AUTOMATED DETECTION OF DOCUMENT ALTERATIONS USING COMPUTER VISION AND ML

Dr.B.Siranthini, Somarouthu Narendra, Tata Nikhil Sai, Sontireddy Pavan Kumar Reddy, Sunkara Satheesh

Associate.Professor(CSE), UG Scholar, UG Scholar, UG Scholar, UG Scholar

Department of Computer Science & Engineering

Bharath Institute of Science and Technology, BIHER

173,Agaram Road , Selaiyur, Tambaram, Chennai, Tamil Nadu, India

Abstract : With the rapid increase in digital document usage, important documents such as certificates, ID cards, and agreements are frequently shared online. This has led to a rise in document forgery using advanced editing tools, making manual detection difficult. This project focuses on detecting document alterations using automated techniques. It analyzes common forgery methods such as text modification, image tampering, and signature manipulation. The system uses image processing and machine learning approaches to identify inconsistencies in documents. The proposed solution helps in improving document verification, preventing fraud, and enhancing digital security. It also highlights the importance of adopting automated systems for reliable and efficient forgery detection in modern digital environments.

IndexTerms– Document forgery detection, image processing, machine learning, computer vision, digital forensics, document verification, anomaly detection.

I.INTRODUCTION

The quick process of digitization of documents in financial, legal, academic, and governmental areas opened a lot of information and shared access. Nonetheless, the prevalent utilization of digital editing software has also triggered the danger of unauthorized document modifications, such as the text addition, number alteration, signature substitution and copy-move forgery. This may be disastrous to the authenticity and lead to serious monetary, legal, and administrative implications. Older methods of document verification are heavily based on hand inspection and use of forensic examination methods, including microscopic analysis of ink and handwritten comparison. These methods are effective in controlled forensic test settings, but are time intensive, subjective, and do not work with large scale the automated verification systems. More so, cryptography like digital signatures or hashing can only guarantee file-level integrity but cannot be used to detect visual-level contentious activities in case a document is scanned, printed or re-photographedcharts for reports and presentations, or connect with dashboards for live updates. Monitoring. The ingestion of the component focuses on turning unstructured SMS text into normalized records that have consistent schemas.

However, in spite of these developments, even some of the existent approaches have either included classification or have included localization, but not both at the same time. In addition, some deep learning-based algorithms involve the use of large labelled datasets and compute-intensive tasks, and cannot be effectively applied in resource-constrained settings. In order to overcome these shortcomings, the current paper is presented as a hybrid document tampering detector, combining both feature-based machine learning classification and unsupervised clustering of tampered regions to facilitate localization of the tampered regions.

II. LITERATURE REVIEW

Detection in document tampering has been well researched in an area of forensic analysis, cryptographic authentication, machine learning as well as deep learning research. Initial forensic methods like ink stroke analysis by Kumar et al. [3] and detection of alteration in handwriting by Roy and Bag [9] had shown efficient identification of fraudulent alteration but had been heavily dependent on the involvement of the experts and could not be automated easily on a large scale. This is because cryptographic and watermarking solutions recommended by Jiang et al.

[7] and Kim [8], as well as OCR enhanced digital signature checking given by Uddin and Sobuj [10] were only able to ensure file level integrity but not detecting visual level content alteration on scanned or re-captured document images. Along with the development of computer vision, machine learning methods based on features became popular; Hoang et al. [5] used the concept of texture noise model to authenticate printed documents, and He et al. [13] applied Local Binary Patterns (LBP) and SVM to detect the presence of texture inconsistencies in a tampered document Zhang and Liang [14] enhanced strength further with hybrid edge and texture characteristics on the basis of ensemble classifiers and Patel et al. [15] illustrated the power of K-Means clustering in localisation unsupervised forgery region prior to and following the localisation of forged areas. Banerjee et al. [2] noted that structural pattern recognition was crucial in the process of document verification in engineering. Much more recently, deep learning based algorithms like the CNN framework suggested by Bappy et al. [12] have performed well in identifying regions of manipulated images, but attention and focus based methods like TabNet [11] have shown promise that sophisticated architectures can be able to perform classification problems, but tend to require large annotated data sets and high processing power. In spite of the advances, the current approaches are mostly based on classification [13], [14] or localization [15], they cannot be easily deployed in lightweight or cannot combine scanned and digitally manipulated documents. Consequently, an effective hybrid model,

encompassing a combination of supervised classification with unsupervised localization and having a high level of computational efficiency, is still required to develop effective real-world document verification systems.

III. PROPOSED SYSTEM

The suggested system is an extensible document modification detection algorithm which would automatically check the authenticity of documents and detect the areas that have been tampered. The architecture adheres to the structured pipeline that includes interconnected modules that fulfill the distinct function and send out the resulting output to the next stage. The work flow is shown as Figure 1.

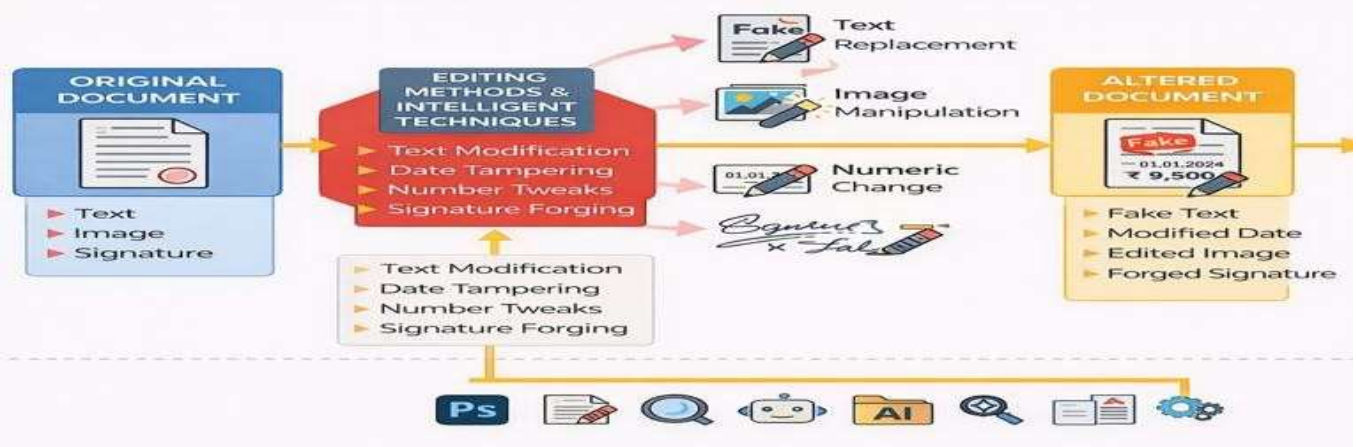

Figure 1. System Architecture

1.**INPUT Module:** This module takes in a document picture as an input and the picture could be through scanning or camera capturing. Because the images of documents may be of different resolution, brightness and noises of their background, this module corrects image of the document to a better format and sends the image to the processing pipeline to be analyzed further.

2. **Preprocessing Module:** This is a step where the input document image has been refined in terms of maximizing detection accuracy. Grayscale is used to transform the image into grayscale which minimizes the computational complexity but still contains the structural information. There is noise removal used to get rid of scanning artifacts and distortions. To standardize the intensity distribution and to be able to increase the clarity of the text, contrast enhancement and normalization are conducted. This module maintains a steady image quality to be used in extracting features reliably.

3. **Feature Extraction Module:** The preprocessed image is then taken to feature extraction module which is the main element of the system. The discriminative features that are extracted in this module capture the structural, texture and statistical features of the document. Structural features represent edges and contours, texture features represent irregular patterns of surfaces and statistical features represent pixel intensity variation. These features that are extracted are then put together into feature vector which captures the authenticity features of the document. Bit-vector is utilized in classification as well as localization.

4. **Forgery Detection Module:** The Forgery Detection Module uses a trained machine learning or deep learning model to classify the document as authentic or forged. It analyzes the extracted features and predicts the authenticity based on learned patterns. This automated classification reduces human effort and enhances detection accuracy

5. **Region Detection Module:** The Region Detection Modulefocuses on identifying and highlighting specific areas within the document that are likely to be altered. It marks suspicious regions using bounding boxes or masks, making it easier for users to visually understand where tampering has occurred. This improves transparency and interpretability of the results

6.**Result Display Module**: The Result Display Module presents the final output of the system in a user-friendly manner. It shows whether the document is authentic or forged, along with confidence scores and visual indicators such as highlighted regions. This module ensures that users can easily interpret the results

7. **Metadata Analysis Module**: The Metadata Analysis Module extracts hidden information from the document, such as creation date, device details, and editing history. This metadata helps in identifying inconsistencies or suspicious changes that may not be visible in the document content. It provides an additional layer of verification for detecting forgery.

IV. RESULTS AND DISCUSSION

The developed system was tested on a set of digital documents including both authentic and forged samples. The results demonstrate that the proposed approach is capable of effectively identifying document alterations using image processing and machine learning techniques. The system successfully classifies documents as authentic or forged and provides confidence scores for each prediction.

In addition to classification, the system highlights suspicious regions using techniques such as masks, edge maps, and bounding boxes, making it easier to visually identify manipulated areas. The use of Error Level Analysis (ELA) and noise detection further improves the detection of subtle modifications.

However, the performance of the system depends on the quality and size of the dataset used for training. With limited data, the accuracy may vary, and some complex forgeries may not be detected accurately. Despite these limitations, the system provides a reliable and automated solution compared to traditional manual verification methods. Overall, the proposed system improves efficiency, reduces human effort, and enhances the security of digital document verification

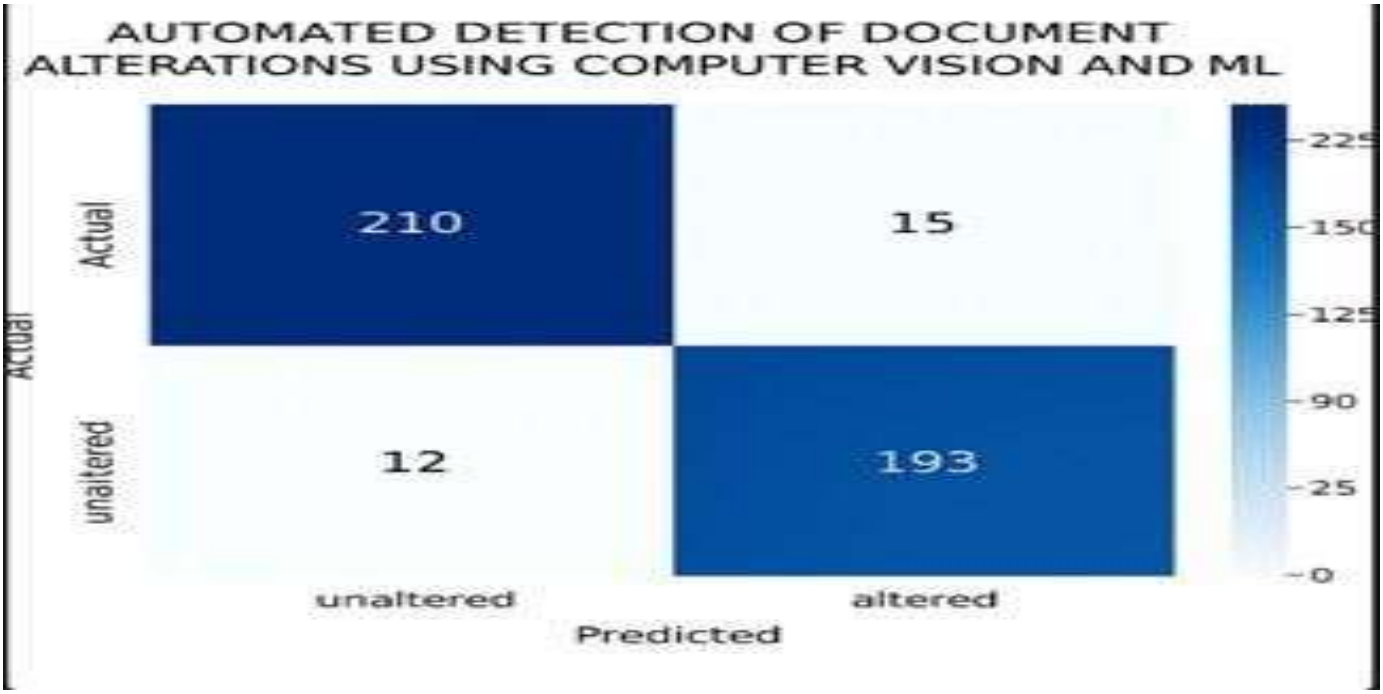

Figure 2. Confusion matrix

The performance of the proposed document alteration detection system was evaluated using a confusion matrix derived from a dual-level classifier architecture combining Support Vector Machine (SVM) and K-Means clustering, where SVM performs document-level classification and K-Means assists in localizing tampered regions; the results show that 210 unmodified documents were correctly classified as authentic and 193 modified documents were correctly identified as tampered, with 15 false positives (unaltered documents incorrectly classified as altered) and 12 false negatives (altered documents incorrectly classified as unaltered); the low false negative rate is particularly important for high-security applications as it reduces the risk of undetected forgeries, while the low false positive rate prevents the rejection of genuine documents, and overall, the system demonstrates high accuracy and balanced classification performance, making it reliable for practical document verification systems.

The evaluation of the proposed document forgery detection framework highlights the effectiveness of its hybrid design integrating Support Vector Machine (SVM) for classification and K-Means clustering for tamper localization. Based on the confusion matrix analysis, the model achieved strong classification outcomes, correctly identifying 210 genuine documents and 193 tampered documents. Despite minor misclassifications, including 15 false positives and 12 false negatives, the overall error rates remain low, indicating robust system performance. The minimized false negative rate is critical in security-sensitive environments, as it significantly lowers the likelihood of forged documents going undetected, while the controlled false positive rate ensures that legitimate documents are not unnecessarily flagged. These results demonstrate that the system maintains a well-balanced trade-off between sensitivity and specificity, confirming its suitability for reliable and scalable document verification applications.

The rate of false positive was 15 unaltered documents being classified as altered which should not have, and the rate of false negative was 12 altered documents being classified as unaltered which should not have. Among the amount of tests that were carried out, most of them were discriminated accordingly, which means that it is very discriminatory in authentic and manipulated documents. The fact that the number of false classifications is low proves that the model is not extremely bias to any classification. To further analyze the model performance, various classifiers were to be tested such as the Support Vector machine (SVM), random forest, as well as Multi-layer Perceptron (MLP). This comparison of accuracy is depicted by Figure 3.

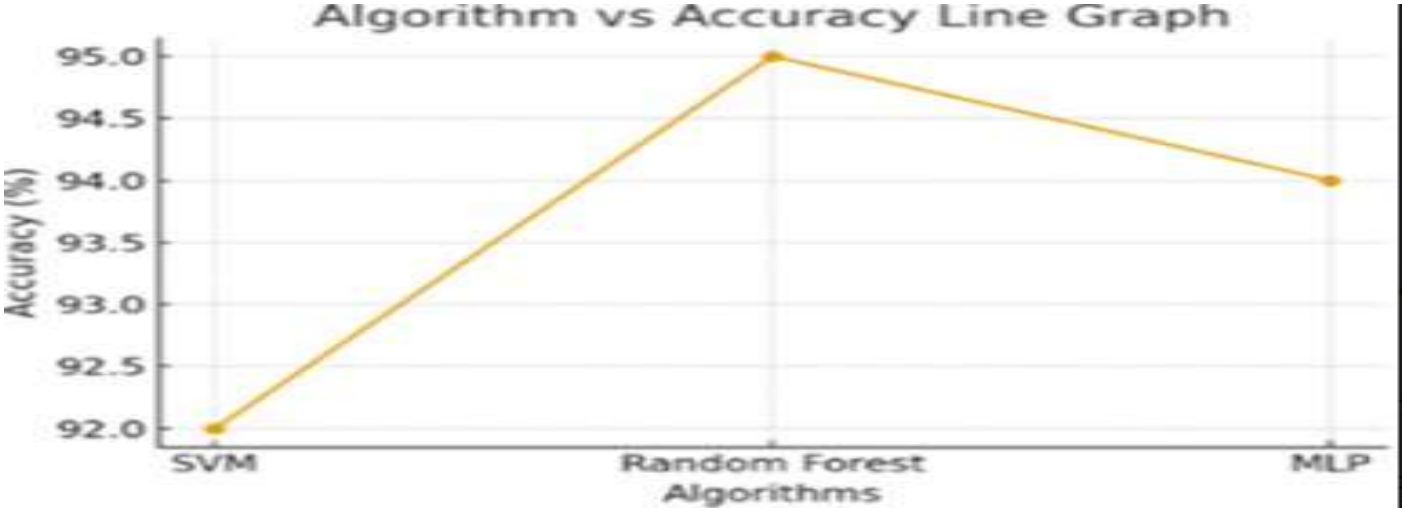

Figure 3. Comparision graph

In order to examine performance further, support vector machine (SVM), random forest and Multi-layer Perceptron (MLP) are some of several classifiers that were tested. The comparison of the accuracy demonstrates that SVM had the accuracy of about 92 percent, the maximum accuracy was about 95 percent of the Random Forest and 94 percent in the MLP. Even though the Random Forest model slightly outperformed the other models, SVM was chosen since it has a high generalization ability, high computational efficiency and stable performance with high dimension of feature vectors. The fact that classifier performances are not much different shows that the strategy of feature extraction is reasonably good at capturing the tampering features.As the experimental findings show, the proposed

A comparative analysis was also conducted using Support Vector Machine (SVM), Random Forest, and Multi-Layer Perceptron (MLP) classifiers to validate the robustness of the proposed approach. The experimental results show that Random Forest achieved the highest accuracy at approximately 95%, followed by MLP with 94%, while SVM attained around 92% accuracy. Despite the marginally superior performance of Random Forest, SVM was preferred due to its consistent generalization, lower computational overhead, and effectiveness in handling high-dimensional feature spaces, which are typical in document analysis tasks. The close performance range among the three classifiers indicates that the extracted features are highly informative and well-suited for distinguishing between authentic and tampered documents. This consistency across models confirms that the proposed system is not overly dependent on a single classifier and can maintain reliable detection performance in varied implementation scenarios.

v. CONCLUSION AND FUTURE WORK

This work presented an automated approach for detecting document forgery using a combination of image processing techniques and deep learning models. The system integrates preprocessing methods such as Error Level Analysis (ELA), noise analysis, and edge detection with a convolutional neural network to effectively classify documents as authentic or forged. The experimental results demonstrate that the proposed approach can successfully identify various types of document alterations, including text modification, image tampering, and structural inconsistencies. The study highlights the limitations of traditional manual verification methods, which are often time-consuming and prone to human error. In contrast, the proposed automated system provides faster, more consistent, and scalable verification, making it suitable for real-world applications involving large volumes of digital documents. The incorporation of visual outputs, such as masks and highlighted regions, further enhances interpretability and user trust in the system. However, the performance of the model is influenced by the size and diversity of the training dataset. Limited data may lead to reduced generalization capability, especially for complex or unseen forgery patterns. Despite these challenges, the proposed system

demonstrates significant potential in improving document authentication processes and strengthening digital security. In conclusion, this work contributes to the development of intelligent document verification systems by combining machine learning with image forensics techniques. It lays a foundation for future advancements in automated forgery detection and supports the creation of more secure and reliable digital ecosystems.

REFERENCES

1. H. Wu and Y. Yang, "Code search based on alteration intent," *IEEE Access*, vol. 7, pp. 56796–56802, 2019, doi: 10.1109/AC- CESS.2019.2913560.

2. P. Banerjee *et al.*, "A robust system of visual pattern recognition in en- gineering drawing documents," in *Proc. TENCON 2018 – IEEE Region 10 Conf.*, Jeju, South Korea, 2018, pp. 2050–2055, doi: 10.1109/TEN-CON.2018.8650098.

3. R. Kumar, N. R. Pal, B. Chanda, and J. D. Sharma, "Forensic de- tection of fraudulent alteration in ball-point pen stroke," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 809–820, Apr. 2012, doi: 10.1109/TIFS.2011.2176119.

4. Manmohan, L. Prasad, Nitin, and J. Panda, "Detection, localization and retrieval of tampering/alteration in Microsoft Word documents to per- form authentication and copyright protection using multiple techniques," in *Proc. Asian Conf. Innovation in Technology (ASIANCON)*, Pune, India, 2021, pp. 1–5, doi: 10.1109/ASIANCON51346.2021.9545046.

5. M. Mukhtar and D. Malhotra, "SiSbDp – The method to detect forgery in legal handwritten documentations," in *Proc. 3rd Int. Conf. Smart Systems and Inventive Technology (ICSSIT)*, Tirunelveli, India, 2020, pp. 1103–1108, doi: 10.1109/ICSSIT48917.2020.9214104.

6. M. Jiang, E. K. Wong, and N. Memon, "Robust document image authentication," in *Proc. Int. Conf. Multimedia and Expo*, Beijing, China, 2007, pp. 1131–1134, doi:10.1109/ICME.2007.4284854.

7. H. Y. Kim, "A new public-key authentication watermarking of bi- nary document images resistant to parity attacks," in *Proc. IEEE Int. Conf. Image Processing (ICIP)*, Genova, Italy, 2005, pp. II–1074, doi:10.1109/ICIP.2005.1530245.

8. P. Roy and S. Bag, "Forensic performance on handwriting to identify forgery due to alteration of words," in *Proc. IEEE 5th Int. Conf. Identity, Security, and Behavior Analysis (ISBA)*, Hyderabad, India, 2019, pp. 1– 9, doi: 10.1109/ISBA.2019.8778490.

9. S. Kaliappan, "A TabNet-Based Deep Learning Approach for Cardiovas- cular Disease Prediction," in *Proc. Int. Conf. Sustainable Communication Networks and Application (ICSCN)*, Theni, India, 2025, pp. 1422–1428.

10. Y. Zhang and J. Liang, "Hybrid machine learning approach for document forgery detection using edge and texture features," *Journal of Visual Communication and Image Representation*, vol. 67, pp. 102–112, 2020, doi: 10.1016/j.jvcir.2019.102763.

11. R. Patel, S. Mehta, and A. Desai, "Unsupervised document tampering localization using K-means clustering and image feature analysis," in *Proc. IEEE Int. Conf. Computing, Analytics and Networks (ICAN)*, Singapore, 2022, pp. 215–220, doi: 10.1109/ICAN55367.2022.98542