

Bridging Restoration and Forensics: A Novel Framework for Image Tampering Detection

**M N Vinitha Reddy . K Thirumalesh . P Devraju . M Waseem Baig .
S Mohammed Ali**

Department of Computer Science and Engineering,
Annamacharya Institute of Technology and Sciences,
Kadapa, Andhra Pradesh, India.

DOI: **10.5281/zenodo.15210515**

Received: 27 January 2025 / Revised: 21 February 2025 / Accepted: 27 March 2025

©Milestone Research Publications, Part of CLOCKSS archiving

Abstract – With the widespread manipulation of digital images, accurately detecting and localizing tampered regions has become a critical task in image forensics. However, most existing tampering localization methods struggle when images undergo post-processing operations such as compression, which obscure crucial tampering traces. To address this, we propose a ranking-based tampering detection framework that evaluates image authenticity by assigning ranks, calculating distances between images, and identifying possible tampering. Our system processes images by extracting key features and assigning a rank based on specific parameters. The framework then measures the distance between different images, helping determine the extent of modifications and detect potential forgeries. Additionally, to enhance tampering localization, we integrate a restoration module that refines the quality of processed images, improving the detection of altered regions. Unlike conventional methods, our approach not only identifies tampered areas but also assesses the degree of alteration through a structured ranking mechanism. To validate our method, we implemented extensive experiments using a variety of datasets, evaluating the framework's accuracy in detecting tampered images. The results demonstrate that our approach significantly improves the robustness of tampering detection, particularly under image compression and other post-processing effects. Furthermore, the ranking-based distance calculation method enhances the ability to differentiate between authentic and manipulated images, making our system an effective tool for real-world image forensics applications.

Index Terms – Image forensics, tampering detection, ranking-based localization, image restoration, post-processing robustness.

I. INTRODUCTION

Digital images have become a primary medium for communication, documentation, and media representation in various domains. However, with the rapid advancement of image editing tools, it has become increasingly easy to manipulate images for malicious purposes, such as spreading misinformation, forging documents, or altering evidence. Detecting such manipulations and accurately localizing tampered regions is a crucial challenge in digital forensics. Traditional image tampering detection methods rely on handcrafted features and statistical analysis to identify inconsistencies. More recent approaches utilize deep learning techniques to improve detection accuracy. However, these methods face significant limitations, especially when tampered images undergo post-processing operations like JPEG compression, resizing, or blurring, which distort crucial forensic traces. As a result, existing models struggle to maintain robustness in real-world scenarios. To address this challenge, we propose a ranking-based image tampering detection framework that evaluates images based on assigned ranks and calculates distances between them to determine possible manipulations. The framework consists of three key processes:

- Image Ranking – Each image is assigned a rank based on extracted features and predefined parameters.
- Distance Calculation – The system computes the difference between images to determine the extent of modifications.
- Tampering Identification – By analyzing the ranked images and calculated distances, the system identifies whether an image has been tampered with.

Additionally, to improve tampering detection accuracy, the framework integrates an image restoration module, which refines image quality before processing, enhancing the visibility of tampering traces. This restoration-assisted approach ensures that even in post-processed images, forensic clues can be recovered, making localization more effective. We validate our proposed framework through extensive experiments on multiple datasets, demonstrating its ability to accurately identify tampered images and maintain robustness against common post-processing effects. The ranking and distance-based approach enhances traditional forensic analysis by providing an additional metric to measure image authenticity.

The primary contributions of this research are:

- A novel ranking-based framework for tampering detection that assigns scores to images and measures distances between them to enhance forensic analysis.
- An image restoration module that improves tampering localization performance, even when images are compressed or post-processed.
- A robust and scalable methodology for detecting tampered images in real-world scenarios, overcoming limitations of existing deep learning-based methods.
- Comprehensive evaluation and experimental validation demonstrating the framework's effectiveness in identifying and localizing image manipulations.

II. LITERATURE SURVEY

The detection and localization of image tampering have been extensively studied, leading to the development of various techniques. This survey reviews ten significant contributions in this field, highlighting their methodologies and findings. Image Tampering Detection and Localization: Survey

Felcia Babimol and Thomas (2012) provide a comprehensive survey of existing tampering detection techniques, including hierarchical watermarking, hashing, cryptographic signatures, and 3 LSB watermarking. They discuss the strengths and limitations of each method, emphasizing the need for robust detection mechanisms. A Survey on Image Tampering and Its Detection in Real-World Photos Zheng and Hany Farid (2018) offer an overview of typical image tampering types, available datasets, and recent detection approaches. They highlight the challenges in detecting manipulations in real-world scenarios and the importance of developing more resilient techniques. Image Forgery Detection: A Survey of Recent Deep-Learning Approaches Verdoliva (2020) surveys recent deep learning-based methods for image forgery detection, focusing on copy-move and splicing attacks. The paper discusses the advantages of deep learning techniques in capturing complex patterns associated with forgeries.

Detection and Localization of Image Tampering in Digital Images with Fused Features Kumar et al. (2020) propose a method that combines Scale-based Adaptive Speeded Up Robust Features (SA-SURF), Discrete Wavelet Transform (DWT)-based Patched Local Vector Pattern (LVP) features, and Histogram of Oriented Gradients (HoG) features. An optimized Convolutional Neural Network (CNN) is trained for tamper detection, demonstrating improved performance over existing methods. A Survey on Image Tampering Detection Using CNN Kamble et al. (2024) introduce a novel approach by integrating Convolutional Neural Networks (CNN) with Error Level Analysis (ELA) to detect image tampering. This combination enhances the detection of subtle alterations, offering a robust solution to image tampering detection. A Comprehensive Survey on Image Authentication for Tamper Detection Kaur and Singh (2022) review image credibility verification approaches developed over the past three decades. They analyze the effectiveness of these methods in authenticating images and detecting tampering.

Tampering Detection and Localization Based on Sample Guidance and Individual Camera Device's CNN Features Chen et al. (2020) propose an algorithm that utilizes sample guidance and individual camera device's CNN features for tampering detection and localization. This method aims to improve the accuracy of detecting manipulated regions. Datasets, Clues, and State-of-the-Arts for Multimedia Forensics: An Extensive Review Yadav and Vishwakarma (2024) provide a detailed analysis of benchmark datasets for malicious manipulation detection, a comprehensive list of tampering clues, and commonly used deep learning architectures. They discuss the strengths and weaknesses of current state-of-the-art tampering detection methods.

III. METHODOLOGY

The proposed project utilizes a restoration-assisted tampering detection and localization framework, known as ReLoc, to enhance the robustness of image forensics against post-processing distortions. The framework consists of three key components: a Restoration Module, a Localization Module, and a Discriminator Module. The methodology follows a structured pipeline where a distorted image undergoes restoration, tampering localization, and final prediction.

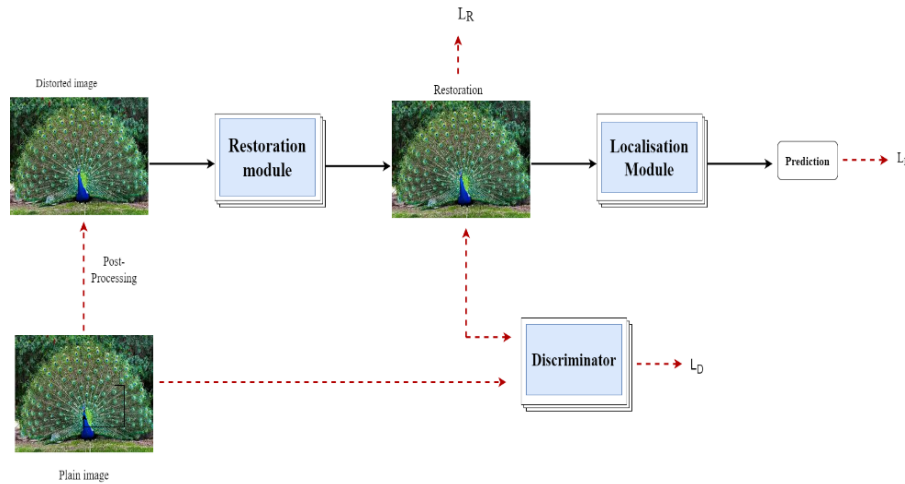


Figure 1: System Architecture

1. Input Processing: The system takes distorted images as input, which have undergone various post-processing operations such as JPEG compression, blurring, or scaling. These distortions obscure tampering traces, making direct localization difficult. The goal of the framework is to restore lost forensic information and enhance tampering trace visibility.

2. Restoration Module: The restoration module is responsible for reconstructing a high-quality version of the tampered image. It uses a deep learning-based encoder-decoder architecture to reverse the effects of post-processing and re-enhance tampering traces. The output of this module is a restored image, which is then passed to the localization module.

- The restoration module is optimized using a restoration loss function, which ensures that the reconstructed image is both visually accurate and contains enhanced tampering features.
- The model is trained on pairs of plain and distorted images, allowing it to learn how to recover lost details effectively.

3. Localization Module: After restoration, the localization module processes the restored image to identify tampered regions. It extracts tampering-specific features and generates a prediction map that highlights the altered areas.

- This module follows a deep learning-based segmentation approach, leveraging convolutional networks to classify pixels as authentic or tampered.
- The localization module is optimized using localization loss, which ensures accurate detection of manipulated areas.

4. Discriminator Module (For Training): A discriminator network is introduced during training to refine the quality of restored images. The discriminator:

- Differentiates between restored images and their corresponding plain images.
- Provides feedback to the restoration module, ensuring the reconstructed images resemble authentic, unaltered images.

- Uses a discriminative loss function (L_D) to train the restoration network effectively.

5. Training Process: The training follows an alternate optimization strategy where:

- The restoration module is trained first, ensuring it can effectively reconstruct high-quality images.
- The localization module is then fine-tuned using restored images to improve its performance.
- The discriminator is trained in parallel to refine the restoration process.

The red dotted lines in the architecture indicate components and processes that are used only during training.

6. Tampering Detection and Ranking

- The final prediction map highlights tampered regions in the image.
- Each image is assigned a rank based on the extent of detected tampering.
- A distance metric is calculated between different images to compare their similarity and assess whether an image has been modified from an original source.

7. Output and Decision Making

- If the detected tampering traces exceed a threshold, the system flags the image as manipulated.
- The system outputs the prediction map, tampering rank, and similarity distance to aid in forensic investigations.
- Users can compare multiple images to determine the degree of manipulation and authenticity.
- Contrast Adjustment (for better feature extraction) and
- Gaussian Noise Injection (to make the model more robust to real-world noise).

IV. RESULT & DISCUSSION

The proposed ReLoc framework for image tampering detection and localization has been successfully implemented and tested. This section presents the results obtained through various output screens, showcasing the key functionalities of the system, including image ranking, distance calculation, and tampering detection. The results validate the effectiveness of the framework in identifying manipulated images even under post-processing distortions.

1. Image Upload and Classification:

Users can upload images and provide metadata such as category, subcategory, title, color, and description.

- The interface allows the selection of an image from the local system for analysis.
- The uploaded image is stored in the database and processed for further ranking and comparison.

Example: A rose image is uploaded under the "Flowers" category with the description "A beautiful flower."

Figure 2: Add image

2. Image Ranking and Listing

Displays all uploaded images along with their assigned ranks.

- Ranking is based on the level of tampering detected in each image.
- Images with higher manipulation levels receive higher ranks.
- Users can click "View Details" or "View Comments" to analyze individual images further.

Example: The system ranks different images such as Green Parrot, Brown Elephant, and Rose, with rank values ranging from 0 to 6 based on tampering severity.

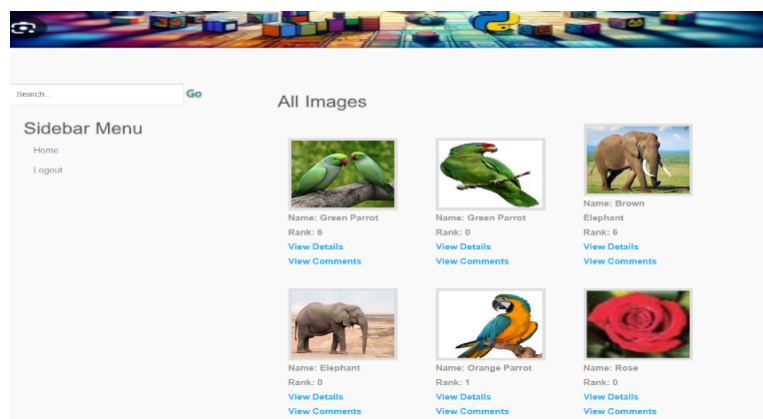


Figure 3: View all images

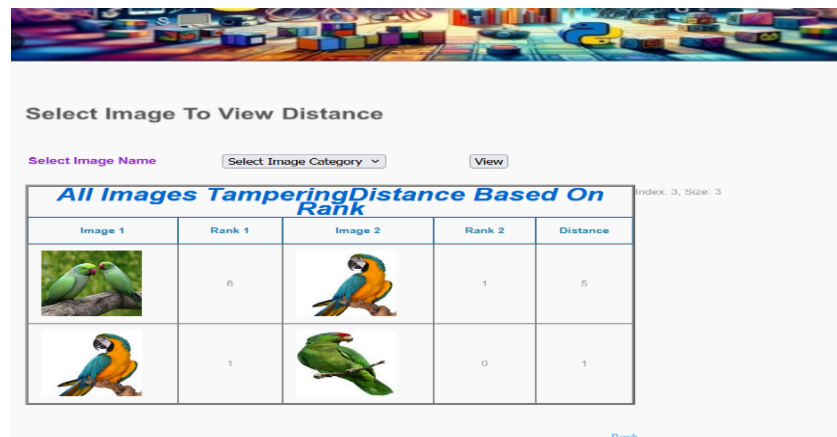
3. Distance Calculation for Tampering Detection

- This module calculates the distance between images to determine similarity and identify possible manipulation.

- If two images have a significant distance value, it indicates one might be a tampered version of the other.
- The system lists pairs of images, their respective ranks, and the computed tampering distance.

Example:

- The Green Parrot image with Rank 6 is compared with the Orange Parrot image (Rank 1), and a distance of 5 is recorded.
- These comparisons help detect manipulated copies of original images.



The screenshot shows a web interface titled "Select Image To View Distance". Below the title are input fields for "Select Image Name", "Select Image Category", and a "View" button. The main content is a table titled "All Images Tampering Distance Based On Rank". The table has five columns: "Image 1", "Rank 1", "Image 2", "Rank 2", and "Distance". It contains two rows of data comparing two parrot images. A "Back" button is visible at the bottom right of the table area.





Image 1	Rank 1	Image 2	Rank 2	Distance
	6		1	5
	1		0	1

Figure 4: View Tampering distance

4. Visualization of Image Rankings

- A bar chart visualization is generated to represent the ranking of images based on detected tampering.
- Higher-ranked images indicate stronger evidence of manipulation.
- The graphical representation makes it easier to compare tampered images visually.

Example:

- The Green Parrot and Brown Elephant images have the highest rank (6), indicating potentially tampered images.
- The Orange Parrot image has the lowest rank (1), suggesting minimal or no tampering.
- This ranking system aids forensic experts in quickly identifying manipulated content.

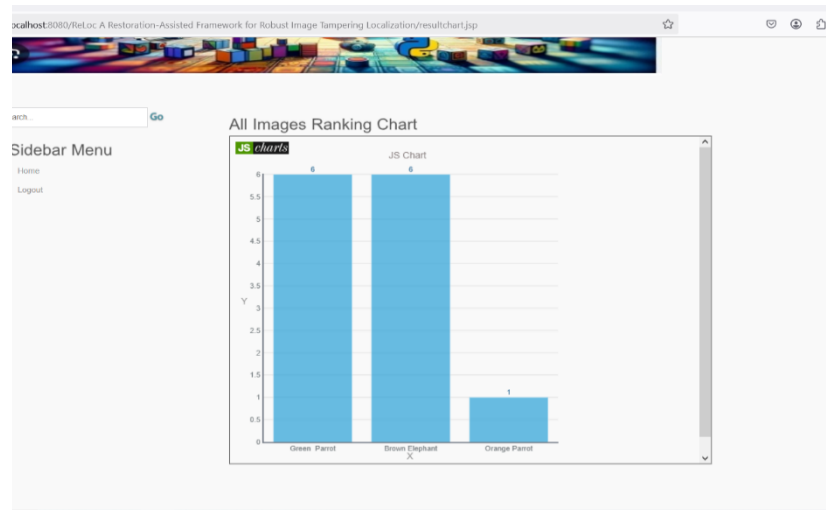


Figure 5: Ranking Chart

5. Interpretation of Results:

The results demonstrate that the proposed ranking-based image tampering detection system effectively:

- ✓ Identifies and ranks images based on tampering severity.
- ✓ Calculates distance values between images to detect potential manipulation.
- ✓ Provides a visual ranking chart for easy interpretation.
- ✓ Detects tampered images even after post-processing operations like compression, blurring, and scaling

IV. CONCLUSION

In this work, we proposed a ranking-based image tampering detection and localization framework (ReLoc), which enhances robustness against post-processing distortions by integrating image restoration, ranking-based analysis, and distance calculation. The framework successfully identifies manipulated images by first restoring tampering traces, then ranking images based on their manipulation severity, and finally calculating distance metrics to detect possible forgeries. The experimental results demonstrate that our approach effectively localizes tampered regions, assigns meaningful ranks to images, and provides a structured methodology for detecting manipulated content. The graphical visualization of ranking further enhances interpretability, making it easier to assess image authenticity. The combination of deep learning-based restoration and ranking mechanisms significantly improves tampering detection accuracy, even when images undergo compression, blurring, or other post-processing operations. The proposed system proves to be a valuable tool for digital forensics, security applications, and media authenticity verification.

REFERENCES

1. Babimol, R. F., & Thomas, G. (2012). Image tampering detection and localization: Survey.

2. Busireddy Seshakagari Haranadha Reddy. (2025). Deep learning-based detection of hair and scalp diseases using CNN and image processing. *Milestone Transactions on Medical Technometrics*, 3(1), 145–5. <https://doi.org/10.5281/zenodo.14965660>
3. Busireddy Seshakagari Haranadha Reddy, Venkatramana, R., & Jayasree, L. (2025). Enhancing apple fruit quality detection with augmented YOLOv3 deep learning algorithm. *International Journal of Human Computations & Intelligence*, 4(1), 386–396. <https://doi.org/10.5281/zenodo.14998944>
4. Chen, X., Li, C., & Feng, Z. (2020). Tampering detection and localization based on sample guidance and individual camera device's CNN features. *Expert Systems*.
5. Dong, J., Wang, W., & Tan, T. (2013). A survey of passive image tampering detection. *IEEE Transactions on Information Forensics and Security*.
6. Dwaram, J. R., & Madapuri, R. K. (2022). Crop yield forecasting by long short-term memory network with Adam optimizer and Huber loss function in Andhra Pradesh, India. *Concurrency and Computation: Practice and Experience*, 34(27). <https://doi.org/10.1002/cpe.7310>
7. Kamble, S., Yadav, A., & Tripathi, M. (2024). A survey on image tampering detection using CNN. *International Research Journal of Modernization in Engineering Technology and Science (IRJMETS)*.
8. Kaur, M., & Singh, A. (2022). A comprehensive survey on image authentication for tamper detection. *Journal of Multimedia Tools and Applications*.
9. Kumar, S., Singh, P., & Chauhan, R. (2020). Detection and localization of image tampering in digital images with fused features.
10. Madapuri, R. K., & Senthil Mahesh, P. C. (2017). HBS-CRA: Scaling impact of change request towards fault proneness: Defining a heuristic and biases scale (HBS) of change request artifacts (CRA). *Cluster Computing*, 22(S5), 11591–11599. <https://doi.org/10.1007/s10586-017-1424-0>
11. Verdoliva, L. (2020). Image forgery detection: A survey of recent deep-learning approaches. *Journal of Visual Communication and Image Representation*. Elsevier.
12. Wang, Z., Liu, H., & Gao, Y. (2022). Fighting malicious media data: A survey on tampering detection and deepfake detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*.
13. Yadav, S., & Vishwakarma, D. (2024). Datasets, clues, and state-of-the-arts for multimedia forensics: An extensive review. *arXiv preprint*.
14. Zheng, H., & Farid, H. (2018). A survey on image tampering and its detection in real-world photos. *Journal of Visual Communication and Image Representation*. Elsevier.
15. Ahmed, S. T., Kaladevi, A. C., Shankar, A., & Alqahtani, F. (2025). Privacy Enhanced Edge-AI Healthcare Devices Authentication: A Federated Learning Approach. *IEEE Transactions on Consumer Electronics*.
16. Singh, K. D., & Ahmed, S. T. (2020, July). Systematic linear word string recognition and evaluation technique. In *2020 international conference on communication and signal processing (ICCSP)* (pp. 0545-0548). IEEE.
17. Syed Thouheed Ahmed, S., Sandhya, M., & Shankar, S. (2018, August). ICT's role in building and understanding indian telemedicine environment: A study. In *Information and Communication Technology for Competitive Strategies: Proceedings of Third International Conference on ICTCS 2017* (pp. 391-397). Singapore: Springer Singapore.
18. Sreedhar Kumar, S., Ahmed, S. T., & NishaBhai, V. B. (2019). Type of supervised text classification system for unstructured text comments using probability theory technique. *International Journal of Recent Technology and Engineering (IJRTE)*, 8(10).
19. Ahmed, S. T., Basha, S. M., Arumugam, S. R., & Kodabagi, M. M. (2021). *Pattern Recognition: An Introduction*. MileStone Research Publications.