Automated Detection of Forgeries in Documents Using Segmentation Neural Networks

Lohvynenko Serhii Romanovych
Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, serhii.lohvynenko@nure.ua

Prosolov Vladyslav Valeriiovych
Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, vladyslav.prosolov@nure.ua

Abstract: *This paper presents a neural network–based approach for automated detection of forged areas in PDF documents. The method converts document pages into image representations and applies semantic segmentation to localize manipulations such as inserted signatures or replaced text. U-Net and DeepLabV3+ architectures were trained on a dataset of authentic and synthetically forged samples. Experimental results show that segmentation models achieve high accuracy (IoU ≈ 0.91), outperforming traditional metadata-based techniques. The proposed solution can be integrated into electronic document management and cybersecurity systems for automated authenticity verification.*

Keywords: *document forgery detection; PDF integrity; U-Net; DeepLabV3+; semantic segmentation; deep learning; cybersecurity; document analysis.*

I. Introduction and Problem statement

With the digitalization of legal and financial workflows, PDF has become the main format for storing and exchanging documents. Ensuring their authenticity is essential to prevent fraud and maintain data integrity. Traditional verification methods such as metadata or checksum analysis work only for unchanged files and fail to detect localized manipulations like inserted signatures or altered text [1].

Deep learning has transformed digital forgery detection. Convolutional neural networks (CNNs) can identify subtle texture and structural inconsistencies that traditional algorithms miss. Recent studies demonstrate the superiority of such models for document image analysis [2]. For example, Al-Ameri et al. [2] proposed an unsupervised graph-based framework, while Bae et al. [3] developed edge-focused models for boundary localization. Li et al. [4] improved accuracy through spatial-frequency and multi-scale features.

However, most existing methods classify entire documents as forged or authentic without locating the specific manipulated regions. This study aims to develop a segmentation-based approach capable of detecting and localizing forged areas in PDF documents using U-Net and DeepLabV3+ architectures [5].

II. Problem solution and Results

The proposed system functions as an end-to-end pipeline for automated forgery localization in PDF documents. Each page is first converted into a high-resolution RGB image, preserving the visual layout and typography. Ground-truth masks are created to distinguish authentic and manipulated regions, forming the dataset for supervised training. To improve model robustness, data augmentation is applied, introducing noise, compression, and blurring that imitate scanning artifacts and low-quality exports.

The core of the method is based on semantic segmentation using U-Net [6] and DeepLabV3+ [5] architectures implemented in TensorFlow and PyTorch. These models classify every pixel as genuine or forged. Evaluation using IoU, precision, and recall metrics shows that U-Net achieves high boundary accuracy in detecting small manipulations, while DeepLabV3+ provides better stability under compression and layout variations.

Experimental results, consistent with recent studies on texture- and edge-aware networks [5], demonstrate that the combined approach achieves about 0.90 IoU and 95% pixel accuracy, outperforming traditional metadata-based techniques. The method enables clear visualization of tampered regions, offering interpretable and efficient document verification suitable for real-world digital forensics and cybersecurity applications.

III. Conclusions

Segmentation-based neural networks effectively detect and localize forgeries in PDF documents. The combination of U-Net and DeepLabV3+ provides accurate boundary recognition and stable performance across various document types, outperforming traditional metadata-based methods. The proposed approach can be integrated into electronic document management and cybersecurity systems. Future work will focus on expanding the dataset with real forged samples, optimizing model performance for real-time use, and combining segmentation with cryptographic verification to ensure complete document integrity.

REFERENCES

[1]. M. Zanardelli, F. Guerrini, R. Leonardi, N. Adami “Image forgery detection: a survey of recent deep-learning approaches” *Multimedia Tools and Applications*, vol. 82, pp. 18747–18779, 2023.

[2]. M. A. A. Al-Ameri, B. Mahmood, B. Ciylan, A. Amged “Unsupervised Forgery Detection of Documents: A Network-Based Framework,” *Electronics*, vol. 12, no. 7, p. 1682, 2023.

[3]. Y.-Y. Bae ,D.-J. Cho, K.-H. Jung “Enhancing Document Forgery Detection with Edge-Focused Deep Learning,” Symmetry, vol. 17, no. 8, 1208, 2025.

[4]. L. Li, Y. Bai, S. Zhang, M. Emam “Document forgery detection based on spatial-frequency and multi-scale feature network” *Journal of Visual Communication and Image Representation*, vol. 98, 104952, 2025.

[5]. X. Liao, S. Chen, J. Chen, T. Wang, X. Li, “CTP-Net: Character-Texture Perception Network for Document Forgery Localization,” *arXiv preprint*, 2023.

[6]. L.-C. Chen, Y. Zhu, G. Papandreou, F. Schroff, H. Adam “Encoder-Decoder with Atrous Separable Convolution for Semantic Image Segmentation” *ECCV*, 2018.