Novateur Publications
International Journal of Innovations in Engineering Research and Technology [IJIERT]
ISSN: 2394-3696 Website: ijiert.org
Volume 11, Issue 03, March-2024

CONTRIBUTION TO THE AUTHENTICITY OF DIGITIZED HANDWRITTEN SIGNATURES THROUGH DEEP LEARNING WITH RESNET-50 AND OCR

Tsanta Christelle Nadège Ralaibozaka
Ecole supérieure de Polytechnique d’Antananarivo,
University of Antananarivo, Antananarivo, Madagascar
*ralaichristel@gmail.com

Maminiaina Alphonse Rafidison
Ecole supérieure de Polytechnique d’Antananarivo,
University of Antananarivo, Antananarivo, Madagascar
*mamynyaina@gmail.com

Hajasoa Malalatiana Ramafiarisona
Ecole supérieure de Polytechnique d’Antananarivo,
University of Antananarivo, Antananarivo, Madagascar
* mhramafiarisona@yahoo.fr

Article History: *Received on: 10/01/2024*
Accepted on: 19/03/2024

DOI: *https://doi.org/10.26662/ijiert.v11i3.pp20-25*

ABSTRACT

This paper explores the contribution of authenticity to digitized handwritten signatures using a deep learning-based approach, implementing ResNet-50 and optical character recognition (OCR). Signature authentication is a crucial issue in various fields, such as transaction security, protection of official documents, and fraud prevention. Our approach aims to improve the reliability of signature verification systems by exploiting the advanced capabilities of deep neural networks. Experimental results demonstrate a high authentication accuracy of 94% on our collected database and 100% on ICDAR 2011, validating the effectiveness of the proposed approach. The advantages of this method include more excellent resistance to circumvention techniques, adaptability to different signature styles, and robustness against intentional tampering.

I. INTRODUCTION

Authenticating handwritten signatures has long been an essential process for guaranteeing the security and validity of official documents. With the advent of digital technologies, the need to develop more sophisticated verification methods has increased. Deep learning offers a promising solution, enabling in-depth analysis of signatures' subtle characteristics. This article looks at using ResNet-50, a deep neural network architecture, in conjunction with OCR to improve the authentication accuracy of digitized handwritten signatures.

II. METHODS

We chose ResNet-50 because of its ability to process complex images and extract meaningful features.

The process of an authentication system

A classification system for signature verification typically involves the following steps: acquisition, pre-processing, segmentation, feature extraction, feature selection and classification.

1.1.1 Data acquisition

The dataset plays a central role in forming a signature authentication model. For this study, two primary data sources were exploited:

- public databases: We examined freely available datasets, often used in similar research work. This ensures a broader comparison of the model's performance with existing approaches.
- Customized collections: Signatures have been collected in a customized way to enrich the diversity of the data.

Each of these sources is evaluated according to its relevance and representativeness regarding the diversity of writing styles.

1.1.2 Selection criteria

Signature selection criteria have been rigorously defined to guarantee the quality and diversity of the training set. Criteria included:

- signature clarity: only clear signatures were retained, avoiding excessive overlap and distortion.
- diversity of signatories: the dataset was designed to include signatures from people of different ages, professions, and cultural backgrounds.
- Variability of scanning conditions: To reinforce the model's robustness, signatures were acquired under different lighting conditions, resolutions, and orientations.

1.2 Deep learning with ResNet-50

1.2.1 ResNet-50 architecture

ResNet-50, a deep convolutional neural network architecture, was selected to effectively capture complex features. This section offers a detailed explanation of the ResNet-50 architecture, highlighting its residual blocks, depth, and specific use for the signature authentication task.

1.2.2 Adapting ResNet-50 to the task of signature authentication

Adapting ResNet-50 for the specific task of signature authentication requires careful adjustments to guarantee optimum performance in recognizing the unique characteristics of handwritten signatures.

1.2.2.1 **Signature image pre-processing**

Signature images are specifically pre-processed before being fed into ResNet-50. Details of the transformations applied, such as normalization, regularization, and color transformation, are provided. These preprocessing are designed to maximize ResNet-50's ability to extract discriminating features from signatures.

1.2.3 Performance measurement

To evaluate our performance throughout the study, we decided to consider the metrics of precision, recall, accuracy and F1 score. However, let's try to understand the information provided by each of these metrics.[1]

1.2.3.1 **Precision**

Precision is the ratio of true positives to the sum of false positives and true negatives (formula (2.01)). It is also known as positive predictive value.

$$Precision = \frac{\text{True Positives}}{\text{True Positives} + false\ positives} \tag{2.01}$$

$$= \frac{\text{True Positives}}{positive\ predictive\ value} \tag{2.02}$$

1.2.3.2 **Recall**

Recall is the ratio of correctly predicted results to all predictions (formula (2.02)). It is also called sensitivity or specificity.

$$recall = \frac{true\ positives}{true\ positives + false\ negatives} \tag{2.03}$$

$$= \frac{true\ positives}{current\ positive\ value} \tag{2.04}$$

1.2.3.3 **Accuracy**

Accuracy is the ratio of correct predictions to all predictions made by an algorithm (formula (2.05)).

$$Accurary = \frac{(TP + TN)}{(TP + FP + TN + FN)} \tag{2.05}$$

1.2.3.4 **F1 score (F-measure)**

The F1 score combines these three measures into a single measure ranging from 0 to 1 and considers both precision and recall (formula (2.06)).

$$F1 = 2 \times \frac{precision * recall}{precision\ + recall} \tag{2.06}$$

1.2.4 Model training

The process of training the ResNet-50 model for signature authentication is a critical step that requires careful planning and constant monitoring.

1.2.4.1 **Data set partitioning**

The criteria used to partition the dataset into training and test sets are detailed, including strategies based on randomization. Justification for the selected criteria is provided, highlighting their impact on the representativeness of each set.

1.2.4.2 **Training monitoring**

Confusion matrices, dynamically updated during training, are examined to assess the model's ability to discriminate between different signature classes.[2]
Tables 1 shows the confusion matrix.

Tables 1. Confusion matrix

Confusion matrix		**Reality**	
		Genuine	**Falsification**
Prediction	**Genuine**	True Positive	False Positive
	Falsification	False Negative	True Negative

Learning monitoring is essential for evaluating model performance throughout the training process. The creation and analysis of learning curves are detailed. This includes graphs illustrating the evolution of performance metrics (precision, recall, F1-score, etc.) on the training and test set over time.

III. Results

For our study, we used 2 data.

- For the first database: we used handwritten signatures collected by people who have signed documents. Tables 2. illustrates the performance measures based on the confusion matrix.

Tables 2. Performance measurement based on collected data

Precision	**Recall**	**Accuracy**	**F1 score**
0,94	0,73	0,79	0,82

- For the second database, we used an ICDAR 2011 database from the SigComp international signature verification competition of the International Conference on Document Analysis and Recognition. Tables 3. shows the performance measures based on the confusion matrix

Tables 3. Mesure de performance sur la base de données ICDAR 2011 SigComp

Précision	**Recall**	**Accuracy**	**F1 Score**
1	0,89	0,94	0,94

Figures 2.01 and 2.02 illustrate the results of our study on signature authenticity performance.

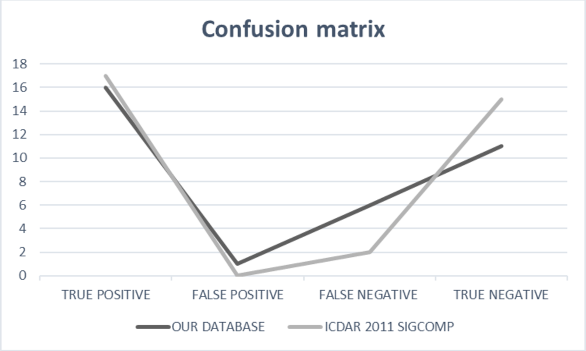

Figure 1.01 : Confusion matrix

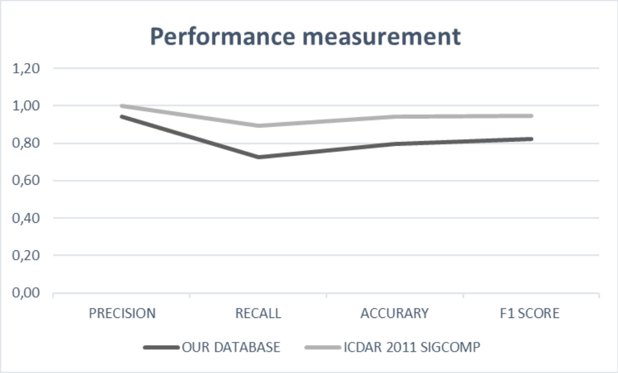

Figure 1.02 : Performance measurement

1.3 Interpretation of results

- High precision suggests that the model minimizes misclassification of genuine signatures.
- High recall indicates that the model is effective in detecting most genuine signatures.
- Accuracy gives an overview of the model's overall performance.
- A high F1 Score confirms a balance between accuracy and recall, crucial for tasks where false positives and false negatives have significant implications.

The encouraging results of this study suggest that our signature authentication system achieves high levels of precision and reliability.

IV. Discussion

The study of the impact of the signatures selected revealed that high performance is mainly achieved for simple signatures, which are not very complex to execute. The data used is effective for simple signatures, but insufficient for more complex signatures. In some cases, obtaining new signatures from the authentic user can strengthen the database and improve the efficiency of the authentication system. The addition of digitized handwritten signatures helped to improve performance, underlining the importance of handwritten signatures for effective authentication. Despite the positive results, limitations such as image quality, the diversity of handwriting styles and subtle variations need to be considered, underlining the need to improve the robustness of the model. Compared with other work, our authentication system generally achieved better results, demonstrating its effectiveness. However, future research could improve the methodology, explore new network architectures, or integrate advanced OCR techniques. Extending the approach to other document types, such as legal forms or contracts, could also extend its scope.

V. Conclusion

Authenticating digitized handwritten signatures is a crucial challenge in document security. This innovative study, based on deep learning with ResNet-50 and advanced OCR techniques, opens up promising prospects for electronic transaction security and fraud prevention. The results demonstrate the effectiveness of ResNet-50 in capturing discriminating signature features, thanks to seamless integration with OCR, resulting in a consistent model. Practical applications are wide-ranging, offering solutions to enhance online security and prevent document forgery. However, the limitations of the study, such as variable image quality and diverse handwriting styles, need to be acknowledged. Future research should focus on methodological improvements and the exploration of more sophisticated architectures, broadening the scope of application. Despite the challenges, the commitment to excellence persists, anticipating future iterations to raise document security standards with continued advances in deep learning and OCR. This significant contribution places ResNet-50 and OCR at the heart of an innovative approach, underlining the importance of continuing this exploration to shape a more secure and reliable digital future.

REFERENCES

1 https://www.nomidl.com/machine-learning/what-is-precision-recall-accuracy-and-f1-score/ consulted july 2023

2 https://kobia.fr/classification-metrics-precision-cprecall/#:~:text=La%20precision%20est%20%C3%A9galement%20appel%C3%A9e,lors%20d'une%20pr%C3%A9diction%20positive consulted july 2023