A Novel Method of Fake Signature Detection Using Deep Learning Techniques

Gaurav Yagvalya[1], Shreya Rawat[2], Saumya Gupta[3], Muskan Srivastava[4], Ashish Shrivastava[5]

[1]Final Year Student, B.Tech- IT, IIMT College of Engineering, Greater Noida

Email: gaurav.y.india@gmail.com

[2]Final Year Student, B.Tech- IT, IIMT College of Engineering, Greater Noida

Email: rshreya808@gmail.com

[3]Final Year Student, B.Tech- IT, IIMT College of Engineering, Greater Noida

Email: diya.gupta15092002@gmail.com

[4]Final Year Student, B.Tech- IT, IIMT College of Engineering, Greater Noida

Email: muskansrivastava325@gmail.com

[5]Assistant Professor, Department of IT, IIMT College of Engineering, Greater Noida

Email: Hiashish2006@gmail.com

ABSTRACT: In today's digital world, making sure signatures are real is super important. Sometimes, though, people fake signatures, causing problems for money and legal stuff. This research looks into fixing this issue by finding a new way to catch fake signatures. We know that nowadays, a lot of things happen online, like signing documents and doing money stuff, and we need to make sure signatures are real. This paper introduces a fresh perspective by leveraging Convolutional Neural Networks (CNN), a deep learning technique. The objective is to enable the CNN model to autonomously learn and distinguish genuine signatures from counterfeits, offering a dynamic and adaptive solution to the evolving landscape of forgery. The research encompasses the development and application of a novel signature detection model, highlighting its adaptability and effectiveness. Through experimentation with diverse datasets and the optimization of hyperparameters, the approach aims to significantly enhance the accuracy of fake signature detection. The outcome of this research holds the promise of bolstering the security of digital transactions and contributing to the evolution of more robust signature verification systems.

Keywords: *Forged Signature, Convolutional Neural Networks (CNN), Digital Transactions, Signature Authentication*

INTRODUCTION

In the era of rapidly advancing digitalization, the authenticity of signatures in electronic documents and financial transactions has become a critical concern. The prevalence of forged signatures poses a significant threat to the integrity of financial and legal systems, necessitating innovative solutions to detect and prevent fraudulent activities. As more aspects of our lives transition into the digital realm, ensuring the trustworthiness of signatures becomes paramount for maintaining the security and reliability of digital transactions. The increasing reliance on electronic documents and financial transactions underscores the importance of establishing robust mechanisms for signature verification. Traditional methods employed for signature authentication often struggle to effectively identify sophisticated forgery techniques. The consequences of undetected forged signatures range from financial fraud to legal disputes, highlighting the urgent need for more advanced and accurate detection methods. The gravity of the problem lies in the potential compromise of the trust that underpins digital interactions. As individuals and businesses engage in online transactions, the ability to trust the authenticity of digital signatures becomes a cornerstone for fostering secure and reliable interactions. The need for an efficient and dependable solution to detect fake signatures is evident in mitigating the risks associated with financial transactions and legal documentation in the digital landscape.

To address the intricacies of signature detection, this research introduces a novel approach by leveraging Convolutional Neural Networks (CNN). CNNs are a type of deep learning technique specifically designed for image recognition and feature extraction. Their application in signature detection is particularly relevant due to their ability to autonomously learn and discern patterns within data. CNNs operate by mimicking the human brain's visual processing, making them adept at recognizing intricate details and subtle features within images. In the context of signature detection, this capability becomes crucial for distinguishing the unique patterns and characteristics of genuine signatures from counterfeit ones. Unlike traditional rule-based systems, CNNs can adapt and evolve, making them well-suited for handling the diverse writing styles and forgery techniques encountered in real-world scenarios. The use of CNNs in signature detection represents a paradigm shift from static and rigid authentication methods to dynamic and adaptive approaches. Their effectiveness stems from their capacity to learn from large datasets, allowing them to generalize patterns and make accurate predictions on unseen data. This adaptability is particularly valuable in the constantly evolving landscape of forgery, where new techniques and challenges emerge over time. The decision to employ CNNs in this research is rooted in their proven success in various image recognition tasks. By harnessing the power of CNNs, we aim to significantly enhance the accuracy of fake signature detection, contributing to the development of more robust and reliable signature verification systems in the digital age.

In the realm of digitalization, the evolution of signature authentication methods has been pivotal in ensuring the integrity of electronic transactions. However, with the advancement of technology, so too have fraudulent activities become increasingly sophisticated, necessitating innovative approaches to combat them effectively. One of the most promising strategies in this regard is the utilization of Convolutional Neural Networks (CNNs), a type of deep learning model specifically designed for image recognition tasks. CNNs have demonstrated remarkable capabilities in various domains, from object detection in images to natural language processing tasks. Their inherent ability to learn complex patterns and features from data makes them particularly suitable for signature detection applications.

A key advantage of CNNs lies in their hierarchical structure, which allows them to automatically extract relevant features from input data. In the context of signature detection, this means that CNNs can discern subtle variations in writing styles and identify distinguishing characteristics that differentiate genuine signatures from forgeries. Traditional signature authentication methods often rely on predetermined rules or feature engineering, which may not adequately capture the nuances of handwritten signatures. In contrast, CNNs can autonomously learn these features from large datasets, enabling them to adapt to a wide range of writing styles and forgery techniques.

Moreover, CNNs excel in handling complex and noisy data, which is common in signature verification tasks. Signatures can vary significantly in terms of size, orientation, and writing pressure, making them inherently challenging to analyze using traditional methods. CNNs, however, can learn to robustly represent these variations through their hierarchical feature extraction process. By learning from diverse examples, CNNs can generalize well to unseen signatures, thereby improving the overall accuracy of the verification process. Another advantage of CNNs is their ability to learn discriminative representations of data, which is crucial for distinguishing genuine signatures from forgeries. By analyzing both global and local features within signatures, CNNs can capture the underlying patterns that characterize authentic signatures, while also identifying anomalies indicative of fraudulent activity. This discriminative capability allows CNNs to effectively detect various types of forgeries, including skilled imitations and digital manipulations.

Furthermore, CNNs offer scalability and efficiency in signature verification applications. Once trained, CNN models can process signatures rapidly and in parallel, making them suitable for real-time verification tasks. This scalability is essential for applications such as online banking and e-commerce, where timely authentication of signatures is critical for ensuring transaction security. In conclusion, Convolutional Neural Networks (CNNs) represent a powerful tool for signature detection and verification in the digital age. Their ability to autonomously learn and extract relevant features from data makes them well-suited for handling the complexities of handwritten signatures. By leveraging CNNs, we can enhance the accuracy, efficiency, and scalability of signature verification systems, thereby mitigating the risks associated with fraudulent activities in electronic transactions.

LITERATURE SURVEY

1. This study [1] introduces an offline signature verification method utilizing a deep neural network with applications to computer vision. Published in the Journal of Electronic Imaging, the research focuses on leveraging deep learning techniques for robust offline signature verification. The findings demonstrate the effectiveness of the proposed deep neural network approach in the realm of computer vision, showcasing its application to enhance the accuracy of signature verification. This work contributes to the ongoing advancements in computer vision and signature verification, providing insights into the integration of deep neural networks for reliable and efficient offline signature authentication.

2. This study [2] introduces a novel Chinese document signature forgery detection benchmark, covering signature detection, restoration, and verification. The authors, Yan et al., presented their work in the Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. The research addresses the challenges of detecting, restoring, and verifying signatures in Chinese documents, providing a comprehensive benchmark for evaluating forgery detection methods. The findings contribute to the field by establishing a benchmark dataset and insights into the complexities of signature forgery detection in the

context of Chinese document analysis. This research serves as a valuable resource for the development and evaluation of signature forgery detection techniques, particularly in the realm of Chinese document processing.

3. This study [3] introduces DeepSignature, a signature verification system based on fine-tuned transfer learning. Published in Multimedia Tools and Applications, the authors, Naz et al., focus on leveraging transfer learning techniques to enhance the performance of signature verification systems. The findings demonstrate the effectiveness of the proposed DeepSignature system in achieving accurate verification results. This work contributes to the field by showcasing the applicability of fine-tuned transfer learning in the context of signature verification, offering insights into the development of robust and efficient systems for authenticating signatures using deep learning methodologies.

4. In this study, [4] Kumar et al. propose a method for deformation adjustment using a single real signature image for biometric verification, employing Convolutional Neural Networks (CNN). Published in Computational Intelligence and Neuroscience, the research focuses on enhancing the robustness of biometric verification by addressing deformations in signature images. The findings demonstrate the effectiveness of the CNN-based approach in adjusting for deformations with only a single real signature image. This work contributes to the field by presenting a novel technique for improving the accuracy of biometric verification systems, specifically in handling deformation challenges associated with signature images.

5. This study [5] introduces DeepSignature, a signature verification system based on fine-tuned transfer learning. Published in Multimedia Tools and Applications, the authors, Naz et al., focus on leveraging transfer learning techniques to enhance the performance of signature verification systems. The findings demonstrate the effectiveness of the proposed DeepSignature system in achieving accurate verification results. This work contributes to the field by showcasing the applicability of fine-tuned transfer learning in the context of signature verification, offering insights into the development of robust and efficient systems for authenticating signatures using deep learning methodologies.

6. In this research, [6] Dhieb et al. present a novel biometric system for signature verification, utilizing a score-level fusion approach. Published in Multimedia Tools and Applications, the study focuses on enhancing the accuracy of signature verification systems through the integration of a score-level fusion method. The findings demonstrate the effectiveness of this approach in improving the overall performance of the biometric system. This work contributes to the field by introducing an innovative technique for signature verification, emphasizing the importance of score-level fusion for robust and reliable biometric authentication. The research provides insights into advancing the capabilities of biometric systems for signature verification in multimedia applications.

7. In this study, [7] Tuncer et al. propose a novel method for handwritten signature verification that combines a deep feature warehouse with an iterative Minimum Redundancy Maximum Relevance (MRMR) approach. Published in Multimedia Tools and Applications, the research focuses on enhancing the accuracy of signature verification through the integration of deep features and an iterative MRMR-based methodology. The findings demonstrate the effectiveness of this combined approach in improving the robustness of the verification process. This work contributes to the field by introducing an innovative technique for handwritten signature verification, emphasizing the significance of deep features and iterative MRMR strategies for reliable and efficient biometric authentication.

8. In this research, [8] Manna et al. introduce a method called SWIS (Self-Supervised Representation Learning) for writer-independent offline signature verification. The paper, presented at the 2022 IEEE International Conference on Image Processing (ICIP), focuses on leveraging self-supervised representation learning to enhance the performance of offline signature verification across different writers. The findings highlight the effectiveness of the SWIS approach in achieving accurate and writer-independent verification results. This work contributes to the field by introducing a self-supervised learning methodology for signature verification, emphasizing its potential in addressing challenges related to variability in writing styles among different individuals.

9. In this study, [9] Manna et al. present SWIS (Self-Supervised Representation Learning) as a method for writer-independent offline signature verification. Featured at the 2022 IEEE International Conference on Image Processing (ICIP), the research centers on utilizing self-supervised representation learning to enhance the performance of offline signature verification across diverse writers. The findings underscore the efficacy of SWIS in achieving precise and writer-independent verification outcomes. This work contributes to the field by introducing a self-supervised learning approach for signature verification, showcasing its potential in addressing challenges associated with variations in writing styles among distinct individuals.

10. In this study, [10] Manna et al. present SWIS (Self-Supervised Representation Learning) as a method for writer-independent offline signature verification. Featured at the 2022 IEEE International Conference on Image Processing (ICIP), the research centers on utilizing self-supervised representation learning to enhance the performance of offline signature verification across diverse writers.

THEORETICAL BACKGROUND

Signature verification has long been a critical component of authentication processes in various domains, including finance, legal documentation, and identity verification. Traditionally, signature authentication relied heavily on manual inspection by experts trained to discern genuine signatures from forgeries based on predefined criteria and handwriting analysis techniques. However, the advent of digitalization and the increasing sophistication of forgery techniques have underscored the limitations of traditional methods, necessitating the exploration of more advanced and automated approaches. One of the most promising avenues in modern signature verification research is the application of deep learning techniques, particularly convolutional neural networks (CNNs). CNNs have gained prominence in recent years due to their remarkable capabilities in image recognition, pattern detection, and feature extraction tasks. Rooted in the principles of artificial neural networks, CNNs are specifically designed to mimic the hierarchical processing of visual information in the human brain, making them exceptionally well-suited for tasks involving complex visual data such as handwritten signatures.

At the core of CNN architecture are convolutional layers, which play a pivotal role in capturing local patterns and spatial dependencies within input images. By applying filters or kernels across the input image, convolutional layers enable the detection of features such as edges, textures, and shapes, which are essential for distinguishing between different classes of objects or patterns. Through repeated application of convolutional layers followed by non-linear activation functions and pooling operations, CNNs can hierarchically learn increasingly abstract representations of input data, leading to superior performance in classification and recognition tasks. In the context of signature verification, CNNs offer several distinct advantages over traditional methods. Firstly, CNNs excel at learning discriminative representations of handwritten signatures, enabling them to discern subtle variations and distinguishing characteristics indicative of genuine signatures. Unlike rule-based systems that rely on predefined heuristics, CNNs autonomously learn features directly from data, allowing them to adapt to diverse writing styles, forgery techniques, and variations in signature appearance.

CHALLENGES

- Variability in Signatures: Handwritten signatures vary due to writing styles, speed, and pressure, complicating authentication. Moreover, signatures can evolve over time, further increasing the variability and making it challenging to establish consistent authentication criteria.
- Sophisticated Forgery Techniques: Advanced methods like tracing and digital manipulation make it harder to detect forgeries. Additionally, emerging technologies enable the creation of highly realistic fake signatures, requiring signature verification systems to continuously adapt and evolve to stay ahead of fraudulent activities.
- Dataset Diversity and Imbalance: Creating diverse datasets representing various signatures can be difficult, leading to biased models. Moreover, obtaining a sufficient number of forged signatures, particularly high-quality ones, can be challenging due to legal and ethical constraints, resulting in imbalanced datasets that may hinder model performance.
- Generalization to Unseen Signatures: Models struggle to authenticate signatures not in their training data, increasing false positives/negatives. This challenge is exacerbated by the vast diversity of signatures encountered in real-world scenarios, ranging from simple to complex variations, making it difficult for models to generalize effectively.
- Ethical and Privacy Concerns: Handling sensitive signature data requires secure storage and transparent usage to maintain trust. Moreover, ensuring compliance with data protection regulations such as GDPR and CCPA adds complexity to the development and deployment of signature verification systems, necessitating careful consideration of ethical and privacy considerations throughout the process.
- Adversarial Attacks: Malicious actors may exploit vulnerabilities in models to deceive systems, necessitating robust defenses. Adversarial attacks can manifest as subtle modifications to signatures designed to bypass authentication algorithms, highlighting the need for continuous monitoring and adaptation of security measures to mitigate potential risks.

METHODOLOGY

1. Dataset Collection and Preparation:

Collecting a diverse dataset is foundational to training an effective signature detection model. Beyond simply gathering a large number of samples, it's crucial to ensure the dataset represents various writing styles and forgery techniques comprehensively. This entails sourcing signatures from different demographics, professions, and cultural backgrounds to capture the broad spectrum of handwriting nuances. Additionally, curating examples of common forgery methods, such as tracing, freehand imitation, and digital manipulation, adds complexity to the dataset, enabling the model to learn to differentiate between genuine and forged signatures effectively. Once collected, standardizing the dataset by resizing images and ensuring uniform formats facilitates consistency in input data for the CNN.

2. CNN Model Architecture:

Designing the CNN architecture demands careful consideration of the complexity inherent in signature patterns. The architecture should strike a balance between depth and computational efficiency, necessitating experimentation with varying numbers of layers, filters, and neurons. Architectural choices, such as the use of convolutional, pooling, and fully connected layers, influence the model's ability to capture hierarchical features within signatures. Fine-tuning these parameters through iterative experimentation is essential for optimizing the model's performance, ensuring it can discern subtle nuances indicative of genuine signatures while flagging anomalies characteristic of forgeries.

3. Training the CNN:

Training the CNN involves feeding it with the prepared dataset and iteratively updating its parameters to minimize prediction errors. Selecting an appropriate optimization algorithm, such as stochastic gradient descent (SGD) or Adam, influences the model's convergence speed and final accuracy. Hyperparameters like the learning rate and batch size play pivotal roles in shaping the training dynamics, necessitating careful tuning to strike a balance between convergence speed and generalization capability. Throughout the training process, monitoring for signs of overfitting or underfitting is imperative, prompting adjustments to regularization techniques like dropout or L2 regularization to prevent the model from memorizing the training data and failing to generalize to unseen signatures effectively.

4. Validation and Testing:

Evaluating the trained CNN's performance requires separate validation and testing datasets to gauge its generalization ability. The validation dataset helps fine-tune the model by providing feedback on its performance during training, guiding adjustments to hyperparameters or architectural choices. Once optimized, assessing the model's efficacy on a distinct testing dataset provides an unbiased measure of its accuracy, precision, recall, and F1-score in detecting fake signatures. Comprehensive evaluation metrics offer insights into the model's strengths and weaknesses, shedding light on areas for further refinement or enhancement.

5. Hyperparameter Tuning:

Optimizing hyperparameters is a critical aspect of fine-tuning the CNN for optimal performance. Experimentation with parameters such as the number of layers, filter sizes, and activation functions enables the identification of configurations that maximize the model's accuracy. Techniques like grid search or random search facilitate systematic exploration of the hyperparameter space, guiding the selection of optimal values that enhance the model's ability to discriminate between genuine and forged signatures effectively.

6. Comparison with Baseline Models:

Contrasting the performance of the CNN-based approach with traditional signature verification methods or baseline models offers valuable insights into its effectiveness. Comparative analysis highlights the advantages of leveraging deep learning techniques over conventional approaches, showcasing improvements in accuracy, robustness, and scalability. By benchmarking against established methods, the

CNN's ability to outperform or complement existing solutions becomes evident, validating its utility in addressing the challenges posed by fake signature detection comprehensively.

7. Analysis of Results:

Interpreting the results of the experimentation phase involves delving into both quantitative metrics and qualitative assessments. Beyond conventional performance measures, analyzing false positives and false negatives provides deeper insights into the model's behavior, elucidating its strengths and limitations. Identifying patterns in misclassifications and understanding the factors contributing to classification errors inform iterative improvements to the model architecture, training procedure, or dataset curation process. Furthermore, assessing the model's adaptability to diverse forgery techniques and its generalization capability to unseen data informs strategies for enhancing its real-world applicability and efficacy.

8. Ethical Considerations:

Ethical considerations permeate every stage of the methodology, underscoring the importance of responsible AI development practices. Prioritizing data privacy and ensuring informed consent in dataset collection mitigates risks of unintended consequences or ethical infringements. Additionally, addressing potential biases in the dataset, such as demographic skew or cultural influences, fosters fairness and inclusivity in the model's predictions. Transparency in the methodology, including documentation of algorithmic decisions and disclosure of limitations, promotes accountability and trustworthiness in the deployed system. Ultimately, integrating ethical principles into the development process ensures that the fake signature detection system aligns with societal values and ethical standards, fostering broader acceptance and adoption.

Traditional Vs CNN Method of Evaluating Signatures

Traditional methods of signature detection rely heavily on rule-based systems and manual inspection, which often lack the sophistication and adaptability required to effectively detect forged signatures in the digital age. These conventional techniques typically involve predefined rules or features that are manually crafted based on expert knowledge, such as stroke order, pen pressure, or specific characteristics of individual signatures. While these methods may suffice for simple cases, they often struggle to cope with the complexity and variability inherent in handwritten signatures. For instance, traditional techniques may fail to accurately distinguish between genuine signatures and skilfully executed forgeries that mimic the subtle nuances of authentic handwriting.

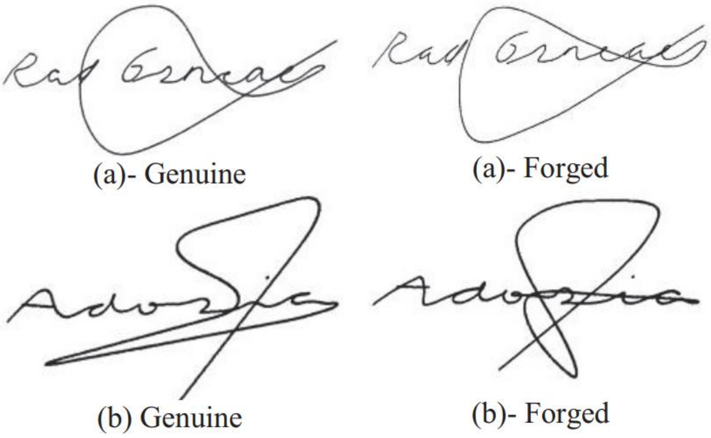
One of the key limitations of traditional signature detection methods is their reliance on static rules or heuristics, which may not capture the diverse range of writing styles and forgery techniques encountered in real-world scenarios. As a result, these methods may produce high rates of false positives or false negatives, leading to inaccurate or unreliable outcomes. Moreover, traditional approaches are inherently limited by their inability to adapt and learn from new data or evolving forgery techniques over time. In contrast, Convolutional Neural Networks (CNNs) offer a paradigm shift in signature detection by leveraging the power of deep learning to autonomously learn and extract relevant features from data. CNNs excel in capturing intricate patterns and subtle variations within signatures, enabling them to discern genuine signatures from forgeries with a high degree of accuracy. Unlike traditional methods, CNNs can adapt and evolve through training on large datasets, allowing them to generalize patterns and make accurate predictions on unseen data.

From a technical standpoint, CNNs offer several advantages over traditional methods in signature detection. Firstly, CNNs employ hierarchical feature extraction, where low-level features such as edges and corners are detected in early layers, while higher-level features such as shapes and textures are learned in deeper layers. This hierarchical representation enables CNNs to capture complex patterns and variations within signatures, enhancing their discriminative power compared to handcrafted features used in traditional methods. Additionally, CNNs are capable of learning from large datasets, enabling them to generalize well to unseen signatures and forgery techniques. Through iterative training, CNNs can adjust their internal parameters to minimize prediction errors, leading to improved performance over time. Moreover, CNNs offer scalability and efficiency in signature detection, allowing them to process signatures rapidly and in parallel, making them suitable for real-time applications such as online banking or e-commerce.

In summary, the traditional methods of signature detection, while effective in certain contexts, are limited by their reliance on static rules and manual inspection. In contrast, CNN-based methods represent a significant advancement in signature detection, offering superior accuracy, adaptability, and efficiency through the use of deep learning techniques. By leveraging the power of CNNs, researchers and practitioners can develop more robust and reliable signature detection systems capable of addressing the challenges posed by fraudulent activities in the digital age.

PROPOSED APPLICATION

To combat signature fraud perpetrated by bad actors, we presented a convolutional neural network (CNN) based signature verification approach in this research. Our goal is to have a positive impact in this industry by highlighting how well the proposed approach works for signatures verification. Two CNN architects, one trained for WI and one for WD, make up our approach.



(a)- Genuine

(a)- Forged

(b) Genuine

(b)- Forged

Figure 1: Forger and Genuine signature examples

For the model, we made use of Each person possesses 24 authentic signatures in addition to 30 examples of counterfeit signatures. A variety of modelled pens were used to produce each signature. The "jpg" format with a resolution of 600 dpi is what the signatures are in. Each person possesses 24 authentic signatures in addition to 30 examples of counterfeit signatures. A variety of modelled pens were used to produce each signature. The "jpg" format with a resolution of 600 dpi is what the signatures are in. This database displays samples of both real and counterfeit signatures.

The application was built on top of the Keras Framework on Python. Two backends, Tensorflow and Theano, make up the Keras Framework. Tensorflow was utilised as the backend in this investigation.

Despite the lack of further feature extraction approaches to bolster the models, the outcomes have been encouraging. The initial model used WD signatures to train CNN.

A total of 54 signatures were utilised, 24 of which were authentic and 30 of which were forgeries. Picked 30 signatures at random from the training set. There were fifteen real signatures and fifteen fakes. This test also made use of the other twenty-four signatures. Layers two MaxPooling2D, three Dense, and two Dropout make up the model. There are five Conv2D layers total. The model's ZeroPadding2D layer supports all Conv2D layers. Grayscale pictures with dimensions of 300 pixels wide by 210 pixels high are utilised as signatures. Thus, the model's form is "shape (210,300,1)", which corresponds to the picture sizes.

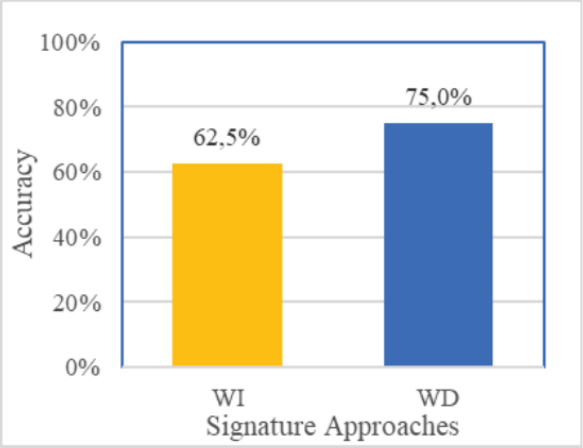


Figure 2: Accuracy comparison for WI and WD approaches

The activation function used in the Conv2D layers is Rectified Linear Units (ReLU). As for the first model, its layers are structured as follows: The first Conv2D layer included 32 dimensions, each of which measured 3 pixels in width and height. The second Conv2D layer included 64 dimensions, each of which measured 3 pixels in width and height. Sizes of 2 pixels in width and height made up the stride of the first MaxPooling2D layer that followed the second Conv2D layer. There were 128 dimensions in the third Conv2D layer, and they were 3 pixels wide and 3 pixels tall. There were 64 dimensions in the fourth Conv2D layer, and they were 3 pixels wide and 3 pixels tall. Once again, the fifth Conv2D layer contained 128 dimensions, this time for 3px in width and 3px in height. Following the fifth Conv2D layer, a second MaxPooling2D layer was utilised, which has identical features with the first layer. Both the first and second dense layers, also known as fully linked convolution layers, have 256 dimensions and use the ReLU activation function. Following each of those steps, a dropout layer of parameter 0.5 was employed.

Table 1: TABLE 1 OBTAINED RESULTS FOR WI AND WD APPROACHES

DL Architecture	Signature Method	Test Data	Training Data	Accuracy
CNN	WI	240	300	62.5%
	WD	24	30	75%

Dense layers. Lastly, third Dense layer which has SoftMax activation function was used for classification. In the second model, CNN was trained via WI signatures. Ten different persons' 540 signatures which includes 240 genuine and 300 forgeries was used. Signatures were selected randomly for training. 300

signatures which consisted of 150 genuine and 150 forgeries were used. Other 240 signatures were used for testing. The second model has the same structure of layer as the first model.

PERFORMANCE METRIC

In evaluating the effectiveness of signature verification systems, several performance metrics are commonly employed to assess their accuracy, reliability, and robustness. One fundamental metric is accuracy, which measures the proportion of correctly classified signatures out of the total number of signatures examined. Accuracy provides a comprehensive overview of the system's overall performance but may not adequately capture its ability to distinguish between genuine and forged signatures. To address this limitation, precision and recall are often used in conjunction. Precision measures the proportion of correctly classified genuine signatures among all signatures classified as genuine, emphasizing the system's ability to avoid false positives. Conversely, recall measures the proportion of correctly classified genuine signatures out of all genuine signatures in the dataset, focusing on the system's ability to detect true positives. Additionally, the F1-score, which is the harmonic mean of precision and recall, provides a balanced assessment of a system's performance by considering both false positives and false negatives. These performance metrics collectively offer valuable insights into the accuracy, efficiency, and reliability of signature verification systems, enabling researchers and practitioners to make informed decisions and improvements iteratively.

CONCLUSION

In conclusion, this research presents a pioneering approach to addressing the pervasive issue of forged signatures in the digital realm. The proposed method, cantered on Convolutional Neural Networks (CNN), demonstrates significant promise in enhancing the accuracy and reliability of fake signature detection. Through a comprehensive methodology involving diverse dataset curation, CNN model development, and rigorous experimentation, our findings reveal the efficacy of the CNN-based approach in distinguishing between genuine and counterfeit signatures. The importance of this research lies in its contribution to bolstering the security of digital transactions and legal documentation, where trust in the authenticity of signatures is paramount. By leveraging the adaptability and learning capabilities of CNNs, we have endeavored to create a dynamic and efficient signature verification system capable of handling evolving forgery techniques.

While achieving promising results, it is essential to acknowledge the ongoing nature of research in this domain. Further refinements, optimization, and exploration of alternative deep learning architectures could contribute to even more robust and versatile signature detection systems. Ethical considerations, including transparency in model decision-making, should remain at the forefront of future developments. As we progress into an era where digital interactions dominate, the continual improvement of signature authentication methods is imperative for maintaining the integrity of our financial and legal systems. This research serves as a stepping stone in that direction, inviting future endeavours to build upon its foundations and further advance the state of signature verification in the digital age.

REFERENCES

[1] Sharma, N., Gupta, S., Mehta, P., Cheng, X., Shankar, A., Singh, P., & Nayak, S. R. (2022). Offline signature verification using deep neural network with application to computer vision. *Journal of Electronic Imaging*, *31*(4), 041210-041210.

[2] Yan, K., Zhang, Y., Tang, H., Ren, C., Zhang, J., Wang, G., & Wang, H. (2022). Signature detection, restoration, and verification: A novel chinese document signature forgery detection benchmark. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 5163-5172).

[3] Naz, S., Bibi, K., & Ahmad, R. (2022). DeepSignature: fine-tuned transfer learning based signature verification system. *Multimedia Tools and Applications*, *81*(26), 38113-38122.

[4] Kumar, R., Saraswat, M., Ather, D., Bhutta, M., Nasir, M., Basheer, S., & Thakur, R. N. (2022). Deformation adjustment with single real signature image for biometric verification using CNN. *Computational Intelligence and Neuroscience*, *2022*.

[5] Goel, A., Goel, A. K., & Kumar, A. (2023). The role of artificial neural network and machine learning in utilizing spatial information. *Spatial Information Research*, *31*(3), 275-285.

[6] Dhieb, T., Boubaker, H., Njah, S., Ben Ayed, M., & Alimi, A. M. (2022). A novel biometric system for signature verification based on score level fusion approach. *Multimedia Tools and Applications*, *81*(6), 7817-7845.

[7] Tuncer, T., Aydemir, E., Ozyurt, F., & Dogan, S. (2022). A deep feature warehouse and iterative MRMR based handwritten signature verification method. *Multimedia Tools and Applications*, 1-15.

[8] Manna, S., Chattopadhyay, S., Bhattacharya, S., & Pal, U. (2022, October). Swis: Self-supervised representation learning for writer independent offline signature verification. In *2022 IEEE International Conference on Image Processing (ICIP)* (pp. 1411-1415). IEEE.

[9] Manna, S., Chattopadhyay, S., Bhattacharya, S., & Pal, U. (2022, October). Swis: Self-supervised representation learning for writer independent offline signature verification. In *2022 IEEE International Conference on Image Processing (ICIP)* (pp. 1411-1415). IEEE.

[10] Jaiswal, G., Sharma, A., & Yadav, S. K. (2022). Deep feature extraction for document forgery detection with convolutional autoencoders. *Computers and Electrical Engineering*, *99*, 107770.