



كلية القانون  
College of Law

Tikrit University Journal for Rights

Journal Homepage : <http://tujr.tu.edu.iq/index.php/t>

# The Scientific, Criminal and Applied Foundations of the Electronic Fingerprint

**Asst. Prof. Dr. Nibras Salim Khudhair**

**Law Department ,Al Kunooze University College, Basra, Iraq**

[nibras.s@knuoozu.edu.iq](mailto:nibras.s@knuoozu.edu.iq)

## Article info.

### Article history:

- Received 24 May 2024
- Accepted 19 September 2024
- Available online 1 December 2024

### Keywords:

- Electronic Fingerprint
- Digital Fingerprint
- Legislation
- Security
- Market Size
- Criminal Evidence

**Abstract.:** In today's technological landscape, electronic or digital fingerprinting is a well-established method for enhancing security. This technology is increasingly adopted by various institutions, including government agencies, to address and prevent illegal activities. Prior to the integration and application of this technology, it is essential to understand its foundational aspects. This includes the evolution of electronic fingerprinting and the associated legislation, both on a global scale and within specific national contexts.

The market for fingerprint sensors is expanding rapidly, with projections suggesting a growth from USD 3.5 billion to USD 7.1 billion by the end of 2024. This growth indicates a rising acceptance of electronic fingerprints across various sectors, including public institutions. Consequently, a thorough understanding of the foundational principles of this technology is crucial before its widespread implementation (Rusinek et al.,

---

2019).

This paper explores the scientific, legal, and practical foundations of electronic fingerprinting. The term "foundation" is used here in its legal sense, referring to "evidence." The research focuses on evaluating the evidence related to electronic or digital fingerprints from multiple perspectives. It aims to investigate the scientific, criminal, and practical underpinnings of electronic fingerprinting, while also discussing the relevant legal frameworks. The primary objective of this study is to provide a comprehensive discussion on the foundation of electronic fingerprinting, encompassing scientific, legal, and practical viewpoints (Rusinek et al., 2019). Additionally, the paper will address various legal aspects associated with electronic or digital fingerprints, particularly those targeting illegal activities related to this technology.

---

© 2023 TUJR, College of Law, Tikrit University

---

# الأسس العلمية، الجنائية والتطبيقية لبصمة الأصابع الإلكترونية

أ.م.د. نبراس سالم خضير

قسم القانون، كلية الكنوز الجامعة، البصرة، العراق

[nibras.s@knuoozu.edu.iq](mailto:nibras.s@knuoozu.edu.iq)

## معلومات البحث :

### تواريخ البحث:

- الاستلام : ٢٤ / ايار / ٢٠٢٤

- القبول : ١٩ / ايلول / ٢٠٢٤

- النشر المباشر : ١ / كانون الاول / ٢٠٢٤

## الكلمات المفتاحية :

- بصمة الإصبع الإلكترونية

- بصمة الإصبع الرقمية

- التشريع

- الأمان

- حجم السوق

- الأدلة الجنائية

**الخلاصة:** في المشهد التكنولوجي الحالي، تُعتبر بصمة الإصبع الإلكترونية أو الرقمية طريقة

راسخة لتعزيز الأمان. يتم تبني هذه التقنية بشكل متزايد من قبل مؤسسات متعددة، بما في ذلك

الوكالات الحكومية، لمكافحة الأنشطة غير القانونية ومنعها. قبل دمج وتطبيق هذه التقنية، من

الضروري فهم أساسياتها. يشمل ذلك تطور بصمة الإصبع الإلكترونية والتشريعات المرتبطة بها

على المستوى العالمي وفي سياقات وطنية محددة.

سوق أجهزة استشعار بصمات الأصابع يشهد توسعاً سريعاً، مع توقعات بزيادة من ٣.٥ مليار

دولار أمريكي إلى ٧.١ مليار دولار أمريكي بحلول نهاية عام ٢٠٢٤. هذه الزيادة تشير إلى

قبول متزايد لبصمات الأصابع الإلكترونية عبر مختلف القطاعات، بما في ذلك المؤسسات

العامة. وبناءً على ذلك، من الضروري فهم المبادئ الأساسية لهذه التقنية قبل تنفيذها على

نطاق واسع. (Rusinek et al., 2019) -تستكشف هذه الورقة البحثية الأسس العلمية

والقانونية والتطبيقية لبصمة الإصبع الإلكترونية. يُستخدم مصطلح "الأساس" هنا بمعناه

القانوني، أي "الدليل". يركز البحث على تقييم الأدلة المتعلقة ببصمات الإصبع الإلكترونية أو

الرقمية من وجهات نظر متعددة. تهدف الدراسة إلى التحقيق في الأسس العلمية والقانونية

والتطبيقية لبصمة الإصبع الإلكترونية، بالإضافة إلى مناقشة الأطر القانونية ذات الصلة.

الهدف الرئيسي من هذه الدراسة هو تقديم مناقشة شاملة حول أساس بصمة الإصبع الإلكترونية،

بما في ذلك وجهات النظر العلمية والقانونية والتطبيقية. (Rusinek et al., 2019) علاوة

على ذلك، ستتناول الورقة البحثية الجوانب القانونية المختلفة المرتبطة ببصمات الإصبع

الإلكترونية أو الرقمية، مع التركيز على الأنشطة غير القانونية المتعلقة بهذه التقنية.

## I. INTRODUCTION

According to the definition of Economic Times, the electronic fingerprint or the digital fingerprint can be depicted as a technology that will help a content owner to protect their content through the copyright system. This technology is based on a particular algorithm which encompasses some content property which includes the object movement, frame snippets, camera cuts and brightness level (Wang *et al.*, 2021). There are different kinds of infliction that have come into the picture through this technology which embrace the security, and piracy of software. In addition to that, it is also used to curb the illegal activities in a credit card. In the modern days, the governments of different countries have incorporated this technology in the biometric context where it can determine the identification of a person.

This is advantageous to store the metadata in a valid database system which will ultimately secure the data. It is not uncommon that there are multiple criminal activities associated with this technology. For instance, numerous hackers have already taken their stand by decrypting the messages and the information which has already been encrypted through this technology (Bengtson *et al.*, 2020). This literature review section of this research paper will concentrate on the foundation that means evidence of the electronic fingerprint. Some legislation has been founded by the respective countries to protect and conceal the data through this technology. Electronic or digital fingerprint technology cannot be established without information technology (Godfrey *et al.*, 2021). That is the reason most of the countries have strength and their information technology act. In countries like India, the government has already set in motion the Information Technology Act 2000 or IT Act (Gada, 2021). This legislation remains successful for data protection as the country has experienced lots of vulnerable issues due to the database hacking. On the other hand, countries like the UK also collaborated with other European countries to strengthen the legislation which will be discussed in the below segment.

## II-IMPORTANCE OF THE RESEARCH

The importance of this research lies in elucidating the scientific, legal, and practical foundations of electronic fingerprint technology. As this technology becomes increasingly utilized by various governmental and private institutions to enhance security and prevent illegal activities, understanding its underlying principles is crucial. The rapid growth in the fingerprint sensor market, projected to double by the end of 2024, reflects the rising acceptance of this technology across multiple sectors. Therefore, the research aims to provide a comprehensive discussion of these foundations, including the legal and security challenges associated with electronic fingerprinting.

## III-RESEARCH OBJECTIVES

### 1. Explore the Scientific Foundations of Electronic Fingerprint Technology:

- Explain how fingerprint sensors work, including the differences between optical and capacitive technologies.
- Study the uniqueness and authenticity of electronic fingerprints compared to other biometric methods, such as DNA.

### 2. Review the Legal Foundations Related to Electronic Fingerprint Technology:

- Analyze local and international legislations governing the use of this technology, such as the General Data Protection Regulation (GDPR) in the European Union and biometric information protection laws in the United States.
- Evaluate how these legislations address issues related to security breaches and identity theft.

### 3. Examine the Practical Foundations of Electronic Fingerprint Technology:

- Review the applications of this technology in various fields such as education, healthcare, and information security.
- Investigate how electronic fingerprints are used to combat criminal activities and improve personal and public safety.

#### 4. Provide Recommendations for Improving the Use and Development of Electronic Fingerprint Technology:

- Suggest ways to enhance security and data protection related to electronic fingerprints.
- Propose strategies for developing laws and policies related to this technology to ensure alignment with international and security standards.

In summary, the research aims to offer a comprehensive and in-depth view of how electronic fingerprint technology operates and its impact on security and law, with a focus on improving its applications and regulatory frameworks in the future.

#### **IV-PROBLEM STATEMENT:**

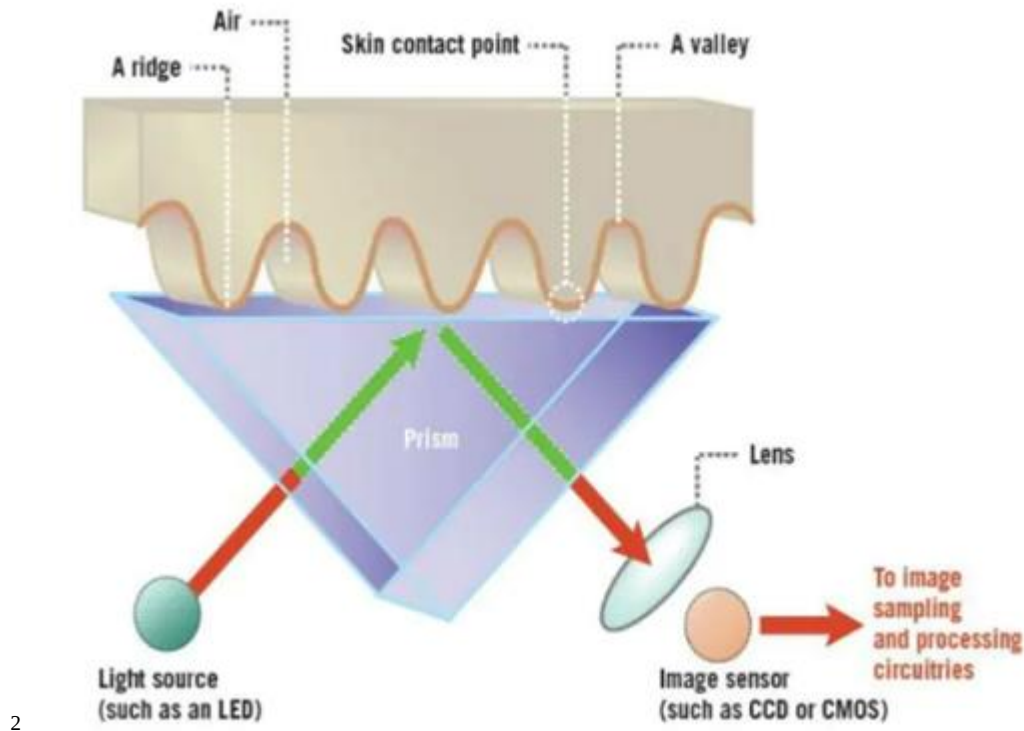
The problem of this research lies in the urgent need to understand the scientific, legal, and practical foundations of electronic fingerprinting. Despite the increasing use of this technology in enhancing institutional security and combating illegal activities, the current understanding of how it operates, the legal challenges it faces, and its practical applications remains insufficient. The research aims to analyze these foundations from scientific, legal, and practical perspectives, and to provide recommendations for improving the use of electronic fingerprints and developing the necessary legal frameworks to ensure their effectiveness and safety.

#### **V- BACKGROUND AND LITERATURE REVIEW**

##### ***1- Scientific foundation of electronic fingerprint and the relevant legislation***

The scientific foundation of electronic fingerprint will help to know the core of electronic or digital fingerprint. The fingerprints are in the form of tiny ridges. The fingerprint of a person is totally unique and it is proven that the electronic fingerprint is more unique and authentic than the DNA of a person (Lai *et al.*, 2020). The scientific foundation of the electronic fingerprint helps to define how the fingerprint scanners properly work and what is the difference between optical and capacitive. There are multiple models and internet of things technologies which fully depend on the fingerprint sensors. It will not be important for

safeguarding the information but it also hold<sup>1</sup>s the identity of a person which is most important in this regard.



**Figure 1: The emergence of light source in digital image of electronic fingerprint**

(Source: Lai *et al.*, 2020)

The two different fingerprint sensors have been used these days such as optical and capacitive. Optical unique fingerprint sensors have been around for some time. The way

<sup>1</sup>Lai, Q., Wan, Z., Akgul, A., Boyraz, O. F., &Yildiz, M. Z. (2020).Design and implementation of a new memristive chaotic system with application in touchless fingerprint encryption.*Chinese Journal of Physics*, 67, 615-630

[https://www.researchgate.net/profile/Oemer-Boyraz/publication/343921090\\_Design\\_and\\_Implementation\\_of\\_a\\_New\\_Memristive\\_Chaotic\\_System\\_with\\_Application\\_in\\_Touchless\\_Fingerprint\\_Encryption/links/5f61d8fd92851c07896a4d1e/Design-and-Implementation-of-a-New-Memristive-Chaotic-System-with-Application-in-Touchless-Fingerprint-Encryption.pdf](https://www.researchgate.net/profile/Oemer-Boyraz/publication/343921090_Design_and_Implementation_of_a_New_Memristive_Chaotic_System_with_Application_in_Touchless_Fingerprint_Encryption/links/5f61d8fd92851c07896a4d1e/Design-and-Implementation-of-a-New-Memristive-Chaotic-System-with-Application-in-Touchless-Fingerprint-Encryption.pdf)

<sup>2</sup>Katta, P., Mohammed, O. A., Prabaakaran, K., Divya, M., Jayashree, G., &Keerthika, D. (2021, May).Smart voting using Fingerprint, Face and OTP Technology with Blockchain. In *Journal of Physics: Conference Series* (Vol. 1916, No. 1, p. 012139). IOP Publishing.<https://iopscience.iop.org/article/10.1088/1742-6596/1916/1/012139/pdf>

through which the optical scanner functioning and also shining with the light above the fingerprint of a person so that it can take the automatic photo. There is a microchip which helps to click the high definition picture by concentrating the different direction of edges that generally present in fingerprint. It also converted them into the 0's and 1's (Katta et al., 2021). The figure 1 is shows the way where in the light sources experiments the information that has been captured. In this case, the high definition photo can be intimated. It is as of now talked about that optical and capacitive fingerprints are broadly utilized innovation these days whether it is mechanical use or biometrical reason. From these two sensors, the use of capacitive sensors is tolerably expanding because of the electrostatic effectiveness strategies. In the modern world, fingerprint scanners are coming out with the typical functions which are also found in smartphones (Ioannou, Tussyadiah& Lu, 2020). For example, there are different kinds of features such as touch screens. In addition to that, it can also focus on human conductivity and also make the electrostatic field that is ultimately made up of technology.

| <b>Colour of the background</b> | <b>Lightning colour for filter</b> | <b>Darkening colour for filter</b> |
|---------------------------------|------------------------------------|------------------------------------|
| Blue                            | Blue                               | Red                                |
| Red                             | Red                                | Blue                               |
| Green                           | Green                              | Red or Blue                        |
| Orange                          | Yellow                             | Blue                               |
| Yellow                          | Yellow                             | Blue                               |

**Table 1: Background Colours of the Electronic Fingerprint Technology**

(Source: Katta et al., 2021)

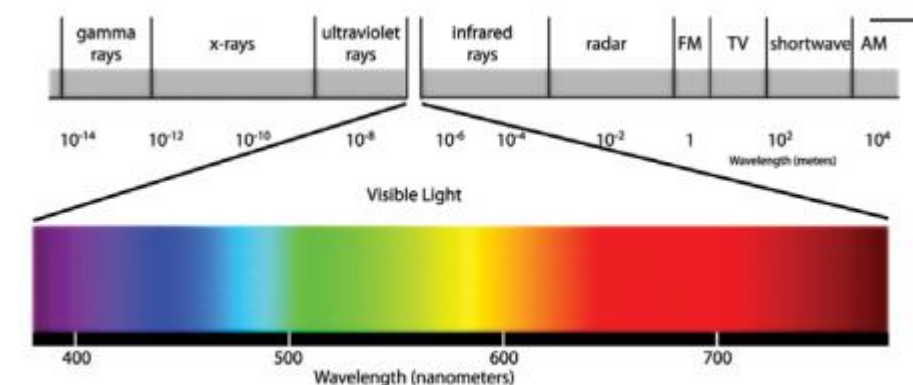
For describing the capacitive images of the fingerprint technology there are required imprint scanner which utilizes the little capacitor for showing the circuits so that it can track the detail of fingerprint. It also taken account the edges off the fingerprint over the conductive plates which can change the charge within the capacitor. On the other hand, the airways in the fingerprint scanner helps to hold the full charge within the capacitor (Khozaimi, Putro&Yaqin, 2021).

It is already discussed that there are some vulnerable issues associated with this technology. That is the reason, the different administrations of different countries have been approached for the multiple summit so that it will be beneficial on the matter of reinforcement of the laws on the matter of electronic fingerprints. <sup>1</sup>Apart from that, there are many developing countries who are not even concerned and initiated any problems using this technology. For example, a country like Bangladesh does not have any data and information privacy act as the resources of this country are limited. This country should take the guidance of other countries such as India for establishing their data protection law in this regard. Some countries are not even interested in the foundation of application in this regard. Countries like China are one of them. In the year of 2021, the country has banned the provision of incorporating information and data from the citizens through using the electronic fingerprint technology including the face recognition Technology. In that case, they will be using the another technology as the country is technological prolific.

---

<sup>1</sup>Khozaimi, A., Putro, S. S., &Yaqin, A. (2021). Improve The Performance and Security of Medical Records using Fingerprint and Advance Encryption Standart.

<https://www.scitepress.org/Papers/2020/103331/103331.pdf>



1

**Figure 2: The Electromagnetic Spectrum of Electronic Fingerprint**

(Source: Khozaimi, Putro&Yaqin, 2021)

In that case, the “forensic science of fingerprint” is usually taken into account by the law enforcement departments of different countries. In this backdrop, the term named forensic science is most relevant because it helps to identify the different kinds of laws and legislation associated with it. Countries like the USA have been focused on numerous laws including Federal rules of evidence. 702 is one of them which is most vital when it comes to the context of electronic fingerprints. The definition and employment of expert testimony, which are likewise material to people performing measurable erosion edge impression assessments, are communicated in FRE 702 (Haack, 2020).

Inside a couple of years, the unique mark mechanization focal point of Japanese scientists had changed. By 1969, the Recognizable proof Segment of the Criminal Examination Department, Public Police Office of Japan (NPA), moved toward NEC to foster a framework for the computerisation of unique finger impression recognisable proof. NEC confirmed that it's anything but a computerized unique mark recognizable proof framework utilizing a comparative particulars based way to deal with that being utilized in the FBI framework being worked on. Around then, it was thought that a completely robotized framework for looking through fingerprints would not be acknowledged for 5 to 10 years. In 1969, NEC and NPA delegates visited the FBI and started to learn about the present status of the workmanship for the FBI's AFIS plans. During a similar period, NPA delegates additionally

teamed up with Moore and Wegstein from NIST. Extra AFIS locales were visited where data was gained with respect to and useless methodologies that had been endeavored. The entirety of this data was assessed and utilized in the improvement of the NEC framework.

## ***2- The criminal foundation of electronics fingerprint and the relevant legislation***

The criminal foundation of the electronic fingerprint will help to show the tools and techniques that is required for recognising the criminal activities in this regard. According to the opinion of Juan Vucetich, the statistician of Central police department in Argentina, there is required the classification systems for identifying the fingerprint of the criminals. In that case, this person also made the classification Vucetich's characterization framework and individualization of detainees using fingerprints were the principal commonsense employments of the finger impression science by law authorization staff. Different nations soon investigated utilizing a unique mark framework to recognize detainees (Khozaimi, Putro&Yaqin, 2021). To decrease the criminal activities in this regard, the different administrations of different countries have<sup>1</sup> collaborated with the aim of strengthening the data protection law. Global steps have been incorporated by the countries so that the laws can be secured against the criminal activities.

2

| Sensor                  | Advantage                                                                               | Disadvantage                                                                                                                        |
|-------------------------|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Optical contact sensors | <ul style="list-style-type: none"> <li>• very quick</li> <li>• user-friendly</li> </ul> | <ul style="list-style-type: none"> <li>• not resistant to dirt</li> <li>• not hygienic</li> <li>• Don't recognise living</li> </ul> |

<sup>1</sup>Khozaimi, A., Putro, S. S., &Yaqin, A. (2021). Improve The Performance and Security of Medical Records using Fingerprint and Advance Encryption Standart.<https://www.scitepress.org/Papers/2020/103331/103331.pdf>

<sup>2</sup>Wu, X., Hanke, W., Fink, M., Klett, M., &Thomale, R. (2020).Harmonic fingerprint of unconventional superconductivity in twisted bilayer graphene.*Physical Review B*, 101(13), 134517.<https://arxiv.org/pdf/1909.03514>

|                                |                                                                                                                      |                                                                                                                                |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
|                                |                                                                                                                      | tissue                                                                                                                         |
| Electronic contact sensors     | <ul style="list-style-type: none"> <li>● Resistant to dirt</li> <li>● Very quick</li> <li>● User-friendly</li> </ul> | <ul style="list-style-type: none"> <li>● not hygienic</li> <li>● don't recognise living tissue</li> </ul>                      |
| Capacitive contact sensors     | <ul style="list-style-type: none"> <li>● very quick</li> </ul>                                                       | <ul style="list-style-type: none"> <li>● not resistant to dirt</li> <li>● don't recognise living tissue not hygenic</li> </ul> |
| Temperature contact sensors    | <ul style="list-style-type: none"> <li>● recognise living tissue</li> <li>● very quick</li> </ul>                    | <ul style="list-style-type: none"> <li>● not hygienic</li> </ul>                                                               |
| Optical non contact sensors    | <ul style="list-style-type: none"> <li>● Resistant to dirt</li> <li>● Hygienic</li> <li>● Very quick</li> </ul>      | <ul style="list-style-type: none"> <li>● don't recognise living tissue</li> </ul>                                              |
| Ultrasonic non contact sensors | <ul style="list-style-type: none"> <li>● resistant to dirt</li> <li>● Hygienic</li> <li>● very quick</li> </ul>      | <ul style="list-style-type: none"> <li>● don't recognise living tissue</li> </ul>                                              |

**Table 2: Contact and Non-contact Fingerprint Sensor**

(Source: Khozaimi, Putro&amp;Yaqin, 2021)

One such legislation is “General Data Protection Regulation For European Member States” which can address the decryption activities by the hackers. It has initiated some pertinent steps which have shown below.

There are 28 countries including the United Kingdom currently provisioned the guidelines that can be set up in terms of legislation when it comes to maintain the security in the electromagnetic fingerprint. There are multiple government who has initiated the provision of information assortment of the people through biometric process. Nevertheless, Washington has followed Texas and Illinois through the biometric protection laws 2017. California also altered the security guidelines on the year of 2018.

According to Jordanet al.,(2021), the law (CCPA and now its new layer named CPRA) is habitually introduced as an expected model for a U.S.data protection law. Virginia and New York also followed the techniques of California so that they can control the biometric information with the zero error. In the year 2017, the apex court and high courts of the India has controlled the fundamental right for taking the biometric information through this technology so that it can be maintained under an appropriate security.

### **3- The applied foundation of electronic fingerprint and the relevant laws**

There are numerous non profit social organisations which focus on the partnership with the different countries and their administration so that palpable laws and legislation can be secured against the fraud activities. One such social organisation is Sovrin Foundation that made the partnership for the “Applied Recognition”.

An organization with Applied Acknowledgement will permit the Sovrin Establishment to convey biometric restriction to improve the protection and security of its computerized certifications and advanced wallets, to handle fraud (Yang, Duan&Tehranipoor, 2020). The biometric restricting will be a standard component of another advanced wallet delivered by Sovrin, alongside broad interoperability across personality environments, as a feature of the Establishment's endeavors to reinforce the security of computerized certain accreditations, as indicated by a joint assertion.

Sovrin needs to dispatch a worldwide standard computerized wallet utilizing facial acknowledgment to get the wallet and the qualifications, with biometric preparation performed inside the wallet to decrease the danger of information spillage contrasted with in the cloud (Fan, 2020). The non-benefit Sovrin Establishment chips away at innovation and foundation to help 'Personality for All' furnished with Security by Plan and Default. The wallet subsequently is proposed to help consistency with information insurance guidelines all throughout the planet including the EU General Information Security Guideline (GDPR), the Canadian Individual Data Assurance and Electronic Records Act (PIPEDA), and the California Purchaser Protection Act (CCPA).

The benefits of biometric restricting as far as ensuring buyers against data fraud, as per the organizations, incorporate the opportunities for a qualification guarantor to check the personality of a wallet proprietor utilizing their government provided picture ID joined with Applied Acknowledgment's face biometrics prior to giving the accreditation (Santa Daría,

Avila & Mátyus, 2021). Unquestionable qualifications can likewise be bound to the substance of the proprietor to decrease hazard of certification burglary or parodying, and give more grounded affirmation to dependent parties that the accreditation is being introduced by the real proprietor.

The computerised wallet application is relied upon to be accessible on iOS and Android with help for five dialects at dispatch (Kyaria, 2020). Applied Acknowledgement is centered around security safeguarding biometric arrangements, and says its innovation is accessible for reconciliation into any computerized wallet, as they multiply and are embraced by society.

Numerous nations are presently "modernizing" their ID data sets to incorporate biometric identifiers that confirm or check personality dependent on actual attributes like fingerprints, iris, face and palm prints, step, voice and DNA (Tarbert, 2020). While allies contend that biometric identifiers are a productive method to precisely distinguish individuals, biometrics are expensive, inclined to blunder, and present outrageous dangers to protection and individual opportunity.

Once biometric information is caught, it as often as possible streams among administrative and private area clients (Goldsack et al., 2020). Organizations have created biometric frameworks to control admittance to spots, items and administrations. Residents can be requested a thumbprint to get to e-taxpayer supported organizations or go into a room in a corporate central command. Geolocation following, video reconnaissance and facial acknowledgment programming based on top of enormous biometrics assortments can additionally empower unavoidable observation frameworks.

After 9/11, numerous legislatures started gathering, putting away and utilizing biometrics identifiers in public IDs. Specialists defended these drives by contending that biometric ID and confirmation gets borders, check business and migration, arraign lawbreakers, and battle personality extortion and psychological warfare. Regardless of this pattern, the residents of numerous nations have effectively gone against biometric public ID plans including Australia, Canada, New Zealand, the UK, and the US.

There are different kinds of applications of the electronic fingerprints including the identification of the genetic problems and issues. In this scenario, it is becoming obsolete

gradually because of the introduction and application of the DNA method. There are many scholars who have already published their research where they present “ the inheritance of the figure print styles”. In these modern days, the utilisation of fingerprints has been increasing gradually by different organisations and industries, especially if the business sectors are willing to incorporate some strategy regarding it. It will ultimately help to identify the persons who are not willing to work and sometimes they evade their work. The ridge formation is a concept which is associated with this electronic fingerprint technology but there is some corruption that has been identified by the scientist. In that case, they uphold their consciousness and concerns to the different administrations of the different countries so that they can make some guidelines on legislation in this regard. The governments of the democratic countries are especially concerned about the corruption that is happening when it comes to exercise and application of this technology.

Most of the countries have been working on legislation for this technology but the United States of America worked in this regard in a prior manner. As of now, there are three states mainly working on this field. For example, the state of Illinois has made the legislation named Biometric information privacy act (BIPA). This protocol was passed in the real of 2008 in the general assembly of Illinois. Countries like the USA have passed several legislation including the non compliance penalty. In addition to that, countries like Kenya are also concerned about this matter. That is the reason they have prioritised consumer protection.

The legislation, like biometric information time, has clearly stated the provision where it assures to provide statutory damages for the violation. Countries like Kenya have also initiated some programs to increase awareness in this regard. The high court and apex court of this country work collaboratively and present a program named the national identity biometric program. It will protect the information of the general public and minorities of this country until the country enact laws on this specific topic. The Government of this country also categorised some fields where the identities by using the biometrics or the electronic fingerprint is required. For example, in the educational field, Health Care institutions, and the people who are from outside are required to put their information through this technology.

## VI-CONCLUSIONS

The research paper has described the foundation of electronic fingerprints in different perspectives. The entire research has been divided into different modules so that it can be accomplished in a structured manner. At the initial stage of this research paper, the research aim, objectives and research questions have been described in this regard. In addition to that, the literature review section of this paper has also depicted the scientific, criminal and applied foundation of the electronic fingerprint. First it describes the scientific evolution and evidence of the electronic fingerprint. This paper also incorporated some global laws that have been incorporated by the different countries so that the criminal activities can be reduced.

## VII-Results

### 1. Understanding of Electronic Fingerprinting:

The research highlights that electronic fingerprinting has evolved as a critical security technology, distinguishing itself by providing unique and reliable identification methods compared to traditional biometric systems. The study confirms that electronic fingerprints are often more unique than DNA, emphasizing their importance in personal identification.

### 2. Legal Frameworks:

The analysis of existing legislation reveals a patchwork of laws globally. Countries like the United States, India, and members of the European Union have enacted various regulations addressing the collection, use, and protection of biometric data, such as GDPR and BIPA. These laws aim to safeguard individual rights while enhancing security measures.

### 3. Practical Applications:

The research demonstrates the broad applications of electronic fingerprinting across sectors, including healthcare, finance, and law enforcement. The use of this technology significantly aids in crime prevention and enhances security measures in institutional settings.

#### 4. Challenges Identified:

The study identifies challenges related to data security, privacy concerns, and the potential misuse of biometric information. It also notes the technological disparities between developed and developing countries regarding the implementation of electronic fingerprint systems.

### VIII- Recommendations

#### 1. Enhancing Legal Frameworks:

A- Standardization of Laws: Countries should work towards creating standardized international laws governing electronic fingerprinting to facilitate cross-border data sharing and security.

B-Regular Updates: Existing laws should be periodically reviewed and updated to keep pace with technological advancements and emerging threats.

#### 2. Investment in Technology:

A-Research and Development: Governments and private institutions should invest in R&D to enhance the accuracy and security of fingerprint technologies, including developing advanced algorithms to prevent spoofing and hacking attempts.

B-Public Awareness Campaigns: Educating the public about the benefits and risks associated with electronic fingerprinting can foster trust and encourage responsible use.

#### 3. Interdisciplinary Collaboration:

A-Partnerships Across Sectors: Collaboration between governments, tech companies, and civil society organizations can lead to the development of better security measures and ethical guidelines for using biometric data.

B-Global Forums: Establishing international forums for sharing best practices and experiences related to biometric technology can enhance collective understanding and improve regulatory measures.

#### 4. Focus on Privacy Protection:

A-Data Protection Regulations: Stricter regulations must be put in place to ensure that individuals' biometric data is collected, stored, and used responsibly, with clear penalties for non-compliance.

B-User Consent: Policies should mandate explicit user consent for data collection, ensuring individuals are informed about how their biometric data will be used and protected.

#### 5. Encouraging Inclusive Technology Development:

A-Support for Developing Countries: Wealthier nations should assist developing countries in establishing legal frameworks and technological infrastructure to adopt electronic fingerprinting responsibly.

A-Adaptable Solutions: Solutions must be adaptable to different cultural and legal contexts to ensure that biometric technologies serve all populations effectively and ethically.

By addressing these recommendations, stakeholders can create a more secure, trustworthy environment for electronic fingerprinting that protects individual rights while enhancing security across various sectors.

## REFERENCE LIST

1. BENGTON, A. M., KUMWENDA, W., LURIE, M., KLYN, B., OWINO, M., MILLER, W. C., ...&HOSSEINIPOUR, M. C. (2020). IMPROVING MONITORING OF ENGAGEMENT IN HIV CARE FOR WOMEN IN OPTION B+: A PILOT TEST OF BIOMETRIC FINGERPRINT SCANNING IN LILONGWE, MALAWI. *AIDS AND BEHAVIOR*, 24(2), 551-559.
2. [HTTPS://WWW.NCBI.NLM.NIH.GOV/PMC/ARTICLES/PMC6994376/](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6994376/)
3. FAN, W. (2020). DEEP ENCODER-DECODER NEURAL NETWORK FOR FINGERPRINT IMAGE DENOISING AND INPAINTING. *ARXIV PREPRINT ARXIV:2005.01115*. [HTTPS://ARXIV.ORG/PDF/2005.01115](https://arxiv.org/pdf/2005.01115)
4. GADA, D. (2021). RETHINKING THE INFORMATION TECHNOLOGY ACT IN THIS NEW CYBER AGE. *INTERNATIONAL JOURNAL OF MODERN AGRICULTURE*, 10(2), 1410-1416. [HTTP://WWW.MODERN-JOURNALS.COM/INDEX.PHP/IJMA/ARTICLE/DOWNLOAD/862/755](http://www.modern-journals.com/index.php/IJMA/article/download/862/755)
5. HAACK, S. (2020). JUDGING EXPERT TESTIMONY: FROM VERBAL FORMALISM TO PRACTICAL ADVICE. *QUAESTIOFACTI. INTERNATIONAL JOURNAL ON EVIDENTIAL LEGAL REASONING*, 1, 13-30. [HTTPS://DUGI-DOC.UDG.EDU/BITSTREAM/HANDLE/10256/17746/JUDGINGEXPERT%20.PDF?SEQUENCE=1](https://dugi-doc.udg.edu/bitstream/handle/10256/17746/JUDGINGEXPERT%20.PDF?sequence=1)
6. JORDAN, S., NAKATSUKA, Y., OZTURK, E., PAVERD, A., & TSUDIK, G. (2021). VICEROY: GDPR-/CCPA-COMPLIANT ENFORCEMENT OF VERIFIABLE ACCOUNTLESS CONSUMER REQUESTS. *ARXIV PREPRINT ARXIV:2105.06942*. [HTTPS://ARXIV.ORG/PDF/2105.06942](https://arxiv.org/pdf/2105.06942)
7. KATTA, P., MOHAMMED, O. A., PRABAARAKARAN, K., DIVYA, M., JAYASHREE, G., & KEERTHIKA, D. (2021, MAY). SMART VOTING USING FINGERPRINT, FACE AND OTP TECHNOLOGY WITH BLOCKCHAIN. IN *JOURNAL OF PHYSICS: CONFERENCE SERIES* (VOL. 1916, NO. 1, P. 012139). IOP PUBLISHING. [HTTPS://IOPSCIENCE.IOP.ORG/ARTICLE/10.1088/1742-6596/1916/1/012139/PDF](https://iopscience.iop.org/article/10.1088/1742-6596/1916/1/012139/pdf)

8. KHOZAIMI, A., PUTRO, S. S., &YAQIN, A. (2021). IMPROVE THE PERFORMANCE AND SECURITY OF MEDICAL RECORDS USING FINGERPRINT AND ADVANCE ENCRYPTION STANDART.
9. [HTTPS://WWW.SCITEPRESS.ORG/PAPERS/2020/103331/103331.PDF](https://www.scitepress.org/Papers/2020/103331/103331.pdf)
10. LAI, Q., WAN, Z., AKGUL, A., BOYRAZ, O. F., &YILDIZ, M. Z. (2020).DESIGN AND IMPLEMENTATION OF A NEW MEMRISTIVE CHAOTIC SYSTEM WITH APPLICATION IN TOUCHLESS FINGERPRINT ENCRYPTION.*CHINESE JOURNAL OF PHYSICS*, 67, 615-630.
11. [HTTPS://WWW.RESEARCHGATE.NET/PROFILE/OEMER-BOYRAZ/PUBLICATION/343921090 DESIGN AND IMPLEMENTATION OF A NEW MEMRISTIVE CHAOTIC SYSTEM WITH APPLICATION IN TOUCHLESS FINGERPRINT ENCRYPTION/LINKS/5F61D8FD92851C07896A4D1E/DESIGN-AND-IMPLEMENTATION-OF-A-NEW-MEMRISTIVE-CHAOTIC-SYSTEM-WITH-APPLICATION-IN-TOUCHLESS-FINGERPRINT-ENCRYPTION.PDF](https://www.researchgate.net/profile/OEMER-BOYRAZ/publication/343921090_Design_and_implementation_of_a_new_memristive_chaotic_system_with_application_in_touchless_fingerprint_encryption/links/5f61d8fd92851c07896a4d1e/Design-AND-IMPLEMENTATION-OF-A-NEW-MEMRISTIVE-CHAOTIC-SYSTEM-WITH-APPLICATION-IN-TOUCHLESS-FINGERPRINT-ENCRYPTION.PDF)
12. RUSINEK, R., GANCARZ, M., KREKORA, M., &NAWROCKA, A. (2019).A NOVEL METHOD FOR GENERATION OF A FINGERPRINT USING ELECTRONIC NOSE ON THE EXAMPLE OF RAPESEED SPOILAGE.*JOURNAL OF FOOD SCIENCE*, 84(1), 51-58.[HTTPS://ONLINELIBRARY.WILEY.COM/DOI/PDF/10.1111/1750-3841.14400](https://onlinelibrary.wiley.com/doi/pdf/10.1111/1750-3841.14400)
13. SANTA DARÍA, A. M., AVILA, G., &MÁTYUS, E. (2021). FINGERPRINT REGION OF THE FORMIC ACID DIMER: VARIATIONAL VIBRATIONAL COMPUTATIONS IN CURVILINEAR COORDINATES. *PHYSICAL CHEMISTRY CHEMICAL PHYSICS*, 23(11), 6526-6535. [HTTPS://ARXIV.ORG/PDF/2012.03010](https://arxiv.org/pdf/2012.03010)
14. WAILI, T., ZAID, A. N. M., &ALKAWAZ, M. H. (2020).ADVANCED VOTING SYSTEM USING FINGERPRINT.*INTERNATIONAL JOURNAL ON PERCEPTIVE AND COGNITIVE COMPUTING*, 6(2), 18-21.
- 15.
16. [HTTPS://JOURNALS.IIUM.EDU.MY/KICT/INDEX.PHP/IJPCC/ARTICLE/DOWNLOAD/172/126](https://journals.iium.edu.my/kict/index.php/IJPCC/article/download/172/126)
17. WANG, Y., ZHAO, C., WANG, J., LUO, X., XIE, L., ZHAN, S., ...& YING, Y. (2021). WEARABLE PLASMONIC-METASURFACE SENSOR FOR NONINVASIVE AND UNIVERSAL MOLECULAR FINGERPRINT DETECTION

- ON BIOINTERFACES.SCIENCE ADVANCES, 7(4), EABE4553.  
[HTTPS://ADVANCES.SCIENCEMAG.ORG/CONTENT/ADVANCES/7/4/EABE4553.FULL.PDF](https://advances.sciencemag.org/content/advances/7/4/EABE4553.full.pdf)
18. WU, X., HANKE, W., FINK, M., KLETT, M., & THOMALE, R. (2020). HARMONIC FINGERPRINT OF UNCONVENTIONAL SUPERCONDUCTIVITY IN TWISTED BILAYER GRAPHENE. *PHYSICAL REVIEW B*, 101(13),
19. 134517. [HTTPS://ARXIV.ORG/PDF/1909.03514](https://arxiv.org/pdf/1909.03514)
20. DARWIS, M., NISWATY, R., & ARHAS, S. H. (2021, MAY). FINGERPRINT ELECTRONIC ATTENDANCE APPLICATION. IN *IOP CONFERENCE SERIES: MATERIALS SCIENCE AND ENGINEERING* (VOL. 1125, NO. 1, P. 012076). IOP PUBLISHING. [HTTPS://IOPSCIENCE.IOP.ORG/ARTICLE/10.1088/1757-899X/1125/1/012076/PDF](https://iopscience.iop.org/article/10.1088/1757-899X/1125/1/012076/pdf)
21. YANG, Y., DUAN, Z., & TEHRANIPOOR, M. (2020). IDENTIFY A SPOOFING ATTACK ON AN IN-VEHICLE CAN BUS BASED ON THE DEEP FEATURES OF AN ECU FINGERPRINT SIGNAL. *SMART CITIES*, 3(1), 17-30.
22. [HTTPS://WWW.MDPI.COM/2624-6511/3/1/2/PDF](https://www.mdpi.com/2624-6511/3/1/2/pdf)
23. KYARIA, A. K. (2020). MANAGING FINTECH'S DESTRUCTION THROUGH INNOVATIVE BANKING: AN EMPIRICAL INVESTIGATION. *TECHNOLOGY*, 13(1).  
[HTTPS://WW.IJCC.NET/IMAGES/VOL\\_13/13121\\_KYARI\\_2020\\_E\\_R.PDF](https://www.ijcc.net/images/vol_13/13121_kyari_2020_e_r.pdf)
24. TARBERT, H. P. (2020). MODERNIZING CFIUS. *GEORGE WASHINGTON LAW REVIEW ARGUENDO*, 88(6). [HTTPS://WWW.GWLR.ORG/WP-CONTENT/UPLOADS/2021/01/88-GEO.-WASH.-L.-REV.-1477.PDF](https://www.gwlr.org/wp-content/uploads/2021/01/88-GEO.-WASH.-L.-REV.-1477.pdf)
25. GOLDSACK, J. C., CORAVOS, A., BAKKER, J. P., BENT, B., DOWLING, A. V., FITZER-ATTAS, C., ... & DUNN, J. (2020). VERIFICATION, ANALYTICAL VALIDATION, AND CLINICAL VALIDATION (V3): THE FOUNDATION OF DETERMINING FIT-FOR-PURPOSE FOR BIOMETRIC MONITORING TECHNOLOGIES (BIOMETS). *NPJ DIGITAL MEDICINE*, 3(1), 1-15.  
[HTTPS://WWW.NATURE.COM/ARTICLES/S41746-020-0260-4](https://www.nature.com/articles/S41746-020-0260-4)

26. GODFREY, A., VANDENDRIESSCHE, B., BAKKER, J. P., FITZER-ATTAS, C., GUJAR, N., HOBBS, M., ...&IZMAILOVA, E. S. (2021). FIT-FOR-PURPOSE BIOMETRIC MONITORING TECHNOLOGIES: LEVERAGING THE LABORATORY BIOMARKER EXPERIENCE. *CLINICAL AND TRANSLATIONAL SCIENCE*, 14(1), 62-74.<https://ascpt.onlinelibrary.wiley.com/doi/pdf/10.1111/CTS.12865>
27. IOANNOU, A., TUSSYADIAH, I., & LU, Y. (2020).PRIVACY CONCERNS AND DISCLOSURE OF BIOMETRIC AND BEHAVIORAL DATA FOR TRAVEL.*INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT*, 54, 102122.[https://www.researchgate.net/profile/IIS\\_TUSSYADIAH/PUBLICATION/341340368\\_PRIVACY\\_CONCERNS\\_AND\\_DISCLOSURE\\_OF\\_BIOMETRIC\\_AND\\_BEHAVIORAL\\_DATA\\_FOR\\_TRAVEL/LINKS/5F9178C792851C14BCDB7E36/PRIVACY-CONCERNS-AND-DISCLOSURE-OF-BIOMETRIC-AND-BEHAVIORAL-DATA-FOR-TRAVEL.PDF](https://www.researchgate.net/profile/IIS_TUSSYADIAH/PUBLICATION/341340368_PRIVACY_CONCERNS_AND_DISCLOSURE_OF_BIOMETRIC_AND_BEHAVIORAL_DATA_FOR_TRAVEL/LINKS/5F9178C792851C14BCDB7E36/PRIVACY-CONCERNS-AND-DISCLOSURE-OF-BIOMETRIC-AND-BEHAVIORAL-DATA-FOR-TRAVEL.PDF)