IJARCCE

ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101208

AN EFFICIENT KEYPOINT FEATURE EXTRACTION TECHNIQUES TO DETECT COPY MOVE IMAGE FORGERY

Mukala Gayatri [1], Ch. Srinivasa Rao [2]

[1]MTech scholar, Department of Electronics and Communication Engineering, University College of Engineering, Vizianagaram, Jawaharlal Nehru Technological University Kakinada, Andhra Pradesh

[2]Professor of Department of Electronics and Communication Engineering, University College of Engineering, Vizianagaram, Jawaharlal Nehru Technological University Kakinada, Andhra Pradesh

Abstract: Digital images are highly manipulated without degrading their visual quality and resolution with advanced and easily available software's. Copy Move Forgery (CMF) is a common manipulation procedure in digital images that involves copying the object or segment of an image and partially pasting it on another area of the same image. Many block-based detection methods are present to identify the copy move forgery in images. However, their performance got deteriorated considerably under the shape of the regions that cannot be exactly identified, and shows limited robustness based on performance metrics like precision and recall. A novel and robust algorithm is introduced in this paper to overcome that problem. The use of non-overlapping segmentation compared to the overlapping method used is to reduce the computational complexity compared to the regular blocks and irregular blocks to obtain better performance to find the forged region accurately. Here, input images are segmented using the SLIC algorithm, and to detect forgery, the key point features are extracted from each block using the Scale Invariant Feature Transform (SIFT) algorithm along with Speeded Up Robust Feature (SURF). Block matching and labelled feature point matching is used to detect the forgery from these extracted results. Block matching process is used to identify the distance between regions of the divided images. Copy move forgery region is identified by the similarities between the features of the image. Precision, Recall and F-measure of the input image are used to assess the performance of proposed scheme. It is observed that 98.97% precision is achieved with the SLIC algorithm on the MICC-F220 database.

Keywords: Image forgery, Copy-move, SLIC, SIFT, SURF, LPF

I. INTRODUCTION

Manipulation of a digital images has become very simple in recent years due to the free availability of image editing software's. These software's can edit an image in such a way that its quality is preserved while no visible changes are made. It has become an important tool to transfer information within no time through various advanced technologies available these days. With the increased usage of digital images in various fields, misuse by tampering the actual images is being carried out by unethical and immoral people. It has become critical to find whether the image is original or tampered one. Hence, there is an urge to find the authenticity of these digital images. Various techniques are found for this purpose. Copy move forgery is widely used technique for manipulating digital images. Essentially, forgeries are implemented in two ways. To begin, hide an object or part of an image by copying and pasting the area onto another area of the same image. With a small change in some qualities "such as size" by copying the object and pasting this object on another area of the same image. To identify the copy, move forgery region different image processing techniques are used, such as blurring, compression, and scaling etc. The debasement detection methods are can be classified into two methods one is block based method and another method is key point-based method. In block-based method segmentation and segmented block matching algorithms are performed, in key point-based method the debasement region extracted algorithms are computed. In the existing block – based techniques to identified the forgery region, the images are segmented in the form of overlaying blocks regular manner. At rest, even the existing methods locate the forgery region very well, but those methods failed to extract key point features with accuracy results and perform the less accuracy to identify the tampered region. The remainder of the paper is laid out as follows. The SLIC algorithm, as well as key point features extraction and Label Feature Points, are discussed in the following section. Section 4 contains the Experimentation and Results. Finally, in the final section, a conclusion and future enhancements are provided.

II. RELATED WORK

A block- based copy move tampered technique using the quantized DCT coefficients is presented in [1]. This method is able to survive against noise, compression and retouching. yet it is unable to detect the forgery region in case of copied blocks in performance metrics. In order to perform the matching by the SIFT algorithm a single key point is matched with cluster key point [2]. The content of two matching object is compared by using object shape and texture analysis. Lower false positive rate is observed in this work. An improved block-based method is presented in [3] by dividing the image into circular blocks and extract the local image features based on the Discrete Radial Harmonic Fourier Moments (DRHFMS). It is observed that it requires more computational cost. In paper [4] the key point descriptor matching is performed based on the SIFT algorithm using 2NN procedure. It is observed that some of the improvements are need to detect the copied region of image. An efficient key point matching is performed by the SURF algorithm along with MSER. It is observed that it could not be able to identify the copied shape of the region of regular and irregular blocks [5]. The SIFT key point extraction algorithm [6] is used to extract the features from the image regions, these regions are classified into smoothed and non-smoothed regions. For smoothed region zernike moments and non-smoothed regions SIFT algorithm is used. It is observed that computational cost is high. In [7] invariant quaternion exponent moments (QEM) are used for feature extraction. This method is efficient to detect the copied regions in images and fails to detect the copy move region using different performance metrics. Block-based methods are less robust when compared to key point based techniques [8].The existing block-based techniques has drawbacks. Because the process was based on block matching, as the image size increased, so did the time complexity and algorithm complexity, as well as the features extracted using block-based approaches. If the copy moves regions have some transformations, block-based methods cannot precisely identify the copy move areas. The shape of the regions cannot be precisely identified using block-based approaches. The process's performance, as measured by performance metrics, indicates that the approaches need to be improved further.

III. BACKGROUND

3.1 Speeded up robust features(SURF)

The SURF algorithm contains the Gaussain second order derivatives to assign the key point features.

$$I_{integral}(\mathrm{x},\mathrm{y}) = \sum_{i=0}^{i\le x}\sum_{j=0}^{j\le y} I(x,y) \qquad (1)$$

SURF is a **scale and** rotation invariant interest point descriptor is used to extract key point feature descriptors and matching is performed based on the finding the points **correspondence between** the both of the images. The main steps of the SURF algorithm is structed as follows. 1)Interest point detection is based on the convolution of the gaussian second order derivative to choose the box filters .

$$\det(H_{approx}) = C_{xx}C_{yy} - 0.9(C_{xy})^2 \qquad (2)$$

2) key point detection and SURF point descriptor extraction is based on the intergral image and hessian matrix, the length of the SURF descriptor vector is 64 is extracted from each key point, in this SURF descriptors are formed based on the haar wavelet responses and are added to the each sub block.

$$V = (\Sigma d_x, \Sigma d_y, \Sigma|d_x|, \Sigma|d_y|) \qquad (3)$$

3)SURF descriptors matching to perform in images based on the Euclidian distance, in the both image of key point descriptors. Some times in the images many key point descriptors are matched. This performance is based on the immediate neighbor and the alternative neighbor is smaller than the threshold vale. Based on this relevant keypoints are matched.

3.2 Scale Invariant Feature Transform (SIFT)

The key points are extracted based on the Scale Invariant Feature Transform (SIFT) algorithm. It provides set of image characteristics that are unaffected by several of the difficulties encountered in different techniques, such as object scaling and rotation, and are therefore resistance to the effects of noise in the image. SIFT retrieves the image and converts it into a large set of local feature vectors during image feature generation. Each of the vectors is stationary to the object's scaling, rotation, or interpretation (image). Mainly the SIFT algorithm involves four major steps. It detects the keypoints based on the extrema key point features of scale- space. For this detection the scale space extrema contain in the image DOG (Difference of Gaussian) pyramid, and performs convolution operation of the image and gaussian operation. To detect the unwanted keypoints SIFT algorithm is used. The SIFT algorithm processed the following steps based on the image contributions. The first step is the to detect the keypoints and scales of the image, and then it removes unstable and poor contrast of image edge points because to improve the efficiency noise intransigence of the matching.

Extrema detection of scale space

$$L(X, Y, \sigma) = G(X, Y, \sigma) * I(X, Y) \qquad (4)$$

Location of keypoints:

After perfrormance of Extrema detection of scale space it evulates the so many key points, in this some of the keypoints are unstable. In this it allows the stable keypoints based on the location, scale and curvatures by comparing the neighborhood pixels. For each sample contains 4 x 4 array location and 8

Orientation position:

The **key point** descriptors are generated based on the rotation and image gradient directions. And the **key point** orientation is calculated from the orientation histogram of the local **gradients**. For each sample contains 4 x 4 array **location and 8 orientation** bins in 128 element dimension of key point descriptor. After keypoint descriptor is com[puted based on before operations then matching is perfomed .

4. PROPOSED METHOD

The feature point based and block based matching processes are used in the forgery detection process in photographs. The key point features were calculated of the input image. With the help of the Simple Linear Iterative Clustring (SLIC) algorithm, the pictures were over segmented. The hybrid algorithm SIFT and SURF segment the images the key point features determined from the segmented image. The Scale Invariant Feature Transformations (SIFT) process was used to extract the key point features. The feature descriptors are constructed by extraction of the square sub regions of the wavelet transform of the interest points. Labeled feature points (LPF) were calculated from the extracted blocks features. To identify the forgied regions in the images, the LPF are matched. The process's performance is measured using perfomance metrics such as precision and recall.

Flow diagram

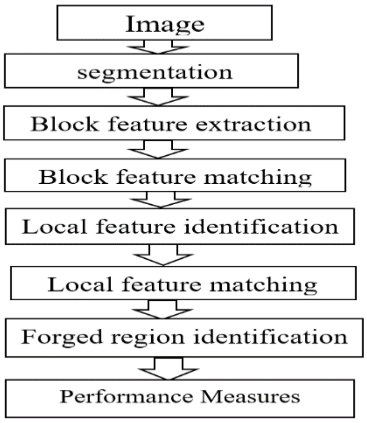

Fig.1 Proposed algorithm flow diagram

As illustrated in Figure.1 the host image is over segmented using a simple linear iterative clustering algorithm (SLIC). The feature points are then extracted from each block. To locate labelled feature points to perform the block feature matching. By this method the suspected forgery regions are identified and then performance is measured.

A. Pre-processing:

In this section the input image is recomputed into uniform size. And the RGB image is converted into grayscale image.

B. SLIC Segmentation

SLIC algorithm is familiar to use extract the super pixel blocks of an image based on color similarity and distance on image plane. SLIC accommodates the k-means clustering to generate the super pixels. The number of super pixels and their compactness can be easily adjusted. SLIC is a five dimensional [labxy] space. In CIELAB color space, the pixel vector indicates the dimension [lab] and position of the pixel is [xy]. Assuming an image has N pixels, k cluster centres are initialised with the interval S = $\sqrt{N/K}$ from all pixels, and these cluster centres are moved to the minimum gradient value in a 3 x 3 neighbourhood. For a new cluster centre, the SLIC algorithm searches the 2s X 2s area around the cluster centre and takes the average value of the pixels in the super pixel. To stable the threshold range and moving distance of the cluster centre the insistent searching process will be extended. The SLIC method was used to pre – segment the original images into super pixels, and information in the super pixels was transferred to a matrix.

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101208

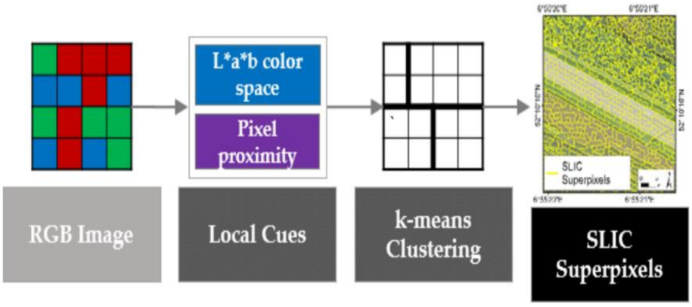

Fig.2 Processing pipeline of SLIC segmentation

In clustering process to avoid the seed locations in image edges. To get the similarity degrees between for each super pixel is calculated between itself and nearest seed, and assign the label of the most similar seed to this pixel.

The particular steps are as follows:

1: Is a set of five-dimensional cluster centre parameters Ck = [lk, ak, bk, xk, yk] T is computerized by the grid stepped as
S = $\sqrt{N/K}$ and then each pixel is computerized afterwards.
2: The clustering centre is moved to the lowest gradient positions of n x n neighbourhood location.
3: For every clustering centre of Ck this process is repeated.
4: To identify the surrounding clustering centres from the
2s x 2s square area the best matching pixels are assigned.
5: The novel centre pixels are calculated based on the segmented super pixels and calculated residual error.
6: Step 2 and 4 repeated, and the super pixel generation will be end to the minimum error.

B. Keypoints Feature Detection and Extraction

The key points are detection and extraction are based on the Scale Invariant Feature Transform (SIFT) algorithm and Speeded Up Robots Features (SURF). These are providing set of image characteristics that are unaffected by several of the difficulties encountered in different techniques, such as object scaling and rotation, and are therefore resistance to the effects of noise in the image. SIFT retrieves the segmented image and converts it into a large set of local feature vectors during image feature generation and extraction.

C. Key Point Feature Matching

The extracted key point features are used to locate the forgery region of image. To identify the forgery region of the segmented blocks of the image the matching process is performed based on the SURF and SIFT. The SURF and SIFT algorithms perform the so many matching descriptor pairs are drawn. To identify the specific matched pairs of the image based the same shift vectors then the threshold value is calculated. And finally, the matched region blocks are drawn out.

D. Label Feature Points

After collecting the LPF (labelled feature points), we must identify the forgery region. As forgery regions, the extracted LPF regions are used. The super pixels are obtained by the segmentation of the host image to improve the accuracy of the forgery region, algorithm of LPF consists the obtain suspected regions (SR) replace the large super pixels with small super pixels. Based on the following steps the labelled regions are identified and get the merged regions to get detection results.

In step–1, Let us consider

$$LPF = \langle LP_1, \overline{LP_1}\rangle, \langle LP_2, \overline{LP_2}\rangle, \ldots, \langle LP_n, \overline{LP_n}\rangle\ \langle LP_1, \overline{LP_1}\rangle\ represents\ a\ matched\ feature\ point\ pair, I$$
$$represents\ the\ I\ th\ labelled\ feature\ point\ pair$$
$$I\ = 1,2, - - n\ and\ n\ is\ the\ total\ number$$
$$of\ feature\ points\ in\ LFP,$$

The suspected region will be obtained by the replacement of small super pixels in the labeled feature points.

SR=$\{\langle LS_1, \overline{LS_1}\rangle, \langle LS_2, \overline{LS_2}\rangle,\ \ldots\ , \langle LS_n, \overline{LS_n}\rangle\}$.

To the result of the forgery region extraction algorithm, nearby shading highlight is the same as that of the speculated districts, the neighbour super pixels are converged into the contrasting presumed districts. This combining procedure results in blended districts (MR). Finally, morphological operation is linked to this consolidated area in order to procedure the distinguished duplicate move falsification districts.

The neighbouring blocks are identified for each suspected region SR_i= $\{\langle LS_i, \overline{LS_i}\rangle$

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101208

SR_i _neighbour = $\{\langle LS_i\_\Theta, \overline{LS_{i\_\theta}}\rangle$ where
$\Theta = \{45^\circ, 90^\circ, 135^\circ, 180^\circ, 225^\circ, 270^\circ, 315^\circ, 360^\circ\}$;

$$F_C\_LS_i = \frac{R(LS_I) + \mathrm{G}(LS_i) + \mathrm{B}(LS_i)}{3} \quad (5)$$

$$F_C\_\overline{LS_i} = \frac{R(\overline{LS_i}) + \mathrm{G}(\overline{LS_i}) + \mathrm{B}(\overline{LS_i})}{3} \quad (6)$$

$$F_C\_LS_i\_\Theta = \frac{R(LS_{I\_\Theta}) + \mathrm{G}(LS_{i\_\Theta}) + \mathrm{B}(LS_{i\_}\Theta)}{3} \quad (7)$$

$$F_C\_\overline{LS_i} = \frac{R(\overline{LS_i}) + \mathrm{G}(\overline{LS_i}) + \mathrm{B}(\overline{LS_i})}{3} \quad (8)$$

The suspected regions of local features are satisfying the following conditions:

$$|F_{C\_LS_i}\_F_C\_LS_{i\_\Theta}| \leq \mathrm{T}\, R_{sim} \quad (9)$$

$$|F_{C\_\overline{LS_\iota}}\_F_C\_\overline{LS_{\iota\_\Theta}}| \leq \mathrm{T}\, R_{sim} \quad (10)$$

Where $F_{C\_LS_i}$ *and* $F_C\_LS_{i_\Theta}$ is the suspected region of local colour features $SR_i = \langle LS_{i,}\overline{LS_\iota}\rangle$; $F_C\_LS_i\_\Theta$ and $F_C\_\overline{LS_\iota\_\Theta}$ are the local colour features of its neighbouring blocks. SR_i neighbor=$\langle LS_i\_\Theta, \overline{LS_\iota\_\Theta}\rangle \mathrm{T}R_{sim,}$ *is to measure the threshold similarity between the* local colour features. Finally, the structural element used in the close operation is defined in this step as a circle whose radius is proportional to the size of the host image. To get the shape of the region the to perform close operation, this operation will apply to fill the gaps between the merged regions.

5. EXPERIMENTATION AND RESULTS

In this section, the standard database was considered for experimental purposes, the propose method of performance measures method were evaluated, and the results are compared with the existing method.

Database: Using the available dataset, evaluate the proposed algorithm. The report of experimental results based on MICC-F220 [14] is presented in this work. The MICC- F220 dataset contains of 220 images, 110 of which are duplicated images and 110 of original images.

Table 1
Database description

Type/version	Image size	No. of images
MICC-F220	722 × 480 to 800 × 600	220

Performance measures: Experiments are carried out on HP notebook computer with an Intel core i3-8130U (2.20 GHz) processor and 8 GB of memory. The proposed tampered detection algorithm performance is considerate based on the parameters False Positive Rate (FPR) and True Positive Rate (TPR), which are defined as follows:

True Positive (TPR) = The positive value is classified correctly; it is considered to be a true positive value.
False Positive (FPR) = The positive value is classified incorrectly; it is considered as a false positive.
True Negative (TNR) = The negative value is classified correctly; it is considered to be a true negative value.
False Negative (FNR) = The negative value is classified incorrectly; it is considered as a false negative.

Accuracy: Accuracy is defined as its ability to correctly distinguish between true positive and true negative cases. To estimate the accuracy, we must compute the proportion of true positive and true negative results in all evaluated cases. This can be expressed mathematically as:

Accuracy = (TP+TN)/ (TP+TN+FP+FN) (11)

Analysis of algorithm: Many block-based algorithms are Unable to detect forged region of the image has been subjected to performance measures. To address this issue, this work is to perform block matching by comparing the performance measures of the labelled region and the merged region.

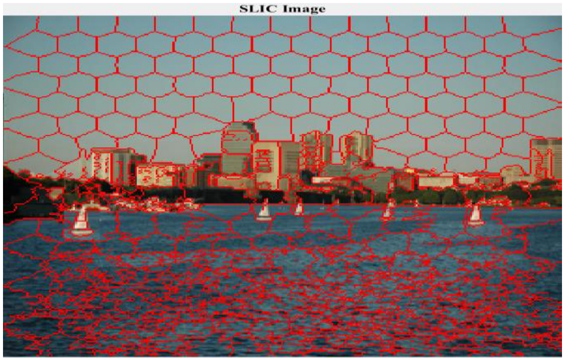

Fig.3(a). Test images of copy move forgery detection

As illustrated in Fig. 3(a), the left image is a tampered image, while the right image is the original image. The original image is nothing more than a placeholder that is used before tampering with an image. To detect the duplicate region of the image, in this paper the copy move forgery method is used, but before applying all the techniques first we know which is the original image.

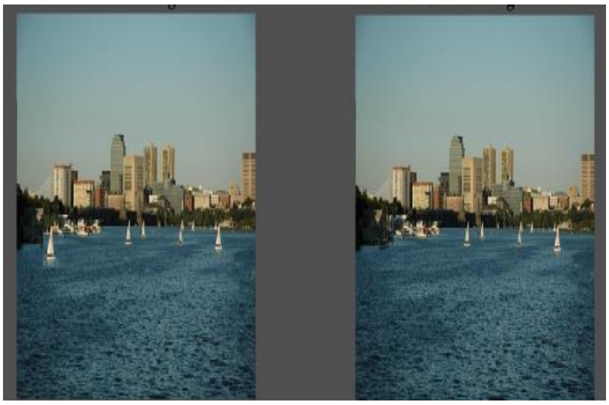

Fig.3(b). pre-processing (Geometric transformations)

As shown in Fig.3(b) pre-processing is used to focus an image's content while reducing computation complexity. In this case, the host image is resized into a uniform size and the RGB image is converted into a gray scale image.

Fig.3(c). Segmented SLIC image

As shown in figure in Fig.3(c) the segmentation process is performed based on the key point extraction from each clustered image block and these are described by SURF and SIFT points.

DOI: 10.17148/IJARCCE.2021.101208

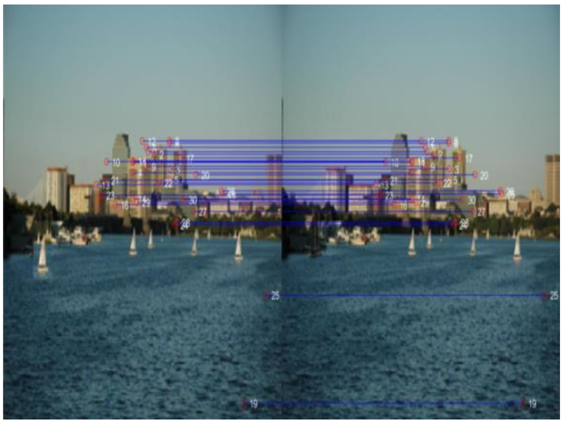

Fig.3(c). point matching based on SURF Features

As shown in Fig.3(c) In point matching process will give the specific point pair as a output and if there are same shift vectors then the threshold value is calculated then the matched points are which specified to the same shift vector are identified as the regions of copied or moved.

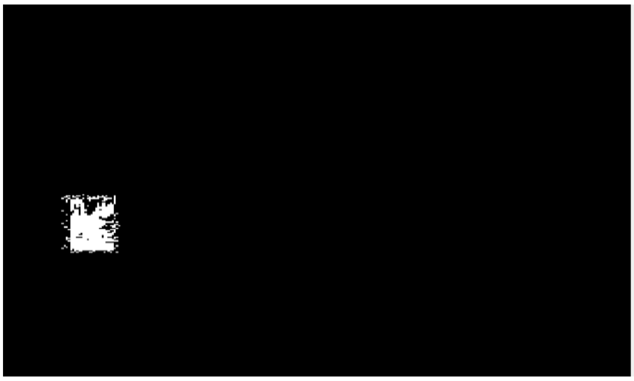

Figure 3(d): Labelling feature point

As shown in Fig. 3(d), the LPF regions are extracted to improve the perfection of the forgery region. The extracted LPF regions are used as the forgery regions.

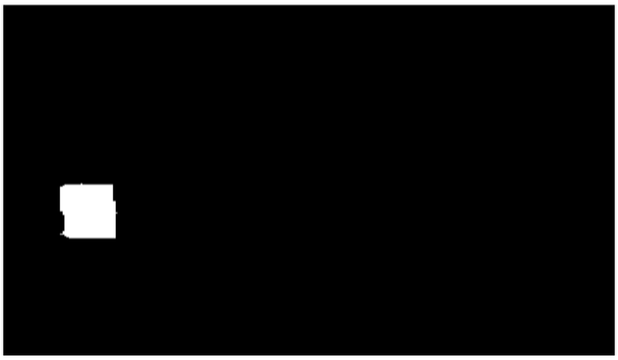

Figure 3(e): Merged region

As shown Fig .3(e), to get the better visual the neighbour super pixels are converged into the comparing pretends locality when the nearby shading highlight is the same as that of the hypothesise domains. This concentrated procedure results in concreted locality (MR).

DOI: 10.17148/IJARCCE.2021.101208

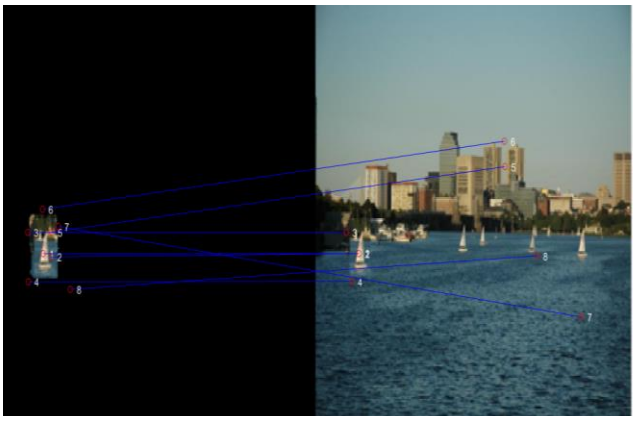

Figure 3(f): Detection results based on SIFT and SURF

As shown in Fig .3(f) The forgery region is extracted based on proposed methods by pointing with the original image region.

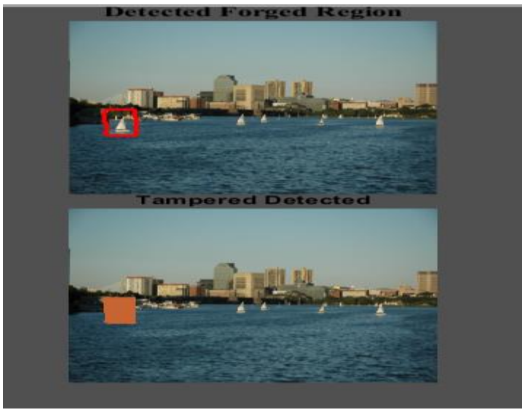

Figure 3(g): image forgery detection

In Fig.3(g), certainly detected forgery region is identified by the colour shading, to know better extracted part from original image.

Table 2
Proposed method of MICC-F220 dataset image block size, TPR, FPR and computational time.

Size of block	Time (in sec)	Precision	Recall	TPR%	FPR%
4 × 4	2.06	98.9901	99.7037	99.1726	0.8274

Table 3
Comparison of proposed method and existing method with performances computational time, TPR, FPR values in (%) and precision

Methods	Time (in sec)	Precision	Recall	TPR%	FPR%
Proposed method	2.06	98.9901	99.7037	99.1726	0.8274
Existing method	4.08	95.68	96.83	89.17	1.37

Finally, the detected area is displayed. The experiments results are based on the MICC- F220 dataset, respectively. For images in the MICC-F220 dataset, the FPR and TPR values are zero and 99%, respectively.

DOI: 10.17148/IJARCCE.2021.101208

4. CONCLUSIONS

This paper proposed a novel copy move falsification location conspiracy that make use of versatile over – division and highlight point coordinating. To identify the regular and irregular shape of the image regions, a novel tamper detection SLIC algorithm is proposed. To choose an appropriate piece introductory size to improve the precision of falsification location and at the same time to diminish estimation costs. Key point features are extracted based on the SIFT algorithm. The extracted features are then used to match the blocks, matching using SURF and then identified Local Feature Points, the extracted local feature points are taken as tampered region. Performance measures such as precision and recall are used to calculate the process of performance. The forgery area is detected with 98.99 percent of accuracy, which is higher than the existing systems. The process can be improved further by implementing various image segmentation algorithms.

5. ACKNOWLEDGEMENTS

This project was supported by project grants received from RUSA, Department of Electronics and Communication Engineering, JNTUK Kakinada, Vizianagaram campus, AP.

6. REFERENCES

[1]Y. Huang, W. Lu, W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images," *Forensic Science International*, vol. 206, no. 1–3, pp. 178–184, 2011.

[2] Ardizzone E, Bruno A, Mazzola G. Detecting multiple copies in tampered images. In: IEEE international conference on image processing; 2010. p. 2117–20. doi:10.1109/ICIP.2010.5652490

[3] Zhong J, Gan Y, Young J, Huang L, Lin P. A new block-based method for copy move forgery detection under image geometric transforms. Multimed Tools Appl 2017;76(13):14887–903.

[4] Amerini I, Ballan L, Caldelli R, Bimbo AD, Serra G. A sift-based forensic method for copy-move attack detection and transformation recovery. IEEE Trans Inf Forensics Secur 2011;6(3):1099–110

[5] Soni, B., Das, P. K., & Thounaojam, D. M. (2019). Geometric transformation invariant block-based copy-move forgery detection using fast and efficient hybrid local features. Journal of Information Security and Applications.

[6] Zheng J, Liu Y, Ren J, Zhu T, Yan Y, Yang H. Fusion of block and keypoints based approaches for effective copy-move image forgery detection. Multidimens Syst Signal Process 2016;27(4):989–1005.

[7] Wang XY, Liu YN, Xu H, et al. Robust copy-move forgery detection using quaternion exponent moments. Pattern Anal Appl 2016;21(2):451–67.

[8] Warif NBA, et al. CMF-iteMS: an automatic threshold selection for detection of copy-move forgery. Forensic Sci Int 2019; 295:83–99.

[9]I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099–1110, 2011.

[10] Herbert Bay, Andreas Ess, Tinne Tuytelaars, Luc Van Gool, SURF: Speeded Up Robust Features, Computer Vision and Image Understanding (CVIU), Vol. 110, No. 3, pp. 346-359, 2008.

[11] Badr, A., Youssif, A., & Wafi, M. (2020). A Robust Copy-Move Forgery Detection in Digital Image Forensics Using SURF. 2020 8th International Symposium on Digital Forensics and Security (ISDFS).

[12] J. Fridrich, D. Soukalm, and J. Lukas, "Detection of copy-move forgery in digital images," in *Proceedings of the Digital Forensic Research Workshop*, pp. 19–23, Cleveland, Ohio, USA, August 2003.

[13]Amerini I, Ballan L, Caldelli R, Bimbo AD, Serra G. A sift-based forensic method for copy-move attack detection and transformation recovery. IEEE Trans Inf Forensics Secur 2011;6(3):1099–110.

[14] S. B. G. T. Babu and C. S. Rao, "An optimized technique for copy–move forgery localization using statistical features," ICT Express, Aug. 2021, doi: 10.1016/j.icte.2021.08.016.

[15] Ch. Srinivasa Rao and S. B. G. Tilak Babu, "Image Authentication Using Local Binary Pattern on the Low Frequency Components," in Lecture Notes in Electrical Engineering, vol. 372, Springer Verlag, 2016, pp. 529–537.

[16] S. B. G. T. Babu and C. S. Rao, "Statistical Features based Optimized Technique for Copy Move Forgery Detection," 2020 11th Int. Conf. Comput. Common. Netw. Technol. ICCCNT 2020, 2020.

[17] Fridrich J, Soukal D, Lukas J. Detection of copy-move forgery in digital images. In: Digital forensic research workshop; 2003. p. 55–61.

[18] Lowe DG (2004) Distinctive image features from scale-invariant keypoints. Int J Comput Vis 60(2):91– 110

[19] Zhu, Y., Ye, L., Wang, J., & Zhang, Q. (2015). *An improved SLIC super pixel algorithm based on nonlinear filtering. 2015 IEEE Advanced Information Technology, Electronic and Automation Control Conference (IAEAC).*

[20] Suresh, G., & Rao, C. S. (2020). *Copy Move Forgery Detection Through Differential Excitation Component-Based Texture Features. International Journal of Digital Crime and Forensics, 12(3), 27–44.* doi:10.4018/ijdcf.2020070103.

[21] Suresh, G., & Srinivasa Rao, C. (2016). *RST Invariant Image Forgery Detection. Indian Journal of Science and Technology, 9(22).* doi:10.17485/ijst/2016/v9i22/8922

.