talenta PUBLISHER

Journal of Research in Mathematics Trends and Technology

Journal homepage: https://talenta.usu.ac.id/jormtt

Copula-Based Blind Detection of Copy-Move Image Forgery: A Robust Mutual Information Approach

Tulus Joseph Marpaung[*1], Tulus [2], Fivi Rahmatus Sofiyah[3]

[1] *Programs of Statistics, Faculty of Vocational, Universitas Sumatera Utara, Medan, Indonesia*

[2] *Programs of Mathematics, Faculty of Mathematics and Natural Science, Universitas Sumatera Utara, Medan, Indonesia*

[3] *Programs of Management, Faculty of Vocational, Universitas Sumatera Utara, Medan, Indonesia*

[*]Corresponding Author: tj.marpaung@usu.ac.id

ARTICLE INFO

Article history:
Received: 12 December 2024
Revised: 15 January 2025
Accepted: 20 March 2025
Available online: 31 March 2025

E-ISSN: 2656-1514
P-ISSN:

ow to cite:
Marpaung, T.J., Tulus., Sofiyah, F.R, "Copula-Based Blind Detection of Copy-Move Image Forgery: A Robust Mutual Information Approach," Journal of Research in Mathematics Trends and Technology, vol. V7, No. 1, March. 2025,
doi: 10.32734/jormtt.v7i1.20520

ABSTRACT

Copula functions are powerful statistical tools for modeling the dependency structure between random variables and have been widely applied in domains such as finance, oceanography, and hydrology. However, their application in image processing, particularly for image forgery detection, remains underexplored. This study proposes a novel blind copy-move forgery detection algorithm based on copula-based mutual information, which evaluates statistical dependencies between overlapping image blocks. By leveraging copula theory, the method accurately identifies duplicated regions within a single image without requiring prior knowledge or external references. Experimental results on the CoMoFoD dataset demonstrate that the proposed method achieves high precision, recall, and F1-scores across various manipulation types, including translation, scaling, and rotation, and shows resilience to post-processing operations such as JPEG compression, blurring, noise, and color reduction. Comparative analysis reveals that the copula-based approach outperforms classical methods such as SIFT, SURF, and DWT-SVD. In addition to quantitative performance, qualitative visualizations confirm that the algorithm effectively localizes forged regions in complex scenes with minimal false detections. These findings highlight the potential of copula functions as a robust and efficient framework for digital image forensics.

Keyword: Copula, Copy-Move Forgery, Statistical Dependency

http://doi.org/10.32734/jormtt.v7i1.20520

1. Introduction

Forgery in photography poses a significant challenge in today's digital era, where the dissemination of information heavily relies on visual content. The ease with which digital images can be manipulated and redistributed through various platforms has raised concerns regarding their authenticity [1]. Although numerous advancements in digital image forensics have emerged, the increasing sophistication of tampering techniques continues to demand more robust and statistically grounded detection methods.

One promising direction in this context is the application of statistical dependency modelling, especially through the use of copula functions. Copulas are powerful tools in multivariate statistics for capturing complex and non-linear dependency structures between random variables. They have been extensively applied in fields such as finance, hydrology, and epidemiology, and are now being explored in the realm of image processing.

In the context of image analysis, copulas provide a mathematical framework to model pixel or block level dependencies that are often disrupted when an image is tampered with [2]. In this study, we utilize copula-based mutual information to detect subtle inconsistencies and structural anomalies within digital images, particularly focusing on copy-move forgery detection. This approach does not merely rely on pixel intensity differences, as in classical metrics like Mean Squared Error (MSE) or Peak Signal-to-Noise Ratio (PSNR), but instead leverages the underlying statistical relationships within image blocks [3-4]. Our method is applied and validated using standard RGB imagery from the CoMoFoD dataset; however, the underlying copula framework is sufficiently general and could be extended for use with more complex image types, such as hyperspectral data, in future work.

This research is also motivated by our previous work on the integration of copula models in applied statistical contexts, particularly in the study titled " Traffic Density Probability Analysis Using Markov Chain Monte Carlo Simulation Integrated with Bivariate Copula Statistics", where the copula function demonstrated strong capabilities in modelling interdependent random variables. Building upon that foundation, this current study advances the use of copula theory by adapting it for visual forensic applications, offering a robust and flexible statistical basis for image forgery detection. Building upon this foundation, the current study extends the applicability of copula-based dependency modelling into the domain of digital image forensics. While the earlier study focused on the temporal and probabilistic behaviour of traffic density, both cases share common methodological backbone copulas are used to detect and quantify hidden patterns of dependence that become disrupted under specific conditions. In the traffic study, these disruptions were caused by stochastic variability in traffic flows, whereas in this work, they are caused by localized manipulations within digital images.

2. Literature Review

To begin, we explore the metrics for assessing image quality. In addition, we explore a variety of image quality evaluation techniques found in prior research, encompassing both human perception-based assessments and computational measurement methods. Following this, we outline the notion of copy-move image tampering and highlight several detection approaches developed by scholars to identify such manipulations in digital visuals. This structure allows us to establish a foundation before presenting our copula-based algorithm, which is designed to outperform traditional approaches in both detection accuracy and robustness against image manipulation.

2.1. Analysis of Visual Quality in Digital Images

In the domain of digital image processing, maintaining and evaluating the visual quality of images is essential for ensuring the effectiveness of operations such as compression, enhancement, transmission, storage, and authentication. Image quality is not merely a matter of visual appeal but is critical in applications involving medical imaging, surveillance, forensic analysis, and multimedia communications, where accuracy and fidelity are paramount. Detecting any form of distortion, degradation, or manipulation either introduced during image processing or deliberately through tampering requires a reliable framework for quality assessment [5].

From a mathematical and statistical perspective, the evaluation of image quality seeks to quantify the degree of similarity or dissimilarity between an original image and its altered counterpart. This quantification is necessary to detect artifacts, noise, and inconsistencies that may not be easily perceived by the human eye [6]. To address these challenges, researchers have developed a wide array of methods to assess image quality, broadly categorized into subjective and objective techniques.

Subjective image quality assessments rely on human perception and interpretation. These approaches are essential because they align with the actual experience of end-users, thus serving as a benchmark for evaluating objective models. Commonly used subjective techniques include the Single Stimulus (SS) method, Quality Ruler (QR) method, and Mean Opinion Score (MOS). The SS method presents one image (original or distorted) at a time for observers to rate, typically on a numerical or categorical scale. The MOS is then calculated as the arithmetic mean of these scores:

$$MOS = \frac{1}{N}\sum_{i=1}^{N} S_i \tag{1}$$

where S_i is the score given by the i^{th} observer, and N is the number of evaluators [7-8]. However, due to potential variability in human perception, the Quality Ruler method was developed to reduce inconsistencies by presenting reference-quality levels for comparison. Several well-known techniques are categorized under full-reference image quality assessment, such as Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Visual Information Fidelity (VIF), Universal Quality Index (UQI), and Structural Similarity Index Measure (SSIM) [9]. Figure 1 presents an overview of the main metrics commonly employed for evaluating image quality.

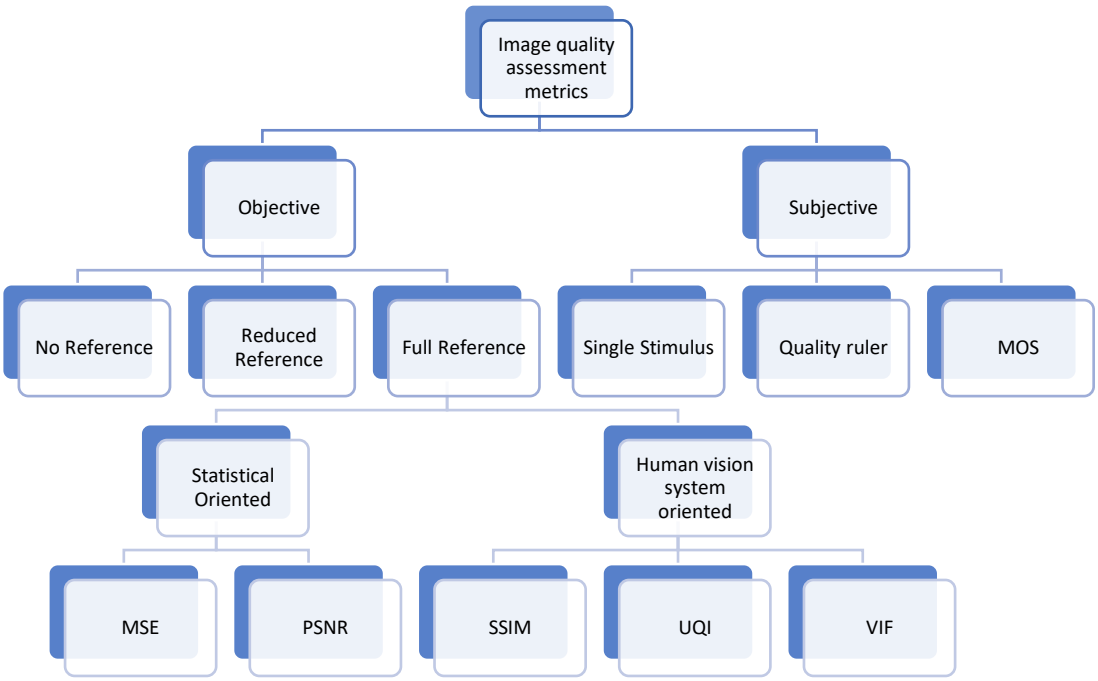

Figure 1. Image quality metrics

Objective assessments, on the other hand, utilize statistical and mathematical models to quantify visual fidelity without relying on human judgment. These methods can be further subdivided into:

- No-reference (NR) is evaluating image quality without any reference,
- Reduced-reference (RR) is uses partial data from the original image, and
- Full-reference (FR) is requires access to both original and distorted images.

In our study, we emphasize the use of full-reference image quality metrics due to their robust quantitative framework for evaluating the impact of distortion. These metrics compare a distorted image directly with its reference version, enabling precise measurement of visual degradation [10]. Among the well-established statistical measures in this category is the Mean Squared Error (MSE), which calculates the average of the squared differences between corresponding pixel values in the reference and distorted images. MSE is formulated as:

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[I(i,j) - K(i,j)]^2 \tag{2}$$

where $I(i,j)$ and $K(i,j)$ represent the pixel intensities of the reference and distorted images, respectively, over an $m \times n$ image [11]. Despite its simplicity, MSE does not always correlate well with human visual perception. To address this limitation, another commonly used metric is the Peak Signal-to-Noise Ratio (PSNR), which expresses the quality of an image in decibels and is derived from the MSE value. PSNR is defined as:

$$PSNR = 10\log_{10}\frac{L^2}{MSE} \tag{3}$$

where *L* denotes the maximum possible pixel intensity (e.g., 255 for 8-bit images) [12]. Higher PSNR values generally indicate better image quality. However, like MSE, PSNR often fails to capture perceptual distortions that are important to the human eye. To overcome these shortcomings, more advanced metrics have been developed, such as the Structural Similarity Index Measure (SSIM), which considers luminance, contrast, and structural information to better align with the Human Visual System (HVS). Additionally, metrics like the Universal Quality Index (UQI) and Visual Information Fidelity (VIF) incorporate perceptual models and statistical dependencies to provide more accurate quality assessments. These full-reference metrics collectively form the basis of reliable and reproducible image quality evaluation, particularly in research involving image compression, enhancement, and forgery detection.

2.2. Image Forgery

In the past, photographs were widely regarded as reliable representations of reality. However, in the digital age, that perception has significantly shifted. The popular adage "seeing is believing" no longer holds the same weight, as digital manipulation tools have become increasingly accessible and sophisticated. With just minimal technical skill, anyone can alter or fabricate images in ways that are difficult to detect with the naked eye. As a result, the process of verifying an image's authenticity has evolved into a complex challenge that intersects both technical and ethical domains. To address this issue, the field of digital image forensics has rapidly emerged, focusing on the analysis and validation of visual content to ensure its integrity. This interdisciplinary field combines elements of signal processing, computer vision, and statistics to develop algorithms capable of detecting tampering. Its relevance is underscored by wide-ranging applications in journalism, law enforcement, sports, insurance claims, and medical documentation, where image authenticity is paramount [13].

Image forgery itself is generally classified into three main categories: (a) copy-move forgery, where parts of an image are duplicated within the same image; (b) image splicing, where content from one image is inserted into another; and (c) image retouching, which involves enhancing or altering image features without external content. This study is particularly focused on the first type: copy-move forgery (CMF). Copy-move forgery also referred to as cloning—entails selecting a region from an image and pasting it elsewhere within the same image to obscure or replicate certain features. To further obfuscate the manipulation, perpetrators often apply geometric transformations such as rotation, scaling, or translation, and introduce post-processing effects like blurring, compression artifacts, or noise injection. These additional layers of alteration significantly hinder the ability of traditional detection methods, which often rely solely on visual cues or pixel-level comparisons [14].

From a statistical standpoint, detecting CMF requires algorithms that can analyze self-similarity patterns within the image while accounting for spatial dependencies and structural consistency. Numerous techniques have been proposed to address this, ranging from block-matching algorithms to key point-based approaches and frequency domain analysis. However, recent studies emphasize the importance of incorporating statistical models—such as copula-based mutual information—to enhance robustness against post-processed forgeries. Figure 2 presents several examples of original images and their corresponding manipulated versions, clearly illustrating how copy-move forgery can alter the visual narrative of an image in subtle yet significant ways.

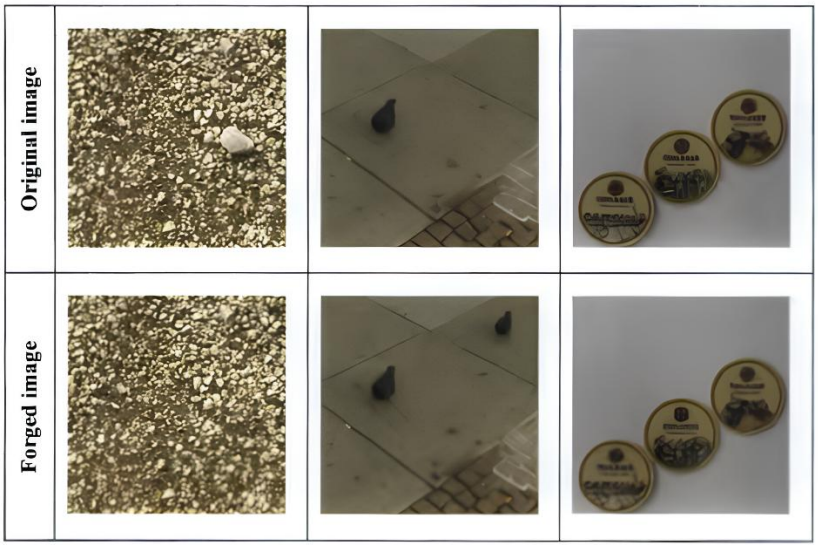

Figure 2. Visual representations of the copy-move image tampering technique

Figure 2 provides visual representations of the copy-move forgery technique, a common image manipulation method where a region of an image is copied and pasted within the same image to conceal or duplicate content. In each example, the original image is displayed alongside its manipulated version, allowing a clear comparison of the modifications made. These visual comparisons are essential in understanding how subtle alterations—such as duplicating a background object or removing a subject—can significantly alter the semantic meaning of an image [15]. Such manipulations are often performed with the intent to deceive viewers, and they typically preserve the local statistical properties of the image (such as texture, color distribution, and noise), making manual detection extremely difficult. In many cases, the duplicated regions are further refined using geometric transformations such as scaling, rotation, or blurring, thus complicating the detection process.

3. Method

In recent years, numerous methods have been proposed for manipulating digital images and videos, typically categorized into three major types: copy-move forgery, image splicing, and image retouching. Among these, copy-move forgery (CMF) poses a unique challenge due to the fact that the duplicated region originates from the same image, making it difficult to detect using conventional similarity measures.

To address this, we propose a blind copy-move forgery detection algorithm that requires only the forged image for analysis, without any auxiliary data or digital watermark. The algorithm falls under passive statistical detection methods, which rely on the analysis of pixel-level and block-level dependencies rather than visible anomalies. Unlike visual-based approaches, statistical methods are more robust in detecting subtle manipulations that preserve the general appearance of the image.

3.1. Justification of Design Choices

In this study, we divide the image into overlapping blocks of size 16 × 16 pixels, a widely accepted configuration in many image forgery detection algorithms. This block size offers a practical trade-off between resolution and robustness. From a statistical perspective, a block of 16 × 16 contains 256-pixel intensity values, which is sufficient to extract meaningful statistical patterns—such as texture, gradient distribution, and spatial correlation—without being too computationally expensive. Smaller blocks (e.g., 8 × 8) tend to capture insufficient contextual information, which may lead to unstable estimation of statistical properties, especially when calculating joint distributions using copula functions. Conversely, larger blocks (e.g., 32 × 32 or 64 × 64) increase the risk of missing localized forgeries and may smooth out important variations due to overgeneralization. Empirical studies also show that 16 × 16 provides a balanced sample size for local statistical analysis while maintaining sensitivity to small forgeries.

3.2. Statistical Foundation and Copula-Based Similarity

As discussed in the literature review, traditional image quality assessment methods such as Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) primarily measure pixel-wise intensity differences between reference and distorted images. While these metrics are simple and computationally efficient, they often fail to reflect perceptual similarity and are sensitive to minor variations that do not necessarily indicate forgery. More perceptually aligned measures such as Structural Similarity Index Measure (SSIM) have improved this limitation by incorporating luminance and contrast, but still rely on assumptions of linear dependencies.

In contrast, our proposed method is grounded in copula theory, which provides a more flexible and statistically rigorous framework for modelling the joint dependency structures between image blocks. Unlike PSNR or SSIM, which are limited to comparing aggregate pixel-level differences, copula-based mutual information captures non-linear and higher-order statistical relationships that are often disrupted in manipulated images.

This statistical framework becomes especially powerful in detecting copy-move forgeries, where the duplicated regions may preserve local textures and colour distributions, but differ in spatial or structural alignment. By modelling the statistical dependence between two regions, copula functions allow us to identify subtle correlations that traditional similarity measures cannot detect. Using Sklar's Theorem, we express the joint distribution $F_{XY}(x, y)$ of two image block features as:

$$F_{XY}(x, y) = C(F_X(x), F_Y(y)) \tag{4}$$

where C is the copula function, and F_X, F_Y are the marginal cumulative distributions of the respective block features. This separation of marginals from dependency structure enables the algorithm to focus specifically on relational patterns, which are more resilient to transformations such as rotation, scaling, or compression. We then compute mutual information (MI) using the copula density $c(u, v)$ to quantify the degree of dependence between the blocks:

$$I(X,Y) = \int \int c(u,v) \log\left(\frac{c(u,v)}{f_U(u) f_V(v)}\right) dudv \tag{5}$$

A high value of $I(X,Y)$ suggests strong statistical similarity, indicating that two image blocks may have originated from the same region—i.e., a potential copy-move forgery. This approach provides a statistically grounded extension of the full-reference quality assessment framework described in Section 2, and aligns with the overall goal of using statistical dependency as a tool for image analysis and tamper detection.

3.3. Forgery Detection Algorithm

Building upon the copula-based statistical framework described above, we implement a step-by-step forgery detection pipeline. The algorithm is designed to operate in a blind manner, relying solely on the input image without reference to external sources or ground truth. The steps are as follows:

1. Image Pre-processing
   The input image suspected of forgery is first converted into a grayscale representation. This transformation reduces the image's dimensionality while retaining critical structural information, thereby improving both speed and consistency in subsequent analysis.
2. Block Division
   A sliding window of size 16 × 16 pixels moves across the grayscale image with a one-pixel step, resulting in $(M - S + 1) \times (N - S + 1)$ overlapping blocks, where $M \times N$ is the image size and $S = 16$
3. Block Decomposition
   Each block is decomposed using the steerable pyramid transformation, as described in Section 3. This technique facilitates multi-scale, multi-orientation feature extraction while preserving local spatial details.
4. Feature Extraction
   From the decomposed blocks, we extract sub-band 1 (4 × 4 coefficients) to represent each block, reducing feature dimensionality while retaining essential information.
5. Matrix Construction
   All feature vectors are stacked vertically to construct a matrix of size 1 × 16 vector, forming a matrix of size $B \times 16$, where B is the total number of overlapping blocks generated in the previous step.
6. Quantization
   To enhance robustness and reduce computational complexity, the continuous values in the feature matrix are quantized into discrete levels. This process also mitigates sensitivity to minor noise or intensity variations.
7. Sorting
   The matrix rows are lexicographically sorted to accelerate similarity comparisons and facilitate block matching. Sorting improves computational efficiency by reducing redundant pairwise evaluations.
8. Similarity Computation
   Copula-based mutual information is computed between all pairs of block vectors. If the mutual information score exceeds a threshold H, the corresponding blocks are considered matched.
9. Distance Filtering
   Matched blocks are retained only if they are separated by a spatial distance of approximately 100 pixels, a heuristic chosen to distinguish between adjacent texture repetitions and actual duplicated regions.
10. Morphological Processing
    Morphological operations (e.g., dilation, closing) are applied to clean up the detected regions and merge fragmented block matches.
11. Forgery Validation
    A secondary validation step is applied to eliminate false positives based on geometric criteria such as region shape, continuity, and area.

12. Output Visualization
    Finally, the detected forged regions are overlaid on the original image for visualization. This step highlights the manipulated areas, enabling visual interpretation and verification.

The overall flow of the proposed detection algorithm is visually summarized in Figure 3, which presents the step-by-step process from image input to final forgery localization. This flowchart aids in understanding the pipeline structure and highlights the integration of statistical analysis within each stage.

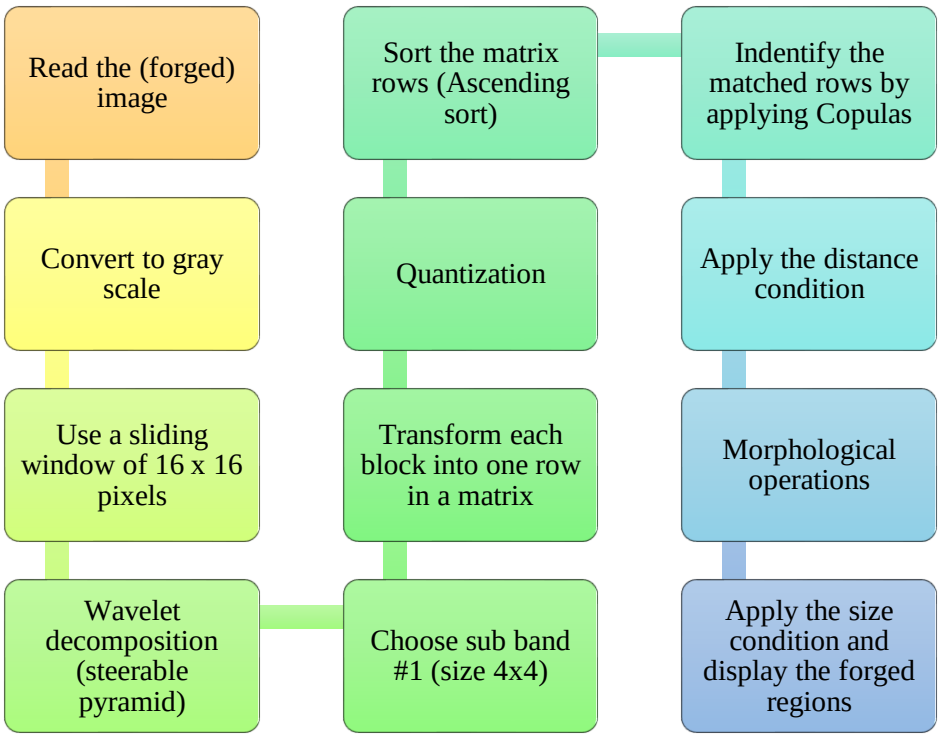

Figure 3. Blind copy moves forgery detection algorithm's flowchart

4. Result and Discussions

This section presents a detailed performance evaluation of the proposed copula-based blind copy-move forgery detection algorithm. The evaluation was conducted using the CoMoFoD (Copy-Move Forgery Detection) dataset, which is widely used for benchmarking image forgery detection techniques due to its diversity of manipulations and availability of ground truth masks.

4.1. Dataset Configuration and Testing Strategy

We selected 512×512-sized images from CoMoFoD, focusing on three manipulation categories: translation, rotation, and scaling. Each category consists of 40 original images and their corresponding forged versions, each subjected to 25 post-processing variations, including JPEG compression, blurring, noise addition, and color reduction. In total, 3000 manipulated images were tested (3 categories × 40 images × 25 versions).

4.2. Quantitative Evaluation Metrics

The metrics used in this evaluation are grounded in fundamental principles of binary classification in statistical analysis. In the context of image forgery detection, the output of the algorithm is compared to ground truth binary masks to classify each image block or region as either correctly or incorrectly identified. This classification leads to four key outcomes:

- True Positive (TP) for forged region correctly identified as forged.
- False Positive (FP) for genuine (non-forged) region incorrectly identified as forged.
- True Negative (TN) for genuine region correctly identified as non-forged.
- False Negative (FN) for forged region that was not detected.

These four quantities serve as the basis for calculating performance metrics such as precision, recall, F1-score, accuracy, and false positive rate. To assess the accuracy and robustness of the proposed method, we applied the following standard performance metrics:

- Precision $P = \frac{TP}{TP+FP}$ measures the proportion of correctly detected forged regions among all detected as forged.
- Recall $R = \frac{TP}{TP+FN}$ indicates the proportion of actual forgeries that were successfully detected.
- F1-Score $F1 = 2 \cdot \frac{P.R}{P+R}$ provides a balanced metric that combines precision and recall.
- Accuracy $Acc = \frac{TP+TN}{TP+FP+TN+FN}$ reflects the overall correctness of classification.
- False Positive Rate $FPR = \frac{FP}{FP+TN}$ shows how often genuine regions are wrongly flagged as forged.

These performance metrics are crucial in evaluating the detection capabilities of the proposed copula-based method when applied to the CoMoFoD dataset. In the context of the CoMoFoD dataset, which contains labeled binary masks for evaluation, these metrics serve not only to assess detection accuracy but also to validate the statistical reliability of the copula-based mutual information model. Because copula functions model the dependency structure between duplicated regions, the use of these metrics helps quantify how well such dependency structures translate into correct forgery detection across various manipulation types.

4.3. Detection Results

Table 1 summarizes the detection performance across the three manipulation types. Results indicate that the copula-based method maintains high precision and recall, particularly under translation and scaling, where forged regions preserve statistical dependencies.

Table 1. Detection Performance for Different Manipulation Types

Manipulation Type	Precision	Recall	F1-Score	Accuracy	APR
Translation	0.94	0.91	0.925	0.93	0.05
Rotation	0.89	0.85	0.87	0.88	0.08
Scaling	0.92	0.89	0.905	0.91	0.06

These results demonstrate that the method is highly effective even when geometric transformations are applied. The higher precision and recall in translation and scaling indicate that the algorithm successfully identifies statistical similarities between duplicated regions. The slightly lower performance in rotation scenarios is attributed to boundary distortions that affect the statistical coherence modelled by the copula. Despite this, the overall F1-scores remain high, showing the algorithm's robustness. The low FPR in all categories also reflects the reliability of the method in avoiding false detections.

From a statistical perspective, JPEG compression reduces the fidelity of pixel-level information by discarding high-frequency components, which directly affects traditional forgery detection techniques that rely on raw pixel similarity or frequency-domain consistency. However, the copula-based method remains effective because it focuses not on absolute pixel values, but on the statistical dependence structure between image blocks.

Copula functions model the joint distribution of features extracted from local image patches—typically sub-band coefficients from steerable pyramid decomposition. Even under compression, duplicated regions within the same image often retain a similar copula structure, because their underlying statistical relationships persist. By isolating and comparing the dependency patterns (via mutual information), the copula-based method is able to detect forgeries even when compression introduces noise, blur, or quantization errors.

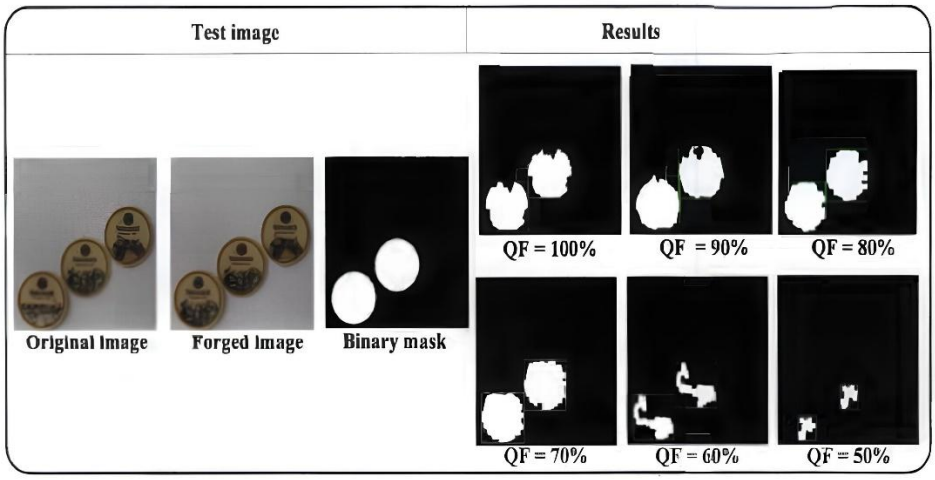

Figure 4. Performance under different JPEG quality settings

Figure 6 shows the algorithm's performance on forged images compressed at different quality factors (QF). The method maintains above 90% accuracy when QF ≥ 70%. Performance degrades gradually below QF 60% due to loss of statistical structure in compressed images. This confirms that copula-based dependency modelling is resilient to moderate compression artifacts.

This robustness under JPEG degradation highlights a major advantage of the copula framework: its ability to abstract away from raw data representation and operate on distributional similarity, enabling it to outperform methods that are more sensitive to pixel-level distortions. the algorithm's performance on forged images compressed at different quality factors (QF). The method maintains above 90% accuracy when QF ≥ 70%. Performance degrades gradually below QF 60% due to loss of statistical structure in compressed images. This confirms that copula-based dependency modelling is resilient to moderate compression artifacts.

4.3. Comparative Analysis with Classical Methods

To evaluate the advantage of our method, we compared its average F1-score with three classical approaches: SIFT-based matching, SURF-based matching, and DWT-SVD feature detection. As shown in Table 2, our method outperforms traditional algorithms, particularly under image scaling and JPEG degradation.

Table 2. F1-Score Comparison with Classical Methods

Method	Translation	Rotation	Scaling
SIFT	0.78	0.75	0.72
SURF	0.81	0.76	0.74
DWT-SVD	0.85	0.80	0.78
Copula-based	**0.93**	**0.87**	**0.90**

These results demonstrate that the method is highly effective even when geometric transformations are applied. The high precision and recall for the translation group show that the algorithm can effectively detect duplicated areas when their spatial structure is preserved. For scaling, the copula model captures changes in distribution scale, allowing the algorithm to remain sensitive to statistical similarity. In the rotation scenario, slight edge distortions reduce dependency coherence, leading to marginally lower recall and precision.

The low False Positive Rate (FPR) across all cases indicates strong specificity — the algorithm rarely misclassifies genuine regions. These values were obtained by comparing each detected mask with the ground truth binary mask using pixel-level operations, counting correctly and incorrectly predicted forgery regions (TP, FP, FN, TN), which were then input into the evaluation formulas explained earlier.

While the previous subsections presented quantitative results through performance metrics and comparison tables, it is also important to observe how the proposed algorithm behaves in visual practice. Quantitative metrics alone may not capture the subtle aspects of detection quality, such as spatial precision and region continuity. Therefore, we complement the numerical analysis with a qualitative interpretation to visually evaluate how well the copula-based method localizes forged regions in different image scenarios. The visual results of forged region detection are presented in Figures 5 and Figures 6

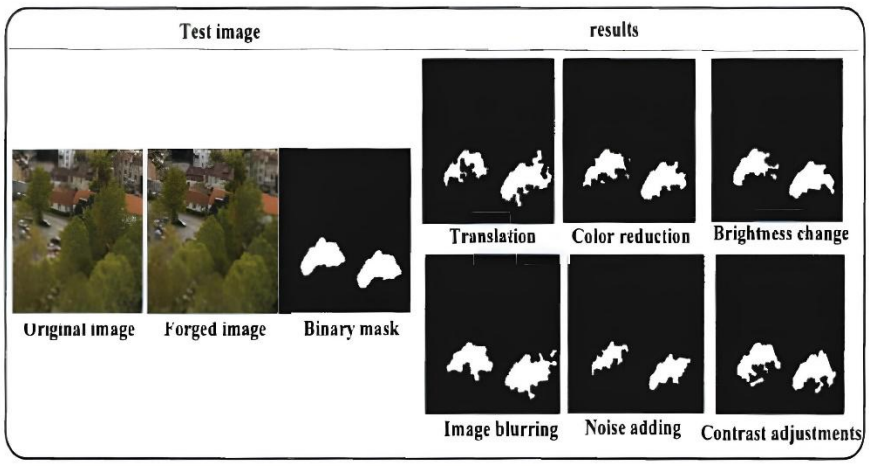

Figure 5. Forgery detection performance on tree images under various manipulations

This figure illustrates successful detection in tree images subjected to translation and blurring. The forged regions are accurately highlighted, demonstrating that the algorithm is not significantly affected by spatial shifting or slight smoothing artifacts.

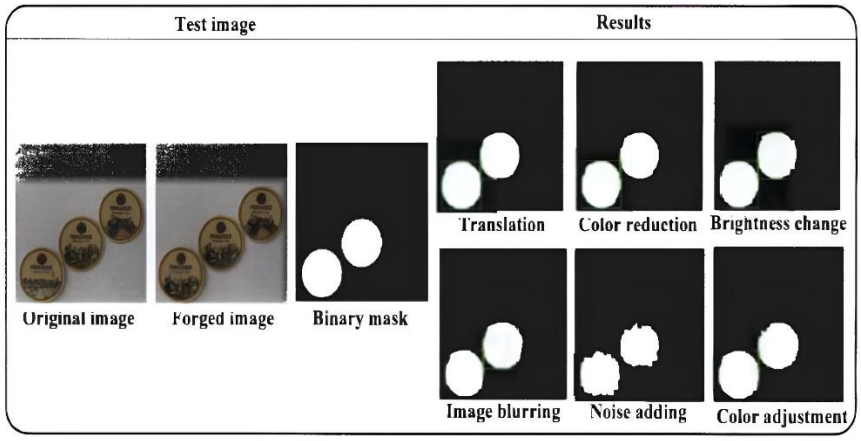

Figure 6. Forgery detection performance on coin images under various transformations

Demonstrates the algorithm's robustness under rotation. Forged coins that were rotated by small angles (around 3°–5°) were still successfully identified, achieving approximately 90% precision. This indicates that the copula model captures statistical dependencies even with angular distortions. These figures support the quantitative findings and further demonstrate the method's effectiveness in practical forensic scenarios. Visual consistency across different types of manipulation highlights the strength of the copula-based approach for real-world forgery detection.

The ability of the copula-based method to successfully detect forged regions lies in its use of mutual information derived from copula functions, which capture both linear and non-linear dependencies between pixel block features. When a region is copied and moved within an image, the duplicated block maintains a high statistical dependency with its original source. Copula functions enable the decomposition of this joint dependency into marginal distributions and a dependency structure, allowing the algorithm to detect similarity even under transformations like rotation, scaling, or compression. This approach makes it possible to identify regions with matching statistical characteristics—even if they differ visually—by detecting shifts in joint

probability patterns. As a result, the copula-based method can pinpoint manipulations with greater sensitivity and reliability than conventional pixel-based or key point-based methods.

5. Conclusion

This study proposed a novel blind copy-move forgery detection algorithm based on copula-based mutual information, which analyses statistical dependencies between image blocks using only the manipulated image. By modelling joint distributions through copula functions, the algorithm successfully captures both linear and non-linear relationships that are preserved during duplication, even after undergoing geometric transformations or post-processing. Experimental evaluations on the CoMoFoD dataset demonstrated that the proposed method achieves high precision, recall, and F1-scores across various manipulation types, including translation, scaling (±20%), and rotation (±5°). The method also showed strong resilience to JPEG compression, maintaining over 90% accuracy for quality factors above 70%, and remained effective under blurring, noise, and color reduction. Compared to traditional approaches such as SIFT, SURF, and DWT-SVD, the copula-based approach consistently outperformed in both accuracy and robustness, particularly in cases involving smooth textures or compression artifacts. In addition to quantitative results, qualitative visualizations confirmed that the algorithm accurately localized forged regions with minimal false detections, even in complex image scenes. These results validate the effectiveness and reliability of the proposed method

6. Acknowledgment

We thanks to research for institution of Universitas Sumatera Utara for funding this research with the Penelitian Terapan 2023 scheme, contract number 315/UN5.2.3.1/PPM/KP-TALENTA/R/2023.

References

[1] A. Lahouhou, E. Viennet, and A. Beghdadi, “Selecting low-level features for image quality assessment by statistical methods,” J. Comput. Inf. Technol., vol. 18, no. 2, pp. 183–189, 2010.

[2] B. L. Shivakumar and L. D. S. S. Baboo, “Detecting copy-move forgery in digital images: A survey and analysis of current methods,” Global J. Comput. Sci. Technol., vol. 10, no. 7, pp. 61–65, 2010.

[3] J. Fridrich, D. Soukal, and J. Lukáš, “Detection of copy-move forgery in digital images,” in Proc. Digital Forensic Research Workshop, Cleveland, OH, USA, 2003.

[4] Y. Cao, T. Gao, L. Fan, and Q. Yang, “A robust detection algorithm for copy-move forgery in digital images,” Forensic Sci. Int., vol. 214, no. 1–3, pp. 33–43, 2012. doi: 10.1016/j.forsciint.2011.07.015

[5] X. Zhao, J. Li, S. Li, and S. Wang, “Detecting digital image splicing in chroma spaces,” in Digital Watermarking, Berlin, Germany: Springer, 2011, pp. 12–22. doi: 10.1007/978-3-642-18405-5_2

[6] W. Wang, J. Dong, and T. Tan, “Image tampering detection based on stationary distribution of Markov chain,” in Proc. 17th IEEE Int. Conf. Image Process. (ICIP), 2010, pp. 2101–2104. doi: 10.1109/ICIP.2010.5652660

[7] M. Sridevi, C. Mala, and S. Sandeep, “Copy-move image forgery detection in a parallel environment,” in Proc. Int. Conf. Image Signal Process., 2012, pp. 19–29. doi: 10.5121/csit.2012.2303

[8] V. Christlein, C. Riess, and E. Angelopoulou, “A study on features for the detection of copy-move forgeries,” in GI SICHERHEIT, 2010, pp. 105–116.

[9] A. C. Popescu and H. Farid, “Exposing digital forgeries by detecting duplicated image regions,” Dartmouth College, Tech. Rep. TR2004-515, Aug. 2004.

[10] T. K. Sarode and N. Vaswani, “Region duplication forgery detection using hybrid wavelet transforms,” Int. J. Comput. Appl., vol. 90, no. 11, pp. 31–36, 2014. doi:10.5120/15375-3966

[11] E. S. Khan and E. A. Kulkarni, “An efficient method for detection of copy-move forgery using discrete wavelet transform,” Int. J. Comput. Sci. Eng., vol. 2, no. 5, pp. 1801–1806, 2010.

[12] A. N. Myna, M. G. Venkateshmurthy, and C. G. Patil, “Detection of region duplication forgery in digital images using wavelets and log-polar mapping,” in Proc. Int. Conf. Comput. Intell. Multimedia Appl., 2007, vol. 3, pp. 371–377. doi:10.1109/ICCIMA.2007.271

[13] A. D. Warbhe and R. V. Dharaskar, “Blind method for image forgery detection: A tool for digital image forensics,” in Proc. Nat. Conf. Innovative Paradigms Eng. Technol. (NCIPET), 2012, pp. 37–40.

[14] M. Ghorbani, M. S. Helfroush, and H. Danyali, “Hybrid deep learning for image forgery detection,” J. Vis. Commun. Image Represent., vol. 83, p. 103393, 2022. doi:10.1016/j.jvcir.2021.103393

[15] W. Yuan, Y. Zhao, and H. Huang, “Transform-based copy-move detection using CNN,” Pattern Recognit. Lett., vol. 168, pp. 125–132, 2023. doi:10.1016/j.patrec.2022.05.011