Calibrating Thresholds Based on Trade-Offs Between Detection Accuracy and FPR for Copy Move Forgery Detection

Savita Walia, Krishan Kumar

***Abstract**: In this paper, prominent keypoint based features are compared in order to analyze their reliability and efficiency against forgery detection. Four features specifically SURF, KAZE, Harris corner points and BRISK features are used individually on a set of images. The method includes four phases: Image pre-processing, keypoint detection, feature vector description and feature vector matching. In feature matching, MaxRatio has been chosen as a varying parameter for calculating values of false positives and false negatives for each feature. MaxRatio defines the ratio for rejecting ambiguous matches of feature descriptors in the images. The optimal threshold value for MaxRatio is calibrated with the help of trade-off between detection accuracy and false positive ratio. The changes in false negative ratio and false positive ratio are picturized in order to find out optimal threshold for detection accuracy. ROC curves are also plotted for each feature at different values of MaxRatio and area under the ROC curves are calculated. The experiments are performed on two benchmark datasets, namely CASIA version 2.0 and MICC-F600. It has been perceived from experimental outcomes that KAZE features gave best values for all the performance metrics namely accuracy, precision, area under the ROC curve and F1-score with little compromise in time complexity, whereas Harris corner points gave the worst results as compared to rest of the features. Further, in order to improve the execution time, the computation of non-linear scale space process in KAZE can be simplified and GPU programming for real-time performance may also be used.*

***Index Terms**: Digital image forensics, Image forgery detection, passive methods, copy-move, keypoint detection, threshold calibration.*

I. INTRODUCTION

Image forgery is not a modern concept, it comes along with the invention of photography [1]. With the advancement of the technology and the internet, countless photo editing tools have been established which made the digital image manipulations [2] much more easier. That is how it comes in limelight nowadays. Malicious modification of an image with intent to deceive for the sake of altering the public perception is termed as Digital image forgery. The modifications are done in such a way that it hardly leaves any visually detectable traces. Such images are accepted as a certification of truthfulness almost by everyone and everywhere [3]. So confirmation of an image's authenticity is required which done with the help of digital image fakery detection methods [4].

There are several types of image forgeries exposed to date and correspondingly several detection methods. Digital image forgeries can be categorised broadly into three types: Image splicing, copy-paste and retouching. In retouching, the image itself does not fundamentally changes, but there is an enhancement of the surface of the image. Image retouching is most commonly used in fashion photography and in magazines to make photographs more attractive. Splicing is a method in which the images are consolidated to make an altered image [5]. A piece of one image is taken and fixed into another image. Sometimes various image processing operations are applied in order to blend the pasted region into the original image. In copy-paste type of forgery, a piece of an image is generally reproduced and inserted into another part of the image with an intention to conceal some object or important detail in the image [6]. As the copied part remains to be of the same image, no visible significant changes are there. Therefore, its detection is tough and moreover copy-move is the most commonly used forgery in digital images, so the work in this paper is focused on the identification of copy move forgery detection.

The techniques for identification of forgeries in digital images are broadly classified [7] into two classes shown in Figure 1. Active methods and Passive methods [8]. Active methods require aforementioned knowledge about the image in order to check whether the image is authentic or not. Digital signatures [9] and digital watermarks [10] are used for that matter. The digital signature or watermarks [11] are embedded into the image, if the image is ever forged then the digital watermark or signature will also change. In case of passive methods, there is no preliminary information available about the image. Only one image is there under consideration for forgery detection. Passive methods [12] use the fact that the forgeries alter the consistency of intrinsic features of the images. Such inconsistencies in the images can be used to detect the modifications performed by the forger.

Revised Manuscript Received on 30 July 2019.

***** Correspondence Author
Savita Walia*, University Institute of Engineering and Technology, Panjab University, Chandigarh, India.
Krishan Kumar, University Institute of Engineering and Technology, Panjab University, Chandigarh, India.

In copy-move forgery detection, different parts of the image are strongly correlated with each other in terms of features. The features are computed either by dividing an image into blocks or by computing local keypoints for the complete image.

Keypoints are the points or the spatial locations in the image that tells what is interesting in an image. These are important because of the reason that no matter what how image changes, whether it rotates, shrink, expand or distorted, key-points remain almost same in the modified image.

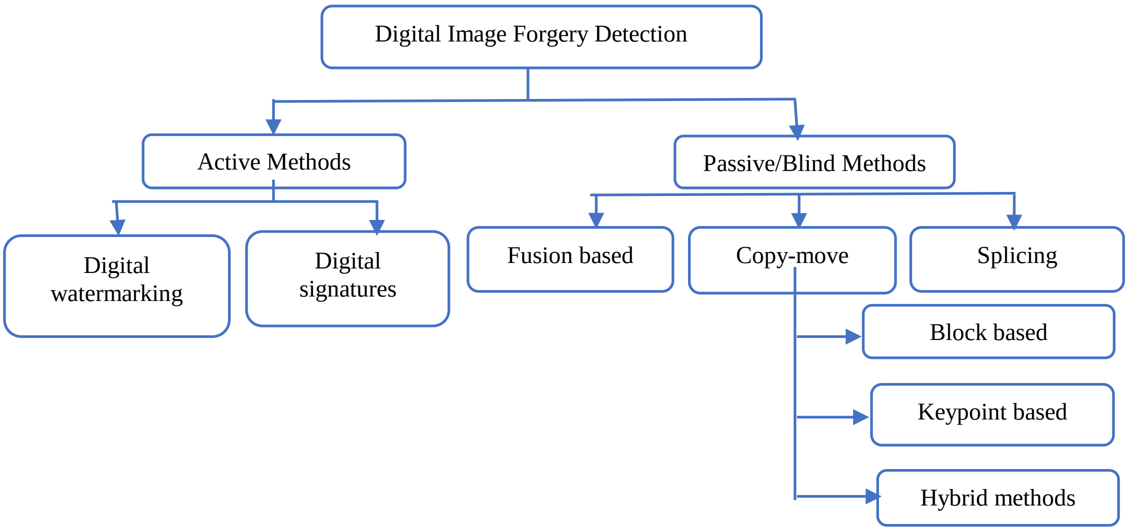

Figure 1. Types of forgery detection techniques

Various keypoint based features are discovered like Scale invariant feature transform, KAZE, Speeded Up Robust Features, Harris corner points and BRISK. SIFT features [13] are the oldest and widely used for various applications of image processing applications. Though SIFT features are highly distinctive in nature and robust but they suffer from a major drawback that it is highly complex in terms of computation. In order to improve the computational cost, researchers started working towards its improvement which lead to development of SURF. SURF [14] is simply a speeded up version of SIFT. In our approach, we already know SIFT is highly time consuming so we opted SURF along with other features for our study. The features are compared on premise of accuracy, precision and F1 score. The trade-off between false negatives and false positives for individual features is also provided.

Major contributions of our work are as below:

1. Performance analysis of different keypoint based features using various metrics is provided for copy-paste fakery detection.
2. Threshold calibration is performed using trade-off between detection accuracy and false positive ratio.
3. ROC curves are plotted using recall and fall-out for better presentation of the experimental results.

The organisation of the paper is given as follows: Next section throws light at some prominent papers based on identification of digital image forgeries with the help of keypoint feature extraction algorithms. Further, the methodology used and the experimental results are presented. Conclusions are drawn in last section.

II. RELATED WORK

Various features have been used in literature for the detection of copy-move forgeries in digital images. SIFT [13] [15] features are most widely used feature set in the history of computer vision and image processing applications. In case of SIFT features, a Gaussian scale space is used by applying a difference of Gaussians (DoG) operator in order to obtain the maxima and to obtain the feature locations. For detected keypoints, gradient orientation is used over a local area of interest around that keypoint for building the descriptors. A feature descriptor vector of 128 columns is yielded by using a rectangular grid usually of 4×4 subregions and histograms of oriented gradients. In [14], a Speeded Up robust feature set was developed with the an inspiration from SIFT. SURF exhibit various characteristics like repeatability, distinctiveness and robustness as compared to SIFT features as SURF makes use of the integral image which means that it uses simple box filters which do not computes the entire Gaussian scale space. Gaussian derivatives are approximated at different scale levels. The dimension of descriptor is usually 64 and 128 for its extended counterpart. In [16], harris corner points are employed with uniform distribution all over in order to attain an adequate number of feature points. In case of BRISK [17] features, the rotation invariance is achieved by identifying characteristic direction of each keypoint. In [18], authors used SURF algorithm for locating copy-moved regions. SURF descriptors of an image are compared by arbitrarily separating the SURF keypoints into two sets. The nearest neighbors are discovered in these groups by saving the matching entries and the process is repeated for each group obtained until all the entries are processed. The experiments were done on images with various post processing operations such as rotation, resizing, blurring and Gaussian noise insertion. Such methods have complications in locating the cloned parts in case of homogeneous regions as there are no sufficient keypoints extracted.

In [19], Kd-trees are used to extract and store the SURF keypoints. Kd-tree makes it easier to find the nearest neighbor and generates lower false negatives. The paper does not provide sufficient experimental validation, only the visual results are provided for resizing, rotation and Gaussian noise. In [20], several popular methods of copy paste fakery identification methods are analyzed based on their performance under different situations. It was conveyed that the use of Zernike moments, PCA, KPCA or DCT may achieve acceptable detection results. Keypoint based methods give best precision results in most critical scenarios such as large rotation angles, scaling and higher compression rates are implemented on the copied segments, while the effectiveness of the rest of the approaches decline remarkably.

III. METHODOLOGY USED

The technique used in this paper is based upon matching of keypoint descriptors for copy-move forgery detection [21]. Firstly, an RGB color image is transformed into grayscale. Secondly, keypoint detection is performed using SURF (Speeded Up Robust Features), KAZE, Harris corner points and BRISK (Binary Robust Invariant Scalable Keypoints) algorithms. Then, the corresponding feature descriptors are calculated. Finally, matching of descriptors is performed in order to find out whether there exists any copied region in the image or not. If any of the feature descriptors do not match, then the image is not forged, otherwise the image is forged. The general methodology is shown in Figure 2.

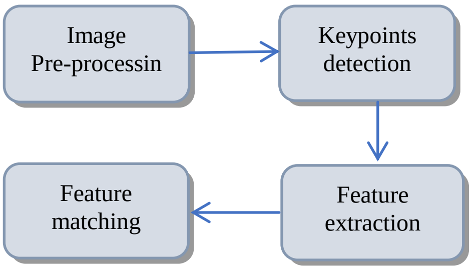

Figure 2 General methodology

A. Image pre-processing

A color image is transformed into a grayscale image by transforming the RGB values into 8-bit grayscale values. The conversion of RBG image to grayscale is performed by removing the hue and saturation components while the luminance is preserved. R, G and B components are added by taking their weighted values to transform RGB values to grayscale values using (1):

$$A = 0.2989 * R + 0.5870 * G + 0.1140 * B \qquad (1)$$

where R, G and B represent the red, green and blue color channels of the input image respectively. A represents the converted grayscale image. Submit your manuscript electronically for review.

B. Feature detection

SURF: Speeded Up Robust Features [14] finds blob features of an image using Hessian blob detector. The region in the image where some properties are constant or approximately constant are called as blobs. The points in a blob are almost similar to each other due to the fact that their properties are nearly constant. The change in the local area around the point is measured using the determinant of the Hessian matrix. The key-points are selected where the value of determinant is maximal. SURF feature descriptors are based on the sum of the Haar wavelet response around the point of interest.

KAZE: KAZE [21] uses feature point detection in nonlinear scale spaces whereas SIFT and SURF are based on Gaussian scale space. For detecting key-points for KAZE, multiple scale levels are used for computation of the response by scale normalized determinant of the Hessian matrix.

Harris corner points: Harris corner detector [22] is based on a fundamental notion that feature points are linked with highest value of the local autocorrelation function.

BRISK: The BRISK [17] descriptors are made up of a binary string by integrating the outcomes of simple brightness evaluation tests on a given set of key-points which consists of sub-pixel refined image locations and corresponding floating point scale values.

C. Feature Extraction

Feature vectors, also called descriptors are extracted from a binary or intensity image. Pixels surrounding an interest point are used to derive the descriptors. Feature descriptors are required to define and match features quantified by a location of single point. 64-dimensional feature descriptors are extracted for all the features.

D. Feature Matching

The matching of features [22][23] is performed using the nearest neighbours algorithm that computes the pair-wise distance between all the feature vectors of the image. A same matching criterion is used for all the four features under consideration. If no feature vectors match in an image, then the image is an authentic image otherwise it is concluded as a forged image. Further, a ratio threshold is specified which gives a scalar for rejecting ambiguous matches called as MaxRatio. The value of MaxRatio ranges from 0 to 1. The more the value of MaxRatio, more the number of matches are returned.

IV. EXPERIMENTAL OUTCOMES

In this segment, the experimental setup and the outcomes are discussed. In our experiments, four different features specifically, SURF, KAZE, Harris corner points and BRISK are assessed for copy-paste fakery detection in images. The images are gathered from CASIA version 2.0 [24] and MICC-F600 [15] datasets. The experimentation is performed on 90 authentic images and 90 forged images having dimensions 384*256.

The manipulations on the images include copy-paste with translation, rotation and scaling of copied region. The experiments are completed on an individual PC having processor with Intel Core i5-7200U CPU @2.50GHz, NVIDIA GeForce 940MX 4GB graphics card with 8GB of RAM.

MATLAB 2017b was used on Microsoft Windows 10 Home Version 10.0.16299 to generate the code for the proposed procedure.

In our method, the performance of feature detectors and descriptors is evaluated. We compare the performance results of all the features on the basis of results of matching algorithm. Various evaluation metrics used are discussed below and the results are shown in Table 1.

Precision: Precision is defined as the proportion of the correctly detected fake images to the total count of detected fake images. (see (2))

$$Precision = \frac{TP}{TP + FP} \tag{2}$$

Accuracy: Accuracy provides the quality of detection based on the true positive rate and true negative rate. It indicates the percentage of correctly detected images (forged and authentic) to the total number of images in the dataset. (see (3))

$$Accuracy = \frac{TP + TN}{TP + FN + TN + FP} \tag{3}$$

F1-score: F1-score is computed using the harmonic mean of the sensitivity and precision i.e. true positive ratio. It is computed using (4).

$$F1 - score = \frac{2TP}{2TP + FP + FN} \tag{4}$$

Timing: Timing evaluation is performed for the whole process and a comparison with each other namely, KAZE, SURF, Harris corner points and BRISK is done. We take into account the detection of the features, description of the features and matching of feature descriptors. All of the timing results were obtained on an i5- 7200U CPU @ 2.50 GHz laptop computers. The implementation is done in MATLAB.

Table 1 Performance Evaluation

Feature	Prec (%)	Acc (%)	F1	Time (s)
SURF	77.11	75.00	0.74	9.70
KAZE	90.22	91.11	0.91	46.30
Harris	36.59	43.89	0.23	18.19
BRISK	78.38	73.33	0.71	77.00

As it can be seen from Table 1, SURF and BRISK features gives comparable results, but BRISK has a much higher time complexity than all the other three features. Harris corner points turned out to be inappropriate for our purpose as it gives poor performance in terms of all the metrics used. In most of the sequences, KAZE has superior detector repeatability. KAZE is more time complex as compared to Harris corner points and SURF mainly due to the calculations of the nonlinear scale space that is the most time-consuming step in KAZE. However, at the price of a considerable rise in computational cost, KAZE results as a more efficient feature set.

Further, ROC curves have been provided in for all the features. The receiver operating characteristic (ROC) curve is a picturization that demonstrates the ability of a binary classification system as its discrimination threshold is varied. A perfect system (no false positives or false negatives) has a Threshold 1.0. An ROC curve is a way to compare detection rate with the false positive rate. As the true positive rate increases, there is an increase in false positive rate i.e. if the false positive rate is compromised then superior detection rate can be reached while negotiating on detection rate can facilitate a much better false positive rate. Major detection parameter we used in our experiments is *MaxRatio*. It gives the ratio threshold for rejecting the ambivalent matches. As the value for *MaxRatio* varies, false matches also vary. The choice of *MaxRatio* is, however, a difficult task. A particular value of *MaxRatio* may not be appropriate for all feature values. Too small and too large threshold value results in high number of false alarms and lower detection rate respectively. So, the *MaxRatio* should match the overall functioning of four features. Hence, for an individual method, a cautious examination of performance measures, i.e. (*TPR*) and (*FPR*), is performed in order to find the value of the area under the ROC curve.

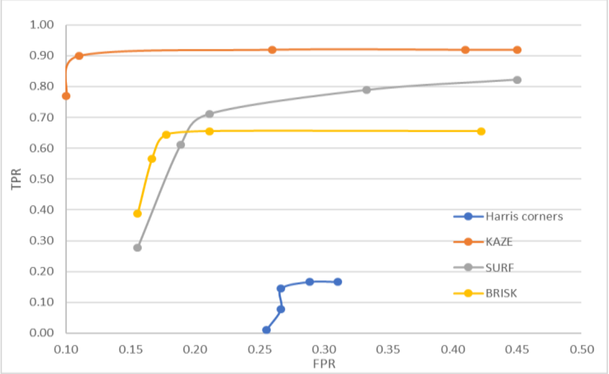

Figure 3. ROC curves for different features for Copy-move forgery detection

Figure 3 shows the ROC curves plotted between detection accuracy and false positive ratio for all the features. The area under the ROC curve can be find out using mathematical formula given in (5). In case of SURF, as the threshold value increases the curve also increases and last value denotes the point where curve becomes stable. KAZE seems to be more accurate than SURF as it is visible that area under the ROC curve for KAZE is more than SURF. Moreover, accurateness for KAZE features is 91.11% which is 16.11% more than SURF. Similar results can be drawn from Harris Corner and BRISK features from Figure 3. Harris corner points are capable of detecting corners only and rest of the important information of the image is discarded, because of which there is a drastic downfall in its accuracy. Also, BRISK features give comparative results to SURF features as there is a slight difference in the observations.

$$Area\ under\ the\ curve = \int_a^b f(x)dx \tag{5}$$

Further, we have picturized the change in false positive ratio (FPR) and false negative ratio (FNR) in order to discover an optimal threshold. FPR gives the effectiveness of the system whereas FNR (i.e. 1-TPR) provides an extent of the system trustworthiness. Variations in *MaxRatio* have been used to quantify false positives and false negatives which assist in making a decision on the optimal conditions for the detection.

The graphs shown in Figure 4 to Figure 7 are obtained by calculating false positive ratio and false negative ratio at different values of *MaxRatio*. This particular point determines the best value of MaxRatio threshold in order to achieve the ideal values of FPR and FNR. For SURF features in Figure 4, FPR and FNR crosses at third observation that is for MaxRatio = 0.6.

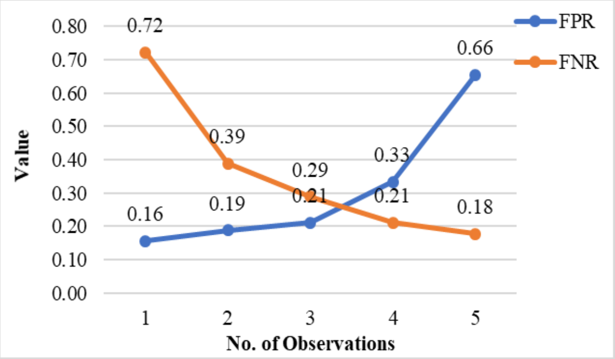

Figure 4. Detection accuracy for different values of 'MaxRatio' for SURF

In Figure 5, the curves for false positive rate and false negative rates for KAZE features cross each other at second observation i.e. at MaxRatio = 0.4. For Harris corner points in Figure 6, the lines for FNR and FPR do not intersect. It is concluded that there exist no such point which can provide better results in case of Harris points. As it can also be seen from Table 1, Harris corner points result in worst performance in all aspects. Similarly, for BRISK features in Figure 7, the lines intersect at fifth observation i.e. MaxRatio = 1.0. Therefore, BRISK gives optimal results at threshold 1.0.

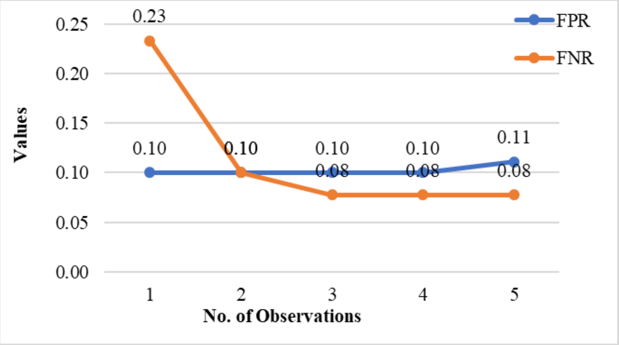

Figure 5. Detection accuracy for different values of 'MaxRatio' for KAZE

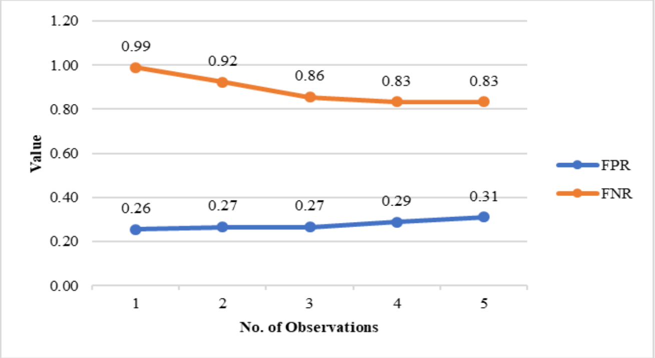

Figure 6. Detection accuracy for different values of MaxRatio' for Harris Corner Points

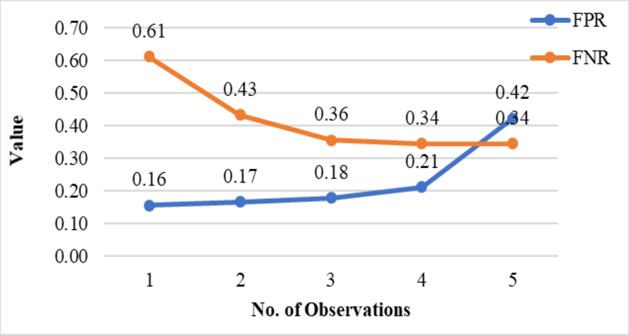

Figure 7. Detection accuracy for different values of 'MaxRatio' for BRISK

After carefully scrutinizing the results obtained for various features shown in Table 2, it has been concluded that KAZE gives a more reliable feature set for copy-move forgery detection. It obtained highest accuracy and precision with a huge margin in comparison to SURF and BRISK with a little compromise on time complexity.

Table 2. Results at different values of 'MaxRatio'

Feature Name	MaxRatio	TPR	FPR	FNR	TNR
SURF	0.2	0.28	0.16	0.72	0.84
	0.4	0.61	0.19	0.39	0.81
	0.6	0.71	0.21	0.29	0.79
	0.8	0.79	0.33	0.21	0.67
	1.0	0.82	0.66	0.18	0.34
KAZE	0.2	0.77	0.10	0.23	0.90
	0.4	0.90	0.10	0.10	0.90
	0.6	0.92	0.10	0.08	0.90
	0.8	0.92	0.10	0.08	0.90
	1.0	0.92	0.11	0.08	0.89
HARRIS CORNER	0.2	0.01	0.26	0.99	0.74
	0.4	0.08	0.27	0.92	0.73
	0.6	0.14	0.27	0.86	0.73
	0.8	0.17	0.29	0.83	0.71
	1.0	0.17	0.31	0.83	0.69
BRISK	0.2	0.39	0.16	0.61	0.84
	0.4	0.57	0.17	0.43	0.83
	0.6	0.64	0.18	0.36	0.82
	0.8	0.66	0.21	0.34	0.79
	1.0	0.66	0.42	0.34	0.58

V. CONCLUSION

In this paper, a comparison for feature detection, description and matching in Gaussian and nonlinear scale spaces for copy-move image forgery detection is provided. The technique includes four phases:

Image pre-processing, keypoint detection, feature description and feature vector matching. Four features are implemented individually through this technique and results are compared. The comparison of features is performed in order to find out that which of the feature set is performing well for copy-paste forgery identification. It has been observed in literature that calibration of threshold is not performed by any author. Usually a threshold value is provided directly in most of the articles available without mentioning how the threshold value is obtained. In this paper, a trade-off between detection accuracy and FPR is provided in order to calibrate the threshold by manually varying threshold values. Despite of reasonable upsurge in computational cost in terms of time, results for KAZE expose a footstep forward in performance in detection and matching against other features such as SURF, Harris corner points and BRISK. SURF and BRISK gave comparable results but BRISK features are lot more time consuming than any other feature. KAZE outperforms SURF and BRISK in terms of accuracy and precision, but a bit more time consuming than SURF. In future, the computation of nonlinear scale space in KAZE can be simplified in order to boost-up the process by using the GPU acceleration for real-time performance. Furthermore, KAZE features can also be clubbed along with block-based methods of copy-paste forgery detection for better results.

REFERENCES

1. "Photo Tampering throughout history," *Fourandsix Technologies, Inc.* [Online]. Available: http://pth.izitru.com/. [Accessed: 08-Jul-2019].
2. H. Farid, "Digital Image Forensics," *Sci. Am.*, vol. 298, no. 6, pp. 66–71, 2008.
3. D. Hu *et al.*, "On digital image trustworthiness," *Appl. Soft Comput.*, vol. 48, pp. 240–253, 2016.
4. A. M. Anoop, "Image forgery and its detection : A survey," in *International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, 2015, pp. 1–9.
5. Z. Zhang and Y. Zhou, "Study of Image Splicing Detection," *Adv. Intell. Comput. Theor. Appl. With Asp. Theor. Methodol. Issues*, vol. 5226, pp. 1103–1110, 2008.
6. F. Y. Shih and Y. Yuan, "A Comparison Study on Copy– Cover Image Forgery Detection," *Open Artif. Intell. J.*, vol. 4, pp. 49–54, 2010.
7. S. Walia and K. Kumar, "Digital image forgery detection: a systematic scrutiny," *Aust. J. Forensic Sci.*, pp. 1–39, 2018.
8. L. U. O. Weiqi, Q. U. Zhenhua, P. a N. Feng, and H. Jiwu, "A Survey of Passive Technology for Digital Image Forensics," *Front. Comput. Sci. China*, vol. 2, pp. 1–14, 2007.
9. X. Wang, J. Xue, Z. Zheng, Z. Liu, and N. Li, "Image Forensic Signature for Content Authenticity Analysis," *J. Vis. Comun. Image Represent.*, vol. 23, no. 5, pp. 782–797, Jul. 2012.
10. I. Cox, M. L. Miller, and J. A. Bloom, *Digital watermarking*. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2002.
11. C. Rey and J.-L. Dugelay, "A Survey of Watermarking Algorithms for Image Authentication," *EURASIP J. Adv. Signal Process.*, vol. 2002, no. 6, pp. 613–621, 2002.
12. J. G. R. Elwin, T. S. Aditya, and S. M. Shankar, "Survey on Passive Methods of Image Tampering Detection," *Int. Conf. Commun. Comput. Intell.*, pp. 431–436, 2010.
13. D. G. Lowe, "Distinctive Image Features from Scale-Invariant Keypoints," *Int. J. Comput. Vis.*, vol. 60, no. 2, pp. 91–110, Nov. 2004.
14. H. Bay, A. Ess, T. Tuytelaars, and L. Van Gool, "Speeded-Up Robust Features (SURF)," *Comput. Vis. Image Underst.*, vol. 110, pp. 346–359, 2008.
15. I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 1099–1110, 2011.
16. D. M. Uliyan, H. A. Jalab, A. W. A. Wahab, and S. Sadeghi, "Image Region Duplication Forgery Detection Based on Angular Radial Partitioning and Harris Key-Points," *Symmetry (Basel).*, vol. 8, no. 7, 2016.
17. S. Leutenegger, M. Chli, and R. Y. Siegwart, "BRISK : Binary Robust Invariant Scalable Keypoints," in *2011 IEEE International Conference on Computer Vision*, 2011, pp. 2548–2555.
18. J. Wang, "Detection of Image Region Duplication Forgery Using Model with Circle Block," in *2009 International Conference on Multimedia Information Networking and Security Detection*, 2009, pp. 25–29.
19. B. L. Shivakumar and S. Baboo, "Detection of Region Duplication Forgery in Digital Images Using SURF," *Int. J. Comput. Sci. Issues*, vol. 8, no. 4, pp. 199–205, 2011.
20. C. R. V. Christlein, J. Jordan, C. Riess, and E. Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 6, pp. 1841–1854, 2012.
21. A. Kaur, S. Walia, and K. Kumar, "Comparative analysis of different keypoint based copy-move forgery detection methods," in *Proceedings of 2018 Eleventh International Conference on Contemporary Computing (IC3)*, 2018, pp. 172–176.
22. M. Hassaballah, A. A. Abdelmgeid, and H. A. Alshazly, *Image Features Detection , Description and Matching*. Springer, Cham, 2016.
23. E. Karami, S. Prasad, and M. Shehata, "Image Matching Using SIFT , SURF , BRIEF and ORB : Performance Comparison for Distorted Images," in *2015 Newfoundland Electrical and Computer Engineering Conference*, 2015.
24. J. Dong, W. Wang, and T. Tan, "CASIA Image Tempering Detection Evaluation Database (CAISA TIDE)," in *2013 IEEE China Summit and International Conference on Signal and Information Processing*, 2013, pp. 422–426.