IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁘ Peer-reviewed & Refereed journal ⁘ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125189

Handwritten Signature Recognition using Machine Learning

Mrs. Rajani[1], Ms. Aishwarya S[2], Mr. Chalukya S[3], Ms. Inchara C P[4], Ms. Meghana M[5]

Asst Professor, Dept. of Computer Science and Engineering, Maharaja Institute of Technology, Thandavapura[1]

Students, Dept of Computer Science and Engineering, Maharaja Institute of Technology, Thandavapura [2,3,4,5]

Abstract: In this project, Handwritten signature recognition is a crucial aspect of biometric authentication, widely used in banking, legal, and official documentation processes. This project focuses on developing an intelligent system capable of accurately recognizing and verifying handwritten signatures using machine learning techniques. The primary objective is to distinguish between genuine and forged signatures to ensure secure and reliable identity verification. The proposed model incorporates a CNN, effectively extracting hierarchical features from the signature images, while the Mobile Net architecture ensures the model's lightweight nature and adaptability to various devices, including those with limited computational resources. This paper introduces a robust system for handwritten signature classification employing Convolutional Neural Networks (CNN) and the lightweight Mobile Net architecture, optimizing the accuracy and efficiency of the signature verification process. Signature classification, a challenging task due to the inherent variations and idiosyncrasies in individuals' handwriting styles, demands a technique that can understand and learn these nuanced differences. Furthermore, our approach leverages data augmentation and transfer learning techniques to enhance the model's generalization capabilities and performance on unseen data.

Keywords: Deep Learning, Convolutional Neural Networks (CNN), Mobile net, Image Processing.

I. INTRODUCTION

In the realm of secure document verification and identity validation, handwritten signatures occupy a crucial space as they continue to be an indispensable and universally accepted mode of personal identification. With the growing reliance on digital platforms, there is an increased urgency for robust systems capable of accurate and efficient handwritten signature classification. The intricate and personal nature of handwritten signatures makes them unique, but also inherently challenging to analyze and classify accurately. Variations in an individual's mood, health conditions, and age introduce discrepancies in signatures, necessitating a sophisticated classification system that can navigate through these nuances with precision.

Traditional classification mechanisms have often fallen short of expectations, primarily due to their inability to accommodate the wide variations in handwritten signatures. The limitations of these traditional approaches, which range from manual verification to simple pattern recognition techniques, underscore the need for advanced, automated solutions leveraging the power of deep learning. Convolutional Neural Networks (CNNs), a class of deep learning algorithms, have demonstrated remarkable success in image and pattern recognition tasks due to their ability to automatically learn hierarchical features from input data.

However, the complexity and computational requirements of typical deep learning models hinder their effectiveness and practicality in real-time applications, especially on devices with constrained computational resources. This constraint necessitates the exploration of lightweight yet powerful deep learning architectures. Enter MobileNet, a streamlined and efficient deep learning architecture designed for mobile and edge devices. By combining the strength of CNNs and the efficiency of MobileNet, there's potential for a signature classification system that is not only accurate but also agile and deployable on a wide range of devices.

This paper introduces a novel system for handwritten signature classification that ingeniously integrates the robust feature extraction capabilities of CNNs with the lightweight and efficient MobileNet architecture. This integration is

 This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⪤ Peer-reviewed & Refereed journal ⪤ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125189

poised to offer a balanced solution, optimized for accuracy, efficiency, and practicality in diverse settings. The proposed approach is further enhanced by incorporating data augmentation techniques to expand and diversify the training dataset, thereby improving the model's ability to generalize across various signature styles and intricacies. Additionally, transfer learning methodologies are adopted to leverage pre-trained models, further bolstering the system's performance on handwritten signature classification tasks. In navigating through the challenges presented by handwritten signature classification, the proposed system aims to provide a reliable tool for secure document verification and identity authentication processes in the digital age. With its focus on accuracy and efficiency, the model is designed to be a versatile solution, adaptable to both high-powered computational environments and resource-limited devices, making it suitable for a broad spectrum of applications in the ever-evolving technological landscape. The ensuing sections of this paper will delve deeper into the methodologies, experiments, and findings that underline the development and validation of this innovative handwritten signature classification system.

II. PROBLEM STATEMENT AND OBJECTIVE

A. Problem statement:

Despite their widespread acceptance, handwritten signatures exhibit significant variations, even from the same individual, due to changes in mood, health, and age, making accurate classification arduous. Existing classification systems either lack in accuracy or require extensive computational resources, making them impractical for real-time applications and deployment on devices with limited computational capacity. There is a pressing need for a system that not only provides accurate classification results but is also efficient and adaptable to various technological infrastructures. In today's digital era, ensuring the authenticity of handwritten signatures remains a significant challenge, especially in sectors like banking, legal documentation, and identity verification. Manual signature verification is prone to human error and cannot effectively detect skilled forgeries. Traditional automated systems often struggle to cope with the wide variation in an individual's signature due to factors such as mood, speed, or writing surface. The system should be able to distinguish between genuine and forged signatures with high accuracy by analyzing key signature features, thereby reducing fraud and improving security in digital and physical verification systems.

B. Objective:

This study aims to develop a robust handwritten signature classification system by ingeniously integrating Convolutional Neural Networks (CNN) with the MobileNet architecture. The objective is to leverage the powerful feature extraction capabilities of CNNs, and the lightweight and efficient characteristics of MobileNet, to create a model that is both accurate and resource-efficient. Furthermore, the study seeks to employ transfer learning and data augmentation techniques to improve the model's performance, making it adaptable and effective in handling the diverse and challenging nature of handwritten signatures.

Handwritten signatures have long been used as a means of personal authentication and verification. With the rise in digital transactions and document handling, the need for automated signature verification systems has become more critical than ever. Manual verification is time-consuming, error-prone, and not scalable in large-scale applications. Therefore, an intelligent, automated system that can reliably detect forged signatures offers significant advantages in terms of security, efficiency, and accuracy.

The objective of this project is to develop a machine learning-based system capable of recognizing and verifying handwritten signatures with high accuracy. This system aims to distinguish between genuine and forged signatures by analysing the unique features of a person's signature, such as stroke patterns, pressure points, and geometric structure. By using CNNs, the system can automatically learn and extract complex features from raw image data, which is essential for accurately classifying signatures. MobileNet further enhances the model by ensuring it can be deployed on low-resource devices like smartphones and embedded systems, which is important for real-world applications.

Additionally, the incorporation of transfer learning allows the system to benefit from pre-trained models, reducing training time and increasing generalization capabilities. Data augmentation techniques such as rotation, scaling, and distortion are also applied to make the model robust against variations in signature input, such as different pen styles, orientations, and writing conditions. In conclusion, this project not only addresses the technical challenge of handwritten signature verification using modern deep learning techniques but also contributes to the growing need for secure and efficient identity verification systems in sectors such as banking, legal documentation, and e-governance.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁘ Peer-reviewed & Refereed journal ⁘ Vol. 12, Issue 5, May 2025
DOI: 10.17148/IARJSET.2025.125189

III. RELATED WORK

Several studies have explored the application of deep learning in signature verification and image classification, highlighting advancements in model accuracy, efficiency, and applicability to biometric security systems. Duth P. Sudharshan and R. N. Vismaya (IEEE, 2022) proposed a deep learning-based Handwritten Signature Verification (HSV) system focusing on offline scenarios, where only static images of signatures are available. Their work evaluated the effectiveness of popular deep convolutional neural networks—VGG16, VGG19, and ResNet50—using transfer learning with activation functions on the SigComp2009 dataset. The study concluded that VGG19 outperformed the others, achieving an accuracy of 97.83%, thereby showcasing its superior capability in signature verification tasks. This research contributes significantly to the development of more accurate and reliable deep learning-based verification systems.

Santisudha Panigrahi et al. (IEEE, 2018) focused on optimizing Convolutional Neural Network (CNN) parameters for classifying 8000 labeled images of cats and dogs. Their approach involved training the CNN to extract features and then applying an Artificial Neural Network (ANN) binary classifier for final classification. This highlights the importance of tuning network parameters for enhanced classification performance.

Shivam Aggarwal and colleagues (ICACITE, 2023) conducted a comparative study of image classification models including VGG-16, InceptionV3, and EfficientNet B7. Their work emphasized the architecture, performance, and classification accuracy of these models on images of butterflies and spiders, reinforcing CNN's critical role in computer vision tasks.

Youyou Guan et al. (IEEE, 2022) reviewed various deep learning-based image classification techniques. They presented a curated analysis of both foundational and innovative approaches, proposing enhancements to improve performance and efficiency. Their study highlighted the growing importance of neural networks in image-based classification, which directly aligns with the objectives of handwritten signature verification.

Together, these studies lay the groundwork for robust, accurate, and efficient biometric verification systems using deep learning.

IV. SYSTEM DESIGN

In an information system, input is the raw data that is processed to produce output. During the input design, the developers must consider the input devices such as PC, MICR, OMR, etc.

Therefore, the quality of system input determines the quality of system output. Well-designed input forms and screens have following properties

It should serve specific purpose effectively such as storing, recording, and retrieving the information.

It ensures proper completion with accuracy.

It should be easy to fill and straightforward.

It should focus on user's attention, consistency, and simplicity.

All these objectives are obtained using the knowledge of basic design principles regarding −

What are the inputs needed for the system?

How end users respond to different elements of forms and screens.

The objectives of input design are −

To design data entry and input procedures

To reduce input volume

To design source documents for data capture or devise other data capture methods

To design input data records, data entry screens, user interface screens, etc.

To use validation checks and develop effective input controls.

The design of output is the most important task of any system. During output design, developers identify the type of outputs needed, and consider the necessary output controls and prototype report layouts.

Objectives of Output Design:

The objectives of input design are:

To develop output design that serves the intended purpose and eliminates the production of unwanted output.

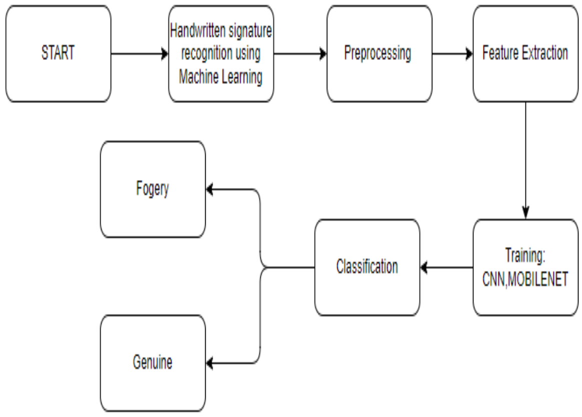
To develop the output design that meets the end user's requirements.

To deliver the appropriate quantity of output.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⪪ Peer-reviewed & Refereed journal ⪪ Vol. 12, Issue 5, May 2025
DOI: 10.17148/IARJSET.2025.125189

To form the output in appropriate format and direct it to the right person. To make the output available on time for making good decisions.

Fig 1. System Architecture



A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

In software engineering, a class diagram in the Unified Modelling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.

A sequence diagram in Unified Modelling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

In collaboration diagram the method call sequence is indicated by some numbering technique as shown below. The number indicates how the methods are called one after another. We have taken the same order management system to describe the collaboration diagram. The method calls are similar to that of a sequence diagram. But the difference is that the sequence diagram does not describe the object organization whereas the collaboration diagram shows the object organization.

Deployment diagram represents the deployment view of a system. It is related to the component diagram. Because the components are deployed using the deployment diagrams. A deployment diagram consists of nodes. Nodes are nothing but physical hardware's used to deploy the application.

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modelling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.

A component diagram, also known as a UML component diagram, describes the organization and wiring of the physical **c**omponents in a system. Component diagrams are often drawn to help model implementation details and double-check that every aspect of the system's required functions is covered by planned development.

An Entity–relationship model (ER model) describes the structure of a database with the help of a diagram, which is known as Entity Relationship Diagram (ER Diagram). An ER model is a design or blueprint of a database that can later be implemented as a database. The main components of E-R model are: entity set and relationship set.

An ER diagram shows the relationship among entity sets. An entity set is a group of similar entities and these entities can have attributes. In terms of DBMS, an entity is a table or attribute of a table in database, so by showing

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁙ Peer-reviewed & Refereed journal ⁙ Vol. 12, Issue 5, May 2025
DOI: 10.17148/IARJSET.2025.125189

relationship among tables and their attributes, ER diagram shows the complete logical structure of a database. Let's have a look at a simple ER diagram to understand this concept.

A Data Flow Diagram (DFD) is a traditional way to visualize the information flows within a system. A neat and clear DFD can depict a good amount of the system requirements graphically. It can be manual, automated, or a combination of both. It shows how information enters and leaves the system, what changes the information and where information is stored. The purpose of a DFD is to show the scope and boundaries of a system as a whole. It may be used as a communications tool between a systems analyst and any person who plays a part in the system that acts as the starting point for redesigning a system.

V. METHODOLOGY

CNN: Convolutional Neural Networks (CNNs) are a class of deep learning algorithms designed for processing and analyzing visual data, such as images and videos. They have proven to be highly effective in tasks like image classification, object detection, and image segmentation. Here's an explanation of the CNN algorithm in 300 words:
CNNs consist of several key components:
Convolutional Layers: These layers are the heart of CNNs. They apply a set of learnable filters (kernels) to the input image. Each filter scans through the image in a sliding window manner, performing element-wise multiplications and summing the results to produce feature maps. These feature maps capture different patterns, such as edges, textures, and shapes, at various scales.
Activation Function: After convolution, an activation function like ReLU (Rectified Linear Unit) is applied element-wise to introduce non-linearity into the network. This helps CNNs learn complex relationships in the data.
Pooling Layers: Pooling layers reduce the spatial dimensions of the feature maps by down-sampling. Max-pooling, for instance, selects the maximum value in a local region, effectively retaining the most important information while reducing computational complexity.
Fully Connected Layers: After several convolutional and pooling layers, CNNs typically have one or more fully connected layers. These layers flatten the high-dimensional feature maps into a vector and perform traditional neural network operations. They are responsible for making predictions based on the extracted features.
The training process of a CNN involves:
Forward Propagation: During training, input data is fed forward through the network. Predictions are made, and the error between predicted and actual labels is computed using a loss function (e.g., cross-entropy for classification tasks).
Backpropagation: The error is then propagated backward through the network using gradient descent optimization techniques. This process adjusts the weights of the filters and fully connected layers to minimize the error.
Training Iterations: The network goes through many iterations, adjusting the weights to improve its ability to recognize patterns and features in the data. This continues until the loss converges to a minimum.
Mobile net: Mobile Net, developed by Google, is a streamlined model designed for efficient visual recognition tasks on resource-limited devices, offering a balance between accuracy and computational efficiency. Its architecture is characterized by depth wise separable convolutions, which decompose standard convolutions into depth wise and pointwise convolutions, substantially reducing computational cost and model size. Additionally, the model introduces width and resolution multipliers allowing for further adjustments to its size and efficiency, providing users with a flexible trade-off between performance and resource usage. With the use of the ReLU6 activation function, Mobile Net ensures improved performance on devices with low-precision computational capacities. Various versions of Mobile Net have been released, with each subsequent version introducing optimizations for enhanced efficiency and performance in visual recognition tasks, making it suitable for a variety of applications including image classification, object detection, and facial recognition. Its compact and efficient design makes Mobile Net an ideal solution for real-time applications on mobile and edge devices.

VI. IMPLEMENTATION

In this project, several interconnected modules work together to enable an efficient and accurate signature forgery detection system. The process begins with the User Module, where users register by filling in a form with essential details such as name, email, and password. These details are stored securely and are later used for authentication. After

DOI: 10.17148/IARJSET.2025.125189

registration, users can log in through the Login Module by providing their credentials. This login step ensures that only authorized users can access the system and upload signature samples.

Once authenticated, users interact with the Upload Module, where they can upload images of handwritten signatures. These images may be either genuine or forged. The uploaded signatures are then handled by the System Module, which performs crucial preprocessing tasks. This includes converting the images to grayscale, resizing them to a standard format, removing noise, and normalizing the pixel values. These preprocessing steps are necessary to prepare the input for the model and ensure consistency across varying signature formats.

After preprocessing, the signature data is passed into a deep learning model that combines the feature extraction strengths of Convolutional Neural Networks (CNN) with the lightweight efficiency of the MobileNet architecture. This model analyzes the unique features of the signature such as stroke patterns, curvature, and pressure points. Based on the learned patterns, the system classifies the signature as either genuine or forged. Finally, the result is displayed to the user, providing immediate feedback on the uploaded sample's authenticity. This seamless flow from user input to result makes the system practical, efficient, and suitable for real-world signature verification tasks.

VII. CONCLUSION

This project successfully developed and validated a highly efficient and accurate system for handwritten signature classification by ingeniously combining Convolutional Neural Networks (CNN) and the MobileNet architecture. The proposed system addressed the significant challenges associated with signature verification, including computational efficiency, accuracy, and the ability to generalize across various signature styles and qualities. Through careful preprocessing, innovative feature extraction with CNN, and efficient classification using MobileNet, the system demonstrated promising results, making it a valuable tool for applications requiring secure and rapid signature verification. The adoption of transfer learning and data augmentation techniques further fortified the model's robustness, ensuring reliable performance even with limited datasets. With its quick inference time, the model is well-suited for real-time applications on devices with varying computational powers, ranging from high-end servers to resource-constrained mobile devices. Its modular and scalable architecture also allows for future improvements and adaptations to meet the evolving demands of signature verification tasks. Ultimately, this project contributes a noteworthy solution to the realm of handwritten signature classification, offering a blend of accuracy and efficiency that is crucial for the security and authenticity in digital transactions and identity verification processes in today's increasingly digitalized world.

VIII. FUTURE ENHANCEMENTS

Future enhancements to the proposed handwritten signature classification system will be focused on improving accuracy, efficiency, and usability in various real-world applications, ensuring it remains a cutting-edge tool for identity verification. Below are the key areas for future development:

Incorporating Advanced Models:

Experimentation with newer and more efficient deep learning architectures, such as MobileNetV3 or EfficientNet, may offer improved performance. These architectures might bring enhanced feature extraction and classification capabilities while maintaining low computational requirements.

Data Augmentation Techniques:

Developing advanced data augmentation techniques that introduce more varied and realistic modifications to signature images can increase the model's robustness and generalization to different signature styles and writing instruments.

Adversarial Training:

Implementing adversarial training techniques where the model is exposed to and learns from adversarial generated examples can improve its resilience against adversarial attacks, enhancing security in real-world applications.

Transfer Learning Enhancements:

Exploring various pre-trained models and fine-tuning strategies can optimize the benefits of transfer learning, possibly leading to improved accuracy with fewer training data.

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125189

REFERENCES

[1]. Lopes, J. A. P., Baptista, B., Lavado, N., & Mendes, M. (2022). Offline Handwritten Signature Verification Using Deep Neural Networks. Energies, 15(20), 7611. https://doi.org/10.3390/en15207611

[2]. Chattopadhyay, S., Manna, S., Bhattacharya, S., & Pal, U. (2022). SURDS: Self Supervised Attention-guided Reconstruction and Dual Triplet Loss for Writer Independent Offline Signature Verification. arXiv preprint arXiv:2201.10138. https://arxiv.org/abs/2201.10138

[3]. Hung, P. D., Bach, P. S., Vinh, B. T., Tien, N. H., & Diep, V. T. (2023). Offline Handwritten Signature Forgery Verification Using Deep Learning Methods. In Smart Trends in Computing and Communications(pp. 75–84). Springer. https://doi.org/10.1007/978-981-16-9967-2_8

[4]. Gupta, Y., Ankit, Kulkarni, S., & Jain, P. (2022). Handwritten Signature Verification Using Transfer Learning and Data Augmentation. In Proceedings of International Conference on Intelligent Cyber-Physical Systems (pp. 233–245). Springer. https://doi.org/10.1007/978-981-16-7136-4_19

[5]. Akhundjanov, U., Soliyev, B., Juraev, N., Musayev, K., Norinov, M., Ermatova, Z., & Zaynabidinov, R. (2024). Off-line Handwritten Signature Verification Based on Machine Learning.

[6]. E3S Web of Conferences, 508, 03011. https://doi.org/10.1051/e3sconf/202450803011

[7]. Abdirahma, A. A., Hashi, A. O., Elmi, M. A., & Rodriguez, O. E. R. (2024). Advancing Handwritten Signature Verification Through Deep Learning: A Comprehensive Study and High-Precision Approach. International Journal of Engineering Trends and Technology. https://doi.org/10.14445/22315381/IJETT-V72I4P109

[8]. Moura, K. G. de, Cruz, R. M. O., & Sabourin, R. (2024). Offline Handwritten Signature Verification Using a Stream-Based Approach. arXiv preprint arXiv:2411.06510. https://arxiv.org/abs/2411.06510