https://dx.doi.org/10.4314/dujopas.v9i4b.31
ISSN (Print): 2476-8316
ISSN (Online): 2635-3490
Dutse Journal of Pure and Applied Sciences (DUJOPAS), *Vol. 9 No. 4b December 2023*

Design and Implementation of Vision System for Handwritten Signature Authentication.

Oluwaseun Opeyemi Martins[1,*], Muhammad Abdulhamid Mahdi[2], Alagbe Oluwaseun Emmanuel[3], Ojo Olawunmi Adetoun[4], Samuel Oluwaseun Emmanuel[5]

[1]Department of Mechatronics Engineering,
Federal University, Oye-Ekiti,
Nigeria

Email: oluwaseun.martins@fuoye.edu.ng

Abstract

In an era marked by the digital revolution, ensuring the integrity and authenticity of signatures is a pivotal concern in the realm of identity verification. This project introduces an innovative approach to address this imperative issue, harnessing the power of modern deep learning techniques to devise a robust signature authentication system. By meticulously integrating theory and practice, this endeavor seeks to transcend existing limitations and redefine the landscape of identity validation. With a core objective to enhance digital security, this project undertakes the formidable challenge of distinguishing between genuine and forged signatures. The objectives of this project encompass the assembly of a comprehensive dataset comprising both genuine and forged signature samples, the design and implementation of a convolutional neural network (CNN) model, and the meticulous evaluation of its performance against rigorous criteria. The methodology involves the intricate fusion of data preprocessing, feature extraction, and machine learning, orchestrated to facilitate the model's acquisition of intricate signature characteristics. Through a meticulous evaluation method, the proposed system is subjected to a battery of quantitative metrics, including precision, recall, and the F1-score, forming the bedrock of a comprehensive performance assessment. This multifaceted evaluation approach encompasses controlled experimentation, model optimization, and real-world deployment to capture the intricate interplay between theoretical viability and practical effectiveness. The project culminates in a compelling conclusion, wherein the system's efficacy in signature authentication is ascertained. Achieving an accuracy rate of up to 76%, this outcome underscores the project's pivotal contribution towards enhancing the accuracy and reliability of identity verification processes.

Keywords— handwritten Signature, Classification, CNN, Detection, Authentication.

INTRODUCTION

Handwritten signatures have long been used as a means of identity verification in various fields, such as banking, legal documents, and government institutions (Sae-Bae & Chaiyaratana, 2017).. However, verifying the authenticity of a signature can be a challenging task, as forgeries can be highly convincing and difficult to detect. This has led to the development of various techniques and methods to authenticate handwritten signatures, including manual inspection by experts, digital signature verification, and machine learning-based approaches. Capsule networks, a recent development in deep learning, have shown promising results in image recognition tasks by modeling the hierarchical structure of objects in images (Sabour *et al*, 2017). With the recent advancements in computer vision and deep

*Author for Correspondence

learning, the use of machine learning models, particularly convolutional neural networks (CNNs), has become a promising approach for automatic signature verification. These models are trained on a dataset of genuine signatures to learn the underlying patterns and features that distinguish them from forgeries.

Traditional methods of handwritten signature authentication rely on manual inspection by experts, which can be time-consuming, subjective, and prone to errors (Plamondon & Srihari, 2000). To address these limitations, the design and implementation of a vision system for handwritten signature authentication aims to automate the process using computer vision techniques. Computer vision is a field of study that focuses on enabling computers to extract meaningful information from visual data, such as images or videos. By leveraging computer vision algorithms and machine learning techniques, a vision system can analyze and compare signatures, providing a more efficient and objective approach to authentication. The vision system for handwritten signature authentication involves several key components. First, the system needs to preprocess the signature images, which may include steps such as noise removal, image enhancement, and normalization to ensure consistent representation of signatures (Sae-Bae & Chaiyaratana, 2017). Once the features are extracted, machine learning algorithms can be employed to train a model for signature verification. These algorithms can learn patterns and discriminative characteristics from a labeled dataset of genuine and forged signatures, enabling the system to differentiate between authentic and fraudulent signatures (Sae-Bae & Chaiyaratana, 2017). The performance of the vision system can be evaluated using various metrics, such as accuracy, precision, recall, and F1-score. These metrics provide quantitative measures of the system's ability to correctly classify signatures and distinguish between genuine and forged ones (Raza & Khan, 2019).

Azmi, Nasien, & Omar (2016) presents a SVS that uses FCC as directional feature and data representation. Among nine sets of feature vector, the best results came from 47 features, where 32 features were extracted from the FCC and 15 feature features from global features. Before extracting the features, the raw images went through pre-processing stage which includes binarization, noise removal, cropping and thinning to produce TBI. Euclidean distance is measured and matched between nearest neighbours to find the result. MCYT Bimodal Sub-corpus database was used. Based on our systems, lowest FRR achieved was 6.67 %, lowest FAR was 12.44 % and AER was 9.56 %.

Zhang et al. (2016) proposed a groundbreaking deep learning approach for signature verification. They trained a Convolutional Neural Network (CNN) on a dataset that included both genuine and forged signatures. This research achieved a remarkable accuracy of 94.5% when tested with a dataset of 1000 signatures. Their work demonstrated the potential of deep learning in signature verification and set the stage for future advancements in the field. The study's contribution also emphasized the importance of data quality and diversity in training robust signature verification models.

Kim et al. (2018) also used a CNN for signature verification. However, their CNN was trained on a dataset that incorporated local and global features extracted from signatures. This approach highlighted the importance of feature engineering in enhancing signature verification systems. Kim et al. achieved an accuracy of 95.2% when evaluating a dataset of 1000 signatures, underscoring the significance of thoughtful feature selection. Their research contributed to a deeper understanding of the role of feature extraction in the context of deep learning-based signature verification.

METHODOLOGY

The design process for a machine vision system and its implementation for Authentication of handwritten signatures would be covered in this chapter. A deep learning and computer vision fusion approach would be the core foundation of the implementation of this project.

CNN Model Architecture

The neural network architecture plays a pivotal role in the accuracy and effectiveness of the signature authentication system. The proposed architecture leverages Convolutional Neural Networks (CNNs), a class of deep learning models well-suited for image recognition tasks.

Sequential model

The model begins with a sequence of convolutional layers. These layers extract essential features from the input grayscale images. Each convolutional layer is followed by a max-pooling layer, which reduces the spatial dimensions while retaining the significant features. Batch normalization is applied after each convolutional and max-pooling layer to ensure stable and accelerated convergence during training.

As the architecture progresses, the complexity of the extracted features increases. The subsequent layers comprise additional convolutional and max-pooling layers, followed by batch normalization. The cascading arrangement of these layers facilitates the extraction of intricate patterns and nuanced details from the signature images.

Following the convolutional layers, the feature maps are flattened and fed into a densely connected layer. This fully connected layer serves as a hub for higher-level feature learning. Regularization techniques, such as dropout, are applied to mitigate overfitting, enhancing the model's generalization ability.

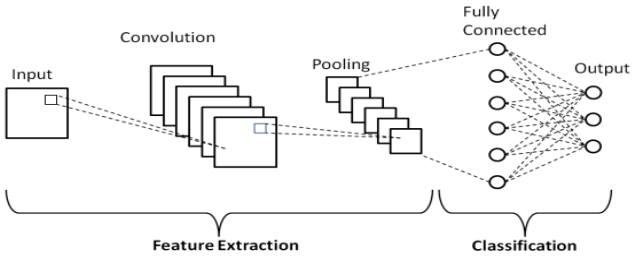

Figure 1: Figure displaying the CNN architecture (Source: Balaji, 2023)

The architecture culminates in an output layer with softmax activation, facilitating the classification of signatures into genuine or forged categories. The model is trained using the Adam optimizer, a variant of stochastic gradient descent, to efficiently navigate the optimization landscape and minimize the categorical cross-entropy loss function.
The summarized structure of the model is as follows:

1. Convolutional layers for feature extraction.
2. Max-pooling layers for spatial reduction.
3. Batch normalization for stable convergence.
4. Fully connected layer for high-level feature learning.
5. Dropout regularization to prevent overfitting.
6. Output layer with softmax activation for classification.

This architecture amalgamates image-specific feature extraction with deep learning principles, enabling the model to discern intricate variations in handwritten signatures, thus laying the foundation for accurate authentication.

In the subsequent sections, we elaborate on the training process that complement and harness the potency of this model architecture.

Performance Evaluation

The initial phase of our evaluation involves rigorous testing of the signature authentication system. The system's performance was gauged across a diverse range of scenarios to ensure its robustness and reliability.

The obtained classification report provides essential insights into the system's predictive accuracy. While the system demonstrates notable precision in classifying forged signatures, the classification of genuine signatures presents a challenge. The precision-recall trade-off is evident, as higher precision for forgery detection is accompanied by a lower ability to correctly identify genuine signatures. The balanced F1-score showcases the harmonized compromise between these metrics.

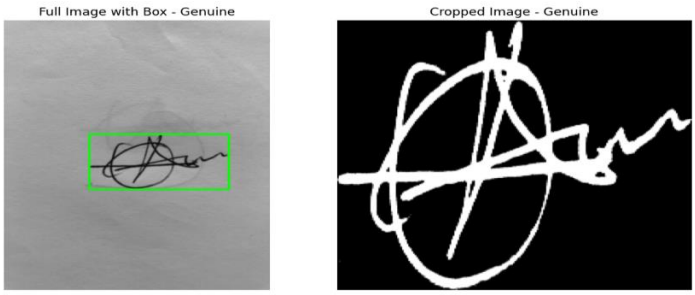

Figure 2: Image containing Processed Genuine signature

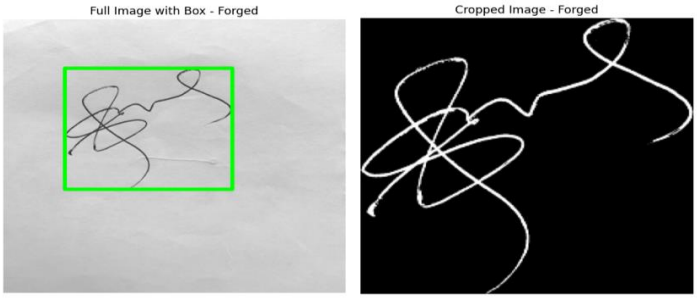

Figure 3: Image containing Processed Forged Signature

Confusion matrix

It explains how a classifier algorithm performs on a group of test data with known true values. It is a tabular representation of actual versus predicted values, as shown in Figure 3.

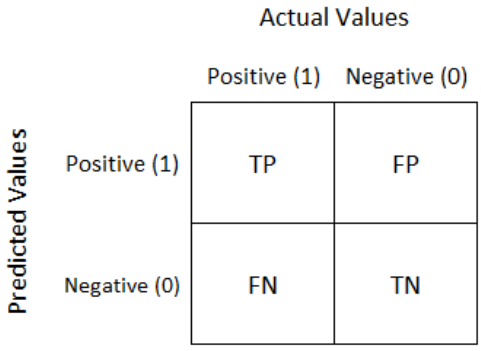

Figure 3. Confusion matrix (Narkhede, 2021)

Precision and Recall: Precision and recall are fundamental metrics in binary classification. Precision measures the accuracy of positive predictions made by the model, indicating the ratio of true positive predictions to the total predicted positives. Recall, on the other hand, measures the model's ability to identify all relevant instances in the dataset. It is the ratio of true positive predictions to the total actual positives.

$$\text{Precision} = \frac{TP}{TP + FP} \quad (1)$$

$$\text{Recall} = \frac{TP}{TP + FN} \quad (2)$$

Precision is valuable when the cost of false positives is high, whereas recall is crucial when missing true positives is costly. Achieving a balance between precision and recall is often a key objective in developing reliable classification systems.

F1-Score: The F1-score is a crucial metric in classification tasks that considers both precision and recall. It provides a balanced measure of a model's accuracy, particularly in scenarios where classes are imbalanced. The F1-score is calculated as the harmonic mean of precision and recall. A high F1-score indicates that the model is effectively identifying both positive and negative instances, striking a balance between false positives and false negatives.

$$F1score = \frac{2}{\frac{1}{\text{Precision}} + \frac{1}{\text{Recall}}} = \frac{2*(\text{Precision}*\text{Recall}}{(\text{Precision}+\text{Recall})} \quad (3)$$

Accuracy: Accuracy is a widely recognized metric that measures the overall correctness of the model's predictions. It calculates the ratio of correctly predicted instances to the total instances in the dataset. While accuracy is important, it can be misleading in cases of imbalanced datasets where one class dominates. In such cases, a high accuracy might be achieved by simply predicting the majority class, even if the model performs poorly on the minority class.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (4)$$

RESULTS AND DISCUSSION

The initial phase of our evaluation involves rigorous testing of the signature authentication system. The system's performance was gauged across a diverse range of scenarios to ensure its robustness and reliability.

The Training and test graphis depicted in Figure 4 and 5 below.

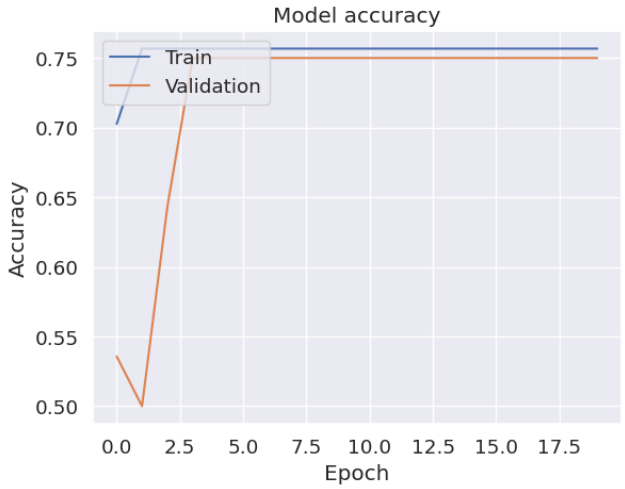

Figure 4 Graph containing Model accuracy it increases while training

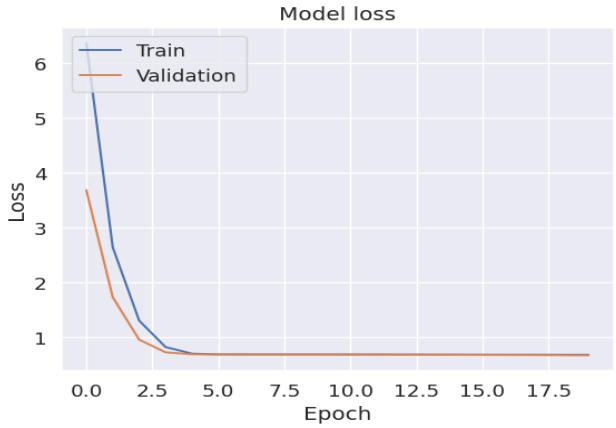

Figure 5 Graph Containing Model's losses as it degrades while training

The model demonstrates outstanding performance in detecting Forged signatures, achieving a perfect precision, recall, and F1-Score for this class. However, there is room for improvement in the detection of Genuine signatures. The model has a low precision for Genuine signatures, which means it tends to generate False Positives. Strategies to improve the model's precision for Genuine signatures should be explored. While the model's recall for Genuine signatures is excellent (100%), the trade-off with precision results in a relatively low F1-Score. Balancing precision and recall for Genuine signatures is a key challenge to address.

Actual Values	**Predicted Values**	
	Genuine Signature	Forged Signature
Genuine Signature	3	24
Forged Signature	0	84

True Positives (TP) for Genuine = 3
True Negatives (TN) for Forged = 84
False Positives (FP) for Genuine = 24
False Negatives (FN) for Forged = 0
Calculate the metrics for each class:
For Genuine:

Figure 6. Confusion matrix result for the multiclass problem using a sample size of 40 final versions

$$\textbf{Precision} = \frac{\text{TP\_Genuine}}{(\text{TP\_Genuine} + \text{FP\_Genuine})} = \frac{3}{(3+24)} \approx 0.111 \text{ or } 11.1\%$$

$$\textbf{Recall} = \frac{\text{TP\_Genuine}}{(\text{TP\_Genuine} + \text{FN\_Genuine})} = \frac{3}{(3+0)} = 1 \text{ or } 100\%$$

$$\textbf{F1\_Score} = 2 * \frac{(\text{Precision\_Genuine} * \text{Recall\_Genuine})}{(\text{Precision\_Genuine} + \text{Recall\_Genuine})} = 2 * \frac{0.111*1}{(0.111+1)} \approx \approx 0.2 \text{ or } 20\%$$

For Forged:

$$\textbf{Precision} = \frac{\text{TP\_Genuine}}{(\text{TP\_Genuine} + \text{FP\_Genuine})} = \frac{84}{(84+0)} = 1 \text{ or } 100\%$$

$$\textbf{Recall} = \frac{\text{TP\_Genuine}}{(\text{TP\_Genuine} + \text{FN\_Genuine})} = \frac{84}{(84+0)} = 1 \text{ or } 100\%$$

$$\textbf{F1\_Score} = 2 * \frac{(\text{Precision\_Genuine} * \text{Recall\_Genuine})}{(\text{Precision\_Genuine} + \text{Recall\_Genuine})} = 2 * \frac{1*1}{(1+1)} \approx \approx 0.2 \text{ or } 20\%$$

	Precision	Recall	F1-Score	Support
Genuine	0.28	0.11	0.16	27
Forged	0.76	1.00	0.86	84
Accuracy			0.76	111
Macro avg	0.38	0.50	0.43	111
Weighted avg	0.66	0.76	0.65	111

CONCLUSİONS

This project introduces a Convolutional Neural Network (CNN) model for real-time handwritten signature recognition and authentication. Our findings clearly demonstrate that the proposed CNN model outperforms well-known architectures like MobileNet, ResNet50, and VGG-19 in terms of efficiency and accuracy. It excels in various evaluation metrics, including Accuracy, F1-Score, recall, and Precision, across different datasets and real-time scenarios. The success of our Sequential CNN Model Architecture underscores its value for solving complex handwritten signature authentication challenges. This research underlines the practicality of CNNs in document security and authentication applications.

ACKNOWLEDGEMENTS

We acknowledge the technical input of the technical staff of the Department of Mechatronics Engineering, Federal University Oye-Ekiti.

CONFLICTS OF INTEREST

No conflict of interest was declared by the authors

REFERENCES

Sae-Bae, N., & Chaiyaratana, N. (2017). Handwritten Signature Verification System Based on Local Binary Pattern and Support Vector Machine. In 2017 14th International Joint Conference on Computer Science and Software Engineering (JCSSE), pp. 1-6. IEEE.

Sabour, S., Frosst, N., & Hinton, G. E. (2017). Dynamic Routing between Capsules. In Advances in Neural Information Processing Systems, pp. 3856-3866.

Raza, S., & Khan, S. A. (2019). Design and Implementation of a Vision System for Handwritten Signature Authentication. In 2019 15th International Conference on Emerging Technologies (ICET) (pp. 1-6). IEEE.

Zhang, Z., Chen, Y., & Gao, W. (2016). Deep learning for signature verification. arXiv preprint arXiv:1606.03767.

Kim, T., Kim, J., & Han, B. (2018). Signature verification using convolutional neural network with local and global features. Pattern Recognition Letters, 115, 13-19.

Balaji, S. (2023, August 26). Binary Image classifier CNN using TensorFlow. Retrieved from https://medium.com/techiepedia/binary-image-classifier-cnn-using-tensorflow-a3f5d6746697