International Journal of Innovative Research in Science and Engineering
Volume 08, Issue 06, 2022
www.ijirse.com
ISSN: 2454-9665

COPY MOVE FORGERY DETECTION WITH QUADTREE DECOMPOSITION AND SEGMENTATION

Grandhi Supriya, Atukuri Dhana Lakshmi, Akula Naga Chandrika, Gali Makara Jyothi

grandhisupriya2002@gmail.com,atukuridhanalakshmi7@gmail.com,akulanagachandrika@gmail.com, jyothigmk999@gmail.com

Under the Guidance of **B. THRIVENI,** M. Tech.**,** Assistant Professor**,** Department of Electronics and Communication Engineering, Tirumala Engineering College (JNTUK), Narasaraopet, Jonnalagadda, Andhra Pradesh, Guntur District – 522601.

Guide Email: bollavaraputhriveni1@gmail.com

Abstract— The increasing usage of digital images and the wide availability of easy-to-use image editors have made the authenticity of images questionable. Copy-move is one of the mostapplied forgery types. The keypoint-based copy move forgery detection methods in the literature cannot detect forgeries with smooth regions. In this paper to overcome this problem, a new copy-move forgery detection technique is proposed. In the proposed scheme, the input image is segmented into two sub-image via Quadtree Decomposition. The sub-images are labeled as smooth and textured. The textural form of the smooth labeled segment is obtained based on LBPROT approach. Then the keypoints are extracted from both textured segment and textural form of the smooth segment. After that, they are matched with each other to obtain forgery clues. By matching the extracted keypoints, it is revealed whether the image is forged or not. The experimental results show that the proposed method is robust under scaling and rotation attacks.

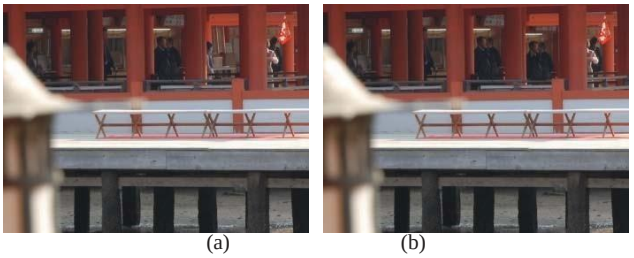
Keywords—copy move forgery; Quadtree decomposition; segmentation based forgery detection;

I. INTRODUCTION

Digital images are frequently used in our daily lives and have wide use in many important fields such as medical systems, journalism, evidence in a court, etc. Easy use of freely available image editing software made it possible to create forged images by malicious users. These forgeries are made so professionally that they are indistinguishable from the original ones. So, to prove the authenticity of digital images has become an important topic in recent years.

The most common type of digital image forgery detected by passive methods is copy move forgery. In this type of forgery, a region copied from the image is pasted to another region of the image to hide or replicate a region or multiple regions without leaving visual clues. An example of copy moveforgery operation is given in Fig. 1. While Fig. 1(a) shows the original image, its forged version is given in Fig. 1(b). In this scenario, the two women in the picture are aimed to be hidden.For this purpose, the region that two men place between columns is copied and moved to the right area, where a womanstands, so the woman in the image was hidden.

The copy move forgery detection methods are divided into two classes according to the main steps of the algorithms to obtain statistical features from input image: Block based and Keypoint based methods.



(a) (b)

Fig. 1. (a)Original image (b) Forged image

The methods in the first group are based on finding similar features extracted from sub-blocks of the suspected image. For this purpose, firstly divide the input image into fixed- size circular/square overlapping blocks. Then generally, to obtain spectral features (frequency-based features), texturalfeatures, moment invariants, or geometric features via log-polartransform the feature extraction step is realized. After obtainingfeature vectors of each block, they are lexicographically sortedto make the similar vectors closer and the most similar vectors are matched. At the last stage, if any, incorrect matches are eliminated using the filtering process. The feature extraction of each block and matching phases are time-consuming steps, this is the disadvantage of these methods. To cope with the higher execution time problem of the block-based methods researchers proposed keypoint-based methods. In this scheme, keypoints are extracted from an input image which represents interests points of the image and do not change even after somegeometric transformations such as rotation, scaling, etc. Besides, the descriptor vectors of each keypoint are extracted and then matched to each other to determine suspicious regions.Although keypoint-based methods have the advantage in termsof lower execution time and invariance to geometric transformation attacks, they fail if the forgery was done with low contrast region. In this work, we aim to use the priorities ofthese methods to suggest better copy move forgery detection when compared to similar works in the literature.

International Journal of Innovative Research in Science and Engineering
Volume 08, Issue 06, 2022
www.ijirse.com
ISSN: 2454-9665

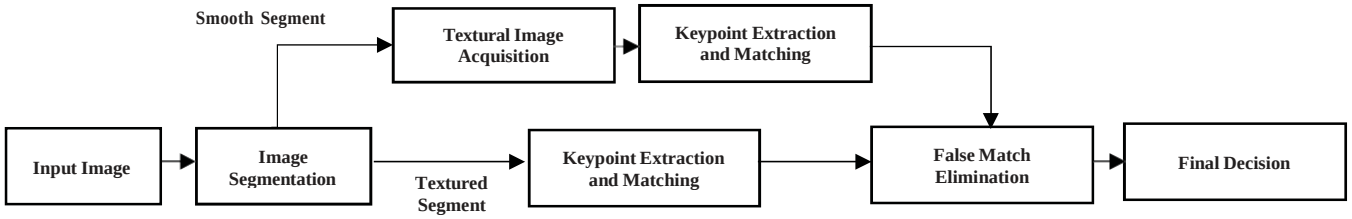


Fig. 2. Main steps of the proposed method

Our proposed scheme firstly extracts suspicious forge regions using a dense keypoint based approach. For this purpose, structural texture information of the image is acquired using Local Binary Pattern Rotation Invariant (LBPROT) to make the keypoint extraction techniques more successful. Then, Scale Invariant Feature Transform (SIFT) interest points on the textural image are obtained. After keypoint matching via their descriptor vectors, a rectangular region around keypoint matches is considered as suspicious region.

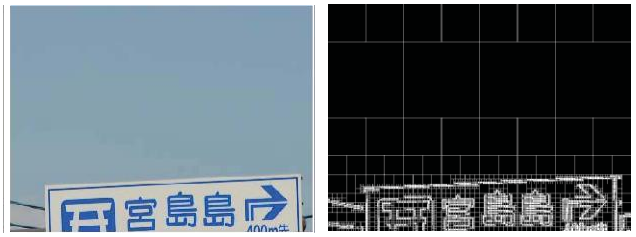
The paper is organized as follows; While the details of the proposed method will be given in the second section, the experimental results will be given in the third section, and the final evaluations will be given in the last section.

II. PROPOSED METHOD

In this work, to overcome the deficiency of the copy move forgery detection methods, a new method is proposed with considering the advantages and disadvantages of the methods in the literature. The method firstly segments the input image into two sub-segments, smooth segment and textured segment using the Quadtree Decomposition based approach. For the smooth segment, the textural form of this segment is obtained by using LBPROT to obtain more significant keypoints. For the textured segment the keypoints are obtained from this segmented image. The keypoints are obtained using the SIFT (Scale Invariant Feature Transform) algorithm to provide geometric transformation invariance. After keypoint matching possible false matches are eliminated via RANSAC (Random Sample Consensus). Finally, if there are enough matches, the image is revealed to be forged or not. Fig. 2 shows the block diagram of the method and the details of the mentioned steps will be given in the following sections.

A. Quadtree Decomposition based Segmentation

Quadtree decomposition is an image analysis approach that splits the image into more homogeneous four blocks than it does [12]. With this technique, information about the structure of the image can be obtained. The algorithm divides the image into four squares of the same size. It is checked whether each sub-block meets the homogeneity criterion. If a block does not meet this condition, the block is again split into four sub-blocks. In Figure 3 an example of the block representation of the Quadtree blocks are combined to form a smooth segment, creating a smooth segment image and with other blocks form a textured segment. Thus, the image is divided into two as textured and smooth segment. If there is no smooth block in the image, the whole image is evaluated as textured.



(a) (b)

Fig. 3. (a)Input image (b) Block representation of the Quadtree Decomposition

Figure 4 shows the two image obtained by Quadtree Segmentation of Figure 3(a). While Fig.4 (a) shows smooth segment image, (b) shows textured segment image.

(a) (b)

Fig. 4. (a)Smooth Segment Image (b) Textured Segment Image

B. Keypoint Extraction and Matching

After image segmentation, for smooth segment image, the textural form of it is obtained before keypoint extraction. The proposed method reveals the structure of these regions by using the LBPROT operator. Thus, the more meaningful keypoints can be obtained from the textural form of the image. LBPROT, the rotation invariant version of the basic LBP. LBP is given in (1),

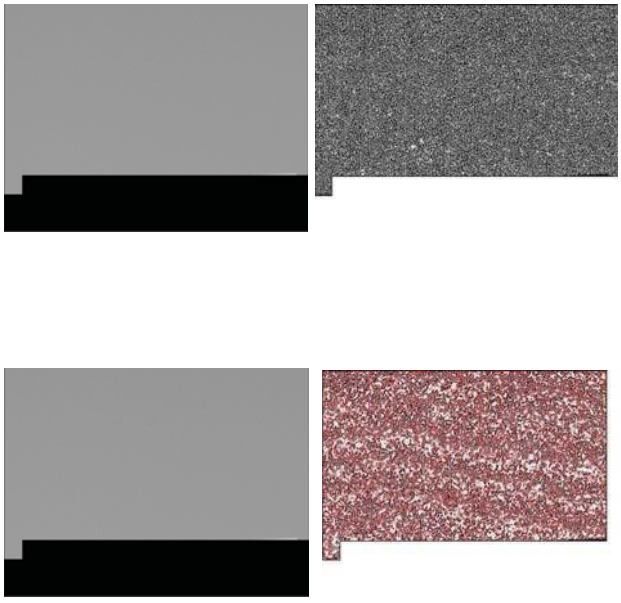
$$LBP(x_p, y_p) = \sum_{p=0}^{7} s(i_p - i_c)\, 2^p \quad (1)$$

Let I represent a gray level image and $i_c = I(x, y)$ be a pixel. Circular neighborhoods ∂ of the point with radius r, are

International Journal of Innovative Research in Science and Engineering
Volume 08, Issue 06, 2022
www.ijirse.com
ISSN: 2454-9665

Decomposition is given. In this representation, the smaller block means that the region of the image is more textured that is, there is no homogeneity. Based on this, it is understood that the quads with small blocks are more complex and the quads that do not divide into the lower block are smooth. In the proposed method after Quadtree Decomposition of the input image, the blocks greater than 64x64 are considered smooth blocks. And all small

$x\ y$



denoted by i_p, the point is obtained as in (2). (In this work as a result of experiments taken as ∂=3 and r=8.) The sampling points represented P are obtained similarly.

$$i_p = I(x_p, y_p), p = 0, \dots P-1$$
$$x_p = x + rcos(2np/P)$$
$$y_p = y - rsin(2np/P) \quad (2)$$

When $ROR(x,\ i)$ denotes circular bitwise right rotation of bit sequence x by i steps. LBPROT operator given in (3) chooses the minimum LBP code among the results of circular bitwise operations. Minimum LBP code, and obtained $LBPROT^{ri}_{p\ p}$ is used to label the center pixel of the current block. In Fig. 5. Obtained textural form of the smooth segmentis given.

$$LBPROT^{ri} = min\ ROR(LBP(x\ ,y\ ), i) \quad (3)$$
$$x_p,y_p \qquad i \qquad p\ \ p$$

(a) (b)

Fig. 5. (a)Smooth segment image (b) Textural form of the smooth segment

The method extracts keypoints using Scale Invariant Feature Transform (SIFT) algorithm both from the obtained textural image of smooth segment and texture segment [14] SIFT keypoints are robust to geometric changes, illumination variations, JPEG compression and noise addition. In Fig. 6 the obtained keypoints are shown both from smooth segment image and textural form of the smooth segment image. While no keypoints are found from smooth segment image, 25726 keypoints are found from textural form of it.

(a) (b)

Fig. 6. Obtained keypoints (a)No keypoints found (b) 25726 keypoints are found

International Journal of Innovative Research in Science and Engineering
Volume 08, Issue 06, 2022
www.ijirse.com
ISSN: 2454-9665

an iterative scheme. The matches that suit this model are labeled as 'inlier', while others are labeled as 'outlier' and removed from the matching matrix M. In Figure 7 an example forgery image is given from GRIP dataset. The matched keypoints are shown in (a) with lines. There were incorrect matches because the image contains very similar patterns. This problem was overcome by using the RANSAC algorithm and outliers are eliminated. The inliers are shown in (b).

(a) (b)

Fig. 7. (a) The matched keypoints before RANSAC (b) The matchedkeypoints labeled as 'inliers' via RANSAC

III. EXPERIMENTAL RESULTS

In the proposed method extracted keypoints are matched via generalized 2NN (g2NN) matching technique in this work [9].

It is the general form of the 2NN test with iteration. Assume that D=$\{d_1, d_2, \ldots d_{n-1}\}$ represents sorted Euclidean distances between a descriptor and other descriptors. 2NN method matches the keypoints if the $d_1/d_2 < T$condition is met. g2NN uses iterating d_1/d_2 tests until ratio becomes greater than the predefined threshold T. (In this work T=0.6) If iteration stops at k $1 \leq k < n$, this means that index of the last keypoint which ensures the condition $d_{k-1}/d_k < T$ is k.

B. False Match Elimination

Random Sample Consensus (RANSAC) algorithm that is proposed by Fischler et. al. is utilized by the method to estimate inliers and outliers of matches [15]. It estimates general parameters of a certain model between matched keypoints with

In this section, we give some experimental results to show the effectiveness of the proposed method and to compare it with some state-of-the-art keypoint based methods [9, 10, 11]. [11] has been proposed to prevent failure of keypoint-based methods in smooth regions. All measurements are performed on a desktop computer with 3.4-GHz Intel Core i7 CPU and 8 GB RAM memory, running Matlab R2015a. Publicly available image dataset GRIP [4] is used to evaluate the performance of the proposed scheme and the other works. GRIP dataset consists of 80 uncompressed PNG true color images of size 768 × 1024 pixels. Dataset includes realistic copy move forgeries such that size of the forged region is approximately less than 1% of the image.

The performance analyses were done at image-level. In the image-level, the obtained results are evaluated according to forged/original image label. In the evaluations, Precision, Recall and F-measure metrics are used, which are defined in (4). T_p, F_p and F_N have different meaning. T_p is the number of images that have been correctly detected as forged, F_P is the number of incorrectly detected forged images and F_N is the falsely missed forged images.

$$Precision = \frac{T_P}{T_P + F_P}, \qquad Recall = \frac{T_P}{T_P + F_N},$$

$$F - measnre = 2x\frac{Precicion\ .RecaII}{Precicion+RecaII} \tag{4}$$

F-measure is the harmonic mean of Precision and Recall, so it considers both false positives and false negatives into account with a single value and F-measure ∈ [0, 1]. The closer F-measure value are to 1, the higher accuracy in detecting forgery pixel.

The first experiment is realized under plain copy move forgery. 80 images in dataset with plain copy move forgery are used and obtained average F-measure results of the methods are given in Table 1. As seen in the table, the proposed method has higher average F-measure value compared other methods.

International Journal of Innovative Research in Science and Engineering
Volume 08, Issue 06, 2022
www.ijirse.com
ISSN: 2454-9665

TABLE I. AVERAGE F-MEASURE UNDER PLAIN COPY MOVE FORGERY

Methods	F-measure
[11]	0,67
[12]	0,72
[13]	0,86
Proposed	0,90

In the second experiment, the robustness of the method under scaling attacks was tested. In Fig. 7 the obtained Average F-measure values of the methods under scaling attack are given with graphical representation.

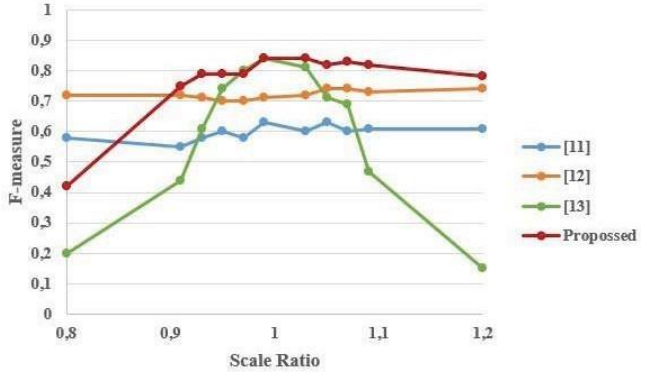


Fig. 7. Average F-measure values of the methods under scaling attack

In the last experiment, the robustness of the method under rotation attack was tested. In Fig. 8 the obtained Average F-measure values of the methods under rotation attack are given with graphical representation.

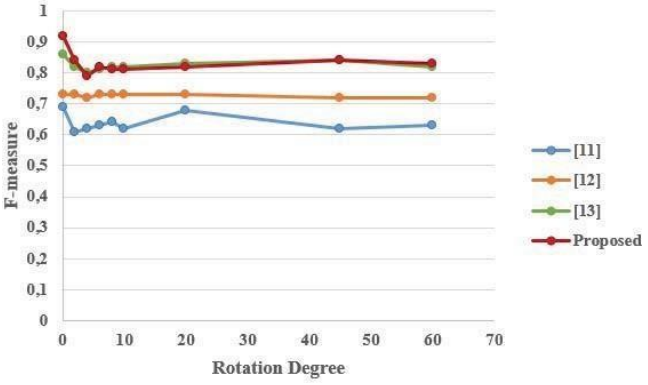


Fig. 8. Average F-measure values of the methods under scaling attack

IV. CONCLUSION

In this work, we proposed a new method to detect copy move forgery. The first stage segments the input image into smooth segments and textured segments. In order to extract more meaningful information from smooth segments, texture information of these segments are obtained with LBPROT. After that SIFT keypoints are obtained both from textural form of the smooth segments and textured segments. And then the keypoints are matched. After false match elimination the image revealed as forged or not. According to the given experimental results using online available dataset GRIP, we can say that proposed scheme has better detection results even for challenging forgeries that are made with smooth regions or forged image have similar but genuine regions. Results indicate that the proposed method detects copy move forgery attacks with higher accuracy when compared to similar works.

APPENDIX A

This work was supported by the Scientific and Technological Research Council of Turkey (TUBİTAK) with Project No: 119E045

REFERENCES

[1] G Fridrich, A. J., Soukal, B. D. and Lukáš, A. J., Detection of Copy-Move Forgery in Digital Images, Digital Forensic Research Workshop (DFRWS), 2003.

[2] Bravo-Solorio, S. and Nandi, A.K., Exposing Duplicated Regions Affected by Reflection, Rotation and Scaling, Intl. Conference on Acoustics, Speech and Signal Processing, Mayıs 2011, Prague, Proceeding Book: 1880–1883.

[3] Ryu, S., Kirchner, M, Lee, M. and Lee, H., Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments, IEEE Transaction on Information Forensics and Security, 8, 8 (2013) 1355–1370.

[4] D. Cozzolino, G. Poggi, and L. Verdoliva, "Efficient dense-field copy-move forgery detection," IEEE Transactions on Information Forensics and Security, vol. 10, no. 11, pp. 2284–2297, 2015.

[5] Ustubioglu, B., Baykal, E., Muzaffer, G., and Ulutas, G. Blur Invariant Image Forgery Detection Method Using Local Phase Quantization. Journal of Energy and Power Engineering, 10(6), 358–363. 2016

[6] X. Bi and C.-M. Pun, ''Fast reflective offset-guided searching method for copy-move forgery detection,'' Inf. Sci., vols. 418–419, pp. 531–545, Dec. 2017.

[7] Bi X, Pun CM (2018) Fast copy-move forgery detection using local bidirectional coherency error refinement. Pattern Recogn 81:161–175.

[8] Huang, Y., Lu, W., Sun, W. and Long, D., Improved DCT Based Detection of Copy Move Forgery in Images, Forensic Science International, 206 (2011) 178–184.

[9] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, L. Del Tongo, and G. Serra, "Copy-move forgery detection and localization by means of robust clustering with J-linkage," Signal Processing: Image Communication, vol. 28, no. 6, pp. 659–1669, 2013.

[10] Li J, Li X, Yang B (2015) Segmentation-based image copy-move forgery detection scheme. IEEE Trans Inf. Forensics Secur 10(3):507–51

[11] M. Zandi, A. Mahmoudi-Aznaveh and A. Talebpour, "Iterative Copy - Move Forgery Detection Based on a New Interest Point Detector," Transactions on Information Forensics and Security, 2016.

[12] Smith, J. et al., "Quad-Tree Segmentation for Texture-Based Image Query" Proceeding ACM Multimedia 94, pp. 1-15, San Francisco, 1994.

[13] Ojala T, Pietikäinen M, Mäenpää T: Multiresolution gray-scale and rotation invariant texture classification with local binary patterns, IEEE Trans Pattern Anal Mach Intell. 24(7):971–87, 2002

[14] Lowe, D. G., Object Recognition From Local Scale-Invariant Features, International Conference on Computer Vision, September 1999, Kerkyra, Proceeding Book: 1150-1157.

[15] M. A. Fischler and R. C. Bolles, "Random sample consensus: A paradigm for model fitting with applications to image analysis and automated cartography," Commun. ACM, vol. 24, no. 6, pp. 381–395, Jun. 1981