

Deep Learning Innovations in Fingerprint Recognition: A Comparative Study of Model Efficiencies

Received: Sept 09, 2024

Revised: Oct 17, 2024

Accepted: Nov 05, 2024

Publish: Nov 06, 2024

Lusiana Efrizoni*, Sheeba Armoogum, Mohd Zaki Zakaria

Abstract:

Fingerprint recognition technology is integral to biometric security systems, providing secure and reliable identification through unique human fingerprint patterns. However, challenges such as low contrast, high intra-class variability, and partial fingerprints often compromise the efficiency and accuracy of traditional recognition systems. This research addresses these challenges by employing advanced deep learning techniques, specifically Convolutional Neural Networks (CNNs), to enhance fingerprint recognition performance. We propose a methodological approach that leverages state-of-the-art CNN architectures tailored to capture intricate fingerprint details. The study utilizes the Sokoto Coventry Fingerprint Dataset (SOCOFing), which includes diverse fingerprint types and synthetic alterations to evaluate model performance under realistic conditions. Through a comparative analysis of various CNN configurations, we assessed the models based on efficiency and accuracy, using metrics such as accuracy, precision, recall, and F1-score. Our experimental results demonstrate significant improvements in fingerprint recognition capabilities. The optimized CNN model achieved an accuracy of 98.61%, a precision of 97.12%, a recall of 97.46%, and an F1-score of 97.29%. These results validate the effectiveness of CNNs in handling complex biometric data and underscore their potential to enhance the reliability and security of fingerprint recognition systems. The study concludes that deep learning, through the use of CNNs, offers a powerful solution to the limitations of traditional fingerprint recognition techniques. This will pave the way for more sophisticated and accurate biometric security systems in practical applications. The research findings contribute to ongoing advancements in neural network architectures, enhancing their applicability in increasingly automated and data-driven security environments.

Keywords: Comparative study, Deep learning, Fingerprint recognition

1. INTRODUCTION

Fingerprint recognition technology is a cornerstone in biometric security systems, harnessing unique patterns in human fingerprints to provide secure and reliable identification (Subitha et al., 2024). Despite its widespread adoption, achieving high accuracy and efficiency in fingerprint recognition remains a pivotal concern in the face of varying quality and complex fingerprint patterns (Yang et al., 2019).

Traditional fingerprint recognition systems often grapple with low contrast, high intra-class variability, and partial fingerprints, which can severely degrade their performance. Moreover, the increasing demand for fast and reliable authentication in high-throughput

environments calls for more robust and adaptive algorithms that cope with diverse fingerprint qualities and environmental conditions (Pillin, 2019).

Fingerprint recognition research has evolved from traditional feature-based and minutiae-based techniques to more advanced machine learning methods. Initially, the field focused on direct pattern matching and feature extraction techniques, which were limited by their inability to effectively handle the high variability and common distortions in fingerprints, such as smudging and partial prints (de Alcaraz-Fossoul & Narowskis, 2021). Recent advancements have embraced machine learning and deep learning methods, demonstrating superior capabilities in managing these challenges. A comprehensive literature review indicates a progressive shift towards increasingly sophisticated models. These machine learning models, particularly deep learning approaches, have drastically improved recognition rates by adeptly navigating the complexities inherent in fingerprint imaging (Jain et al., 2016).

Convolutional Neural Networks (CNNs) have brought transformative changes in the broader image classification and recognition domain, proving particularly effective across various applications,

Publisher Note:

CV Media Inti Teknologi stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright

©2024 by the author(s).

Licensee CV Media Inti Teknologi, Bengkulu, Indonesia. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution-ShareAlike (CC BY-SA) license

(<https://creativecommons.org/licenses/by-sa/4.0/>).

including biometrics (Li et al., 2022). In the context of fingerprint recognition, CNNs have been pivotal due to their ability to extract deep, invariant features from images, which are crucial for handling issues like smudging, rotation, and scale changes (Chaman, 2022).

Numerous studies have explored various CNN architectures, tweaking network depths, adjusting filter sizes, and refining learning strategies to enhance performance. This exploration has led to notable improvements in the robustness and accuracy of fingerprint recognition systems, with CNNs setting new benchmarks in the field (Liu et al., 2021). These studies highlight CNNs' adaptability to different biometric recognition tasks and underscore their potential to develop more resilient and efficient recognition systems that can be applied in high-security areas and consumer electronics (Minaee, 2023).

This study introduces an innovative approach by employing a series of state-of-the-art CNN architectures to tackle the problem of fingerprint recognition. The proposed method leverages CNN's powerful feature extraction capabilities, capturing intricate details and patterns in image data. We optimize the network structure to accommodate fingerprints' unique characteristics better, enhancing the recognition system's accuracy and processing speed.

Our study utilizes the Sokoto Coventry Fingerprint Dataset (SOCOFing), widely recognized for its fingerprint types and the diversity of synthetic alterations (Ruizgara, 2018). The dataset is a robust platform for evaluating the effectiveness of CNN-based models. It includes various transformations like scratches, rotations, and noise levels, simulating real-world conditions that challenge the robustness of recognition systems.

The experimental strategy is structured around a comparative analysis of different CNN architectures, assessing their efficiency and accuracy. We implement a cross-validation approach to ensure the generalizability of our findings, coupled with a comprehensive analysis of the impact of different hyperparameters and training techniques. The performance of each model is rigorously evaluated against standard metrics such as accuracy, precision, recall, and F1-score to determine the most effective

CNN architecture for fingerprint recognition (Meiramkhanov & Tleubayeva, 2024).

By providing a comparative analysis of CNN models using the SOCOFing dataset, this study aims to push the boundaries of fingerprint recognition technology, offering insights into the configurations and strategies that yield the best performance. This exploration enhances our understanding of CNN's capabilities in biometric security and sets the stage for future innovations in fingerprint recognition systems.

2. MATERIAL AND METHOD

Fingerprint recognition is a crucial component of biometric authentication systems, widely employed across various security-dependent applications, from unlocking smartphones to controlling access in secure facilities. Fingerprints' inherent uniqueness makes them ideal for identifying and verifying individuals. However, traditional methods of fingerprint analysis, such as feature extraction and pattern matching, often struggle with the complexities presented by the varying qualities and environmental conditions of fingerprint scans. These challenges include distortions, different pressure levels, skin elasticity, and noise from the capturing devices.

Convolutional Neural Networks (CNN) in Deep Learning.

Deep learning, particularly through CNNs, has revolutionized fingerprint recognition by significantly enhancing the ability to interpret and classify complex image data. Unlike traditional algorithms that rely on predetermined rules for feature extraction, CNNs autonomously learn to identify the most effective patterns and features for classification tasks through their hierarchical structure.

CNNs use mathematical operations to process and transform input image data. The primary components include:

- **Convolutional Layers:** Apply filters to the input to create feature maps, highlighting specific features in the image. The convolution operation is defined as:

$$f(x, y) = (g * h)(x, y) = \sum_{m=-a}^a \sum_{n=-b}^b g(m, n) \cdot h(x - m, y - n) \quad (1)$$

where g is the input image, h is the filter, and f is the output feature map.

- **Activation Function:** Typically a Rectified Linear Unit (ReLU) that introduces non-linearity to the model, defined as:

$$f(x) = \max(0, x) \quad (2)$$
This helps the network learn complex patterns in the data.
- **Pooling Layers:** Reduce the dimensionality of each feature map independently, summarizing features with operations like max or average pooling.
- **Fully Connected Layers:** After several convolutional and pooling layers, the high-level reasoning in the neural network is done via fully connected layers where classification decisions are made based on the features extracted and condensed by previous layers.
- **Softmax Layer:** Used in the output layer for multi-class classification tasks like fingerprint identification, providing probabilities for each class.

Fingerprint Recognition Methodology

Deep learning methodologies, particularly those using CNNs, offer a transformative approach to fingerprint recognition, offering several substantial benefits over traditional methods. One of the primary advantages is the capability of feature learning. CNNs can autonomously learn to identify the most relevant features directly from raw fingerprint images without requiring manual feature extraction. This is especially critical in adapting to the wide array of fingerprint qualities and types encountered in real-world scenarios, where conventional methods often falter.

Moreover, deep learning models exhibit robustness to variability, a crucial factor in biometric authentication. Through extensive training on large and diverse datasets, these models develop resilience against common issues such as smudging, partial prints, and rotational discrepancies that traditionally hinder the performance of fingerprint recognition systems. This inherent robustness ensures that deep learning-based systems maintain high accuracy and reliability under varied conditions.

Another significant advantage is scalability. Deep learning models generally improve their predictive accuracy as they are exposed to larger volumes of data. This scalability means that as more fingerprint data becomes available, these models can be trained to become even more accurate and efficient, making them well-suited to growing security needs.

Finally, the ease of integration of deep learning models into various platforms highlights their practicality. Once trained, these models require only forward passes through the network to perform classification or verification tasks, simplifying the implementation process. This ease of integration makes deep learning appealing for developers looking to embed advanced fingerprint recognition capabilities into various applications, from mobile devices to high-security access control systems.

Evaluation Matrix for Fingerprint Recognition

The evaluation of fingerprint recognition models involves a set of metrics designed to measure the system's accuracy and reliability under various conditions. Each metric offers insights into different aspects of model performance, enabling a comprehensive assessment of its effectiveness.

Accuracy is a fundamental metric that indicates the overall effectiveness of the model. It is calculated as the proportion of total correct predictions made by the model out of all predictions. This metric provides a straightforward measure of the model's ability to correctly identify or verify a fingerprint, offering a quick snapshot of performance.

Precision and Recall are more detailed metrics that provide deeper insights into the model's performance. Precision measures the ratio of correctly predicted positive observations to the total predicted positives. This metric is crucial when the consequences of false positives are significant. Recall, or sensitivity, measures the ratio of correctly predicted positive observations to all actual positives in the dataset. It is especially important when it is critical to capture as many positives as possible. These metrics are useful for balancing the trade-offs between missing true positives and falsely predicting positives.

The F1 Score is the harmonic mean of precision and recall. It is a single metric that combines precision and recall to provide a balanced view of the model's performance. This is especially useful when false positives and negatives carry significant costs. The ROC Curve and AUC (Area Under the Curve) are metrics used to evaluate the model's performance across various threshold settings. The ROC curve plots the true positive rate against the false positive rate, showcasing the trade-off between sensitivity and specificity. The AUC provides a scalar value representing the likelihood that the model will rank a randomly chosen positive instance higher than a randomly chosen negative one. A higher AUC value indicates better model performance. These metrics form a robust framework for evaluating the effectiveness of fingerprint recognition models, helping developers and researchers to refine and

optimize their approaches for enhanced security solutions.

3. RESULT AND DISCUSSION

In the field of fingerprint recognition, using the Sokoto Coventry Fingerprint Dataset (SOCOFing) provides a unique opportunity to evaluate the effectiveness of various Convolutional Neural Network (CNN) architectures. This part of the study focuses on the experimental setup, the results obtained from implementing different CNN models, and a comprehensive discussion of the findings.

The experiment assesses how different CNN configurations accurately recognize and classify altered and unaltered fingerprint images under varied conditions. By systematically applying different architectural tweaks, filter sizes, and learning parameters, the study aims to uncover which combinations yield the highest accuracy and robustness, particularly against common challenges such as smudging, rotation, and synthetic alterations found in the dataset.

The Exploration of the Dataset

The Sokoto Coventry Fingerprint Dataset (SOCOFing) is a comprehensive resource on Kaggle. It is designed to develop and test biometric identification and verification systems, focusing on fingerprint recognition. It features fingerprint images from 600 African subjects, totaling 6,000 images, all

stored in BMP format for high-quality analysis by Ruizgara (2018), which can be accessed at <https://www.kaggle.com/datasets/ruizgara/socofing>.

This dataset is uniquely annotated with biometric and demographic details, including the subject's ID, gender, and which hand and finger the print came from. It also includes synthetic alterations to simulate real-world challenges, such as `Obliteration`, `Central Rotation`, and `Z-cut`. These alterations mimic scenarios like scars or deformities that can affect fingerprint recognition, making SOCOFing particularly valuable for testing the robustness of recognition algorithms against spoofs and other common issues.

The PreProcessing

Pre-processing is a critical step in preparing data for use in machine learning models, especially in complex image recognition tasks like fingerprint recognition. For the Sokoto Coventry Fingerprint Dataset (SOCOFing), which includes various fingerprint images with synthetic alterations, proper pre-processing enhances the effectiveness of subsequent analysis using Convolutional Neural Networks (CNNs). The pre-processing processes include image normalization, image resizing, image augmentation, synthetic alterations, greyscale conversion, edge enhancement, and binary thresholding.

After that process, the image can be visualized to show the real image in greyscale, as shown in Figure 1.

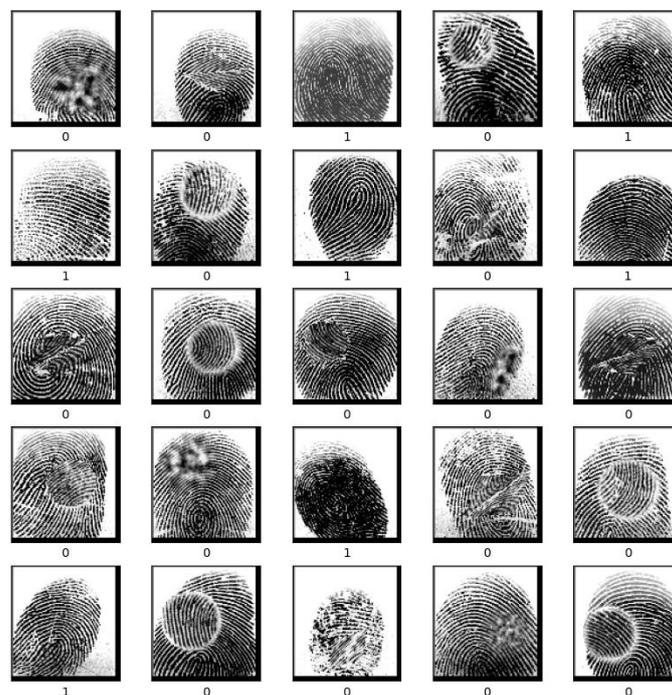


Figure 1. Visualize data of fingerprint from SOCOFing dataset.

Create a Convolutional Base Model

Creating a convolutional base model is foundational in building a Convolutional Neural Network (CNN) for tasks like fingerprint recognition. This process

involves defining the network's architecture, which includes selecting the type and sequence of layers that will effectively extract features from the input images. Figure 2 and Figure 3 show the Python code used to create the CNN model.

```

model = models.Sequential()
model.add(layers.Conv2D(32, (3, 3), activation='relu', input_shape=(103, 96, 3)))
model.add(layers.MaxPooling2D((2, 2)))
model.add(layers.Conv2D(64, (3, 3), activation='relu'))
model.add(layers.MaxPooling2D((2, 2)))
model.add(layers.Conv2D(64, (3, 3), activation='relu'))

model.summary()
    
```

Figure 2. Python code to create CNN model

Layer (type)	Output Shape	Param #
conv2d (Conv2D)	(None, 101, 94, 32)	896
max_pooling2d (MaxPooling2D)	(None, 50, 47, 32)	0
conv2d_1 (Conv2D)	(None, 48, 45, 64)	18,496
max_pooling2d_1 (MaxPooling2D)	(None, 24, 22, 64)	0
conv2d_2 (Conv2D)	(None, 22, 20, 64)	36,928

Figure 3. The CNN model summary

This CNN shows in Figure 3 an architecture involving multiple layers, each contributing to processing and transforming the input image into a form the network can use to make predictions or classifications. The network begins with a convolutional layer (conv2d), which applies 32 filters to the input image, resulting in 32 feature maps. This layer effectively captures basic patterns like edges and textures, with its output being 101x94 pixels for each feature map. The number of parameters here, 896, reflects the size and number of filters used, including a bias term for each filter.

Following the first convolutional operation, a max pooling layer (max_pooling2d) reduces the spatial dimensions of these feature maps by approximately half, making the feature maps 50x47 pixels. Max pooling is used here to decrease the computational burden and to make the network less sensitive to the exact locations of features within the image. This layer does not introduce any new parameters because it merely selects the maximum value in each patch of the feature map.

The process continues with a second convolutional layer (conv2d_1), which increases the complexity of the model by using 64 filters to delve deeper into the feature detection. This layer produces 64 feature maps, each 48x45 pixels, containing more refined

features, such as parts of fingerprint ridges or unique marks, facilitated by 18,496 parameters. Another max pooling layer (max_pooling2d_1) follows, further reducing each feature map's dimensions to 24x22 pixels. This reduction continues to help reduce data dimensions and computational costs, preparing the data for even more detailed analysis in subsequent layers without adding extra parameters.

The sequence ends with a third convolutional layer (conv2d_2), which does not change the number of filters but refines the feature maps to even more detailed components necessary for accurate recognition tasks. This final convolutional layer outputs 64 feature maps with dimensions of 22x20 pixels each. It involves the highest number of parameters in the sequence, 36,928, indicating its role in capturing the most intricate and decisive features from the input.

This architecture demonstrates a methodical approach to feature extraction, where each layer progressively increases in complexity and capability. Successive convolutional and max pooling layers help the network learn detailed and complex patterns necessary for fingerprint recognition, balancing depth of analysis, and computational efficiency.

Training the model

The next process is the training model. Figure 4 shows the Python coding to process the training

```
x, y = load_data([real_path, altered_path], (96, 103))
x_train, y_train, x_val, y_val, x_test, y_test = split_data(x, y, test_size=0.2)

model.compile(optimizer='adam',
              loss=tf.keras.losses.SparseCategoricalCrossentropy(from_logits=True),
              metrics=['accuracy'])

history = model.fit(x_train, y_train, batch_size = 32, epochs=100,
                  validation_data=(x_val, y_val))
```

Figure 4. Python code to split and train the model.

Figure 5 shows the accuracy graph results of the training process based on Figure 4. Then, we do

model. Before the data was used for training, the dataset was split 80% and 20% for training and testing, respectively.

the prediction or evaluation process with the testing dataset, as shown in Figure 6.

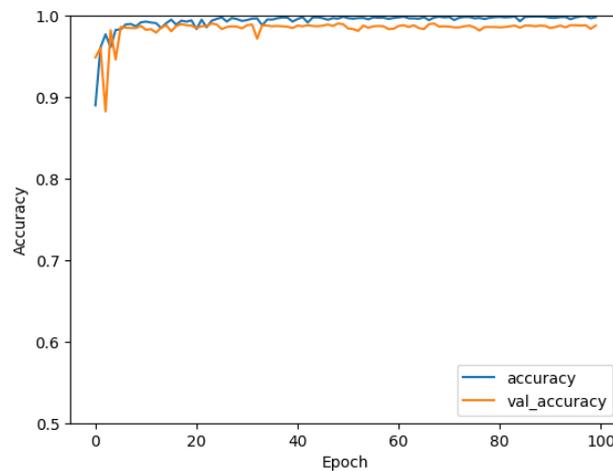


Figure 5. The accuracy and validation of accuracy the training process.

```
y_pred = model.predict(x_test)
y_pred_argmax = np.argmax(y_pred, axis=1)

accuracy = tf.keras.metrics.Accuracy()(y_test, y_pred_argmax)
precision = tf.keras.metrics.Precision()(y_test, y_pred_argmax)
recall = tf.keras.metrics.Recall()(y_test, y_pred_argmax)
f1 = 2 * (precision * recall) / (precision + recall)

print("Accuracy: %", format(accuracy.numpy()*100))
print("Precision: %", format(precision.numpy()*100))
print("Recall: %", format(recall.numpy()*100))
print("F1-score: %", format(f1.numpy()*100))

73/73 ————— 1s 7ms/step
Accuracy: % 98.61291646957397
Precision: % 97.12837934494019
Recall: % 97.45762944221497
F1-score: % 97.29272723197937
```

Figure 6. The prediction or evaluation process

Figure 5 provides a neural network's training process result, showing the training and validation accuracy over 100 epochs. The plot starts with both accuracies at a high level, with the training accuracy beginning near 90% and quickly stabilizing close to 100%. This indicates that the model effectively learns or memorizes the training data. On the other hand, the

validation accuracy, which assesses the model's generalization ability on unseen data, begins similarly high but experiences a sharp drop and recovery in the early epochs. This fluctuation suggests initial overfitting, where the model too closely learns the specifics of the training data, including noise and anomalies, before stabilizing.

As the training progresses beyond about 20 epochs, both accuracy curves show little change, indicating that the model has largely converged and additional training does not significantly enhance performance. The validation accuracy remains consistently below the training accuracy but still high, generally above 95%, demonstrating that the model generalizes well to new data.

The consistent and high validation accuracy toward the later epochs suggests that the model is well-tuned and could perform effectively on similar unseen data. The close tracking of the validation accuracy with the training accuracy without a wide gap further reinforces that there is no significant overfitting at the later stages of training. This plot signifies that the neural network is robust, learning effectively, and suitable for deployment without extensive training.

Based on Figure 6, accuracy is calculated as the percentage of correct predictions. In this case, the model achieves an accuracy of 98.61%, which is exceptionally high. This indicates that the model correctly predicts the outcome most of the time. Precision measures the accuracy of positive predictions. Specifically, it reflects the proportion of true positive results in all positive cases predicted by the model. The model's precision is 97.12%, suggesting that it is correct about 97% of the time when it predicts a label or category.

Recall (or sensitivity) assesses the model's ability to identify all relevant instances correctly. A recall of 97.46% means the model identifies 97% of all actual positives, which is crucial in scenarios where missing a positive is significantly detrimental. F1-score combines precision and recall into a single metric by taking their harmonic mean. It is particularly useful when the balance between precision and recall is important. The F1-score for this model is 97.29%, which confirms the model's robustness in terms of precision and recall.

This output indicates that the model is well-tuned and performs excellently across multiple metrics, making it effective for applications requiring high reliability. The consistency between all these metrics above 97% showcases a well-balanced model that does not sacrifice one aspect (like recall) over another (like precision), ensuring an overall high performance.

4. CONCLUSION

This research evaluates the performance of a neural network model specifically designed for classification tasks using advanced machine learning techniques such as Convolutional Neural Networks

(CNNs) for the Fingerprint Recognition research area. The study focuses on a detailed assessment of key performance metrics, including accuracy, precision, recall, and F1-score. The aim is to thoroughly determine the model's efficacy in classifying data accurately and its reliability across various conditions.

The findings reveal that the neural network model is highly effective and robust, particularly in fingerprint recognition tasks. It achieved an accuracy rate of 98.61%, demonstrating its ability to identify and classify fingerprints accurately. The precision rate stood at 97.12%, indicating a reliable performance in positive predictions. The model also showed a recall rate of 97.46%, highlighting its ability to correctly identify almost all positive cases—a crucial feature in critical applications. Furthermore, the F1-score of 97.29% confirms the model's balanced performance between precision and recall.

These results highlight the potential of advanced neural networks in handling sensitive security tasks like fingerprint recognition, where high accuracy and reliability are essential. The model's impressive performance suggests it could be effectively deployed across various practical applications, from law enforcement to securing personal devices. This study reinforces the applicability of neural networks in biometric identification and sets the stage for future research to further enhance these systems' sophistication and accuracy.

Neural networks continue to lead the revolution in machine learning by handling complex patterns and large datasets effectively. This study used a well-curated test dataset to analyze the model's capabilities comprehensively. It aims to shed light on its practical applications in real-world scenarios where accurate and reliable classifications are paramount. The outcomes of this research are expected to significantly contribute to ongoing improvements in neural network architectures and their integration into increasingly automated and data-centric environments.

AUTHOR INFORMATION

Corresponding Authors

Lusiana Efrizoni, Universitas Sains dan Teknologi Indonesia, Pekanbaru, Indonesia.

Email: lusiana@stmik-amik-riau.ac.id

Authors

Sheeba Armoogum, Department of Information & Communication Technologies, Moka, Mauritius.

Mohd Zaki Zakaria, University Technology Mara, Malaysia.

<https://doi.org/https://doi.org/10.1016/j.tifs.2021.04.042>

Meiramkhanov, T., & Tleubayeva, A. (2024). Enhancing Fingerprint Recognition Systems: Comparative Analysis of Biometric Authentication Algorithms and Techniques for Improved Accuracy and Reliability. *IEEE AITU: Digital Generation*. <https://www.researchgate.net/publication/379757930>

Minaee, S., Abdolrashidi, A., Su, H., Bennamoun, M., & Zhang, D. (2023). Biometrics recognition using deep learning: a survey. *Artificial Intelligence Review*, 56(8), 8647–8695. <https://doi.org/10.1007/s10462-022-10237-x>

REFERENCE

- Chaman, S. (2022). Revolutions in Infant Fingerprint Recognition—A Survey. In D. Gupta, R. S. Goswami, S. Banerjee, M. Tanveer, & R. B. Pachori (Eds.), *Pattern Recognition and Data Analysis with Applications* (pp. 1–14). Springer Nature Singapore.
- de Alcaraz-Fossoul, J., & Narowski, M. A. (2021). Latent Fingerprint Aging in 3D: Uncovering Hidden Degradation Patterns. In J. de Alcaraz-Fossoul (Ed.), *Technologies for Fingerprint Age Estimations: A Step Forward* (pp. 159–204). Springer International Publishing. https://doi.org/10.1007/978-3-030-69337-4_6
- Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, 79, 80–105. <https://doi.org/https://doi.org/10.1016/j.patrec.2015.12.013>
- Li, Z., Liu, F., Yang, W., Peng, S., & Zhou, J. (2022). A Survey of Convolutional Neural Networks: Analysis, Applications, and Prospects. *IEEE Transactions on Neural Networks and Learning Systems*, 33(12), 6999–7019. <https://doi.org/10.1109/TNNLS.2021.3084827>
- Liu, Y., Pu, H., & Sun, D.-W. (2021). Efficient extraction of deep image features using convolutional neural network (CNN) for applications in detecting and analysing complex food matrices. *Trends in Food Science & Technology*, 113, 193–204.
- Pillin, J. A. (2019). A Systematic Approach to Fingerprint Identification via Source Probabilities. University of Leicester. Thesis. <https://doi.org/10.25392/leicester.data.10303637.v1>
- Ruizgara. (2018). *Sokoto Coventry Fingerprint Dataset (SOCOFing)*. <https://www.kaggle.com/datasets/ruizgara/socofing>
- Subitha, D., Rahul, S. G., & Uddin, P. (2024). Artificial Intelligence in Biometric Systems. *AI Based Advancements in Biometrics and Its Applications*, 47–67. <https://doi.org/10.1201/9781032702377-3>
- Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (2019). Security and Accuracy of Fingerprint-Based Biometrics: A Review. *Symmetry*, 11(2). <https://doi.org/10.3390/sym11020141>