JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

ROBUST FEATURES FOR IDENTIFICATION OF COPY-MOVE FORGERY

[1]A. Subhadra,[2]K. Padma Priya

[1]M.Tech Student, [2]Professor, Department of ECE
[1]Department of ECE,
[1] University College of Engineering, JNTUK, Kakinada, Andhra Pradesh, India
[2]University College of Engineering, JNTUK, Kakinada, Andhra Pradesh, India

Abstract: The copy-move forgery is the simplest image manipulation technique. In copy-move forgery, a copied portion of the image is pasted on another part of the same image. By grouping Scale Invariant Feature Transform (SIFT) keypoints and HARRIS corner points, this paper suggests an effective way to identify copy move forgeries. Tampered areas are then found by exploring similar neighborhoods and clustering SIFT keypoints and HARRIS corner points. The values of true positive rate, false positive rate, and F1 score are improved. The matlab tool is used to evaluate the experimental results.

Index Terms **- copy-move forgery, SIFT Keypoints, HARRIS corner points.**

I. INTRODUCTION

Digital image forgery is the process of altering the original images to produce forged images. Previously, it used to be limited to the arts and literature and it had no impact on the common people. However, as technology and networks advance, it has become much easier to get and alter digital images, placing their validity at risk and creating a significant threat [1]. Furthermore, it is nearly impossible for the human visual system to determine with a naked eye whether the image is genuine or has been altered. Since digital photos can be used as evidence in court, as a component of medical records, as news items, and as financial documents, it is crucial to build better algorithms to certify their honesty and authenticity.

Consequently, one of the main goals of digital image forensics is to identify forgeries in images. The classification of digital image forgery detection is shown in Fig.1.

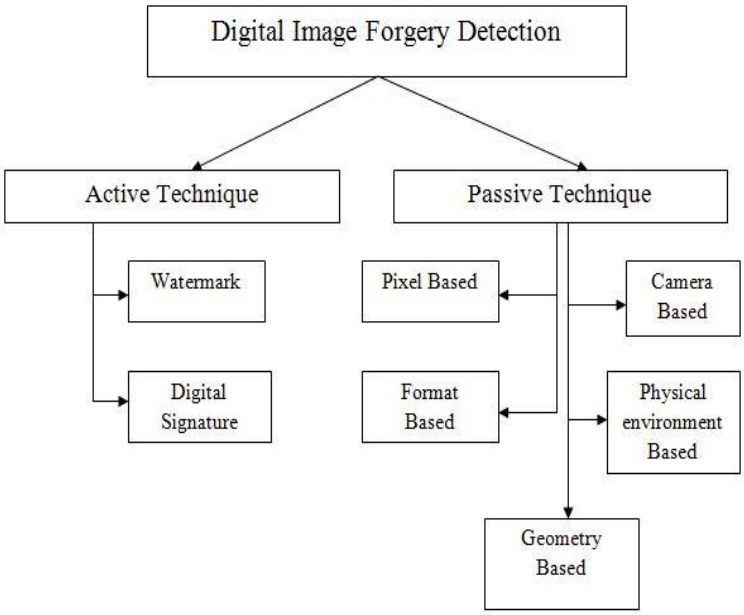

Figure 1: Classification of digital image forgery detection

In digital image forgery detection, the active forgery detection requires pre-embedded data which includes digital watermarking and digital signature [2].The images created using passive approaches do not need to have any digital signatures or watermarks included in them. The ability to recognize a fake image depends on the presence of traces left behind by the various processing stages used during image alteration.

The passive forgery detection techniques are classified into 4 types. They are Copy-Move (cloning), Splicing, Resampling, and Statistical. We mainly focus on Copy-Move Forgery (CMF) which is simple to make by cloning portions of an image to cover areas within the same image, but it is challenging to detect [3].

In this paper, the robust features for identification of copy-move forgery is proposed which are HARRIS corner points are used along with the SIFT keypoints to detect the tampered regions clearly.

II. RELATED WORKS

In this section, the various works related to the detection techniques are discussed.

The author **HAIPENG CHEN *et al.* [1]** proposed an effective approach based on SIFT keypoints scale-color clustering and comparable neighborhoods searches is developed using the conventional CMFD methodology. This approach includes feature extraction, keypoint clustering, feature matching, mismatches removal, and the location of tampered regions. Here SIFT was first chosen to describe keypoints. The keypoints are then clustered based on scale and colour, dividing them into a number of smaller clusters that have been individually matched. Mismatches are eliminated, and the affine transformation matrix is estimated, using the J-Linkage technique. In order to find altered regions, matching pairs' similar neighborhoods are finally searched. However, in large-scale forging, this method is not robust and has shown to be ineffective. Though the results display the tampered regions, there exists some noise at the corners of the images.

The author **Shailaja Rani, P. B *et al.* [2]** discussed various ways for detecting fake digital images and with the aid of Adobe Photoshop, JPEG is one of the devices that make all images available in a format which is the simplest way to detect the image forgery. The researchers have demonstrated how well various identifying approaches perform. In this they did not discussed the proper tampering of images.

The author **Ansari, M. D. *et al.* [3]** introduced several areas of image forgery detection and discussed about established methods in image forgery detection using pixels and provided a comparative analysis of the advantages and disadvantages of the available methods.

The author **D. G. Lowe [4]** proposed the method for extracting distinctive invariant features from images that may be used to reliably match between various views of an object or scene and also discusses an approach using these features for object recognition. Individual learning characteristics that are most adapted to identifying specific object categories have not been worked on. This is crucial for generic object classes since they have to account for a wide range of potential appearances.

The author **X. Bo *et al.* [5]** proposed that from the forged image, SURF descriptors are extracted and matching between the descriptor subsets is done. It has been found that the procedure works well with small-sized images and is quick. Localization of forgeries, however, is not carried out.

The author **Amerini, I. *et al.* [6]** made emphasis to the scenario in which a portion of an image is copied and then pasted into another region to produce duplication or to erase something that was awkward. The problem of determining whether a picture has been faked is examined. A unique approach based on the Scale Invariant Features Transform (SIFT) is suggested to find these alterations. Although significant keypoints are not recovered in the cloned picture patch with very uniform texture, further work on this topic needs to look into ways to improve the detection phase. An image segmentation technique will also be used to extend the clustering phase.

The author **R. Toldo *et al.* [7]** proposed J-linkage, a new agglomerative clustering technique. The method does not require manual parameter tuning or a prior definition of the number of models. Consensus threshold, like in RANSAC, is the free parameter. This method demonstrated its effectiveness in comparison with state-of-the-art competing algorithms.

This paper presents the robust features for identification of copy-move forgery where the noise at the corners of the images can be removed and can locate tampered regions clearly by using the SIFT features along with the Harris corner detection, which also improves the evaluation metrics such as true positive rate, false positive rate, F1 score.

III. EXISTING MODEL

The existing method proposed that by grouping SIFT keypoints and looking for similar neighborhoods to discover tampered regions, the existing method suggests an effective CMFD solution. This method consists of feature extraction, keypoints clustering, feature matching, mismatches removal and tampered region location [1].

3.1 Problem of the existing method

The existing work uses SIFT features to extract the keypoints and locate the tampered regions of image. Though it is showing the results of the tampered regions, there exists some noise at the corners of the images.

In this paper, the problem noise at the corners of the images can be removed and locate tampered regions clearly by using the SIFT features along with the Harris corner detection, which improves the results of the existing work.

IV. PROPOSED MODEL

There are different stages present in copy-move forgery detection. Proposed model block diagram is shown in Fig.2.

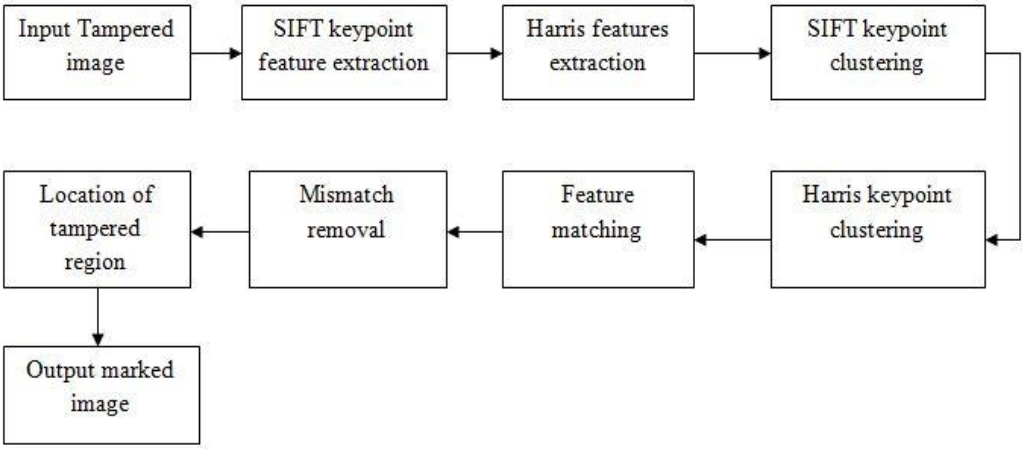

Figure 2: The block diagram of proposed model

4.1 SIFT keypoint feature extraction

In the area of forgery detection, SIFT is a well-known and still widely used feature descriptor. Finding keypoints (feature points) in various scale spaces and determining their dominant orientation are the main goals of the SIFT method. Corners, edges, bright spots in dark areas, and dark spots in bright areas are just a few of the very prominent points that SIFT identified as being the most important and which are unaffected by lighting, affine transformation, or noise [1] .

4.2 Harris features extraction

The Harris corner detector is a method that computer vision systems employ to extract corners and infer visual properties. Since the Harris detector does not require moving patches for every 45-degree angle, it is more accurate at differentiating between edges and corners because it directly takes into account the difference in corner score with respect to direction.

4.3 SIFT and HARRIS Keypoints clustering

There are two issues with matching because to the abundance of SIFT keypoints, particularly in high quality images:
1) The feature matching process has an O (n2) time complexity, where n is the total number of keypoints. When n is greater, the time complexity will rise in square order;
2) Correct matching pairs only make up a small part of the total. Each point in matching must be compared to other n-1 points, although the majority of these comparisons are not necessary.

Therefore, in order to lower feature matching's computational complexity, keypoint clustering is required before feature matching. The clustering framework based on SIFT and HARRIS keypoints scale-color is shown in Fig.3.It consists of two parts:1)clustering based on overlapped scale,2)clustering based on color of keypoints.

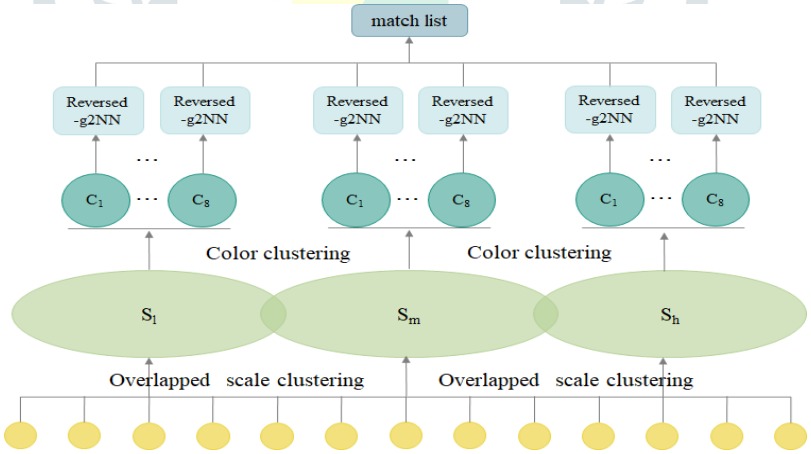

Figure 3: Clustering based on scale and colour

4.3.1 Clustering based on overlapped scale

- SIFT and HARRIS keypoints are extreme points in the space of Gaussian scales.
- Each octave of keypoints has a scale that corresponds to it, which is represented by the third element σk in the descriptor.
- Most keypoints that can be matched have scales that are similar; in other words, there are relatively few instances when the scales of the two keypoints in matching pairs are significantly dissimilar.
- In order to minimize unnecessary matching and comparison, the major goal of this stage is to maximize the separation of keypoints from different scales.
- We group the small-scale range and retain the large-scale range because we know that the number of large-scale keypoints is significantly lower than the number of small-scale keypoints.
- To preserve the stability of scaling attack tampering, scale clustering is done simultaneously via overlapped scale.

4.3.2 Clustering based on overlapped colour

- The temporal complexity is further decreased by doing colour-based clustering.
- Due to the similarity between the tampering region and the source region, even though an image has been subjected to geometric alteration or post-processing procedure, the matching points will not significantly differ in colour.

- When a colour image is turned into a grey image, many RGB values might be transformed to the same grey value, which could lead to some degree of inaccuracy and redundancy.
- However, the RGB value of the keypoint in the altered area does not vary significantly, which can retain the image's visual features as much as possible.

4.4 Feature matching

Traditional g2NN [6] can detect multiple copy-move forgery, calculate the distance set D={d1,d2,..dn-1}between keypoint and other (n-1) keypoints in the cluster and rank them in ascending order. When (1) is satisfied, ki is matched with the keypoints corresponding to d1.

$$d1 / d2 < = t, \text{ where t belongs to } (0, 1) \quad (1)$$

When the several copy-move forgery regions are extremely similar, g2NN may, therefore, omit some valid matching pairs. Reversed-g2NN is employed for feature matching as a result of this. Similar to g2NN, the distance set of keypoints is calculated first, and the distance ratio Ti=di-1/di, i=10 is calculated in reverse order [1].

4.5 Mismatches removal

J-Linkage [7], which is a robust clustering algorithm to eliminate duplicates and calculate affine transformations, is proposed.

4.6 Tampered regions localization

Here, a localization algorithm that locates nearby locations by looking for similar neighborhoods is proposed. This approach analyses pixels, the smallest unit, one by one, much like the region-growing algorithm. The following are the algorithm's primary ideas:

- Affine transformation is used to locate the first keypoint's corresponding point after adding the first keypoint to the expansion queue and setting the queue's head element as the seed point.
- When comparing the PCT feature and PSNR of the seed point and the corresponding point, if both are fulfilled they are marked and the eight neighbourhoods of seed point are added to the expansion queue and the seed point is deleted at the same time.
- If not, the seed point will be immediately deleted and the queue's head element will be chosen as the seed point to allow for further expansion [1].

V. RESULTS AND DISCUSSION

5.1 Experimental Results

The experimental results are obtained using matlab. Here the input is tampered image as shown in Fig.4, firstly the SIFT features shown in Fig.5 and HARRIS features shown in Fig.6 are extracted and then the SIFT keypoints clustering shown in Fig.7 and HARRIS keypoints clustering shown in Fig.8 are performed and detection results are obtained for SIFT features where there exists some noise at the corners of the detected images it is shown in Fig.9 and finally the result of copy move forgery detection based on SIFT and HARRIS features overcoming the problem of noise at the corners of the image are obtained as shown in Fig.10.

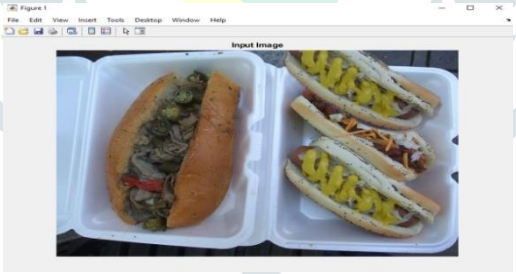

Figure 4: Input image

Figure 5: SIFT features

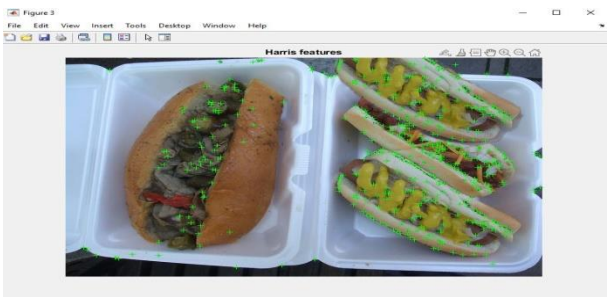

Figure 6: Harris features

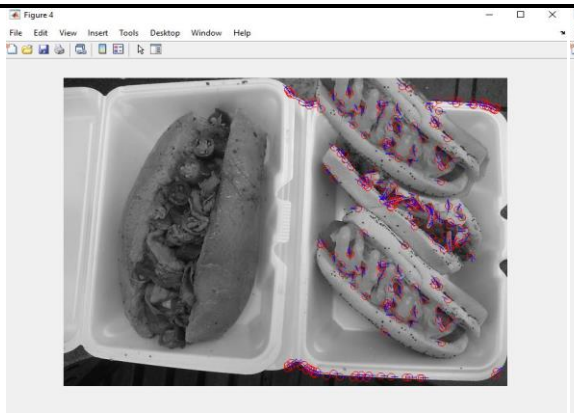

Figure 7: SIFT keypoints clustering

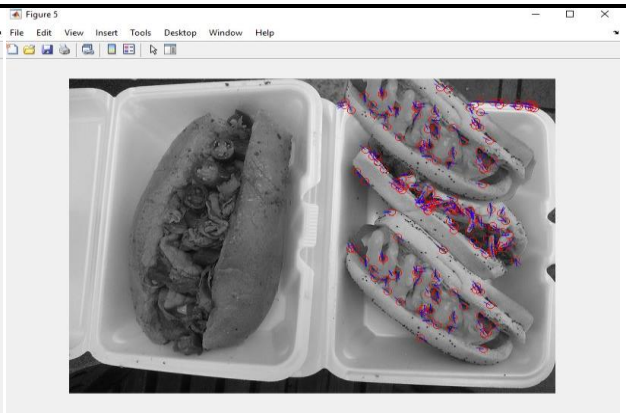

Figure 8: Harris keypoints clustering

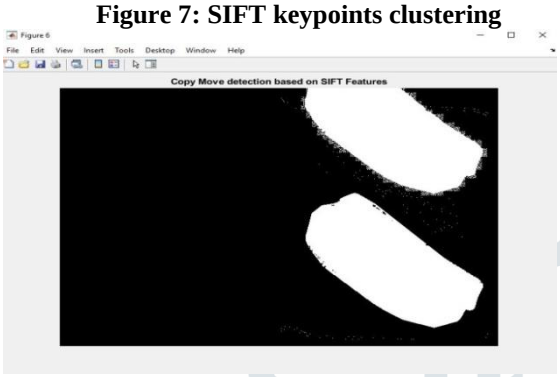

Figure 9: Copy Move detection based on SIFT features

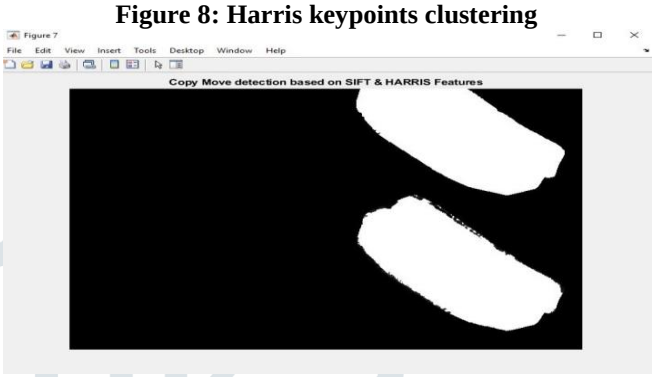

Figure 10: Copy Move detection based on SIFT and HARRIS features

5.2 The comparative analysis results of geometric transformation forgery detection

Here the comparative analysis of F1 score between the existing and proposed methods for different rotations as shown in Fig.11, scaling as shown in Fig.12, compression as shown in Fig.13 and noise as shown in Fig.14 of the images are obtained in graphical form.

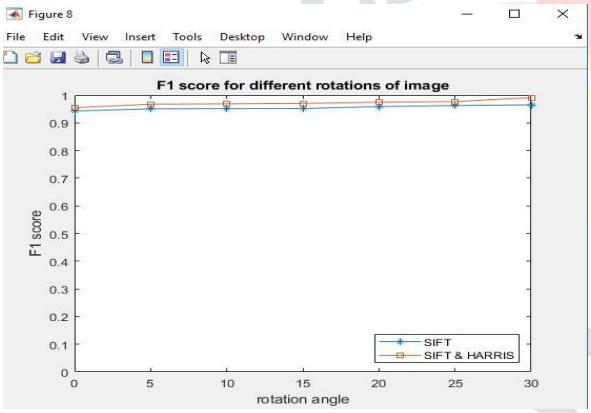

Figure 11: F1 score for different rotations of image

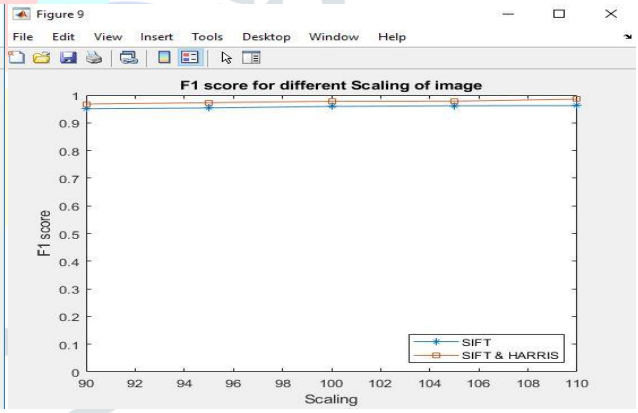

Figure 12: F1 score for different scaling image

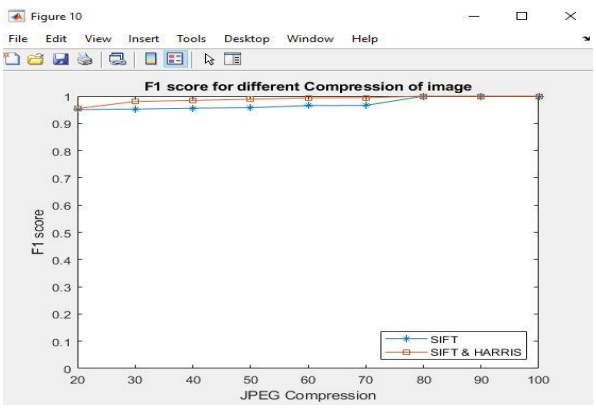

Figure 13: F1 score for different compression of image

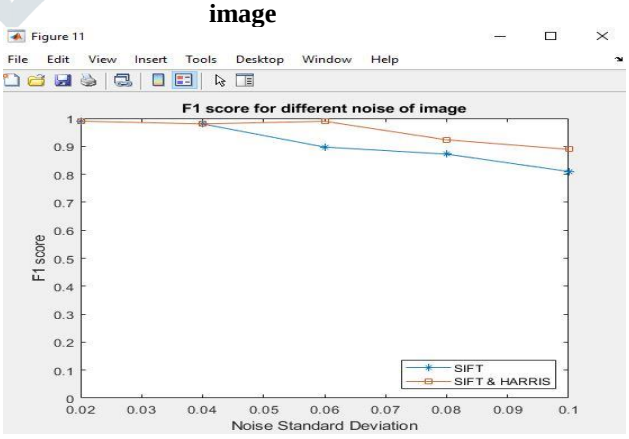

Figure 14: F1 score for different noise of image

Table 1: Experimental results regarding evaluation metrics of existing and proposed models

Methods	Image level			Pixel level		
	TPR (%)	FPR (%)	F1-image (%)	TPR (%)	FPR (%)	F1-pixel (%)
SIFT(Existing)	90.33	9.89	90.20	99.56	99.63	99.59
SIFT+HARRIS (Proposed)	**92.17**	**8.52**	**91.78**	**99.88**	**99.60**	**99.84**

In this paper, Table 1 shows the improvement in evaluation metrics which are the True Positive Rate (TPR), False Positive Rate (FPR), and F1 are used to assess the effectiveness of the suggested approaches by considering the tampered images/pixels as positive samples and the authentic images/pixels as negative ones.

True Positive Rate

TPR, also known as recall rate, stands for the proportion of real tampered images in the detection results. We expect the higher the value, the better.

$$\mathrm{TPR} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}}$$

False Prediction Rate

FPR is the proportion of real images that have been incorrectly identified as having been altered. It should be as low as possible.

$$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}}$$

F1 Score

As a harmonic average of recall rate and precision, F1 is a comprehensive evaluation index. The ability to reflect experimental results is improved with a greater value of F1.

$$\mathrm{F1} = \frac{2\mathrm{TP}}{2\mathrm{TP} + \mathrm{FP} + \mathrm{FN}}$$

TPR, FPR, and F1-image are used at the image level and F1-pixel is used at the pixel level.

VI. CONCLUSION

In this paper, we provide a novel CMFD method that combines SIFT keypoint and Harris keypoints to locate the doctored regions at the pixel level. The experimental results demonstrate the method's effectiveness. The Harris keypoints counts minutes corners while the SIFT keypoints has a high dimension and typically extracts tens of thousands or even hundreds of thousands of keypoints for an image, placing a significant pressure on feature matching. The detection efficiency is increased by clustering both the SIFT and the Harris keypoints as the values of TPR, F1 Score are increased and FPR value is decreased. Our approach is more reliable and capable of finding tampered regions clearly without noise at the corners of the image.

REFERENCES

[1]Chen, H., Yang, X., & Lyu, Y. (2020). Copy-Move Forgery Detection Based on Keypoint Clustering and Similar Neighborhood Search Algorithm. IEEE Access, 8, 36863–36875.

[2]Shailaja Rani, P. B, & Kumar, A. (2019). Digital Image Forgery Detection Techniques: A Comprehensive Review. 2019 3rd International Conference on Electronics, Communication and Aerospace Technology(ICECA).

[3] Ansari, M. D., Ghrera, S. P., & Tyagi, V. (2014). Pixel-Based Image Forgery Detection: A Review. IETE Journal of Education, 55(1), 40–46.

[4] Lowe, D. G. (2004). Distinctive Image Features from Scale-Invariant Keypoints. International Journal of Computer Vision, 60(2), 91–110.

[5] Bo, X., Junwen, W., Guangjie, L., & Yuewei, D. (2010). Image Copy-Move Forgery Detection Based on SURF. 2010 International Conference on Multimedia Information Networking and Security.

[6] Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., & Serra, G. (2011). A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery. IEEE Transactions on Information Forensics and Security, 6(3), 1099–1110.

[7] R. Toldo and A. Fusiello, ‘‘Robust multiple structures estimation with JLinkage,’’ in*Proc. Eur. Conf. Comput. Vision.*, Berlin, Germany, 2008,pp. 537–547.