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

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 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 to 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 like 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 the 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]. In Section 3, the experimental results with various constraints is presented. Section 4 concludes the paper with future enhancements.

2. Related Work

In olden days the forgery can be detected by comparing the light intensity between the images. If two photos taken at the same time also have some difference in their light intensity [6].

In this forgery detection technique, the forged images is resampled and from the blurred images in block edges the forged portion present on tampered image is detected [7].

DOI: https://doi.org/10.54216/IJWAC.090203
Received: February 05, 2025 Revised: February 20, 2025 Accepted: March 22, 2025

Using picture characteristics like 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 the inconsistent of quantization table is utilized to detect tampered regions [10-11].

The digital image forgery is detected by inconsistency in the blocking artefacts.

3. Proposed Methodology

Detecting the forged area of the 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. Here's how to determine the ratio R between two images, img1 and img2.

$$R = F(img1) \times conj(F(img2)) / \| F(img1) \times conj(F(img2)) \| \quad (1)$$

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.

This phase deals with the detection of reference and matching shown in figure 1.

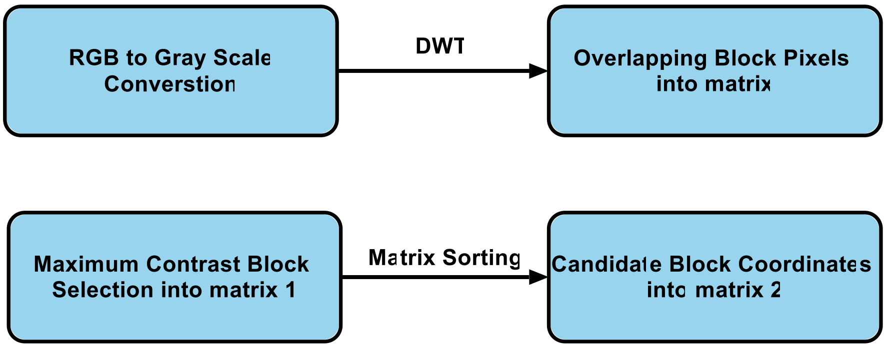

Figure 1. Detection of Reference and Match Blocks

As a result of this phase we obtain the candidate detected blocks.

A. Algorithm

- ✓ Examine the picture input. Convert the incoming image to a grayscale format if it isn't already one.
- ✓ Utilize DWT on the image in grayscale.
- ✓ For every LL overlapping b × 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) × (N-b+1) rows.
- ✓ Create a second matrix (1) with the same row as the previous one and two extra columns to store the top-left coordinates.
- ✓ Disregard blocks with minimal contrast and Matrix A can be sorted lexicographically. 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.
- ✓ Record the top left coordinates of the relevant reference block and the matching block form matrix (2) if the greatest phase correlation value is greater than a predetermined threshold value t. Consequently, the candidate discovered blocks are acquired.

This phase deals with checking on different DWT levels

DOI: https://doi.org/10.54216/IJWAC.090203
Received: February 05, 2025 Revised: February 20, 2025 Accepted: March 22, 2025

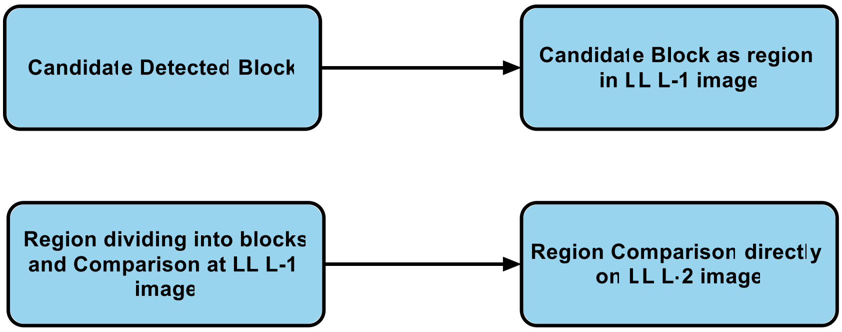

Figure 2. Comparison of reference and matching blocks

After the above step region comparison is directly done on original image and duplicated block detection. Representation of this process is shown in figure 2.

B. Algorithm

- ✓ Create a reference region and matching region for the lower LL level by padding the b × b reference block and match block with m pixels on all sides.
- ✓ For every b × b overlap in the region of reference. Using phase correlation, locate the corresponding match in the matching region.
- ✓ 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.
- ✓ To create a reference region and matching region with a low LL level compared to the original image, pad the b × b reference block and match block with m pixels on each side, then compare the results using phase correlation.
- ✓ Should the highest phase correlation value surpass a predetermined

This phase deals with detection of reference and matching blocks on the lowest level of wavelet transform compressed image. The figure 3 demonstrate the detection of reference and math block of this process.

The next phase deals with checking on different DWT levels to produce more robust output**.** The comparison of reference and match blocks are illustrating the figure 4.

4. Results and Discussion

The proposed method has been implemented using MATLAB 2009 version Experimental environment is on a personal computer.

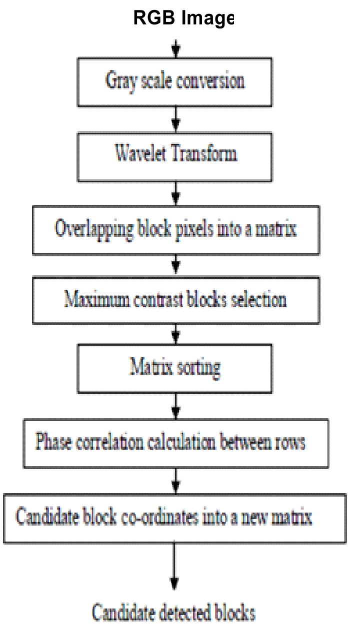

Figure 3. Comparison of reference and matching blocks

DOI: https://doi.org/10.54216/IJWAC.090203
Received: February 05, 2025 Revised: February 20, 2025 Accepted: March 22, 2025

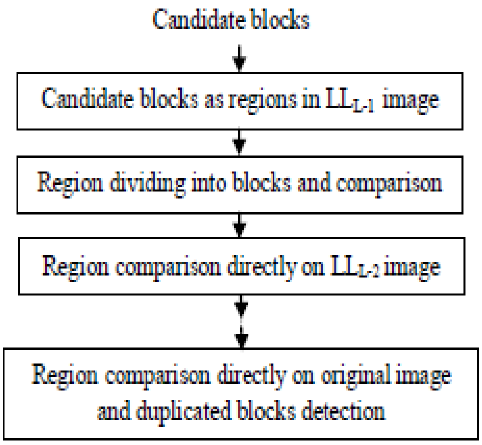

Figure 4. Comparison of reference and matching blocks

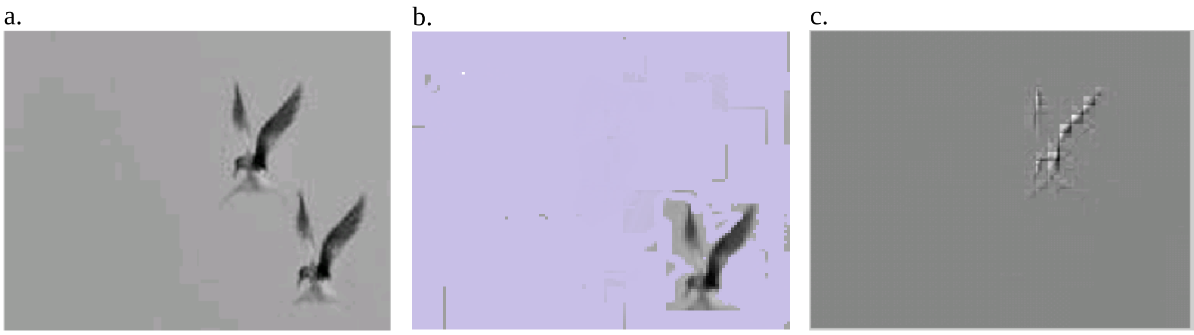

Figure 5. (a) Original Image (b) Copy Image (c) Forged portion

The figure 5 depicted the original Image, Copy Image and forged portion of the original image. By applying geometrical transformations such as rotation property, and scaling property to the input we get the corresponding output as shown below figure 6.

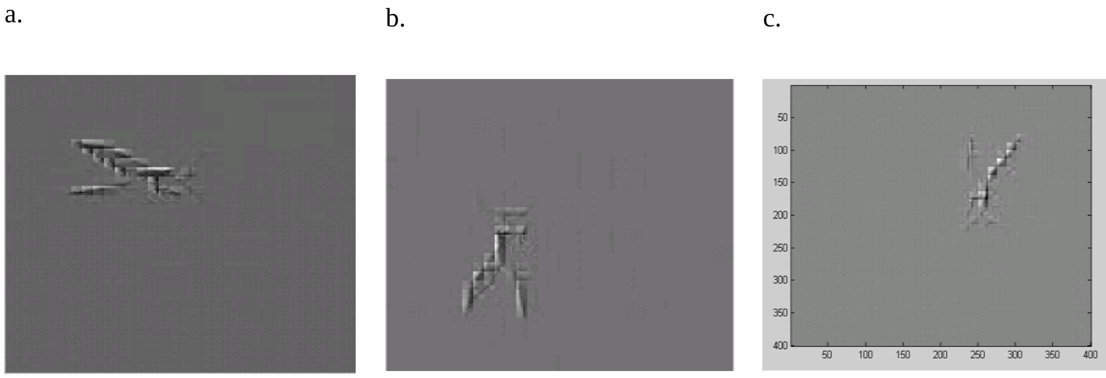

Figure 6. (a) Rotating 90 degree (b) Rotating 180 degree (c) scaling

- ✓ Rotate property can withstand at 90 and 180 degrees, fails at 45 degree
- ✓ Scaling can be done only at1:40 value

By applying noise such as Salt and pepper, Gaussian, Poisson, and Speckle to the input we get the corresponding output as shown below figure 7.

DOI: https://doi.org/10.54216/IJWAC.090203
Received: February 05, 2025 Revised: February 20, 2025 Accepted: March 22, 2025

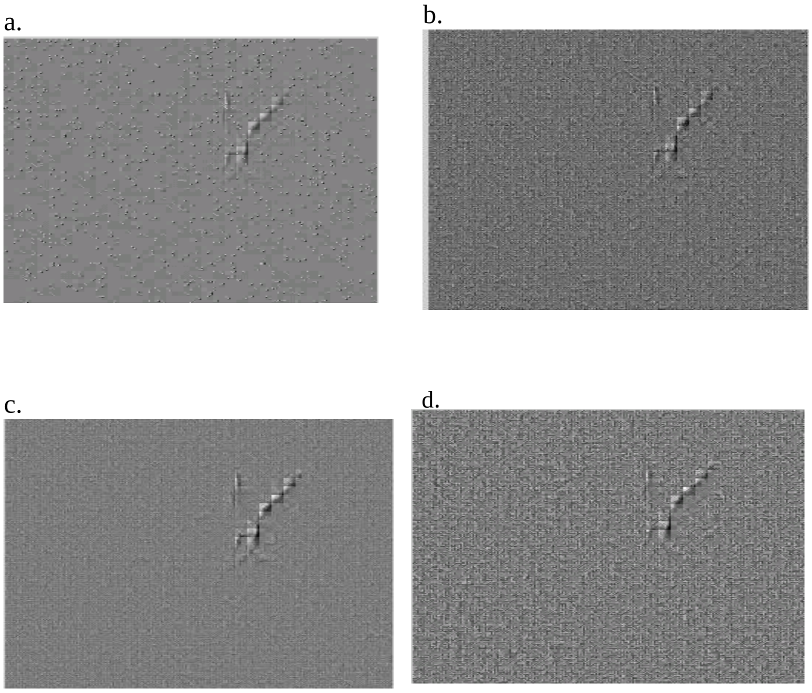

Figure 7. (a) Salt and pepper noise (b) Gaussian noise (c) Poisson noise (d) Speckle noise

This algorithm can withstand Salt and pepper, Gaussian, Poisson, and Speckle noise.

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 rotate across angles are recognized. In the future, this algorithm can be extended to support JPEG compressions and multiple forging region detection.

Funding: “This research received no external funding”

Conflicts of Interest: “The authors declare no conflict of interest.”

References

[1] S. Khan and A. Kulkarni, "Reduced Time Complexity for Detection of Copy-Move Forgery using Discrete Wavelet Transform," *Int. J. Comput. Appl.*, vol. 6, no. 7, Sep. 2010.

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

[3] B. Ahmed, T. A. Gulliver, and S. alZahir, "Blind copy-move forgery detection using SVD and KS test," *SN Appl. Sci.*, vol. 2, no. 1377, 2020, doi: 10.1007/s42452-020-3181-6.

[4] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy-move forgery in digital images," in *Proc. Digit. Forensic Res. 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 *Proc. ACM SIGKDD Int. Conf. Knowl. Discov. Data Min.*, 2000, pp. 26–33.

DOI: https://doi.org/10.54216/IJWAC.090203
Received: February 05, 2025 Revised: February 20, 2025 Accepted: March 22, 2025

[7] I.-K. Jung and S. Lacroix, "A Robust Interest Point Matching Algorithm," in *Proc. Int. Conf. Comput. Vis.*, 2001.

[8] N. Sugirtham et al., "Modified Playfair for Text File Encryption and Meticulous Decryption with Arbitrary Fillers by Septenary Quadrate Pattern," *Int. J. Netw. Distrib. Comput.*, vol. 12, pp. 108–118, 2024, doi: 10.1007/s44227-023-00019-4.

[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," *Int. J. Imaging Syst. Technol.*, vol. 31, no. 2, pp. 682–694, 2021.

[10] [Authors not specified], "A Hybrid SWT-SVD Based Multiresolution Features for Robust Image Copy-Move Forgery Detection," *Multimed. Tools Appl.*, vol. [Volume], no. [Issue], pp. [Pages], 2022, doi: 10.1007/s11042-023-17279-5.

[11] [Authors not specified], "An approach for copy-move image multiple forgery detection based on an attention mechanism," *Knowl.-Based Syst.*, vol. [Volume], pp. [Pages], 2022, doi: 10.1016/j.knosys.2023.109197.

DOI: https://doi.org/10.54216/IJWAC.090203
Received: February 05, 2025 Revised: February 20, 2025 Accepted: March 22, 2025