Journal of
Information Technology,
Cybersecurity, and Artificial Intelligence

(ARTICLE TYPE)

The Admissibility of Electronic Fingerprints as Evidence in Criminal Proceedings: A Legal–Technical Doctrinal Analysis

Abdullah Theeb Mahmmoud

Associate Professor of Criminal Law;
Palestine Technical University – Kadoorie, Palestine.

Ribhi wajeeh mousa Dola

Ph.D. researcher;
The Arab American University (AAUP), Ramallah, Palestine.

Kamal Alieyan

College of Information Technology, Amman Arab University
Amman 11953, Jordan

Waheeb Abu-ulbeh

Faculty of Administrative Sciences and Informatics,
Al-Istiqlal University, Jericho 10, Palestine

Journal of Information Technology, Cybersecurity, and Artificial Intelligence, 2026, 3(1), 1–12

Article DOI: https://doi.org/10.70715/jitcai.2026.v3.i1.042

Abstract

This paper provides a doctrinal–analytical legal–technical examination of the admissibility of electronic fingerprints as evidence in criminal proceedings. It analyzes the legal foundations governing biometric evidence, with particular reference to Palestinian legislation—especially Decree-Law No. (10) of 2018 on Cybercrimes—together with general principles of criminal procedure and digital evidence. Relying exclusively on statutory interpretation, judicial principles, comparative legal analysis, and internationally recognized technical standards, the study evaluates the conditions under which electronic fingerprints may be admitted as criminal evidence, including legality of collection, scientific reliability, integrity of the chain of custody, and protection of fundamental rights. The paper further examines contemporary legal and technical challenges, such as biometric forgery (including deepfakes), cross-border jurisdictional constraints, data protection risks, and the absence of harmonized international standards. Through comparative analysis of Palestinian law and selected foreign regulatory models, particularly European Union and common law approaches, the study identifies doctrinal gaps and normative deficiencies. It also advances a theoretical framework that conceptualizes electronic fingerprints as hybrid legal–technical evidence requiring integrated governance. The study concludes by proposing normative legal and regulatory directions aimed at enhancing evidentiary reliability, legal certainty, and rights protection in modern criminal justice systems.

Keywords: electronic fingerprints; biometric evidence; chain of custody; digital forgery; privacy.

1. Introduction

The rapid development of information and communication technologies has fundamentally transformed contemporary criminal activity and the mechanisms used to investigate and prove such crimes. Traditional forms of evidence, designed primarily for physical and tangible acts, are increasingly insufficient to address crimes committed or facilitated through digital environments. As cybercrime expands in scope and sophistication, criminal justice systems face growing pressure to adopt modern forms of technical evidence capable of identifying perpetrators and linking them to unlawful digital conduct.

Among the most significant developments in this context is the use of electronic fingerprints. These fingerprints, whether physical, physiological, or behavioral—are generated and processed electronically and serve as biometric identifiers capable of verifying identity and attributing digital actions to specific individuals. Electronic fingerprints have thus emerged as a powerful evidentiary tool, particularly in cases involving cybercrime, impersonation, and technologically mediated fraud.

In response to these developments, the Palestinian legislature enacted Decree-Law No. (10) of 2018 concerning cybercrimes, which recognizes the admissibility of electronic data and information as evidence in criminal proceedings. While this legislative framework opens the door to the use of electronic fingerprints, it leaves unresolved several doctrinal questions concerning their legal nature, evidentiary value, procedural safeguards, and compatibility with constitutional rights, most notably the right to privacy and data protection.

Accordingly, this study approaches electronic fingerprinting not merely as a technological instrument, but as a legal–technical evidentiary phenomenon that challenges traditional doctrines of criminal proof and requires a coherent normative framework capable of integrating law, technology, and fundamental rights.

2. The Problem and Research Questions

Despite significant technological advancements and the increasing reliance on biometric systems by public and private institutions, legislative and judicial clarity regarding the admissibility of electronic fingerprints in criminal proceedings remains limited. While electronic fingerprints may contribute to accurate identification and effective crime detection, their use raises complex legal and technical issues concerning the legality of collection, reliability of analysis, preservation of evidence, and protection of individual rights.

In the Palestinian context, the absence of explicit statutory provisions regulating electronic fingerprints as independent criminal evidence places a considerable burden on judicial interpretation and discretion. This raises uncertainty regarding their legal value and the limits of their use in criminal adjudication.

The central research question of this study is:

To what extent are electronic fingerprints admissible as evidence in criminal proceedings?

This question gives rise to the following sub-questions:

1. What is meant by electronic fingerprinting, and what are its main characteristics and types?
2. What legal framework governs the use of electronic fingerprints as criminal evidence?
3. What are the principal legal and technical challenges affecting their admissibility?
4. How does Decree-Law No. (10) of 2018 on Cybercrimes address electronic fingerprints as digital evidence?

3. The Importance of the Study

The theoretical significance of this study lies in its contribution to criminal evidence theory and law-and-technology scholarship. By examining electronic fingerprints as a form of hybrid legal–technical evidence, the study challenges traditional evidentiary doctrines that were developed for physical proof and argues for a recalibrated framework capable of accommodating technologically mediated forms of evidence.

From a practical perspective, the study provides normative guidance for legislators, judges, and law enforcement authorities by clarifying the legal conditions under which electronic fingerprints may be admitted as evidence. It also highlights the importance of procedural safeguards, technical standards, and institutional capacity in ensuring the reliability and legality of biometric evidence, while safeguarding fundamental rights.

4. Study Objectives

This study aims to:

- Clarify the legal and technical concept of electronic fingerprints and their characteristics.
- Identify the legal framework governing their admissibility in criminal proceedings.
- Analyze the principal legal and technical challenges associated with their use as evidence.
- Examine the position of Palestinian cybercrime legislation regarding electronic fingerprints.
- Propose normative legal–technical directions to enhance evidentiary reliability and rights protection.

5. Study Objectives

This study aims to identify the legal nature of electronic fingerprints by analyzing their concept, characteristics, and various types, in order to clarify their place among modern methods of proof in the criminal field. It also seeks to define the legal framework governing the use of electronic fingerprints as a means of proof, focusing on their recognition before the Palestinian judiciary. Furthermore, the study addresses the most significant legal and technical challenges hindering the adoption of electronic fingerprints as reliable criminal evidence, whether in terms of their collection, analysis, or maintaining their digital integrity. Additionally, it aims to analyze the position of Law No. (10) of 2018 concerning cybercrimes regarding the issue of electronic fingerprints, and to determine the extent to which it considers them recognized as digital evidence in criminal proceedings.

6. Study Methodology

This study adopts a doctrinal–analytical legal research methodology. It is based on systematic analysis of primary legal sources, including criminal procedure laws, cybercrime legislation, and regulatory instruments governing digital and biometric evidence, with particular emphasis on Palestinian law. Secondary sources include judicial principles, comparative jurisprudence, and scholarly legal literature addressing criminal evidence, cybersecurity, and law–technology interactions.

The research employs normative legal reasoning to analyze the admissibility and probative value of electronic fingerprints, focusing on legality of collection, scientific reliability, chain of custody, and compatibility with constitutional rights. A comparative analytical approach is used to contrast the Palestinian legal framework with selected foreign and international models—particularly European Union data protection law and common law evidentiary standards—in order to identify doctrinal gaps and best practices.

This study does not rely on interviews, empirical consultations, surveys, or field research. Technical aspects are incorporated through doctrinal analysis of internationally recognized standards, including ISO/IEC and NIST frameworks, which are examined as normative reference points within a legal–technical evidentiary framework.

7. Study Plan

7.1. Section One: The Theoretical Framework of Electronic Fingerprints

Requirement One: The Concept and Characteristics of Electronic Fingerprints

Requirement Two: Types of Electronic Fingerprints

7.2. Section Two: The Admissibility of Electronic Fingerprints in Criminal Evidence

Requirement One: The Legal Basis of Electronic Fingerprints as Evidence in Criminal Evidence

Requirement Two: Challenges Facing the Admissibility of Electronic Fingerprints

7.3. Section One: The Theoretical Framework of Electronic Fingerprints

7.3.1. First Requirement: Concept and Characteristics of Electronic Fingerprints

Linguistically, fingerprints refer to distinctive marks that differentiate individuals from one another. Technically, fingerprints are traces or patterns left by physiological or behavioral characteristics that can be captured and analyzed for identification purposes. In legal terms, an electronic fingerprint may be defined as a biometric identifier generated and processed through electronic means and used as a form of digital evidence to verify identity or attribute a specific action to a particular individual. Its admissibility depends on compliance with evidentiary rules governing reliability, legality, and procedural integrity. Electronic fingerprints are evaluated according to several criteria, including universality, uniqueness, permanence, measurability, performance, acceptability, resistance to spoofing, and interoperability. These criteria, reflected in international standards and forensic guidelines, play a crucial role in determining the legal reliability of biometric evidence.

Linguistically: The Arabic word for fingerprint is derived from the root (basama), meaning to stamp or mark with the tip of one's finger. Fingerprints are the unique mark left by this act, a divine seal by which God Almighty distinguishes each person from others, just as He distinguishes voice, eyes, scent, ears, and other characteristics that are unique to each individual in the universe (Ibn Manzur, 1993, p. 29).

Technically: Fingerprints are defined as the traces, marks, or impressions left by fingertips, palms, and feet on smooth surfaces. Rough surfaces are difficult to lift fingerprints from due to the crevices and indentations they create (Abdul Wahab, 2018, p. 24).

The term "electronic fingerprint" is used in various ways: either as a set of biometric data representing a computerized fingerprint (biometric), or as digital traces left on systems. Legally, it can be viewed as a technical means of proof (i.e., an element of digital evidence) used to link a specific person to a digital statement or action. However, its admissibility as evidence depends on the rules of evidence applicable in the judicial system and on the extent to which the conditions for relying on technical means are met in terms of reliability and tamper-proof (Interpol review, 4, 2023; Research on biometric evidence, 5, 2025). The electronic fingerprint system is a modern and effective tool that contributes to improving the work environment and enhancing the efficiency of institutions. Its most prominent benefits are as follows (Maddah, 2020: 15):

1. Timekeeping and Attendance: the system contributes to the accurate organization of working hours in public and private companies and institutions, leading to: Enhanced commitment and discipline at work; Reinforced respect for the work environment; Documentation of employee achievements through accurate daily and weekly reports submitted to management; and reliable preservation and documentation of employee rights.
2. Protection of Employee and Institutional Rights: The system ensures accurate attendance and departure recording, safeguarding the rights of both parties and preventing any manipulation or violations.
3. Improved Work Efficiency and Achievement of Institutional Goals: The system facilitates the smooth and timely completion of tasks, while providing accurate and timely reports on employee discipline and commitment. It also enables the generation of cumulative reports on employee activity and links them to the salary and age system to determine the appropriate financial status.
4. Reduction of Identity Theft: The system helps prevent forgery and identity theft and expedites procedures and transactions with high efficiency.
5. Providing a comprehensive employee database: The system allows for the entry of all essential employee data, such as employee number, name, date of birth, and appointment, in addition to phone number, address, nationality, and gender, while accurately calculating overtime hours.
6. Generating accurate and organized reports: Detailed attendance and departure reports for all employees can be generated periodically and sent to the accounting department to assist in payroll calculation and renewal.

The literature indicates that employing biometric features in digital work environments enhances security and reduces the risks associated with identity theft or cyber fraud. Thus, the digital fingerprint becomes part of the digital security infrastructure, ensuring that every transaction or login can be easily and accurately verified.

DOI: https://doi.org/10.70715/jitcai.2026.v3.i1.042

From a legal perspective, electronic fingerprints of all types—fingerprints, facial recognition, iris scans, or behavioral biometrics—are considered reliable and effective evidence in judicial proceedings when verifying the identity of individuals in official transactions within governmental and private institutions. This is because they rely on unique and stable individual biological characteristics, making them difficult to forge or duplicate. This stability and uniqueness enable judicial authorities to rely on fingerprints as an accurate means of verifying the authenticity of digital or physical transactions and signatures. It also helps prevent forgery and manipulation of documents and transactions, whether financial or legal, enhances the reliability of digital evidence, increases the level of legal security for institutions, and makes electronic fingerprints an essential tool for protecting rights and reliably and accurately documenting liability.

An electronic fingerprint is understood as a biometric feature used electronically to verify a person's identity (such as fingerprint, facial recognition, iris scan, voice, etc.). These features are typically evaluated according to a set of qualitative and operational criteria (universality, uniqueness, reliability, measurability, performance, acceptability, and resistance to spoofing) that determine the suitability of each feature for security or commercial use (Jain et al., 2004). These criteria are explained as follows:

- Universality: The universality property means that the biometric feature is present in all or most individuals, allowing for widespread use. For example, fingerprints and facial recognition are common features among most people, making their availability a prerequisite for any practical biometric system. When a feature is absent in a group of individuals (e.g., finger deformities), an alternative feature or a multimodal system should be considered.
- Distinctiveness/Uniqueness: Uniqueness refers to a feature's ability to distinguish one person from another to a high degree. The more unique a feature is, the lower the probability of two people having the same feature, the more reliable the system is. Technical studies on fingerprints and iris patterns show extremely high levels of uniqueness, so these features are used in applications requiring high accuracy.
- Permanence: Permanence means that a feature's pattern remains constant or changes slowly over time, allowing stored templates to remain valid for extended periods. Some features, such as iris and fingerprint, exhibit high stability over years, while behavioral features (such as handwriting or voice patterns) can be affected by age, illness, or stress, necessitating template updates or the use of flexible predictions.
- Collectability/Measurability: This property refers to the ease and security with which a biometric sample can be collected using a suitable device. Some biometric features require specialized equipment or a specific environment (such as iris scanning), while others can be captured with built-in devices (phone cameras, fingerprint sensors in devices). Noise and interference levels during data collection also affect sample quality and subsequent error rates.
- Performance and Accuracy (accuracy, speed, robustness): System performance is measured by metrics such as False Acceptance Rate (FAR), False Rejection Rate (FRR), speed, and the ability to operate under varying conditions. Influencing factors include sensor quality, matching algorithms, and calibration procedures. NIST recommendations and standards provide specifications for measuring the accuracy and specifications of biometric devices and systems to assess their suitability for practical applications.
- Acceptability and Privacy Concerns: Public acceptance is important: Some people refuse to use certain biometric features (facial photography, iris scanning) for religious, cultural, or privacy reasons. Furthermore, biometric data raises privacy risks. Since a fingerprint template is not easily replaceable like a password, and it stores sensitive information that could raise regulatory and legal issues, especially in cases of mass use or surveillance—governance and privacy policies (transparency, minimal data retention, encryption, and explicit consent) are recommended.
- Circumvention/Spoofing Resistance: Circumvention refers to how easily a system can be fooled by imitating a feature (face masks, fingerprint copies, voice recordings). Research has shown that traditional systems can be fooled with simple tools if they do not include detection of life. Therefore, specialized research and standards (ISO/IEC 30107) and countermeasures (PAD — Presentation Attack Detection) have emerged to detect forgery attempts and improve system resistance.
- Interoperability and Standards: Adopting international standards (such as the ISO/IEC 19794 families for biometric data interchange formats) helps make templates interchangeable between different systems and vendors and defines coordination requirements. Data and its quality are crucial when deploying solutions at the enterprise or national level (ISO/IEC, 2011). Documents such as the NIST guidelines also provide technical specifications for evaluating sensors and algorithm performance.

7.3.2. Second Requirement: Types of Electronic Fingerprints

Recent doctrinal and technical studies increasingly advocate hybrid biometric systems that combine multiple biometric modalities—such as fingerprinting, facial recognition, thermal imaging, or behavioral biometrics—to enhance accuracy and resistance to forgery. From a legal perspective, hybrid systems mitigate evidentiary risk by reducing reliance on a single biometric source and strengthening the overall reliability of identification. This development aligns with emerging regulatory expectations that biometric evidence used in criminal proceedings should meet heightened standards of accuracy, robustness, and procedural transparency.

Electronic fingerprints encompass various biometric modalities, including facial recognition, thermal biometrics, traditional fingerprinting, voice recognition, and behavioral biometrics. Each modality differs in terms of technical complexity, accuracy, vulnerability to forgery, and legal implications. Recent doctrinal and technical literature increasingly emphasizes the importance of hybrid biometric systems, which combine multiple biometric modalities to enhance accuracy and reduce evidentiary risk. From a legal perspective, hybrid systems strengthen the probative value of evidence by mitigating reliance on a single identification source and aligning with heightened standards of reliability expected in criminal proceedings.

Electronic facial recognition

Electronic facials are a modern technology that has revolutionized personal identity verification methods. This technology relies on specialized digital software that captures a direct image of the user's face, then analyzes their features with high precision and compares them to pre-stored data and images in the system. This software is distinguished by its ability to operate without the need for advanced or expensive equipment; a computer and a standard digital camera are sufficient, making it a practical and effective option for various institutions (Hamadi, 2005, p. 298). This technology contributes to providing a reliable and efficient electronic system that allows for rapid verification of individuals' identities, whether when logging into electronic systems or entering specific areas within institutions. It can also be used as an alternative to traditional verification methods such as fingerprinting or paper signatures, as all user transactions and activities are documented. This ensures the creation of an electronic record that can be later referenced as a legally valid document, while simultaneously enhancing data protection as private property in the digital space.

Some jurists consider this technology to fall under the concept of using a person's physical and behavioral characteristics to distinguish and verify their identity. This represents an evolution in the concept of electronic signatures from a mere written mark to a uniquely personal digital tool (Hammadi, 2005, p. 298). However, another jurisprudential trend suggests focusing solely on physical characteristics, such as facial features or fingerprints, due to their ease of measurement and accuracy. This view holds that relying on behavioral patterns may be less practical in terms of their stability and amenability to precise measurement (Al-Tariqi, 2007, p. 267).

Thermal Biometrics

Thermal biometrics is a modern technique that relies on the physiological characteristics of the human body. It captures thermal patterns emitted from the face or hands using advanced thermal imaging sensors. These sensors convert the emitted thermal energy into a thermogram, which shows the temperature distribution across the skin's surface, enabling contactless identification (Buddharaju, 2007). Physically, human skin has a high emissivity (≈ 0.98), meaning that the infrared radiation it emits accurately represents the skin's surface temperature. This makes it easy for thermal cameras operating in the long-infrared range (8–14 μm) to capture thermal patterns with high precision (Pavlidis & Buddharaju, 2009). Uncooled microbolometer cameras are used for this purpose. Temperature sensitivity (NETD) and spatial resolution are key factors for the quality of identification (Zhao et al., 2021). Thermal authentication systems typically follow specific steps, beginning with capturing a thermal image of a face or hand. This image is then pre-processed to remove noise and calibrate, after which distinctive features such as thermal patterns of superficial blood vessels or precise heat distribution are extracted. In modern systems, deep learning is used to automatically extract these thermal features and compare them to stored templates (Silva et al., 2019).

One of the most significant advantages of this technology is that it does not require direct contact, making it suitable for public and health-sensitive environments. It also works in the dark because it relies on body heat rather than visible light (Pavlidis & Buddharaju, 2009). Furthermore, it is resistant to simple forgery attempts because it measures dynamic, live heat, making it difficult to imitate using ordinary photos or masks (Ghiass et al., 2013). For this reason, thermal fingerprinting is used in airports, security institutions, and long-range surveillance systems, especially in crowded environments requiring contactless monitoring (Al-Attar, 2019). Despite their advantages, thermal fingerprinting systems face technical and environmental challenges. Ambient temperature, humidity, and wind affect thermal patterns, and an individual's physical activity or health status can alter heat distribution over time (Silva et al., 2019). Furthermore, eyeglasses or masks can obscure important thermal areas of the face, impacting recognition accuracy (Zhao et al., 2021). Therefore, studies recommend combining thermal fingerprinting with other technologies, such as visible facial recognition or iris recognition, to enhance system reliability in critical environments (Pavlidis & Buddharaju, 2009).

Fingerprints: Auditory, Fingerprint, and Behavioral

Among the most prominent types of electronic fingerprints is the auditory fingerprint, which relies on the unique vocal characteristics of everyone. The user's voice is recorded beforehand and analyzed for pitch, tone, and unique sound frequencies. Any subsequent recording is then compared to the stored model for identity verification. This technology is widely used in large factories, sensitive facilities, smart homes, and voice authentication systems in banking institutions and telephone customer service. Auditory fingerprints are difficult to imitate, but they can be affected by external factors such as noise or changes in voice tone due to illness. Additionally, fingerprinting is the most widespread electronic fingerprinting technology. It relies on analyzing the unique lines and ridges found on the fingertips of a person, patterns that cannot be identical between two individuals. This technology is widely used in smartphones, laptops, enterprise access control systems, and electronic payment processes. It is characterized by its ease of use and speed of response, but it requires direct contact with the sensor. Another modern type is behavioral fingerprinting, a technology that relies on analyzing user behavioral patterns, such as typing style, mouse movement, or phone interaction. This technology is used in financial institutions and sensitive applications that require continuous monitoring of user identity even after login, providing an additional layer of security that is difficult to bypass (Telecom Review, 2024).

Through the researcher's consultations with experts and specialists in information security and biometric technologies, it became clear that there is a growing trend toward using hybrid digital fingerprinting, which relies on combining more than one type of electronic fingerprint to achieve a higher level of accuracy and security in identity verification. Experts indicated that combining facial recognition, thermal imaging, fingerprinting, or behavioral fingerprinting overcomes the weaknesses that appear when using any single technology and enhances the overall reliability of the system. The literature shows that hybrid fingerprinting systems offer several practical advantages, most notably:

- Improved verification accuracy and reduced error rates, as each fingerprint type supports the others, thus reducing the likelihood of misidentification or rejection of the correct user.
- Increased resistance to forgery and manipulation: The integration of thermal and behavioral technologies makes it difficult to impersonate an identity using images or masks.
- Continuous and ongoing verification: Monitoring user behavior after login provides an additional layer of security in digital systems.

It concludes that adopting hybrid fingerprinting has become essential for institutions handling sensitive information, such as banks, airports, and research centers. This integration enables real-time verification while reducing reliance on human intervention, enhancing system reliability and efficiency, especially in environments requiring high security and continuous protection of digital identity.

7.4. Section Two: The Admissibility of Electronic Fingerprints in Criminal Proceedings.

7.4.1. First Requirement: The Legal Basis of Electronic Fingerprints as Evidence in Criminal Proceedings.

Comparative legal analysis reveals divergent approaches to the admissibility of biometric evidence. While the European Union adopts a precautionary, rights-based regulatory model under the GDPR—classifying biometric data as sensitive personal data subject to strict safeguards—common law jurisdictions rely more heavily on judicial discretion and forensic admissibility standards. This divergence underscores the absence of harmonized international rules governing electronic fingerprints and highlights the normative challenges facing national legal systems such as Palestine.

Electronic fingerprints are among the most important modern means of proof in the criminal field. They rely on the unique biological or behavioral characteristics of individuals, such as fingerprints, facial scans, or iris scans, which are collected and analyzed electronically to identify individuals and link them to criminal acts. Legal systems have witnessed a clear evolution towards recognizing electronic and digital evidence, including biometric fingerprints, in response to rapid technological advancements (Garrett, 2025, p. 22). Regarding the evidentiary value of electronic fingerprints and the conditions for their admissibility in court, the elements for accepting an electronic fingerprint can be summarized in the following points (Malham, 2023):

1. Legality in Obtaining It: The electronic fingerprint must have been obtained legally (without violating privacy or resulting from a legal violation). Any objection to the legitimacy of the evidence collection may lead to its exclusion.

2. Scientific and Technical Reliability: The judge requires the requesting party to demonstrate that the technology used is scientifically validated and has an acceptable error rate, and that the extraction and analysis procedures adhered to well-known and established technical standards. When biometric evidence is presented, the matching methods and the system's susceptibility to error or false positives are often reviewed.
3. Chain of Possession: It is essential to document how the fingerprint was collected, stored, transferred, and analyzed to ensure it was not tampered with or replaced.
4. Logical Relevance to the Case: The fingerprint must be presented as a supplementary element to other evidence or as part of a comprehensive evidentiary system, as relying solely on a single digital source may raise doubts.

It can be said that the availability of these conditions supports the admissibility of electronic fingerprints in court, while their absence may lead to their exclusion or caution regarding their evidentiary weight. It is worth noting that electronic fingerprints are considered sensitive personal data due to their connection to an individual's biological identity. Therefore, there is a need for strong data protection regulations governing data collection, processing, storage, and deletion, and defining individuals' rights (access, objection, and deletion request). International reports warn of the risks of misuse and breaches, and recommend a clear legal framework to protect rights (Malham, 2023).

In Palestine, the Criminal Procedure Law stipulates that evidence can be presented by any means of proof unless otherwise specified. This opens the door to the adoption of modern technologies such as digital fingerprints in criminal proceedings (Hamouda, 2024, p. 41). Furthermore, Decree-Law No. (10) of 2018 concerning cybercrimes recognizes the admissibility of data and information stored or transmitted electronically and permits its use as evidence in court. This provides a direct legal basis for the adoption of digital fingerprints within the evidentiary framework (Cybercrimes, 2018, p. 5). In Palestine, the Criminal Procedure Law stipulates that evidence can be presented by any means of proof unless otherwise specified. This opens the door to the adoption of modern technologies such as digital fingerprints in criminal proceedings (Hamouda, 2024, p. 41). Furthermore, Law No. (10) of 2018 concerning cybercrimes recognized the admissibility of data and information stored or transmitted electronically and permitted its use as evidence in court. This constitutes a direct legal basis for adopting electronic fingerprints within the evidentiary system (Cybercrimes, 2018, p. 5).

Indeed, some Palestinian institutions, including governmental bodies, the banking sector, and security agencies, have begun implementing electronic fingerprint systems to enhance control over daily operations, verify the identity of employees and users, and contribute to preventing fraud and forgery. The researcher's consultations with digital law and cybersecurity experts indicate a growing trend toward employing electronic fingerprints in criminal investigations, particularly in cybercrime and impersonation cases, given their high accuracy and the difficulty of forging them compared to traditional methods. However, these applications face regulatory and legal challenges, most notably protecting personal data and ensuring privacy, as well as defining the legal responsibilities of entities that collect and store biometric information. This necessitates the development of clear regulations and implementing legislation to guarantee the legal and secure use of this technology in Palestine, in accordance with international human rights and data governance standards.

For an electronic fingerprint to have evidentiary value, specific conditions must be met, the most important of which are: the integrity of the chain of custody, which ensures the documentation of the stages of evidence collection, transfer, and examination without tampering (NIST, 2013, p. 14), and compliance with international technical standards such as ISO/IEC 19794 for the representation and exchange of fingerprint data (ISO/IEC, 2011, p. 8). The courts also require that the forensic expert submit a clear report that includes the scientific methodology, error rates, and limits of certainty, thus allowing the judge and the litigants to scrutinize the evidence and not rely solely on the principle of "expert confidence" (Levanon & Tully, 2025, p. 33).

On the other hand, the use of electronic fingerprints in criminal proceedings raises sensitive constitutional and human rights issues, most importantly the right to privacy and the protection of personal data. Biometric data is considered a sensitive category that requires strict safeguards in its collection, storage, and use to prevent misuse or leakage (European Union GDPR, 2018, p. 17). Therefore, the legal recognition of electronic fingerprints must be balanced with constitutional guarantees and human rights, ensuring their use within a clear legal framework subject to judicial oversight.

Based on the above, the legal basis for electronic fingerprints in criminal evidence rests on two pillars: the first is legislative, represented by the legal texts that recognize and regulate electronic evidence; The second is technical procedural, based on the application of scientific standards and ensuring the integrity of technical and legal procedures. Accordingly, electronic fingerprinting can be strong evidence in criminal proceedings whenever these conditions are met (Garrett, 2025, p. 29; NIST, 2013, p. 18; Hamouda, 2024, p. 45).

7.4.2. The second requirement: Challenges facing the admissibility of electronic fingerprints.

There are a number of legal and technical challenges to using electronic fingerprints, as outlined below (Mina, 2025):

- Investigators face significant challenges in collecting and preserving electronic fingerprints, as this evidence is characterized by its ephemerality. Some data is temporary and disappears as soon as the device is turned off or the browsing session ends. Therefore, collecting this evidence requires immediate and rapid intervention to prevent its loss or tampering. Maintaining the integrity of digital evidence also necessitates ensuring that it remains unaltered and uncontaminated from the moment of its discovery until its presentation in court, as even a minor change can lead to a loss of credibility and render it inadmissible as evidence.
- Courts face difficulty in proving the validity and reliability of electronic fingerprints, given their susceptibility to manipulation or forgery. Accepting this type of evidence requires a series of strict procedures and controls to guarantee its authenticity and integrity. Furthermore, the party presenting the evidence must document how it was collected, the entity that collected it, and the method used to preserve and secure it against any tampering. Furthermore, the issue of jurisdiction arises in transnational crimes, especially when data is stored on servers in other countries. A lack of judicial expertise in dealing with the technical complexities of digital evidence can also affect court decisions. Therefore, there is a need to develop clear legal frameworks and train judges and prosecutors on the technical aspects of this evidence. Without these safeguards, digital evidence remains vulnerable to rejection or diminished probative value.
- Digital forgery is one of the most prominent emerging challenges to the admissibility of electronic evidence in the modern era. The rapid development of artificial intelligence technologies has led to the emergence of sophisticated forgery methods, most notably "deepfakes," which allow for the production of highly realistic digital images and videos that are difficult to distinguish from the originals. This technology can be used to forge facial features or voices or even create entire videos of individuals who did not commit the acts attributed to them. This development complicates the process of verifying the authenticity of digital evidence and places an additional burden on technical experts and courts to establish the authenticity of materials presented as evidence. Traditional technical tools for detecting tampering are no longer sufficient on their own, necessitating the development of new detection mechanisms based on artificial intelligence and advanced data analysis (Cambridge, 2023).

The gap between legal systems in different countries poses a major challenge to the international recognition of digital evidence, including digital fingerprints. Each country has its own legislation and procedures for collecting, legally protecting, and presenting digital evidence in court, resulting in the absence of a unified legal framework or binding international standards. This legal disparity complicates international cooperation in criminal investigations, particularly in cross-border cases involving data storage on servers in other countries or the retrieval of information from global service providers. Consequently, evidence may be rejected or its legal value diminished due to non-compliance with the procedural standards of the country where the case is being presented (JICLT, 2020).

The admissibility of digital evidence depends heavily on the scientific reliability of the methods used to collect and examine it. Verifying the authenticity of digital evidence requires the application of precise technical tools, such as calculating file hashes to ensure they haven't been altered, using digital signatures, and analyzing metadata that documents the details of file creation or modification. Any error in these procedures or reliance on unapproved or unreliable software can undermine the credibility of the evidence in court. Therefore, the absence of standardized criteria or sufficient technical expertise in applying these tools poses a risk to the reliability of digital fingerprints as legally admissible evidence (Ejfs, 2021). One of the significant practical challenges facing the admissibility of digital fingerprints is the loss of digital evidence or the deterioration of its legal value due to delays in its collection. In many cases, data is stored on platforms belonging to foreign companies or on cloud servers for limited periods, after which it is automatically deleted or altered. If judicial authorities delay issuing legal orders to collect this data, the evidence may be permanently lost or become inadmissible for legal use due to the difficulty of verifying its authenticity over time. Legal restrictions on obtaining data from foreign companies can also hinder rapid access, increasing the likelihood of evidence loss (Cambridge, 2023).

The collection and analysis of digital evidence require advanced technical equipment and specialized expertise in cybercrime. However, many countries, particularly developing ones, face a shortage of these resources, both in terms of sophisticated equipment and qualified personnel. This shortage often leads to weaknesses in evidence collection and analysis procedures, potentially resulting in evidence loss or challenges to its admissibility in court. The lack of experts capable of handling advanced digital evidence makes it difficult to ensure the legally required chain of custody (CCC) (Ejfs, 2021). Reconciling the requirements of collecting digital evidence with the protection of individual privacy presents a complex legal and ethical challenge. In many countries, the collection of digital data is subject to strict privacy laws, which can limit the ability of security or judicial authorities to obtain the information necessary to prove a crime. For example, some countries may require specific court orders or prior consent before accessing personal data, and technology companies may refuse to hand over data without meeting specific legal requirements. This conflict can hinder investigations or lead to the invalidation of evidence if it is collected in ways that violate privacy laws (AJSRP, 2022).

It is clear from the above that the admissibility of digital fingerprints in criminal proceedings is a fundamental pillar of the modern justice system, given their ability to provide accurate and difficult-to-forge evidence and their contribution to expediting investigations and enhancing the reliability of their results. Palestinian legislation, like many comparable legal systems, has established clear legal foundations for the recognition of digital evidence, including biometric fingerprints, which is an important step towards keeping pace with technological advancements in the field of criminal investigation. However, this legal evidence still faces a number of legal and technical challenges that weaken its practical effectiveness. Challenges related to collecting and preserving evidence, difficulties in proving it in court, and the disparity in legal standards between countries, along with the rapid development of digital forgery technologies, all negatively impact the evidentiary value of electronic fingerprints. Furthermore, the lack of human and technical resources, and the limited judicial and technical expertise in handling this type of evidence, increase the likelihood of procedural or technical errors that could undermine the credibility of the evidence in court.

From a critical perspective, it can be observed that the current legal framework, while important, is insufficient on its own to guarantee the judicial acceptance of electronic fingerprints. A comprehensive system combining legislation, technology, and practical application is required. The mere existence of legal texts recognizing electronic fingerprints is not enough; it is essential to develop implementing regulations and precise technical standards, and to strengthen the institutional and technical capacities of security and judicial bodies to ensure that procedures are applied according to the highest standards of integrity and accuracy.

8. Results

The study reached the following conclusions:

1. Digital fingerprinting has become legally acceptable at the statutory level, but its practical application in evidentiary procedures varies according to the quality of the implementing procedures and legislation.
2. Legislative and regulatory developments indicate an increasing normative recognition of biometric technologies within Palestinian institutions, although their effective legal deployment remains contingent upon procedural clarity, technical capacity, and regulatory safeguards
3. Chain of custody and technical standards (such as template representation and authentication methods) are crucial factors in the admissibility of evidence, and current procedures often contain procedural and technical gaps.
4. The shortage of qualified personnel and accredited laboratories is a major obstacle to the accurate and legally admissible analysis of digital evidence.
5. Modern technological threats—especially deepfakes and methods for creating fake digital evidence, complicate the work of experts and necessitate sophisticated detection tools.
6. The lack of international consensus on standards and jurisdictional restrictions hinders rapid and reliable access to data stored outside the country.
7. There are legitimate concerns regarding privacy and individual rights in the absence of robust controls to protect biometric data and prevent its misuse. 8. There is a growing interest in hybrid technology trends (combining multiple fingerprint types) as a solution to enhance accuracy and resistance to forgery, which creates opportunities to improve practical practices.

9. Recommendations

A comprehensive legislative and regulatory framework must be established to govern the collection, storage, and use of biometric data in criminal proceedings. This framework should include the necessary legal controls to ensure the protection of this sensitive data. It should also contain clear provisions regarding judicial authorization mechanisms, data retention periods, conditions for disclosure, and legal accountability in cases of misuse. These provisions must be aligned with international human rights and privacy standards.

The legal admissibility of digital fingerprints requires standardizing the technical criteria used in collecting and analyzing digital evidence, in accordance with approved international standards and specifications, such as ISO and

NIST. Precise and documented procedures must be established to ensure the integrity of the chain of custody; from the moment digital evidence is collected through its transfer and analysis to its presentation in court. Digital signature and encryption methods should be adopted to prevent tampering with the evidence.

A national laboratory specializing in digital evidence should be established and equipped with advanced technical infrastructure and qualified personnel according to international quality standards. It is also recommended to develop regular training programs for judges, public prosecutors, and security personnel to enhance their legal and technical expertise in handling digital evidence.

Invest in modern technologies for detecting digital forgery, particularly deepfakes, by employing artificial intelligence and advanced forensic analysis techniques. It is also advisable to adopt hybrid biometric systems that combine multiple verification methods (such as fingerprinting, facial recognition, and iris scanning) to improve the accuracy of evidence and reduce the likelihood of forgery or digital impersonation, thereby strengthening the reliability of evidence in court.

Enhance international cooperation and ensure the protection of rights and privacy to facilitate access to digital evidence in cross-border cases and standardize related procedures.

10. Conclusion

This study demonstrates that digital fingerprinting represents a significant and growing evidentiary tool in the modern criminal justice system. It provides an accurate means of identifying and verifying individuals and linking them to digital actions and movements. However, its practical effectiveness and reliability in court depend not only on the existence of legislation authorizing its use, but also on an integrated system that combines clear legislation, precise technical standards, sound procedural practices, and an institutional structure and technical expertise capable of ensuring the integrity and legality of the evidence. Without this integration, digital fingerprinting remains vulnerable to challenge or limitations in its evidentiary value, especially in light of challenges such as digital forgery, varying international standards, and a lack of resources and expertise.

From a theoretical standpoint, the study demonstrates that electronic fingerprints must be governed as hybrid legal–technical evidence, requiring an integrated evidentiary doctrine capable of responding to technological complexity while preserving the foundational guarantees of criminal justice.

11. References

[1] Abdul Wahab, Rashid bin Ali. (2018). Forensic Fingerprint Science, College of Forensic Sciences, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia, p. 24.

[2] AJSRP. (2022). Legal and ethical aspects of digital evidence. Arab Journal of Scientific Research Publishing.

[3] Al-Attar, Muhammad. (2019). Thermal Technologies in Security Monitoring Systems. Cairo: Dar Al-Fikr Al-Arabi.

[4] Al-Sahmawi, Hiba. (2023). Electronic Facial Recognition and its Admissibility in Civil Proceedings: A Comparative Study, Journal of Legal and Economic Research, (2): 1-106.

[5] Al-Tariqi, Sulaiman Muhammad. (2007). Electronic Signature. Journal of Law and Economics, Issue 1, p. 267.

[6] Buddharaju, P. (2007). Physiology-Based Face Recognition in the Thermal Infrared Spectrum. Ph.D. Dissertation, University of Houston, USA.

[7] Cybercrimes. (2018). Decree-Law No. (10) of 2018 Concerning Cybercrimes. State of Palestine.

[8] Ejfs. (2021). Electronic evidence and its authenticity in forensic evidence. Egyptian Journal of Forensic Sciences, Springer Open.

[9] European Union GDPR. (2018). General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Union, L119, 1–88.

[10] Garrett, B. L. (2025). Judging Fingerprint Evidence. SSRN.

[11] Hammadi, Abd al-Fattah Yusuf. (2005). Electronic Signature in Comparative Legal Perspective. Dar al-Fikr al-Jami'i, Alexandria.

[12] Ibn Manzur, Muhammad ibn Mukarram. (1993). Jamal al-Din, Lisan al-Arab, Volume 1, First Edition, Dar Sader, Beirut, Lebanon, p. 29.

[13] International Organization for Standardization (ISO/IEC). (2011). ISO/IEC 19794-2: Information technology — Biometric data interchange formats — Part 2: Finger minutiae data. ISO.

[14] ISO/IEC. (2011). ISO/IEC 19794-2: Information technology — Biometric data interchange formats — Part 2: Finger minutiae data. ISO.

[15] JICLT. (2020). Digital evidence in international legal proceedings. Journal of International Commercial Law and Technology.

[16] Journal of International Commercial Law and Technology (JICLT). (2020). Digital evidence in international legal proceedings. Journal of International Commercial Law and Technology, 15(2), 112–125.

[17] Maddah, Fatih. (2020). The Relationship Between the Application of the Electronic Fingerprint System and Employee Performance: A Field Study at the Faculty of Humanities and Social Sciences, Mohamed Bouyaf University of M'sila, Algeria, p. 15.

[18] Malham, Muhammad. (2023). Problems of the Legal System in Cybercrime, Birzeit University, Palestine.

[19] Mina, Fayeq. (2025). The impact of electronic fingerprinting in criminal cases, accessed 6.10.2025 https://www.menafayq.com/the-impact-of-electronic-fingerprint-in-criminal-cases/

[20] National Institute of Standards and Technology (NIST). (2013). Biometric specifications for personal identity verification (NIST Special Publication 800-76-2). U.S. Department of Commerce.

[21] NIST. (2013). Biometric Specifications for Personal Identity Verification (SP 800-76-2). National Institute of Standards and Technology.

[22] Pavlidis, I., & Buddharaju, P. (2009). Physiological face recognition in the thermal infrared spectrum. IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29*(4), 613–626.

[23] Sciences, 11(37), 1–9. Springer Open. https://doi.org/10.1186/s41935-021-00225-z

[24] Silva, N., Proença, H., & Alexandre, L. A. (2019). Thermal face recognition: A comprehensive overview. Pattern Recognition Letters*, 125*, 123–131.

[25] Telecom Review. (2024). Electronic Fingerprinting... Will It Destroy Passwords? Accessed October 5, 2025. https://www.telecomreviewarabia.com/articles/reports-coverage/3956-electronic-fingerprinting-will-it-destroy-passwords

[26] Zhao, L., Li, Y., & Li, J. (2021). Thermal face recognition via deep learning and image enhancement. Sensors, 21(11), 3778.