Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th February 2025. Vol. 4. No. 2; e-ISSN: 2808-4519

Authenticity Accuracy Improvement Through the Analysis of Signature Ownership Using Convolutional Neural Network Algorithm

Sangdiah[1]*, Nana Suarna[2], Irfan Ali[3], Dendy Indriya Efendi[4]

[1,2] Faculty of Informatics Engineering, STMIK IKMI, Cirebon, Indonesia
[3] Faculty of Software Engineering, STMIK IKMI, Cirebon, Indonesia, Indonesia
sangdiahcirebon@gmail.com [1*]

Abstract

This research aims to improve the accuracy of signature authenticity classification using a Convolutional Neural Network (CNN) model, implemented in a web-based application using the Flask framework. In the digital era, signature authentication has become a crucial component in maintaining data security and transaction validity. However, the classification of genuine and forged signatures presents its own challenges due to the unique variations in patterns and styles of each individual. Using a public dataset from Kaggle consisting of 1,084 signature images (620 forged and 464 genuine), the CNN model was trained to recognize important patterns that can differentiate genuine signatures from forged ones. The research stages include data preprocessing, CNN model training, and evaluation using Confusion Matrix metrics, including precision, recall, and F1-score, to ensure the accuracy of prediction results. The results show that the implemented CNN model achieved an accuracy of 98% in signature classification, proving its effectiveness in distinguishing between genuine and forged signatures. Additionally, the integration of the model into a Flask-based application allows users to upload signature images and receive real-time classification results, enhancing user convenience and practicality. In conclusion, this CNN model can serve as a reliable signature-based authentication solution and has the potential to be applied in various digital security applications. This research contributes to the development of more advanced and secure digital signature authentication systems.

Keywords: *Convolutional Neural Network, Authenticity of Signature, Prediction Accuracy*

1. Introduction

The rapid advancements in the field of informatics have significantly influenced various aspects of human life, including technology, business, and education. Continuous progress in information technology has introduced numerous innovations that simplify communication, business transactions, and distance learning. In the technological realm, the integration of artificial intelligence and computational algorithms enhances machines' capabilities in processing information, analyzing data, and making predictions. Within the business sector, automation through information technology boosts operational efficiency while reducing human error. However, these advancements also bring new challenges, such as ensuring data security and authenticity, particularly in the implementation of digital signatures.

The authenticity of a digital signature is vital, as it guarantees the validity and integrity of electronic documents amidst the widespread adoption of digital technology. In the field of informatics, signature forgery poses a serious issue, compromising the security and reliability of identity verification systems. The evolution of digital technology has made forging signatures increasingly sophisticated, directly impacting the credibility of authentication processes. Traditional manual verification methods often struggle to detect forged signatures accurately, as humans have limitations in identifying subtle differences between genuine and fake signatures. Consequently, there is a pressing need for more robust and precise technology-based solutions, particularly for systems relying on signature authentication as a core security measure. Convolutional Neural Networks (CNNs) provide a promising approach, thanks to their advanced capabilities in recognizing patterns and visual features. Despite their strengths in image classification, challenges persist in signature classification, particularly in achieving high accuracy in distinguishing genuine from fake signatures. These challenges are further compounded by variations in individual signatures influenced by factors such as writing speed, pressure, or the device used. Additionally, there is a noticeable gap in existing literature concerning the performance analysis of CNN models in signature classification, particularly in assessing key metrics such as True Positive and False Negative rates.

This study aims to address this gap by evaluating the model using precision, recall, and F1-score, ensuring that the developed system achieves high prediction accuracy. Several previous studies have investigated the application of artificial intelligence, particularly CNN, in signature verification and pattern recognition. Research by [1] shows that CNN has superior capability in recognizing complex visual

patterns in digital signatures, resulting in higher accuracy compared to conventional methods. However, this research is still limited by the number of datasets used, which may affect the generalizability of the results. Meanwhile, [2] developed a CNN architecture for batik motif image classification, which is relevant in the context of signature verification because both involve unique pattern recognition. This study successfully implemented CNN with fairly high accuracy, but the main challenge lies in the wide variation of motifs, similar to the challenge in individual signature variations. Another study by [3] used CNN for handwriting recognition in the Lota Ende script, where they found that modifications to the CNN architecture and data pre-processing techniques could improve accuracy. This is relevant to signature verification, but this approach has not been fully implemented in the context of electronic signatures. [4] also conducted a study using CNN for fruit type classification and showed that the use of platforms such as Google Colab can improve the accessibility and efficiency of the model training process, an aspect that is still under-explored in real-time signature verification. Finally, the study by [5] focuses on the optimization of CNN accuracy in identifying garbage types, which successfully improves the accuracy through better hyperparameter selection.

This study provides insight into the importance of parameter optimization in CNN, but its application in digital signatures is still rarely explored. Although these studies have demonstrated the potential of CNN in various applications, there is still room to further explore factors such as signature variation, the use of larger datasets, and the integration of better optimization techniques to improve the accuracy in electronic signature verification. The main objective of this study is to develop a Convolutional Neural Network (CNN) model that is able to classify signatures into two categories, namely genuine and fake, with a high level of accuracy. With this model, it is expected to create a more reliable and accurate signature verification system, which ultimately can reduce the risk of identity forgery in various security applications.

This study has important significance in the field of Informatics, especially in the development of image-based verification and authentication technology, which currently still has challenges in achieving optimal accuracy. The CNN-based approach allows for deeper identification of visual patterns and textures in signatures, thereby capturing specific details that are often missed by conventional methods. In addition, this study contributes to filling the knowledge gap related to the effectiveness of CNN for signature classification on images that have varying conditions, such as differences in resolution and lighting. From a practical perspective, the results of this study have the potential to be applied to various authentication systems, such as banking services, digital documents, and other security systems that require identity verification. Thus, this study not only provides academic contributions in the use of CNN for image authentication, but also has high applicative value in improving the security and efficiency of the verification process in various sectors.

2. Research Methods

This study employs a Convolutional Neural Network (CNN) model as its methodological approach, leveraging one of the deep learning algorithms known for its efficiency in pattern recognition tasks, particularly for distinguishing between genuine and fake signatures. CNN excels at identifying and extracting crucial visual features, including edges, textures, patterns, and shape details, which are essential for verifying signature authenticity. The CNN model developed in this research is designed to classify signature images into two categories-genuine and fake-to enhance the accuracy of signature-based authentication systems.The research begins with preprocessing the signature image data, which involves critical steps such as resizing images to align with the input requirements of the model and normalizing pixel values to maintain consistency.

This normalization aims to accelerate the training process and improve model accuracy. Additionally, data augmentation is applied to the training dataset to introduce variability, enabling the model to better identify genuine and fake signatures under diverse conditions.Following preprocessing, the signature images are passed through a series of convolutional layers in the CNN model. These layers progressively extract visual features, ranging from basic to complex, to identify unique characteristics in each class. This aids the model in understanding patterns that differentiate genuine signatures from forged ones. Each convolutional layer is paired with a pooling layer, which reduces the dimensionality of the data while retaining critical information. This step not only ensures computational efficiency but also helps mitigate overfitting by focusing the representation on essential features. After feature extraction through convolutional and pooling layers, the processed data is fed into a fully connected (dense) layer. This layer integrates the extracted features to form meaningful information, which is used for the final prediction. The classification process is concluded using the softmax activation function, which calculates the probability of each class-genuine or fake-allowing the model to select the most likely category for a given input. To enhance model accuracy and generalization, regularization techniques such as dropout are incorporated. Dropout reduces dependency on specific neurons by randomly deactivating them during training, thereby minimizing the risk of overfitting. Additionally, hyperparameter tuning is conducted to optimize the model's performance. Adjustments are made to parameters such as batch size, learning rate, and the number of epochs to ensure consistent and accurate signature recognition. Once the model is trained, its performance is evaluated using metrics like accuracy, precision, recall, and F1-score. Accuracy measures the proportion of correct predictions, while precision assesses how well the model correctly identifies genuine or fake signatures without significant errors. Recall evaluates the model's ability to identify all instances of a specific class, critical for minimizing missed detections. The F1-score, as the harmonic mean of precision and recall, offers a balanced assessment, particularly in cases of class imbalance between genuine and fake signatures. By analyzing the prediction results through these metrics, the CNN model is expected to deliver reliable and accurate classification outcomes for signature verification. This approach not only focuses on achieving high accuracy but also ensures the model's robustness in detecting signature authenticity. The findings hold potential applications in authentication systems requiring high security, such as identity verification in digital environments. Consequently, this research makes a meaningful contribution to enhancing trust and security in systems relying on digital signatures.

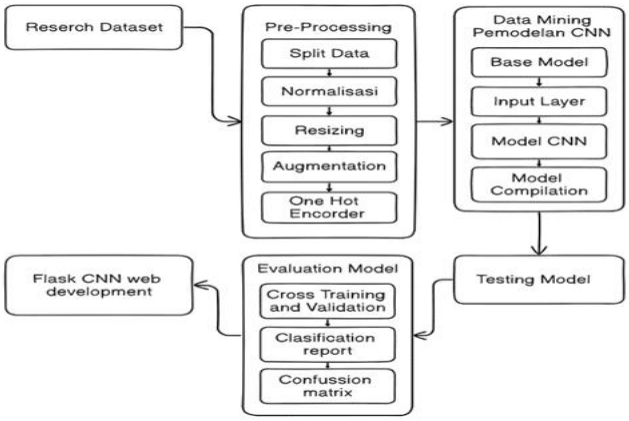

Fig. 1: Research Methods

3.1. Data selection

In this study, the data collection technique used is secondary data collection through the Kangle platform. The dataset obtained consists of 1,084 signature images that have been labeled as genuine or forged, with each category totaling 620 forge signatures and 464 genuine signatures.

3.2. Preprocessing

In the data preprocessing step in this study, it begins with a data split, which is dividing the dataset into three subsets with a proportion of 80% for training data, 10% for testing data, and 10% for validation data. This division is done to ensure that the model is trained, validated, and tested on separate data, so that the results of the model evaluation truly reflect its ability to classify data that has never been seen before. After the data is divided, the next step is to normalize the pixel values in each image, where the pixel values are changed to the range [0, 1] by dividing each pixel value by 255. Furthermore, for the training data, data augmentation is carried out to increase variation in the dataset and prevent overfitting. Augmentation includes random transformations on images, such as rotation, flipping, brightness changes, and zooming, so that the model learns from various conditions and is better able to recognize patterns in real data. This augmentation is only applied to training data to enrich data variation without affecting validation and testing data which must remain representative of the original distribution. The final step in preprocessing is resizing, which is changing the size of the images to the same dimensions (224x224 pixels) to fit the input of the Convolutional Neural Network (CNN) model. Resizing ensures that each image has a consistent size, so that features can be optimally extracted by the model during the training process. With these preprocessing steps, the data is prepared in the best condition to train the model efficiently and accurately in classifying real and fake signatures.

3.3. Data Mining (CNN Modeling)

After the data goes through the preprocessing stage, the next step is to build a Convolutional Neural Network (CNN) model as the main tool in the signature authenticity classification process. At this stage, the CNN model architecture is designed, including the selection of key components such as convolution, pooling, and fully connected layers that are adjusted to the characteristics of the prepared dataset. The construction of this CNN model aims to enable the network to recognize and extract specific visual patterns in the signature image, so that it can accurately distinguish between genuine and fake signatures. The selection of the right architecture and configuration in the CNN model is very important, because it will determine the effectiveness of the model in identifying relevant features that support the accuracy and reliability of the model in the desired classification task. After the Convolutional Neural Network (CNN) model has been successfully built and compiled, the next step is to test the model through the training process. The results of this model test will provide an overview of the effectiveness and stability of the model in the signature classification process.

3.4. CNN model performance evaluation

At this stage, the model will be evaluated to assess its performance on the test data. This evaluation aims to measure the generalization ability of the model in classifying genuine and fake signatures on data that has never been seen before. By using the test data, it is expected to obtain an objective picture of the accuracy and reliability of the model in handling variations that exist outside the training data. The results of this evaluation will provide important information regarding the effectiveness of the model that has been built, as well as assist in the decision-making process for the use of the model in real applications or for further improvements.

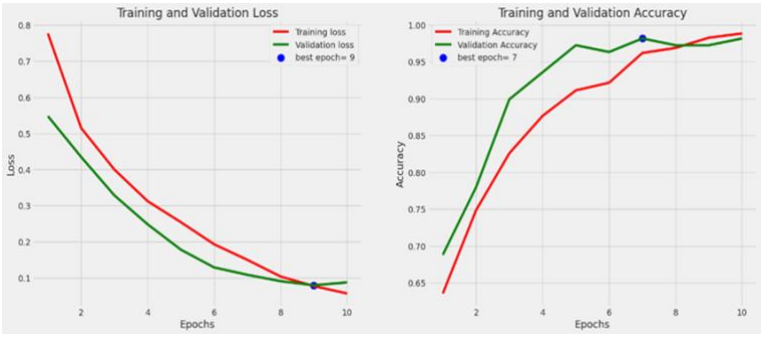

Fig. 2: Training and Validation Graphs

Overall, this graph shows that the trained CNN model has a good ability to learn and generalize patterns from both training and validation data. The consistent decrease in loss and steady increase in accuracy indicate that the model not only fits the training data but also performs well on the validation data, indicating strong generalization.
The following is an evaluation of the model using the Confusion Matrix.

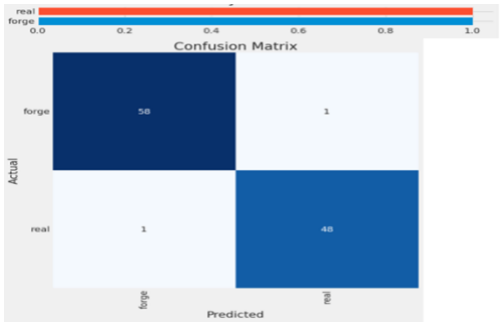

Fig. 3: Confusion Matrix

Confusion Matrix of CNN model classification results to distinguish between genuine and forged signatures. This matrix shows the model performance in terms of the number of correct and incorrect predictions in each class.

a. True Positive (TP): The model successfully classified 58 forged signatures correctly as “forged.”
b. True Negative (TN): The model also managed to correctly classify 48 authentic signatures as “real.”
c. False Positive (FP): The model incorrectly classifies 1 original signature as “forge” which means the original signature is identified as fake.
d. False Negative (FN): The model also incorrectly classified 1 fake signature as “real” which means the fake signature was identified as genuine.

The following are the results of the Classification Report:

```
Classification Report:
----------------------
              precision    recall  f1-score   support

       forge       1.00      0.95      0.97        59
        real       0.94      1.00      0.97        49

    accuracy                           0.97       108
   macro avg       0.97      0.97      0.97       108
weighted avg       0.97      0.97      0.97       108
```

Fig. 4: Classification Report

Classification Report which is the result of evaluating the performance of the Convolutional Neural Network (CNN) model on the test data. This report presents three main metrics, namely precision, recall, and f1-score for each class, namely forge (fake signature) and real (original signature). In addition, this report also includes support, which is the number of instances in each class in the test data. For the "forge" class, the precision is 1.00, which means that the model is able to correctly identify all "forge" predictions as fake without error. The recall for this class is 0.95, indicating that 95% of the fake signatures in the test data were correctly identified by the model. The f1-score, which is the harmonic mean of precision and recall, is 0.97, indicating a very good balance of performance for the "forge" class. For the "real" class, the precision is 0.94, indicating that 94% of the "real" predictions are correct. The recall for this class is 1.00, meaning that the model is able to identify all original signatures in the test data without error. The F1-score for the “real” class also reached 0.97, showing consistent performance with the “forge” class. At the bottom of the report, the overall accuracy of the model was recorded at 0.97 or 97%, indicating a very high level of accuracy on the test data. The macro avg and weighted avg values for precision, recall, and f1-score were all also at 0.97, confirming that the model has balanced and reliable performance for both classes. Overall, this classification report shows that the trained CNN model has excellent ability to distinguish real and fake signatures, with a very low error rate and high consistency across all evaluation metrics.

3.5. CNN flask web development

Flask- based Convolutional Neural Network (CNN) model to develop a web application capable of automatically classifying signature authenticity. This implementation aims to provide a platform that allows users to upload signature images and receive real-time classification results, namely predictions about the authenticity of the signature, whether it is in the original or fake category.

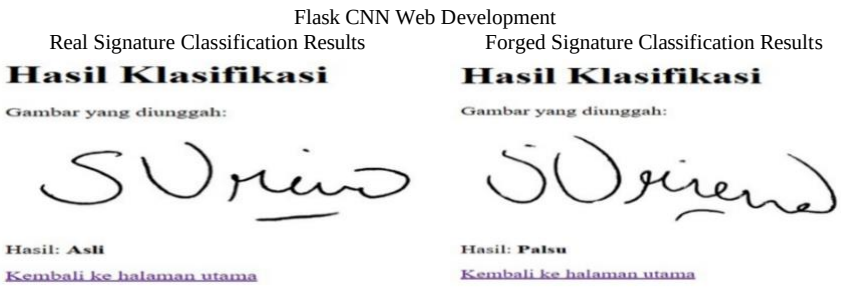

Fig. 5: Flask CNN Web Development

4. Conclusion

This study successfully implemented a Convolutional Neural Network (CNN) model for signature authenticity classification. The developed CNN model showed high capability in recognizing visual patterns in signatures, which is very useful for distinguishing between genuine and fake signatures. Preprocessing processes such as resizing, normalization, and data augmentation helped ensure data quality and improved the model's ability to recognize signature variations. The training results showed that the CNN model achieved a very high level of accuracy, with training accuracy of 99.1% and validation accuracy of 98.1%. Evaluation using precision, recall , and F1-score metrics shows that the model is not only accurate but also has a balance in classifying genuine and fake signatures. This proves that the model is able to avoid bias towards one class, which is important in the context of authentication. The Confusion Matrix results show that the model is able to minimize the classification error, with only 1 False Positive and 1 False Negative of the total predictions. This shows that the model has a very high level of reliability in distinguishing genuine signatures from fake ones, giving confidence that this model can be used in signature-based authentication applications. This research makes a significant contribution to the development of accurate and reliable CNN-based signature authentication systems. This model can be used as a basis for further development of signature verification systems, which have the potential to be used in various applications that require high security, such as banking, legal, and digital transaction systems. Although this model shows high performance, this research also opens up opportunities for further development, for example by using more diverse datasets or more complex model architectures to improve the robustness and generalization of the model.

Reference

[1] S. M. A. Navid, S. H. Priya, N. H. Khandakar, Z. Ferdous, and A. B. Haque, "Signature Verification Using Convolutional Neural Network," *2019 IEEE Int. Conf. Robot. Autom. Artif. Internet-of-Things, RAAICON 2019*, no. May, pp. 35–39, 2020, doi: 10.1109/RAAICON48939.2019.19.

[2] A. Prayoga, Maimunah, P. Sukmasetya, Muhammad Resa Arif Yudianto, and Rofi Abul Hasani, "Arsitektur Convolutional Neural Network untuk Model Klasifikasi Citra Batik Yogyakarta," *J. Appl. Comput. Sci. Technol.*, vol. 4, no. 2, pp. 82–89, 2023, doi: 10.52158/jacost.v4i2.486.

[3] R. Aryanto, M. Alfan Rosid, and S. Busono, "Penerapan Deep Learning untuk Pengenalan Tulisan Tangan Bahasa Aksara Lota Ende dengan Menggunakan Metode Convolutional Neural Networks," *J. Inf. dan Teknol.*, vol. 5, no. 1, pp. 258–264, 2023, doi: 10.37034/jidt.v5i1.313.

[4] Edwin Febrywinata, "Pengenalan Dan Klasifikasi Jenis Buah Menggunakan Metode CNN Secara Sederhana Dengan Menggunakan Google Colab," *Merkurius J. Ris. Sist. Inf. dan Tek. Inform.*, vol. 2, no. 4, pp. 185–193, 2024, doi: 10.61132/merkurius.v2i4.162.

[5] Rima Dias Ramadhani, A. Nur Aziz Thohari, C. Kartiko, A. Junaidi, T. Ginanjar Laksana, and N. Alim Setya Nugraha, "Optimasi Akurasi Metode Convolutional Neural Network untuk Identifikasi Jenis Sampah," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 2, pp. 312–318, 2021, doi: 10.29207/resti.v5i2.2754.

[6] I. G. Adnyana, P. Sugiartawan, and I. N. B. Hartawan, "Hyperparameter Optimization Techniques for CNN-Based Cyber Security Attack Classification," no. x, pp. 1–11, 2012, doi: 10.22146/ijccs.xxxx.

[7] E. Setia Budi, A. Nofriyaldi Chan, P. Priscillia Alda, and M. Arif Fauzi Idris, "RESOLUSI : Rekayasa Teknik Informatika dan Informasi Optimasi Model Machine Learning untuk Klasifikasi dan Prediksi Citra Menggunakan Algoritma Convolutional Neural Network," *Media Online*, vol. 4, no. 5, p. 509, 2024, [Online]. Available: https://djournals.com/resolusi

[8] I. P. W. Prasetia and I Made Gede Sunarya, "Image Classification of Balinese Seasoning Base Genep Based on Deep Learning," *J. Nas. Pendidik. Tek. Inform.*, vol. 13, no. 1, 2024, doi: 10.23887/janapati.v13i1.67967.

[9] Tri Wahyu Qur'ana, "Implementasi Metode Convolutional Neural Network (CNN) untuk Klasifikasi Motif pada Citra Sasirangan," *Media Inform.*, vol. 7, no. 2, p. 10, 2023, [Online]. Available: http://jurnal.big.go.id/index.php/GM/article/view/810

[10] J. Naranjo-Torres, M. Mora, R. Hernández-García, R. J. Barrientos, C. Fredes, and A. Valenzuela, "A review of convolutional neural network applied to fruit image processing," *Appl. Sci.*, vol. 10, no. 10, 2020, doi: 10.3390/app10103443.

[11] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," *Commun. ACM*, vol. 60, no. 6, pp. 84–90, 2017, doi: 10.1145/3065386.

[12] L. Husna and S. Novia Rizki, "Pemanfaatan JST Pengenalan Keaslian Pola Tanda Tangan untuk Pencegahan Tindakan Pemalsuan Tanda Tangan," *J. Tek. Inform. Unika ST. Thomas*, vol. 08, no. 01, pp. 2657–1501, 2023.

[13] A. M. Triutama, "KLASIFIKASI PENYAKIT TANAMAN PADA DAUN KENTANG DENGAN METODE CONVOLUTIONAL NEURAL NETWORK ARSITEKTUR MOBILENET," vol. 9, no. 9, pp. 356–363, 2022.

[14] M. Tripathi, "Analysis of Convolutional Neural Network based Image Classification Techniques," *J. Innov. Image Process.*, vol. 3, no. 2, pp. 100–117, 2021, doi: 10.36548/jiip.2021.2.003.

[15] S. Patil, A. Pawar, S. Khanna, A. Tiwari, and S. Trivedi, "Computer Technology & Applications Text Summarizer using NLP (Natural Language Processing)," *J. Comput. Technol. Appl.*, vol. 12, no. 3, pp. 1–6, 2021, doi: 10.37591/JoCTA.

[16] A. E. Ilesanmi and T. O. Ilesanmi, "Methods for image denoising using convolutional neural network: a review," *Complex Intell. Syst.*, vol. 7, no. 5, pp. 2179–2198, 2021, doi: 10.1007/s40747-021-00428-4.