International Journal of Multidisciplinary Research and Publications
ISSN (Online): 2581-6187

Forensic Fingerprinting Through the Ages: A Critical Evaluation of Techniques from Traditional Powdering to Digital Scanning

Maryam Zulfiqar, Ayesha Asif, Urwa Tul Wusqa*, Hasnain Azam, Amna Rani, Muhammad Asad Ullah, Zaheer Ahmad, Humaira Bibi, Sadia Nazeer, Sidra Majeed
Institute of Biological Sciences, Khwaja Fareed University of Engineering and Information Technology Rahim Yar khan 64200, Punjab, Pakistan
*Corresponding Authors: Urwa Tul Wusqa

Abstract*—Criminal activity has always been a concern, prompting the development of the Automated Fingerprint Identification System (AFIS). Fingerprints are unique and do not change over time, making it necessary to develop a foundational fingerprint system. Various methods have been discovered to reveal latent fingerprints in crime scenes, including physical methods like powdering, chemical methods like iodine and ninhydrin solution, iodine fuming and silver nitrate solution. However, hand sanitizers, oils, and lotions can impact digital fingerprint recording, making it difficult for experts to identify real offenders. A study examined the effects of different lubricants on plain white paper fingerprints. Non-slick cream and alcohol-free hand sanitizer had no effect, while grease and oil had no effect. The study recommends proper hand washing for better fingerprint impressions. The powder technique for latent fingerprint detection uses a finely split formulation applied to fingermark impressions, adhering mechanically to sweat residue. The ridge pattern is defined by the powder's color, and the latent print is considered developed. Fingerprints are crucial for biometric identification in forensic investigations, law enforcement. The dye solution incubated allowed for clear visibility, and the cyanoacrylate fuming method allowed for level 1 to level 3 details from fine fingerprint structures. The study compared two approaches to understand the impact of the pre-treatment stage. Mass death identification involves gathering and examining scientific identifiers and background data. A recent paradigm change necessitates expedited identification to meet media, legislative, and survivor demands. Postmortem fingerprint identification is a quick and effective method, and digital fingerprint capture will be crucial in disaster victim identification scenarios*.

***Keywords*—** *Fingerprint, AFIS, Forensic Investigation, Ninhydrin, Iodine Fuming, Silver Nitrate, Disaster Victim*.

I. INTRODUCTION

The little ridges that emerge on the fingers' volar pads during embryonic development are called fingerprints, and they enable one to hold onto objects without slipping. (1) Even while scientists have long questioned whether fingerprints are truly unique, people nevertheless use them to identify one person from another, even identifical twins.(2)Furthermore, the fingerprints remain the same over time and are permanent. They are useful pieces of evidence at a crime scene because of these qualities. One of the most important pieces of evidence at a crime scene is a fingerprint, which can be used to establish guilt. (3) A major problem with fingerprinting in crime detection is that the more police and crime detection officers know about the most recent advancements in the field, the quicker criminal investigations will be, and the judge will have an easier time casting a vote and deciding who the offender is. This allows the judge to render a decision with a clear conscience. The judge would be less inclined to reach a decision if there was more carelessness in the evidence gathering process. As a result, scientific crime detection can be useful in expediting the resolution of a case and avoiding its prolongation. The importance of fingerprinting, the distinctive qualities of fingerprints, and the ability to identify people, criminals, and offenders using fingerprints are all important issues. In the event that technical issues are accurately recorded, maintained, and observed, fingerprints may be used as evidence in the same way as other types of evidence.(4) The publications in this study that discuss the use of different unconventional, widely accessible powders to uncover latent fingerprints were published between 2009 and 2020.(5)This paper discussed importance of fingerprints and their processing in the fields of criminal investigation, law enforcement, and the successful identification of a deceased person's body have all been covered in this essay. Additionally, we have showcased its cutting-edge fingerprint algorithms in the domains of identification, matching, classification, fingerprint spoof detection, and feature extraction. Furthermore, we highlighted fingerprint applications for the future and demonstrated how they are used in our daily lives. (6) Ancient Babylonian, Greek, Chinese, and Roman civilisations all used fingerprints. The earliest friction ridge skin impressions discovered to date are thought to be fingerprints. However, whether its deposition in ancient civilization was accidental or intended for a particular purpose—such as ornament or symbolism—is unclear. This process is known as offline fingerprint acquisition.(7) Henry Faulds brought attention to the usefulness of finger prints in the 1880s, which marked the beginning of the contemporary use of fingerprints, even if the Chinese may have used them as a crude form of identification, and in the detection of criminals.(8)In the late 1800s, fingerprints were first employed in criminal trials.In 1902, the first fingerprint evidence was used in London, and in 1905, it was used in a murder trial in the United Kingdom. The acceptance of fingerprint evidence as competent evidence—that is, evidence that may be accepted

Maryam Zulfiqar, Ayesha Asif, Urwa Tul Wusqa, Hasnain Azam, Amna Rani, Muhammad Asad Ullah, Zaheer Ahmad, Humaira Bibi, Sadia Nazeer, and Sidra Majeed, "Forensic Fingerprinting Through the Ages: A Critical Evaluation of Techniques from Traditional Powdering to Digital Scanning," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 6, pp. 190-196, 2024.

on its own merits and does not require confirmation from other sources—by UK courts began with these British instances. The acceptance of palm, foot, and toe prints in UK courts did not take long (9).

Fingerprint detection technique Conventional methods for detecting fingerprints involve Using a glass-fibre or camel-hair brush, a finely split formulation is applied to the fingermark impression in the powder technique for latent fingerprint detection. The ridge pattern is defined by the powder's mechanical adhesion to the perspiration residue. The latent print is considered to have developed when the ridge pattern becomes apparent due to the powder's typical colouring. The most straightforward and widely used method for creating latent fingerprints is powder dusting. Additionally, fingerprint experts have been using this method for the longest time. No complex equipment is needed for this. By brushing and tapping, even a novice hand may develop the prints. The identification of prints might be done in a lab or at the crime scene. (10) The Chemical Approach Ninhydrin and eosin were used as chemical reagents in two different procedures that were compared to the more modern superglue fuming method. It was discovered that the type of surface the prints were placed on affected the chemical enhancement of the three methods. The results shown that latent fingerprints on non-porous surfaces might be enhanced using the eosin method and superglue fuming.(11)Physical Techniques involves Vacuum metal breakdown. A thin-film deposition method called vacuum metal deposition coats a substrate by evaporating the source metal in a vacuum. The method has long been used in industry to apply metal coatings on materials like glass to create mirrors. Tolansky first suggested the use of VMD as a tool for the forensic enhancement of latent fingermarks in 1964, but it would take over ten years for the technique to get sufficient recognition to be taken seriously as a feasible development methodology. The article to be improved is placed inside the deposition chamber at a high vacuum, usually less than 3 ÿ $10^{n}4$ mbar, as part of the therapy. Additionally, the chamber has a glass that lets the operator observe the deposition process and filaments to hold the metal to be deposited. The most often utilised metals in the VMD therapy of latent fingermarks are zinc and gold, with zinc being applied after gold.(12)In contrast to ordinary lifters, gel lifters contain a different kind of adhesive. The adhesive is comprised of flexible, low-adhesive gelatin material, which makes it easier for the lifters to conform to the surface. This makes the lift from textured surfaces easier to remove. A fingerprint with noticeable ridge detail may be lifted from non-porous surfaces using BVDA gel lifters; the lifted prints indicated that the powder was reacting with the adhesive gel because the ridges were lighter than the furrows.(13) The BVDA gel lifter was also tested for successfully lifting fingerprints from porous surfaces, however it was unsuccessful. The raised fingerprint's non-porous surface allowed for the collection of DNA. It is unknown whether the BVDA gel lifter will be able to remove a detailed fingerprint from a textured surface without experiencing the same issues as the standard adhesive fingerprint lifter because the research did not evaluate the lifter's performance on textured surfaces (14).

Early Digital Imaging Techniques:

In the 1970s and 1980s, optical scanners made the first attempts to digitize fingerprints, aiming to replace the manual ink-and-paper process. A scanner that took a digital picture of the fingerprint was usually used in the procedure. The resolution and processing capacity of the technology available at the time placed restrictions on early systems.(15)

Optical Scanners: The earliest optical scanning systems recorded the ridges and valleys of a fingerprint using reflected light. These were frequently costly and inconvenient.(16)

Resolution: Because of the comparatively poor resolution of these early scanners, digital images were not always crisp or detailed enough for precise matching.

Automatic Fingerprint Identification Systems (AFIS) 1980s and 1990s

Automated Fingerprint Identification Systems (AFIS), which stored, searched, and matched fingerprint data using computer technology, were developed in the 1980s. Fingerprints were digitized by early AFIS implementations, making it possible to search through huge databases more quickly.(17)

Digitization and Encoding: Using early image capture technologies, fingerprints were digitized, and important characteristics (such as minutiae points) were encoded as a collection of numerical values.

Image Enhancement: Techniques for manipulating digital images started to appear, such as algorithms for enhancing scanned fingerprints. The photos were made more suitable for matching algorithms by applying techniques including ridge strengthening, noise reduction, and contrast correction.

Biometric Integration (2000s-Present)

The use of fingerprints for identification and authentication in security systems had made fingerprinting a crucial component of biometric systems by the early 2000s.(18) The methods for digital imaging were regularly improved in order to increase scalability, speed, and reliability.

High-Resolution Imaging: Real-time, high-resolution, high-quality fingerprint photographs were made possible by developments in digital camera technology and optical sensors.(19)

Multimodal Biometrics:

In order to increase accuracy and dependability, fingerprint systems started to be included in bigger biometric systems that could combine fingerprint recognition with additional biometric data types, such as voice recognition, iris scans, or facial recognition.

Faster Processing:

Real-time fingerprint matching and verification are made possible by modern digital imaging techniques that make use of powerful computers. This is especially crucial for law enforcement, border control, and other security application. (20)

Maryam Zulfiqar, Ayesha Asif, Urwa Tul Wusqa, Hasnain Azam, Amna Rani, Muhammad Asad Ullah, Zaheer Ahmad, Humaira Bibi, Sadia Nazeer, and Sidra Majeed, "Forensic Fingerprinting Through the Ages: A Critical Evaluation of Techniques from Traditional Powdering to Digital Scanning," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 6, pp. 190-196, 2024.

Live Scan Fingerprinting

Live scan (without the use or ink or paper) fingerprinting is the process of electronically taking a person's fingerprints with a scanner. It offers a quick, precise, and hygienic substitute for conventional inked fingerprinting. Live scan technology directly takes digital pictures of a person's fingerprints, which are subsequently saved and sent electronically, as opposed to the ink-and-paper approach, which involves rolling the fingerprints onto a card.(21)

Technology behind live live scan Optical Sensor: Optical fingerprint sensors perform by illuminating light on the fingerprint and then using a camera to take a picture of the reflected image. The fingerprint ridges are usually illuminated by infrared light, and the picture of the fingerprint is captured by a digital camera or a charge-coupled device (CCD). A fingerprint's ridges and valleys reflect light differently when a finger is placed on the glass plate of an optical sensor, producing a contrast. A digital image is created by capturing this variation in reflection. A high-resolution digital representation of the fingerprint is acquired in the image, which can then be processed further for comparison, improvement, and minutiae extraction.

Capacitive Sensors: In contrast, capacitive fingerprint sensors measure the electrical charge at various locations on the surface of the finger. When a finger is put on these sensors, changes in the electrical field are measured by an array of tiny capacitors. (22) A change in capacitance occurs at the locations where a finger is placed on a capacitive sensor because the fingerprint's ridges make closer contact with the sensor array. The capacitance changes less in the valleys because they are farther from the sensor. A digital image is then created by mapping this variation. Because capacitive sensors can detect even minute ridge and valley variations, they frequently produce incredibly detailed images

3D Scanning Technologies

Overview of 3D fingerprint capture: Using proficient sensors, 3D fingerprint capture produces a three-dimensional map of the fingerprint's surface, including its ridges, valleys, and minute details. (23) Usually, the technology underlying this procedure uses one of the following techniques:

Structured light scanning

The basic idea behind structured light scanning is that a predetermined pattern of light typically grids or stripes is projected onto the fingerprint's surface. A camera records the pattern's distortion from the ridges and valleys in order to produce a three-dimensional model. Offers detailed, high-resolution 3D images with little physical touch, making it appropriate for post-mortem reconstruction as well as live scan. (24)

Laser scanning (LIDAR):

Laser-based methods scan the fingerprint using a laser beam. To create a three-dimensional surface, the laser bounces off the ridges and valleys, and the time it takes for the light to return is measured. Extremely precise, capable of capturing intricate fingerprint features, and useful in forensic settings where surface detail is crucial.

Contactless 3D Scanning: This technique uses optical sensors and high-resolution cameras to take a fingerprint without making physical contact. The sensor measures the light reflection from the finger's surface to produce a three-dimensional depiction.(25) It is hygienic and non-invasive, enabling a thorough fingerprint scan without physical contact.

Application in forensic reconstruction and matching

Reconstructing Forensic Evidence: Even in cases where a deceased person's fingerprints are damaged or deteriorated, post-mortem identification aids in their reconstruction. Increases the accuracy of identification by taking precise three-dimensional pictures of deformed or partial fingerprints collected at crime scenes.

Fingerprint Matching: High-quality 3D fingerprint scans are digitally stored for later investigation, even in the event that real prints deteriorate. Because 3D data includes surface and depth details, it improves the accuracy of matching damaged or partial fingerprints. More precise searches, particularly for difficult prints, in fingerprint databases.

Biometric Security: Enhanced security systems make it more difficult to forge or spoof fingerprints by adding an extra degree of protection to fingerprint-based verification. For more safe and dependable identification in high-security environment. (26)

Forensic Fingerprinting in Legal Context

Fingerprint Evidence in Court:

Although fingerprint evidence is essential to criminal investigations and court cases, there are significant legal requirements that must be met for it to be admitted. These guidelines are intended to guarantee that fingerprint evidence is trustworthy, relevant to the matter at hand, and valid from a scientific standpoint.

Legal standards for admissibility of fingerprint evidence:

The 1993 Daubert Standard: The U.S. Supreme Court established rules for the acceptance of scientific evidence in federal courts in the Daubert v. Merrell Dow Pharmaceuticals case, which gave rise to the Daubert Standard. This criterion is used to assess the scientific validity and applicability of the approach utilized in a particular sort of evidence (like fingerprint analysis). All evidence should be relevant to the current case. The evidence must be derived from a trustworthy scientific technique. Examining the methods' peer review, general acceptability, mistake rates, and controlled testing are all part of this process. To prove the legitimacy of the technique and the link between the defendant and the evidence, expert testimony is necessary.(27)

The Frye Test (1923): Another legal criterion for determining whether scientific evidence is admissible is the Frye Test, which was developed in the case of Frye v. United States. It stipulates that the relevant scientific community must usually approve the scientific method or approach employed to generate proof. The methodology or procedure must be deemed genuine and dependable by the majority of the

Maryam Zulfiqar, Ayesha Asif, Urwa Tul Wusqa, Hasnain Azam, Amna Rani, Muhammad Asad Ullah, Zaheer Ahmad, Humaira Bibi, Sadia Nazeer, and Sidra Majeed, “Forensic Fingerprinting Through the Ages: A Critical Evaluation of Techniques from Traditional Powdering to Digital Scanning,” *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 6, pp. 190-196, 2024.

relevant scientific community. The Frye Test determines if the scientific community as a whole agrees that the evidence is reliable and accurate. In the context of fingerprinting, this indicates that the evidence will probably satisfy the requirements for admissibility of the Frye Test if the majority of forensic fingerprint experts accept a specific technique of fingerprint identification (such as ridge-counting or minutiae analysis).(28)

Challenges and Controversies in Admissibility:

Even while fingerprint evidence is widely accepted in court, there are still arguments against its inclusion, especially in light of growing scientific scrutiny. Among the main issues are:

Error Rates: The issue of error rates presents a significant obstacle in fingerprint situations. Concerns of misidentification have arisen as a result of the lack of established procedures for fingerprint comparison, particularly when examiners depend on their own subjective evaluation of minute details.

Cognitive Bias: Confirmation bias can have an impact on experts, especially if they are aware of the case's background (such as whether the suspect has already been identified). This may result in conclusions that are not accurate.

High-profile cases where fingerprint evidence has been contested

FBI's Brandon Mayfield (2004) Misidentification:

The 2004 erroneous arrest of American lawyer Brandon Mayfield in relation to the Madrid train bombings is one of the most well-known instances of fingerprint misidentification. Mayfield's fingerprints were mistakenly identified by the FBI as being on a plastic bag that contained detonators. Subsequent analysis revealed that the fingerprints were, in fact, those of an Algerian guy. The possibility of human error in fingerprint recognition was brought to light by the FBI's erroneous research and overconfidence in the match. The validity of fingerprint analysis was seriously called into doubt by this case, especially since it was conducted in the absence of adequate supporting documentation. *Result:* The FBI acknowledged their mistake and Mayfield was freed from custody after two weeks. This instance was crucial.(29)

The West Memphis Three (1993-2011) – The Role of Contested Evidence:

In 1994, the West Memphis Three—Jason Baldwin, Jessie Misskelley, and Damien Echols were found guilty of killing three 8-year-old boys in West Memphis, Arkansas. A forced confession, questionable witness testimony, and forensic evidence including fingerprint evidence were all used in the case against them. The prosecution insisted on the connection, despite the defense's contention that fingerprint evidence from the crime scene could not be conclusively linked to the accused. Experts then challenged the interpretation that a fingerprint obtained at the crime scene matched one of the defendants because it was too ambiguous to be deemed definitive. The case also brought up more general issues regarding the precision of fingerprint analysis and the dangers of depending too much on uncorroborated forensic evidence.

Result: The three men were freed in 2011 following years of court cases and the discovery of fresh DNA evidence. The case brought to light the dangers of relying on fingerprint evidence that has not been adequately verified to sustain erroneous convictions. (30)

The Case of The Unsolved Robbery (2007) – Fingerprint and DNA Evidence Conflict:

In a 2007 robbery case, a piece of stolen property had a suspect's fingerprints on it, but DNA evidence later disproved the link to the defendant. According to the defense, fingerprint evidence by itself was insufficient to prove a clear connection to the crime. The defense emphasized that fingerprint evidence does not always indicate criminal behavior because innocuous fingerprints can be left behind. They maintained that, particularly in the absence of additional proof, a suspect's print on an item does not always prove that they committed the crime. *Result:* Because of discrepancies between DNA analysis and fingerprint evidence, the court finally favored acquittal, casting doubt on the validity of forensic evidence in certain situations. (31)

Evolving Standards with Digital Fingerprinting

To identify unique user behaviors and make online environments safer, digital fingerprinting standards have rapidly evolved as technology advances. By collecting and examining data points such as device information, IP addresses, browser settings, and user activity, this technique allows websites and platforms to generate a unique "fingerprint" for each visitor. Because digital fingerprinting is more accurate and efficient at identifying suspicious activity and stopping fraud, it can be a helpful tool for businesses and digital platforms trying to protect their users and data. However, new digital fingerprinting standards also need to combine privacy concerns with legal requirements.

The growing sophistication of fingerprinting technologies raises questions about user consent and the potential for data exploitation. Regulatory bodies like the CCPA and GDPR are keeping a close eye on these activities and are pressuring companies to adopt transparent rules and provide customers greater control over their data. As standards advance, attention turns to creating digital fingerprinting technologies that, by boosting security and safeguarding user privacy, support a digital ecosystem that is both safer and more private. (32)

Legal challenges and acceptance of digital fingerprints:

As politicians debate the morality of gathering and utilizing user-specific data, the legal environment surrounding digital fingerprinting continues to face difficulties. Though this same feature poses privacy concerns, digital fingerprints can be quite accurate in identifying individuals based on device setups, browsing behaviors, and other unique data points. Digital fingerprints are frequently regarded as sensitive data by legal frameworks such as the California Consumer Privacy Act (CCPA) in the United States and the General Data Protection Regulation (GDPR) in Europe, which place stringent restrictions on the collection and processing of

Maryam Zulfiqar, Ayesha Asif, Urwa Tul Wusqa, Hasnain Azam, Amna Rani, Muhammad Asad Ullah, Zaheer Ahmad, Humaira Bibi, Sadia Nazeer, and Sidra Majeed, “Forensic Fingerprinting Through the Ages: A Critical Evaluation of Techniques from Traditional Powdering to Digital Scanning,” *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 6, pp. 190-196, 2024.

personal data. Adoption of the technology is made more difficult by the need for businesses to secure user consent, make data-gathering procedures clear, and guarantee that fingerprinting procedures comply with legal requirements. (33)

Role of expert testimony and validation of digital methods:

Validating digital fingerprinting techniques requires expert evidence, particularly in court settings where the precision and dependability of these approaches may be questioned. To help juries and judges comprehend the technological foundations and constraints of this data, experts in court offer insights on the collection, analysis, and interpretation of digital fingerprints. Since they clarify elements like device uniqueness, data accuracy, and the likelihood of false positives, their testimony is crucial for proving the legitimacy of digital evidence. In situations involving fraud or cybercrime, where digital fingerprinting is utilized to connect people to online activity, this can be especially crucial.(34)

Comparative Evaluation of Methods

To choose the most trustworthy and efficient strategy for user identification and fraud protection, a comparative analysis of digital fingerprinting techniques is necessary. (35) Numerous data pieces, including browser settings, device-specific traits, and behavioral patterns, are captured by different fingerprinting approaches. Each technique has its advantages and disadvantages. (36) For example, behavioral fingerprinting offers more detailed information about user behavior but may be more susceptible to variations and false positives, while device fingerprinting may be excellent in terms of consistency but may have trouble tracking users across multiple devices. Organizations can determine which strategy best suits their security requirements and legal requirements by contrasting various options.

Accuracy and Reliability:

When contrasting digital and conventional powder-based fingerprinting procedures, it becomes clear that surface type and ambient factors have a significant impact on accuracy and dependability. (37) On smooth, nonporous surfaces, where the powder sticks effectively to fingerprints, powder-based methods work quite well. However, fingerprint impressions may be imperfect or deteriorated on rough, porous, or textured surfaces, where they frequently struggle. By capturing finer details independent of surface texture, digital techniques like digital imaging or laser-based scanning can get over these restrictions and produce findings that are crisper and more reliable. Accuracy can also be impacted by environmental factors such as temperature, humidity, and dust exposure. Digital methods can frequently take prints in a larger range of conditions, improving reliability across a variety of scenarios, whereas powder may smear or disperse in specific environments. (38)

Efficiency and Speed

The move from manual to automated digital methods has significantly increased fingerprint analysis speed and efficiency. Conventional powder-based methods are time-consuming and labor-intensive since they need to be applied carefully and lifted by hand.(39) The time needed for analysis in forensic labs is significantly decreased by automated digital technologies, which can scan, process, and analyze prints in a matter of seconds. High-throughput processing is becoming more and more crucial in modern labs, and this speed gain improves workflow overall. By automating search and match activities, digital tools like Automated Fingerprint Identification Systems (AFIS) further streamline the process and free up forensic experts to concentrate on more intricate analysis and validation work. Because of this change, law enforcement organizations are now able to process cases more quickly and effectively. (40)

Cost-Effectiveness:

There is a notable difference in the initial costs and long-term savings when comparing the cost-effectiveness of traditional and digital fingerprinting techniques. Due to their low equipment and material requirements, traditional powder-based processes are typically less expensive to execute initially. However, in large-scale operations, these labor-intensive and time-consuming approaches may result in higher cumulative costs. High-tech digital systems are more cost-effective in the long run while being more costly to set up since they require sophisticated hardware and software. Rapid fingerprint analysis and matching save money for the legal and law enforcement systems by cutting down on staff hours and processing delays. Investing in digital fingerprinting technology can have significant cost benefits in high-volume settings, increasing overall productivity and accelerating return on investment. (41)

Limitations and Challenges

Technical Limitations: Despite their improvements, digital fingerprinting techniques still have technical issues, especially when it comes to obtaining clear prints in challenging environments. For example, conventional powder-based methods have trouble adhering to wet or greasy surfaces, which causes smudged or insufficient impressions. Similar restrictions apply to digital sensors since residue, oil, or moisture can mask fingerprint ridges, decreasing the accuracy and dependability of photos that are taken. (42) Digital techniques can also distort or obscure important features due to sensor limitations like image noise and resolution restrictions. The quality of digital capture may deteriorate in poor light or when resolution is reduced, which could affect identification accuracy. (43)

Privacy and Ethical Concerns: Fingerprinting raises important privacy and ethical concerns, especially in digital settings. Concerns regarding privacy violations are raised by the growing usage of digital fingerprints as biometric data in security and surveillance systems. There is a risk of abuse when biometric data is widely used to track or monitor people, particularly when it comes to illegal data sharing or surveillance.(44) Furthermore, the expansion of digital fingerprinting databases makes them attractive targets for hackers, raising the possibility of data breaches. Since fingerprints cannot be altered as passwords can, people who

Maryam Zulfiqar, Ayesha Asif, Urwa Tul Wusqa, Hasnain Azam, Amna Rani, Muhammad Asad Ullah, Zaheer Ahmad, Humaira Bibi, Sadia Nazeer, and Sidra Majeed, "Forensic Fingerprinting Through the Ages: A Critical Evaluation of Techniques from Traditional Powdering to Digital Scanning," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 6, pp. 190-196, 2024.

have their biometric data compromised suffer long-term privacy risks. This risk emphasizes the necessity of stringent data security protocols, moral standards, and openness to preserve personal privacy while weighing the security advantages of fingerprinting technology.(45)

Future Trends in Forensic Fingerprinting

Emerging Technologies: With their sophisticated imaging techniques and ultra-sensitive detection procedures, emerging technologies are completely changing the fingerprinting industry. The sensitivity of detection has been greatly increased by innovations like nanotechnology and quantum dots, which enable analysts to identify even weak or deteriorated prints that may otherwise go undetected.(46) Specifically, quantum dots can draw attention to minute minutiae in fingerprints, improving resolution and increasing the accuracy of identification. Simultaneously, multispectral and hyperspectral imaging are being used to scan many light wavelengths to acquire prints in higher detail. These imaging approaches provide a fuller and more accurate fingerprint profile by revealing information that is not detectable by conventional methods, such as underlying skin patterns and residues.(47)

Role of Big Data and Cloud Computing

By making it possible to incorporate international fingerprint databases into cloud-based solutions, big data, and cloud computing are revolutionizing fingerprint analysis.(48) This interface speeds up and simplifies cross-jurisdictional collaboration by enabling quick data sharing between forensic labs and law enforcement organizations around the globe. However, there are additional security and standardization issues brought up by this data centralization. Because centralized fingerprint databases are appealing targets for cybercriminals, maintaining data security becomes essential. Furthermore, because global interoperability is complicated by differences in technology, legal norms, and data protection legislation, harmonizing fingerprinting protocols across nations and authorities can be challenging.(49)

Potential for Fully Automated Forensic Laboratories

Fully automated forensic labs, where AI-driven systems manage real-time analysis and expedite fingerprint processing, are becoming possible because to advancements in AI. Artificial intelligence (AI) algorithms might quickly process, match, and classify fingerprints in these futuristic labs with little assistance from humans. In addition to expediting case resolution, this technology could improve reliability by lowering the possibility of human error. AI-driven laboratories would probably rely on machine learning models and real-time data analysis to quickly identify suspicious trends and make accurate identifications. Although these technologies have potential, their broad use will necessitate significant financial outlays as well as careful handling of privacy and data handling issues in completely automated systems.(50)

II. CONCLUSION

Fingerprinting remains a cornerstone of criminal investigation and biometric identification, evolving significantly through technological advancements. Traditional methods, such as powder techniques, continue to be fundamental for forensic applications, while modern innovations like digital scanning and automated fingerprint identification systems (AFIS) enhance accuracy and efficiency in complex cases. Despite its strengths, fingerprinting faces challenges, including susceptibility to environmental factors and privacy concerns in digital contexts. Emerging technologies, such as 3D fingerprinting and multispectral imaging, show promise for capturing higher-quality data, potentially transforming forensic capabilities. With the integration of big data and AI, fingerprint analysis is poised to become faster, more reliable, and less dependent on human interpretation. As fingerprinting techniques continue to progress, they hold immense potential for forensic science, provided ethical and privacy considerations are carefully addressed to ensure the responsible use of this powerful identification tool.

REFERENCES

1. Wertheim, K. (2011). Embryology and morphology of friction ridge skin. *The fingerprint sourcebook*, *1*.
2. Jain, A. K., Prabhakar, S., & Pankanti, S. (2002). On the similarity of identical twin fingerprints. *Pattern Recognition*, *35*(11), 2653-2663.
3. Williams, R., & Johnson, P. (2007). Trace biometrics and criminal investigations. *Handbook of criminal investigation*, 357-380
4. Gorelick, J. S., Marzen, S., & Solum, L. (1995). *Destruction of evidence*. Wolters Kluwer.
5. Vadivel, R., Nirmala, M., & Anbukumaran, K. (2021). Commonly available, everyday materials as non-conventional powders for the visualization of latent fingerprints. *Forensic Chemistry*, *24*, 100339.
6. Jagannath, A., Jagannath, J., & Kumar, P. S. P. V. (2022). A comprehensive survey on radio frequency (RF) fingerprinting: Traditional approaches, deep learning, and open challenges. *Computer Networks*, *219*, 109455.
7. Hoover, J. E. (1971). The role of identification in law enforcement: An historical adventure. . *John's L. Rev.*, *46*, 613.
8. Cole, S. A. (2009). *Suspect identities: A history of fingerprinting and criminal identification*. Harvard University Press.
9. Berry, J., & Stoney, D. A. (2001). The history and development of fingerprinting. *Advances in fingerprint Technology*, *2*, 13-52.
10. Batra, N., Kaur, A. P., Banerjee, T., Sodhi, G. S., & Kaur, J. (2020). Development of Fingerprints on Dry and Wet Surfaces.
11. Ahmad, U. K., & Musa, A. (2002). Superglue fuming for the chemical enhancement of latent fingerprints. *Jurnal Teknologi*, 83â-91.
12. Swiontek, S. E., & Lakhtakia, A. (2015). Vacuum-metal-deposition and columnar-thin-film techniques implemented in the same apparatus. *Materials Letters*, *142*, 291-293.
13. Purtell, J., Speers, J., & Cottrill, E. (2021). *Development of a method to recover fingerprints from textured surfaces* (Doctoral dissertation, Murdoch University).
14. Hammell, L., Deacon, P., & Farrugia, K. J. (2014). Chemical enhancement of soil-based marks on nonporous surfaces followed by gelatin lifting. *Journal of Forensic Identification*, *64*(6), 583-608.
15. Stiefel, C. (2017). *Investigating Fingerprints*. Enslow Publishing, LLC.
16. Sandström, M. (2004). Liveness detection in fingerprint recognition systems.
17. Komarinski, P. D. (2017). Automated fingerprint identification systems. In *Cold Case Homicides* (pp. 317-326). CRC Press.
18. Allen, R., Sankar, P., & Prabhakar, S. (2005). Fingerprint identification technology. In *Biometric systems: Technology, design and performance evaluation* (pp. 22-61). London: Springer London.

Maryam Zulfiqar, Ayesha Asif, Urwa Tul Wusqa, Hasnain Azam, Amna Rani, Muhammad Asad Ullah, Zaheer Ahmad, Humaira Bibi, Sadia Nazeer, and Sidra Majeed, "Forensic Fingerprinting Through the Ages: A Critical Evaluation of Techniques from Traditional Powdering to Digital Scanning," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 6, pp. 190-196, 2024.

19. Mohamed Abdul Cader, A. J., Banks, J., & Chandran, V. (2023). Fingerprint Systems: Sensors, Image Acquisition, Interoperability and Challenges. *Sensors*, *23*(14), 6591.
20. Jain, A. K., & Ross, A. (2015). Bridging the gap: from biometrics to forensics. *Philosophical Transactions of the Royal society B: Biological sciences*, *370*(1674), 20140254.
21. Jain, A., & Pankanti, S. (2001). Automated fingerprint identification and. *Proc. Adv. Fingerpr. Technol*, *275*.
22. Tartagni, M., & Guerrieri, R. (1998). A fingerprint sensor based on the feedback capacitive sensing scheme. *IEEE Journal of Solid-State Circuits*, *33*(1), 133-142.
23. Kumar, A. (2018). *Contactless 3D fingerprint identification*. Springer International Publishing.
24. Rajeev, S., KM, S. K., & Agaian, S. S. (2016, May). Method for modeling post-mortem biometric 3D fingerprints. In *Mobile Multimedia/Image Processing, Security, and Applications 2016* (Vol. 9869, pp. 159-168). SPIE.
25. Kumar, A. (2018). *Contactless 3D fingerprint identification*. Springer International Publishing.
26. Ametefe, D. S., Sarnin, S. S., Ali, D. M., & Zaheer, M. Z. (2022). Fingerprint liveness detection schemes: A review on presentation attack. *Computer Methods in Biomechanics and Biomedical Engineering: Imaging & Visualization*, *10*(2), 217-240.
27. Berger, M. A. (1993). Procedural paradigms for applying the Daubert test. *Minn. L. Rev.*, *78*, 1345.
28. Bretz, R. J. (1986). Scientific evidence and the Frye rule: The case for a cautious approach. *Cooley L. Rev.*, *4*, 506.
29. Oig, A. (2006). Review of the FBI's Handling of the Brandon Mayfield Case. *Office of the Inspector General, Oversight and Review Division, US Department of Justice*, 1-330.
30. Hughes, S. (2017). American monsters: Tabloid media and the satanic panic, 1970–2000. *Journal of American Studies*, *51*(3), 691-719.
31. Lynch, M., & McNally, R. (2009). Forensic DNA databases and biolegality. *Handbook of genetics and society*, 283-301.
32. Kitchin, R. (2016). Getting smarter about smart cities: Improving data privacy and data security.
33. Wahyuningtyas, S. Y., & Singgalen, Y. A. (2023). Mapping Stakeholder Perceptions: Navigating Biometric Data Protection Initiative and Face Recognition Technology Support in Indonesia.
34. Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. Computer Law & Security Review, 21(5), 408-414.
35. Ogbanufe, O., & Kim, D. J. (2018). Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. Decision Support Systems, 106, 1-14.
36. Kumar, V., & Paul, K. (2023). Device fingerprinting for cyber-physical systems: a survey. ACM Computing Surveys, 55(14s), 1-41.
37. Powell, C. J., & Seah, M. P. (1990). Precision, accuracy, and uncertainty in quantitative surface analyses by Auger-electron spectroscopy and x-ray photoelectron spectroscopy. Journal of Vacuum Science & Technology A: Vacuum, Surfaces, and Films, 8(2), 735-763.
38. Chan, H. N., Tan, M. J. A., & Wu, H. (2017). Point-of-care testing: applications of 3D printing. Lab on a Chip, 17(16), 2713-2739.
39. Hoffmann, M., & Elwany, A. (2023). In-space additive manufacturing: A review. Journal of Manufacturing Science and Engineering, 145(2), 020801.
40. Erciyes, E. (2018). A new change management approach for a law enforcement organization. International Journal of Police Science & Management, 20(1), 52-65.0
41. Poirier, C. C., & McCollum, D. (2006). RFID Strategic Implementation and ROI: a practical roadmap to success. J. Ross Publishing.
42. Merkel, R. (2014). New solutions for an old challenge: chances and limitations of optical, non-invasive acquisition and digital processing techniques for the age estimation of latent fingerprints. Logos Verlag Berlin GmbH.
43. Aasen, H., Honkavaara, E., Lucieer, A., & Zarco-Tejada, P. J. (2018). Quantitative remote sensing at ultra-high resolution with UAV spectroscopy: a review of sensor technology, measurement procedures, and data correction workflows. Remote Sensing, 10(7), 1091.
44. Carmona, M. M. S. (2018). Is Biometric Technology in Social Protection Programmes Illegal Or Arbitrary?: An Analysis of Privacy and Data Protection. ILO.
45. Karole, P. A. (2024). Biometric Technology in National Security: Legal Boundaries and Ethical Issues. Biometric Technology Today, 25-31.
46. Fakayode, S. O., Lisse, C., Medawala, W., Brady, P. N., Bwambok, D. K., Anum, D., ... & Grant, C. (2024). Fluorescent chemical sensors: applications in analytical, environmental, forensic, pharmaceutical, biological, and biomedical sample measurement, and clinical diagnosis. Applied Spectroscopy Reviews, 59(1), 1-89.
47. Gomes, F. M., de Pereira, C. M. P., de Cássia Mariotti, K., Pereira, T. M., dos Santos, N. A., & Ro mão, W. (2023). Study of latent fingerprints. Forensic Chemistry, 100525.
48. Manimuthu, A., Dharshini, V., Zografopoulos, I., Priyan, M. K., & Konstantinou, C. (2021). Contactless technologies for smart cities: big data, IoT, and cloud infrastructures. SN computer science, 2(4), 334.
49. Bhise, Y. D. (2024). Cross-Border Sharing of Biometric Data: Legal Complexities and Agreements. Biometric Technology Today, 21-30.
50. Braun, T., Fung, B. C., Iqbal, F., & Shah, B. (2018). Security and privacy challenges in smart cities. Sustainable cities and society, 39, 499-507.