Kongunadu Research Journal 10 (1): 16-21, 2023
Publisher: Kongunadu Arts and Science College, Coimbatore.

https://krjournal.com/index.php/krj/article/view/605

DOI:10.26524/krj.2023.3

RESEARCH ARTICLE

Radial search for accelerating block matching to detect copy-move forgery in digital photographs

Velmurugan, S.[a]*, Subashini, T. S.[b], Saravana Moorthy, R.[a]
[a]Department of Computer Science, Kongunadu Arts and Science College, Coimbatore - 641029, Tamil Nadu, India
[b]Department of Computer Science and Engineering, Annamalai University, Annamalai Nagar - 608002, Tamil Nadu, India

ABSTRACT

One of the exciting areas of image processing research right now is image forensics. The most common kind of image forgery is copy-move (CM) forgery. In this study, a method for quickly detecting CM counterfeiting is proposed. The suggested approach speeds up the block matching process by employing the proposed radial search method. DCT features are extracted from each block and only the most "R' significant features are considered to create the feature vector which in turn shortens the processing time for feature matching. Then radix sorting is used to sort the blocks based on the DCT coefficients, and the proximity of blocks is used to indicate how similar they are. Each pair of adjacent blocks has their difference measured, and if the difference between two blocks is less than a predetermined threshold, the blocks are deemed comparable. Once a match is found, the nearby eight blocks are located using the radial search strategy, which eliminates the need for the traditional sequential block comparison. As opposed to exhaustive block matching, the radial search approach is experimented with which gives commendable improvement in copy move forgery detection.

Keywords: Copy-move image forgery, block based, radial search, radix sort, DCT.

1. INTRODUCTION

The goal of the emerging research domain namely image forensics is to confirm the legitimacy of an image. Advanced image editing software makes it simple to forge photographs in a number of ways, including copy-move forging [8], the topic of this study. Copy-move forgery changes the content of the image by copying a portion of an image and pasting it in a different location inside the same image, Fraudsters occasionally utilise post-processing techniques like rotation, scaling, multiple copy-move, and others to conceal their crimes and deceive viewers. In Fig. 1, the clock in the tower has been copied and moved to the small tower next to the big tower and this is an example of copy move forgery. The CMFD techniques are broadly classified into blocks and key-point based strategies. Block-based approaches collect features from an image by segmenting it into overlapping blocks [1]. The regions of forgeries are determined by comparing one block's resemblance to the remaining blocks. Key-point descriptors are extracted and matched to key points in the entire image to categorize the areas that have been altered in the case of key-point-based techniques.

1.1 Previous Work

This section gives a brief overview on the work done using block based methods to detect and localize copy-move forgeries. The easiest technique to identify copy-moved portions in an image is to conduct a thorough search, but this can only be done for extremely small images because it is computationally expensive. The cloned section is processed by the fraudster to hide the tampering, which is another reason why this practise is ineffective. The most popular method for detecting the copied section begins with separating the suspected image into overlapping chunks. The most durable traits must be extracted from the blocks after division in order to increase decision rates.

*Correspondence: S. Velmurugan, Department of Computer Science (SF), Kongunadu Arts and Science College, Coimbatore - 641029, Tamil Nadu, India. E.mail: svelmurugan_cs@kongunaducollege.ac.in

Figure 1. Example of copy-move forgery:(a) Genuine image, (b) Copy-moved forged image

Fig. 2 depicts the many kinds of CMFD techniques. This study is based on block-based approach to detect copy-move forgery in digital photographs.

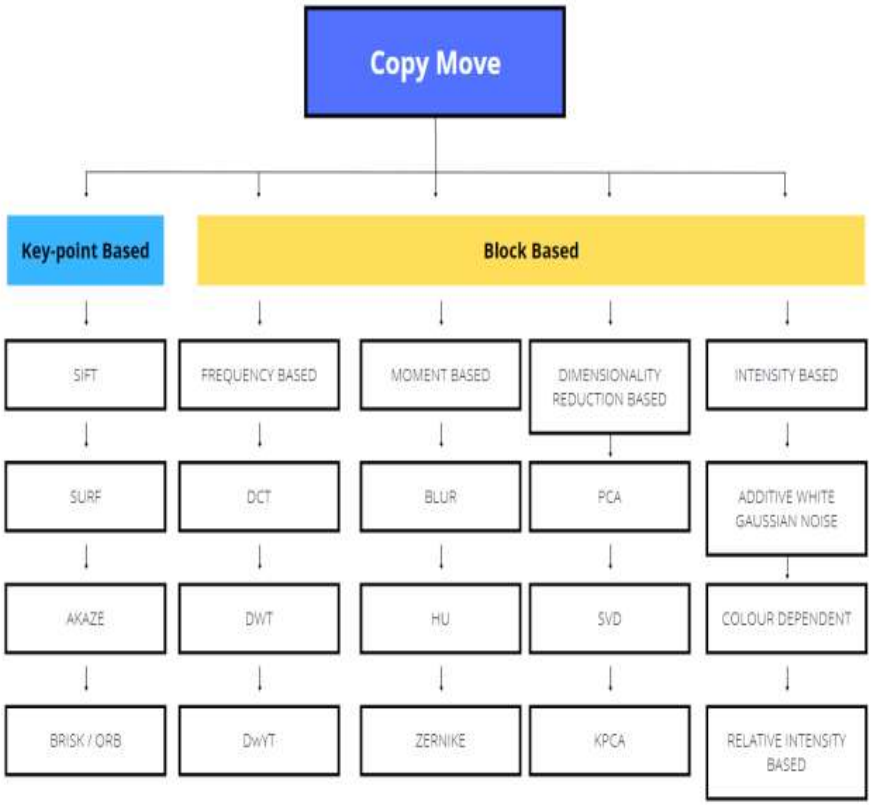

Figure 2. Categories of CMFD techniques

The paper is organized as follows. Section 1.1 gives an overview of the previous work on block based methods. The proposed methodology is discussed in Section2 and experimental results are given in Section 3 Finally, Section 4 draws conclusions.

Finally, the features are ordered depending on the similarity between subsequent pairings in order to determine if a block is false or real. A few scholars have investigated the use of the Fourier transform and fast Fourier transform for block-based forgery detection. The approach suggested in [2] uses Euclidean distance metrics to determine the veracity of the image block and local binary Pattern Histogram Fourier features collected from each overlapping block.

2. Methodology

The presence of duplicated areas in an image can be detected using CMFD algorithms. To try to look at all conceivable pairs of duplicated sections with different shapes and sizes would be computationally difficult because the form and size of the duplicated parts are unknown. The image is divided into overlapping halves for purpose. The blocks are then converted into vectors after each block has its features retrieved using DCT. Taking only the most 'L' significant coefficients using the Zigzag ordering of coefficients helps to reduce the dimension of the features which in turn shortens the processing time for feature matching. The blocks are then lexicographically sorted according to their features using radix sort. Each pair of adjacent blocks has their difference measured, and if the difference between two blocks is less than a predetermined threshold, the blocks are deemed comparable. In order to reduce false detection, the spatial gap between these blocks has been constructed. It is suggested to use the radial search strategy rather than exhaustive block matching. By just comparing the neighbours of suspected similar blocks, the proposed method speeds up copy-move forgery detection. The radial search approach is used to locate the neighbouring eight block neighbours after a match is discovered, thereby eliminating the sequential block comparison process. Fig. 3 shows the proposed CMFD system. First the given colour image is converted into gray scale image as shown in Eqn.1, where R, G and B are the red, green and blue colour values and I is the gray colour image.

$$I = 0.228R + 0.587G + 0.114B \quad (1)$$

Next the gray image of size M × N, is divided into small fixed-size overlapping blocks of ob × ob pixels, resulting in NoB number of blocks as shown in Eqn.2.

$$NoB = (M - ob + 1) \times (N - ob + 1) \quad (2)$$

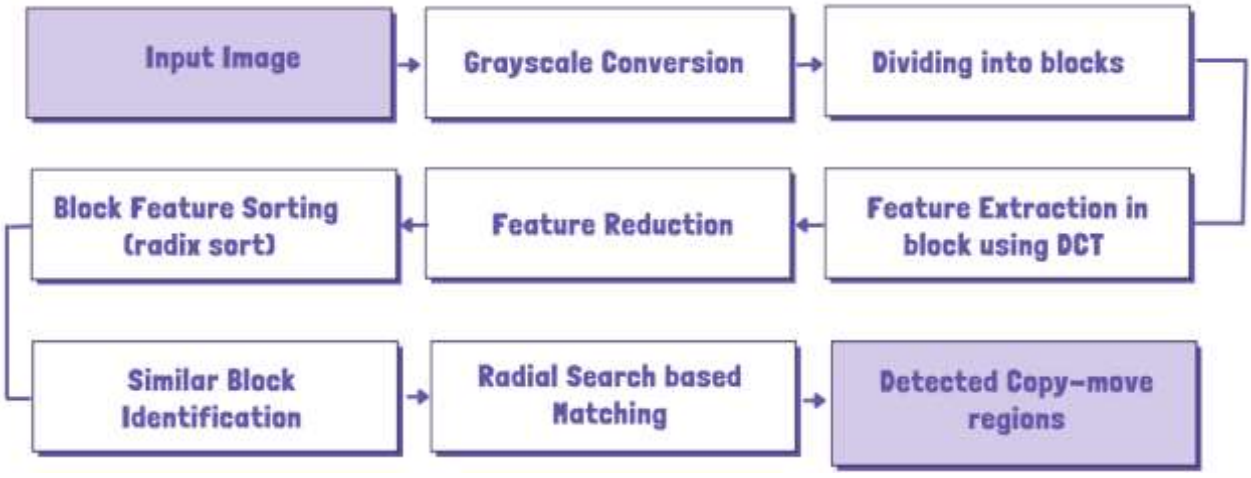

Figure 3. Proposed copy-move forgery detection method

The DCT coefficients serve as a feature representation for each block. The converted coefficients matrix has b2 elements if the block size is obxob. The blocks are transformed into vectors via a zigzag scan as shown in Fig. 4. DCT coefficients are same for similar blocks. For comparing blocks, low frequency coefficients are adequate. The DCT coefficient vector is truncated up to the 'R' coefficients to reduce the dimension of the feature vector for speeding up further processing. Then all the condensed block features are lexicographically sorted by radix sort [7] and saved in the sorted matrix M_s based on their "R" features.

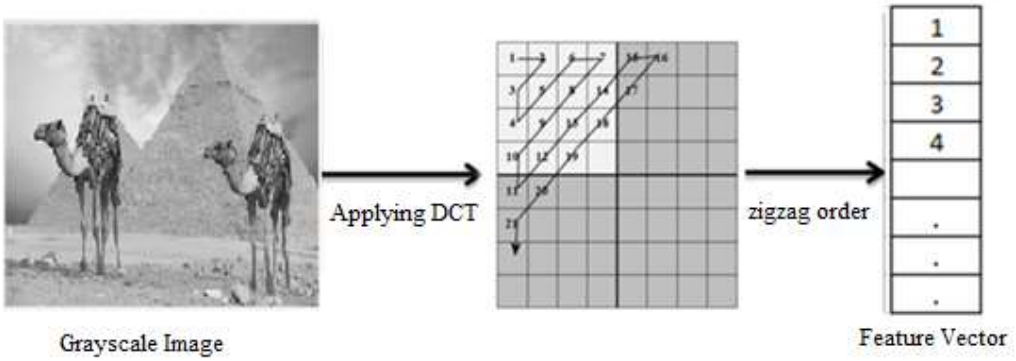

Figure 4. Formation of Feature vector

The next step is to determine the duplicated region. For this, the feature vectors of adjacent blocks M_{si} and $M_{si+1}$are considered and the difference between them is calculated as shown in Eqn. 3

$$D = \sum_{j+1}^{L} \left| MS_i^j - MS_{i+1}^j \right| / L \qquad (3)$$

where "R" denotes the feature vector's length. Two blocks are assumed to be comparable if D if is smaller than a threshold, "Th." In order to weed out false positives, Eqn. 4 also tests for spatial distance.

$$Dis = \sqrt{\left(P_i^x - P_{i+1}^x\right)^2 + \left(P_i^y - P_{i+1}^y\right)^2} \qquad (4)$$

where $(P_i^x, P_i^y)$and $(P_{i+1}^x, P_{i+1}^y)^2$are the locations of block *i* and blocki+1. Bocks whose distance is less than BD alone are considered. Finally, the matched regions are marked in the map image. The matched blocks are retrieved as MB1 and MB2 after a match is found, and their positions are set to (x1, y1) for MB_1 and (x2, y2) for MB_2.For each of the two matched blocks MB_1 and MB_2 eight neighbouring blocks (Ne_1, Ne_2,...Ne_8) are retrieved. The neighbouring blocks of MB_1 and MB_2 in the same direction are compared according to Eqn. 3. The proposed Radial Search algorithm is then applied and the flowchart of the same which is depicted in Fig. 5.The blocks lying in the same directions radiating from the center of blocks MB1 and MB_2 are compared. If the search reaches the boundary or if the blocks are not similar the search in that direction is halted. Else if blocks are similar, it is marked in the map image and the search is extended in the same direction until either search reaches the image boundary or the blocks are not similar. The process is repeated for all the other 7 neighbouring pixels in the other seven directions.

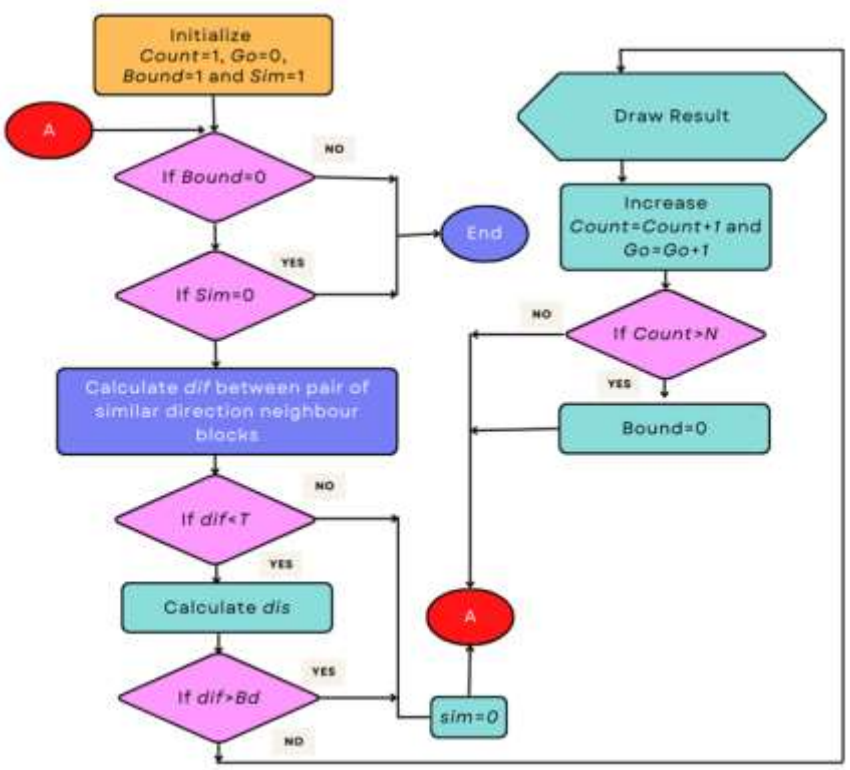

Figure 5. Flow chart of the Radial Search Algorithm

3. Experimental Results

The experiments were carried out on the Matlab R2016a, The images used in this experiments were synthesized using Photoshop. First the images were resized to 128 x 128 and the parameters used in this algorithm were found out empirically and were set as., o*b=9x9, Th = 0.2, BD = 10, R=20.*False Positive Rate (FPR) and True Positive Rate are used to evaluate the proposed system (TPR).In this work 30 synthesized images and 30 original images were considered for calculating FPR and TPR. Since synthesized images were used in this study no comparison was made with other methods seen in the literature.

$$TPR = \frac{No.of forged images correctly Identified}{Total No.of Forged Images}$$

$$FPR = \frac{No.of genuine images dentified as forged}{Total No.of Genuine Images}$$

The sample copy move forgery detected is shown in Fig. 6. The flower in Fig. 6(a) is copied and pasted in another region as shown in Fig. 6(b), to create a copy move forged image. The detected copy moved region is shown in Fig 6 (c). Table 1 shows the performance metrics.

(a) Original image (b) Tampered image (c) Result Image

Figure 6. Copy Move Forgery Detection Results

Table 1. Performance metrics of the proposed methods

TPR (%)	FRP(%)	Detection Time in Seconds
88.9	11.1	1.09

4. CONCLUSION

To speed up the copy-move forgery detection system a radial search method is proposed in this work. Features were extracted from each overlapping block by applying DCT, and the block is then transformed into a vector by taking only the most 'R' significant coefficients using the Zigzag ordering. The blocks are then lexicographically sorted according to their features using radix sort. Each pair of adjacent blocks has their difference measured, and if the difference between two blocks is less than a predetermined threshold, the blocks are deemed comparable. In order to reduce false detection, the spatial gap between these blocks has been constructed. t is suggested to use the radial search strategy rather than exhaustive block matching. By just comparing the neighbours of suspected similar blocks, the proposed method speeds up Copy move forgery detection. The radial search approach is used to locate the neighbouring eight block neighbours after a match is discovered, thereby eliminating the sequential block comparison process.

REFERENCES

1. Velmurugan, S., Subashini, T.S. (2020) "Dissecting the Literature for studying various Approaches to Copy Move Forgery Detection", International Journal of Advanced Science and Technology, Vol. 29, No. 4, pp. 6416 – 6438, ISSN: 2005-4238.
2. Badal Soni and Pradip, K. (2018), "Dual System for Copy-move Forgery Detection using Block-based LBP-HF and FWHT Features", Engineering Letters, 26:1, EL_26_1_20.
3. Cao, Gang; Zhao, Yao; Ni, Rongrong; Li, Xuelong (2014), "Contrast Enhancement-Based Forensics in Digital Images", IEEE Transactions on Information Forensics and Security, 9(3), 515–525.
4. Wang, Yang; Gurule, Kaitlyn; Wise, Jacqueline; Zheng, Jun (2012), "Wavelet Based Region Duplication Forgery Detection", Ninth International Conference on Information Technology: New Generations (ITNG) - Las Vegas, NV, USA, 30–35.
5. Muhammad, Najah; Hussain, Muhammad; Muhammad, Ghulam; Bebis, George (2011), "Copy-Move Forgery Detection Using Dyadic Wavelet Transform", Eighth International Conference on Computer Graphics, Imaging and Visualization (CGIV) - Singapore, 103–108.
6. Böhme, Rainer; Fong, Philip W. L.; Safavi-Naini, Reihaneh (2010), "Detection of Copy-Rotate-Move Forgery Using Zernike Moments", Lecture Notes in Computer Science, Information Hiding Volume 6387, 10.1007/978-3-642-16435-4(Chapter 5), 51–65. Zagha, Marco; Blelloch, Guy E. (1991), "Radix sort for vector multiprocessors", ACM/IEEE conference - Albuquerque, New Mexico, United States, Proceedings of the Supercomputing, 712–721.
7. Velmurugan, S., T.S. Subashini., (2022) "Binary descriptors for Copy-Move Forgery Detection in Digital Photographs,", Proceedings of the 6thInternational Conference on Computing Methodologies and Communication (ICCMC 2022), Erode India, pp. 1359-1366. IEEE Xplore.