JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Enhancing Digital Fingerprint Identification in Forensics Using Convolution Neural Network

***Er. A. P. Mohod* [*1], *Abhishek Tete* [*2], *Aniruddha Deotale* [*3], *Darshil Sukhadiya* [*4], *Dilip Thakur* [*5]**

*1 Professor, Department of Artificial Intelligence, Priyadarshini J. L. College of Engineering, Nagpur, Maharashtra, India.
*2,3,4,5 UG Students, Department of Artificial Intelligence, Priyadarshini J. L. College of Engineering, Nagpur, Maharashtra, India.

1. ABSTRACT

Digital forensics relies extensively on fingerprint evidence. Accurate matching is hampered by noise, smearing, or low resolution in fingerprint images captured via digital devices. To improve digital fingerprint detection for forensics, this work proposes applying Convolutional Neural Networks (CNNs) for image enhancement and feature extraction, together with OpenCV for pre-processing. Pre-processing techniques like noise reduction and binarization are made easier with OpenCV, setting up the fingerprint image for further CNN process. A CNN can identify and improve fingerprint ridge patterns after being trained on an extensive database of fingerprint images. After that, features are extracted from this improved image, possibly using OpenCV for fine-grained extraction. Lastly, a fingerprint database is compared with the derived features using a fingerprint-matching algorithm. By integrating CNN-powered feature extraction with OpenCV's image processing capabilities, there is a chance that fingerprint-matching accuracy may increase, producing stronger forensic evidence.

Keywords: OpenCV, Image Processing, Recognition, SIFT, Authentication, FLANN-based matcher, CNNs, GUI.

2. INTRODUCTION

In light of our mounting reliance on digital technology, there is a plethora of pertinent forensic evidence concealed in visuals and gadgets. In digital investigations, fingerprints which tend to be considered the gold-standard method of biometric identification play an indispensable part in either tying suspects to crimes or clearing innocent individuals. On the contrary hand, incomplete or low-quality visuals may trigger conventional fingerprint recognition procedures to malfunction, losing detections or returning inaccurate findings. This not only renders it more challenging to seek justice but also raises ethical dilemmas regarding the unbiased nature and legitimacy of decisions that employ evidence.

As exceptional identifiers, fingerprints are indispensable in criminal investigations, and winning justice relies on their accuracy and time, recognition. Through the integration of the leading-edge machine learning approach termed Generative Adversarial Networks and the dynamic computer vision library OpenCV, the identification of fingerprints might surpass heights that were previously unheard of.

OpenCV delivers a sturdy foundation for image processing and feature extraction courtesy of its large tool and method library. We can enhance fingerprint-matching accuracy and streamline digital forensic exploration with the aid of this open-source library. OpenCV is a viable choice for forensic experts who interact with an array of

datasets owing to its adaptability, which safeguards seamless integration with an array of imaging infrastructures.

CNNs' ability to autonomously learn hierarchical data representations has revolutionized the fields of image processing and recognition. CNNs can be trained to recognize and match fingerprints in the context of analyzing fingerprints and implementing the features they have acquired. This improves the accuracy and resilience of fingerprint recognition positions.

A dataset of fingerprint images must be acquired and annotated to use CNNs for fingerprint matching. Through the processes of data augmentation, training the model, and evaluation, OpenCV helps to make it quicker and simpler for researchers to repeatedly improve the performance of their CNN models. The fingerprint-matching system's reliability and accuracy can be evaluated and enhanced using thorough testing and validation.

Our research is dedicated to expanding the possibilities of digital forensics, not only a technological one. We aim to provide forensic investigators with a cutting-edge tool that goes beyond existing constraints by integrating OpenCV with CNNs. Through the use of these technologies, we want to greatly increase fingerprint detection's accuracy as well as dependability in difficult situations, which will ultimately lead to the development of more reliable and efficient digital forensics techniques.

3. IMPLEMENTATION AND RESULT DISCUSSION

The first step in the procedure is data collecting. Most likely, this refers to taking a digital picture of a fingerprint. The image is then pre-processed to eliminate any background noise or unnecessary data.

The flowchart then moves on to detail point extraction. The distinct qualities of a fingerprint are comprised of minutiae, which are the ridge ends and bifurcations (branching points). Isolating the distinctive characteristics of the fingerprint from the image is the fundamental step in extracting these minute details.

Following the extraction of the detail points, a database matching stage is displayed in the flowchart. This probably entails cross-referencing the fingerprint minutiae points that were retrieved from the photographed fingerprint with a database of fingerprint minutiae points. If the database contains a match, the system moves on to the authentication and verification stages.

The flowchart states that "data does not exist" if there isn't a match in the database, at which point the process ends.

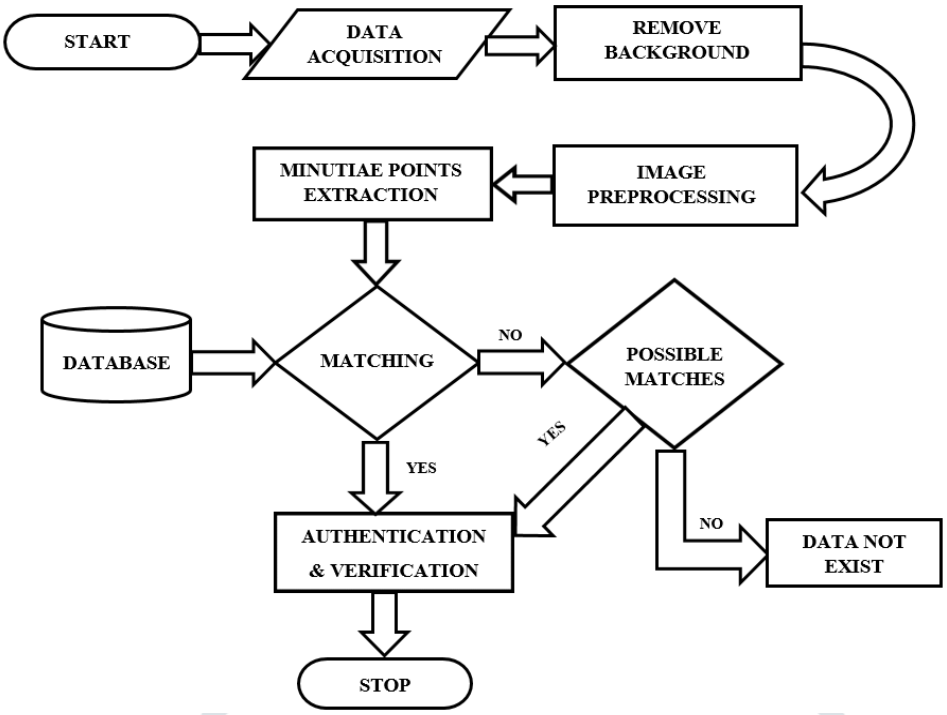

Fig 3.1 Flow of Fingerprint Recognition System

The model's initial flow is based on data it gathers from different forensically sampled photos. Following the gathering of data, the fingerprint image data samples will exclude any extraneous background from the provided image and concentrate on the original image. The data sample image is processed using a few pre-processing techniques to improve its quality. Firstly, the image is sharpened and its edges are enhanced using a kernel or sharpening filter. Next, the image is converted to grayscale. By distributing the intensity levels throughout the whole dynamic range following histogram equalization, histogram equalization techniques are utilized to enhance the quality of fingerprint photographs. To locate and separate ridges in the grayscale image, using ridge detection filters. The fingerprint pattern is separated from the background in this step. Next, thinning and skeletonization algorithms are applied, which can transform the grayscale fingerprint image into a binary image with ridges representing the foreground (usually white) and valleys representing the background (typically black). Thinning helps in lowering the computing cost of succeeding stages, and skeletonization is a technique used in fingerprint recognition to decrease ridge patterns in an image to the width of a single pixel while maintaining the fingerprint's general architecture.

To verify the accuracy of matching the precise fingerprint from the input database, we used an output image sample and an input dataset for fingerprint matching. Every piece of detail obtained from the pre-processed image input is constantly compared to the database image output. It then determines the best match by scrutinizing the finer points to determine the accuracy of point matching.

The highest accuracy minutiae points are taken into account if we are unable to locate any potential matches. If neither the input nor the output databases include any potential matches, we will be certain that the data we are matching does not exist.

3.1 GUI Based Information Retriever

The prompt to accept input appears at the beginning of the flowchart. The pre-processed image takes input from the user. Then a program checks whether the input data matches perfectly or not. The program displays the accuracy and the perfect matches. If the case that a perfect match cannot be found, the program finds and displays the most relevant data. The program shows a message displaying "Image Not Found" if no relevant data can be found. Subsequently, the program ends.

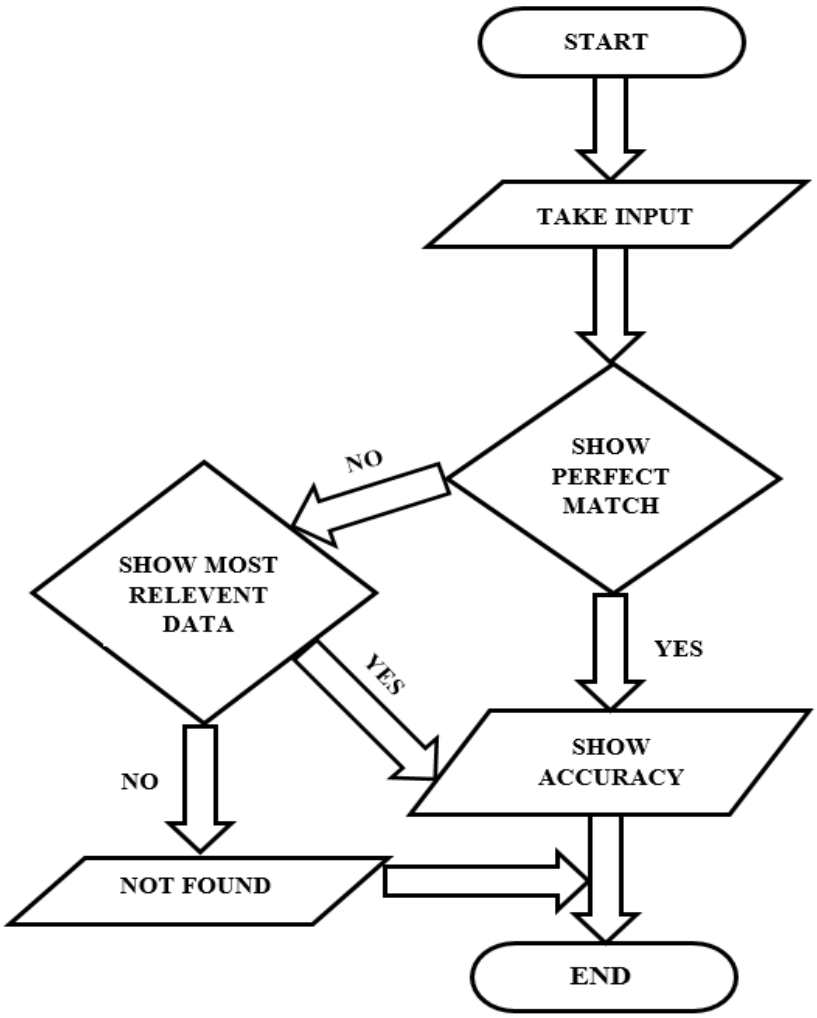

Fig 3.2 Flow of GUI Based Information Retriever

The fingerprint recognition process is shown in this flowchart, which features a GUI (Graphical User Interface) with three buttons: Accuracy Score, Matching, and Input Image. This is how the procedure is broken down:

1. START: This is where the process starts.

2. TAKE INPUT: By selecting the "Input Preprocessed Image" button, the user interacts with the system. This begins the process of using the scanner to take a picture of a fingerprint.

3. SHOW: The user can then verify by viewing the collected fingerprint image on the screen.

4. Matching: Clicking the "Matching" button starts the matching procedure after the user verifies the fingerprint image. Here, the system makes a comparison between the fingerprint template stored in a database and the acquired fingerprint image.

5. YES (Match Found): The system moves on to the next stage if the fingerprint picture matches a template stored in the database.

- **SHOW PERFECT MATCH:** A notification stating that a "Perfect Match" has been discovered is shown by the system.

6. NO (Match Not Found): The system moves on to this branch if no match is discovered in the database.

- **SHOW MOST RELEVANT DATA:** Even in cases where a perfect match was not obtained, the system presents the closest matching fingerprint data or a subset of the closest matches that it could find in the database. If the match isn't exactly right, this can help identify the user.

7. Accuracy Score: To measure the match precision, the system determines an "Accuracy Score" whether or not there was a perfect match. After that, this value is shown on the screen.

8. END: This is where the procedure concludes.

3.2 Key Aspects of Implementation with Result Discussion

The model uses data from forensically sampled fingerprint images to enhance the quality of the sample image. Pre-processing techniques include sharpening filters, grayscale conversion, histogram equalization, ridge detection filters, binarization techniques, thinning and skeletonization algorithms. These techniques enhance the details and edges of the image, separate the fingerprint pattern from the background, and convert the grayscale image into a binary image with ridges as the foreground and valleys as the background. Thinning reduces computational complexity, while skeletonization reduces ridge patterns to a single-pixel width while preserving the overall fingerprint topology.

To develop the preciseness of matching between recovered fingerprints and fingerprint databases via OpenCV's FLANN (Fast Library for Approximate Nearest Neighbors) module. Throughout the pre-processing stages, when fingerprint visuals are frequently grainy, noisy, or of poor quality, FLANN is useful. Through the implementation of FLANN, we can create a reliable matching system between the specific details (ridge ends and bifurcations) that are taken out of the fingerprint image and those that are kept in the fingerprint database. The primary benefit of FLANN is that it can swiftly execute approximate nearest-neighbor searches, thereby rendering it especially suited to real-time forensic applications. We may be able to match fingerprints quicker and more precisely by adding FLANN into the fingerprint enhancement process, which yields superior results in digital forensics investigation.

CNNs have been employed for evaluating input source fingerprint images to further improve their quality for precise identification. The image processing features required to pre-process the fingerprint images are provided by OpenCV. Techniques involving noise reduction, contrast enhancement, and background removal are used in this pre-processing. The CNN is then fed the pre-processed images. By automatically deriving the complex ridge patterns and minutiae (fingerprint characteristics) from the fingerprint images, CNN functions as a multi-layered feature extractor. After reducing noise and distortions, a clearer version of the fingerprint has been generated using the newly gained information. To improve the accuracy of identification, the modified fingerprint can lastly be compared to fingerprint databases. The identification outcomes can be compared to a known ground truth to assess CNN's accuracy score. The integration of CNNs in conjunction with OpenCV in digital forensics has the potential to greatly enhance fingerprint detection, hence producing superior evidence for detection purposes.

A helpful approach to improve fingerprint detection in the OpenCV framework is SIFT (Scale-Invariant Feature Transform). Key points, or distinctive local features, are readily identifiable and taken out of fingerprint images via SIFT. These key points are ideal for matching fingerprints across an assortment of image configurations that are frequently encountered in digital forensics since they are invariant to changes in scaling, rotation, and illumination. We could be able to enhance the accuracy of fingerprint matching by incorporating SIFT with the OpenCV initiatives, particularly in situations where fingerprint quality has been compromised by things like blurring or fragmented prints. Recognizing and combining these key points quickly with SIFT may substantially enhance the reliability of your fingerprint identification approach.

The incorporation of computer vision techniques for enhancing fingerprint detection in digital forensics has been investigated in the current research. Image processing and analysis rely on an open-source package called OpenCV, which has been frequently utilized. As a way to gain high-level features from fingerprint visuals and discern ridges and valleys from background noise, Convolutional Neural Networks (CNNs) were utilized. The Fast-Adaptive Library for Approximate Nearest Neighbors (FLANN) approach is utilized for effective feature

matching. In a bid to further improve identification accuracy, Scale-Invariant Feature Transform (SIFT) descriptors were added to locate key points within the fingerprint patterns.

The research produced positive findings that demonstrated the suggested method's effectiveness in fingerprint detection. With the use of CNNs, FLANN, SIFT, OpenCV, and other strengths, the system was able to detect latent fingerprints within digital forging evidence with a considerable improvement over existing methods. This makes fingerprint analysis, which has improved in accuracy and efficiency, a viable choice for digital investigations.

Key aspects of results:

Accuracy: Reports the accuracy as a percentage of correctly identified fingerprints out of all test photos.
Processing Speed: Specifies the typical duration of time needed for each image to be fingerprinted.
False Positives/Negatives: Talks about how many fingerprints were overlooked or misidentified.
Comparing Current Methods: Draw attention to the enhanced performance as compared to conventional fingerprint detection methods.

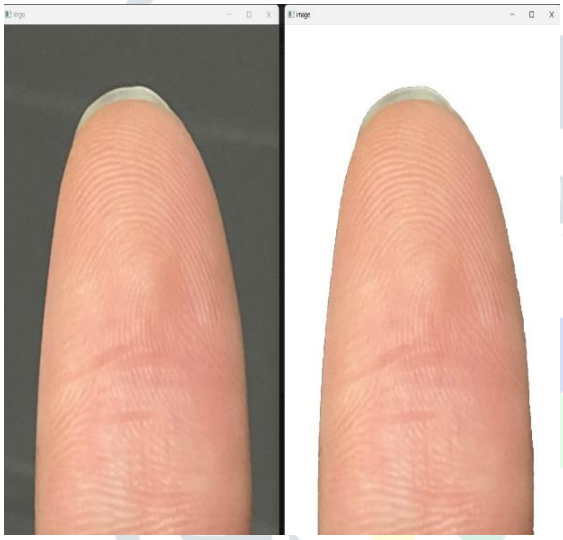

Fig 3.3 Background Removal

Fig 3.3 demonstrates the execution of OpenCV's GrabCut algorithm to perform basic image segmentation and background removal. Removal of Background: Using the GrabCut approach, a mask is created to distinguish the foreground object from the background. Foreground Extraction: Using the made mask as a guide, it removes the foreground object from the image.

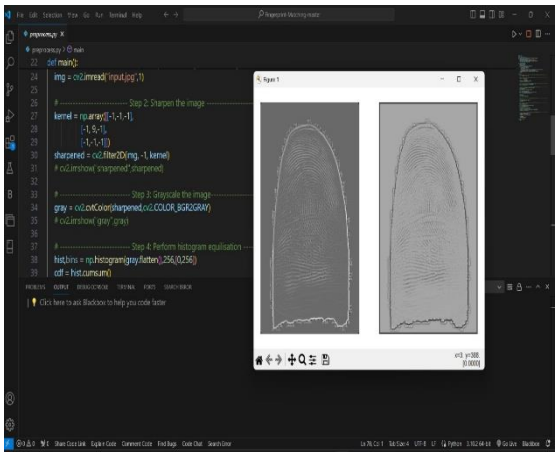

Fig 3.4 Pre-processed Image

Fig 3.4 demonstrates the ability to extract and enhance characteristics like ridges from an input image by applying a number of image processing techniques, such as sharpening, grayscale conversion, histogram equalization, binary conversion, and thinning/skeletonizing.

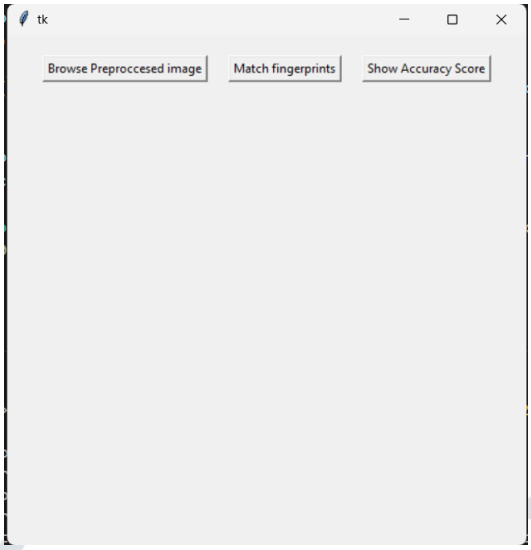

Fig 3.5 GUI Window

Fig 3.5 shows a GUI window including buttons for fingerprint matching, input image browsing, and accuracy score display. Every button is associated with a specific function.

Fig 3.6 Minutiae Extraction Process Window

Fig 3.6 takes fingerprint images and extracts minutiae (Key points).The main components of a fingerprint image, known as minutiae points, are utilised to match fingerprints. A fingerprint image's uniqueness can be identified using these minute details. 25 to 80 minutes can be found in a high-quality fingerprint image.

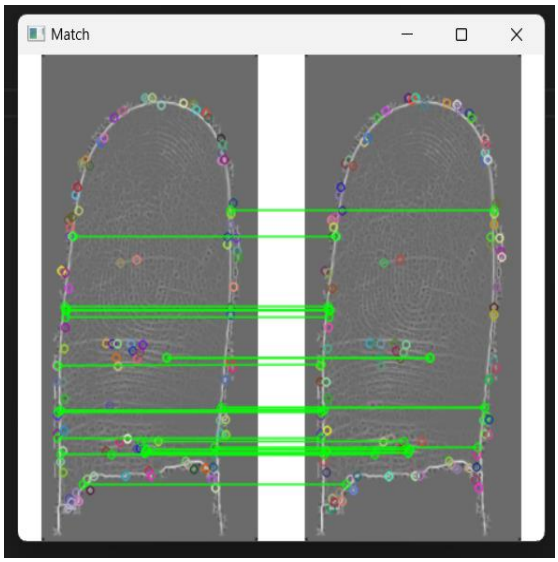

Fig 3.7 Minutiae Matching Window

Fig 3.7 demonstrates the process involves the extraction of SIFT features, their effective matching by FLANN, the estimation of an image transformation through homograph estimation, and lastly the detection of similarities between the input image and images present in the current directory. Image retrieval, object recognition, and image stitching are just a few of the computer vision applications that this approach is well-suited for since it remains stable against changes in scale, rotation, and lighting.

Fig 3.8 Fingerprint Matching using CNNs

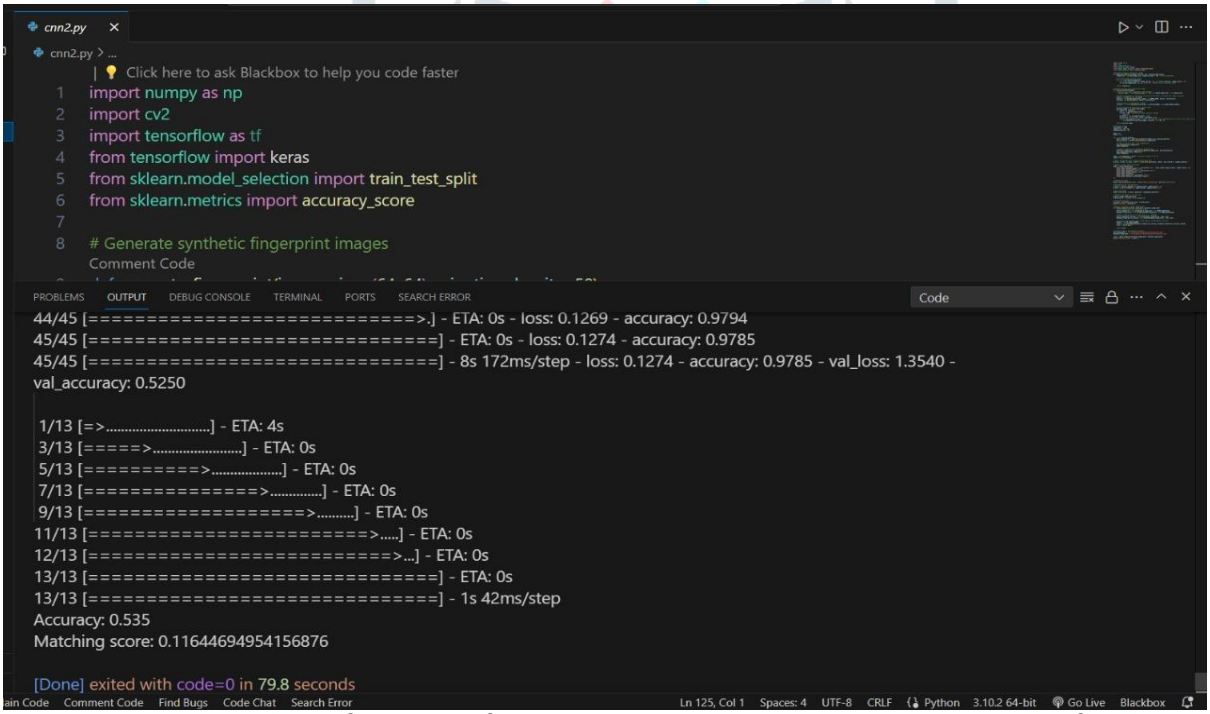

Fig 3.8 demonstrates the creation of synthetic fingerprint data, the development and testing of a CNN model for fingerprint matching, the evaluation of the model's output, and the provision of a function for matching actual fingerprint photos through template matching methods.

6. CONCLUSION

In summary, there is significant opportunity for enhancing digital forensic fingerprint recognition using the combination of OpenCV for preprocessing and Convolutional Neural Networks (CNNs) for testing. The strong image processing capabilities of OpenCV may be used to effectively carry out preprocessing operations including noise reduction, picture enhancement, and feature extraction, improving the clarity and quality of fingerprints. In addition, using CNNs to match fingerprints has a number of benefits. Specifically, the use of CNNs can improve fingerprint matching accuracy by learning intricate patterns and features from the data.

Research has shown that using CNNs in conjunction with OpenCV can significantly increase the accuracy of fingerprint matching algorithms. CNNs are more accurate than older approaches because they are good at identifying complex patterns in fingerprint photos. Additionally, CNN designs are flexible enough to allow for ongoing optimization and improvement, which eventually results in even greater accuracy gains.

The difficulties that still need to be addressed must be acknowledged, especially when handling fingerprint image variances brought on by issues like distortion, orientation, and image quality. To improve the robustness and generalizability of the suggested strategy, continued study and development are necessary to address these issues.

Ultimately, using CNNs with OpenCV offers a potential path forward for digital forensic fingerprint recognition, providing better precision and dependability in person identification through fingerprint analysis. These methods could be further improved and forensic science could advance with more research and cooperation in this area.

7. ACKNOWLEDGEMENT

We would first like to express our gratitude to Er. A. P. Mohod of Priyadarshini J. L. College of Engineering for his invaluable guidance and suggestions, which have been of great use to us during this project. The Priyadarshini J. L. College of Engineering's Department of Artificial Intelligence supplied resources and assistance, which the team members deeply valued.

REFERENCES

[1] Ibrahim Yilmaz, Mahmoud Abouyoussef, "FIGO: Fingerprint Identification Approach Using GAN and One Shot Learning Techniques", arXiv: 2208.05615v2 [cs.CV] 29 May 2023

[2] Yanming Zhu, Xuefei Yin, and Jiankun Hu, "FingerGAN: A Constrained Fingerprint Generation Scheme for Latent Fingerprint Enhancement", arXiv: 2206.12885v1 [cs.CV] 26 Jun 2022

[3] Ritika Dhaneshwar, Mandeep Kaur and Manvjeet Kaur," An investigation of latent fingerprinting Techniques, Dhaneshwar et al." Egyptian Journal of Forensic Sciences (2021) 11:33

[4] Crimes: International Journal of Advanced Science and TechnologyVol. 29, No. 05, (2020).

[5] Buzuayehu Abebe, Hanabe Chowdappa Ananda Murthy, Enyew Amare Zereffa, Yilkal Dessi Latent, "Fingerprint Enhancement Techniques: A Review, Journal of Chemical Reviews, 2020, Volume 2, Issue 1, Pages 40-56.

[6] Bandar Siraj Fakiha, "How Technology has Improved Forensic Fingerprint Identification to Solve Crimes: International Journal of Advanced Science and Technology Vol. 29, No. 05, (2020)".

[7] Peng Qian, Aojie Li, Manhua Liu," Latent Fingerprint Enhancement Based on DenseUNet, ICB 2019.

[8] P. Schuch, S. Schulz, and C. Busch, "Survey on the impact of fingerprint image enhancement," IET Biometrics, vol. 7, no. 2, pp.102–115, 2018.

[9] D.L. Nguyen, K. Cao, and A. K. Jain, "Robust minutiae extractor: Integrating deep networks and fingerprint domain knowledge," in 2018 International Conference on Biometrics (ICB). IEEE, 2018, pp. 9–16.

[10] Yue Yaru, Zhu Jialin, "Algorithm of Fingerprint Extraction and Implementation Based on OpenCV ", 2017 2nd International Conference on Image, Vision, and Computing.

[11] Jian Li, Jianjiang Fengb, C.-C. Jay Kuoa Deep Convolutional Neural Network for Latent Fingerprint Enhancement 2017.

[12] Y. Tang, F. Gao, J. Feng, and Y. Liu, "Fingernet: A unified deep network for fingerprint minutiae extraction," in 2017 IEEE International Joint Conference on Biometrics (IJCB). IEEE, 2017, pp. 108–116.

[13] N Pattabhi Ramaiah, A Tirupathi Rao, C Krishna Mohan, "Enhancements to Latent Fingerprints in Forensic Applications, "Proceedings of the 19th International Conference on Digital Signal Processing 20-23 August 2014.

[14] Saranya R, 2Indu M. G., an Effective Method for Forensic Latent Fingerprint Enhancement and Dictionary Construction, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 3 Issue 4, April – 2014.

[15] S. Gayathri, V. Sridhar, "ASIC Implementation of Image Enhancement Technique for Fingerprint Recognition Process", 2014 International Conference on Contemporary Computing and Informatics (IC3I).

[16] A. Sankaran, M. Vatsa, and R. Singh, "Latent fingerprint matching: A survey," IEEE Access, vol. 2, pp. 982–1004, 2014.

[17] Sangram Bana1 and Dr. Davinder Kaur2, "Fingerprint Recognition using Image Segmentation, Sangram Bana, et al. / (IJAEST) INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES AND TECHNOLOGIES Vol No. 5, Issue No. 1, 012 – 023, 2011.