assessment employs a methodical narrative style to examine the efficacy, dependability, and legal relevance of fingerprint recognition systems. Pertinent literature was sourced from peerreviewed articles that concentrate on AFIS performance, forensic uses, and judicial acceptance; nevertheless, the narrow selection of studies introduces potential bias and limits thorough exploration of the discipline.

While research such as Hicklin et al. indicates high accuracy among examiners in controlled settings, their conclusions depend heavily on laboratory conditions and may exaggerate reliability in actual forensic scenarios where print quality and environmental pressures fluctuate considerably.[12] Conversely, Smith and Horne highlight the practical value of fingerprint systems in criminal inquiries, yet their evaluation lacks solid quantitative backing and does not adequately scrutinize error margins or decision-making biases.[13] Mahalakshmi's legal review underscores the increasing acceptance of fingerprint evidence; however, it is still confined by jurisdiction-specific interpretations and does not engage with current discussions about the scientific credibility and consistency of fingerprint evidence across different legal frameworks.[14] Together, these studies bolster the perceived trustworthiness of fingerprint identification systems, yet notable limitations remain, including inadequate focus on examiner bias, a lack of methodological clarity, and minimal comparative evaluations across a variety of forensic environments. These flaws ultimately restrict the generalizability and scientific soundness of the insights drawn from the existing literature.

1.1 Overview of Automated Fingerprint Identification System

The Automated Fingerprint Identification System (AFIS) is a biometric device that stores digital representations of friction ridge skin, such as fingerprints, palm prints, and footprints, and can quickly search databases to find matches between impressions. AFIS provides an electronic database for accurate record management and quick access to pertinent information [5]. Furthermore, AFIS simplifies the identification process by digitizing and

automating fingerprint comparison, which considerably reduces manual effort. Modern fingerprint analysis techniques are highly accurate, fast, and efficient, with the ability to examine complicated ridge patterns in detail. Although AFIS has significantly increased the speed and accuracy of fingerprint recognition, some obstacles remain, particularly in the analysis of low-quality or partial latent fingerprints, which may influence matching performance [15].

1.2 Historical development of the automated fingerprint identification system (AFIS)

The Automated Fingerprint Identification System (AFIS) evolved from old manual fingerprint classification approaches, such as the Henry system, which needed substantial time and human effort to evaluate big fingerprint databases. Pioneers such as Edward Henry and Francis Galton created fingerprint identification as a reliable approach in the early 1900s, eventually replacing earlier anthropometric techniques and becoming common practice in law enforcement departments around the world [16]. During the 1960s, the rapid expansion in criminal fingerprint data necessitated the development of automatic identification systems. With improvements in digital computing, biometric technologies began to grow, resulting in the creation of AFIS. In 1974, the Federal Bureau of Investigation launched AFIS, which used digitally stored minutiae points—unique ridge characteristics—to perform automated fingerprint comparison. Over time, technological improvements have substantially enhanced the efficiency and accuracy of fingerprint recognition systems. Modern AFIS can search millions of fingerprint records in seconds, making it an indispensable tool for criminal investigations and international data sharing between law enforcement agencies. In this context, fingerprint recognition has become a critical component of global biometric security systems[17]. Furthermore, the Integrated Automated Fingerprint Identification System (IAFIS) improved the speed and accuracy of forensic identification. Subsequent improvements have resulted in more advanced and efficient AFIS implementations, boosting its importance in

modern forensic science (Moses, 1986; IAL, 1999).

1.2.1 Historical Development of AFIS in Pakistan:

In Pakistan, the Automated Fingerprint Identification System (AFIS) was developed as part of measures to modernize law enforcement and improve criminal identification processes. In 2008, the National Police Bureau initiated the AFIS project for the Khyber Pakhtunkhwa police. Phase I of the project was carried out in 60 districts throughout Pakistan, including the Khyber Pakhtunkhwa province. Phase II, which has yet to be fully completed, aims to expand the system to the other districts in the country. The Pakistan AFIS project aims to connect the Federal Investigation Agency headquarters with provincial and district police agencies via a centralized network. This integration allows for more effective data sharing of criminal records, particularly in the investigation of serious and transnational organized crimes. AFIS allows fingerprint evidence obtained from crime scenes to be quickly compared with existing database records, considerably improving the speed and accuracy of criminal identification and investigation operations [18].

1.3 Operational Architecture of the Automated Fingerprint Identification System

1.4 An Automated Fingerprint Identification System, or AFIS, combines methods for retrieving, processing, and analyzing fingerprint data with identifying technologies. The fundamental methods of AFIS are as follows:

1.3.1 Capturing the Fingerprints:

Scanners work on the basis of gathering light and high-quality images of fingerprints, whether they are rolled or flat. Electronic capacitance-based sensors detect ridges and grooves on the print's surface. An ultrasonic scanner gives clear ridge details and operates based on sound imaging in a two-dimensional plane. The workflow of AFIS is illustrated in Fig. 2.

1.3.2 Processing Images:

Improving fingerprint images involves adjusting contrast, filtering out noise, and correcting distortion. Segmentation: Makes the fingerprint

stand out from the background so it can be easily observed. Binarization: For efficient data extraction, the gray areas are divided into black and white.

1.3.3 Extraction of Features:

The technique of identifying specific pattern elements, such as ridge ends, bifurcations, and their layouts, that are helpful in matching procedures is known as "minutiae detection." Pattern recognition is the study of various finger forms and patterns, such as loops, whorls, and arches, for categorization and comparison.

1.3.4 Storage of databases:

The process of turning the collected features into plots that are stored on a disk for later comparison is known as template creation. Database management is the identification and modeling of the procedures involved in the use and storage of numerous people's fingerprints.

1.3.5 Matching Fingerprints:

One-to-One Matching: To determine whether a fingerprint template is accepted or rejected, the verification procedure compares each user-specified fingerprint template with the stored fingerprint template. (control of access). One-to-Many Matching: To ascertain the user's identification, the verification procedure compares the user-specified fingerprint template with a database containing all of the enrolled fingerprints. (illegal behaviour) Score Calculation: To determine whether or not two representations match within a predetermined threshold, algorithms calculate how similar their representations are and issue a match score.

1.3.6 Analysis After Match:

Making a Decision: Depending on the match score, the system either accepts or rejects the identification. Human Verification: Qualified experts may do customized verification in delicate circumstances.

1.3.7 Ongoing Education and Development:

Machine Learning Algorithms: By learning from previous identification comparisons and misidentifications, a modern AFIS can use machine learning techniques to improve its accuracy over time. The presented patterns

The diagram illustrates the fingerprint identification process, divided into two main stages: Enrollment and Identification.

Enrollment: This stage starts with "Ten prints or Livescan images" (represented by a grid of small fingerprint images). These images are processed by a "Quality Checker" and then a "Features Extractor". The output of the Features Extractor is stored in the "Fingerprint Database" (represented by a cylinder icon).

Identification: This stage starts with an "Unknown fingerprint" (represented by a large fingerprint image). This fingerprint is processed by a "Features Extractor" and then a "Pattern Matcher". The output of the Pattern Matcher is a "Top N ranking list" (represented by three small fingerprint images with vertical ellipsis between them). This list is then reviewed by an "Expert examiner" (represented by an icon of a person with a magnifying glass).

1.4 Pros of the automated fingerprint identification system (AFIS)

1.5 Limitations of the automated fingerprint identification system (AFIS)

Furthermore, some approaches may need extensive processing periods, making them

unsuitable for real-time or online applications. In such circumstances, an additional quality assessment module is frequently required to ensure valid findings, particularly when dealing with low-quality fingerprint photos [21].

1.6 Recent advancement of the automated fingerprint identification system (AFIS)

Future improvements in the Automated Fingerprint Identification System (AFIS) are projected to emphasize the use of artificial intelligence (AI) and machine learning (ML) to improve matching accuracy and reduce identifying errors. These technologies can automate pattern identification, improve decision-making, and reduce human involvement in forensic investigations [22]. Advancements in database management systems and real-time processing capabilities are also expected to boost the efficiency of large-scale fingerprint searches. Furthermore, the use of

modern sensors and multimodal biometric systems will improve the reliability and security of AFIS in law enforcement settings. Emerging advancements in nanotechnology and material science, such as the utilization of macromolecules and nanoparticles, provide promise for improving latent fingerprint detection. Magnetic and fluorescent nanoparticles can improve sensitivity and resolution, allowing the recovery of fingerprints that would otherwise be difficult to identify using traditional methods [23]. Furthermore, integrating 3D imaging technology into AFIS is predicted to dramatically improve fingerprint analysis. Three-dimensional imaging enables the collection of ridge depth and micro-relief patterns, resulting in improved matching precision. The use of AI and computer vision algorithms with 3D fingerprint data can improve spoof detection, ridge detail analysis, and overall system dependability while minimizing reliance on manual examination, as shown in Fig. 3 [23].



Figure 3: Artificial intelligence, 3D imaging, and machine-learning framework for future AFIS and advanced fingerprint recognition. illustrates the combination of artificial intelligence, machine learning, and 3D imaging technology in contemporary AFIS systems. These technologies improve fingerprint identification accuracy, enhance pattern extraction, and enable faster database searches. AI is expected to dramatically improve the reliability and efficiency of fingerprint identification in the future.

1.7 Application of AFIS in Forensic Science:

AFIS serves an important part in current forensic science and law enforcement through a variety of applications:

Rapid Identification: Allows fast matching of crime scene fingerprints with big databases, speeding up suspect identification.

Forensic Intelligence and Cold Cases: Re-analyzing old documents can help relate unresolved cases and identify repeat criminals.

Database Interoperability enables the sharing of fingerprint data across agencies and countries, hence boosting collaboration [5]

Access and Security Control: Used in authentication systems and criminal investigations to verify identities. **Post-Mortem Identification:** Aids in identifying deceased or unrecognizable individuals, particularly in catastrophe victim identification [14].

AFIS is widely used to link multiple crime scenes by matching latent fingerprints from different locations, helping investigators identify serial offenders and establish connections between related cases. [24].

DISCUSSION:

The Automated Fingerprint Identification System (AFIS) is becoming more and more important in contemporary forensic investigations, as this study demonstrates. AFIS greatly improves fingerprint identification speed, accuracy, and efficiency when compared to traditional manual fingerprint examination methods. The system makes it possible to quickly compare fingerprint impressions with sizable digital databases, which increases the efficiency of criminal investigations while lightening the forensic examiners' workload. These results are in line with earlier research that highlights how automated fingerprint technologies can improve forensic identification procedures [6].

The accuracy and dependability of fingerprint recognition systems have been further enhanced by recent technological developments, especially the combination of artificial intelligence (AI) and machine learning (ML) algorithms. Latent fingerprints, which are frequently incomplete, distorted, or of poor quality, can be analyzed thanks to these sophisticated computational techniques. As a result, contemporary AFIS systems outperform conventional techniques, particularly when managing intricate forensic evidence [3].

However, several shortcomings of AFIS are still apparent in spite of these developments. Matching accuracy can be greatly decreased by

elements like distortion, partial ridge patterns, low-quality latent prints, and inadequate evidence gathering. Furthermore, algorithmic constraints could result in false positives or false negatives, casting doubt on the accuracy of completely automated identification. AFIS should therefore be viewed as a supplementary tool rather than a total replacement for forensic specialists, as human fingerprint examiners are still necessary for verification and final decision-making [7].

From a critical standpoint, the reliance on AFIS also presents significant moral and legal issues. Significant obstacles include concerns about data privacy, illegal access to biometric databases, and possible misuse of fingerprint data. Furthermore, the lack of transparency in certain algorithmic processes—so-called 'black box' issue in AI systems—may have an impact on the admissibility of evidence in court and raise concerns about bias and accountability in forensic decision-making. Furthermore, while AFIS makes it easier to store large amounts of data and share information between agencies, its full potential may be hampered by differences in database standards, interoperability problems, and a lack of consistent protocols across regions. This suggests that fingerprint data management systems need to be globally standardized. A lack of focus on enhancing AFIS performance in real-world scenarios, where fingerprint quality is frequently subpar, is a significant research gap noted in the literature. The creation of more reliable algorithms that can handle partial and damaged fingerprints should be the top priority for future research. Studies on ethical frameworks, data security measures, and the explainability of AI-based forensic systems are also necessary. Practically speaking, AFIS performance is still heavily influenced by the quality of input fingerprint images. Low-resolution photos, smudging, and incomplete ridge details can all have a detrimental effect on matching results. As an outcome, suitable procedures for gathering, preserving, and enhancing images are crucial. Strict procedural guidelines must be followed by forensic professionals in order to guarantee accurate and trustworthy identification results. To sum up, AFIS is still essential to forensic science all over the world. Its limitations, ethical ramifications, and technical difficulties cannot be

disregarded, even though it offers substantial benefits in terms of speed, efficiency, and database management. To increase the dependability and efficacy of AFIS, ongoing advancements in algorithm design, database security, examiner training, and regulatory frameworks are required. In order to ensure accurate and reliable forensic identification, AFIS should be seen as an essential complementary tool where automated technology and human expertise collaborate [6][7]. This review provides a comprehensive overview of AFIS technology, its forensic applications, and recent technological advancements. However, the study is limited by the use of a narrative review approach and the limited number of included studies. Future research should focus on empirical evaluation of hybrid AI-AFIS systems and real-world forensic database performance.

FUTURE RECOMMENDATION:

- Development of more robust algorithms for low-quality fingerprints
- Integration of AI and deep learning models in AFIS
- Standardization of international fingerprint databases
- Improvement in data security and privacy protection
- Training of forensic experts for hybrid human-AI systems
- Development of 3D fingerprint recognition systems

CONCLUSION:

In conclusion, the efficiency of fingerprint analysis in forensic science has significantly increased with the creation of Automated Fingerprint Identification Systems (AFIS). AFIS helps forensic professionals identify people more accurately and efficiently by facilitating the quick comparison of latent prints with large databases. Even when working with incomplete or poor-quality prints retrieved from crime scenes, the reliability of fingerprint matching has been reinforced by the incorporation of sophisticated algorithms and digital technology. The system's performance may still be impacted by some issues, such as poor fingerprint quality or missing database records, although these

constraints are being addressed by ongoing technological advancements. In the end, AFIS has developed into a potent and essential instrument in contemporary forensic investigations, greatly aiding in precise human identification and bolstering the criminal justice system as a whole. With continuous advances in AFIS, it is anticipated to become even more important in the future of forensic science and criminal investigation due to developments in biometric technologies. Also, it is anticipated that the growing integration of artificial intelligence and sophisticated biometric technologies would significantly improve the accuracy and efficiency of AFIS in forensic labs. The system's capacity to evaluate complicated or deteriorated fingerprint evidence will probably be enhanced by ongoing research and technological advancement. As a result, AFIS will continue to be a key piece of forensic identification technology and an important tool for contemporary criminal investigations.

Conflict of interest

None

Funding source

None

Acknowledgment

None

DATA AVAILABILITY STATEMENT: No new data were created or analyzed in this study.

List of abbreviations

AFIS – Automated Fingerprint Identification System

IAFIS – Integrated Automated Fingerprint Identification System

CNN – Convolutional Neural Network

AI – Artificial Intelligence

ML – Machine Learning

NGI – Next Generation Identification

REFERENCES:

1. Faisal SM, Khan AS, Shahid A. The role of forensic evidence in modern criminal investigations. Pakistan Islamicus. 2024;4(1):1–12. Available from: <http://www.pakistanislamicus.com/index.php/home/article/view/93>

2. Suryani WI, Letri DA, Wahyudi AA. The function of fingerprints in the investigation process to identify criminal offenders. *Shishya Stud Perspect Law Justice*. 2025;1(2):61-67. Available from: <https://doi.org/10.63306/kj66wd05>
3. Herke C. Automated fingerprint identification: The role of artificial intelligence in crime scene investigation. *Forensic Sci*. 2026;6(1):1-10. Available from: <https://doi.org/10.3390/forensicsci6010006>
4. Patil SU. Automated fingerprint identification system. *Int J Res Appl Sci Eng Technol*. 2024;12:279-284. Available from: <https://doi.org/10.22214/ijraset.2024.64498>
5. Gibb C, Rieman J. Towards better AFIS practice and process in fingerprint analysis. *Forensic Sci Int Synergy*. 2023;7:100336. Available from: <https://doi.org/10.1016/j.fsisyn.2023.100336>
6. Singla N, Kaur M, Sofat S. Automatic latent fingerprint identification system: Review. *Forensic Sci Int*. 2020;309:110187. Available from: <https://doi.org/10.1016/j.forsciint.2020.110187>
7. Dror IE, Mnookin JL. The use of technology in human expert domains: Challenges and risks arising from automated fingerprint identification systems. *Law Probab Risk*. 2010;9(1):47-67. Available from: <https://doi.org/10.1093/lpr/mgp031>
8. National Institute of Justice, "Fingerprint Database Interoperability," March 27, 2013, Available from: <https://nij.ojp.gov/topics/articles/fingerprint-database-interoperability>
9. Arifin MD, Muslim M, Octaviani F, Faturachman D. Review of automatic identification system: Application, challenges, and limitations. *Int J Mar Eng Innov Res*. 2024;9(3):464-475.
10. Kirvel V. Fingerprint analysis (AFIS) and biometric system of identification by fingerprints: Issue of artificial papillary pictures. *Society and Innovations*. 2023. Available from: <https://inscience.uz/index.php/socinov/index>
11. Li J, Feng J, Kuo CCJ. Deep convolutional neural network for latent fingerprint enhancement. *Signal Process Image Commun*. 2018;60:52-63. Available from: <https://doi.org/10.1016/j.image.2017.08.010>
12. Hicklin RA, Richetelli N, Taylor A, Buscaglia J. Accuracy and reproducibility of latent print decisions from AFIS searches. *Forensic Sci Int*. 2025;112457. Available from: <https://doi.org/10.1016/j.forsciint.2025.112457>
13. Smith JH, Horne JS. The processing of forensic investigative leads in criminal investigations conducted by the South African Police Service. *Int J Soc Sci Res Rev*. 2024;7(4):284-303. Available from: <https://doi.org/10.47814/ijssrr.v7i4.1984>
14. Mahalakshmi V. Admissibility of fingerprint recognition evidence in Indian criminal trials: An ICT and legal perspective. *Indian J Legal Rev*. 2025;5(13):539-552. Available from: <https://iledu.in/>
15. Ragmac AR, Allanic EA. Enhancing fingerprint system: Bridging gaps to improve efficiency, standardization, and public trust. *Mediterr J Basic Appl Sci*. 2025;9(2):166-179. Available from: <https://doi.org/10.46382/MJBAS.2025.9215>
16. Guimarães F, Moita P, Morgado SMA. Enhancing law enforcement efficiency: A comparative study of manual and biometric systems. *Hungarian Law Enforcement*. 2025;25(Special Issue):111-125. Available from: <https://doi.org/10.32577/MR.2025.KS.Z.1.7>

17. Singh S. The evolution of forensic science in crime solving: From traditional methods to artificial intelligence. *J Forensic Sci Med.* 2026;12:11–14.
18. Shah SAA. Forensic fingerprints: An evidential clue for police officers in forensic investigation in Khyber Pakhtunkhwa, Pakistan. *Pak J Crim Justice.* 2025;5(1). Available from: <https://doi.org/10.62585/pjcj.v4i2.100>
19. Davitaia A. Advancements in fingerprint recognition: Applications and the role of machine learning. *SSRN Electronic Journal.* 2025. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5268481
20. Alagos J. Issues and challenges encountered by police officers in automated fingerprint identification system operation. *J Electr Syst.* 2024;20:1589–1599.
21. Hong L, Jain AK, Pankanti S, Bolle RM. Fingerprint enhancement. In: *Proceedings of the IEEE Workshop on Applications of Computer Vision.* 1998. Available from: https://www.researchgate.net/publication/2266348_Fingerprint_Enhancement
22. Ametefe DS, Sarnin SS, Ali DM, et al. Advancements and challenges in fingerprint presentation attack detection: A systematic literature review. *Neural Comput Appl.* 2025;37:1797–1819. Available from: <https://doi.org/10.1007/s00521-024-10423-8>
23. Hussain S, Khan A, Asif S, Zaib S, Saeed S. Magnetic fingerprinting, AFIS and beyond in forensic science: A review. *Kashf J Multidiscip Res.* 2024;1:40–72. Available from: <https://www.researchgate.net/publication/387966172>
24. Hefetz I, Liptz Y, Vaturi S, Attias D. Use of AFIS for linking scenes of crime. *Forensic Sci Int.* 2016;262:e25–e27. Available from : [doi:10.1016/j.forsciint.2016.03.003](https://doi.org/10.1016/j.forsciint.2016.03.003)

