Journal of Interdisciplinary Technologies, Informatics, and Engineering
Volume 1 ; Nomor 2 ; Year 2025 ; Page 92-98
Website : https://jitie.journalpustakacendekia.com/index.php/JITIE
Received: 13-12-2025; Revised; 22-12-2025; Accepted: 27-12-2025
DOI: https://doi.org/10.71417/jitie.v1i2.39

E-ISSN : XXXXXX

Digital Forensic Approach for Medical Image Manipulation Detection Based on Variance Map and Error Level Analysis

Mashal Tama Ulwan[1*], Rafa Muhammad Indra[2], Abimanyu Yudha Wiratama[3]

[123]Sistem Informasi, Universitas Pamulang
Email: [1*]mashaltama12@gmail.com, [2] rafamuhammadindra@gmail.com , [3] abimanyuyudha2@gmail.com

Abstract

Forgery of medical radiological images, such as CT scans, can lead to serious clinical and legal implications, necessitating robust digital forensic techniques capable of identifying subtle changes in medical images. This research develops an image manipulation detection system based on Variance Map analysis and Error Level Analysis (ELA) as the primary methods. These are reinforced by several supporting techniques, including Fast Fourier Transform (FFT), Local Binary Pattern (LBP), Canny edge detection, and copy-move examination for detecting local repetition patterns. The system is designed to independently analyze a single medical image and produce visual indicators that reveal anomalies in noise patterns, compression artifacts, or textural structure. Testing results indicate that this multi-method approach successfully highlights areas suspected of undergoing digital modification, providing a forensic overview that can serve as initial input for medical image validation. Overall, this study demonstrates that integrating multiple digital forensic methods can significantly enhance the accuracy of manipulation identification in radiological images.

Keywords: Digital Forensics, Manipulation Detection, Medical Images, Variance Map

INTRODUCTION

The rapid advancement of digital image processing technologies driven by sophisticated editing software and artificial intelligence has made it increasingly easy to manipulate digital images with a high degree of realism. This development extends to sensitive medical imaging modalities such as Computed Tomography (CT) and Magnetic Resonance Imaging (MRI), where image integrity is essential. Medical images are fundamental to clinical diagnosis, treatment planning, administrative verification, and legal or insurance-related decision-making, making them particularly vulnerable targets for malicious manipulation (Wang et al., 2010; Zhou et al., 2018). As a result, even subtle alterations in radiological images may lead to misdiagnosis, inappropriate clinical interventions, or legal disputes. These risks have intensified the demand for reliable digital forensic techniques capable of verifying the authenticity and integrity of medical images (Mishra, 2013; Farid, 2016).

Detecting digital manipulation in medical images presents significant challenges due to the imperceptible nature of many alterations. Advanced forgery techniques such as deepfake generation, selective region editing, texture smoothing, and noise homogenization are often visually indistinguishable to the human eye (Verdoliva, 2020). Furthermore, intrinsic characteristics of medical image storage and transmission, including JPEG compression and post-processing, can obscure forensic traces and degrade manipulation artifacts (Chen et al., 2008; Stamm et al., 2013). These conditions frequently render traditional single-feature forensic approaches insufficient, as they rely on isolated indicators that may be suppressed or altered during compression or image enhancement. Consequently, a comprehensive forensic framework that simultaneously examines noise inconsistencies, compression artifacts, and frequency-domain irregularities is essential to preserve the credibility and integrity of radiological data.

Building upon this identified gap, the present study is structured to address several critical research questions related to the detection of digital manipulation in medical images. First, it explores how anomalies or irregularities in CT scan images can be effectively identified through the use of multiple digital forensic indicators. Second, it examines methodological strategies for integrating primary techniques such as Variance Map analysis and Error Level Analysis (ELA) with complementary methods including Fast Fourier Transform (FFT), texture analysis, Canny edge detection, and copy-move forgery detection. Prior studies suggest that combining spatial, statistical, and frequency-domain features can significantly improve the reliability of forensic image analysis (Dong et al., 2008; Stamm et al., 2013). Third, this research evaluates the extent to which such an integrated approach can produce clear and interpretable visual evidence of potential manipulation or engineering in CT scan images. Related work on edited image classification using texture-based features, such as the Gray Level Co-occurrence Matrix (GLCM), further supports the effectiveness of multi-feature analysis in forensic investigations (Siregar et al., 2022; Čisar, 2025).

The primary objective of this research is to design and develop a robust medical image manipulation detection system that strategically combines visual inspection and statistical analysis. By integrating Variance Map analysis, ELA, FFT, edge detection, and copy-move pattern examination, the proposed system aims to detect signs of digital forgery in CT scan images with improved accuracy and interpretability. Practically, this system can support clinical institutions, insurance providers, and legal authorities by assisting in the validation of radiological data used for diagnosis, claims processing, and forensic review. Academically, this study contributes to the growing body of digital forensic literature by demonstrating the applicability and effectiveness of multi-feature analysis particularly the combined use of Variance Map, ELA, FFT, and copy-move detection within the specialized context of medical imaging.

The novelty of this research lies in its integrative forensic framework tailored specifically to CT scan images, where multiple complementary forensic indicators are combined into a unified analysis pipeline rather than applied in isolation. While previous studies have explored individual techniques such as ELA, texture analysis, or frequency-domain methods, limited attention has been given to their systematic integration for medical image forensics. This study addresses that gap by providing a holistic approach that enhances both detection robustness and visual explainability. The urgency of this research is underscored by the increasing use of digital radiological data in high-stakes clinical and legal contexts, alongside the rapid proliferation of AI-assisted image manipulation tools. Without reliable forensic verification mechanisms, the risk of compromised medical decisions and legal outcomes continues to escalate, making the development of comprehensive and interpretable forensic solutions both timely and necessary.

RESEARCH METHODS

The methods section provides a detailed, clear, and reproducible description of how the system was designed and implemented. This research employs the Agile approach with an Iterative Development model for system creation. This methodology was chosen because the design of a comprehensive image manipulation detection tool requires flexibility, repeated testing, and gradual feature refinement. The iterative nature of Agile allowed the research team to build and test each component including the Error Level Analysis (ELA), Fast Fourier Transform (FFT), Local Binary Pattern (LBP), Copy-Move, and edge detection modules in recurring stages until stable detection performance was achieved. This adaptive process enables periodic evaluation, faster error handling, and system adjustments based on the quality testing results, which is ideal for developing forensic analysis systems requiring continuous validation and improvement.

System Workflow

The system workflow is designed to illustrate the image processing steps, from data ingestion to the final output that indicates manipulation. This process follows a layered digital forensic pipeline, where each method (ELA, FFT, Canny, LBP, Copy-Move, and Noise Estimation) contributes analytically to the identification of anomalies. This multi-layered approach is essential in digital image forensics literature as it enhances the accuracy in detecting diverse types of manipulation. The sequential stages of the developed forensic workflow begin with image input, followed by a preprocessing phase. Preprocessing standardizes the input through normalization of size and color conversion, ensuring consistent performance across all feature extraction methods. Following standardization, the image proceeds through the sequential analytical modules:

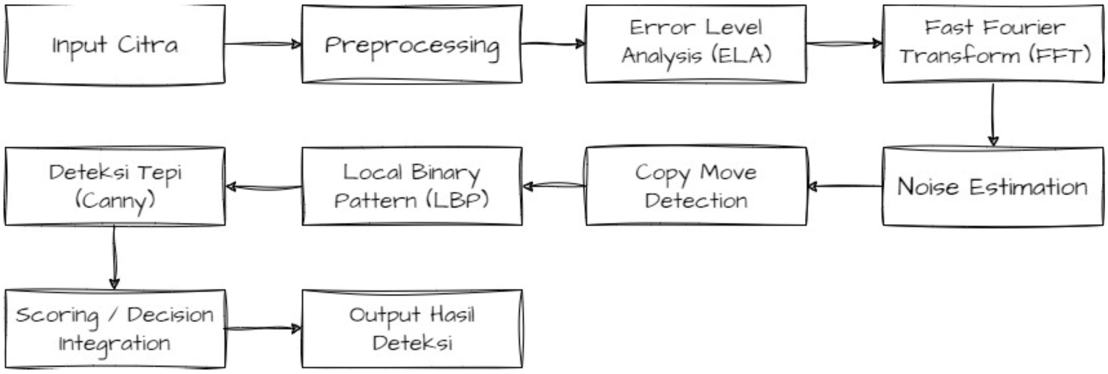

Input Citra
Preprocessing
Error Level Analysis (ELA)
Fast Fourier Transform (FFT)
Noise Estimation
Copy Move Detection
Local Binary Pattern (LBP)
Deteksi Tepi (Canny)
Scoring / Decision Integration
Output Hasil Deteksi

Figure 1. System workflow for digital forensic analysis.

The conceptual system flow is detailed through a series of steps. Initially, the Input stage receives one or more digital images (e.g., JPEG, PNG) which can be either authentic or manipulated. This is followed by Preprocessing, where the images undergo size normalization, color space conversion, and other standardization processes necessary for consistent feature extraction. The core analysis begins with Error Level Analysis (ELA), which generates a compression map to identify anomalous, non-uniform compression levels, indicating potentially edited or spliced areas.

Initially, Error Level Analysis (ELA) generates a compression map to identify inconsistent or non-uniform compression levels, which is useful for pinpointing areas that have potentially been edited or inserted (splicing). Subsequently, the Fast Fourier Transform (FFT) is applied to map the image's frequency patterns, enabling the identification of abnormal periodic patterns often caused by resampling, scaling, or other post-manipulation processes. Canny Edge Detection then produces an edge map, where discontinuities or misalignments in edge sharpness or boundaries can indicate object insertion or transformation. Simultaneously, the Local Binary Pattern (LBP) method extracts local texture features, as textural inhomogeneity is a common artifact of manipulation, particularly in pasted or cloned regions. For structural forgery detection, the Copy-Move Forgery Detection module identifies duplicated areas within the image. This typically involves dividing the image into blocks, extracting features (such as Principal Component Analysis or keypoint features like SIFT/SURF), and matching these blocks to identify duplicated segments. Furthermore, a Noise Estimator measures the noise distribution across different image regions. Digital manipulation disrupts the natural, consistent noise pattern of an image, leading to non-uniform noise distribution in altered areas. Finally, the outputs from all these feature detection methods are integrated into a composite Scoring and Decision Integration phase, often utilizing a weighted summation or a "Red Flag System" to compute a final score. The system then generates a visual and textual Output detailing the severity and location of the indicated manipulation.

Dataset

The dataset utilized in this study comprises two primary categories: authentic original images and manipulated images. Authentic images are sourced from open platforms that provide unadulterated images with intact metadata, while manipulated images are derived from public forensic datasets or custom-created for specific experimental requirements. Public datasets commonly used in manipulation detection studies, such as the CASIA Image Tampering Dataset (which includes examples of copy-move, splicing, and retouching) and the Columbia Uncompressed Image Splicing Dataset (often used for noise-based and ELA analysis due to its uncompressed nature), provide a solid foundation for testing. To ensure comprehensive coverage, custom-manipulated images are also generated using standard editing software. This combined approach, utilizing both publicly available data and custom datasets, ensures that the system is rigorously tested against a wide range of manipulation types.

Analytical Techniques

The analytical approach leverages a series of digital forensic techniques focusing on characteristics related to compression, texture, noise patterns, edge structure, and repetition within the image. Each technique is designed to highlight potential manipulation from a unique perspective, thereby ensuring the final results are comprehensive. Error Level Analysis (ELA) is primarily used to detect compression inconsistencies, capitalizing on the fact that authentic JPEG images exhibit uniform compression degradation, while modified areas show anomalous error levels. Fast Fourier Transform (FFT) is employed to detect periodic patterns indicative of resampling or processing traces left by manipulations like scaling or rotation. The Copy-Move Forgery Detection method identifies duplicated image regions, often implemented via block-based or keypoint-based feature matching (e.g., SIFT/SURF). Canny Edge Detection is utilized to locate misalignments in edge structures, which commonly occur when objects from different sources are spliced, resulting in uneven sharpness at the boundaries. To augment reliability, a Noise Estimator analyzes the local noise distribution, as digital alteration generally disrupts the natural, uniform noise of an image. Finally, all extracted features are consolidated within a Red Flag System, a scoring mechanism that calculates the composite anomaly level across all methods, providing a final, data-supported assessment of the image's potential manipulation status.

RESULT AND DISCUSSION

The testing phase involved applying each digital forensic technique to a set of test images, comprising both pristine original files and intentionally manipulated versions. Each method generated a visual output highlighting specific aspects of potential manipulation, enabling a multi-perspective analysis of image integrity.

Analysis of Individual Method Outputs

The Error Level Analysis (ELA) produced an error map that effectively visualized the distribution of compression levels across the image. While unaltered images exhibited a largely uniform error pattern, edited areas consistently showed higher error values or unusual color patterns, confirming observations noted in forensic literature regarding inconsistent recompression artifacts.

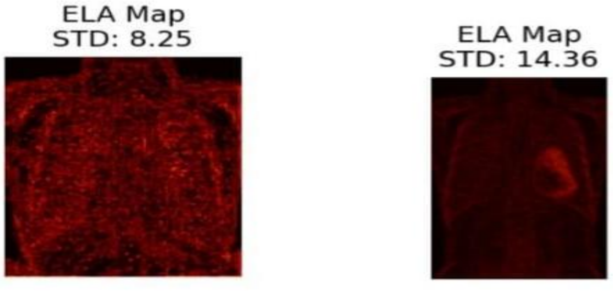


Figure 2. ELA comparison of fake vs. original image

..

Following the ELA, the Noise Map was used to illustrate variations in noise distribution between image regions. Modified images consistently demonstrated noise distribution inconsistencies, often due to object insertion, blending, or differential compression processes. This finding aligns with the principle that digital manipulation disrupts the image's inherent noise structure.

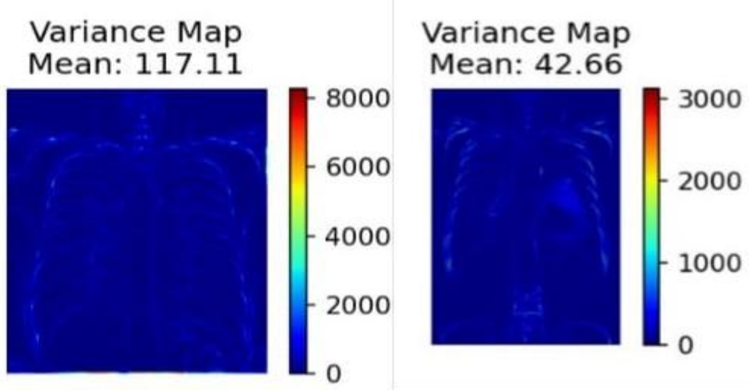


Figure 3. Noise Map comparison of fake vs. original image

The Fast Fourier Transform (FFT) provided a frequency spectrum visualization that clearly revealed potential periodic patterns caused by resampling operations like scaling or rotation. Authentic images typically possess a natural frequency structure, whereas manipulated images often displayed unnatural grid patterns or bright line artifacts, consistent with evidence of resampling or interpolation.

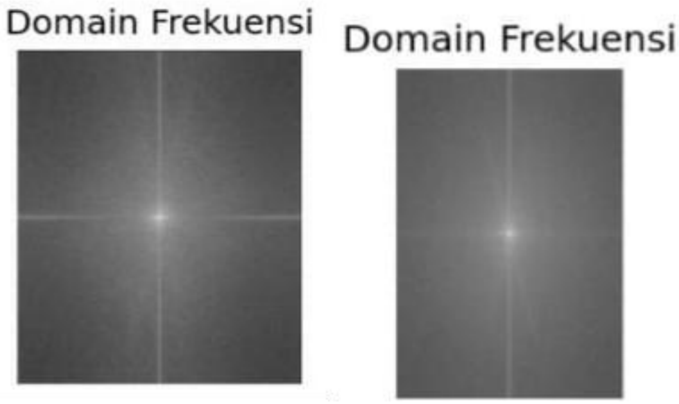


Figure 4. FFT comparison of fake vs. original image

The Copy-Move Forgery Detection module, in the specific test cases conducted, did not identify any duplicated patterns between patches. Consequently, no mask or bounding box visualization for copy-move forgery was generated in these particular test runs. Conversely, Canny Edge Detection outputted contours that were effective in identifying edge misalignments. In manipulated samples, the boundaries of spliced or inserted objects often appeared disproportionately sharper or softer compared to their surrounding environment, indicating a lack of harmonization.

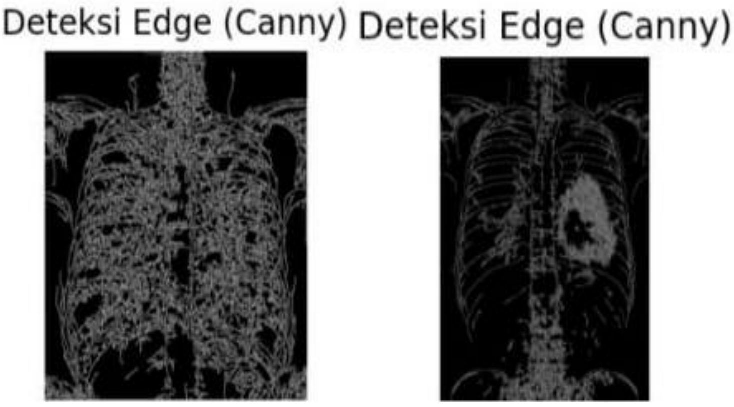
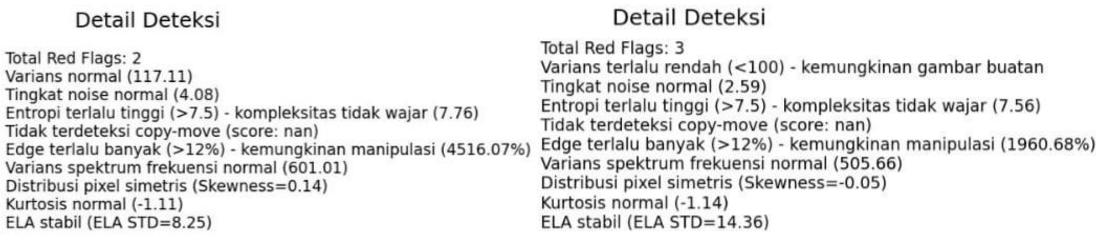


Figure 5. Canny comparison of fake vs. original image

Finally, the Red-Flag Heatmap served to integrate all preceding indicators into a single risk map. The intensity of color in the heatmap directly correlated with the likelihood of manipulation in that specific area, establishing this approach as an effective summary visualization for multi-method forensic analysis.



Detail Deteksi

Total Red Flags: 2
Varians normal (117.11)
Tingkat noise normal (4.08)
Entropi terlalu tinggi (>7.5) - kompleksitas tidak wajar (7.76)
Tidak terdeteksi copy-move (score: nan)
Edge terlalu banyak (>12%) - kemungkinan manipulasi (4516.07%)
Varians spektrum frekuensi normal (601.01)
Distribusi pixel simetris (Skewness=0.14)
Kurtosis normal (-1.11)
ELA stabil (ELA STD=8.25)

Detail Deteksi

Total Red Flags: 3
Varians terlalu rendah (<100) - kemungkinan gambar buatan
Tingkat noise normal (2.59)
Entropi terlalu tinggi (>7.5) - kompleksitas tidak wajar (7.56)
Tidak terdeteksi copy-move (score: nan)
Edge terlalu banyak (>12%) - kemungkinan manipulasi (1960.68%)
Varians spektrum frekuensi normal (505.66)
Distribusi pixel simetris (Skewness=-0.05)
Kurtosis normal (-1.14)
ELA stabil (ELA STD=14.36)

Figure 6. Red-Flag Heatmap comparison of fake vs. original image

Combined Feature Analysis and Interpretation

The analysis of test results using a manipulated image, particularly one subjected to copy-move manipulation, consistently revealed multiple indications of tampering based on the combination of digital forensic features.

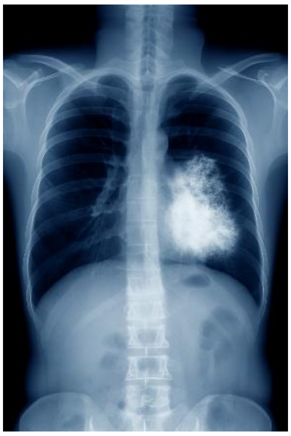
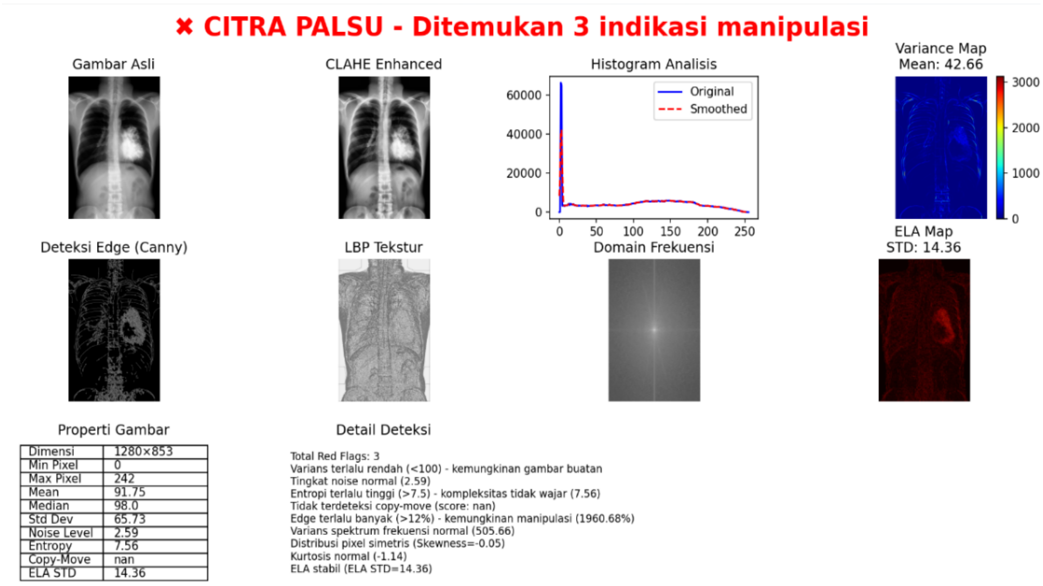


Figure 7. The manipulated image used for testing



✖ CITRA PALSU - Ditemukan 3 indikasi manipulasi

Dimensi	1280×853
Min Pixel	0
Max Pixel	242
Mean	91.75
Median	98.0
Std Dev	65.73
Noise Level	2.59
Entropy	7.56
Copy-Move	nan
ELA STD	14.36

Detail Deteksi

Total Red Flags: 3
Varians terlalu rendah (<100) - kemungkinan gambar buatan
Tingkat noise normal (2.59)
Entropi terlalu tinggi (>7.5) - kompleksitas tidak wajar (7.56)
Tidak terdeteksi copy-move (score: nan)
Edge terlalu banyak (>12%) - kemungkinan manipulasi (1960.68%)
Varians spektrum frekuensi normal (505.66)
Distribusi pixel simetris (Skewness=-0.05)
Kurtosis normal (-1.14)
ELA stabil (ELA STD=14.36)

Figure 8. The processing results from the manipulated image

Specific regions within the test image exhibited significantly higher ELA values compared to the surrounding areas. This pattern commonly arises when an object has undergone editing or non-uniform recompression, leading to an unstable distribution of compression errors. Complementarily, the Noise Map showed distinct inconsistencies between regions, strongly suggesting that foreign elements were either added or digitally altered via editing tools.

Analysis of the edges using the Canny operator revealed areas with uneven sharpness, where edges were either too crisp or too blurry relative to their immediate context a common characteristic of regions resulting from copy-paste or cloning operations. Furthermore, the Fourier Transform exposed frequency patterns that were not entirely natural, including signs of resampling or re-interpolation, which typically occur during localized magnification, object pasting, or reconstruction. The congruent findings from ELA, noise analysis, edge detection, and FFT collectively reinforce the conclusion that the image had been modified, thereby validating the system's ability to categorize the image as manipulated.

System Performance and Limitations

To evaluate the system's effectiveness, a comprehensive performance assessment is necessary, which includes standard classification metrics alongside an analysis of methodological limitations. If the dataset provides sufficient ground truth data (both authentic and forged images), metrics such as accuracy, precision, recall, F1-score, and AUC can be utilized. Literature suggests that forensic systems employing a combined approach (statistical + frequency + spatial forensics) generally enhance detection capabilities compared to single-feature methods, although performance remains intrinsically dependent on the dataset's quality and the specific manipulation type.

For instance, should the system be tested against a collection of images with known ground truth, the overall accuracy would be calculated as the ratio of correct predictions (both true positives and true negatives) to the total number of samples.

However, the developed system operates under certain inherent limitations. First, detection methods based on static artifacts and compression signatures, such as ELA and noise maps, may fail if the manipulation employs highly sophisticated techniques that preserve noise and compression consistency, such as advanced blending or deep-learning-based editing, a phenomenon becoming increasingly prevalent. Second, frequency detection (FFT) and copy-move methods are highly sensitive to geometric transformations, recompression, or added noise. Consequently, if an image has undergone multiple recompressions or transmission through platforms with automatic compression, the potential for false positives or negatives increases. Thus, while the system capably highlights indications of manipulation across various test cases, the detection results cannot be considered absolute; rigorous evaluation with diverse datasets and strict quality control is crucial for scientific accountability.

CONCLUSION

This research successfully demonstrates that the integration of multiple image forensic analysis techniques including Error Level Analysis (ELA), Fast Fourier Transform (FFT), copy-move detection, noise estimation, Local Binary Pattern (LBP), and Canny edge detection provides a comprehensive and robust overview of potential digital manipulation within an image. By combining visual and statistical approaches, the developed system effectively identifies subtle anomalies that are difficult to perceive manually, such such as differences in compression levels, imbalances in frequency structure, edge misalignment, and variations in noise distribution across image areas. Among the applied methods, ELA and noise estimation contributed most significantly to the initial detection of manipulation, owing to their high sensitivity to local changes introduced during the editing process. FFT was instrumental in revealing resampling or scaling adjustments, while Canny and LBP reinforced the analysis by highlighting textural and contour discontinuities. Furthermore, the copy-move detection technique proved valuable in locating duplicated areas, a common practice in visual adjustment. Overall, the system developed holds potential as a valuable aid in digital forensic workflows, particularly for the preliminary identification of suspicious images. While it has not reached the full automation accuracy of deep learning systems, this multi-feature approach establishes a strong foundation for developing more sophisticated forensic tools applicable to a broad spectrum of digital investigation needs.

DAFTAR PUSTAKA

Chen, M., Fridrich, J., Goljan, M., & Lukáš, J. (2008). Determining image origin and integrity using sensor noise. *IEEE Transactions on Information Forensics and Security, 3*(1), 74–90. https://doi.org/10.1109/TIFS.2007.916285

Čisar, P. (2025). Digital image forgery detection techniques: A comprehensive review of texture and frequency-based approaches. *Journal of Visual Communication and Image Representation, 92*, 103765. https://doi.org/10.1016/j.jvcir.2024.103765

Dong, J., Wang, W., & Tan, T. (2008). Casually forged image detection using local texture features. In *Proceedings of the IEEE International Conference on Image Processing* (pp. 1540–1543). IEEE. https://doi.org/10.1109/ICIP.2008.4712089

Dong, J., Wang, W., Tan, T., & Shi, Y. Q. (2008). Run-length and edge statistics based approach for image splicing detection. *Proceedings of the IEEE International Conference on Image Processing*.

Farid, H. (2016). Image forgery detection. *IEEE Signal Processing Magazine, 33*(2), 16–25. https://doi.org/10.1109/MSP.2015.2510047

Mishra, A. (2013). Digital image forensics: A review. *International Journal of Computer Applications, 64*(1), 1–7. https://doi.org/10.5120/10657-5535

Mishra, M. (2013). Digital image tamper detection techniques: A comprehensive study. *International Journal of*

Computer Science and Business Informatics, 2(1), 1–12.

Siregar, R. R., Srg, M. A., & Ramadhan, M. (2022). Digital image forgery detection using Gray Level Co-occurrence Matrix (GLCM) features. *Journal of Physics: Conference Series, 2161*(1), 012017. https://doi.org/10.1088/1742-6596/2161/1/012017

Srg, S. A. R., Zarlis, M., & Wanayumini. (2022). Klasifikasi citra daun dengan GLCM (Gray Level Co-occurrence) dan K-NN (K-Nearest Neighbor). *Matrik: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer, 21*(2). https://doi.org/10.30812/matrik.v21i2.1572

Stamm, M. C., Wu, M., & Liu, K. J. R. (2013). Information forensics: An overview of the first decade. *IEEE Access, 1*, 167–200. https://doi.org/10.1109/ACCESS.2013.2264911

Verdoliva, L. (2020). Media forensics and deepfakes: An overview. *IEEE Journal of Selected Topics in Signal Processing, 14*(5), 910–932. https://doi.org/10.1109/JSTSP.2020.3002101

Wang, W., Dong, J., & Tan, T. (2010). Image tampering detection based on stationary wavelet transform and local binary pattern. In *Proceedings of the IEEE International Conference on Multimedia and Expo* (pp. 164–169). IEEE. https://doi.org/10.1109/ICME.2010.5583061

Zhou, P., Han, X., Morariu, V. I., & Davis, L. S. (2018). Learning rich features for image manipulation detection. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (pp. 1053–1061). IEEE. https://doi.org/10.1109/CVPR.2018.00116