

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 4, Issue 3, December 2024

Review on Hand Written Signature Forgery Detection using Deep Neural Networks

Amrutha R¹, Annapoorna A C², Bhavana K N³, Bhoomika K B⁴, Vijetha T S⁵

Under Graduate Students, Department of Electronics and Communication Engineering¹⁻⁴ Assistant Professor, Department of Electronics and Communication Engineering⁵ Alvas Institute of Engineering and Technology, Mijar, Mangalore, India amrutharamesh029@gmail.com, annapoorna.a.c2702@gmail.com ,bhanubhavana334@gmail.com,bhoomikagowdak26@gmail.com,tsvijetha@aiet.org.in

Abstract: Handwritten signature verification is an essential method for authenticating documents in various industries, including banking, legal, and government sectors. However, the increasing prevalence of signature forgery presents a significant challenge to the security and integrity of systems relying on handwritten signatures. Traditional approaches to signature verification, such as the ones based on manual inspection or low-level machine learning techniques, are unable to detect forgeries with reasonable accuracy, especially when variations in writing style or slight changes in the dynamics of a signature occur. Recently, deep neural networks have emerged as a highly promising tool to help with this task. DNNs, such as CNNs and RNNs, provide the capability to automatically extract complex features from signature data, which allows for more accurate and efficient verification.

Keywords: Handwritten signature verification

I. INTRODUCTION

Handwritten signature verification is very crucial in ensuring that documents are authentic in sectors like banking, legal, and governmental operations. A handwritten signature is a good form of identification and authentication since it is one's personal touch and style. With the rise of digital technologies, there has been an increased risk of signature forgery. Signature forgery refers to the process whereby people imitate or replicate other people's signatures for fraudulent purposes[1].

This has resulted in the increasing concerns over the security of systems that depend on handwritten signatures for verification purposes. Signature forgery detection has become one of the important tasks in biometric security and document verification systems. The traditional methods of signature verification involve manual inspection or classical machine learning techniques that take a lot of time and often lead to error.[2]

The methods also struggle with handling large-scale data and complex variations in signatures, like changes in writing speed, pressure, and orientation, hence being less effective in real-world applications. Contrarily, modern methods make use of deep learning models, specifically DNNs, in the process of identifying forged signatures in a more precise and effective manner. [3]

Deep neural networks have exhibited tremendous capabilities in dealing with complex patterns of data, making them ideal for applications such as handwriting recognition and signature verification.[4]

DNNs can learn hierarchical representations of features, which means that they can capture high-dimensional features that may not be easily recognizable by conventional algorithms. Consequently, methods that are based on DNNs can outperform signature verification techniques significantly with their high accuracy, scalability, and robustness against various forgery types.[5]

One of the key features of using deep neural networks with handwritten signature forgery detection, however, is that automatically extracted features from raw signature data obviate the need to manually engineer features.[6]

This process is very helpful in addressing signatures, which have both inter-personal variability, meaning the signature of every individual is different, as well as intra- personal dynamics, meaning a particular person's signature may shift based on the context, such as fatigue or stress .[7]

Copyright to IJARSCT www.ijarsct.co.in

DOI: 10.48175/568





International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 4, Issue 3, December 2024

Deep learning models, especially convolutional neural networks (CNNs) and recurrent neural networks (RNNs), also learn spatial and temporal dependencies in signatures, respectively, improving the system's ability to differentiate between genuine and forged signatures. [8]

The focus of recent research work has been on the application of DNNs to the signature verification task, which gives rise to various architectures, CNNs that are particularly good for processing image-based signature data and RNNs capable of capturing sequential patterns in signature dynamics. [9]

The adoption of deep neural networks (DNNs) in this domain has revolutionized traditional approaches, providing state-of- the-art performance. This literature survey explores significant contributions in the field, emphasizing the role of DNN architectures[10]

II. LITERATURE SURVEY

Insights on Handwritten Signature Forgery Detection

Handwritten signature forgery can be categorized into skilled, random, and simple forgeries. Skilled forgery, where the forger tries to replicate the genuine signature closely, poses the most significant challenge due to its high similarity with the authentic sample. Traditional methods relied on handcrafted features such as geometric and texture-based attributes, which often fell short in generalization. With the advent of deep learning, feature extraction and classification processes have become more robust and automated.

Deep Neural Networks Approaches:

Deep learning models, particularly convolutional neural networks (CNNs), recurrent neural networks (RNNs), and hybrid architectures, have shown remarkable success in signature verification and forgery detection. Below are some pivotal studies

CNN-based Architectures:

Hafemann et al. (2017) proposed a Siamese CNN architecture for offline signature verification. By learning a feature space where genuine signatures are closer together than forgeries, their model achieved significant accuracy on benchmark datasets such as CEDAR and GPDS. [11]

Alaei et al. (2020) extended the CNN-based approach by incorporating attention mechanisms, allowing the model to focus on discriminative regions of the signature, thereby enhancing the robustness against skilled forgeries. [12]

Yang et al. (2019) utilized a combination of CNNs and long short-term memory (LSTM) networks to capture spatial and sequential dependencies in dynamic signatures. Their hybrid model demonstrated improved performance, especially in distinguishing between genuine and skilled forgeries. [13]

Hafemann et al. (2019) further explored the integration of deep metric learning and recurrent structures to handle variations in signature strokes and writing styles. [14]

III. CONCLUSION

The detection of the forgery of a handwritten signature has been an important task that aims to guarantee the authenticity of documents in several sectors including banks, courts of law, and governmental agencies. As verification of signature becomes a key player in combating fraud, the traditional approach, however, has limitations. First, they fail to effectively handle complex variations in patterns of signatures and forgeries. Deep neural networks, however, provide a promising solution in that they utilize advanced algorithms to automatically learn intricate features from signature data, thus making forgery detection more accurate and reliable. Detection of handwritten signature forgery using deep neural networks involves several critical steps, starting from data collection and preprocessing to model training, evaluation, and deployment. The first step would be preparing a diversified, high quality dataset that comprises actual versus forged signatures. The dataset used here would serve as a foundation for any successful deep learning-based signature- verification system. Using both skilled forgeries, random forgeries, and even using a machine to generate forgeries would make sure that the variety of fraudulent attempts to counterfeit signatures are covered by whatever the model might learn on its own. Preprocessing techniques, such as image residing normalization, noise reduction, and data augmentation, are used to standardize and improve input data once it is collected. These ensure that

Copyright to IJARSCT www.ijarsct.co.in DOI: 10.48175/568





International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 4, Issue 3, December 2024

variations in size, orientation, and resolution do not impact the model, hence enabling the model to receive uniform and high-quality data. More preprocessing techniques include segmentation and cropping of signatures from the context in which they appear so that the model can concentrate solely on the signature itself. In terms of feature extraction, deep neural networks prove advantageous because they can automatically learn and extract static and dynamic features from signature data. Both the shape and geometry of a signature are part of static features. For dynamic features, these involve stroke speed, pressure, and order. These help in identifying a genuine and forged signature. Using CNNs and RNNs, the system can capture both spatial patterns in the signature image and temporal dependencies in the writing process. Hybrid models that combine CNNs and RNNs are particularly effective because they use both spatial and sequential data for a more comprehensive analysis. After building the model, it is trained with an appropriate loss function and optimization algorithm to minimize classification errors. Techniques such as dropout and batch normalization are applied to avoid overfitting and ensure that the model generalizes well to unseen data. The trained model is then evaluated on a test set using key metrics such as accuracy, precision, recall, and F1-score, which assess its performance in distinguishing between genuine and forged signatures. After satisfactory results have been achieved, the model is rolled out into real- world applications, such as document authentication systems, where it automatically can classify signatures as either real or forged. This automated process greatly improves signature verification efficiency, minimizes the possibility of human error, and accelerates document processing. In addition, the process of continuous retraining with new data ensures that the system stays updated, and follows new forgery techniques for maintaining high detection accuracy. The deep neural networks for the purpose of detecting handwritten signature forgery represent a huge advance in biometric security and in document authentication. Because of automatically learning complex features and capturing static as well as dynamic aspects of signatures. DNNs represent an effective and reliable means to separate genuine signatures from forgeries. This approach not only makes the signature verification systems accurate but also scalable and robust, thus becoming a critical resource in preventing signature fraud as well as ensuring document integrity in various industries. Deep neural networks have transformed handwritten signature forgery detection, achieving unprecedented accuracy levels. However, addressing existing challenges and exploring innovative architectures will be critical for advancing this field

REFERENCES

[1] Gideon, S. Jerome, et al. "Handwritten Signature Forgery Detection using Convolutional Neural Networks." Procedia computer science 143 (2018): 978-987.

[2] Kumar, L. Ravi, and A. Sudhir Babu. "Genuine and Forged Offline Signature Verification Using Back Propagation Neural Networks." IJCSIT) International Journal of Computer Science and Information Technologies (2011).

[3] Alvarez, Gabe, Blue Sheffer, and Morgan Bryant. Offline Signature Verification with Convolutional Neural Networks. Tech. rep., Stanford University, Stanford, 2016.

[4] Kumar, D. Ashok, and S. Dhandapani. "A Novel Bank Check Signature Verification Model using Concentric Circle Masking Features and its Performance Analysis over Various Neural Network Training Functions." Indian Journal of Science and Technology 9.31 (2016).

[5] Jarad, Mujahed, Nijad Al-Najdawi, and Sara Tedmori. "Offline handwritten signature verification system using a supervised neural network approach." Computer Science and Information Technology (CSIT), 2014 6th International Conference on. IEEE, 2014.

[6] Srinivasan, Harish, Sargur N. Srihari, and Matthew J. Beal. "Machine learning for signature verification." Computer Vision, Graphics and Image Processing. Springer, Berlin, Heidelberg, 2006. 761-775.

[7] Kumar, D. A., and S. Dhandapani. "A Bank Cheque Signature Verification System using FFBP Neural Network Architecture and Feature Extraction based on GLCM." International Journal of Emerging Trends and Technology in Computer Science (IJETTCS) 3.3 (2014).

[8] RamachandraA, C., et al. "Robust Offline signature verification based on global features." Advance Computing Conference, 2009. IACC 2009. IEEE International. IEEE, 2009.

[9] Malekian, Vahid, et al. "Rapid off-line signature verification based on Signature Envelope and Adaptive Density Partitioning." Pattern Recognition and Image Analysis (PRIA), 2013 First Iranian Conference on FEEE, 2013.

DOI: 10.48175/568





International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 3, December 2024

[10] Ribeiro, Bernardete, et al. "Deep learning networks for off-line handwritten signature recognition." Iberoamerican Congress on Pattern Recognition. Springer, Berlin, Heidelberg, 2011.

[11] Hafemann, L. G., Sabourin, R., & Oliveira, L. S. (2017). Offline handwritten signature verification-Deep learning approach. Pattern Recognition, 70, 163-176.

[12] Alaei, A., Pal, U., & Blumenstein, M. (2020). Signature verification using a CNN-based attention model. International Journal on Document Analysis and Recognition, 23(3), 259-275.

[13] Yang, Z., Wang, Y., & Zhao, X. (2019). A hybrid CNN-LSTM model for dynamic signature verification. IEEE Transactions on Information Forensics and Security, 14(9), 2474-2487.

[14] Hafemann, L. G., Sabourin, R., & Oliveira, L. S. (2019). Learning features for offline handwritten signature verification using deep neural networks. Pattern Recognition, 84, 37-51.

