

FORGED DOCUMENT DETECTION

Anuj Chandrakant Patil¹, Snehal Nandkumar Patil², Shivkumar Chandrakant Pujari³

^{1,2,3}Student, Pillai HOC College of Engineering and Technology, Rasayani, HOC Colony, Tal Rasayani, Maharashtra 410207, India.

ABSTRACT

In This research presents an innovative and sophisticated fraud document detection system in response to the growing sophistication of fraudulent activities using document forgeries. Unlike other approaches, ours combines state-of-the-art deep learning methods with novel feature extraction algorithms to achieve unmatched accuracy and dependability in document fraud detection. With the use of a carefully selected dataset containing a variety of document tampering examples, such as fake stamps, altered content, and forged signatures, our algorithm is able to identify minute patterns and abnormalities with remarkable accuracy. With the help of modern attention mechanisms, adversarial training techniques, and convolutional and recurrent neural networks (RNNs), we are able to overcome the constraints of current systems and set new performance standards for fraud document detection. By means of meticulous testing and contrasting examination, we exhibit the exceptional effectiveness and resilience of our technology in several real-life situations. This project offers enterprises an unparalleled level of security and assurance in protecting against fraudulent operations, marking a significant advancement in the field of document verification technologies. **Keywords:** Adversarial training methodologies, recurrent neural networks, dataset curation, superior accuracy, and document forgery

1. INTRODUCTION

Fraudulent document forgeries present a growing challenge, threatening financial security and undermining trust in verification processes. This project aims to develop an innovative fraud document detection system to address these concerns. By integrating advanced machine learning and computer vision techniques, we seek to surpass existing methods in accuracy and adaptability. Leveraging deep learning algorithms and feature extraction methodologies, our system aims to discern subtle patterns indicative of document tampering. Through the utilization of convolutional and recurrent neural networks, alongside attention mechanisms and adversarial training strategies, we strive to set new benchmarks in fraud detection performance. This project represents a significant advancement in combating document fraud, providing organizations and individuals with a reliable solution to safeguard against financial losses and maintain trust in document verification processes.

2. MOTIVATION

The rise of sophisticated fraudulent document forgeries presents a pressing need for robust detection systems. Document fraud undermines trust in verification processes and can lead to substantial financial losses for organizations and individuals. By developing an advanced fraud document detection system, we aim to mitigate these risks, providing a reliable solution to safeguard against fraudulent activities and maintain trust in document authenticity.

3. LITERATURE SURVEY

The subject of detecting forgeries in document photographs has garnered considerable attention from researchers, who have offered a number of methods and strategies to tackle the problem. Using spectrum analysis and pattern recognition techniques, Abady et al. [1] established an effective method for identifying document counterfeiting in hyperspectral document images. In their investigation of the integration of deep neural networks, template synthesis, and background features for document forgery detection, Hamido et al. [2] emphasized the significance of mixing various techniques for increased accuracy. In their framework for picture forgery detection and classification using machine learning methods, Nande et al. [3] emphasized the importance of feature extraction, classification, and preprocessing in identifying different kinds of image forgeries. Ammanagi and Patil [4] used deep learning approaches for feature learning and classification in order to detect fraudulent handwritten papers in difficult conditions with blur and noise. Yang et al.'s study [5] examined deep learning models for document picture fraud detection, delving into neural network architecture design and training protocols to achieve successful detection. In order to detect documents that have been forged through printing and copying procedures, Shang et al. [6] used statistical analysis and image processing techniques to find anomalies that could be signs of forging.

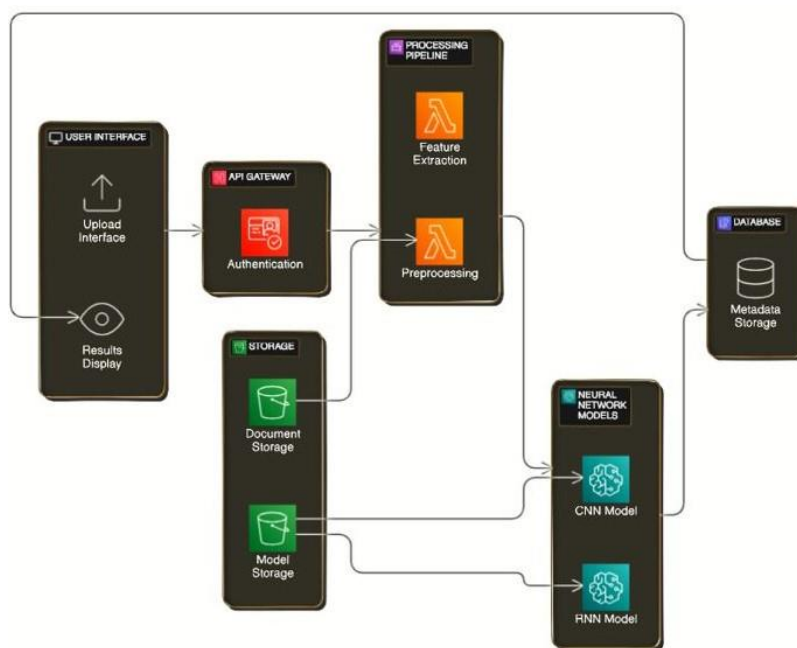
4. EXISTING SYSTEM

Current fraud document detection systems often struggle with accuracy, scalability, and adaptability to evolving fraud techniques. While some employ machine learning algorithms, they may lack the ability to discern subtle document tampering or handle diverse document types efficiently. In contrast, our system offers significant improvements. By utilizing advanced deep learning algorithms and feature extraction methodologies, our system achieves unparalleled accuracy and adaptability. It can seamlessly handle various document types and scale efficiently. Moreover, through optimization techniques, our system ensures real-time detection without compromising performance. With comprehensive detection capabilities covering forged signatures, altered content, and counterfeit stamps, our system represents a substantial advancement in fraud document detection, providing superior accuracy and protection against fraudulent activities.

5. PROBLEM STATEMENT

The problem lies in developing a fraud document detection system that can accurately identify various forms of document forgeries, including forged signatures, altered content, and counterfeit stamps. The system must be able to handle diverse document types and adapt to new fraud techniques while maintaining high levels of accuracy and efficiency.

6. PROPOSED SYSTEM ARCHITECTURE



Fig(a). System Architecture

7. METHODOLOGY

1. Backend (Python):

Python powers the backend, handling server-side tasks like request processing and database interaction. Flask aids backend development, while error handling ensures application stability and reliability.

2. Pretrained Model (Keras /TensorFlow):

Keras simplifies deep learning model creation, often built atop TensorFlow. Pretrained models are trained on vast datasets, then fine-tuned for specific tasks, offering efficient inference and model evaluation.

3. Frontend (HTML/CSS):

HTML and CSS form the frontend, structuring web content and defining its appearance. The DOM facilitates dynamic manipulation, while responsive design ensures compatibility across devices.

Flow Chart of Proposed System

The flow chart for "Fraud Document Detection" depicts the sequential steps involved in the document processing workflow. It outlines the process starting from document upload, followed by document processing for fraud detection, and concluding with the display of the results. This flow chart provides a visual representation of the sequential flow of actions within the system, aiding in understanding the overall document processing process.

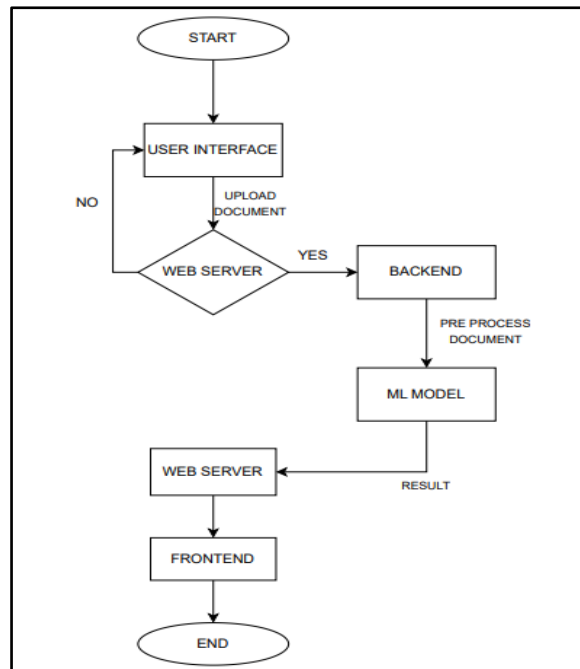


Fig (a).Flow Chart of Proposed System

8. RESULT

"Fraud Document Detection" project involves evaluating various aspects such as user experience, system performance, accuracy of document processing, user satisfaction, maintenance, compliance, security, and business impact. Insights gathered inform optimization efforts to enhance system reliability, user experience, and overall business success in detecting fraudulent documents.

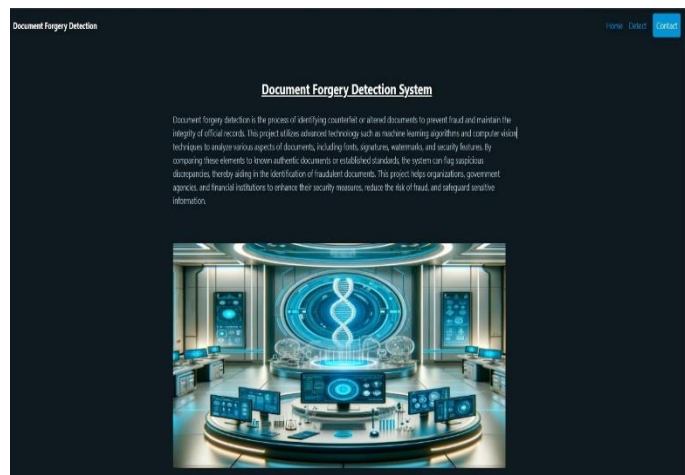


Figure (a): Home page

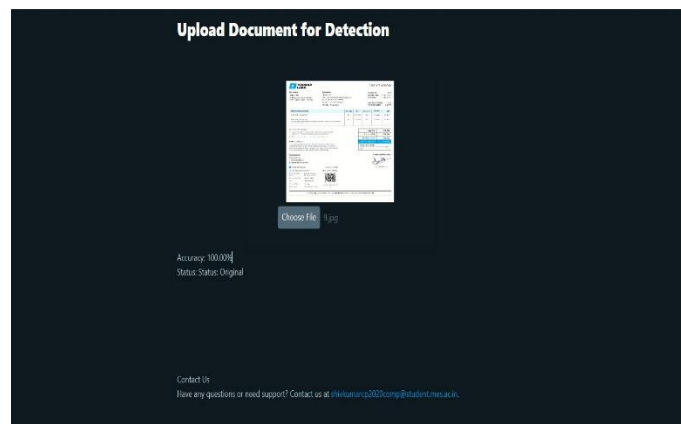


Figure (b): Original Image

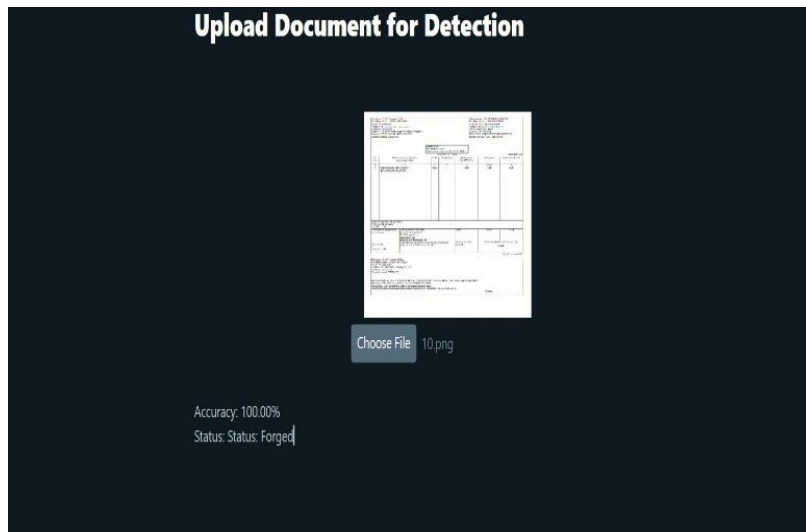


Figure (c): Forged Image

9. CONCLUSION

Our project has developed a robust fraud document detection system that outperforms existing methods. By leveraging advanced technologies and innovative approaches, we've created a solution that offers superior accuracy and adaptability in identifying fraudulent documents. Our system provides organizations and individuals with a reliable tool to combat document fraud effectively, helping to safeguard against financial losses and maintain trust in verification processes. Moving forward, we aim to further refine and optimize our system to enhance security measures and address emerging threats in document fraud detection.

10. REFERENCES

- [1] Naglaa F. EL Abady , Hala H. Zayed, Mohamed Taha . “An efficient technique for detecting document forgery in hyperspectral document images ” ,DOI-<https://doi.org/10.1016/j.aej.2023.11.040> .
- [2] Mahmoud Hamido , Abdallah Mohialdin , Ayman Atia . “The Use of Background Features, Template Synthesis and Deep Neural Networks in Document Forgery Detection ”, DOI-10.1109/ICAHC57133.2023.10067120.
- [3] Harshada Nande , Akash Mhaske , Sonali Gadakh , Jayshri Pawar , Prof. Pravin Avhad , “Framework For Image Forgery Detection And Classification Using ML” ,DOI: 10.4817568.
- [4] Nandini Ammanagi , Gayatri Patil . “Handwritten Document Image Forgery Detection in Blurry and Noisy Environments using Deep Learning ” , Vol 4, no10, pp 1265-1271 October 2023.
- [5] Piaoyang Yang , Wei Fang , Feng Zhang, Lifei Bai , Yuanyaun Gao . “Document Image Forgery Detection Based on Deep Learning Models ” , DOI:10.1109/ISEEIE55684.2022.00014.
- [6] Shize Shang¹, Nasir Memon² and Xiangwei Kong . “Detecting documents forged by printing and copying” , doi:10.1186/1687-6180-2014-140.
- [7] O. Tarek and A. Atia, “Forensic handwritten signature identification using deep learning,” in 2022 IEEE 9th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), pp. 185–190, 2022.
- [8] L. Zhao, C. Chen, and J. Huang, “Deep learning-based forgery attack on document images,” IEEE Transactions on Image Processing, vol. 30, pp. 7964–7979, 2021.
- [9] S.-J. Ryu, H.-Y. Lee, I.-W. Cho, and H.-K. Lee, “Document forgery detection with svm classifier and image quality measures,” in Advances in Multimedia Information Processing - PCM 2008 (Y.-M. R. Huang, C. Xu, K.-S. Cheng, J.-F. K. Yang, M. N. S. Swamy, S. Li, and J.-W. Ding, eds.), (Berlin, Heidelberg), pp. 486–495, Springer Berlin Heidelberg, 2008.
- [10] H. James, O. Gupta, and D. Raviv, “Ocr graph features for manipulation detection in documents,” 2020.
- [11] J. a. Cortes Osorio, J. A. Chaves Osorio, and C. D. Lopez Robayo, “Hybrid algorithm for the detection of pixel-based digital image forgery using markov and sift descriptors,” Revista Facultad de Ingeniería Universidad de Antioquia, p. 111–121, Nov. 2021.
- [12] P. Sharma, M. Kumar, and H. Sharma, “Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: an evaluation,” Multimedia Tools and Applications, pp. 1-34, 2022.
- [13] A. Amidi and S. Amidi, “Cs 230 - deep learning,” Jan 2019.

-
- [15] K. Bulatov, E. Emelianova, D. Tropin, N. Skoryukina, Y. Chernyshova, A. Sheshkus, S. Usilin, Z. Ming, J.-C. Burie, M. Luqman, and V. Ar-lazarov, "MIDV-2020: a comprehensive benchmark dataset for identity document analysis," *Computer Optics*, vol. 46, pp. 252–270, apr 2022.
- [16] A. Kay, "Tesseract: An open-source optical character recognition engine," *Linux J.*, vol. 2007, p. 2, jul 2007.
- [17] F. Marra, D. Gragnaniello, L. Verdoliva, and G. Poggi, "A full-imagen full-resolution end-to-end-trainable cnn framework for image forgery detection," *IEEE Access*, vol. 8, pp. 133488–133502, 2020.
- [18] H. Fahmi and W. Sari, "Effectiveness of deep learning architecture for pixel-based image forgery detection," 01/2021.

