International Journal of Computing and Digital Systems
2025, VOL. 17, NO. 1, 1–17

http://dx.doi.org/10.12785/ijcds/1571022983

A Survey Of Fingerprint Identification System Using Deep Learning

Hussein G. Muhammad[1] **and Zainab A. Khalaf**[1*]

[1]*Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq*
Received 22 April 2024, Revised 24 September 2024, Accepted 28 September 2024

Abstract: The growing need for security in different areas of human life has made biometric technologies essential for reliable identification and authentication. Among these technologies, fingerprint identification is one of the most widely used because it relies on unique patterns specific to each individual. However, traditional fingerprint identification systems face several challenges, such as handling poor-quality images, environmental variability, and vulnerability to spoofing attacks. Recently, many efficient methods have emerged, particularly those utilizing deep learning, which have made solving the problems of traditional methods easier and more effective. This progress has greatly improved fingerprint identification systems in several important ways. It has increased the accuracy of identification, reduced the time needed for processing, and enhanced the systems' ability to prevent spoofing. These innovative approaches have enabled significant advancements in image enhancement, feature extraction, and classification accuracy, effectively addressing critical gaps in traditional systems. This survey seeks to address these gaps by providing an extensive overview of state-of-the-art methodologies used in fingerprint identification systems, with a particular focus on deep learning techniques. The current study also examines various aspects of fingerprint identification, including its applications in secure digital transactions, healthcare systems, and smart city initiatives, as well as the ethical considerations, datasets, and challenges associated with its implementation. It highlights gaps identified in previous studies and offers a thorough review of the latest methods and technologies in the field. By identifying recent trends and advancements, this study provides valuable insights that can guide future researchers in developing more effective and responsible fingerprint identification systems.

Keywords: Fingerprint Identification, Deep learning, Biometric, Spoofing, Survey

1. Introduction

The fast-paced lifestyle and widespread development in all areas of life, especially information technology, have increased the demand for new technologies to determine personal identification in a more secure, reliable and trustworthy way. Traditional technologies used for personal identification, such as symbols or knowledge, need help with many challenges. For example, using an ID card and a passport can be considered a completely insecure traditional method because they can be easily forged, copied, or lost [1]. Given the importance of developing biometric identification systems, deep learning capabilities have been utilized to address the defects of traditional methods. The high ability of deep learning methods to extract accurate, unique, reliable, and personal characteristics is used for individual identification. By adopting the distinctive and unique characteristics of the individuals, these systems provide flexible and highly effective identification solutions that meet increasing security requirements [2].

The significance of using biometric systems in many countries lies in the ability of these systems to accurately identify individuals in many applications, such as voter registration, border control, law enforcement, criminal investigations, and citizen management. These biometric systems provide a robust and reliable authentication mechanism, unlike traditional identification technologies that rely on passwords and access cards, reducing the possibility of identity theft and lost credentials. Various biometric identifiers, including retinal checks, algebra of the hand, facial features, vocal patterns, and digital fingerprints, contribute to the richness of biometric identification [3], [4].

Due to the uniqueness of each person's fingerprint, fingerprint identification has become vital because of its proven effectiveness for identity verification. These distinctive features differ from person to person and cannot be the same for two individuals. Extracting these distinct features when using fingerprint identification systems requires a stringent process to extract these distinctive fingerprint

E-mail address: pgs.hussein.muhammad@uobasrah.edu.iq, zainab.khalaf@uobasrah.edu.iq

individual features. The concerned person will be identified based on the matching percentage between the features extracted from the concerned person's fingerprints and the ones stored in the database. For these reasons, fingerprint identification systems provide a secure and reliable biometric solution. As a result of this importance, these systems are widely used in many applications of human life, including security and financial fields. Fingerprint identification systems are a robust and reliable means of personal identification, even with issues related to privacy and environmental factors [5],[6].

Fingerprint identification, characterized by unique and permanent patterns of friction ridges, has become a cornerstone in the field of biometrics. These intricate ridge patterns, formed by curved lines on the skin surface, provide a reliable method of individual identification due to their distinctiveness. As illustrated in Figure 1, fingerprint patterns consist of dark ridges and white valleys, highlighting the complexity of their structure. However, capturing high-quality fingerprint images remains a challenge, often affected by environmental conditions and user-related factors. To address these challenges, advanced image enhancement techniques are frequently employed, ensuring accurate and reliable identification in various scenarios [7], [8].

Figure 1. The types of fingerprints patterns
Level one (Arrow), Level two (Line), Level three (Circle).

There are three levels of fingerprint identification, as shown in Figure 1. The main focus of Level 1 is on the general ridge flow and overall fingerprint pattern types, such as loops, and arches, whereas Level 2 concentrates on fine-grained aspects, such as precise ridge placements. Level 3 includes a comprehensive set of dimensional attributes, such as shape, width, deviation of the edge route, and additional permanent features. The statistical research indicates that Level 1 traits, which display global fingerprint trends, are not unique, whereas Level 2 features have enough discriminative power to identify individual fingerprints. Level 3 attributes encompass detailed structural characteristics that are fundamentally unique, enduring, and immutable [9], [10], [11], [12].

The current study aims to thoroughly examine how fingerprint biometric identification technologies contribute to improved security measures and identity individual validation. Various biometric traits and the difficulties faced by recognition systems will be covered, with specific attention to issues with sensitivity of data acquisition, privacy concerns, and ethical issues. The developments and challenges unique to fingerprint identification using deep learning will be the focus. Besides, this study offers a comprehensive view of recent studies to identify research gaps. As well as this study provides future directions that pave the way for the development of more flexible and efficient biometric identification systems.

The main objectives of this survey can be summarized as follows:

- Highlights how deep learning methods have been applied to enhance fingerprint recognition systems.
- Discusses improvements in the accuracy and efficiency of fingerprint identification due to deep learning approaches.
- Compares the performance of deep learning-based methods with traditional fingerprint recognition techniques.
- Identifies current challenges and limitations of applying deep learning in this field.
- Suggests potential future research directions and areas where deep learning could further advance fingerprint identification.

The structure of this paper is as follows. First, from sections 2 to 5, the anatomy, functions, uniqueness, and applications of the fingerprint are discussed. Section 6 presents the most significant related works. Challenges and gaps are also presented in Section 7. Sections 8 through 9 discuss fingerprint identification algorithms and datasets, and Section 10 describes the evaluation techniques. Section 11 presents issues related to applied ethics. Lastly, a discussion of the findings and their implications can be found in the remaining sections.

2. Fingerprint Anatomy

The human fingerprint is a remarkable biometric identifier characterized by intricate ridge patterns and specific minutiae points. The human fingerprint is complex, and the skin's surface has a distinct pattern of ridges and furrows, as shown in Figure 2. Each ridge pattern contains various details, including ridge endings, bifurcations, and short ridges,

known as ridge characteristics or minutiae points. Forensic scientists and fingerprint identification devices primarily use these minor details of features to identify individuals.

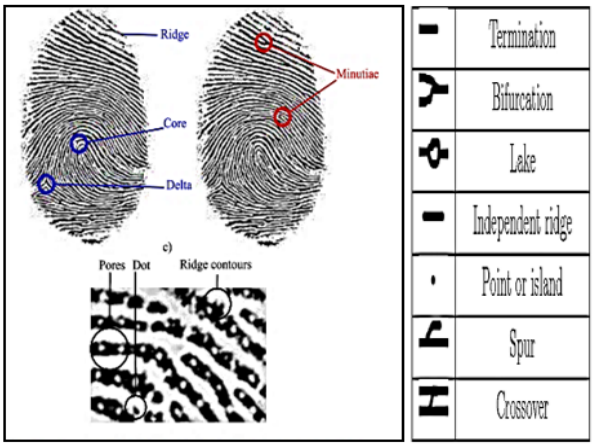

Figure 2. The anatomy of human fingerprints.

The anatomy of human fingerprints consists of the following elements:

A. *Ridge Patterns*

The surface of a fingerprint is characterized by raised, curving ridges and recessed furrows. These ridges create a distinctive pattern that varies from person to person [13].

B. *Minutiae Points*

Minutiae are the precise details within the ridge patterns [14]. They include the following key features:

- Ridge Endings: These happen when a slope abruptly ends.
- Bifurcations: Divisions are points where an individual ridge divides into two distinct ridges.
- Enclosures (or Lakes): A ridge that forms a closed loop, creating an enclosed area.
- Dot (or island): A dot is a tiny, isolated ridge that does not connect to nearby ridges.

C. *Core*

In many fingerprint patterns, the core can be identified as a central point where the ridges flow in circular or spiral patterns [15].

D. *Delta*

A delta is a location where three ridges converge at or close to the center of a ridge pattern [16].

3. Fingerprint Uniqueness

Fingerprint uniqueness is a fundamental characteristic of fingerprints. The pattern and minutiae points in each person's fingerprints are distinctive and won't alter over time. Figure 3 illustrates the concept of fingerprint uniqueness. This uniqueness is the basis for fingerprint identification and has been a cornerstone of forensic science. Fingerprint patterns are unique to each individual, including identical twins. This level of uniqueness made fingerprints invaluable for personal identification and forensic investigations [17].

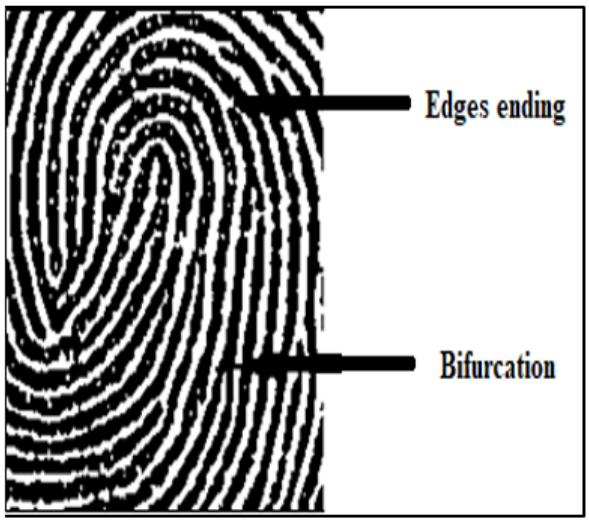

Figure 3. Simplified Fingerprint Uniqueness.

As shown in Figure 3, the ridge patterns form unique, intricate designs on the fingerprint's surface. Minutiae points include ridge endings and bifurcations. Each fingerprint has its own set of minutiae points, as illustrated in Figure 4. The arrangement and position of these points contribute to distinguishing the fingerprint. This uniqueness, combined with the permanence of those features, forms the basis for identifying fingerprints and recognition systems [18].

Figure 4. An example of the uniqueness of fingerprints.

4. Functions of Fingerprint

Biometrics, which authenticates individuals based on physical and unique characteristics, are essential in many applications. These applications range from securing digital devices to ensuring border security and supporting criminal investigations. These applications can be divided into specialized areas, each contributing significantly to the protection and efficiency of the systems in which they are employed [19].

Among these biometric technologies, multidimensional fingerprint identification systems stand out because of their central role. They ensure high accuracy and reliability in identifying individuals, often defeating human evidence. The accuracy and stability of these systems are critical in emphasizing the detection and support of inspection processes, thus increasing the reliability and effectiveness of security measures [20].

The specialized functions of biometrics include the following:

A. *Authentication:*

Biometrics are widely used for authentication, where an individual's identity is confirmed based on biometric data. This process typically consists of a one-to-one comparison that contrasts biometric information with stored systems that allow or deny access [21]. For example, using a fingerprint scan to unlock a smartphone is an authentication function.

B. *Verification:*

Biometric verification uses biometric data to authenticate an individual. This process ensures that identifying an individual is accurately verified based on their unique biometric characteristics. This function typically involves comparing a given biometric sample with a single sample associated with the individual. This type is commonly used in situations such as bank account access or fingerprint confirmation of identity in airport border control [22].

C. *Identification:*

In this case, biometrics is a more general function that involves identifying a person's identity by comparing its biometric details to a database containing multiple stored templates. This function is handy in border control and law enforcement. By comparing biometric data with existing datasets, officials can quickly and accurately identify individuals, identify potential risks, and prevent illegal activities. Multidimensional fingerprint identification systems help in that process, providing reliable indicators that support national security and public safety programs [23].

D. *Recognition:*

Recognition is another function of biometrics. It encompasses the broader scope of identifying or recognizing an individual based on their biometric data, such as facial recognition in surveillance systems. Recognition can involve matching against a big database of individuals to determine a match or recognize a person's face, voice, or other biometric characteristics in real time [24].

Each function serves distinct purposes within the domain of biometric technology. Figure 5 shows the biometric functions.

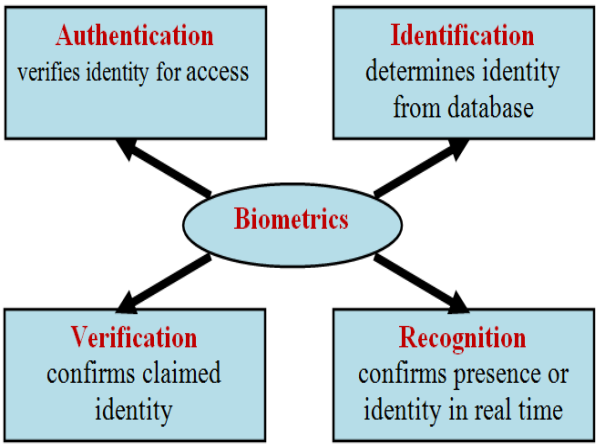

Figure 5. Functions of Biometrics.

5. Fingerprint Applications

Biometrics combines technology and identity verification, using unique physical or psychological traits to identify individuals accurately. Fingerprint identification, a prominent biometric method, relies on distinct ridge patterns and minutiae points of fingerprints. Below are applications that showcase the versatility and effectiveness of fingerprint identification across different domains.

A. *Access Control:*

Fingerprint recognition is commonly used for secure access to restricted areas, buildings, and electronic devices, providing a reliable and convenient method to verify individuals and prevent unauthorized access [25].

B. *Mobile Device Security:*

Fingerprint identification is crucial in mobile device protection which provides a secure and user-friendly means to unlock smartphones, access applications, and conduct safe transactions. This biometric feature has become a standard security measure in modern mobile devices [26].

C. *Financial Transactions:*

Fingerprint identification is used in the banking industry to improve the security of transactions, particularly in online banking and electronic payments. Users can safely access their financial information and authorize deals using fingerprint authentication [27].

D. *Government Services:*

Government agencies utilize fingerprint identification for identity verification in various services, including issuing passports, driver's licenses, and national identification

cards. Fingerprint biometrics ensures the accuracy and authenticity of individuals' identities [28].

E. Border Management and Migration:

Fingerprint identification is crucial for border regulation and entry processes. It enhances security at international borders by verifying travelers' identities and prevents identity fraud and unauthorized entry [29].

F. Criminal Investigations:

Law enforcement agencies leverage fingerprint identification in criminal investigations to match fingerprints found at crime scenes with those in criminal databases. This helps identify and apprehend suspects, contributing to the resolution of criminal cases [30].

G. Time and Attendance Management:

Fingerprint identification systems are widely used for time and attendance management in corporate settings. Employees use their fingerprints to clock in and out, ensuring accurate and secure attendance records while minimizing time fraud [31].

H. Healthcare Access and Patient Identification:

In healthcare, fingerprint identification enhances access control to medical records, medications, and restricted areas within healthcare facilities. It contributes to accurate patient identification and improves the security of sensitive healthcare information [32].

I. Educational Institutions:

Educational institutions deploy fingerprint identification for various purposes, including secure campus access, attendance tracking, and exam verification. This technology ensures the integrity of academic processes by accurately verifying the identities of students and staff [33].

J. Smart Home Security:

Fingerprint identification is integrated into smart home security systems, allowing residents to securely access their homes, control smart devices, and monitor security. This application enhances the overall security and convenience of smart home environments [34].

The FBI's Next Generation Identification (NGI) system is one of the most advanced fingerprint identification systems available today. It was developed to improve biometric identification services by using modern fingerprint recognition techniques that are powered by deep learning algorithms. The NGI system replaces the older Integrated Automated Fingerprint Identification System (IAFIS), which was used by the FBI for many years. By utilizing these new technologies, the NGI system enhances the accuracy and efficiency of fingerprint identification, giving law enforcement agencies better tools for solving crimes and ensuring public safety. Figure 6 (A and B) shows the Integrated Automated Fingerprint Identification System (IAFIS) [35].

[A]

[B]

Figure 6. Automated Fingerprint Identification System (IAFIS).

6. Related Works

In recent years, researchers have tried to use multiple methods in the field of deep learning to obtain high accuracy in fingerprint identification. A group of studies were selected according to their relevance to the subject of the study, as they included deep learning techniques and specialized in relying on fingerprints without other biometrics. In-depth investigation and analysis were conducted regarding fingerprint identification. Some studies are classified into four groups based on their data preparation and improvement as follows:

A. Improving Data Quality

These studies concentrate on enhancing the quality of fingerprint data by utilizing methods like edge enhancement, noise reduction, and pore recognition.

Deshpande et al. [36] designed the Combination of Nearest Neighbor Arrangement Indexing (CNNAI) as a local matching model based on CNN granularity for fingerprint identification. This model creates feature vectors

unaffected by rotation or scale using detailed close features. A hash index was employed to decrease the overall number of retrievals. Matching between the FVC2004 and NIST SD27 latent fingerprint datasets resulted in an identification rate of 80% for the FVC2004 fingerprints and 84.5%

Al-Wajih et al. [37] used deep learning techniques to develop a method to classify fingerprint types. Researchers used a meta-neural network to analyze fingerprints and predict their types. NIST and SOCOFing are two public datasets utilized for training and evaluating the proposed model. The proposed model showed high verification accuracy with both datasets, achieving 90% and 89% accuracy for fingerprint types.

Oladele et al. [38] developed a deep learning method to classify gender based on fingerprints for each of the five types of fingers. They utilized a CNN to train the model, which was then evaluated using fingerprint sample images from 20 individuals representing the five finger types. The overall accuracy achieved was 72%.

Li et al. [39] introduced a streamlined image-processing method based on the Siamese neural network. They also presented an identification method for identifying images from any source without requiring a pre-stored dataset. The proposed approach was applied explicitly to fingerprint identification and evaluation. The outcomes indicated that this method achieved a 92% accuracy rate with an F1 score of 87%.

Jacob et al. [40] proposed a method for using CNNs to study binary sex identification of African fingerprints. They compared four models: VGG 19, VGG 16, InceptionV3, and ResNet-50. The main focus was on improving the performance of traditional deep models by addressing issues of limited available data. Data preprocessing techniques such as rotation, zoom, and reflection were also used to prepare the data. Transfer learning was employed to pre-train various models to expedite the training process and assess the models. Training loss criteria and accuracy were used to evaluate the trained models. VGG 19 achieved the highest accuracy of 71.9%, followed by VGG 16 at 72.3%, InceptionV3 at 67.3%, and ResNet-50 at 60.8%.

Spanier et al. [41] conducted a study on gender classification using various datasets and considering changes in the quality of fingerprint images. Their findings revealed that a used CNN, specifically VGG 19, was influential, achieving an accuracy range of 70% to 84% depending on the fingerprint quality. They also found that Data Concentrate AI (DCAI) methods led to a significant 1-4% improvement. Importantly, for partial or poor-quality fingerprints, the outer areas of the fingerprint became an essential factor in determining gender categorization.

Martins et al. [42] proposed a real-time approach for reducing manual identification in crime scene investigations, which consumes both time and human resources. The proposed method has four steps. First, it preprocesses the image using directed Gabor filters. Next, it creates a model to capture fine details. This model uses polygons to represent these details, including neighboring features. In a random sample of 125 images from the FVC2000 DB1 dataset, the maximum relative and absolute errors between edge lengths, angles between adjacent vertices, and reference details were FMR 0.06%.

B. Data Augmentation

This category includes studies that employ data augmentation methods, such as geometric transformations, color modification, and artificial noise, to boost model performance by diversifying the dataset.

Praseetha et al. [22] conducted a study to authenticate fingerprints, where the initial stage involved filtering out bad-quality fingerprints, followed by verifying the remaining fingerprints. A prototype was used to discard poor-quality fingerprints. If the prototype generates a good fingerprint, it is sent to a verification unit for fingerprint matching. This study improved the accuracy of around 90-95% by combining a comprehensive CNN pre-filter with a highly refined fingerprint verification algorithm.

Liu et al. [43] proposed a new method to identify pores with high accuracy for identification. This method primarily addresses the issue of pore clarification through state-of-the-art direct pore matching technology. Deep convolutional networks were carefully constructed for each sweat pore's Deep Pore ID (DeepPoreID) on fingerprints, taking advantage of their diversity and abundance. Experiments conducted on two public fingerprint datasets of excellent quality demonstrated the effectiveness of the proposed DeepPoreID, especially when matching fingerprints to small image sizes. An increase in accuracy of about 30% was achieved in the FMR1000.

Chhablani et al. [44] suggested using deep neural networks to learn about superpixel interactions to enhance model performance. This objective was achieved by building a hybrid Graphical Neural Network (GNN) and CNN. GNN is used to handle the relative information about the image's superpixels. In contrast, CNN is utilized to extract spatial information from images. Extensive tests on different datasets evaluated the performance of the hybrid model. The study demonstrates that the performance of a regular CNN system can be improved by utilizing superpixel relative information processed by GNN, achieving an accuracy of 93.58%.

Jeong et al. [45] suggested advancing fingerprint recognition technology for smart door locks, incorporating additional features like Bluetooth connectivity and fingerprint recognition. They utilized a CNN model to identify features and verify fingerprint matches. The accuracy of the results on the SOCOFing dataset was an impressive 95.93%.

Murshed et al. [46] developed a deep learning-based

method to generate box boundaries with arbitrary angles. This method accurately identifies fingerprints from axially in-line and hyper-rotated images. They introduced a fingerprint hashing model called the Clarkson Rotated Fingerprint Segmentation Model (CRFSEG). This model is based on the conventional Faster R-CNN architecture. The CRFSEG was trained on a new dataset. Results showed that the model remained stable across different age groups. It also effectively handled over-rotated slap images. The CRFSEG model achieved a matching accuracy of 97.17%.

Suwarno [47] proposed a new method for generating features that does not require preprocessing and combines wavelet decomposition with maximum pooling. The fingerprint image was first analyzed using a 4-level Haar wavelet, followed by a 2x2 filter for maximum pooling. The resulting feature was then used to train the Multilayer Perceptron (MLP) network. The proposed method was trained using the NIST dataset, which included 750 fingerprints, 375 of which were male and 375 of which were female. This method achieves an overall accuracy of 80.1%.

C. Techniques for Filtering and Normalization

This group focuses on studies that remove noise from data and normalize values using filtering and normalization techniques, which enhances model performance.

Chowdhury et al. [48] proposed creating and teaching a patch-based Siamese CNN. This network does not rely on exact point extraction from the beginning. Instead, it aims to learn which features work best for matching fingerprint images. The features learned by this network are examined using Gradient Weighted Class Activation Mapping (Grad-CAM). This analysis checks if the features are linked to specific point locations on the fingerprints. Experiments show that the proposed system learns to focus on important details when matching fingerprints. Accuracies were obtained with the two datasets, CASIA and FVC2000, 89% and 93%, respectively.

Zhu et al. [49] proposed a new method for simulating latent fingerprint optimization using a GAN framework called FingerGAN. It can make the generated fingerprint indistinguishable from its corresponding real-world example fingerprint skeleton related to precise locations and a structured orientation field. Fine details can be extracted directly from a fingerprint skeleton map, and a comprehensive framework for performing latent fingerprint optimizations has been presented. The testing was applied using the NIST SD14 unseen fingerprint dataset that achieved 76.36 accuracy.

Shabrina et al. [50] suggested a novel fingerprint verification method based on deep learning for small-area sensors. A systematic approach combines a Deep Convolutional Neural Network (DCNN) in a Siamese Network for feature extraction and eXtreme Gradient Boosting (XGBoost) for fingerprint similarity training. In addition, a padding technique was introduced to prevent the wraparound error problem. According to the experimental results, the method outperforms the existing methods in the FingerPassDB7 and FVC2006DB1B datasets by 66.6% and 22.6%, respectively.

D. Fingerprint Spoofing

Fingerprint spoofing involves using fake fingerprints to deceive biometric systems, posing significant security risks. Recent studies have explored various spoofing techniques, demonstrating that materials like gelatin and silicone can effectively replicate real fingerprints. This section reviews research focused on methods for detecting and preventing fingerprint spoofing.

Giudice et al. [51] focused on detecting modified fingerprints and identifying the types of changes applied. The main objective was to develop effective techniques to identify and detect fingerprint alterations using deep neural networks. It also aimed to determine gender, hand, and finger information. The Inceptionv3 architecture was used to achieve these goals. Activation maps were included to show which areas the neural network focused on to detect modifications. The method achieved an accuracy of 92.52% for gender identification and 92.18% using the SOCOFing dataset.

Goel et al. [52] developed a CNN-based patch method for segmented accordance estimation. This method trains the network to identify and learn the patterns around shared fingerprint regions. Testing showed that it could predict a cut line with an equal error rate of 5.44. It performed better than several traditional handcrafted features used for detecting multiple identities in fingerprints.

Özkiper et al. [53] developed a fingerprint liveness detection method using the LivDet2015 dataset. It applied Support Vector Machine (SVM) and Convolutional Neural Networks (CNN) as classification methods. The performance of both approaches was compared, with a detailed analysis of the CNN method. Preprocessing steps, such as edge enhancement, transformation, and feature extraction, were used on the images before SVM classification. The SVM method achieved an accuracy of 90%.

Zhang et al. [54] This research proposed a lightweight fingerprint liveness detection network to differentiate between fake and real fingerprints. The approach included foreground extraction, fingerprint image occlusion, pattern transfer, and an enhanced ResNet with a multi-head self-attention mechanism. The network was also used to create fake fingerprints from unknown materials, improving the model's generalization ability. Experiments conducted on the LivDet2011, LivDet2013, and LivDet2015 datasets showed that the proposed method achieved promising results.

Table I summarizes the main areas and studies discussed in the above subsections.

TABLE I: Summary of previous studies.

Seq.	Ref.	Year	Algorithm	Datasets	Contributions	Performance Metrics
1.	[51]	2020	Inception-v3	SOCOFing	The research proposed a method for detecting altered fingerprints using a deep neural network with the Inception-v3 architecture. It identified alteration types and recognized gender, hand, and fingers while generating activation maps to indicate areas affected by alterations.	Accuracy = 92.52%
2.	[22]	2020	Inception-v3	ImageNet	A new methodology for improving security and accuracy, where a secure fingerprint verification platform was developed.	Accuracy = 94%
3.	[36]	2020	CNN	FVC2004, NIST SD27	The study proposed a CNN-based fingerprint matching model using local minutiae features with rotation and scale invariance. Hash indexing was applied to improve retrieval efficiency, and a residual learning-based CNN enhanced feature extraction.	Accuracy = 80%, 84.5%
4.	[48]	2020	CNN	CASIA, FVC-2000	Automatically learning fingerprint characteristics near the precise points of the matching process was demonstrated, and two different visual analyses were used to match fingerprints based on the presence of specific points.	Accuracy = 89%, 93%
5.	[52]	2020	AlexNet	FVC2002	A dataset of fake double fingerprints was developed and made publicly available, in addition to proposing deep learning-based preventive measures to detect them.	EER = 5.44
6.	[43]	2020	CNN	PolyU DBI, DBII	The effectiveness of a new description was demonstrated that takes into account the differences between classes and the similarity within classes in porous points, allowing the fingerprint to be linked to a small overlapping region and finding precise matches in porous points.	35% increase in EER
7.	[37]	2022	CNN, GNN	NIST, SOCOFing	The new classification contributes to enhancing the speed and accuracy of the Automated Fingerprint Identification System (AFIS).	Accuracy = 90%, 89%
8.	[44]	2022	CNN, GNN	SOCOFing	Integrating superpixel-level knowledge into visual systems, especially those based on convolutional neural networks (CNNs).	Accuracy = 93.58%
9.	[45]	2022	CNN	SOCOFing	A new framework capable of recognizing fingerprints through image processing and using multiple fingerprint methods.	Accuracy = 95.93%
10.	[38]	2022	CNN	SOCOFing	A system capable of classifying the input fingerprint image as male or female was developed using convolutional neural networks.	Accuracy = 72%
11.	[39]	2022	Siamese Network	ImageNet	The study proposed a Siamese neural network-based method for fingerprint recognition without relying on pre-constructed databases. This approach enabled recognition from any image source, addressing cross-platform challenges and algorithmic complexity.	Accuracy = 92%
12.	[53]	2022	CNN, SVM	LivDet2015	The study developed a fingerprint liveness detection system using the LivDet2015 dataset. It compared SVM, CNN, and CNN+SVM methods, emphasizing the classification performance of CNN after applying preprocessing steps like edge enhancement and feature extraction.	Accuracy = 90%
13.	[40]	2023	VGG 19, VGG 16, InceptionV3, ResNet-50	SOCOFing	The research used data augmentation techniques, such as rotation and flipping, to address insufficient fingerprint data. Transfer learning pre-trained CNNs, enhancing training efficiency and model performance.	Accuracy = 71.9%, 72.3%, 67.3%, 60.8%

Seq.	Ref.	Year	Algorithm	Datasets	Contributions	Performance Metrics
14.	[41]	2023	VGG 16, VGG 19, ResNet18, ResNet50, ResNet101	SOCOFing	Gender classification evaluation was conducted across different datasets, with enhanced analysis of poor and partial quality fingerprints, and using data-driven artificial intelligence (DCAI) to improve performance.	Accuracy = 83%, 84%, 76%, 75%, 76%
15.	[54]	2023	ResNet34, ResNet50	LivDet DB, ATVS DB	A novel attention-based design for life detection in fingerprints, with a comprehensive evaluation study of the effectiveness of different clustering strategies and comparison with traditional algorithms and insights.	Accuracy = 95.81%, 95.52%, 97.78%, 97.05%
16.	[46]	2023	R-CNN	NIST NFSEG	Two large in-house datasets were developed with a test dataset containing 133,611 fingerprints of children and adults, and all images were manually labeled to create a reference base for comparing the accuracy of different fingerprint segmentation systems.	Accuracy = 97.17%
17.	[47]	2023	MLP	NIST	The study introduced a method that eliminated the need for preprocessing by using wavelet decomposition with max-pooling to extract features. It applied a Haar wavelet of four levels, followed by max-pooling, to generate training data for a Multilayer Perceptron (MLP) network.	Accuracy = 80.1%
18.	[49]	2023	GAN	NIST SD14	A new methodology for improving latent fingerprints as a limited problem in the deep generative network (GAN) architecture, with the application of a fingerprint bone map.	Accuracy = 76.36%
19.	[42]	2024	CNN	FVC2000 DB1	An accurate and efficient methodology was developed to compare two fingerprints and classify them as belonging to the same or different individuals, where a new method for verifying the extracted minutes using the convex shape was proposed.	FMR = 0.06%
20.	[50]	2024	CNN	FVC2006 DB1, FingerPassDB7	A structured approach based on deep convolutional neural networks (DCNN) was used, applying Siamese network for feature extraction, with XGBoost algorithm applied for binary classification.	EER 10.66%, 1.34%

7. Challenges and Gaps in Fingerprint Identification

Fingerprint identification systems play a crucial role in security and identity verification. However, these systems face several challenges that impact their accuracy and effectiveness. Key challenges include the quality of the captured images, the risk of spoofing, and the diversity of fingerprint patterns. To address these issues, it is essential to develop accurate methods that enhance the reliability and performance of fingerprint identification systems. These difficulties include the followings:

A. *Variations in Fingerprints:*

As people age, their fingerprints change, reducing the precision of their identification. Finger stress or injury can alter a fingerprint's physical characteristics [55].

B. *Environmental Factors:*

Extreme temperatures can interfere with sensor performance and affect fingerprint capture, resulting in low-quality images [56].

C. *Sensor Limitations:*

The fingerprint sensor's performance restricts the system's capacity to record minute details, impacting the identification's precision. Furthermore, over time, sensors may deteriorate or lose some sensitivity, producing erroneous and fuzzy images [18].

D. *Spoofing and Security :*

To impersonate fingerprints, hackers employ a variety of materials, including silicone. Furthermore, the system can replay fingerprint data that has been captured to grant unauthorized access. This vulnerability highlights the need for stronger security measures to prevent misuse of stored biometric information [47].

E. *Legal and Privacy Concerns:*

Legal and privacy concerns are important in the use of fingerprint data. Keeping stored fingerprint data safe from hackers and unauthorized access is crucial. It is

also essential to follow privacy laws and regulations when collecting and storing biometric data. Ensuring the security of this sensitive information helps protect individuals' rights and maintain trust in fingerprint recognition systems [57].

F. *Moral Implications:*

Users should obtain consent from individuals for the collection and use of their biometric data. It is also important to avoid biases in fingerprint identification software. These biases can unfairly target specific demographic groups. Addressing these issues promotes fairness and trust in biometric systems [58].

Figure 7 shows some examples of damaged fingerprints.

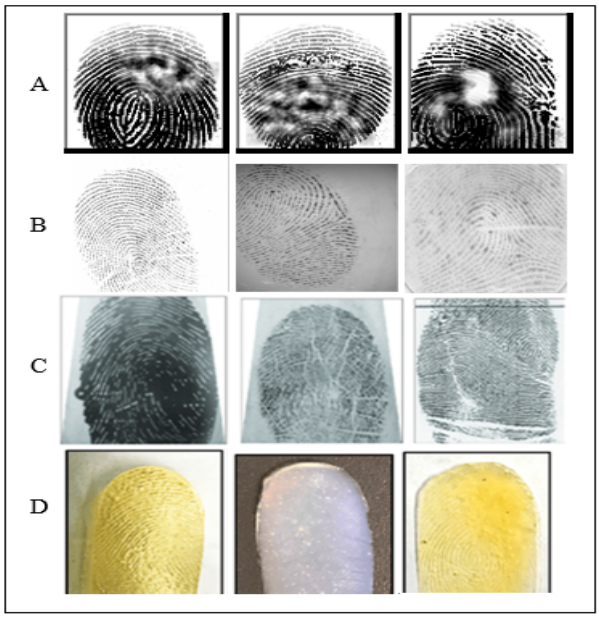

Figure 7. An example of damaged Fingerprints, A. Environmental factors, B. Sensor limitations, C. Variations in fingerprints, D. Spoof fingerprints.

8. Algorithms for Building Fingerprint Identification Systems

Fingerprint identification algorithms play a significant role in the various stages of fingerprint system identification. Traditional fingerprint matching methods fall into three distinct groups: linkage-based comparison, detail-based comparison, and vague feature-based matching. Linkage-based matching algorithms, such as Generative Adversarial Networks (GAN), Stacked Autoencoders (SAE), and Deep Belief Networks (DBN), rely on establishing connections between minor fingerprint points and their surrounding features. Small fingerprint dots indicate specific points on fingerprint creases, and their relative orientation and location are used to determine fingerprint similarity [59].

Details-based matching algorithms can handle complex fingerprint details, using a variety of algorithms to capture and compare small details [60], [61]. Some common examples of these algorithms are:

- Restricted Boltzmann Machine (RBM): A method for extracting features from complex data.
- Recurrent Neural Network (RNN): It handles sequential data where the order and context of data points are essential and analyzes its correlation.
- Radial Basis Function Network (RBFN): Radial basis functions are used for non-linear data processing and classification.
- Probabilistic Neural Network (PNN): Probabilistic modeling processes and categorizes probabilistic data.
- Convolutional Neural Network (CNN): CNNs extract features from spatially structured data, such as images, focusing on 2D data.
- Single-Layer Perceptron (SLP): SLP is a simple and linear data classification algorithm.
- The Multilayer Perceptron (MLP): MLP classifies non-linear and complex data using multiple layers of computing units.

Fingerprint thinning is a critical preprocessing step that simplifies fingerprint images by removing unnecessary pixels to reveal the core structure. There are two primary thinning strategies: iterative boundary removal methods and non-iterative separate transformation methods. Iterative methods, which include sequential and parallel approaches, progressively eliminate boundary pixels to achieve a pixel-wide thin image. In contrast, non-iterative methods, such as mean axis transformations, apply direct transformations to thin the image but are generally less effective and less suited for specific applications compared to iterative techniques [62].

9. Fingerprint Datasets

Fingerprint datasets are collections of fingerprint images or templates gathered for various purposes, including research, algorithm development, and system testing in the field of fingerprint identification. These datasets are essential for training and evaluating fingerprint identification algorithms, assessing system performance, and conducting experiments in biometrics. Summarized the details of these data totals in Table II and commonly employed fingerprint datasets include:

- Fingerprint Verification Competition (FVC) databases are widely used benchmark datasets in the fingerprint identification community. They consist of multiple editions (FVC2000, FVC2002, FVC2004, FVC2006, FVC-onGoing), each containing fingerprint images captured under different conditions [63], [64], [65].

TABLE II: Details about the most frequently used fingerprint datasets.

Seq.	Dataset	Number of images	Year	Image Type	Image Size	Applications
1.	NIST 4	4000	1992	JPEG	128x128	Develop, evaluate and improve deep learning models and neural networks.
2.	FVC2000	880	2000	JPEG	300×300, 256×364, 448×478, 240×320	Widely used benchmark in the fingerprint identification community.
3.	NIST 27	258	2000	LFF	768x800	Improving the accuracy and reliability of fingerprint sensors in various applications.
4.	FVC2002	2960	2001	JPEG	388×374, 296×560, 300×300, 288×384	
5.	FVC2004	880	2003	JPEG	640×480, 328×364, 300×480, 288×384	Widely used benchmark in the fingerprint identification community.
6.	FVC2006	1800	2006	BMP	96×96, 328×364, 640×480	
7.	NIST 14	54000	2001	JPEG	832x768	Commonly used for evaluating minutiae-based fingerprint identification algorithms.
8.	SDUMLA-HMT	25,440	2010	BMP	356x328	Frequently used for evaluating fingerprint identification algorithms in challenging scenarios.
9.	PolyU	1800	2014 - 2016	JPEG	480x640	Often used for research and algorithm testing.

- NIST Special Database 27, this dataset is provided by the National Institute of Standards and Technology (NIST). The dataset includes fingerprint images collected by optical and capacitive sensors. It is commonly used for evaluation in biometric analytics [66].
- NIST Special Database 4 is another contribution from NIST. This dataset contains fingerprint images captured using high-resolution scanners. It is generally used for evaluating minutiae-based fingerprint identification algorithms [67].
- Fingerprint Verification Competition 2006 (FVC2006) is part of the FVC series. This dataset includes datasets for fingerprint verification. It comprises four databases, each with fingerprint images captured using different sensors and under varying conditions [68].
- PolyU Fingerprint Database (PolyU-FP) contains fingerprint images captured using optical sensors. It is often used for research and algorithm testing [69].
- NIST Special Database 14 provides grayscale fingerprint images scanned from inked cards. It is widely used in biometric research to test and improve fingerprint recognition systems. The dataset supports developing algorithms for image processing and identity verification. It is a standard benchmark for evaluating the accuracy of recognition methods [70].
- SDUMLA-HMT Fingerprint Database is a high-resolution dataset containing fingerprint images captured under different conditions. It is often used to evaluate fingerprint identification algorithms in challenging scenarios [71].

10. Evaluation

A variety of evaluation metrics are used to provide a thorough assessment of biometric fingerprint identification systems. These quantitative measures provide information about many aspects of system performance that are useful for evaluating the accuracy of these systems. Some of these evaluation measurements include, but are not limited to:

- **Recall (R):** Recall, also known as sensitivity or True Positive Rate (TPR), is the proportion of actual positives that the fingerprint identification system successfully recognizes. Equation 1 illustrates how recall is computed as the ratio of true positives (TP) to the total of false negatives (FN). This measure shows how well the identification system can detect actual fingerprint matches. A higher sensitivity shows that the system efficiently recognizes a large proportion of actual positive instances matches, indicating its effectiveness in accurately identifying people based only on their fingerprints [72].

$$Recall(R) = \frac{TP}{TP + FN} \tag{1}$$

- **Precision (P):** precision is defined as the percentage of fingerprints that can be effectively identified. Equation 2 illustrates how the system precision can be computed as the ratio of true positives (TP) to the total of true positives and false positives (FP). High precision denotes various false positives because most fingerprints identified in the system are accurate matches. [73]. Precision is calculated as:

$$Precision(\mathrm{P}) = \frac{TP}{TP + FP} \tag{2}$$

- **Accuracy:** Accuracy measures the ratio of all fingerprint identifications (each true match and mismatches) out of the overall quantity of identifications. Accuracy offers a measure of the system's overall performance. However, this measure can be misleading if the dataset includes a significant imbalance between matches and non-matches [74].

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{3}$$

- **F1-Score:** The F1 score is a metric that combines precision and recall into a single value. It helps evaluate a fingerprint identification system's overall performance, particularly in imbalanced accurate matches and non-matches, [75].

$$F1\text{-score} = \frac{2 \times P \times R}{P + R} \tag{4}$$

- **Genuine Acceptance Rate (GAR):** The GAR measures the system's ability to measure the proportion of legitimate users (genuine matches) that are correctly accepted by the system. It indicates how effectively the system identifies and authenticates accurate fingerprint matches without mistakenly rejecting them [76].

$$\text{GAR} = \frac{\text{Number of Cases Accepted Correctly}}{\text{Total Number of Genuine Cases}} \tag{5}$$

- **False Acceptance Rate (FAR):** FAR is a critical metric used in fingerprint identity systems to quantify the percentage of unauthorized users (imposters) mistakenly granted access by the system, being incorrectly identified as legitimate users [25].

$$\text{FAR} = \frac{\text{Total Number of Imposter Attempts}}{\text{Number of False Acceptances}} \tag{6}$$

- **The Recognition Rate (RR):** The recognition rate in biometric security measures the percentage of accurately identified instances out of the total number of identification attempts, particularly in fingerprint recognition systems [77].

$$\text{RR} = \frac{\text{Number Correctly Recognized}}{\text{Number Instances}} \times 100\% \tag{7}$$

- **Total Success Rate (TSR):** TSR in fingerprint identification systems refers to the overall proportion of correctly processed cases, including accurate matches and true non-matches, out of the total number of cases processed [78].

$$\text{TSR} = \frac{\text{Number of Successful Instances}}{\text{Total Number of Instances}} \times 100\% \tag{8}$$

- **Specificity:** Specificity assesses the system's ability to identify actual negative cases accurately. It is crucial to understand how well the system can reject non-matching fingerprints. A higher specificity indicates a system with a lower rate of false positives, thus improving reliability and security [79].

$$\text{Specificity} = \frac{\text{TN}}{\text{TP} + \text{FN}} \tag{9}$$

- **Root Mean Squared Error (RMSE):** RMSE is a metric used to measure the average magnitude of the errors between predicted values ($\hat{y}_i$) and actual values (X_i). [80].

$$\text{RMSE}(X) = \sqrt{\frac{1}{N}\sum_{i=1}^{N} X_i - \hat{y}_i)^2} \tag{10}$$

- **Mean Absolute Error (MAE):** MAE describes the average magnitude of errors in the system's predictions. It is calculated as the average unconditional difference between the actual (y_i) and predicted values (x_i). A lower MAE suggests the system has more minor average prediction errors [35].

$$\text{MAE} = \frac{1}{n}\sum_{i=1}^{n} |y_i - x_i| \tag{11}$$

- **The Receiver Operating Characteristic (ROC) Curve :** ROC represents the compromise between accurate positive results and false positive rates, which aids in the analysis of system performance [23].

- **Fingerprint Image Distortion (FID):** FID measures the degree of distortion in fingerprint images. It aids in determining the high quality and dependability of the captured fingerprint data. The Structural Similarity Index (SSIM) is a widely used method for quantifying distortion for measuring by computing similarity between two fingerprint images [81].

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (12)$$

Where:

x and y are the two images being compared.
μ_x is the mean of image x.
μ_y is the mean of image y.
σ_x^2 is the variance of image x.
σ_y^2 is the variance of image y.
σ_{xy} is the covariance between images x and y.
C_1 is a constant defined as $C_1 = (k_1 L)^2$.
C_2 is another constant defined as $C_2 = (k_2 L)^2$.
L is the dynamic range of the pixel values
k_1 and k_2 are small constants

- **Likelihood Ratio Test (LRT):** LRT is a statistical method used in biometric systems to make decisions. It calculates the likelihood ratio between two competing hypotheses (L_1, L_2) to make informed decisions. The assessment aims to determine the strength of evidence for a specific match by comparing the probability of the fingerprint's association with a known individual against the likelihood of its association with another individual [82].

$$\text{LRT} = -2\left(\ln(L_1) - \ln(L_0)\right) \quad (13)$$

- **Mean Error (ME):** ME is a metric used to measure the common discrepancy among the predicted values (y_i) and the actual values ($\hat{y}_i$) in a fingerprint identification system. It quantifies the system's overall accuracy by evaluating how close the prediction values are to the actual values [83].

$$\text{ME} = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i) \quad (14)$$

All these evaluation measures use mathematical definitions. They give a comprehensive evaluation of biometric fingerprint identification systems. Using these metrics together ensures a thorough review of system performance. Knowing how to evaluate the system allows for continuous improvement and adjustments, which in turn allows for accuracy and reliability that is more consistent with actual results.

11. Applied Ethical Issues

The creation and processing of fingerprint databases face several ethical issues [58]:

A. Privacy:

The collection and storage of fingerprints can breach privacy. There are concerns about how these data usage and accessibility.

B. Security:

Database breaches can lead to misuse of stolen fingerprints. Unlike passwords, fingerprints can not be changed, increasing the risks.

C. Consent:

Explicit consent from individuals is required before collecting fingerprints dataset. Individuals must be informed about the use of the dataset and must give voluntary consent.

D. Legal and Regulatory Information:

Laws and regulations should specify using fingerprints to protect individual rights.

To address these ethical issues, the security and technical benefits of fingerprinting must be balanced with the protection of individual rights and freedoms.

12. Discussion of Key Findings of The Study

The survey presented in this study examined several recent works related to fingerprint identification. This survey included multiple deep learning algorithms using many different models to train the models. These models were evaluated using different datasets based on image quality and size to provide a comprehensive view of the reality of recent scientific research in this field. The main findings derived from this extensive survey will be highlighted to analyze the critical points, advancements, challenges, and future directions in applying deep learning techniques to fingerprint identification.

Figure 8 shows the distribution of recent studies based on the deep learning algorithms and structures used. According to the current study and the papers reviewed in this research, convolutional neural networks (CNNs) are the most commonly used methods in fingerprint recognition, accounting for about 35% of the total techniques currently employed. These networks are known for their ability to extract complex features from images, which enhances recognition accuracy. Following CNNs, ResNet is used at a rate of 21%, and VGG follows with a usage rate of 14%. Generative adversarial networks (GANs) rank fourth, representing approximately 11% of the applications, as they are utilized to generate additional data that improves model performance. Region-based convolutional neural networks (R-CNNs) account for about 9% of the usage but are

less common compared to other methods, as they are primarily designed for object detection in images, focusing on identifying regions of interest. These usage rates in recent research reflect the continuous enhancement of deep learning techniques and their applications in fingerprint identification. Consequently, all of these methods contribute to improving accuracy and reliability in security and identity systems.

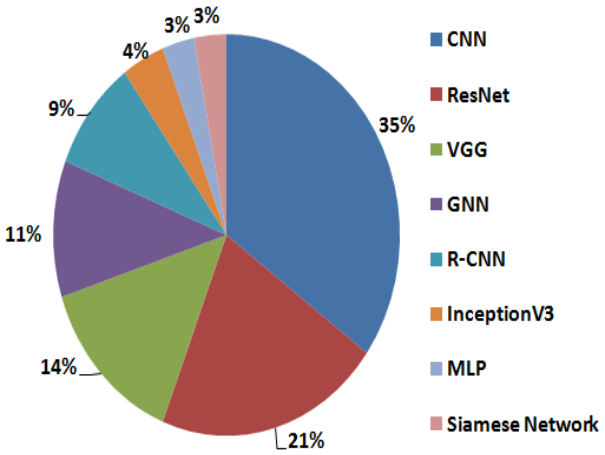

Figure 8. Distribution of deep learning algorithms by survey.

On the other hand, models like InceptionV3, MLP, and Siamese Network are rarely used in fingerprint identification. InceptionV3 is effective in extracting features and classifying images but has been applied in very few studies for fingerprint identification tasks. Similarly, Multi-Layer Perceptrons (MLP), while versatile, are not commonly used in this area. Most researchers prefer models specifically designed for biometric systems.

The Siamese Network has shown potential for fingerprint identification, especially in comparing and matching fingerprints. Its ability to learn pairwise relationships makes it suitable for this purpose. However, it appears in only about 3% of the papers reviewed in this survey. This limited use may be due to the model's complexity or insufficient exploration of its capabilities in fingerprint identification.

Some studies included more than one dataset, either individually or by merging multiple datasets to enhance the evaluation process. In this survey, Figure 9 displays the frequently used datasets. Among these, the SOCOFing database was utilized in 25% of the reviewed studies due to its extensive collection of fingerprints, including both authentic and fabricated samples. It is particularly effective for testing systems' ability to distinguish between real and fake fingerprints, thereby improving fingerprint identification accuracy.

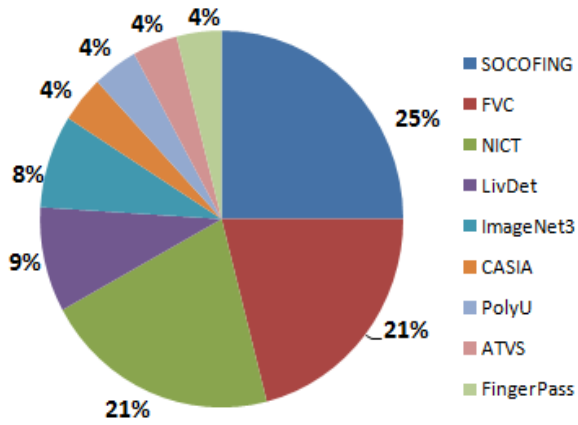

Figure 9. Distribution of datasets used in survey studies.

The FVC (Fingerprint Verification Competition) database accounted for 21% of the studies. It provides diverse fingerprints collected under various conditions, enabling researchers to test the robustness of their algorithms. Similarly, the NIST database, also used in 21% of the studies, offers a large and varied fingerprint collection suitable for algorithm development and testing. Additionally, the LivDet database was featured in 9% of the studies, focusing on spoof detection.

In summary, selecting the right database and model is crucial for effective fingerprint identification systems. A diverse and standardized database provides a wide range of fingerprint samples for testing algorithms in different conditions. This variety ensures that the system is robust and reliable. At the same time, the chosen model must align with the research objectives, whether it is to improve accuracy or address specific challenges like spoof detection. This combination of a suitable database and an appropriate model enhances overall system performance, minimizes errors, and ensures reliable identification in real-world applications.

Based on the findings of the current survey, future research should focus on enhancing the generalizability of fingerprint identification models. This can be achieved by utilizing more extensive and diverse datasets and employing advanced techniques such as transfer learning and data augmentation. Additionally, combining fingerprint recognition with other biometric modalities, such as facial recognition or iris scans, presents a promising path for improving accuracy and robustness. Addressing emerging security concerns is also vital; this includes developing methods to detect and prevent spoofing attacks while ensuring the privacy and security of biometric data through techniques like differential privacy and secure multi-party computation. Collectively, these strategies will advance the reliability and security of fingerprint identification systems.

13. Conclusions

This survey provided a comprehensive review of recent studies on deep learning techniques for fingerprint identification. It analyzed the most commonly used deep learning methods and datasets in previous research, offering insights into current practices for addressing fingerprint recognition challenges. The findings highlighted several key factors affecting the effectiveness of identification systems, including the importance of effective data preparation and the need for ethical considerations related to privacy.

In summary, the survey emphasizes the importance of advancing biometric authentication systems through improved deep learning methodologies. It also concluded with an overview of the challenges faced in fingerprint identifcation, such as data quality, environmental factors, and algorithmic limitations. By addressing these challenges and refining data collection processes, the field can make significant progress in fingerprint recognition technology, ultimately leading to more reliable and secure identification solutions.

References

[1] S. Balakrishnan, V. K. Hameed, and M. S. S. Hameed, "An embarking user friendly palmprint biometric recognition system with topnotch security," in *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*. IEEE, May 2021, pp. 1028–1032.

[2] Z. A. Oraibi and S. Albasri, "Efficient covid-19 prediction by merging various deep learning architectures," *Informatica*, vol. 48, no. 5, 2024.

[3] H. G. Muhammad and Z. A. Khalaf, "Fingerprint identification system based on vgg, cnn, and resnet techniques," *Basrah Researches Sciences*, vol. 50, no. 1, pp. 166–178, 2024.

[4] A. Tamrakar and N. K. Gupta, "Low resolution fingerprint image verification using cnn filter and lstm classifier," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 5, pp. 3546–3549, Jan 2020.

[5] D. Meltzer and D. Luengo, "Efficient clustering-based electrocardiographic biometric identification," *Expert Systems with Applications*, vol. 219, Jun 2023.

[6] R. A. Aljanabi, Z. T. Al-Qaysi, M. A. Ahmed, and M. M. Salih, "Hybrid model for motor imagery biometric identification," *Iraqi Journal For Computer Science and Mathematics*, vol. 5, no. 1, pp. 1–12, Dec 2023.

[7] T. G. Al-Sultan, A. Q. Abduljabar, W. H. Alkhaled, Z. H. Al-Sawaff, and F. Kandemirli, "A new approach to develop biometric fingerprint using human right thumb fingernail," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 1, pp. 98–107, Jul 2023.

[8] T. M. C. Pereira, R. C. Conceição, V. Sencadas, and R. Sebastião, "Biometric recognition: A systematic review on electrocardiogram data acquisition methods," *Sensors*, vol. 23, no. 3, Feb 2023.

[9] K. N. Win, K. Li, J. Chen, P. F. Viger, and K. Li, "Fingerprint classification and identification algorithms for criminal investigation: A survey," *Future Generation Computer Systems*, vol. 110, pp. 758–771, Sep 2020.

[10] J. J. Engelsma, K. Cao, and A. K. Jain, "Learning a fixed-length fingerprint representation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 43, no. 6, pp. 1981–1997, Jun 2021.

[11] Y. Liang and W. Liang, "Reswcae: Biometric pattern image denoising using residual wavelet-conditioned autoencoder," *arXiv preprint arXiv:2307.12255*, Jul 2023. [Online]. Available: http://arxiv.org/abs/2307.12255

[12] N. Ammour, Y. Bazi, and N. Alajlan, "Multimodal approach for enhancing biometric authentication," *Journal of Imaging*, vol. 9, no. 9, p. 168, Aug 2023.

[13] A. T. Mahmoud *et al.*, "An automatic deep neural network model for fingerprint classification," *Intelligent Automation and Soft Computing*, vol. 36, no. 2, pp. 2007–2023, 2023.

[14] J. K. Appati, P. K. Nartey, E. Owusu, and I. W. Denwar, "Implementation of a transform-minutiae fusion-based model for fingerprint recognition," *International Journal of Mathematics and Mathematical Sciences*, vol. 2021, 2021.

[15] E. E. B. Adam and Sathesh, "Evaluation of fingerprint liveness detection by machine learning approach - a systematic view," *Journal of ISMAC*, vol. 3, no. 1, pp. 16–30, Mar 2021.

[16] K. Li, D. Wu, L. Ai, and Y. Luo, "The influence of close non-match fingerprints similar in delta regions of whorls on fingerprint identification," *Journal of Forensic Sciences*, vol. 66, no. 4, pp. 1482–1494, Jul 2021.

[17] S. O. Ogunlana, G. B. Iwasokun, and O. Olabode, "Fingerprint individuality model based on pattern type and singular point attributes," *International Journal of Information Security Science*, vol. 10, no. 3, pp. 75–85, 2021.

[18] A. F. Y. Althabhawee and B. K. O. C. Alwawi, "Fingerprint recognition based on collected images using deep learning technology," *IAES International Journal of Artificial Intelligence*, vol. 11, no. 1, pp. 81–88, Mar 2022.

[19] M. Sharif, M. Raza, J. H. Shah, M. Yasmin, and S. L. Fernandes, "An overview of biometrics methods," in *Handbook of Multimedia Information Security: Techniques and Applications*. Springer International Publishing, 2019, pp. 15–35.

[20] A. Ross, A. Jain, K. Nandakumar, and N. Ratha, "Some research problems in biometrics: The future beckons," in *2019 International Conference on Biometrics (ICB)*. IEEE, Jun 2019, pp. 1–8.

[21] S. Hemalatha, "A systematic review on fingerprint based biometric authentication system," in *International Conference on Emerging Trends in Information Technology and Engineering, ic-ETITE 2020*. Institute of Electrical and Electronics Engineers Inc., Feb 2020.

[22] V. M. Praseetha, S. Bayezeed, and S. Vadivel, "Secure fingerprint authentication using deep learning and minutiae verification," *Journal of Intelligent Systems*, vol. 29, no. 1, pp. 1379–1387, Jan 2020.

[23] N. Singla, M. Kaur, and S. Sofat, "Automated latent fingerprint identification system: A review," *Forensic Science International*, vol. 309, p. 110187, Apr 2020.

[24] V. Jalaja, G. Anjaneyulu, and L. Mohan, "Fingerprint recognition

based on biometric cryptosystem," *Journal of Integrated Science and Technology*, vol. 12, no. 3, pp. 763–763, 2024.

[25] S. Muslimin, Y. Wijanarko, L. I. Kesuma, R. Maulidda, Y. Hasan, H. Basri *et al.*, "Biometric fingerprint implementation for presence checking and room access control system," in *4th Forum in Research, Science, and Technology (FIRST-T1-T2-2020)*. Atlantis Press, 2021, pp. 490–494.

[26] C. Wang, Y. Wang, Y. Chen, H. Liu, and J. Liu, "User authentication on mobile devices: Approaches, threats and trends," *Computer Networks*, vol. 170, p. 107118, 2020.

[27] A. Bodepudi and M. Reddy, "Cloud-based biometric authentication techniques for secure financial transactions: A review," *International Journal of Information and Cybersecurity*, 2020.

[28] A. Thiel, "Biometric identification technologies and the ghanaian 'data revolution'," *Journal of Modern African Studies*, vol. 58, no. 1, pp. 115–136, 2020.

[29] O. T. Omolewa, E. J. Adeioke, O. O. Titilope, A. K. Sakarivan, and A. J. Kehinde, "Border control via passport verification using fingerprint authentication technique," in *2023 International Conference on Science, Engineering and Business for Sustainable Development Goals (SEB-SDG)*, 2023, pp. 1–7.

[30] W. Auliya and J. Hafidz, "Law enforcement against criminal action with fingerprint evidence," *Law Development Journal*, vol. 2, no. 3, pp. 302–306, 2020.

[31] E. O. Badmus, O. P. Odekunle, and D. O. Oyewobi, "Smart fingerprint biometric and rfid time-based attendance management system," *European Journal of Electrical Engineering and Computer Science*, vol. 5, no. 4, pp. 34–39, 2021.

[32] J. Mason, R. Dave, P. Chatterjee, I. Graham-Allen, A. Esterline, and K. Roy, "An investigation of biometric authentication in the healthcare environment," *Array*, vol. 8, p. 100042, 2020.

[33] M. Hernandez-de Menendez, R. Morales-Menendez, C. A. Escobar, and J. Arinez, "Biometric applications in education," *International Journal on Interactive Design and Manufacturing*, vol. 15, no. 2-3, pp. 365–380, 2021.

[34] M. A. Al Rakib *et al.*, "Fingerprint based smart home automation and security system," *European Journal of Engineering and Technology Research*, vol. 7, no. 2, pp. 140–145, 2022.

[35] A. M. M. Chowdhury and M. H. Imtiaz, "Contactless fingerprint recognition using deep learning—a systematic review," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 714–730, September 2022.

[36] U. U. Deshpande, V. S. Malemath, S. M. Patil, and S. V. Chaugule, "Cnnai: A convolution neural network-based latent fingerprint matching using the combination of nearest neighbor arrangement indexing," *Front Robot AI*, vol. 7, 2020.

[37] Y. A. Al-Wajih, W. M. Hamanah, M. A. Abido, F. Al-Sunni, and F. Alwajih, "Finger type classification with deep convolution neural networks," in *Proceedings of the International Conference on Informatics in Control, Automation and Robotics*. Science and Technology Publications, Lda, 2022, pp. 247–254.

[38] M. O. Oladele, T. M. Adepoju, O. A. Olatoke, O. A. Ojo, and Orimogunje, "Convolutional neural network for fingerprint-based gender classification," *Sciences, Engineering & Environmental Technology (ICONSEET)*, vol. 7, no. 14, pp. 112–117, 2022. [Online]. Available: www.repcomseet.org

[39] Z. Li, M. Huang, H. Wu, L. Huang, and Y. Zhang, "A novel fingerprint recognition method based on a siamese neural network," *Journal of Intelligent Systems*, vol. 31, no. 1, pp. 690–705, 2022.

[40] M. Jacob, "Binary gender classification of african fingerprints using cnn," Ph.D. dissertation, Dublin, National College of Ireland, 2023.

[41] A. Spanier *et al.*, "Enhancing fingerprint forensics: A comprehensive study of gender classification based on advanced data-centric ai approaches and multi-database analysis," *Applied Sciences*, vol. 14, no. 1, p. 417, 2024.

[42] N. Martins, J. Silva, and A. Bernardino, "Fingerprint recognition in forensic scenarios," *Sensors*, vol. 24, no. 2, 2024.

[43] F. Liu, Y. Zhao, G. Liu, and L. Shen, "Fingerprint pore matching using deep features," *Pattern Recognition*, vol. 102, 2020.

[44] G. Chhablani, A. Sharma, H. Pandey, and T. Dash, "Superpixel-based knowledge infusion in deep neural networks for image classification," in *Proceedings of the ACM Southeast Conference*. New York, NY, USA: ACM, 2022.

[45] S. Jeong, "Design on novel door lock using minimizing physical exposure and fingerprint recognition technology," *JOIV : International Journal on Informatics Visualization*, vol. 6, no. 1, p. 103, 2022.

[46] M. S. Murshed, K. Bahmani, S. Schuckers, and F. Hussain, "Deep age-invariant fingerprint segmentation system," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 2024.

[47] S. Suwarno, "Gender classification based on fingerprint using wavelet and multilayer perceptron," *Sinkron*, vol. 8, no. 1, pp. 139–144, 2023.

[48] A. Chowdhury, S. Kirchgasser, A. Uhl, and A. Ross, "Can a cnn automatically learn the significance of minutiae points for fingerprint matching?" in *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*, 2020.

[49] Y. Zhu, X. Yin, and J. Hu, "Fingergan: A constrained fingerprint generation scheme for latent fingerprint enhancement," *IEEE Trans Pattern Anal Mach Intell*, vol. 45, no. 7, pp. 8358–8371, 2023.

[50] N. Shabrina, D. Li, and T. Isshiki, "High precision fingerprint verification for small area sensor based on deep learning," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 107, no. 1, pp. 157–168, 2024.

[51] O. Giudice, M. Litrico, and S. Battiato, "Single architecture and multiple task deep neural network for altered fingerprint analysis," in *2020 IEEE International Conference on Image Processing (ICIP)*. IEEE, 2020, pp. 813–817.

[52] I. Goel, N. B. Puhan, and B. Mandal, "Deep convolutional neural network for double-identity fingerprint detection," *IEEE Sensors Letters*, vol. 4, no. 5, 2020.

[53] Z. İ. Özkiper, Z. Turgut, T. Atmaca, and M. A. Aydın, "Fingerprint liveness detection using deep learning," in *2022 9th International Conference on Future Internet of Things and Cloud (FiCloud)*. IEEE, 2022, pp. 129–135.

[54] K. Zhang, S. Huang, E. Liu, and H. Zhao, "Lfldnet: Lightweight fingerprint liveness detection based on resnet and transformer," *Sensors*, vol. 23, no. 15, 2023.

[55] A. A. Frick, A. Girod-Frais, A. Moraleda, and C. Weyermann, *Latent Fingermark Aging: Chemical Degradation Over Time*. Cham: Springer International Publishing, 2021, pp. 205–235. [Online]. Available: https://doi.org/10.1007/978-3-030-69337-4_7

[56] Y. Xun, J. Liu, N. Kato, Y. Fang, and Y. Zhang, "Automobile driver fingerprinting: A new machine learning based authentication scheme," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1417–1426, 2020.

[57] R. Dhaneshwar, M. Kaur, and M. Kaur, "An investigation of latent fingerprinting techniques," *Egyptian Journal of Forensic Sciences*, vol. 11, no. 1, p. 33, 2021.

[58] A. North-Samardzic, "Biometric technology and ethics: Beyond security applications," *Journal of Business Ethics*, vol. 167, no. 3, pp. 433–450, 2020.

[59] M. Diarra, A. K. Jean, B. A. Bakary, and K. B. Medard, "Study of deep learning methods f or fingerprint recognition," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 10, no. 3, pp. 192–197.

[60] J. D. Glover *et al.*, "The developmental basis of fingerprint pattern formation and variation," *Cell*, vol. 186, no. 5, pp. 940–956.e20.

[61] R. P. Krish, J. Fierrez, D. Ramos, F. Alonso-Fernandez, and J. Bigun, "Improving automated latent fingerprint identification using extended minutia types," *Information Fusion*, vol. 50, pp. 9–19.

[62] A. Adjimi, A. Hacine-Gharbi, P. Ravier, and M. Mostefai, "Mutual information based feature selection for fingerprint identification," *Informatica (Slovenia)*, vol. 43, no. 2, pp. 187–198.

[63] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "Fvc2000: Fingerprint verification competition," *IEEE transactions on pattern analysis and machine intelligence*, vol. 24, no. 3, pp. 402–412.

[64] D. M. et al., "Fvc2004: Third fingerprint verification competition," in *International conference on biometric authentication*. Springer Berlin Heidelberg, 2004, pp. 1–7.

[65] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "Fvc2002: Second fingerprint verification competition," in *2002 International conference on pattern recognition*, vol. 3. IEEE, 2002, pp. 811–814.

[66] M. D. Garris and R. M. McCabe, "Nist special database 27: Fingerprint minutiae from latent and matching tenprint images," *NIST Technical Report NISTIR*, vol. 6534, p. 1, 2000.

[67] C. I. Watson and C. L. Wilson, "Nist special database 4," *Fingerprint Database, National Institute of Standards and Technology*, vol. 17, no. 77, p. 5, 1992.

[68] R. Cappelli, M. Ferrara, A. Franco, and D. Maltoni, "Fingerprint verification competition 2006," *Biometric Technology Today*, vol. 15, no. 7–8, pp. 7–9.

[69] M. Kim, W.-Y. Kim, and J. Paik, "Optimum geometric transformation and bipartite graph-based approach to sweat pore matching for biometric identification," *Symmetry (Basel)*, vol. 10, p. 175.

[70] C. I. Watson, "Nist special database 14: Mated fingerprint cards pairs 2 version 2," *technical report, Citeseer*, 2001.

[71] Y. Yin, L. Liu, and X. Sun, "Sdumla-hmt: A multimodal biometric database," in *Lecture Notes in Computer Science*, vol. 2011, 2011, pp. 260–268.

[72] M. A. Hameed and Z. A. Khalaf, "A survey study in object detection: A comprehensive analysis of traditional and state-of-the-art approaches," *J. Basrah Res. (Sci.)*, vol. 50, no. 1, p. 16, Jun 2024.

[73] Z. A. Khalaf and I. A. Sheet, "News retrieval based on short queries expansion and best matching," *Journal of Theoretical and Applied Information Technology*, vol. 97, no. 2, pp. 490–500, 2019.

[74] D. Kothadiya *et al.*, "Enhancing fingerprint liveness detection accuracy using deep learning: A comprehensive study and novel approach," *J Imaging*, vol. 9, no. 8, August 2023.

[75] Q. M. Al Dulaimee, H. M. Ali, S. S. Hammadi, and Z. A. Khalaf, "Diagnosis, treatment and classification of covid-19 disease by complete blood test," *Biochem. Cell. Arch*, vol. 21, pp. 1211–1216, 2021.

[76] P. Patil and S. Jagtap, "Multi-modal biometric system using finger knuckle image and retina image with template security using polyu and drive database," *International Journal of Information Technology*, vol. 12, no. 4, pp. 1043–1050, 2020.

[77] W. Kabir, M. O. Ahmad, and M. N. S. Swamy, "A multi-biometric system based on feature and score level fusions," *IEEE Access*, vol. 7, pp. 59 437–59 450, 2019.

[78] H. Mehraj and A. H. Mir, "A survey of biometric recognition using deep learning," *EAI Endorsed Transactions on Energy Web*, vol. 8, no. 33, pp. 1–16, 2021.

[79] H. Zhang and Z. Yang, "Biometric authentication and correlation analysis based on cnn-sru hybrid neural network model," *Comput Intell Neurosci*, vol. 2023, pp. 1–11, March 2023.

[80] H. Chen, B. D. Rouhani, C. Fu, J. Zhao, and F. Koushanfar, "Deepmarks: A secure fingerprinting framework for digital rights management of deep learning models," in *ICMR 2019 - Proceedings of the 2019 ACM International Conference on Multimedia Retrieval*. Association for Computing Machinery, Inc, 2019, pp. 105–113.

[81] H. Chiroma, "Deep learning algorithms based fingerprint authentication: Systematic literature review," *Journal of Artificial Intelligence and Systems*, vol. 3, no. 1, pp. 157–197, 2021.

[82] F. Alhomayani and M. H. Mahoor, "Deep learning methods for fingerprint-based indoor positioning: a review," *Journal of Location Based Services*, vol. 14, no. 3, pp. 129–200, July 2020.

[83] J. Priesnitz, C. Rathgeb, N. Buchmann, C. Busch, and M. Margraf, "An overview of touchless 2d fingerprint recognition," *Eurasip Journal on Image and Video Processing*, vol. 2021, no. 1, pp. 1–12, December 2021.