Acta Scientific COMPUTER SCIENCES

Volume 6 Issue 6 June 2024

Research Article

Fingerprint Recognition Using the HoG and Lime Algorithm

V Kakulapati*, Shaik Subhani, Deepthi Madireddy, Ramavath Mounika and Ananthoju Bhargavi

Sreenidhi Institute of Science and Technology, Yamnampet, Ghatkesar, Hyderabad, Telangana, India

***Corresponding Author:** V Kakulapati, Sreenidhi Institute of Science and Technology, Yamnampet, Ghatkesar, Hyderabad, Telangana, India.

Received: May 02, 2024

Published: May 10, 2024

Abstract

This biometrics study focuses on the identification of people via fingerprint recognition. Investigate the use of this kind of system. One of the most popular techniques for identifying individuals is fingerprint recognition, which is widely acknowledged. To generate an accurate model for fingerprint identification, this study uses machine learning techniques. The model is tested and trained using a dataset of genuine and highly altered fingerprints, and it achieves a 95% accuracy on the test set. The work integrates Lime (Local Interpretable Model-agnostic Explanations) for interpretability with the Histogram of Oriented Gradients (HOG) for feature extraction. Preprocessing images, training models, and a demonstration of real-time fingerprint recognition are all part of the project structure. This technique is useful in real-world scenarios for biometric authentication, safe access control systems, and forensic investigations. It provides a stable fingerprint recognition system that could enhance security and identity verification.

Keywords: Bi-metric; Lime; Finger; Security; Accuracy; Lime; HOG; Model; ML; Genuine; Imposter; Dataset

Introduction

Physiological or behavioral traits of the human body are used by biometrics technology to authenticate users. This is an image-processing program that has two modes: enrollment and recognition. During the registration process, biometric data is obtained from a sensor and then saved in a database, along with the user's identification. During the process of recognition, the biometric data is obtained again from the sensor and then compared to the data that has been saved to establish the identification of the user. Biometric recognition relies on the distinctiveness and enduring nature of biometric data, ensuring that there are no similarities between various sets of biometric information. Biometrics includes physiological and behavioral traits such as fingerprints, palm prints, iris patterns, facial features, DNA, hand structure, and retinal patterns. Biometric systems have two distinct stages: enrollment and recognition [1].

The graphic patterns of ridges and valleys on fingers that finish and split into minutiae are called fingerprints. Two fundamental presumptions underpin fingerprint identification: singularity and invariance. Fingerprint identification is based on the concept of Invariance, which refers to the constant and unchanging properties of a person's fingerprint throughout their lifetime [2,3].

Fingerprint recognition using Lime involves integrating Lime into the fingerprint recognition pipeline to generate interpretable explanations for individual fingerprint recognition decisions. order to clarify the variables impacting each prediction, Lime fits interpretable surrogate models while varying the input fingerprint pictures [4]. These explanations enhance users' comprehension of the rationale behind a specific choice made by the model, hence promoting belief and trust in the identification of fingerprints method.

Objective of the project

The identification of fingerprints is one of the most reliable and widely utilized biometric authentication methods available today, offering secure and efficient identity verification for a variety of businesses. The increasing complexity of machine learning models used in fingerprint identification systems has raised concerns about their interpretability and openness, hindering their widespread adoption and trust.

To address this challenge, scientists have created a framework known as Lime (Local Interpretable Model-agnostic Explanations). Lime provides explanations that are interpretable at a local level for the predictions provided by machine learning models, including those used in fingerprint identification. Lime enhances the interpretability, transparency, and reliability of fingerprint recognition systems by identifying the specific factors that influence each prediction. This facilitates the implementation of these systems in many practical situations.

The fundamental purpose of fingerprint identification utilizing Lime is to improve the accessibility, comprehensibility and trustworthiness of biological authentication systems—especially those

based on complex machine learning models. Lime enables users, including security specialists, forensic analysts, and end users, to understand and confirm the system's behavior by providing clear reasons for fingerprint recognition choices. This improves the reliability, credibility, and user-friendliness of the system in many practical applications.

Overall, Lime fingerprint identification offers a solid basis for connecting advanced machine learning techniques with real-world uses in biological authentication. Lime enhances the transparency and reliability of fingerprint identification systems by addressing the interpretability issue that emerges with complex machine learning models. Consequently, this aids in the widespread adoption of these technologies across other sectors.

Figure 1: Fingerprint.

The subsequent sections of this study are as: Sec 2 delves into the existing literature and highlights the mainly significant sources of the proposed system. Also, in Sec 3 the implementation methodology, the intent of HOG, and the LIME method. Sec 4 explores the evaluations obtained from the implementation analysis discussed. Finally, Sec 5 provides concluding remarks followed by future work objectives.

Literature Survey

Fingerprint recognition is a sophisticated and detailed method of pattern recognition used for identification employing biometric data. Designing and architecting may be challenging, particularly when working with low-quality picture-capturing equipment [5]. Issues emerge when tiny details become apparent on little fingerprint spots that are not recorded by cameras. It is incorrect to think that fingerprint identification is a fully resolved method for authentication since it still presents challenges because of its complicated and detailed pattern recognition system for identifying individuals [6].

Many domains, including computer vision, robotics, image identification, and voice processing, benefit greatly from the use of deep learning techniques (DL). They are very beneficial in automated fingerprint recognition systems (AFRS) for tasks such as fingerprint pre-processing, quality enhancement, feature extraction, security, and performance improvements. Nevertheless, there is a dearth of studies on the use of deep learning in the modeling of fingerprint biometrics for various tasks within the identification process [7]. This study provides a comprehensive assessment of the literature and analysis of data from the last ten years on the use of Deep Learning in Automatic Facial Recognition Systems (AFRS), with a specific emphasis on models using Convolutional Neural Networks [8].

By employing a pre-processing phase that allows for grayscale photographs on RGB bands and combine them to generate color images, this work provides a deep-learning approach for fingerprint recognition. In order to facilitate the process of making decisions, a technology called deep convolution network is used to recover the fingerprint pictures [9,10]. The technique demonstrates an accuracy above 99.43% and 99.53% when applied to the respective variants.

This paper gives a fresh, thorough implementation based on a decentralized authentication system that uses cryptosystems to safeguard personal privacy. In order to perform matching tasks inside encrypted domains, the system utilizes Finger code templates and Homomorphic encryption [11]. The system has been effectively used and validated in practical situations, showcasing its suitability in conditions where preserving data secrecy is essential and computational performance is acceptable. This approach effectively safeguards against unwanted utilization of biometrics data and the collection of information for user verification [12].

The study discusses the incorporation of machine learning techniques to create fingerprint algorithms for classification that rely on uniqueness features. This approach aims to decrease the number of compares required in automatic fingerprint recognition systems that handle massive data sets [13]. Utilizing computer vision methods for picture pre-processing enhances computational performance, improves the quality of input images, and increases the efficiency of feature extraction [14]. Based on the findings, the Support Vector Machine (SVM) demonstrates superior performance, with an accuracy of at least 95.5%, in two out of the three databases. On the other hand, the Random Forest (RF) technique obtains the maximum accuracy, exceeding 96.75%, across all three datasets.

According to the source cited as [15], there is a heuristic approach available for detecting fingerprints by analyzing anomalies. Nevertheless, this study does not prioritize enhancing image quality since it utilizes singularity point locations. The Galton-Henry classification technique utilizes parallel training and rotation-invariant distance [16] to achieve optimal system time efficiency. Random Forest (RF) is an effective method for quickly handling large-scale datasets. It is capable of solving multi-class classification issues, as well as jobs including categorization and regression. It is an approach to supervised machine learning used to tackle issues associated with regression and classification. An important use of RF is in identifying human body parts based on depth data,

which showcases its effectiveness in solving real-world machine learning challenges. The objective of these algorithms is to enhance the quality and precision of images while lowering the time required by the system [17].

Methodology

The conceptual model that outlines the composition, actions, and perspectives of a system is called a systems architecture, or simply systems architecture. An architectural description is a structured and precise account and depiction of a system. Arranged in a manner that facilitates logical analysis of the system's architecture and activities.

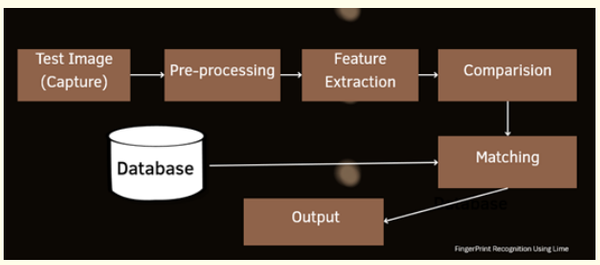

Figure 2: Framework of the proposed System.

SVM (Support Vector Machine)

It is a method for supervised ML that is used to address classification and regression issues. In the field of fingerprint identification, SVM are often used for binary classification tasks. Specifically, SVM is used to differentiate between authentic and fraudulent fingerprints. The SVM algorithm, as described in reference [18], operates by identifying the hyperplane that optimally isolates the data points belonging to distinct classes within a space of features of high dimensionality. The objective is to optimize the margin between different classes while decreasing the number of categorization mistakes.

In fingerprint recognition, SVM utilizes extracted features (such as minutiae points or texture descriptors) to learn a decision boundary that separates genuine and impostor fingerprints. It can handle non-linear decision boundaries using kernel functions like the radial basis function (RBF) kernel.

HOG (Histogram of Oriented Gradients): It is a feature descriptor used for object detection and image classification tasks. It captures the local gradient orientation information in an image to represent its texture and shape characteristics. It is used to apply feature extraction on fingerprint pictures, specifically to get feature vectors that describe the distribution of gradient orientations inside local image patches. The feature vectors are then used to train a biometric classification algorithm, such as a Support Vector Machine [19].

The distinct ridge patterns seen in fingerprint photos may be captured using HOG features as they are resilient to variations in illumination and picture noise. LIME is a method used to clarify the predictions made by intricate models such as support vector machines (SVM) or deep neural networks. The method helps users in comprehending the rationale behind a model's specific result by offering localized explanations for specific projections [20].

The LIME technique may be utilized for fingerprint identification to provide explanations for the classification decisions made by the SVM classifier. The system generates clear visual representations of how certain characteristics of fingerprint images impact the outcome of the categorization process.

Implementation Result

The objective of using Lime is to improve the clarity and understandability of fingerprint recognition algorithms. In order to provide clear and understandable reasons for categorization judgments at a local level, our system integrates Lime into the fingerprint identification workflow.

Biometric Data Collection: The technique first collects fingerprint data from several sources, such as databases or fingerprint sensors. High-quality fingerprint scans are essential for precise identification.

Preprocessing and Feature Extraction: An first round of processing is applied to the collected fingerprint pictures in order to minimize noise and improve clarity. Subsequently, the technique of extraction is used to get distinctive characteristics from the fingerprint photographs.

Training of a Fingerprint identification Model: A fingerprint identification model is trained using machine learning or deep learning techniques. This model has been trained to accurately distinguish and classify fingerprint scans as either authentic or counterfeit.

The incorporation of Lime into the trained fingerprint recognition model enables the provision of locally interpretable explanations for categorization decisions. Lime analyzes each fingerprint picture individually, identifying the distinctive features and regions that have the most significant impact on the categorization outcome.

Interpretability and Openness: Users are provided with justifications generated by Lime, which aid in their understanding of why a particular fingerprint was classified as either real or fake. This enhances the openness and dependability of the fingerprint recognition technology.

Evaluation and verification According to Lime's explanations, users have the ability to provide comments on the classification choices. Over time, this feedback loop contributes to enhancing the reliability and precision of the fingerprint recognition model.

Assessment: The effectiveness of the approach is assessed by measuring indicators such as satisfaction among users, understanding, and correctness.

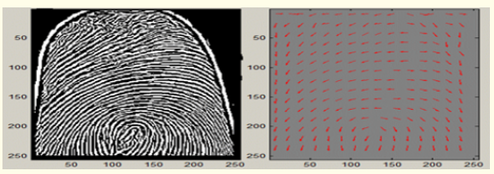

Figure 3: Fingerprint Gradients.

LIME perturbs the input characteristics in the vicinity of a particular instance and monitors the corresponding changes in predictions made by the model. The effectiveness of the intricate model in relation to the specific scenario is then evaluated by fitting a localized comprehensible model, which provides valuable insights into the decision-making procedure of the model.

Figure 4: Validation result for Sample Fingerprint.

Accuracy: 87%

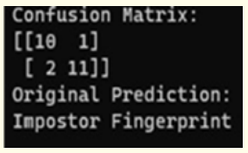

Figure 5: Predicted Impostor Fingerprint.

Figure 6: Another Sample Fingerprint for validation

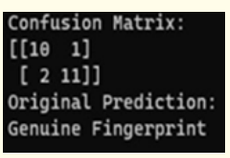

Figure 7: Predicting Genuine Fingerprint.

Conclusion

In this study, we utilized Lime to classify fingerprint scans as either genuine or counterfeit. Lime has provided reliable and transparent insights into the decision-making process of our fingerprint recognition system via careful integration and interpretation. This accomplishment showcases Lime's capacity to enhance the comprehensibility and dependability of biometric identification methods, hence paving the way for their extensive utilization and adoption in diverse sectors.

Future Enhancement

In the future, developments in technology will employ deep learning and pre-processing methods to enhance the accuracy of classifying contactless fingerprints. These strategies have the potential to enhance the efficiency of feature extraction, reduce picture processing time, and improve identification accuracy. The challenges encompass rapid identification in diverse applications, secure and reversible fingerprint templates, distance-based fingerprint authentication, and scientific verification of fingerprint uniqueness.

Bibliography

1. Ali Mouad., *et al*. "Overview of Fingerprint Recognition System". Conference: 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), At DMI College of Engineering, Palanchur, Nazarethpet, Chennai, Tamil Nadu, India (2016).

2. NK Ratha., *et al*. "A real-time matching system for large fingerprint databases". IEEE Trans. Pattern Anal. Mach Intell 18.8 (1996): 779-813.

3. AK Jain and L Hong. "Online fingerprint verification". IEEE Trans. Pattern Anal. Mach Intell 19.4 (1997): 302-341.

4. Ali Mouad., *et al*. "Overview of Fingerprint Recognition System" (2016).

5. Prasad Puja., *et al*. "A Survey of Fingerprint Recognition Systems and Their Applications". (2019).

6. V J Rathod., *et al*. "A survey on fingerprint biometric recognition system". 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Greater Noida, India, (2015): 323-326.

7. Chiroma Haruna. "Deep Learning Algorithms based Fingerprint Authentication: Systematic Literature Review". *Journal of Artificial Intelligence and Systems* 3 (2021):157-197.

8. N Shuping and W Feng. "The research on fingerprint recognition algorithm fused with deep learning". 2020 IEEE International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA), Chongqing, China, (2020): 1044-1047.

9. Diarra Mamadou., *et al*. "Study of Deep Learning Methods for Fingerprint Recognition". *International Journal of Recent Technology and Engineering (IJRTE)* 10 (2021): 192-197.

10. J Zhang., *et al*. "Fingerprint Recognition Scheme Based on Deep Learning and Homomorphic Encryption". 2022 3rd International Conference on Information Science and Education (ICISE-IE), Guangzhou, China, (2022): 103-107.

11. Barni Mauro., *et al*. "A privacy-compliant fingerprint recognition system based on homomorphic encryption and Fingercode templates". Proc. IEEE Int. Conf. Biometrics: Theory Applications and Systems (2010): 1-7.

12. Kalle Karu and Anil K Jain. "Fingerprint classification". *Pattern Recognition* (1996).

13. K Delac and M Grgic. "A survey of biometric recognition methods". Proceedings. Elmar-2004. 46th International Symposium on Electronics in Marine, Zadar, Croatia, (2004): 184-193.

14. Nguyen HT and Nguyen LT. "Fingerprints Classification through Image Analysis and Machine Learning Method". *Algorithms* 12(2019): 241.

15. Karu K and A Jain. "Fingerprint Classification Pattern Recognition". Elsevier: Amsterdam, The Netherlands, (1996): 389-404.

16. Nyongesa H and Al-khayatt S. "Fast robust fingerprint feature extraction and classification". *Journal of Intelligent and Robotic Systems* 40 (2000): 103-112.

17. Nagaty K. "Fingerprints classification using artificial neural networks: A combined structural and statistical approach". *Neural Networks* 14 (2001): 1293-1305.

18. V Kakulapati., *et al*. "A Novel Multimodal Risk Disease Prediction of Covid-19 by Using Hierarchical LSTM Methods", "Taylor and Francis book" Data Science and Data Analytics: Opportunities and Challenges".

19. Kobayashi Takumi. "BFO Meets HOG: Feature Extraction Based on Histograms of Oriented p.d.f. Gradients for Image Classification. Proceedings / CVPR, IEEE Computer Society Conference on Computer Vision and Pattern Recognition". IEEE Computer Society Conference on Computer Vision and Pattern Recognition (2013): 747-754.

20. Rodríguez-Pérez Raquel and Bajorath Jürgen. "Explainable Machine Learning for Property Predictions in Compound Optimization: Miniperspective". *Journal of Medicinal Chemistry* 64 (2021).