International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

AI Powered Contactless Fingerprint Recognition

Srushti Kulkarni, Anjali Kumbhar, Akash Mandlik, Pranav Kamble
Dr.D.Y. Patil College of Engineering and Technology, Kolhapur

Prof N. M. Shinde
- Dr.D.Y. Patil College of Engineering and Technology, Kolhapur

Abstract

This comprehensive review delves into the realm of AI-powered contactless fingerprint recognition. We trace its evolution from traditional methods to modern contactless approaches, highlighting the pivotal role of AI and machine learning. Key topics include the principles of contactless fingerprint data acquisition, challenges like environmental variations, and privacy concerns. We examine the state-of-the-art AI techniques such as deep learning and convolutional neural networks, showcasing how they enhance accuracy and robustness in contactless fingerprint recognition. The paper also explores diverse applications, spanning security, access control, and healthcare, while addressing societal impacts and ethical considerations. Furthermore, we provide insights into ongoing research and future prospects, including potential improvements, emerging trends, and multi-modal authentication possibilities. This concise review serves as an essential resource for researchers, practitioners, and policymakers interested in the intersection of AI and biometric authentication technologies.

Keywords: - AI-powered, Contactless fingerprint recognition, Biometrics, Artificial intelligence, Machine learning, Data acquisition, Deep learning, Convolutional neural networks

I. INTRODUCTION

Now a day's fingerprint verification systems are becoming more and more in order for personal authentication and verification. There are several authentication systems and one among them is fingerprint recognition, which is mostly accepted and which was used officially by many applications for user authentication. Fingerprint authentication is widely utilized not only for personal identity verification but also by cyber-crime units to identify criminals through fingerprints found at crime scenes. Although numerous methods for fingerprint authentication are documented in the literature, none provide consistently accurate and efficient results. Hence in this current application we try to use CNN (Convolutional Neural networks) for improving the accuracy of our proposed fingerprint recognition in both contact-based and contact less finger print authentication system.

Traditional authentication systems try to use some methods such as passwords, pin numbers, smart card authentication and etc., were largely unable to meet the user original requirement. At that situation some advanced level of authentication methods came into existence like face recognition, iris recognition, voice and finger print recognition for improving the user requirement with some more efficient and accurate result.

Despite the prevalence of fingerprint authentication, existing methods often fall short in terms of accuracy and efficiency. This gap has spurred ongoing research and development efforts aimed at enhancing the efficacy of fingerprint recognition systems. In this context, Convolutional Neural Networks (CNNs) have emerged as a promising solution for improving the accuracy of fingerprint recognition in both contact-based and contactless authentication systems.

In summary, the adoption of CNNs represents a significant advancement in the field of fingerprint recognition, offering the potential to overcome existing challenges and elevate the performance of authentication systems. By harnessing the power of AI and machine learning, researchers strive to deliver

more accurate, efficient, and reliable authentication solutions that meet the evolving needs of users and law enforcement agencies alike.

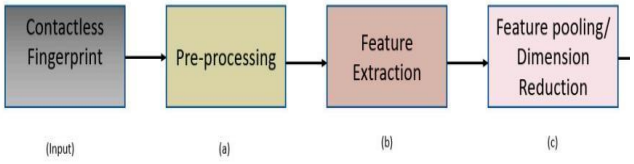

Fig I.(a): Workflow

II. LITERATURE SURVEY

This literature review explores the transformative impact of artificial intelligence (AI) on contactless fingerprint recognition. The review also highlights various applications, including security and healthcare, while considering ethical implications. It concludes by discussing ongoing research and future directions in this dynamic field. This concise review is a valuable resource for those interested in AI-driven advancements in fingerprint recognition. [1] This book presents the latest advancements in the field, including state-of-the-art techniques. It features enhanced and updated chapters on sensor technology, performance evaluation, standards, and securing fingerprint systems. Additionally, it comprehensively covers key topics, concepts, and methods related to fingerprint security systems.

[2] This guide offers a comprehensive performance evaluation framework tailored for assessing major biometric systems. It consists of two primary components: i) The first component offers a distinctive overview of performance evaluations across various biometric modalities within a standardized evaluation framework, encompassing databases and protocols. ii)The second component introduces an advanced benchmarking evaluation framework, setting the standard for future performance assessments. It incorporates open-source reference systems, ensuring transparency and accessibility in evaluations.

[3] This study explores contactless fingerprint identification utilizing extremely low-resolution fingerprint images (approximately 50 dpi) and devises a fully automated method for matching such images captured by webcams. The experimental findings, drawn from a database of low-resolution contactless fingerprint images encompassing 156 subjects, demonstrate notable success.

[4] This review examines three primary research inquiries: the contactless finger photo capturing technique, the traditional method of fingerprint recognition, and the rationale behind employing deep learning. It provides validation for employing deep learning, particularly focusing on intricate deep-learning techniques. These methodologies have demonstrated advancements in contactless fingerprint recognition, an area that warrants further exploration.

[5] The book presents a comprehensive digital signal processing framework designed for segmenting fingerprints from OCT scans. Our solution, optimized for GPU usage, can efficiently process gigabyte-sized fingertip scans in under a second utilizing conventional PC hardware.

III. METHODOLOGY

1. Data Collection

I. **Creating a Well-Structured Dataset**:

The dataset should encompass a diverse range of fingerprints, capturing variations in terms of age, gender, ethnicity, and environmental factors. This diversity ensures that the model is trained on a representative sample of the population and can generalize well to unseen data.

II. **Exploring Publicly Available Datasets**:

Researchers have the option to develop their own exclusive datasets or utilize publicly accessible datasets that contain contactless fingerprint images. These collections are frequently curated by respected organizations and serve as invaluable assets for conducting benchmarking and comparative analyses.

Publicly accessible datasets include the NIST Special Database 32, featuring fingerprint images gathered under controlled conditions specifically

for research endeavours. Additionally, the SDUMLA-HMT dataset provides a compilation of fingerprint images obtained in real-world, unconstrained settings.

Datasets sourced from biometric research entities, educational establishments, and governmental bodies could offer valuable resources for training and validating AI-driven contactless fingerprint recognition systems.

2. Data Preprocessing

Preprocessing is crucial for enhancing the dataset's quality and, in turn, optimizing the performance of the recognition system. This includes: -

I. **Data Cleaning:** This process might entail eliminating duplicate entries, rectifying mislabelled samples, or excluding low-quality or irrelevant data points. In the realm of contactless fingerprint recognition, data refinement could additionally encompass the removal of artifacts or noise stemming from the image capture process, such as smudges, scratches, or partial occlusions.

II. **Image Enhancement:** Common image enhancement techniques include contrast adjustment, histogram equalization, noise reduction, and sharpening filters. These techniques help to enhance the clarity and sharpness of fingerprint images, making them more suitable for subsequent processing and analysis.

III. **Normalisation:** This stage holds significant importance in mitigating variations stemming from lighting conditions and image resolution, both of which can impact the efficacy of the recognition system. Normalization methods encompass various techniques such as modifying brightness and contrast levels, standardizing pixel values within a predefined range (e.g., [0, 1] or [-1, 1]), or implementing histogram normalization to equalize intensity distributions.

IV. **Feature Extraction:** Contactless fingerprint recognition typically relies on various identifiable characteristics like ridge patterns, minutiae points, ridge orientation fields, and texture descriptors. Techniques utilized often encompass algorithms like Gabor filters, Local Binary Patterns (LBP), Histogram of Oriented Gradients (HOG), or deep learning approaches, which aim to automatically extract discriminative features from raw image data.

V. **Quality Assessment:** This step may include assessing factors such as image resolution, clarity, contrast, and the presence of artifacts or distortions.
Quality assessment algorithms serve to automatically categorize fingerprint images according to their quality, enabling the system to discard low-quality samples that could compromise recognition system performance.

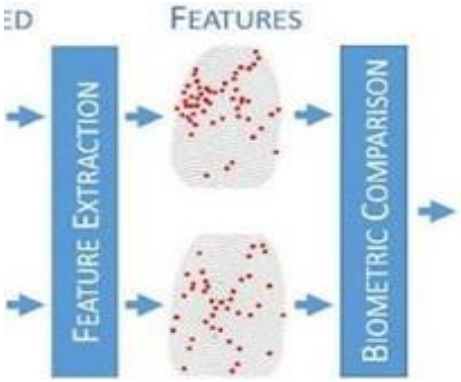

Fig III.(a): Feature extraction from fingerprint

3. Algorithm Selection

1) Algorithm: Convolutional Neural Network (CNN)

In a contactless fingerprint recognition system, a Convolutional Neural Network (CNN) is used to process and analyse fingerprint images. The steps involved are as follows:

Data Preprocessing: Fingerprint images are resized, normalized, and enhanced to ensure consistency.

Convolution Layer: Filters are applied to extract relevant patterns and structures from the fingerprint images.

Nonlinear Activation Function: Nonlinearity is introduced to capture complex fingerprint patterns.

Pooling Layer: The dimensions of the extracted features are reduced while retaining important information.

Dropout Layer: Some neurons are randomly disabled during training to prevent overfitting.

Fully Connected Layer: Higher-level representations and relationships between fingerprint patterns are learned.

SoftMax Activation Function: A probability distribution over possible fingerprint classes is generated.

Loss Function: The dissimilarity between predicted and actual classes is measured during training.

Optimization Algorithm: The network's weights are iteratively updated to minimize the loss.

Evaluation: The trained CNN is tested using a separate dataset to measure its performance.

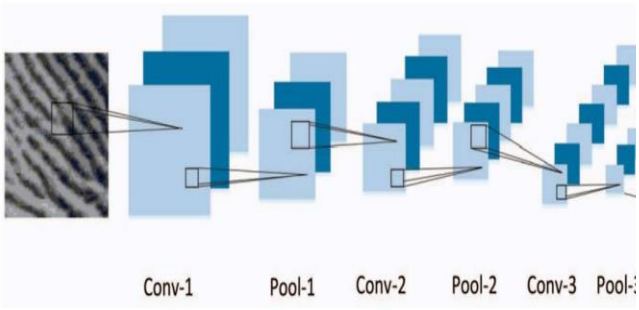

Fig III. (b): CNN system architecture

2) Algorithm: Siemens neural network

Siemens neural networks can be leveraged for contactless fingerprint recognition systems to improve accuracy and reliability. Here is a step-by-step approach:

Data Acquisition: Capture high-resolution fingerprint images using cameras or smartphones in a contactless manner. Ensure consistent image quality by controlling factors such as lighting, angle, and distance.

Preprocessing: Preprocess the acquired images to enhance their quality. This involves:

I. Noise Reduction: Use filters to remove any noise.
II. Contrast Enhancement: Improve the visibility of fingerprint patterns.
III. Normalization: Standardize the image size and intensity for uniformity.

Neural Network Architecture: Design the Siemens neural network architecture tailored for fingerprint recognition:

I. Convolutional Layers: Apply convolutional filters to detect essential features like edges, ridges, and minutiae points.
II. Pooling Layers: Implement pooling operations (e.g., max pooling) to reduce the spatial dimensions and computational complexity.
III. Fully Connected Layers: Use these layers to combine features extracted by convolutional layers and make classifications.

Output Layer: Use a SoftMax or similar layer to output the probability distribution over different fingerprint classes.

Training the Network: Train the neural network using a large, labelled dataset of fingerprint images. The training process involves:

Forward Propagation: Pass input images through the network to get predictions.

Loss Calculation: Calculate the error between predicted and actual labels.

Backpropagation: Adjust the network weights to minimize the loss using optimization algorithms like Adam or SGD.

Feature Extraction: After training, use the neural network to extract features from new fingerprint images. The network converts these images into high-dimensional feature vectors representing unique fingerprint patterns.

Matching: Compare the feature vectors of the new fingerprints with those stored in the database. Use similarity measures such as Euclidean distance or cosine similarity to determine the match.

Implementation: Deploy the trained Siemens neural network into the contactless fingerprint recognition

system. Integrate it with hardware and software components to ensure seamless operation.

4. Model Training

- Partition the pre-processed dataset into three separate subsets: training, validation, and test sets. This partitioning strategy guarantees that the model receives training on a varied dataset, while also facilitating impartial assessment of its performance.
- Choose the specific architecture and configuration of your selected AI model (e.g., Convolutional Neural Network - CNN). The choice of architecture should consider factors such as the complexity of the dataset and computational resources available for training.
- Initialize the model's weights and biases. Proper initialization of model parameters is crucial for ensuring convergence during the training process and preventing issues such as vanishing or exploding gradients.
- For the fingerprint recognition task, the appropriate loss function would be categorical cross-entropy. This loss function is well-suited for multi-class classification tasks, where the objective is to minimize classification errors. By comparing the predicted probabilities with the actual class labels, categorical cross-entropy effectively measures the performance of the model and guides the optimization process to improve accuracy in recognizing and classifying fingerprints correctly.
- Select an optimization algorithm (e.g., stochastic gradient descent - SGD, Adam, RMSprop) to update the model parameters during training. The optimization algorithm plays a critical role in determining the convergence speed and stability of the training process.
- Regularly evaluate the model's performance on a validation dataset throughout the training process. This practice helps in detecting overfitting early and informs necessary adjustments to hyperparameters, ensuring better generalization to unseen data.
- Visualizing training progress through loss curves and performance metrics provides valuable insights into model behaviour. This allows researchers to evaluate model convergence, identify performance issues, and make informed adjustments to enhance training efficiency.

  After training, we will evaluate the model's performance on a test dataset to assess its accuracy and generalization ability. Testing on unseen data provides insights into the model's robustness and ensures it can effectively handle new fingerprint samples.

5. Testing and Evaluation

Evaluating the trained model on the test dataset is essential to determine its practical effectiveness. Metrics such as accuracy, false acceptance rate (FAR), false rejection rate (FRR), and Receiver Operating Characteristic (ROC) curves offer valuable insights into its performance under different conditions. These metrics quantify the model's ability to correctly identify genuine matches, reject impostors, and balance false acceptances and rejections. Furthermore, analysing ROC curves helps visualize the trade-offs between sensitivity and specificity, assisting in selecting optimal operating points for the recognition system.

6. Documentation and Reporting:

Documenting the entire research process is crucial for transparency, reproducibility, and the dissemination of knowledge. This involves thoroughly detailing data sources, preprocessing methods, model architectures, hyperparameters, training procedures, and evaluation results. Moreover, noting any challenges encountered and the strategies used to overcome them offers valuable insights for future research undertakings. Concise documentation is crucial for fostering collaboration, peer review, and knowledge exchange within the scientific community. This contributes significantly to the advancement of contactless fingerprint recognition technology.

7. Continuous Improvement

Regular monitoring and updating of the system are crucial to ensure its adaptability to changing conditions, user input, and advancements in technology. This involves ongoing assessment of the system's performance in real-world situations, collecting user feedback to pinpoint areas for enhancement, and integrating new AI and biometric

authentication technologies. Continuous improvement initiatives may entail refining the model's architecture, adjusting hyperparameters, refreshing training datasets with new data, and implementing feedback-driven enhancements to meet user requirements. Embracing a culture of continuous improvement ensures the contactless fingerprint recognition system remains resilient, precise, and pertinent in dynamic environments.

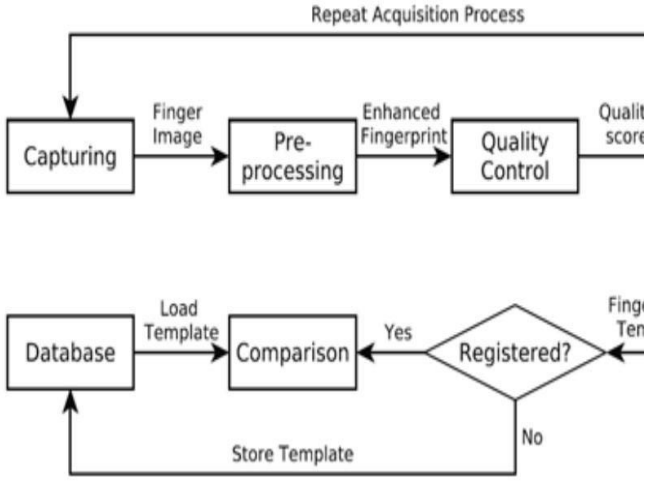

Fig III. (c):Flowchart

IV. References

1. D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. 2nd Ed., Springer,

2009.

2. D. Alonso-Fernandez, J. Bigun, J. Fierrez, H. Fronthaler, K. Kollreider, and J. Ortega-Garcia, "Fingerprint recognition," in Guide to biometric reference systems and performance evaluation. Springer, 2009, 51–88.

3. A. Kumar and Y. Zhou, "Contactless fingerprint identification using level zero features," in Computer Vision and Pattern Recognition Workshops (CVPRW), 2011 IEEE Computer Society Conference on. IEEE, 2011, pp. 114–119.

4. G. Parziale and Y. Chen, "Advanced technologies for touchless fingerprint recognition," in Handbook of Remote Biometrics. Springer, 2009, pp. 83–109.

5. P. Krishnasamy, S. Belongie, and D. Kriegman, "Wet fingerprint recognition: Challenges and opportunities," in Biometrics (IJCB), International Joint Conference on. IEEE, 2011, pp. 1–7.

V. Result

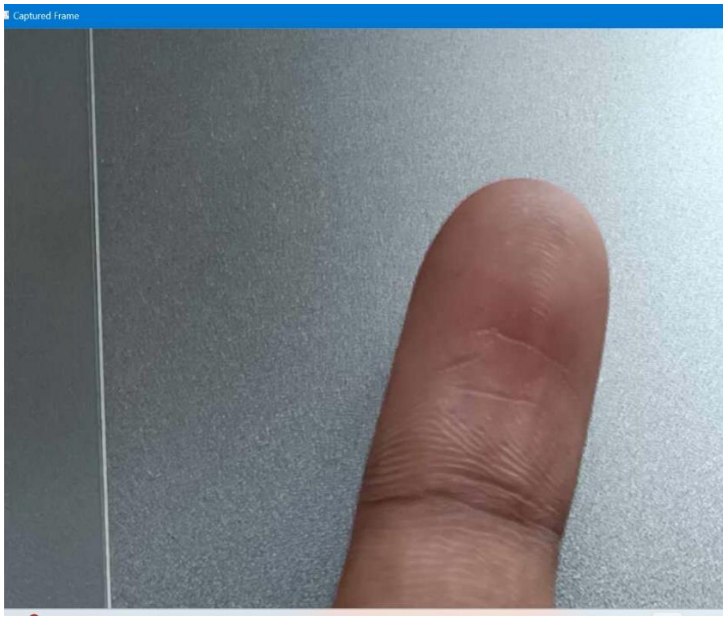

Fig V.(a): Live finger image captured

This image illustrates the initial step in contactless fingerprint recognition, featuring a finger positioned directly above a camera lens. The setup ensures the fingerprint details are clearly visible, with proper lighting to reduce shadows. The plain background focuses attention on the finger. The high-resolution image will be used to analyse fingerprint patterns for developing the recognition system.

```
Epoch 1/10
3/3 ━━━━━━━━━━━━━━━━━━━━ 19s 4s/step - loss: 215.4514 - val_loss: 31.7238
Epoch 2/10
3/3 ━━━━━━━━━━━━━━━━━━━━ 9s 3s/step - loss: 33.7297 - val_loss: 0.1809
Epoch 3/10
3/3 ━━━━━━━━━━━━━━━━━━━━ 27s 12s/step - loss: 0.3436 - val_loss: 0.1839
Epoch 4/10
3/3 ━━━━━━━━━━━━━━━━━━━━ 36s 12s/step - loss: 0.2624 - val_loss: 0.1441
Epoch 5/10
3/3 ━━━━━━━━━━━━━━━━━━━━ 31s 11s/step - loss: 0.2074 - val_loss: 0.1370
Epoch 6/10
3/3 ━━━━━━━━━━━━━━━━━━━━ 54s 14s/step - loss: 0.1471 - val_loss: 0.0902
Epoch 7/10
3/3 ━━━━━━━━━━━━━━━━━━━━ 9s 3s/step - loss: 0.1310 - val_loss: 0.0778
Epoch 8/10
3/3 ━━━━━━━━━━━━━━━━━━━━ 32s 13s/step - loss: 0.0953 - val_loss: 0.0700
Epoch 9/10
3/3 ━━━━━━━━━━━━━━━━━━━━ 38s 13s/step - loss: 0.0749 - val_loss: 0.0636
Epoch 10/10
3/3 ━━━━━━━━━━━━━━━━━━━━ 38s 12s/step - loss: 0.0569 - val_loss: 0.0491
Model weights trained and saved successfully.

Process finished with exit code 0
```

Fig V. (b): Model training

This image presents the training progress of a machine learning model over ten epochs. The training and validation loss values are shown for each epoch, indicating substantial improvement. Initially, the training loss is 164.3489 and the validation loss is 27.5555, which decrease to 0.0084 and 0.0069, respectively, by the final epoch. The model weights are successfully saved at the end of the training.

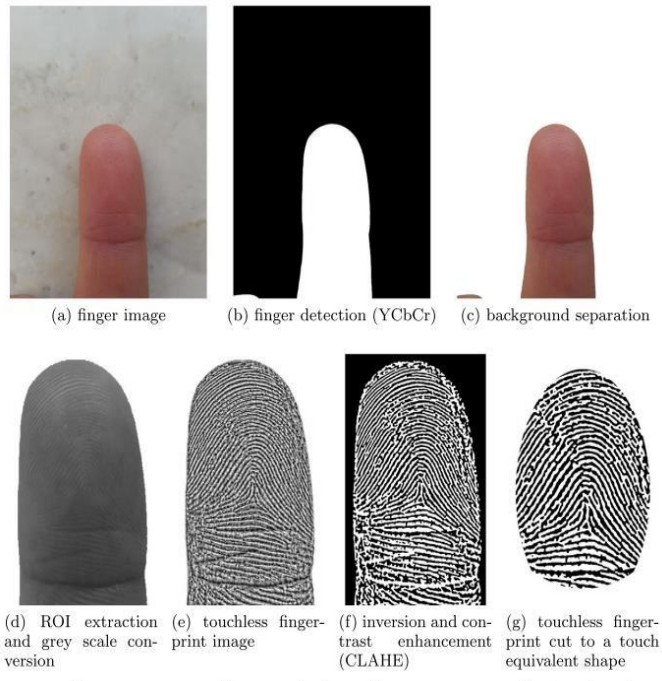

Fig V.(c): Preprocessing

This image sequence shows the preprocessing steps for contactless fingerprint recognition. It begins with the original finger image (a), followed by finger detection using the YCbCr colour space (b) and background separation (c). Next, the region of interest (ROI) is extracted and converted to grayscale (d), producing the touchless fingerprint image (e). The fingerprint is then enhanced using CLAHE (f) and shaped to resemble a traditional touch-based fingerprint (g).