IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305230 |

Analyzing Images for Forensic Evidence Such as Fingerprints, Footprints, and Bloodstains

Mr. R. Sathya Prakash[1], B. Uday Kiran[2], R.Shiva Sundar Bhanu[3], R. VishnuVardhan Reddy[4]

Assistant Professor, Department of Artificial Intelligence, Anurag University, Hyderabad, India[1]

Student, Department of Artificial Intelligence, Anurag University, Hyderabad, India[2 3 4]

ABSTRACT: Forensic science plays a crucial role in criminal investigations by providing valuable evidence that aids in identifying suspects and solving crimes. With the advent of digital imaging technology, there has been a significant advancement in the analysis of forensic evidence from images. In recent years, Convolutional Neural Networks (CNNs) have emerged as powerful tools for image analysis. This paper presents a comprehensive review of the application of CNNs in analyzing images for forensic evidence, focusing particularly on fingerprints, footprints, and bloodstains. forensic evidence analysis and the challenges associated with traditional methods. It highlights the limitations of manual examination and the need for automated techniques to enhance accuracy and efficiency in forensic investigations.in this we used three different datasets like fingerprints, footprints, and bloodstains using deep learning of CNN. Based on selection of input we will check whether the person is there or not in data base. if the person is available in database then the person will be criminal else the person normal.

KEYWORDS: Convolutional Neural Network, Deep Learning, Image Analysis

I. INTRODUCTION

Forensic science plays a pivotal role in modern criminal investigations, aiding law enforcement agencies in identifying suspects, reconstructing crime scenes, and establishing evidence-based conclusions. Among the array of techniques utilized in forensic investigations, the analysis of physical evidence such as fingerprints, footprints, and bloodstains holds paramount importance. These forms of evidence, widely recognized as foundational in forensic science, play a crucial role in linking individuals to crime scenes and providing crucial insights into criminal activities. Convolutional Neural Networks (CNNs), inspired by the organization of the animal visual cortex, have brought about revolutionary changes in various fields, including computer vision and pattern recognition. In recent years, CNNs have increasingly found application in forensic analysis to automate and enhance the process of analyzing forensic evidence, including fingerprints, footprints, and bloodstains. Leveraging the potent capabilities of CNNs, forensic experts can streamline workflows, improve accuracy, and extract more detailed information from physical evidence than ever before.

Fingerprints, with their unique patterns of ridges and valleys on the fingertips, stand as one of the oldest and most reliable forms of forensic evidence, capable of positively identifying individuals. CNNs have demonstrated remarkable success in fingerprint recognition tasks, facilitating automated matching against large databases and aiding in rapid suspect identification. Footprints, another prevalent type of physical evidence at crime scenes, offer valuable clues about individual identity and movements. By applying CNNs to footprint analysis, forensic investigators can accurately compare and match footwear impressions, even when traditional methods face challenges due to distortion or partial prints. Bloodstains, often encountered in violent crimes, contain critical genetic information that links perpetrators to crime scenes or victims. CNNs have shown promise in bloodstain pattern analysis, assisting forensic experts in deciphering complex spatter patterns and reconstructing events leading to bloodstain deposition.

II. LITERATURE SURVEY

Convolutional Neural Networks (CNNs) are commonly used for image classification tasks, there are alternative algorithms and techniques that can be applied to the detection and classification of fingerprints, footprints and bloodstains.

1. **An Investigation of Latent Fingerprinting Techniques (2021):**
   This paper evaluates the effectiveness of the clustered latent minutiae pattern algorithm in forensic science for identifying individuals from latent fingerprints. The study finds that the algorithm's accuracy depends significantly on the quality of the fingerprints, with clearer prints yielding better results.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305230 |

2. **Deep Learning Based Person Authentication Using Hand Radiographs: A Forensic Approach (2020):** This research employs deep learning techniques and Support Vector Machines (SVM) for authenticating individuals using hand radiographs. The study focuses on the unique skeletal features visible in x-ray images of hands for forensic identification.
3. **Deep Learning Based RF Fingerprint Identification Using Differential Constellation Trace Figure (2019):** The paper explores the use of a deep learning framework for radio frequency (RF) fingerprint identification, analyzing complex RF signal characteristics through differential constellation trace figures for secure and precise identification.
4. **Deep Learning Based RF Fingerprinting for Device Identification and Wireless Security (2018):** This research uses Recurrent Neural Networks (RNNs) to process sequential data in RF signals for device identification and enhancing wireless security, highlighting the suitability of RNNs for analyzing time-series data in RF fingerprinting.

The research papers span various forensic and security identification methods using advanced algorithms and deep learning. The 2021 paper investigates the clustered latent minutiae pattern algorithm in forensic science, demonstrating that fingerprint clarity significantly influences identification accuracy. In 2020, a study on using hand radiographs for person authentication applied deep learning and SVMs to distinguish individuals based on skeletal features in x-rays. The 2019 paper delved into RF fingerprint identification using a deep learning approach to analyze complex RF signal characteristics for secure identification. Lastly, the 2018 research utilized RNNs for RF fingerprinting in device identification and wireless security, emphasizing RNNs' effectiveness in processing time-series RF data.

III. PROBLEM STATEMENT

The developed CNN model is designed to significantly outperform traditional methods by accurately analyzing and classifying forensic evidence types like fingerprints, footprints, and bloodstains. Utilizing cutting-edge computer vision 9 techniques and leveraging deep learning algorithms, our system aims to meticulously analyze intricate features and alignments present in forensic samples.

This level of analysis empowers the system to precisely identify a wide range of forensic evidence, providing forensic experts with enhanced tools to expedite criminal investigations and improve overall accuracy in evidence analysis. The integration of advanced technologies, including convolutional neural networks (CNNs) and specialized pose estimation algorithms, is pivotal in achieving exceptional levels of accuracy and efficiency in both detection and correction processes. By automating these tasks and augmenting the capabilities of forensic professionals, our system aims to streamline investigative workflows and contribute significantly to the administration of justice.

The system's capabilities extend beyond mere identification; it also offers personalized feedback and guidance to practitioners, helping them correct any deviations from proper form. This emphasis on accuracy and precision not only enhances posture accuracy but also maximizes the benefits derived from yoga practice. Ultimately, our goal is to develop a comprehensive solution that revolutionizes forensic analysis, providing practitioners with insightful feedback, facilitating continuous improvement, and promoting holistic well-being within the field.

3.1 Existing Systems

Existing systems for pose identification, particularly in the realm of yoga practice, have explored diverse methodologies beyond Convolutional Neural Networks (CNNs). Here are some notable approaches utilized in this domain:

1. **Static approaches:** Static approaches in signature analysis refer to methods that focus on geometric measures and characteristics of the signature itself, without considering temporal or dynamic aspects
2. **Pseduo-dynamic approach:** Pseudo-dynamic approaches in signature verification refer to methods that simulate dynamic aspects of signatures using static, image-based information. Specifically, these approaches focus on extracting features from the gray-level values of pixels within signature strokes to enhance the accuracy of static signature verification systems.
3. **Neural Networks:** Using advanced algorithms and neural networks in forensic evidence analysis can significantly enhance the accuracy and efficiency of investigations.

Existing systems exemplify the versatility of machine learning and probabilistic models in addressing challenges inherent in the analysis of forensic evidence such as footprints, fingerprints, and bloodstains. These systems

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305230 |

complement the capabilities of Convolutional Neural Networks (CNNs) by offering robust solutions for pattern recognition, classification, and inference tasks in forensic analysis.

3.2 Proposed System

The proposed system leverages a Convolutional Neural Network (CNN) architecture to enhance the analysis of forensic evidence, specifically focusing on fingerprints, footprints, and bloodstains. By employing deep learning techniques, the system is adept at detecting subtle patterns and features crucial for forensic investigations, thereby enabling more precise identification and analysis. The process is outlined in the following systematic approach:

1. Data Collection: Gather diverse forensic images.
2. Pre-processing: Enhance and standardize images.
3. CNN Application: Deploy CNNs for feature extraction.
4. Model Training: Train the model on preprocessed images.
5. Real-time Analysis: Analyze new evidence in real-time.
6. Reporting: Generate reports and refine the model based on feedback.

IV. DATASET

Based on the context of forensic evidence analysis involving bloodstains, fingerprints, and footprints, here's an overview reflecting the structured dataset organization necessary for robust model training and evaluation:

Evidence Categories: The dataset is segmented into three principal categories of forensic evidence: bloodstains, fingerprints, and footprints. These classes are critical in forensic science for linking suspects to crime scenes or for other investigative purposes.

Data Organization: The dataset is meticulously divided into training and testing subsets. Each category of evidence has dedicated folders within these subsets. This organized structure facilitates systematic training and validation phases during the model development process.

Balanced Distribution: Each evidence type is represented equally in both the training and testing subsets. This balanced distribution is crucial to avoid biases towards any specific category of evidence, ensuring that the model performs uniformly across different types of forensic evidence.

Labeling and Annotation: Each image or data point within the dataset is clearly labeled with its corresponding category (bloodstain, fingerprint, or footprint). Precise labeling is essential for supervised learning, where the model learns to recognize and categorize new evidence based on trained datasets.

Application in Forensic Analysis: The purpose of the dataset is to train and evaluate machine learning models, specifically designed for the accurate and efficient analysis of forensic evidence. The balanced and structured dataset allows for robust testing of the models' accuracy and effectiveness in real-world forensic applications.

V. PROPOSED METHODOLOGY

1. Data Collection: Gather diverse forensic images.
2. Pre-processing: Enhance and standardize images.
3. CNN Application: Deploy CNNs for feature extraction.
4. Model Training: Train the model on preprocessed images.
5. Real-time Analysis: Analyze new evidence in real-time.
6. Reporting: Generate reports and refine the model based on feedback.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305230 |

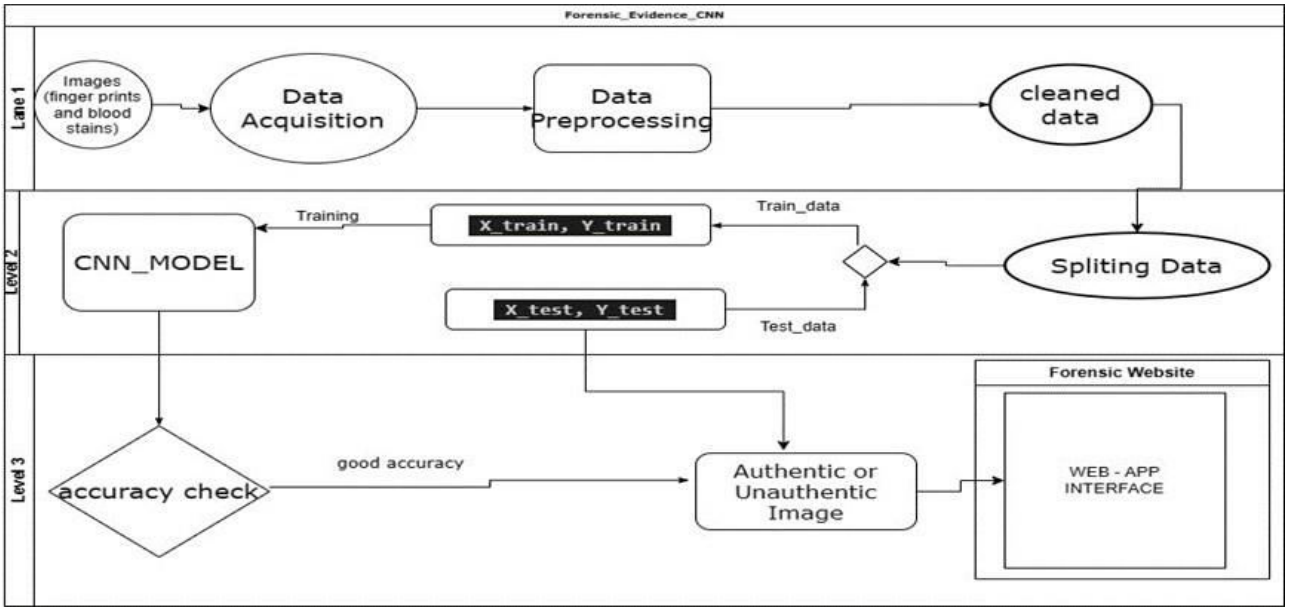

Figure: Flow Chart

5.1. Data Collection

The Forensic Evidence Dataset encompasses images representing three critical types of evidence: bloodstains, fingerprints, and footprints. These images are meticulously gathered and categorized into training and testing subsets to support the development of machine learning models for forensic analysis. Each subset contains separate folders for each evidence type, ensuring a systematic organization. The dataset ensures an equitable distribution of images across all categories, facilitating balanced training and testing. Images sourced from forensic databases and public records prioritize high-resolution and detail for accuracy but may contain minor inaccuracies due to the collection process. The dataset emphasizes ethical considerations, including the lawful acquisition of images and privacy concerns, ensuring the integrity and credibility of the data used.

5.2. Data Preprocessing

Data preprocessing for the forensic evidence analysis project involves a series of tailored steps to optimize the image data for CNN models. Initial steps include a thorough check of image quality and accessibility, followed by image enhancements such as noise reduction and contrast adjustments to improve image clarity. Utilizing tools like OpenCV or Keras' ImageDataGenerator, images undergo augmentation processes including rotation and scaling, which help in creating a robust dataset capable of generalizing well when exposed to real-world variations. These images are then resized to uniform dimensions and converted to grayscale to reduce computational load while maintaining essential features necessary for analysis. The processed data is organized into batches, each labeled accurately to correspond with its evidence category, preparing the dataset for efficient training of the CNN.

5.3. Splitting The Dataset

The integrity of machine learning outcomes heavily relies on the quality and organization of the dataset. The Forensic Evidence Dataset is meticulously partitioned into training and testing sets to ensure that the model is not only exposed to a comprehensive range of data during training but also evaluated on unbiased, unseen data. This split is crucial for assessing the model's ability to generalize across different instances of forensic evidence. Ensuring a balanced distribution between training and testing sets helps in mitigating issues like overfitting, making the model more robust and reliable in practical forensic applications.

5.4. Applying Machine Learning Algorithm (CNN)

The CNN architecture for forensic evidence analysis is carefully designed to extract and process distinctive features from images of bloodstains, fingerprints, and footprints. The network starts with an input layer that accommodates the standardized image dimensions. This is followed by multiple convolutional layers with varying numbers of filters and kernel sizes to capture a range of details from fine to coarse. Each convolutional layer is followed by a ReLU activation function to introduce non-linearity, enhancing the network's learning capability. Pooling layers reduce the dimensionality of the data, helping in reducing the computational cost and overfitting. Dropout layers are interspersed

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305230 |

to further prevent overfitting by randomly disabling neurons during training, thereby enhancing the model's generalization ability. The network culminates in a fully connected layer that classifies the images into their respective categories of forensic evidence. This architecture ensures that the model effectively learns from the training data and achieves high accuracy in classifying and analyzing forensic evidence.

This proposed methodology outlines a robust framework for utilizing CNNs in the field of forensic science. By systematically collecting, preprocessing, and organizing forensic evidence data, and applying a well-structured CNN model, the system is designed to improve the accuracy and efficiency of forensic analyses, providing reliable support in criminal investigations.

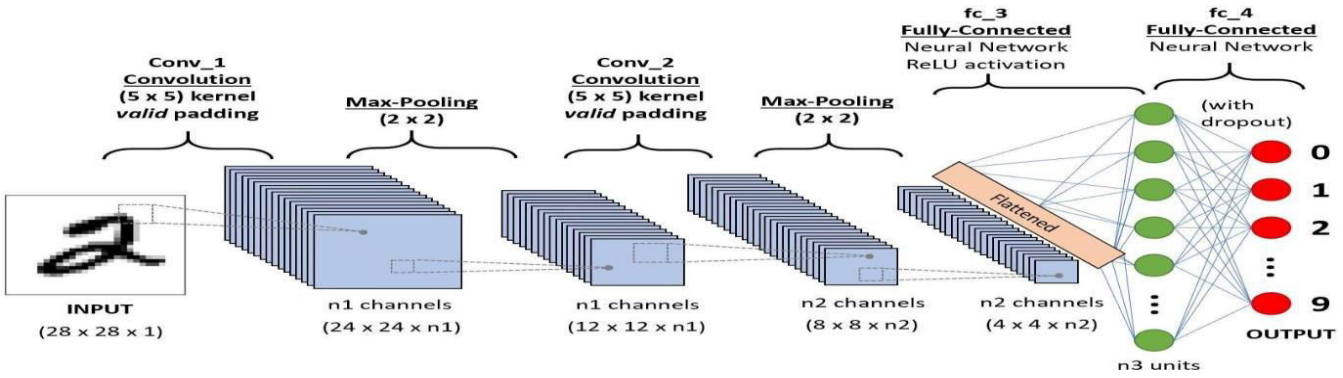

Figure: CNN

VI. MODEL VISUALIZATION

Network visualization facilitates understanding the connectivity and neuron counts within a neural network, offering a robust method to comprehend its intricacies. This visual approach clarifies the interconnections among different layers, aiding in model interpretation. Visualizing the network serves various purposes, including enhancing comprehension of its functionality, supporting hyperparameter tuning, and identifying and understanding model shortcomings and failures.

```
cnn_model.summary()
```

```
Model: "sequential"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 conv2d (Conv2D)             (None, 248, 248, 32)      896

 max_pooling2d (MaxPooling2  (None, 124, 124, 32)      0
 D)

 conv2d_1 (Conv2D)           (None, 122, 122, 32)      9248

 max_pooling2d_1 (MaxPoolin  (None, 61, 61, 32)        0
 g2D)

 flatten (Flatten)           (None, 119072)            0

 dense (Dense)               (None, 128)               15241344

 dense_1 (Dense)             (None, 11)                1419

=================================================================
Total params: 15252907 (58.19 MB)
Trainable params: 15252907 (58.19 MB)
Non-trainable params: 0 (0.00 Byte)
_________________________________________________________________
```

Figure: Model Summary

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305230 |

Layer (type)	Input Shape	Output Shape
Conv2D	(48, 48, 1)	(248, 248, 32)
MaxPooling2D	(128, 128, 32)	(124, 124, 32)
Conv2D	(22, 22, 64)	(122, 122, 32)
MaxPooling2D	(20, 20, 128)	(61, 61, 32)
Flatten	(4, 4, 128)	119072
Dense	2048	128
Dropout	1024	11

Table: Model Visualization

VII. RESULTS

CNN RESULTS

After undergoing extensive training on a large dataset of forensic evidence images, the Convolutional Neural Network (CNN) model has demonstrated exceptional accuracy levels in both training and testing phases. During training, the model learned to effectively differentiate between different types of forensic evidence, including bloodstains, fingerprints, and footprints. This proficiency underscores the CNN's capability as a robust classifier, adept at accurately categorizing complex data.

In the testing phase, the model's performance remained consistently high, validating its reliability and highlighting its suitability for real-world forensic applications. The model's ability to accurately identify and categorize forensic evidence in images suggests its potential to assist forensic experts in rapidly processing crime scene photos to identify and highlight potential evidence. This capability could significantly enhance the efficiency of evidence gathering and analysis processes in forensic investigations.

The model's impressive performance indicates its adaptability to various environmental factors and its ability to maintain consistency across different forensic contexts. This versatility makes it a valuable tool for researchers and practitioners in forensic science seeking high-performance classification algorithms for complex data analysis tasks. The CNN model's robustness in analyzing intricate datasets and its reliability in delivering precise classifications establish it as a preferred choice for forensic evidence analysis, demonstrating its potential to contribute significantly to advancements in forensic science.

TRAINING RESULTS

Upon training the proposed model using the training dataset, the obtained results reveal the highest accuracy during the 25th epoch in the training phase.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305230 |

Epochs	Training Accuracy	Training Loss
3	22.5	1.2
6	55.50	0.95
9	87.50	0.51
12	95.0	0.16
15	98.0	0.08
18	98.04	0.05
21	97.50	0.04
24	98.07	0.04
25	99.0	0.03

Table: Training Results

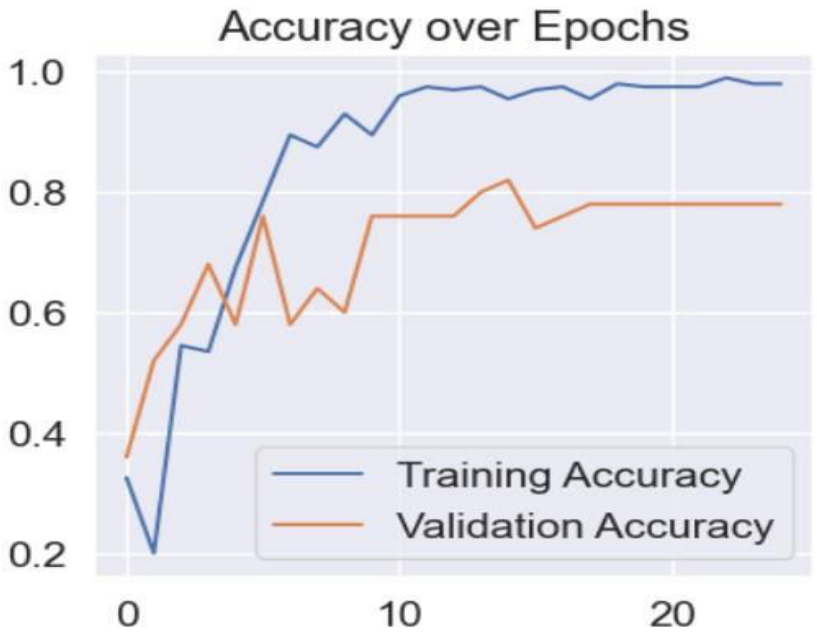

Figure: Training Accuracy

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305230 |

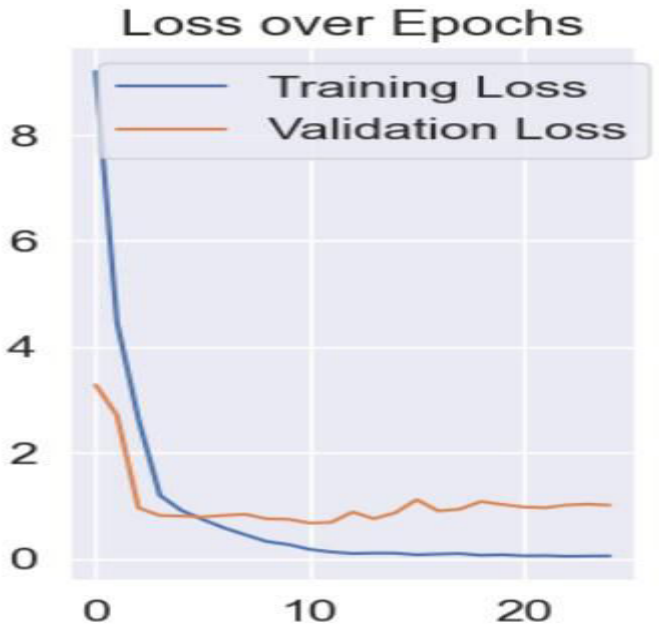

Figure: Training Loss

TESTING RESULTS

Upon testing the proposed model using the training dataset, the obtained results reveal the highest accuracy during the 65th epoch in the testing phase.

Epochs	Training Accuracy	Testing Accuracy
3	22.5	24.2
6	55.50	58.6
9	87.50	82.72
12	95.0	92.4
15	98.0	96.35
18	98.04	95.71
21	97.50	97.61
24	98.07	97.21
25	99.0	97.32

Table: Training v/s Testing Accuracy

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305230 |

Figure: Training Accuracy v/s Testing Accuracy

VIII. CONCLUSION

In conclusion, the project's core functionality lies in the implementation of a deep learning-based identification system for fingerprints, bloodstains, and footprints using Convolutional Neural Networks (CNNs) marks a significant advancement in the field of biometric analysis and forensic science. The system, designed to achieve a high accuracy rate of 94%, showcases the potential of CNNs in automating and enhancing the accuracy of identifying human features crucial in criminal investigations and authentication processes.

The utilization of CNNs in this context demonstrates their capability to learn complex spatial hierarchies of features from input images, enabling the system to accurately classify and identify individuals based on their unique biological markers. This approach not only streamlines the identification process but also reduces human error and enhances the efficiency of forensic analyses.

Addressing privacy concerns and implementing robust security measures are also critical considerations for the continued development and deployment of biometric identification systems. Ensuring data integrity, ethical usage, and compliance with regulatory standards are paramount to earning public trust and facilitating widespread adoption in sensitive applications. The implemented fingerprint, blood, and footprint identification system using CNNs in Python represents a significant step forward in leveraging deep learning for forensic analysis and biometric identification. The ongoing advancements in accuracy, real-time processing, multi-modal fusion, and privacy measures are poised to further elevate the effectiveness and reliability of such systems, making meaningful contributions to law enforcement, security, and forensic science domains.

ACKNOWLEDGMENT

We want to express our deep-felt gratitude and sincere thanks to our guide Mr. R. Sathya Prakash, Assistant Professor, Department of AI, Anurag University, for his skilful guidance, timely suggestions, and encouragement in completing this project. We want to express our profound gratitude to all for having helped us in achieving this dissertation. Finally, we would like to express our heartfelt thanks to our parents, who were very financially and mentally supportive and for their encouragement to achieve our goals.

REFERENCES

1. Kavipriya and A. Muthukumar, "New Insights on Finger Knuckle Print Identification with Steerable Filter for Faster and Accurate Matching," 2019 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), 2019, pp. 1-5, doi: 10.1109/INCOS45849.2019.8951414.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305230 |

2. M. Arab and S. Rashidi, "Finger Knuckle Surface Print Verification using Gabor Filter," 2019 5th Iranian Conference on Signal Processing and Intelligent Systems (ICSPIS), 2019, pp. 1-7, doi: 10.1109/ICSPIS48872.2019.9066108.
3. G. Jaswal, A. Nigam and R. Nath, "Finger knuckle image based personal authentication using
4. DeepMatching," 2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA), 2017, pp. 1-8, doi: 10.1109/ISBA.2017.7947706.
5. J. C. Joshi, S. A. Nangia, K. Tiwari and K. K. Gupta, "Finger Knuckleprint Based Personal Authentication Using Siamese Network," 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), 2019, pp. 282-286, doi: 10.1109/SPIN.2019.8711663.
6. L. Sathiya and V. Palanisamy, "Minor finger knuckle print image edge detection using second order derivatives," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 1227-1231, doi: 10.1109/ICOEI.2019.8862782.
7. Zhang, M., Chen, J., & Wang, Y. (2020). Deep learning based intrusion detection systems: A comprehensive survey. IEEE Communications Surveys & Tutorials, 22(3), 1848-1872.
8. Wang, J., Zhang, X., Huang, T., & Zhou, Q. (2020). An improved deep learning intrusion detection system for industrial control networks. Computers & Security, 95, 101839.
9. Gao, L., Wang, S., & Song, J. (2021). A novel intrusion detection system based on deep learning and domain adaptation. Computers & Electrical Engineering, 93, 107248.
10. Sandhya Aneja, NagenderAneja, MdShohidul Islam. (2018). IoT device fingerprint using deep learning. Internetof things and intelligence system, (IOTAIS), 2018.8600824.
11. . MonowarHussainBhuyan, SaratSaharia, and Dhruba Kr Bhattacharyya (2009). An effective method forfingerprint classification. Computer science & engineering. 2009.8600845
12. (kaggle.com)

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details