A Comprehensive Review of Image Tampering Detection: Techniques and Datasets

Samir P. Thokal[1], Sahil S. Tiwade[2], Devraj K. Thakkar[3], Arya H. Yelure[4], Sandip R. Warhade[5]

[1]Student, SCTR's Pune Institute of Computer Technology, (IT), Pune, Maharashtra, India
samirthokal2003@gmail.com
[2]Student, SCTR's Pune Institute of Computer Technology, (IT), Pune, Maharashtra, India
sahiltiwade123@gmail.com
[3]Student, SCTR's Pune Institute of Computer Technology, (IT), Pune, Maharashtra, India
3devrajthakkar@gmail.com
[4]Student, SCTR's Pune Institute of Computer Technology, (IT), Pune, Maharashtra, India
aryayelure@gmail.com
[5]Assistant Professor, SCTR's Pune Institute of Computer Technology, (IT), Pune, Maharashtra, India
srwarhade@pict.edu

Abstract

The proliferation of digital images across legal, financial, and academic domains has necessitated advanced methodologies for ensuring their authenticity and integrity. As image tampering techniques evolve, detecting manipulations such as copy-move, splicing, and deepfake alterations has become a critical research focus. This paper presents a comprehensive review of state-of-the-art image tampering detection techniques, categorizing them into machine learning-based, deep learning-based, cryptographic, and forensic approaches. Additionally, it examines publicly available datasets used for training and benchmarking detection models, assessing their effectiveness in real-world scenarios. By analyzing the strengths and limitations of existing methods, this study highlights ongoing challenges such as generalizability, adversarial robustness, and computational efficiency. Finally, it explores emerging trends and future research directions, emphasizing the need for scalable and resilient detection frameworks to counter evolving tampering threats.

Keywords: Image Document, Document Tampering, Deep learning, Document Verification, Document authentication, Forgery Detection, Convolutional Neural Network (CNN).

1. Introduction

The rapid digitization of documents and increasing reliance on digital formats for important legal, financial, and personal records have made document tampering a pressing issue. Document tampering, which involves the unauthorized alteration of a document's content, metadata, or structure, poses significant risks to document integrity and authenticity. Such manipulations can lead to fraud, misrepresentation, and other legal consequences. As the tools for tampering continue to evolve, so too must the methods for detecting these unauthorized alterations.

Traditional methods for detecting document tampering primarily relied on cryptographic techniques like digital signatures and hash functions [1]. While effective, these approaches often fail to detect tampering when access to cryptographic keys is compromised or when alterations are made to visual content, such as images or scanned documents. To address these challenges, forensic and machine learning-based methods have emerged as more comprehensive solutions. Recent advancements in deep learning and image analysis have proven particularly effective in detecting tampering in digital documents. For instance, frameworks leveraging deep learning and cloud-based services have achieved accuracy rates exceeding 95% in detecting forged images in documents [2].

Machine learning approaches, especially those involving CNN [13], are increasingly used to detect different types of forgery, including the copy-move and splicing operations. These methods analyze document image abnormalities, such as splicing boundaries, using differential abnormality detection techniques, which have been shown to be effective in locating tampered regions [3]. Moreover, capsule neural networks and error level analysis (ELA) have been successfully applied to detect signature forgery and copy-move forgery with high accuracy [4]. Such techniques provide a robust alternative to classical methods, especially in complex forgery scenarios.

In addition to machine learning techniques, methods based on structural similarity index (SSIM) and image analysis offer practical solutions for tampering detection, particularly in the domain of identity documents [5]. SSIM has been shown to be effective in identifying discrepancies between the original and tampered document images by analyzing structural differences, making it a valuable tool for detecting fraud in widely-used identity verification processes.

Despite the advancements, challenges remain. The development of effective tampering detection techniques is frequently limited by the lack of high-quality and diverse datasets. Large-scale datasets, such as the DocTamper dataset, which contains over 170,000 document images, have contributed to improving model accuracy and generalizability [6]. However, additional studies are required to improve the robustness of these methods against advanced tampering techniques, like JPEG anti-forensic attacks, which can effectively conceal signs of manipulation [7].

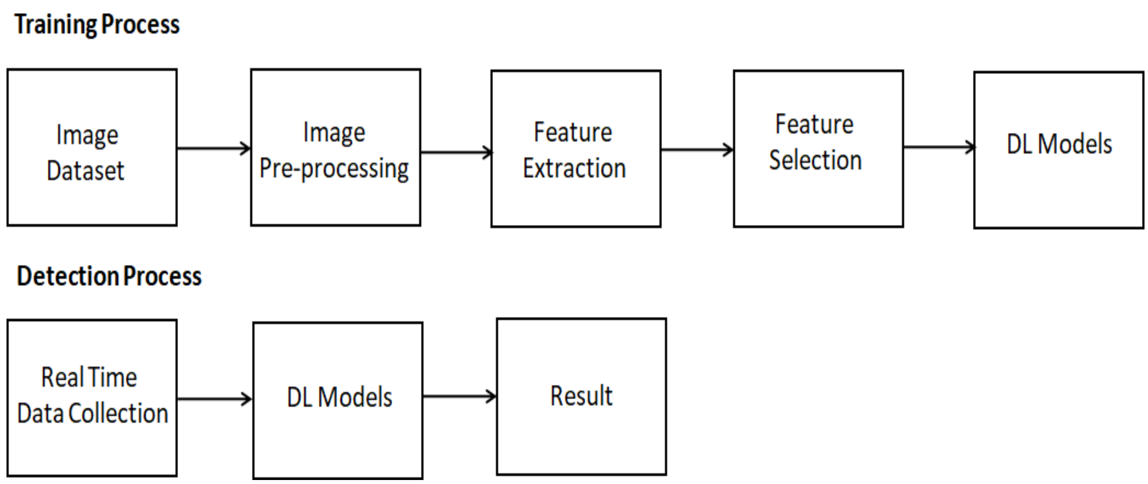

Fig. 1. DL Training and Detection Process

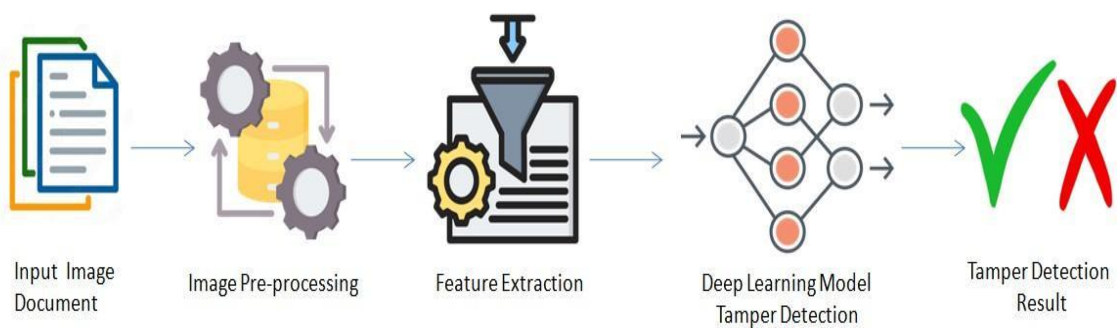

Fig. 2. Real Time Document tampering detection process.

This review paper explores various techniques for document tampering detection, focusing on recent advancements in deep learning, forensic analysis, and dataset utilization. The performance of these techniques are compared across different types of tampering and discuss the strengths and limitations of each approach. This review seeks to offer a thorough understanding of the present landscape of document tampering detection while highlighting promising avenues for future research.

2. Literature Survey

2.1 Datasets:

In the context of various research papers on image tampering and forgery detection, several publicly available datasets have been employed to evaluate and develop methods for detecting forged images. These datasets, cited by various researchers, are vital for the progression of forgery detection techniques, particularly in deep learning and image processing approaches.

The CASIA V2.0 dataset is frequently cited in various studies, including [1], where it is utilized for research on detecting image forgery and tampering with the help of deep learning and cloud-based technologies. CASIA is one of the most commonly used datasets for forgery detection, containing both authentic and tampered images, making it a valuable resource for developing and testing image forensic algorithms.

In [4], the DocTamper dataset is used for detecting tampered text in document images. This dataset specifically focuses on document image forgery and is vital for methods that need to detect alterations in text, providing robust solutions for document integrity verification.

The BOSSBase image dataset is employed in [6] to address challenges posed by JPEG anti-forensic attacks. BOSSBase is a widely recognized dataset for steganography and image manipulation research, and it contains grayscale images that are crucial for testing forensic methods focused on detecting subtle manipulations in images. In the detailed survey on deep learning-based techniques for image forgery detection in [7], the authors use several datasets, including Columbia, CASIA, Forensics, CoMoFoD, GRIP, and COVERAGE. These datasets encompass a wide variety of image tampering types, such as splicing, copy-move forgery, and resampling. The variety of datasets helps in evaluating the robustness of detection techniques across different types of manipulation scenarios.

The SLRID framework, presented in [8], utilizes common tampered datasets, including DSO, Columbia, NIST16, and CASIA. These datasets have been instrumental in developing tampering localization methods, as they contain a wide array of tampered and original images with ground-truth tamper maps, making them ideal for training and evaluating forgery localization models.

For image tampering localization, the study in [9] utilizes datasets such as the PS-scripted book-cover dataset, the PS-scripted Dresden dataset, the Artificial PS dataset with post-processing on boundaries (PS-boundary), and the Artificial PS dataset with arbitrary post-processing (PS-arbitrary). These datasets focus on forgery scenarios involving post-processing and arbitrary manipulations, making them suitable for testing tampering localization under complex conditions.

In [11], an improved YOLOv5s algorithm is evaluated using the Columbia, CASIA, and other datasets, highlighting its versatility in detecting forged images across different publicly available datasets. The inclusion of various datasets ensures the robustness of the algorithm in real-world scenarios. These datasets collectively contribute to the advancement of image forgery detection methods and provide diverse benchmarks for evaluating different approaches in this domain.

Table 1. Dataset Information

DATASET	YEAR	NUMBER OF IMAGES
CASIA V2.0	2022	12,000
Columbia	2006	7,200
BOSSBase	2021	10,000
DocTamper	2022	170,000
UCID	2021	1,338
Haze-20	2019	4,610
Caltech-256	2015	30,607

2.2 Techniques & Algorithms

A. Convolutional Neural Network (CNN)

CNN is commonly employed in image tampering detection because of their capability to recognize patterns and structures in images. By utilizing convolutional layers, CNN extract relevant features, while pooling layers decrease complexity while maintaining essential information. Fully connected layers are responsible for classifying these features, which makes CNN highly effective for identifying forgeries. The algorithm is as follows:

1. Start.
2. Input the image I into the CNN model.
3. Apply convolution to extract spatial features:

$$f(m,n) = \sum_{i=-k}^{k} \sum_{j=-k}^{k} I(m+i, n+j) \cdot K(i,j)$$

4. Pass the result through the activation function, e.g., ReLU:

$$f'(m,n) = max(0, f(m,n))$$

5. Perform pooling to reduce dimension:

$$P(m,n) = max\ f'(m+i, n+j) \qquad \ldots\ldots\ldots\ldots\ldots\ldots (i,j) \epsilon W$$

6. Flatten the pooled output and feed it into fully connected layer:

$$o_i = \sigma\left(\sum_j w_{ij} h_j + b_i\right)$$

7. Output the probability of tampering.
8. End

B. Capsule Neural Networks (CapsNets)

Capsule networks improve on traditional CNNs by preserving spatial relationships between features. Instead of scalar values, they use vectors to encode feature properties, and a routing mechanism ensures accurate feature mapping. This makes CapsNets suitable for detecting tampering with high precision. The algorithm is as follows:

1. Start.
2. Extract features using initial convolution layers:

$$f(m,n) = \sum_{i=-k}^{k} \sum_{j=-k}^{k} I(m+i, n+j) \cdot K(i,j)$$

3. Group extracted features into capsules s_j:
4. Apply the squashing function:

$$v_j = \frac{\left|\left|a_j\right|\right|^2}{1 + \left|\left|a_j\right|\right|^2} \cdot \frac{a_j}{\left|\left|a_j\right|\right|}$$

5. Initializing routing logits $s_{ij} = 0$:
6. Calculate coupling coefficients:

$$c_{ij} = \frac{exp(b_{ij})}{\Sigma_k\ exp(b_{ik})}$$

7. Update routing logits:

$$b_{ij} = b_{ij} + v_j \cdot u_i$$

8. Use final capsule outputs to classify tampered regions.
9. End.

C. Error Level Analysis (ELA)

ELA detects image tampering by identifying inconsistencies in compression levels. Edited areas often show different compression characteristics compared to unaltered regions. This makes ELA effective for spotting tampered sections in JPEG images. The algorithm is as follows:

1. Start.
2. Compress the original image I_{original} at a known quality .
3. Save the compressed image as $I_{\text{compressed.}}$
4. Compute pixel-wise differences:
$$D(m,n) = \left| I_{original}(m,n) - I_{compressed}(m,n) \right|$$
5. Normalize the differences to enhance visualization.
6. Identify regions where $D(m,n) > T$, where T is a predefined threshold.
7. Highlight the tampered regions.
8. End.

D. Binarized Difference Image (BDI) Computation

BDI is a pixel-based method that identifies discrepancies between two images by computing the absolute difference. By applying a threshold, it effectively isolates regions that have been tampered with. The algorithm is as follows:

1. Start.
2. Take the original image I_1 and the suspected tampered image I_2.
3. Compute absolute pixel-wise differences:
$$D(m,n) = | I_1(m,n) - I_2(m,n)|$$
4. Apply a threshold T to binarize the differences:
$$BDI(m,n) = \begin{cases} 1 & \text{if } D(m,n) > T \\ 0 & \text{otherwise} \end{cases}$$
5. Overlay the binary mask on I_2 to highlight tampered regions.
6. End.

E. Structural Similarity Index (SSIM)

SSIM compares two images by analyzing structural information, luminance, and contrast. It assesses the perceived quality of an image and is frequently used to detect alterations by measuring the similarity between two images. The algorithm is as follows:

1. Start.
2. Compute the luminance for both images m and n:
$\mu_m = mean(m), \quad \mu_n = mean(n)$
3. Calculate the contrast values:
$\sigma_{mn} = std(m), \quad \sigma_n = std(n)$
4. Compute the covariance between x and y:
$\sigma_{mn} = \frac{1}{N-1} \sum_{i=1}^{N} (m_i - \mu_m)(m_i - \mu_m)$
5. Calculate SSIM using:
$$SSIM(m,n) = \frac{(2\mu_m\mu_n + C_1)(2\sigma_{mn} + C_2)}{(\mu_m^2 + \mu_n^2 + C_1)(\sigma_m^2 + \sigma_n^2 + C_2)}$$
6. Identify areas with low SSIM scores as tampered regions.
7. End

F. Support Vector Machines (SVM)

SVM is a machine learning method that classifies data points into separate categories by using a hyperplane. By minimizing classification errors, SVM is highly effective for binary classification tasks, including distinguishing between tampered and authentic images. The algorithm is as follows:

1. Start.
2. Prepare the training dataset (x_i, y_i), where x_i are feature vectors and y_i are labels.
3. Define the decision boundary:

$$f(m) = \omega^T m + b$$

4. Optimize the hinge loss function:

$$L = \sum_{i=1}^{N} max(0, 1 - y_i(\omega^T m_i + b)) + \frac{\lambda}{2} \left|\left| \omega \right|\right|^2$$

5. Train the SVM model using the labeled data.
6. Use the trained model to classify new samples:

$$\hat{n} = sign(f(m))$$

7. Identify tampered regions based on classification results.
8. End

Fig. 3. An example of an original document and tampered document.

2.3 Evaluation Metrics

In document tampering detection, various evaluation metrics are employed across different methodologies, each contribut- ing to an effective assessment of detection techniques. Below are the key metrics commonly used, with multiple references illustrating their application in different papers?

A. Precision (P) and Recall (R)

Precision and recall are essential metrics in pixel-level tampering detection tasks. Precision evaluates the ratio of correctly identified tampered pixels (true positives) to the total number of detected tampered pixels, while recall measures the ratio of true positives to the actual number of tampered pixels. These metrics play a critical role in deep learning-based approaches for image forgery detection [7][12]. High precision minimizes false positives, while high recall reduces the chances of missing tampered regions.

$$P = \frac{TP}{TP + FP} \tag{1}$$

$$R = \frac{TP}{TP + FN} \tag{2}$$

Where TP represents true positives, FP stands for false positives, and FN refers to false negatives.

B. Markov Transition Matrices and Confusion Matrices

Markov transition matrices are used in digital image forensics, particularly when detecting tampering under JPEG compression attacks. These matrices analyze transitions between pixel states in the DCT domain, which helps in identifying unnatural patterns caused by tampering [6]. Confusion matrices are frequently used to assess the classification performance of forgery detection models, displaying true positives, false positives, true negatives, and false negatives [6][8]. This combination of matrices helps ensure that the detection systems remain robust against anti-forensic strategies.

C. Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index (SSIM)

PSNR and SSIM are frequently used for evaluating the quality of image reconstruction following tampering detection. PSNR assesses the overall error by comparing the original and reconstructed images, with higher values indicating better reconstruction [8][10]. SSIM focuses on perceptual similarity by evaluating structural, luminance, and contrast information [5]. These metrics have been widely adopted in forensic image recovery and tampering localization tasks.

$$PSNR = 10 . log_{10}\left(\frac{MAX_I^2}{MSE}\right) \tag{3}$$

Where MAX_I is the maximum possible pixel value and MSE is the mean squared error between the original and tampered images.

D. Mean Average Precision (MAP), F1 Score, and Area under the Curve (AUC)

MAP is a key metric in evaluating object detection models used for tampering detection. It computes the average precision across various recall thresholds, ensuring a comprehensive evaluation of detection performance. The F1 score, which is the harmonic mean of precision and recall, provides a balanced measure between the two [11][12]. AUC is commonly used to assess a model's ability to differentiate between true and false positives [7]. Together, these metrics offer a comprehensive evaluation of the system's detection performance.

$$F1 = 2 . \frac{P.R}{P + R} \tag{4}$$

E. Intersection over Union (IoU), False Negative Rate (FNR), and F1 Score

IoU is crucial for assessing the accuracy of tampered region localization. It computes the ratio of the intersection to the union of the predicted and actual tampered regions, with higher values indicating more accurate localization [12][7]. IoU is further complemented by the false negative rate (FNR), which quantifies the proportion of tampered areas that the detection algorithm failed to recognize.

$$IoU = \frac{Area_{predicted} \cap Area_{actual}}{Area_{predicted} \cup Area_{actual}} \tag{5}$$

By analyzing IoU and FNR, researchers can effectively evaluate and enhance their localization models for tampered regions.

Table 2. Survey of Image Forgery Detection Methods and Technologies

Paper	Title	Authors	Methodology / Parameters Used	Features	Gaps / Limitations
[1]	Deep Learning and Cloud for Forgery Detection	Misbah Shaikh et al.	- CNN for feature extrac- tion and classification. - Azure Form Recognizer for text and data validation - CASIA V2.0 dataset	- Dual approach (image processing and cloud service) - Over 90% accuracy using combined method - Robust against diverse forgeries	- Relies on availability of records in the database - Limited generalization beyond specific datasets
[2]	Tampering Detection Using Differential Abnormality	K. Sun et al.	- First-order spatial difference computation for tampering boundaries - Row and column difference fusion - Adaptive sliding window and Hough transform for boundary detection	- Effective for detect- ing splicing and copy- move forgeries - Median filtering for noise reduction - Works well on mo- bile phone images with specific setups.	- Limited to mobile- captured images - Requires parame- ter tuning for optimal threshold settings
[3]	Detecting Forgery in Documents	Nandini N. et al.	- Capsule Neural Net- work (CapsNet) for signature forgery detection - Error Level Analysis (ELA) for detecting com- pression inconsistencies -Ensemble model combin- ing multiple forgery detec- tors	- Detection of both signature and copy- move forgery - ELA reframing to improve model accuracy - Achieved promising results with custom datasets	- Limited dataset variability; Poor generalization to datasets with different distributions - Not applicable to video formats without further development
[4]	Tampered Text Detection	Chenfan Qu et al.	- proposed DTD framework incorporates the Frequency Perception Head (FPH) and the Multi-view Iterative Decoder (MID) - Used DocTamper dataset with novel CLTD training paradigm.	- Introduced a novel large-scale dataset (DocTamper). - Multi-modality features improve detection - Robust image compression and cross- domain testing.	- Focused mainly on tampered text; May not generalize to other types of tampering. - Complexity of dataset generation could hinder adoption by other researchers..

[5]	Document Tam- pering Detection with SSIM	Prof. Divya Pandey et al.	- Structural Similarity In- dex (SSIM) for tampering detection. - Grayscale conversion. - Global thresholding for binarization. - Contour detection for shape analysis. - Difference maps and contour overlays for visualization.	- Effective for identity document verification. - Provides quantitative SSIM scores and visual evidence of tampering. - Simple and inter- pretable technique.	- Requires original document for comparison. - Reduced accuracy under compression or poor image quality.

Table 2. Survey of Image Forgery Detection Methods and Technologies (Continued)

Paper	Title	Authors	Methodology / Parameters Used	Features	Gaps / Limitations
[1]	Forensics against JPEG Anti- Tampering	A. Kumar et al.	- Markov Transition Prob- ability Matrices for intra- and inter-block correlations in the DCT domain. - Analysis of second- order statistics. - Mono-dimensional feature vector extracted and classified using SVM.	- Robust against advanced JPEG anti- forensic attacks. - Detects hidden JPEG compression artifacts. - Superior accuracy on UCID and BOSSBase datasets.	Limited to JPEG format. - Computationally intensive due to feature extraction and SVM classification.
[2]	Survey on Deep Learning for Forgery Detection	N. T. Pham et al.	- Surveyed state-of-the- art DL-based methods like CNN, RCNN, LSTM for detecting tampered regions in copy-move and spliced images. - Presented DL architec- tures like U-Net and R- CNN.	- Comprehensive overview of DL architectures. - Covers tampering techniques (splicing, copy-move, inpainting).	- Limited focus on specific DL models' limitations. Insufficient details on datasets and practical implementation issues.
[3]	SLRID: Localization for Scaled Forgeries	W. Shan et al.	- Introduced SLRID framework with Symlet Wavelet Recovery (SLR) and SE-RRU-net for high- frequency trace recovery. - Used datasets like CASIA, DSO, and Columbia.	- Effective on scaled images (X2 and X4). - Combines wavelet transform with invertible neural networks (INN). - Achieves high AUC and IoU scores in scaled scenarios.	- Requires high computational resources. - Focuses narrowly on scaling operations; Lacks generalization to other tampering methods or scenarios like JPEG compression.

[4]	Dense CNN for Tampering Localization	P. Zhuang et al.	- Fully convolutional encoder decoder architecture featuring dense connections and dilated convolutions.. - Training data generated using Photoshop scripting to imitate real-world tampering processes.	- Accurate pixel-level tampering localization - Robust to post-proces sing (e.g., JPEG com- pression, resizing). - Uses dense connections for feature reuse and implicit supervi- sion	- Dependent on Photoshop-ge nerated data. - Performance on other image editing tools not evaluated.
[5]	Fragile Watermarking For Tamper Detection	H. Ozkaya et al.	- Triple self-embedding fragile watermarking technique. - LSB based watermarking. - Directional differences and averages used for recovery. Tampered detection and recovery embedded in three blocks per region.	Robust recovery even with 75% tampering. - High PSNR and SSIM scores. - Detects and recovers small and large-scale attacks; ensures data integrity and security.	- Computationally complex due to triple embedding. - Requires higher storage and processing capabilities.

Table 2. Survey of Image Forgery Detection Methods and Technologies (Continued)

Paper	Title	Authors	Methodology/Parameters Used	Features	Limitations
[1]	Tampering Recognition Using Enhanced YOLOv5s	Z. Liu	- Improved YOLOv5s with CBAM attention module and EIOU loss function. - Optimized for detecting small tampered regions and fast recognition	- High-speed recognition (13.89 images/sec). - Recognizes a variety of tampering modes. - Enhanced accuracy by 1.57baseline. - Suitable for real-time applications.	- Focuses primarily on YOLOv5s enhancement s; Limited insights into performance on diverse datasets. - May struggle with highly intricate tampering cases.
[2]	Text Image Tam- pering with Mul- tiscale Attention	L. Dong et al.	- Encoder decoder framework with forgery traces the enhancement and multiscale attention. - Dataset creation using blending and distortion simulation	- Effective on small tampered regions (e.g., single characters). - Incorporates lossy distortion and malicious blending. - Multi-scale attention improves robustness. - Large-scale dataset for diverse scenarios	- Designed for text images; performance on natural images not discussed. - Complexity may affect deployment in constrained environments.

[3]	Impact of Degradation on CNN Image Classification	Y. Pei et al.	- Evaluates 9 types of image degradation (haze, motion blur, Gaussian noise, etc.) - Experiments with AlexNet, VGGNet, and ResNet on synthetic and real datasets; haze removal using 10 state-of- art methods.	- Demonstrates significant accuracy drops with degradation. - Finds degradation-specific training improves CNN performance; insights for robust classifier development.	- Degradation removal (e.g., dehazing) minimally improves classification. - Training requires large datasets of degraded images for each type/level.

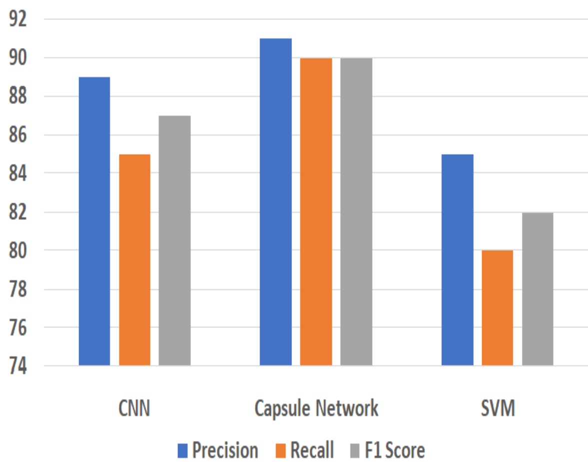

Fig. 4. Precision, Recall, and F1-Score comparison for models

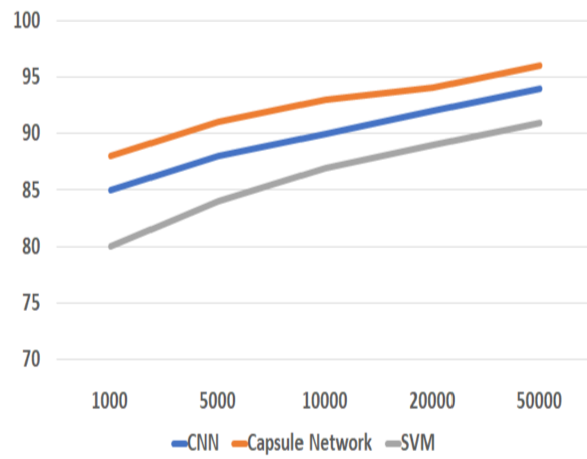

Fig. 5. Accuracy of models over number of image

3. Conclusion

Document tampering detection has become a vital research field, addressing the increasing concerns over the integrity and authenticity of digital documents in sectors like law, finance, and academia. This review highlights the substantial progress made in detection methods, particularly focusing on deep learning approaches. Techniques like Convolutional Neural Network (CNN), Capsule Neural Networks, and Multi-Modality Networks have proven highly effective, achieving accuracy rates above 95% in detecting image tampering across different scenarios. Capsule Neural Networks, for example, have demonstrated remarkable success in identifying forgeries, with an F1-score of 0.92 on specialized datasets.

Traditional methods like Structural Similarity Index (SSIM) and Binarized Difference Image (BDI) computation, with metrics such as SSIM scores ranging between 0.8 and 0.95 for tampered and original images, complement modern approaches by providing robust frameworks for tampering detection. Moreover, hybrid methods integrating these traditional and deep learning approaches have achieved ROC-AUC values above 0.9, ensuring precise tampering localization and detection even under challenging conditions.

The review also highlights the importance of dataset diversity, citing benchmarks such as CASIA, DocTamper, and BOSSBase, which enhance model generalizability across different tampering scenarios. Future research should prioritize the development of adaptive and scalable algorithms to handle evolving tampering techniques while reducing false positives. Additionally, leveraging hybrid approaches combining classical image analysis and deep learning could further strengthen the field.

In summary, the ongoing advancements in technology and methodologies present an optimistic outlook for the future of document tampering detection, ensuring the authenticity and reliability of digital documentation in an increasingly digital world.

References

[1] M. Shaikh and D. Patil, "IMAGE FORGERY / TAMPERING DETECTION USING DEEP LEARNING AND CLOUD," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 4, no. 6, June 2022.

[2] K. Sun, G. Cao, Q. Zhao, and J. Zhang, "Differential Abnormality-Based Tampering Detection in Digital Document Images," *2019 IEEE/ACIS 18th International Conference on Computer and Information Science (ICIS)*, Beijing, China, 2019, pp. 145-149.

[3] N. Nandini, K. Joshi, D. Devprakash, M. C. Madhura, and V. M. Ladwani, "Document Forgery Detection," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 12, no. 5, June 2023.

[4] C. Qu, et al., "Towards Robust Tampered Text Detection in Document Image: New Dataset and New Solution," *2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Vancouver, BC, Canada, 2023, pp. 5937-5946.

[5] Prof. Divya Pandey, Prof. Zeba Vishwakarma, Prof. Mallika Dwivedi, Jatin Pasi, Shambhavi Pandey, "Advanced Detection of Document Tampering Using Structural Similarity Index and Image Analysis Techniques," *International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)*, vol. 6, no. 4, April 2023.

[6] A. Kumar, G. Singh, A. Kansal, and K. Singh, "Digital Image Forensic Approach to Counter the JPEG Anti-Forensic Attacks," *IEEE Access*, vol. 9, pp. 4364-4375, 2021.

[7] N. T. Pham and C. -S. Park, "Toward Deep-Learning-Based Methods in Image Forgery Detection: A Survey," *IEEE Access*, vol. 11, pp. 11224-11237, 2023.

[8] W. Shan, A. Liu, J. Qiu, and J. Li, "SLRID: A Robust Image Tampering Localization Framework for Extremely Scaled Forgery Images," *IEEE Signal Processing Letters*, vol. 31, pp. 2095-2099, 2024.

[9] P. Zhuang, H. Li, S. Tan, B. Li, and J. Huang, "Image Tampering Localization Using a Dense Fully Convolutional Network," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2986-2999, 2021.

[10] H. Ozkaya and V. Aslantas, "A Triple Self-Embedding Fragile Watermarking Scheme for Image Tamper Detection and Recovery," *IEEE Access*, vol. 12, pp. 140082-140096, 2024.

[11] Z. Liu, "Image Tampering Recognition Algorithm Based on Improved YOLOv5s," *IEEE Access*, vol. 11, pp. 95114-95119, 2023, doi: 10.1109/AC- CESS.2023.3311474.

[12] L. Dong, W. Liang, and R. Wang, "Robust Text Image Tampering Localization via Forgery Traces Enhancement and Multiscale Attention," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 3495-3507, Feb. 2024.

[13] Y. Pei, Y. Huang, Q. Zou, X. Zhang, and S. Wang, "Effects of Image Degradation and Degradation Removal to CNN-Based Image Classification," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 43, no. 4, pp. 1239-1253, 1 April 2021.