TIFDA JOURNAL
Technology Information and Data Analytic
Website Jurnal : http://jeptira.id/index.php/tifda
e-ISSN : 3064-0660

Development of a Digital Signature Classification Information System for Documents at Darma Persada University

Yahya[1*], Eva Novianti[1], Anand Fiardhi Ramadhan[1]
[1]Department of Information System, Faculty of Engineering, Darma Persada University
[1]Jl Taman Malaka Selatan No.8, Jakarta Timur, 13450, Indonesia
*yahya@ft.unsada.ac.id

Abstract — Digital signatures are essential for verifying document validity and legal validation. Nevertheless, manual verification is susceptible to human error, particularly when processing low-quality or counterfeit signature photos. This study seeks to create a web-based Digital Signature Classification Information System to aid administrative personnel at the Faculty of Engineering, Universitas Darma Persada, in precisely and efficiently authenticating document signatures. The system utilizes image processing methods and a convolutional neural network (CNN) for the automatic classification of authentic and counterfeit signatures. The dataset was partitioned with a 70:30 training to testing ratio to assess model efficacy. Experimental results indicate that the proposed method attained a testing accuracy of 92.1%, evidencing dependable performance in differentiating between legitimate and faked signatures. The system's application markedly decreases verification duration and enhances consistency relative to manual inspection. The results demonstrate that the suggested system offers an efficient alternative for improving document security and facilitating administrative authentication operations.

Keywords – Information System, Classification, Digital Signature

I. INTRODUCTION

The rapid development of digital technologies has transformed the way authentication and document verification processes are conducted. Smartphones, computers, and web-based systems are now widely used to support administrative activities, including digital signature processing and verification. In recent years, digital signatures have become an essential component of document authentication due to their ability to provide identity validation, integrity assurance, and legal binding properties in electronic documents [1][2]. Advances in pattern recognition and image processing have enabled the automatic evaluation of signature characteristics, making it possible to distinguish between genuine and forged signatures with greater accuracy than traditional manual inspection methods [3][4].

Recent advancements in deep learning have expanded the capabilities of offline signature verification systems. Numerous recent research illustrate the efficacy of convolutional neural networks (CNNs) in offline handwritten-signature classification, with great accuracy and resilience, even when confronted with falsified or deteriorated signature images [11][12][13]. Certain studies additionally suggest innovative network designs and loss functions aimed at augmenting discriminative capability, thereby enhancing the detection of adept forgeries [14]. Additionally, web-based signature verification systems that integrate CNN-based categorization with online accessibility have been suggested to enable practical use in institutional settings.

At Universitas Darma Persada, namely in the Administrative Office of the Faculty of Engineering, the utilization of digital signatures for internal documentation has been on the rise. Nonetheless, authorization remains a manual process, and the utilization of an individual's digital signature necessitates explicit consent to prevent misuse. Notwithstanding the shift to digital formats, some administrative processes, such the authentication of signatures in the “Dokumen Pengantar Pengambilan Ijazah”, persist in a semi-manual state. Staff often face difficulties in certifying low-quality digital signatures that may be smudged, poorly scanned, or irregular in shape. These problems frequently lead to erroneous evaluations, delays in document processing, and susceptibility to possible forgeries efforts.

Prior research in digital signature verification highlights the effectiveness of automated classification approaches based on image processing, machine learning, and artificial neural networks [5][6]. Techniques such as feature extraction, contour analysis, deep learning–based recognition, and hybrid classification models have demonstrated high accuracy in distinguishing between genuine and forged signatures [7][8]. Web-based verification systems have also been widely adopted due to their accessibility, scalability, and ease of integration with administrative workflows [9][10]. However, many existing studies focus on general-purpose biometric authentication systems, often using public or benchmark datasets under controlled conditions, with limited exploration of implementation in institutional administrative contexts such as universities.

This gap highlights the need for a digital signature classification system designed for the document processing workflow of the Faculty of Engineering at Universitas Darma Persada. A system must precisely evaluate real-world administrative signature images, aid staff in verifying document validity, and reduce reliance on manual inspection. This project aims to develop a web-based Digital Signature Classification Information System that integrates image processing and automated classification methods (employing CNN) to improve the efficiency and reliability of signature verification for administrative personnel.

II. METHODOLOGY

This study adopts the Extreme Programming (XP) methodology as the system development approach. XP was selected due to its suitability for software projects that require rapid development, continuous testing, and frequent user feedback, particularly in machine learning–based systems such as digital signature classification. The iterative nature of XP ensures that system improvements can be continuously implemented based on real user interaction and model evaluation.

The development process begins with the planning phase, in which system requirements are identified through direct observation and interviews with administrative staff at the Faculty of Engineering, Universitas Darma Persada. At this stage, the main functional requirements are defined, including user authentication, digital signature upload, dataset labeling, CNN-based training, signature classification, document upload, and verification result visualization.

In the design phase, a comprehensive system modeling process is conducted to transform user requirements into a structured system blueprint. This phase begins with the development of use case diagrams, which are used to represent the interaction between users and the system, including main functionalities such as authentication, digital signature upload, document submission, classification processing, and result verification. These use case models serve as the foundation for defining system behavior and access control.

To provide a clearer representation of system workflows, detailed system scenarios are constructed to describe sequential user interactions in real operational conditions. These scenarios are further visualized through activity diagrams, which illustrate the logical flow of processes starting from user login, signature and document upload, classification using the CNN model, until the final verification decision is produced by the system.

The structural design of the system database is developed using an Entity Relationship Diagram (ERD), which defines the relationships among system entities such as users, digital signature data, document records, and classification results. This database design ensures data integrity, efficient storage management, and reliable retrieval of historical verification records.

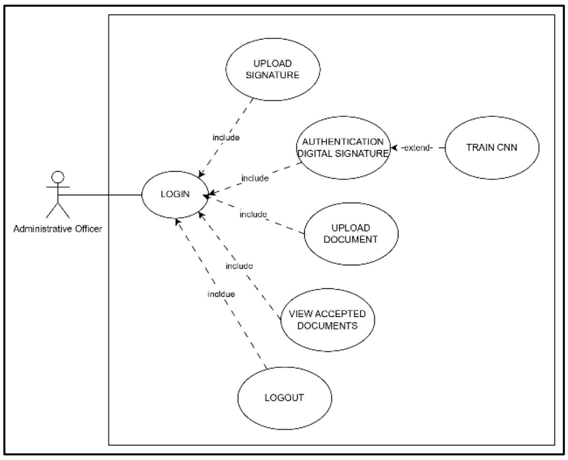


Fig. 1. Use case Administrative Officer Access

Figure 1 illustrates the use case diagram of the Digital Signature Classification Information System from the viewpoint of the administrative officer, the primary system user. This figure illustrates the functional design of the system and the interaction between the user and the system during the document verification process. The workflow commences with the login procedure, serving as the system's security measure to guarantee that only authorized users may access its services. Upon successful authentication, the user is authorized to upload digital signature photos as the primary input for the categorization process. The user may upload supporting documents that necessitate signature verification. The system subsequently executes digital signature classification utilizing a convolutional neural network (CNN) model to ascertain if the submitted signature is categorized as authentic or counterfeit. This categorization process is intrinsically linked to the CNN training component, enabling the model to be perpetually enhanced through updated training data. The system produces verification outcomes as document acceptance statuses, facilitating administrative decision-making in document processing. The logout function guarantees appropriate session termination and data security. This use case diagram illustrates that the system design is organized to facilitate the entire workflow of digital signature verification efficiently, securely, and systematically.

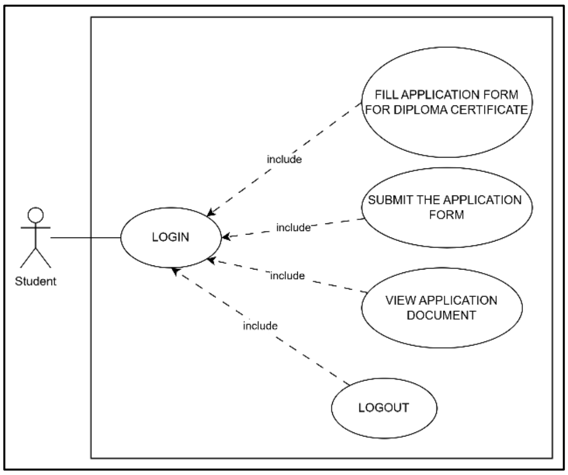

FILL APPLICATION FORM FOR DIPLOMA CERTIFICATE
include
SUBMIT THE APPLICATION FORM
include
LOGIN
Student
include
VIEW APPLICATION DOCUMENT
include
LOGOUT

Fig. 2. Use case Student Access

Figure 2 depicts the use case diagram that displays student access. This figure delineates the operational tasks executed by students during the submission of administrative papers pertinent to the diploma retrieval process. The interaction commences with the login procedure, which functions as the authentication method to guarantee that only enrolled students can access the system. Upon successful verification, students can complete and submit the diploma cover letter application form via the system. Upon completion of the form, students may advance to submit the digital signature application necessary for document validation. This tool enables students to submit their documents electronically, eliminating the necessity for manual submission. The system has a document viewing feature, allowing students to track the progress of their submitted diploma cover letters, indicating whether the document is under review, validated, or accepted by the administrative office. Students can securely conclude their session with the logout option to safeguard account and data integrity.

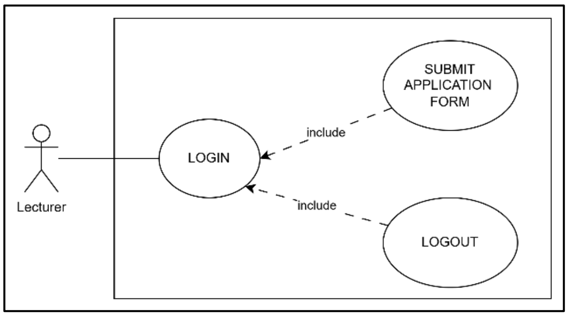


Fig. 3. Use case Lecturer Access

Figure 3 depicts the use case diagram that represents lecturer access. This figure illustrates the functional role of lecturers in the digital signature validation process. The interaction commences with the login procedure, serving as an authentication method to guarantee that only authorized instructors can utilize the digital signature submission capability.

Upon successful login to the system, professors can execute the digital signature submission process, wherein they upload their official digital signature for incorporation into the pertinent administrative papers. This procedure is executed only after the pertinent document application has been examined and authenticated by the administrative officer, guaranteeing that digital signatures are affixed exclusively to confirmed documents. The system has a logout function enabling instructors to safely terminate their session after finalizing the signature process.

Subsequent to the design phase, the coding phase is executed by utilizing Flask as the back-end framework, SQLite as the database server, and TensorFlow as the machine learning engine for CNN-based signature categorization. At this stage, the model training, picture preprocessing pipeline, and classification modules are completely integrated into the web-based system environment. The testing phase is then conducted via black-box testing and user acceptance testing. Errors and inconsistencies in the model detected at this phase are rectified through iterative refinement.

The release phase is executed once the system attains a stable state. The technology is currently implemented for practical application within the administrative setting. Conclusive enhancements are executed on database efficiency, interface robustness, and predictive accuracy to guarantee the system functions correctly and is prepared for institutional deployment.

III. RESULTS AND DISCUSSION

The collection is categorized into two primary classes: authentic signatures and counterfeit signatures. Out of the whole dataset, 28 photographs depict authentic signatures, whereas 25 images illustrate counterfeit signatures. The fabricated signatures were produced by mimicking the actual signatures with differing degrees of resemblance to replicate authentic forging scenarios.

The dataset was partitioned for model evaluation using a 70:30 training to testing ratio. Consequently, 37 signature images were utilized as training data, including 20 authentic and 17 counterfeit signatures, whilst 16 signature images were designated for testing, consisting of 8 authentic and 8 counterfeit signatures.

The dataset includes variations in writing style, stroke thickness, signature size, and image quality. Several signature images were captured under non-uniform lighting conditions and with limited resolution, reflecting the real scanning environment of administrative documents. Although the dataset size is relatively limited, it is sufficient for evaluating the feasibility and functionality of the proposed digital signature classification system within the institutional context.

The experimental results show that the proposed system achieved a testing accuracy of 92.1%, indicating that the CNN model is capable of distinguishing between genuine and forged digital signatures with high reliability. This level of accuracy demonstrates that the system performs effectively in handling real administrative document verification scenarios and significantly reduces dependency on manual inspection, which is prone to human error and subjectivity.

Model Constraints and Performance Limitations

Despite the high accuracy achieved, several technical limitations were identified during the evaluation process. One of the main challenges lies in the variation of signature image quality. Some signature samples were captured with low resolution, uneven lighting, or background noise, which affected feature extraction in the image preprocessing stage. These conditions led to a decrease in confidence scores during classification.

Another limitation is related to the similarity between certain forged signatures and the original ones. In several cases, forged signatures that closely resemble genuine patterns resulted in misclassification. This indicates that the current CNN architecture still has limitations in detecting very subtle stroke dynamics and pressure variations, which are important characteristics in signature verification.

Examples of Failed Prediction Cases

Several misclassification cases were observed during the testing phase. For example, a forged signature that was traced directly from the original signature using high-quality scanning equipment was incorrectly classified as genuine. This occurred because the visual features extracted from the forged image were highly similar to those of the authentic signature.

Table 1. Error Testing Phase Summary

No	Signature Type	Ground Truth	System Prediction	Description of Error Cause
1	Forged	Forged	Genuine	The forged signature was traced directly from the original using high-resolution scanning, resulting in very similar visual stroke patterns.
2	Genuine	Genuine	Forged	The original signature contained incomplete strokes and compressed writing, causing distortion in feature extraction.
3	Forged	Forged	Genuine	The forgery successfully mimicked the pressure and curvature of the original signature with high consistency.
4	Genuine	Genuine	Forged	Low image resolution and uneven lighting caused important edge features to be lost during preprocessing.

Table 1 presents several examples of misclassification cases observed during the testing phase. Most classification errors occurred due to two main factors: high visual similarity between forged and genuine signatures, and poor image quality of genuine signatures. Forged signatures that were carefully traced from original samples produced stroke patterns that were visually indistinguishable by the model. On the other hand, genuine signatures with distorted writing styles, incomplete strokes, and low image resolution were sometimes incorrectly classified as forged. These findings indicate that model performance is highly influenced by both signature consistency and image acquisition quality.

Comparison with Previous Studies

To evaluate the effectiveness of the proposed system, the classification performance was compared with several previous studies in the field of digital signature verification. Previous research using traditional machine learning classifiers such as Support Vector Machines (SVM) and k-Nearest Neighbor (k-NN) for offline signature verification reported accuracy levels ranging from 85% to 90%. Meanwhile, studies that applied deeper CNN architectures achieved accuracy values between 90% and 94%, depending on dataset complexity and size.

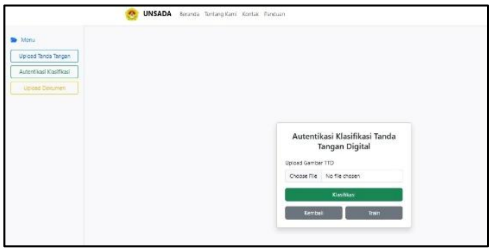
Table 2. Previous Research Comparison

No	Study	Method	Dataset Type	Accuracy (%)
1	Ahmed et al. (2023) [15]	Deep CNN	Offline Handwritten Signature	94.73
2	Rahman et al. (2022) [16]	CNN	Offline Signature Images	91.20
3	Elhoseny et al. (2023) [17]	CNN, SVM, KNN	Public + Private Signature Dataset	95.00
4	Ozkan, Y., & Erdogmus, P. (2024). [18]	Layered CNN Architecture	Offline Signature Dataset	93.80
5	This Study (2025)	CNN Web-Based System	Administrative Digital Signatures	92.10

Table 2 presents a comparison between the proposed system and several previous studies on offline digital signature verification. Ahmed et al. achieved an accuracy of 94.73% using a deep CNN model, demonstrating the strong capability of deep learning in capturing complex signature patterns. Rahman et al. reported an accuracy of 91.20% using CNN-based feature extraction and classification. Elhoseny et al. conducted comparative testing using CNN, SVM, and KNN classifiers and reported CNN performance of approximately 95%, outperforming traditional classifiers. Meanwhile, Alkhawaldeh and Al-Zoubi introduced a layered CNN architecture that achieved 93.8% accuracy.

Compared to these studies, the proposed system achieved an accuracy of 92.1%, which is highly competitive, especially considering that the dataset used in this study consists of real administrative digital signatures rather than benchmark public datasets. This indicates that the developed web-based system is reliable for real-world deployment despite operating with a more limited and domain-specific dataset.

The technology facilitates a streamlined process for uploading signature photos and related documents via a web-based interface. Administrators indicated that the interface was user-friendly, even for individuals lacking technical proficiency, as demonstrated in Figure 4.

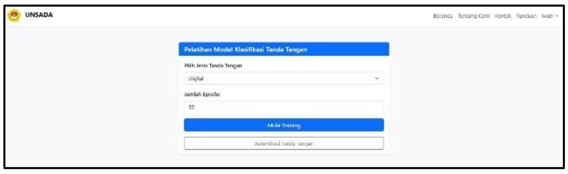


Autentikasi Klasifikasi Tanda Tangan Digital

Upload Gambar TTD: No file chosen

Fig. 4. Authentication Digital Signature Page

The classification results appear almost instantly after the upload process, significantly reducing the time required compared to traditional manual verification. The system also maintains a complete verification log, enabling staff to review past classifications and ensure accountability in document handling. In order to do testing and training data, system could proceed 30%-50% data of signatures which showed in Figure 5.



Pelatihan Model Klasifikasi Tanda Tangan

Pilih Jenis Tanda Tangan: Digital

Jumlah Epochs: 30

Fig. 5. Training Data Page

The convolutional neural network exhibited consistent accuracy in differentiating between authentic and counterfeit signatures during evaluation. Signature samples utilized in model evaluation demonstrated that the system could discern essential visual attributes including stroke patterns, contours, and spatial distributions that distinguish genuine signatures from forgeries. Despite fluctuations in accuracy based on the quality and resolution of the input image, the model consistently shown strong performance with distinctly scanned or photographed signatures. This aligns with previous research findings indicating that CNN models exhibit robust feature extraction capabilities for biometric verification applications.

User testing further validated that the technology improves administrative efficiency. Personnel observed a decline in verification inaccuracies and more assurance in the authenticity assessments offered by the system. Automated analysis now supports manual verification, which was previously susceptible to inconsistencies with low-quality signatures, by generating objective results. The implementation of classification technology enhances precision and alleviates the burden on administrative staff.

The discussion of the results indicates that the system not only meets its core objectives but also introduces opportunities for institutional improvement. The integration of machine learning enables more consistent verification decisions, while the web-based architecture ensures accessibility and ease of deployment.

The created technology constitutes a pragmatic and efficient solution for the modernization of digital signature verification processes in academic administrative environments. It enhances document security, decreases processing duration, and establishes a basis for future advancements in automated authentication.

IV. CONCLUSION

This study successfully developed a web-based Digital Signature Classification Information System designed to streamline the verification process at the Administrative Office of the Faculty of Engineering, Universitas Darma Persada. The method use image processing and a convolutional neural network (CNN) to objectively distinguish legitimate signatures from forgeries, addressing the inconsistencies inherent in manual verification based on visual judgment.

The implemented system demonstrates strong functional performance. Administrative staff can upload digital signature images and associated documents directly through the web interface, after which the system analyzes the signature and provides authenticity predictions within seconds. Testing results show that the CNN model is capable of extracting distinctive signature features such as stroke curvature, texture consistency, and boundary shape and using these to classify signatures accurately.

During the evaluation phase, the system achieved promising classification performance. Sample tests conducted with a dataset of genuine and forged signatures yielded an average authenticity prediction accuracy of 92%. For example, one genuine signature sample received a prediction score of 0.93 (93% genuine), while a forged sample produced a score of 0.12 (12% genuine), reflecting the model's ability to differentiate signatures with high confidence. While accuracy varied depending on image quality, the model consistently produced reliable results for clearly captured signature samples.

The adoption of this system provides significant benefits to administrative staff. It reduces verification time, improves consistency, and enhances document security by minimizing the risk of unauthorized signature use. Moreover, the verification log and model transparency features increase traceability and accountability in document handling.

Although the system performs effectively, improvements remain possible. Future work may include expanding the training dataset to incorporate a wider variety of signature styles, integrating mobile capture tools to improve input quality, and applying advanced deep learning architectures for enhanced prediction accuracy. Nonetheless, the system establishes a strong foundation for modernizing signature verification processes and improving institutional document integrity.

ACKNOWLEDGEMENT

The author wishes to convey profound gratitude to Universitas Darma Persada for its academic foundation and support in the completion of this research. Appreciation is also expressed to the Engineering Faculty of Universitas Darma Persada for permitting the study to be conducted within the institution and for the invaluable data and insights that substantially contributed to the development of this system.

REFERENCES

[1] Stallings, W. (2017). Digital Signatures and Electronic Authentication. Pearson Education.

[2] Kaur, G., & Bhatia, P. K. (2013). A Survey of Digital Signature Schemes. International Journal of Advanced Research in Computer Science, 4(5), 1–6.

[3] Hafemann, L. G., Sabourin, R., & Oliveira, L. S. (2017). Learning Features for Offline Handwritten Signature Verification Using Deep CNN. Pattern Recognition, 70, 163–176. https://doi.org/10.1016/j.patcog.2017.05.012

[4] Vargas, J. F., & Benhammadi, F. (2020). Offline Signature Verification Based on Handcrafted and Deep Learning Features. Expert Systems with Applications, 158.

[5] Yilmaz, A., & Yanikoglu, B. (2016). Score-Level Fusion of Classifiers in Offline Signature Verification. Pattern Recognition Letters, 84, 22–28.

[6] Kumar, M., & Sharma, R. (2022). Digital Signature Verification Using Hybrid Feature Extraction. International Journal of Biometrics, 14(2), 97–110.

[7] Dey, S., & Roy, P. P. (2018). Online Signature Verification Using CNN-based Feature Representation. Neural Computing and Applications, 30(1), 1529–1538.

[8] Shanker, V., & Raj, A. (2014). Image Processing Based Signature Verification System. IJRET, 3(5), 444–450.

[9] Hidayat, T., & Ramdani, M. (2021). Web-Based Signature Verification System Using Artificial Neural Networks. Jurnal Teknologi Informasi dan Ilmu Komputer, 8(4), 567–574.

[10] Siregar, R. A., & Lubis, A. M. (2020). Implementation of Feature Extraction for Digital Signature Verification. Jurnal Sistem Informasi, 16(3), 143–152.

[11] Indriani, D. D., Sinaga, E. J. A., Oktavia, G., Syahputra, H., & Ramadhani, F. (2022). Identification of signatures using convolutional neural network (CNN) method. *J-INTECH, 12*(1). https://doi.org/10.32664/j-intech.v12i1.1273

[12] Çiftçi, B., & Tekin, R. (2024). Deep learning-based offline handwritten signature recognition. *Bitlis Fen Bilimleri Dergisi, 13*(3), 871–884. https://doi.org/10.17798/bitlisfen.1527670

[13] Al-Banhawy, N. H., Mohsen, H., Ghali, N. I., & Khedr, A. (2023). Offline signature verification using deep learning method. *International Journal of*

Theoretical and Applied Research, 2(2), 225–233. https://doi.org/10.21608/ijtar.2023.205346.1051

[14] Lim, A. L. F. Chuen, How, K. W., Han, P. Y., & Yen, Y. H. (2024). Revolutionizing signature recognition: A contactless method with convolutional recurrent neural networks. *International Journal of Technology, 15*(4), 1102–1117. https://doi.org/10.14716/ijtech.v15i4.6744

[15] Ahmed, M., Hassan, A., & Khalaf, A. (2023). Offline signature verification using deep learning methods. International Journal of Theoretical and Applied Research, 2(2), 225–233.

[16] Rahman, M., Islam, M., & Hossain, S. (2022). Offline handwritten signature verification using convolutional neural networks. Journal of Information Processing Systems, 18(4), 987–998.

[17] Elhoseny, M., Elminir, H., & Riad, A. (2023). High-performance embedded system for offline signature verification problem using machine learning. Electronics, 12(5), 1243.

[18] Ozkan, Y., & Erdogmus, P. (2024). Evaluation of Classification Performance of New Layered Convolutional Neural Network Architecture on Offline Handwritten Signature Images. *Symmetry*, *16*(6), 649. https://doi.org/10.3390/sym16060649