Review on Advancements in Fingerprint Analysis: From Historical Developments to Modern Deep Learning Applications

Phebe Tryphena
Sri Ramachandra University

Abstract— **The evolution of fingerprint analysis traces its roots from the early studies by Marcello Malpighi in the 17th century to its crucial role in modern forensic science. Over time, significant advancements in technology, particularly in image processing and machine learning, have revolutionised fingerprint analysis. This paper explores the historical development of fingerprint analysis, the importance of digital processing, and the role of Automated Fingerprint Recognition Systems (AFRS). It further delves into the significance of noise removal and image-denoising techniques, highlighting the impact of state-of-the-art methods such as Convolutional Neural Networks (CNNs) and Generative Adversarial Networks (GANs). The integration of deep learning techniques has significantly enhanced fingerprint-matching accuracy, speed, and reliability, marking a pivotal shift in forensic investigations and biometric authentication.**

Index Terms— **Fingerprint, Automated Fingerprint Recognition System (AFRS), Image Denoising, Convolutional Neural Networks (CNNs), Generative Adversarial Networks (GANs)**

I. INTRODUCTION

The historical evolution of fingerprint analysis highlights the journey from early observations to its crucial role in modern forensic science. In the 17th century, Italian physician Marcello Malpighi studied the unique and permanent patterns of fingerprints [1]. In the late 19th century, British physician Henry Faulds proposed fingerprints for criminal identification, recognizing the potential of fingerprints as a means of individual identification [2]. Ultimately, this idea was furthered by Sir Francis Galton, who established foundational fingerprint characteristics for understanding the class and individual characteristics found within fingerprints in 1882 [3]. Practical application in criminal investigations became prominent in the 20th century with the development of Automated Fingerprint Recognition Systems (AFRS), revolutionizing law enforcement with reliable information in their criminal investigations [4].

Fingerprints, unique and resistant to alteration, became vital in forensic investigations. Issues like poor image quality due to environmental factors and the need for noise removal to extract valuable information from fingerprint images have been persistent hurdles. Over time, advancements in technology, particularly in image processing and machine learning, have significantly enhanced the field of fingerprint analysis. Deep learning models, especially Convolutional Neural Networks (CNN), have demonstrated potential in effectively analyzing, reconstructing, and matching fingerprint images, contributing to the accuracy and efficiency of identification processes. [5]

Digital Processing Steps For Fingerprint Analysis:

Digital processing stands as a crucial phase in fingerprint analysis, harnessing technological advancements to refine, extract, and interpret fingerprint data for forensic investigations. This article delves into the importance, core steps, and ramifications of digital processing in fingerprint analysis.

Significance of Digital processing: -

Digital processing maximises the utility of fingerprint evidence in forensic inquiries. It unveils latent prints, enhances image quality, and extracts pivotal features crucial for identification and matching. Additionally, it streamlines the manipulation, analysis, and comparison of fingerprints, expediting investigative processes.

These are the following Key steps in Digital processing: -

1. Image Enhancement: This starts by improving the visibility and clarity of latent prints by increasing the quality of fingerprint images by sharpening, reducing noise, and adjusting contrast [figure 1]
2. Ridge Structure Extraction: By estimating ridge orientation, thinning and extracting minutiae, algorithms can distinguish distinct fingerprint patterns by identifying ridge structures and minutiae points. [figure 1] [6] [7]
3. Feature Extraction: Important features that help with individualisation and matching such as bifurcation, ridge termination, and ridge counts are extracted, serving as distinct identifiers. [figure 1] [6] [7]
4. Template Creation: To compare and match fingerprints with the Database a digital fingerprint template is created from the features extracted. [figure 1] [6]
5. Matching and Comparison: To aid in the association of evidence or the identification of suspects. This stage makes it easier to compare fingerprint templates by examining and contrasting the similarities and differences to find a potential match. [figure 1] [6]
6. Database Search: To aid in criminal investigations, a database search is done using unknown fingerprints to detect a link between the collected fingerprints and the existing records. [figure 1] [6]

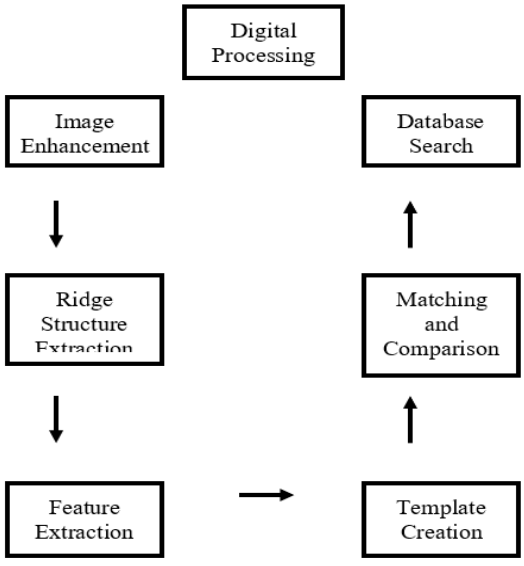


Figure 1: A block diagram explaining the key steps in digital processing

II. LITERATURE SURVEY

A. Significance of Fingerprints in Forensic Investigation

Fingerprints are unique to each and permanent as they remain throughout the lifetime of an individual. They are both indistinctive and permanent. That is why it is more than just a pattern on our fingertips. And because of these unique factors, it has made them indispensable in forensic investigations as they aid the investigation by identifying the individual, linking them to the crime sites and supporting legal systems all over the world. [8]

Forensic investigations rely on tangible evidence to assemble events and identify criminals. Fingerprints are among the most dependable physical evidence obtained at the scene of the crime. They can appear as both Patent fingerprints which are visible imprints and Latent fingerprints, which are invisible to the naked eye and are revealed using special techniques. [9]

At a crime scene, fingerprints are collected and analyzed for numerous purposes. They can validate if someone was there at a given location, back up witness accounts, or directly connect a suspect to a crime. At the same time, fingerprints help to rule out innocent people, making investigations more accurate and efficient. [8] [9]

Given its accuracy and dependability, fingerprint identification is the gold standard in forensic science. Advanced Automated Fingerprint Recognition Systems (AFRS) have further streamlined the process by enabling law enforcement to swiftly compare prints against extensive databases, which not only aids in the identification of suspects and the resolution of crimes but also plays a critical role in preventing wrongful convictions [10].

Fingerprints are highly durable, making them one of the most dependable pieces of evidence. Even when altered or disguised, the basic ridge patterns remain consistent, allowing forensic experts to accurately identify and analyze them. [8]

Fingerprints are important not just in criminal investigations but also in civil identification. They assist in identifying persons following disasters, accidents, or mass casualties, guaranteeing accurate records for legal and administrative purposes.

Technological advancements, notably in image processing and machine learning, have improved fingerprint analysis. Deep learning models, such as

Convolutional Neural Networks (CNNs), have improved the accuracy and efficiency of fingerprint identification, allowing forensic experts to better examine and compare prints. Ultimately, fingerprints are still one of the most potent tools in forensic science. [11]

B. Types of Fingerprint Impressions

The ridges and valleys in the fingerprint form unique and different patterns on the surface of the skin which are classified into distinctive characteristics based on the ridge patterns. This serves forensics as a critical foundation for investigation and identification. Fingerprints are divided into two main categories: Patent prints and Latent prints with each serving a significant part in forensic investigations.

I. Patent Prints:

Patent fingerprints are visible imprints that are left behind on the surfaces when substances like ink [figure 2], grease, blood [figure 3] or dirt get transferred onto them. They can serve as immediate visual evidence as they are commonly seen at the scene of crime. Sometimes forensic professionals utilise chemical processing to improve their clarity and contrast [figure 4], though they are visible to the naked eye [6]. These imprints are categorised based on the imprints that form them such as bloody fingerprints, inked fingerprints or grease-based fingerprints. They are collected using standard forensic methods like photography and lifting techniques.



Figure 2: A fingerprint impression collected on Ink



Figure 3: A greasy fingerprint impression on the tablet screen [6]

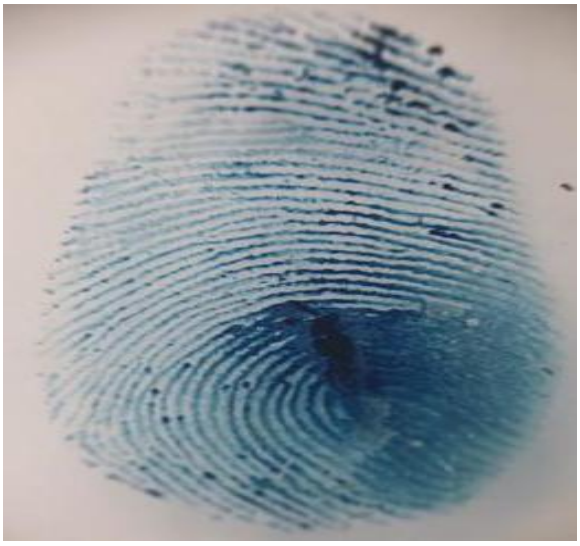


Figure 4: A bloody fingerprint developed with amido black (A chemical reagent) [6]

In the Journal of Forensic Identification (2018), Ashley Sellenraad's case study points out how three patent fingerprints were identified as forgeries on different cheques. They conducted an experiment that demonstrated the skin's flexibility using friction ridge skin and black printer ink and found it difficult to replicate the print with precision, particularly around the edges. The observations found on the fingerprints submitted to be inconsistent and further analysis suggested that stamps were used to place false fingerprints on the cheques. This discovery draws attention to the importance of thorough examination in identifying false patent fingerprints. It also addresses the difficulties associated with attempting to recreate

natural fingerprints for illegal reasons, emphasising the significance of forensic knowledge in identifying genuine impressions from fakes. [11]

II. Latent Prints:

Latent imprints are invisible to the naked eye, unlike patent imprints, and so they require special techniques to enhance the fingerprint to be detected. These impressions are formed by the natural residues that are found in the skin like natural oil, sweat and other substances on the skin, and these cause the impressions to be created when left behind unknowingly. These impressions can be found on various surfaces like glass, paper, wood, metal, plastic etc. and depending on what type of surface, whether porous or non-porous, a specialized technique is used to develop the print using chemical treatment [Figure 4], dusting powder [Figure 5] or alternate light sources [Figure 6] [12].



Figure 5: A fingerprint impression developed using dusting powder [6]

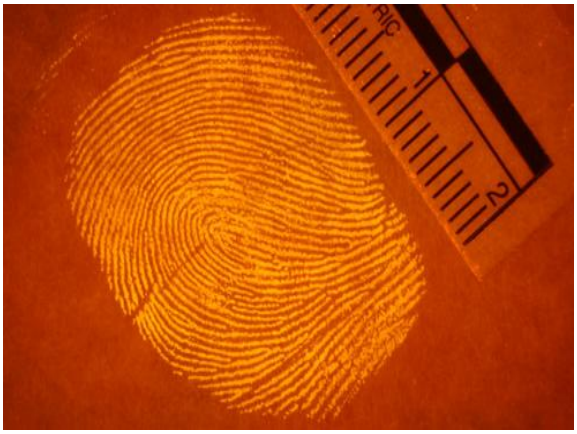


Figure 6: A fingerprint impression visualised using a fluorescent dye stain and an orange alternate light source [6]

A study conducted on Latent fingerprint matching points out the difficulties that a forensic expert faces when identifying, detecting and enhancing a latent imprint that is left behind at the scene of the crime to accurately match these impressions to establish identification. Unlike plain or rolled fingerprint matching, latent fingerprint identification poses difficulties due to poor ridge impressions, limited finger area, and substantial nonlinear distortion. To address this, a system is proposed for matching latent fingerprints to enrolled rolled fingerprints in law enforcement databases. This system incorporates minutiae and extends to utilize additional features like the singularity, ridge quality map, ridge flow map, ridge wavelength map, and skeleton. Testing against databases comprising 29,257 rolled fingerprints revealed a significant enhancement in identification rates, from a baseline of 34.9% to 74% when utilizing these extended features. The study systematically evaluates the importance of each extended feature, highlighting singularity, ridge quality map, and ridge flow map as the most impactful in elevating matching accuracy, offering crucial insights for forensic fingerprint analysis. [13]

Within the realm of latent prints, there are specific classifications based on the impression's quality and distinctiveness:

1. Visible Latent Prints: These are faint impressions that might become visible under certain lighting conditions or angles without enhancement methods.
2. Plastic Prints: Formed when the fingers leave an impression in a soft or malleable material like putty, wax, or clay.
3. Corrosion Prints: These imprints are developed when the metal surfaces react with the natural oils present on the fingertips, causing gradual corrosion and leaving observable impressions.
4. Latent Prints on Porous Surfaces: Porous surfaces such as paper or cloth are absorbent, which makes it challenging to recover fingerprints, so to enhance these impressions specialized techniques are required.

As a forensic expert is it important to understand and distinguish different types of impressions with their subcategories and also to differentiate between latent and patent imprints. This helps the fingerprints to be

collected, enhanced and analysed efficiently and effectively [12]

With machine learning and image processing methods, forensic science progresses to develop to identify and interpret latent impressions with precision. Fingerprint recognition has become more dependable with Deep learning models and their advanced algorithms making fingerprints more competent and precise. Fingerprint analysis and classification ultimately continue to remain a cornerstone of modern forensic science playing an important role in solving crimes and bringing justice all over the world. [11]

C. Automated Fingerprint Recognition System (Afrs)

Automated Fingerprint Recognition Systems (AFRS) have enhanced and modernised the collection and storage process from manual labour to digital cataloguing and have streamlined the identification process by significantly reducing the overall time taken to process the image manually. These advances have greatly benefited law enforcement and forensic investigators.

However, some challenges continue to persist despite the advancement such as poor image quality, overlapping of fingerprints and non-linear distortion Due to these limitations, false identification tends to rise as there are some difficulties in reconstructing and recognising a partial, distorted or degraded fingerprint in the crime scene.

Studies are conducted to improve image clarity, effective database systems and accuracy in algorithms to enhance their performance by using artificial intelligence, machine learning and deep learning models. Studies have shown that partial fingerprint matching using region-based similarity makes it difficult to analyse partial fingerprints. Even scanners or traditional minutiae-based methods fail to capture complete fingerprints and therefore highlight the need to have enhanced recognition technology features. The research proposes fingerprint recognition efficiently by using a correlation coefficient approach comparing a fingerprint pixel-by-pixel overcoming any challenge of minutiae-based recognition and contributing precise and complete fingerprint identification. An efficient metric system is used for scoring and its efficiency is tested by using the Fingerprint Verification Competition (FVC) dataset highlighting the uniqueness of this study. [14]

D. Aadhar's Fingerprint Registration: Technological, Security, And Legal Perspectives

The Government of India launched the Aadhar program in 2009, initially started to providing unique ID to below-poverty-line families but later expanded to identify and document all citizens of India. Key features include biometrics such as fingerprints, iris scans and facial recognition. Fingerprint analysis has played a critical role in this process, providing a robust, cost-effective, and scalable solution to create a unique identifier. [15]

The historical foundation of fingerprint analysis stems from the late 19th century when Sir Francis Galton and others recognized fingerprints' potential for personal identification. By the early 20th century, it became widely accepted for forensic applications. Aadhar's deployment of fingerprint analysis builds on these historical techniques but is integrated into a modern technological infrastructure that enables mass biometric registration. [16]

Aadhar's Biometric system design

Aadhar's fingerprint biometric system is designed with several layers of security:

Unique Identification: Each individual's fingerprint data, along with other biometric information (iris scans), is collected and linked to a 12-digit unique identification number (UID). This creates a non-replicable digital identity. [17]

Multifactor Authentication: Beyond fingerprints, Aadhar integrates additional security layers, including demographic data, mobile phone numbers, and OTP (one-time password) systems to verify user identity. [17]

Encryption: Collected biometric data is encrypted at the source, ensuring that sensitive information is protected from interception during transmission to the Aadhar database. Secure transmission protocols (such as SSL) are used to enhance protection against data breaches. [17]

Anti-Spoofing Mechanisms: To avoid falsification or use of forged fingerprints, Aadhar employs anti-spoofing technologies that differentiate between live fingerprints and replicas. [17]

Technological Framework and Governance

The Fingerprints collected through scanners are stored and maintained by the Unique Identification Authority of India (UIDAI). They use sophisticated tools that

have real-time processing capabilities and supreme matching algorithms. [18]

The complete biometric framework is governed and operated by the Ministry of Electronics and Information Technology, ensuring security, privacy and compliance with standard protocols and regulations [Figure 7]. [19]

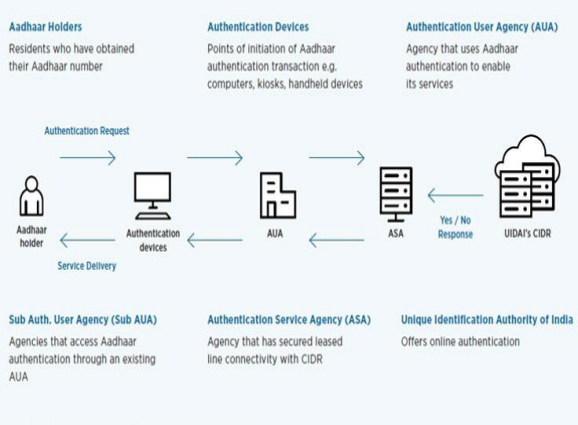


Figure 7: The Technological framework of Aadhar

Security and Privacy Concerns

Some concerns include

1. Data Breaches: This includes identity theft, financial fraud, and misuse of personal information [20]
2. Violation of privacy: Primarily misuse of biometric information i.e. for verification purposes, fear of unnecessary surveillance. [20]
3. Data Access: Misuse of personal information by government agencies [20]

These concerns may be mitigated by using enhanced features like advanced encryption tools, multi-factor authentication and conducting security audits regularly. [21]

Biometric Authentication Challenges

There are some technological challenges in the biometric systems of Aadhaar in fingerprint recognition due to factors like dirt, aged fingerprints, bruises and cuts in the fingerprints etc. which leads to authentication failures though being robust, impacting a user-friendly service [22]

Legal and Ethical Implications

The legal framework for Aadhaar was established in 2016, as the Aadhaar Act, ensuring proper protocols are followed through legally for safe keeping of private information and its ethical concerns. Despite meticulous actions taken, some discrepancies in the Aadhaar Act continue to persist [23]

The Supreme Court identified the need for privacy and enforced rigorous measures for the safekeeping of private information, including the biometric system in 2017. This ruling significantly ensured protection for the citizens that their privacy was not compromised [24].

To standardize the protocols for collecting, storing, and Data handling including biometric information, a Digital Personal Data Protection (DPDP) Act was passed in 2023. This mitigated risks like data breaches, privacy violations and data access. [25]

E. Noise Removal in Fingerprint Analysis

In Fingerprints, noise refers to the distortions that make the ridge patterns unclear, which could have been obtained due to environmental factors or while procuring the fingerprint. This would result in either false positive or false negative Identification making it crucial to remove the noise levels in a fingerprint image, making a significant impact on producing accurate and precise identification while analysing the fingerprint.

Studies have been conducted using histogram equalization, median filtering, and Fourier transform, using Peak Signal-to-Noise Ratio (PSNR) measurement to validate the fingerprint image clarity as they are essential in the image recognition process. [26]

Similarly, another study implemented combining Anisotropic Filtering and Directional Median Filtering (DMF) to reduce noise. Tests on FVC2002 images have shown enhanced fingerprint image quality, making it a significant study. [27]

Image Correction Methods:

Various image correction methods are employed to improve the image quality through noise reduction during the scanning process, they include: [28]

1. Image Enhancement: To enhance the fingerprint image with clarity, techniques like histogram equalization, contrast stretching, and noise reduction are implemented to emphasise the ridges and valleys in a fingerprint for effective matching algorithms [29]

2. Minutiae Detection: Advanced filters help locate minutiae points like ridge ending, bifurcation etc., that are important in identification systems even in a corrupted image [30]
3. Fourier Transform: They reduce noise using Frequency-domain filters while preserving key features of the image. [31]
4. Gabor Filters: These filters are used to enhance the fingerprint ridge pattern by correcting and improving the image quality in partial or distorted fingerprints [32]
5. Contextual Image Correction: They are used to restore the image quality and reconstruct any missing data by learning and understanding the fingerprint image [33]

F. Image Denoising Techniques in Forensic Imaging:

Image denoising in fingerprints is crucial for image quality, clarity, and accuracy in the identification techniques as it removes any distortions that block important information in the fingerprint pattern making it more dependable.

Importance of Image Denoising:

The main goal in denoising an image is to eradicate noise while preserving the integrity of the image. So in a fingerprint, denoising would allow preserve important information by enhancing the image quality while removing noise that could have been caused during image acquisition, or due to environmental factors. [34]

Types of Denoising Techniques:

1. Filter-Based Techniques: Depending on the noise and specific noise character, filters like median, Gaussian, and Wiener are used to denoise while preserving key features from the image.
2. Wavelet-Based Methods: Image denoising depends on Wavelet transform, an instrument that decomposes signal to different frequencies to enhance image quality.
3. Deep Learning-Based Denoising: Neural networks like CNN, denoise images by learning automatically from the inputted images and produce high-resolution images as an outcome. [35]

G. Fingerprint Image Enhancement

The State-of-the-art techniques and innovations in fingerprint image enhancement technology have supremely helped improve quality, efficiency, accuracy and reliability in fingerprint analysis and therefore as a result have enabled scientists and researchers to have a broad range of data to work with. These tools lay the groundwork for futuristic techniques that involve deep learning or machine learning approaches to further enhance accuracy and reliability. [36] [37]

1. Deep Learning-Based Enhancement:

Convolutional neural networks (CNN) which is part of deep learning, have helped improve the quality and accuracy of the image print. CNNs are excellent tools for extracting fingerprint images with intricate details intact, highly accurate, and with the ability to eliminate noise and preserve ridge patterns. The adaptability of this tool only showcases how dynamic and accurate it is, thereby giving us an enhanced image with all the finer details accurately intact. [38]

Fingerprint recognition technologies have widely been used to identify people in areas like security, government, and business. This study presents a new method that uses Gabor filters combined with CNNs to extract finer details, with key features intact for the authentication process. The method includes steps like adjusting image contrast, filtering, and thinning to make features clearer. A special CNN design is also introduced to handle problems with image rotation that older models often struggle with. [38]

The new Gabor-based CNN achieved a high validation accuracy of 99.33% after 64 training cycles, clearly outperforming earlier methods on the same dataset. It handled rotated fingerprints well, showing strong and consistent results. This approach marks a major improvement in both accuracy and flexibility for fingerprint recognition systems. [38]

2. Generative Adversarial Networks (GANs):

Generative Adversarial Networks (GANs), have proven to produce high efficiency in denoising fingerprint images while improving image clarity. It works using two neural networks: A Generator and a Discriminator. The Generator, generate new data that is similar to the inputted data and the Discriminator, learns to identify real data from the fake by differentiating between the real data and the generated data, enabling the generator to generate more realistic data. [39]

A study conducted on “GAN-enabled Latent Fingerprint Enhancement Model for Human Identification System”, showed that the latent prints

collected at the scene of crime from various surfaces were blurred, distorted and unclear impressions making it challenging to analyse the fingerprint. To address these challenges, they used a Generative Adversarial Network (GAN) to eliminate the noise, enhance the image for clear visualisation and recreate a clear image. This resulted significantly in the identification process, from 10.7% similarity to 34.7% after implementing the GAN model. Several metrics such as the Structural Similar Index Metric (SSIM) at 0.996 and the Universal Quality Index (UQI) at 0.002 show how exceptional the model is performed and indicate the similarity of the enhanced image with the original data. [39]

Another study conducted on "NaturalFinger: Generating Natural Fingerprint with Generative Adversarial Networks" used the GAN model to protect intellectual property from being stolen and illegal redistribution. This was done by using the GAN model to generate realistic fingerprints making it harder for the discriminator to detect its unreal or fake targeting the decision difference area making the model more secure and robust. This study has proved to be successful by 17% when compared with other methods. [40]

3. Multi-Scale Approaches:

The multi-scale approach, allows the fingerprint image to be decomposed and enhanced by processing it in different scales or frequencies, allowing it to address issues related to distortion or noise into a high-resolution image preserving critical features such as minutiae points for identification. [41]

4. Adaptive Filtering and Wavelet Transform:

Both techniques are used in signal processing and they complement each other when applied together. Adaptive filtering enhances the fingerprint image quality by addressing the local characteristics like ridge orientation and wavelet transform addresses the noise reduction by deconstructing the image in different frequencies, reducing the noise and enhancing the ridge structure in a selected or targeted site. A combined approach provides improved overall performance. [42]

A study on "Fingerprint Enhancement Based on Wavelet and Anisotropic Filtering" addressed enhancing fingerprint images of low quality such as distorted, blurry, unclear fingerprints by combining the wavelet technique and Anisotropic filtering, the fingerprint images were broken down and made clear and smooth, removing the distortion and noise using the filter while retaining important information. Then the image was put back together. This also addressed a common problem called the block effect. The study has proven that it works well on fingerprints that are difficult to analyse by testing it using the FVC2004 database. Overall, this technique has shown promising results towards fingerprint image enhancement. [42]

5. Fusion of Multiple Techniques:

Fusing multiple techniques will enable overcoming challenges and limitations towards image enhancement by improving the image quality, clarity, and accuracy and making the model more robust and reliable. [43]

Research conducted on "Texture Feature Extraction Using Hybrid Wavelet Type I & II for Finger Knuckle Prints for Multi-algorithmic Feature Fusion" explored the uniqueness of finger knuckle prints for identification of an individual based on the texture, lines, wrinkles, and patterns displayed on the print. This adds another layer of security to the biometric system in cases where fingerprints are unavailable. To extract features from the impression efficiently without losing any important information, various orthogonal transforms are used such as Discrete Cosine Transform, Haar, Hartley, Walsh, and Kekre each serving its purpose. Combining two or more transforms together, Hybrid Wavelet Type I & II are created to aid the model with extracting and detecting sharp edges, texture, pattern, and quick computation processes with complex, image enhancements making it robust and effective in its overall performance. Finally, the features extracted are combined with the other biometric characters like fingerprints etc. for multi-algorithmic fusion improving accuracy in identification systems. [43]

6. Incorporation of Contextual Information:

Contextual filtering is applied using the surrounding information about the image, for instance in the fingerprint image enhancement, based on local characteristics like ridge orientation, spacing, and quality of the image such as noise, distortion etc., the filter is applied, focusing on the relevant feature achieving better and effective results.

7. Real-Time Processing and Computational Efficiency:
Real-time processing systems ensure quick processing time for a fingerprint to recognise and find an accurate match with the database and efficient computational work allows reduced processing work while handling large datasets without any delay using effective algorithms. This makes it very crucial for Fingerprint image recognition and matching to provide a user-friendly experience.

8. Adaptability and Robustness:
The advanced techniques and methods aim to achieve effective and efficient results in image enhancement addressing noise elimination due to various environmental conditions through adaptability and robustness ensuring accuracy and reliability.

H. Deep Learning Framework For Fingerprint Analysis
Neural Networks greatly inspired by humans' visual systems have now become the front line of deep learning models. Convolutional Neural Networks (CNNs) have become a groundbreaking improvement in Artificial Intelligence and Machine Learning. Their exceptional skill in processing visual data has transformed many industries, including computer vision, medical imaging, and natural language processing.
1. Foundation and Architecture:
The architecture of a Convolutional Neural Network (CNN) designed for visual data comprises several layers such as

- Convolutional Layers - In this layer, feature extraction occurs through small learnable filters called kernels as they can detect patterns like textures, edges, and shapes. This filter is applied to every inputted image to generate a feature map. [44]
- Pooling Layers - To make the neural network more computationally efficient and robust, the pooling layers reduce the spatial dimensions while preserving the most important features. [44]
- Fully connected Layers - They are otherwise known as dense layers. Every neuron from one layer is connected with every other neuron from the succeeding layer to gather important information. Having undergone image processing from convolutional and pooling layers, the computer produces a flattened image and turns it into a list which the fully connected layers use to arrive at a decision or prediction based on the list. This layer uses non-linear activation functions to understand complex images making the predictions more precise. [44]

2. Feature Learning and Hierarchical Structure:
One of the strengths of Convolutional Neural Networks (CNN) is its Hierarchical Feature Extraction is its ability to effectively represent data in its complex form starting by identifying the low-level features like edges, and corners and moving progressively to complex features like shapes and figures

3. Transfer Learning and Pre-Trained Models
CNN can be trained on an existing model (Pre-Trained Model) that has undergone training with large datasets and can be fine-tuned and reshaped according to the specific task or need. This benefits by reducing computational time, cost and data size with an efficiency in overall performance. [44]

4. Applications across Various Domains:
CNNs find extensive applications in computer vision, excelling in image classification, object detection, and facial recognition. In medical imaging, they assist in diagnoses, organ segmentation, and anomaly detection in medical scans. Natural language processing benefits from CNNs in text classification, sentiment analysis, and translation tasks. [44]

5. Challenges and Advancements:
While successful, CNNs face challenges like complex model interpretability, overfitting on small datasets, and vulnerability to adversarial attacks. Ongoing research focuses on addressing these issues through attention mechanisms, regularization methods, and architectural improvements for robust and explainable models. [44]

6. Deep learning in Fingerprint Analysis
The application of deep learning to fingerprint analysis has revolutionized the field by improving the accuracy and speed of biometric identification systems. Modern techniques leverage neural networks to automatically extract features, classify fingerprints, and perform matching with unprecedented precision. [45]

7. Autoencoders:

Autoencoders come under the unsupervised deep learning model and they are used often for processing fingerprint images. They contribute to fingerprint analysis in the following ways:

- Data Compression: Autoencoders reduce the dimensionality of fingerprint images, compressing them into latent representations that preserve essential features. This capability is particularly useful for efficiently storing and transmitting biometric data.
- Denoising: Denoising autoencoders remove noise from fingerprint images by learning to reconstruct clean images from noisy inputs, thereby improving overall image quality and recognition accuracy.
- Feature Extraction: In fingerprint analysis, autoencoders can learn to extract features such as minutiae points, ridge patterns, and orientation maps, facilitating better matching performance.

8. Filters in Deep Learning:

Deep learning models, particularly CNNs, utilize filters that automatically learn hierarchical features from fingerprint images: [46]

- Convolutional Layers: Filters in the convolutional layers are responsible for detecting low-level features, such as edges and ridges. As the network deepens, it learns higher-level features, including specific minutiae structures.
- Pooling Layers: These layers reduce the spatial dimensions of the data, retaining only the most salient features. This not only speeds up computation but also enhances robustness to variations in fingerprint orientation or scale.
- Fully Connected Layers: Located at the end of a CNN, these layers aggregate the learned features to perform classification or matching, allowing the system to identify or verify an individual's identity.

Fingerprint analysis has undergone significant transformations, evolving from its early use in forensic science to its integration into large-scale biometric systems like Aadhar. Modern advancements, particularly through deep learning applications, have enhanced the accuracy, efficiency, and scalability of fingerprint identification systems. However, concerns surrounding data privacy, security, and inclusivity remain critical as the technology continues to evolve.

9. Future Directions and Innovation:

The evolution of CNNs continues, aiming to enhance efficiency, interpretability, and generalization capabilities. Innovations like novel architectures, attention mechanisms, self-supervised learning, and ethical considerations drive further advancements in CNN performance and reliability. [44]

Research conducted on "Recreating Fingerprint Images by Convolutional Neural Network Autoencoder Architecture" focuses on recreating fingerprints using autoencoders, by applying CNN to extract features from the image and autoencoders to encode by compressing the image into a small set of features and reconstruct the fingerprint image from the encoding. [47]

Research conducted on "3D CNN-based fingerprint anti-spoofing through optical coherence tomography" detects false imprints using modern technologies such as optical coherence tomography - a specialised scanner with the ability to create 3D images up to the upper dermis layer of the skin and 3D CNNs are used to analyse 3D image data to identify a real image and a spoofed image. By combining them, an improved biometric system is created to detect spoofing accurately [48]

I. Deep Learning Application In Fingerprint Matching

Fingerprint has greatly increased in its speed, precision and dependability in identification in forensic investigations and biometric authentication remarkably, with the use of Deep learning applications and Convolutional Neural Networks (CNN)

Automated Feature Extraction:

CNN is very skilful in extracting features automatically by learning the complex patterns from the fingerprint image making the features extracted accurate and robust. [49]

Minutiae Detection and Classification:

These techniques make it possible to observe and match minutiae points using their algorithms. CNN architectures effectively identify minutiae like ridge endings, bifurcations, or ridge dots, ensuring precise classification and matching of fingerprint features.

Noise Reduction and Image Enhancement:

Deep learning contributes to noise reduction and image enhancement, improving the clarity of ridge

patterns in degraded or low-quality fingerprint images, resulting in more precise matching. [49]

Latent Fingerprint Analysis:

The analysis of latent fingerprints, typically partial or smudged impressions from crime scenes, benefits from CNN-based models, which enhance the quality of latent prints, thus enabling better feature extraction for identification.

Large-Scale Databases and Efficiency:

Deep learning models efficiently handle extensive fingerprint databases, reducing computational time while maintaining high accuracy rates, and enhancing scalability. [50]

Transfer Learning and Adaptability:

Transfer learning techniques adapt pre-trained models on generic datasets for specific fingerprint-matching tasks, enhancing adaptability and performance in scenarios with limited training data. [50]

Biometric Authentication and Security:

Deep learning-powered fingerprint matching systems provide robust biometric authentication, ensuring secure access control in diverse domains, from mobile devices to high-security facilities.

Advancements and Challenges:

Ongoing advancements focus on addressing challenges like domain adaptation and adversarial attacks, leveraging techniques such as domain-specific architectures and attention mechanisms to improve model robustness. [48]

Future Directions and Ethical Considerations:

Continued research aims to enhance interpretability, fairness, and ethical considerations in deep learning models for fingerprint matching, emphasizing transparency and unbiased decision-making.

In conclusion, the integration of CNNs and advanced deep-learning techniques has significantly elevated the accuracy, efficiency, and reliability of fingerprint-matching systems. This advancement paves the way for secure biometric authentication and reliable forensic analysis. Continued innovation and ethical considerations will further enhance the capabilities and ethical use of deep learning in fingerprint-matching applications.

"A Deep Learning-Based Approach to Perform Fingerprint Matching" The research proposes a Vision Transformer (ViT) based Siamese network framework for fingerprint matching in authentication systems, demonstrating significant performance improvements using deep learning approaches. [48]

"Handling Data Scarcity Through Data Augmentation in Training of Deep Neural Networks for 3D Data Processing" This work explores data augmentation techniques for 3D point cloud representation, verifying their effectiveness in retaining information and maintaining characteristics and features within augmented sub-samples. [49]

Research on fingerprint matching and 3D data processing highlights the prospect of deep learning techniques showing their accuracy and reliability in various fields

III. CONCLUSION

The evolution of fingerprint analysis from early observations to modern advancements with deep learning models highlights the importance of forensic science. Historical milestones laid the groundwork for the development of robust Automated Fingerprint Recognition Systems (AFRS), which have transformed criminal investigations. Despite challenges such as noise and poor image quality, technological advancements, particularly in image processing and machine learning, have significantly improved the accuracy and efficiency of fingerprint analysis. The incorporation of Convolutional Neural Networks (CNNs) and Generative Adversarial Networks (GANs) has enhanced image enhancement and fingerprint matching processes, leading to more reliable forensic investigations and secure biometric authentication systems. Future research will continue to address existing challenges and explore new frontiers in fingerprint analysis, ensuring its critical role in maintaining justice and security.

IV. FUNDING

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

V. CLINICAL TRIAL NUMBER

Clinical trial number: not applicable.

VI. ABBREVIATIONS

AFRS - Automated Fingerprint Recognition Systems
CNN - Convolutional Neural Network
GANS - Generative Adversarial Network
FVC - Fingerprint Verification Competition
UDI - Unique Identification Number
SSIM - Structural Similar Index Metric
UQI - Universal Quality Index
OTP - One-Time Password
SSL - Secure Sockets Layer
UIDAI - Unique Identification Authority of India
DPDP - Digital Personal Data Protection
PSNR - Peak Signal-to-Noise Ratio
DMF - Directional Median Filtering
ViT - Vision Transformer

REFERENCES

[1] D. E. Newton, DNA Evidence and Forensic Science. New York, NY, USA: Infobase Publishing, 2008.

[2] G. Tredoux, "Henry Faulds: The invention of a fingerprinter." [Online]. Available: https://galton.org/fingerprints/faulds.htm.

[3] C. R. Lawrence, "Francis Galton (1822–1911)," The Embryo Project Encyclopedia, Apr. 6, 2011. [Online]. Available: https://hdl.handle.net/10776/1800.

[4] K. R. Moses, P. Higgins, M. McCabe, S. Prabhakar, and S. Swann, Automated Fingerprint. [Online]. Available: https://www.ojp.gov/pgffiles1/nij/225326.pdf.

[5] S. Saponara, A. Elhanashi, and Q. Zheng, "Recreating fingerprint images by convolutional neural network autoencoder architecture," IEEE Access, pp. 1–1, 2021, doi: 10.1109/ACCESS.2021.3124746.

[6] H. M. Daluz, Fundamentals of Fingerprint Analysis. Boca Raton, FL, USA: CRC Press, 2018.

[7] C. M. Brislawn, "Fingerprints go digital," Notices of the American Mathematical Society, vol. 42, no. 11, pp. 1278–1283, Nov. 1995.

[8] T. Sharma, S. M. Chaitan, N. S. Somayaji, B. Mahajan, J. P. Rajguru, S. Hajibabaei, and S. Hegde, "The medicolegal importance of establishing human identity by using dactyloscopy and rugoscopy: A comparative study," Journal of Family Medicine and Primary Care, vol. 9, no. 7, pp. 3236–3241, 2020, doi: 10.4103/jfmpc.jfmpc_545_20.

[9] R. Ferreira, R. Paula, A. Okuma, and L. Costa, "Fingerprint development techniques: A review," Revista Virtual de Química, vol. 13, 2021, doi: 10.21577/1984-6835.20210083.

[10] K. R. Moses, P. Higgins, M. McCabe, S. Prabhakar, and S. Swann, "Automated fingerprint identification system (AFIS)," 2015.

[11] N. A. Alam, M. Ahsan, M. A. Based, J. Haider, and M. Kowalski, "An intelligent system for automatic fingerprint identification using feature fusion by Gabor filter and deep learning," Computers and Electrical Engineering, vol. 95, Art. no. 107387, Oct. 2021, doi: 10.1016/j.compeleceng.2021.107387.

[12] R. K. Garg and H. Kumari, "A new technique for visualization of latent fingerprints on various surfaces using powder from turmeric: A rhizomatous herbaceous plant," Egyptian Journal of Forensic Sciences, vol. 1, 2011, doi: 10.1016/j.ejfs.2011.04.011.

[13] Jain and J. Feng, "Latent fingerprint matching," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 33, no. 1, pp. 88–100, 2011, doi: 10.1109/TPAMI.2010.59.

[14] O. Zanganesh, S. Bala, and N. Bhattacharjee, "Partial fingerprint matching through region-based similarity," in Proc. 2014 International Conference on Digital Image Computing: Techniques and Applications (DICTA), 2014, doi: 10.1109/DICTA.2014.7008121.

[15] Unique Identification Authority of India, "About your Aadhaar." [Online]. Available: https://uidai.gov.in/en/my-aadhaar/about-your-aadhaar.html.

[16] C. Barnes and J. Conten, "Chapter history," National Institute of Justice, NCJ No. 225321, Jun. 2021. [Online]. Available: https://www.ojp.gov/pdffiles1/nij/225321.pdf.

[17] Unique Identification Authority of India, "Biometric devices." [Online]. Available: https://uidai.gov.in/en/ecosystem/authentication-devices-documents/biometric-devices.html.

[18] Unique Identification Authority of India, "Operation model." [Online]. Available: https://uidai.gov.in/en/ecosystem/authentication-ecosystem/operation-model.html.

[19] Unique Identification Authority of India, "Security in UIDAI system." [Online]. Available: https://uidai.gov.in/en/my-aadhaar/about-your-aadhaar/security-in-uidai-system.html.

[20] P. Dixon, "A failure to 'do no harm': India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.," Health and Technology, vol. 7, no. 4, pp. 539–567, 2017, doi: 10.1007/s12553-017-0202-6.

[21] T. Devi, "Biometric data, identification and authentication in India: Legal framework, challenges and impact," International Journal of Law Management & Humanities, vol. 4, no. 3, pp. 1001–1036, 2021, doi: 10.10000/IJLMH.11561.

[22] N. Sarfraz, "Adermatoglyphia: Barriers to biometric identification and the need for a standardized alternative," Cureus, vol. 11, no. 2, Art. no. e4040, 2019, doi: 10.7759/cureus.4040.

[23] EGIPMR, "The Gazette of India Extraordinary," pt. II, 2016. [Online]. Available: [URL not provided]. [Accessed: Oct. 16, 2024].

[24] LARRDIS, Lok Sabha Secretariat, Right to Privacy: Members' Reference Service. New Delhi, India: Lok Sabha Secretariat. [Online]. Available: https://loksabhadocs.nic.in/Refinput/New_Reference_Notes/English/Right%20to%20Priva.

[25] Ministry of Electronics and Information Technology, Government of India, Digital Personal Data Protection Act, 2023. [Online]. Available: https://www.meity.gov.in/writeraddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.p.

[26] Hamid, M. Rahim, A. Almazyad, and T. Saba, "Analysis of proposed noise detection and removal technique in degraded fingerprint images," 3D Research, vol. 6, 2015, doi: 10.1007/s13319-015-0067-2.

[27] Wu, Z. Shi, and V. Govindaraju, "Fingerprint image enhancement method using directional median filter," in Proc. SPIE—The International Society for Optical Engineering, 2004, doi: 10.1117/12.542200.

[28] S. Xie, J. Yang, D. Park, S. Yoon, and J. Shin, "Fingerprint quality analysis and estimation approach for fingerprint matching," 2011, doi: 10.5772/20474.

[29] G. Yadav, D. K. Yadav, and P. C. Mouli, "Statistical measures for palmprint image enhancement," in Machine Learning for Biometrics, pp. 65–85. Academic Press, 2022.

[30] S. Shreya and K. Chatterjee, "GAN-enabled latent fingerprint enhancement model for human identification system," Multimedia Tools and Applications, vol. 83, no. 9, pp. 27565–27588, 2024.

[31] H. Wang, R. Ke, and X. Jiang, "Large-region image inpainting using adaptive Fourier neural network and space-frequency domain structural analysis," Journal of Intelligent & Fuzzy Systems, pp. 1–5.

[32] J. Yang, L. Liu, T. Jiang, and Y. Fan, "A modified Gabor filter design method for fingerprint image enhancement," Pattern Recognition Letters, vol. 24, pp. 1805–1817, 2003, doi: 10.1016/S0167-8655(03)00005-9.

[33] K. Liu, J. Li, and S. S. Bukhari, "Overview of image inpainting and forensic technology," Security and Communication Networks, vol. 2022, Art. no. 9291971, 2022.

[34] Y. He, J. Tian, X. Xiping, and T. Zhang, "Image enhancement and minutiae matching in fingerprint verification," Pattern Recognition Letters, vol. 24, pp. 1349–1360, 2003, doi: 10.1016/S0167-8655(02)00376-8.

[35] L. Hong, Y. Wan, and A. K. Jain, "Fingerprint image enhancement: Algorithm and performance evaluation," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, pp. 777–789, 1998, doi: 10.1109/34.709565.

[36] M. Kočevar, B. Kotnik, A. Chowdhury, and Z. Kacic, "Real-time fingerprint image enhancement with a two-stage algorithm and block-local normalization," Journal of Real-Time Image Processing, vol. 13, 2014, doi: 10.1007/s11554-014-0440-z.

[37] T. L. Chang, "Texture analysis of digitized fingerprints for singularity detection," NATO Conference Series, Series 4: Marine Science, vol. 1, pp. 478–480, 1980.

[38] N. Pradeep, "A revolutionary fingerprint authentication approach using Gabor filters for feature extraction and deep learning classification using convolutional neural networks," 2022, doi: 10.1007/978-981-16-8512-5_38.

[39] S. Shreya and K. Chatterjee, "GAN-enabled latent fingerprint enhancement model for human identification system," Multimedia Tools and Applications, pp. 1–24, 2023, doi: 10.1007/s11042-023-16510-7.

[40] K. Yang and K. Lai, "NaturalFinger: Generating natural fingerprint with generative adversarial networks," 2023.

[41] M. Agagu, "Development of an improved multi-filtering matching model for fingerprint recognition," Journal of Image Processing and Intelligent Remote Sensing, pp. 24–38, 2023, doi: 10.55529/jipirs.35.24.38.

[42] J. Jialei, Q. Mupeng, X. Xingeyou, H. Hatemjabbar, and P. Wang, "Fingerprint enhancement based on wavelet and anisotropic filtering," International Journal of Pattern Recognition and Artificial Intelligence, vol. 26, 2012, doi: 10.1142/S0218001412560010.

[43] V. Yadov, V. Bharadi, and S. Yadav, "Texture feature extraction using hybrid wavelet type I and II for fingerprint knuckle prints for multi-algorithmic feature fusion," Procedia Computer Science, vol. 79, pp. 359–366, 2016, doi: 10.1016/j.procs.2016.03.047.

[44] Ravikumar and H. Sriraman, "Understanding convolutional neural network with TensorFlow: CNN," 2023, doi: 10.4018/978-1-6684-8531-6.ch003.

[45] H. Chiroma, "Deep learning algorithms-based fingerprint authentication: Systematic literature review," Journal of Artificial Intelligence and Systems, vol. 3, pp. 157–197, 2021, doi: 10.33969/AIS.2021.31010.

[46] J. Jin, "Convolutional neural networks for biometrics applications," SHS Web of Conferences, vol. 144, Art. no. 03013, 2022, doi: 10.1051/shsconf/202214403013.

[47] S. Saponara, A. Elhanashi, and Q. Zheng, "Recreating fingerprint images by convolutional neural network autoencoder architecture," IEEE Access, pp. 1–1, 2021, doi: 10.1109/ACCESS.2021.3124746.

[48] Y. Zhang, S. Yu, S. Pu, Y. Wang, K. Wang, H. Sun, and H. Wang, "3D CNN-based fingerprint anti-spoofing through optical coherence tomography," Heliyon, vol. 9, Art. no. e20052, 2023, doi: 10.1016/j.heliyon. 2023.e20052.

[49] V. Baghel, S. Patel, S. Prakash, and A. Srivastava, "A deep learning-based approach to perform fingerprint matching," 2023, doi: 10.1007/978-3-031-22018-0_22.

[50] Srivastava, P. Rotte, A. Jain, and S. Prakash, "Handling data scarcity through data augmentation in training of deep neural network for 3D data processing," International Journal on Semantic Web and Information Systems, vol. 18, pp. 1–16, 2022, doi: 10.4018/IJWIS.297038.