International Journal of Wireless and Ad Hoc Communication

♦ ISSN: 2692-4048 Vol: 09, No. 02, 2025 ♦ PP. 14–17

Article DOI: https://doi.org/10.54216/IJWAC.090203

FULL LENGTH ARTICLE

An Efficient Detection of Copy-Move Forgery Using Phase Correlation

L. Chitirap Paavai[1,*] **V. Vadivu**[1] **L. Krishnan**[2]

[1] Assistant Professor, Department of ECE, Knowledge Institute of Technology, Salem, Tamil Nadu, India

[2] Assistant Professor, Department of Civil, Knowledge Institute of Technology, Salem, Tamil Nadu, India

Emails: lcece@kiot.ac.in · vvaece@kiot.ac.in · lkcivil@kiot.ac.in

Received: February 05, 2025 Revised: February 20, 2025 Accepted: March 22, 2025 ⋆ Corresponding author

ABSTRACT

Creating images is one of the main focuses of digital image processing. There are multiple techniques to spot image fraud. This work proposes a new approach to detect attacks that mimic copy-move forgeries. The proposed method applies discrete wavelet transform (DWT) on the input image to create a reduced-dimensional representation of the image. After that, the compressed image is divided into overlapping blocks. After these blocks are sorted, phase correlation is utilized as a similarity criterion to find duplicate blocks. Due to DWT usage, the lowest-level picture representation is first employed for detection. This work also covers the examination of numerous limits that are imposed on the input image, and the results are used in the analysis that follows.

Keywords: Copy-move forgery ▪ Digital forensics ▪ DWT ▪ Phase correlation

1. INTRODUCTION

One use of digital image processing is the detection of image forgeries. With the advent of strong computer graphics editing tools such as GIMP and Corel Paint Shop, the process of making fake photographs has become incredibly easy. Image splicing, copy-move assault, and image retouching are a few techniques used to create a bogus image.

A portion of the original image is copied and pasted into another portion of the identical image in a copy-move fake [1, 2]. This is typically done by overlaying a segment that has been cloned from another area of the image over the object to make it "disappear" from the picture. For this reason, textured areas are perfect. The copied areas will probably blend in with the background, making it difficult for the human eye to pick out any suspicious artefacts [3]. Examples of such textured areas are grass, leaves, gravel, and cloth with random patterns. Because the cloned portions are identical to the original image, their colour scheme, dynamic range, noise level, and most other crucial characteristics will match those of the original and prevent them from being identified by techniques that search for incompatibilities in the statistical measure in different parts of the image [4].

The remainder of this essay is structured as follows. The suggested method for detecting forgeries is covered in Section 2 [5]. The identification of reference and match blocks is covered in Section 2.1. The comparison of reference and match blocks is covered in Section 2.2 [1]. Section 3 presents the experimental results with various constraints, and Section 4 concludes the paper with future enhancements.

2. RELATED WORK

In olden days, forgery could be detected by comparing the light intensity between images. If two photos were taken at the same time, differences in their light intensity could indicate tampering [6].

In another forgery detection technique, the forged image is

© 2025 The Author(s). Published by ASPG. This article is licensed under CC BY 4.0.

resampled, and from the blurred image block edges the forged portion present in the tampered image is detected [7].

Using picture characteristics such as moment- and Markov-based features, image fraud detection is possible. When compared to the original image, the manipulated image will have certain differences in its attributes. This allows for the detection of the forged component [8, 9].

The quantization table is estimated from the candidate region. After quantization table estimation, the variation resulting from inconsistency of the quantization table is utilized to detect tampered regions [10, 11]. Digital image forgery can also be detected by inconsistency in blocking artefacts.

3. PROPOSED METHODOLOGY

Detecting the forged area of a given image is facilitated by the use of phase correlation and DWT. Because wavelet decomposition has intrinsic multiresolution properties, it is employed for image processing. Reducing the image's size at each level is the fundamental notion by use of DWT. The image is divided into four smaller images at each level: LL, LH, HL, and HH. We utilize this image to do additional decomposition. The letters LH, HL, and HH stand for the image's vertical, horizontal, and diagonal components, respectively. Combining these sub-images will recreate the decomposed image. This is the reason why DWTs are used to compare matching blocks iteratively. Every cycle, the images are used to match and overlap.

The following formula is used for phase correlation. The ratio R between two images, img_1 and img_2, is determined as:

$$R = \frac{F(img_1) \times \text{conj}(F(img_2))}{\|F(img_1) \times \text{conj}(F(img_2))\|} \tag{1}$$

where conj is the complex conjugate and F is the Fourier transform. The phase correlation can be expressed as the inverse Fourier transform of R. There are two stages to the work on this study, which are described here.

3.1 Detection of Reference and Match Blocks

This phase deals with the detection of reference and matching blocks, as shown in Figure 1. As a result of this phase, candidate detected blocks are obtained.

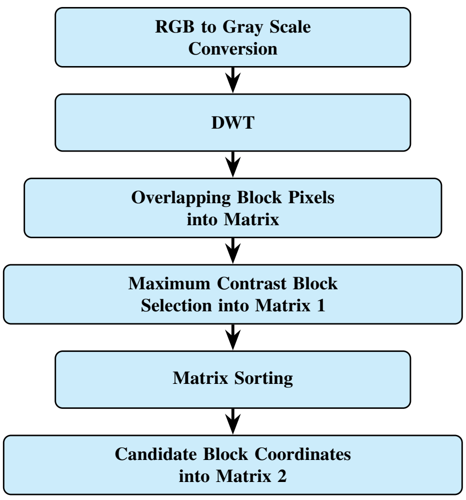


Figure 1. Detection of reference and match blocks.

Algorithm

1. Examine the picture input. Convert the incoming image to a grayscale format if it is not already one.
2. Utilize DWT on the image in grayscale.
3. For every LL overlapping $b \times b$ block image, take out the values of the resultant pixels by rows into a new row to create a matrix with dimension b columns and $(M-b+1) \times (N-b+1)$ rows.
4. Create a second matrix with the same row as the previous one and two extra columns to store the top-left coordinates.
5. Disregard blocks with minimal contrast, and sort Matrix A lexicographically.
6. Using the blocks that correspond to the rows above and below the current row, calculate the phase correlation for the block that matches the current row.
7. Record the top-left coordinates of the relevant reference block and matching block from the matrix if the greatest phase-correlation value is greater than a predetermined threshold value t.

3.2 Comparison of Reference and Matching Blocks

This phase deals with checking on different DWT levels, as shown in Figure 2. After the preceding step, region comparison is directly done on the original image and duplicated block detection.

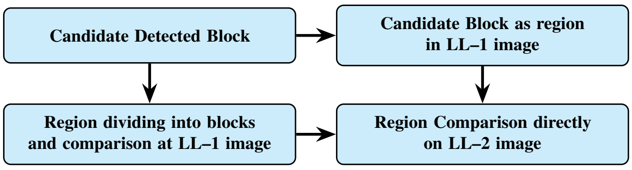


Figure 2. Comparison of reference and matching blocks.

Algorithm

1. Create a reference region and matching region for the lower LL level by padding the $b \times b$ reference block and match block with m pixels on all sides.
2. For every $b \times b$ overlap in the reference region, use phase correlation to locate the corresponding match in the matching region.
3. The top-left coordinates of the matching and corresponding reference blocks are recorded in a new row of a matrix if the maximum phase-correlation value is greater than a predetermined threshold value.
4. To create a reference region and matching region with a low LL level compared to the original image, pad the $b \times b$ reference block and match block with m pixels on each side, then compare the results using phase correlation.
5. If the highest phase-correlation value surpasses the predetermined threshold, retain the detected duplicated block coordinates.

This phase deals with detection of reference and matching blocks on the lowest level of the wavelet-transform compressed image. Figure 3 demonstrates the detection of reference and match blocks in this process. The next phase deals with checking on different DWT levels to produce more robust output. The comparison of reference and match blocks is illustrated in Figure 4.

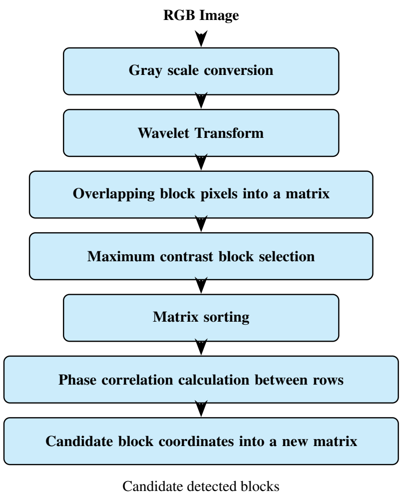


Figure 3. Candidate detected blocks.

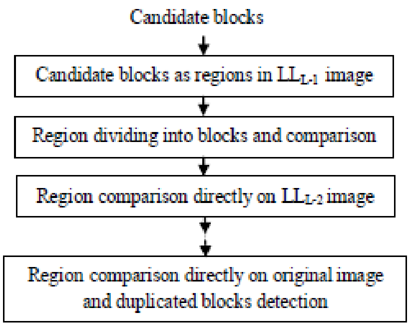


Figure 4. Comparison of reference and matching blocks across DWT levels.

4. RESULTS AND DISCUSSION

The proposed method has been implemented using MATLAB 2009. The experimental environment is a personal computer.

(a) Original image **(b)** Copy image **(c)** Forged portion

Figure 5. Original image, copy image, and forged portion.

Table 1. Original image, copy image, and forged portion.

a.	b.	c.
Original image	Copy image	Forged portion

Figure 5 depicts the original image, copied image, and forged portion of the original image. By applying geometrical transformations such as rotation and scaling to the input, the corresponding output is obtained as shown in Figure 6.

(a) Rotating 90 degrees **(b)** Rotating 180 degrees **(c)** Scaling

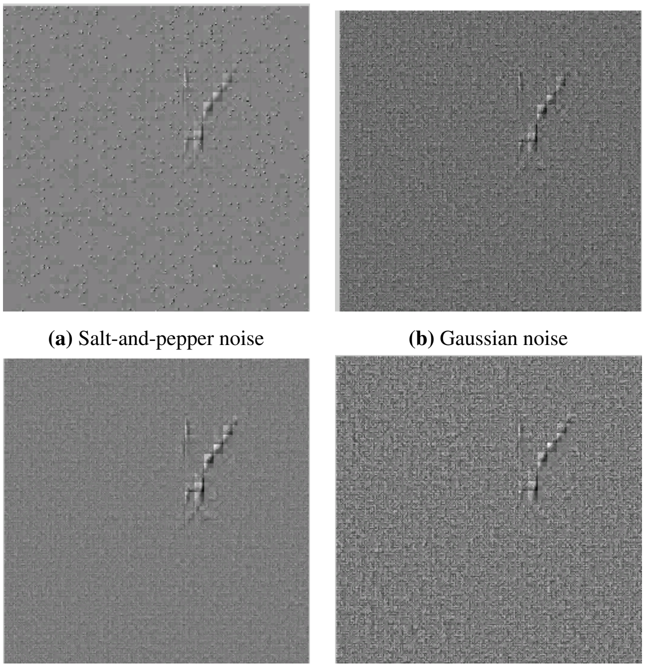
Figure 6. Geometrical transformations: rotation and scaling.

Table 2. Geometrical transformations.

a.	b.	c.
Rotating 90 degrees	Rotating 180 degrees	Scaling

The rotation property can withstand 90 and 180 degrees, but fails at 45 degrees. Scaling can be done only at a 1:40 value.

By applying noise such as salt-and-pepper, Gaussian, Poisson, and speckle noise to the input, the corresponding outputs are obtained as shown in Figure 7. This algorithm can withstand salt-and-pepper, Gaussian, Poisson, and speckle noise.



(a) Salt-and-pepper noise **(b)** Gaussian noise

(c) Poisson noise **(d)** Speckle noise

Figure 7. Noise robustness results.

Table 3. Noise robustness outputs.

a.	b.	c.	d.
Salt-and-pepper	Gaussian	Poisson	Speckle

5. CONCLUSION

This paper suggests a method for detecting copy-move forgeries using wavelet transformations and phase correlation.

This algorithm has low computational complexity. This method works even for photographs in which the attacker has added noise and geometric alterations to complicate detection. Experiments and analysis show that the proposed method is quite robust. Duplicate regions and scaled forged parts rotated across angles are recognized. In the future, this algorithm can be extended to support JPEG compressions and multiple forging-region detection.

REFERENCES

[1] S. Khan and A. Kulkarni, "Reduced time complexity for detection of copy-move forgery using discrete wavelet transform," in *International Journal of Computer Applications*, vol. 6, no. 7, 2010.

[2] T. Zhang and R.-d. Wang, "Copy move forgery detection based on svd in digital image," in *Proceedings of IEEE*, 2009.

[3] B. Ahmed, T. A. Gulliver, and S. alZahir, "Blind copy-move forgery detection using svd and ks test," *SN Applied Sciences*, vol. 2, no. 1377, 2020.

[4] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy-move forgery in digital images," in *Proceedings of the Digital Forensic Research Workshop*, Cleveland, OH, USA, 2003.

[5] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dartmouth College, Hanover, NH, USA, Tech. Rep. TR2004-515, 2004.

[6] D. A. Talbert and D. Fisher, "An empirical analysis of techniques for constructing and searching k-dimensional trees," in *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2000, pp. 26–33.

[7] I.-K. Jung and S. Lacroix, "A robust interest point matching algorithm," in *Proceedings of the International Conference on Computer Vision*, 2001.

[8] N. Sugirtham *et al.*, "Modified playfair for text file encryption and meticulous decryption with arbitrary fillers by septenary quadrate pattern," *International Journal of Networked and Distributed Computing*, vol. 12, pp. 108–118, 2024.

[9] B. Thiyaneswaran, K. Anguraj, S. Kumarganesh, and K. Thangaraj, "Early detection of melanoma images using gray level co-occurrence matrix features and machine learning techniques for effective clinical diagnosis," *International Journal of Imaging Systems and Technology*, vol. 31, no. 2, pp. 682–694, 2021.

[10] S. Mukherjee and A. K. Pal, "A hybrid SWT-SVD based multiresolution features for robust image copy-move forgery detection," *Multimedia Tools and Applications*, vol. 83, no. 16, pp. 48 141–48 163, 2024.

[11] X. Zhu, "An approach for copy-move image multiple forgery detection based on an optimized pre-trained deep learning model," *Knowledge-Based Systems*, vol. 269, p. 110508, 2023.