Chapter 8
Copy–Move Forgery Detection by Using Key-Point-Based Harris Features and CLA Clustering

Kavita Rathi and Parvinder Singh

Abstract Images can easily be manipulated without any visual marks to the naked human eye with massive improvements in image manipulation software. This tampering is the main propelling force for the need of better image forensics such that field is known as image forgery detection. Any digital image with regions where the image contents are identical is said to have copy–move forgery (CMF). Copy–move forgery is performed to improve the visual features or to cover the underlying truth in the image. Many algorithms have been used for CMF detection, and this work is about improved key-point and clustering-based CMF detection scheme. The proposed scheme combines the efficiency of a key-point-based scheme and clustering of these key points to further improve the results. Modified Harris operator-based key-point detection algorithm with clustering using local gravitation is utilized for key-points selection. The average accuracy, PSNR and SSIM rates are used to evaluate the performance of the proposed algorithm with scale-invariant feature transform (SIFT), which is another state-of-the-art key-point algorithm. The paper concluded with the efficiency of the key-point-based scheme.

8.1 Introduction

Image forensics is a vast field used to verify the images to ascertain credibility and authenticity by using various computation approaches [1, 2]. Image forensics is attracting a lot of attention due to its possible applications in various domains. There are various methods in image forgery detection, which can be categorized as active (copy–move forgery detection) and passive (blind forgery detection) [3]. The copy–move forgery detection algorithms are concerned with revealing the forgery

K. Rathi (✉) · P. Singh
Deenbandhu Chhotu, Ram University of Science and Technology, Murthal 131039, India
e-mail: kavita1217@gmail.com

P. Singh
e-mail: Parvindersingh.cse@dcrustm.org

R. Kountchev et al. (eds.), *New Approaches for Multidimensional Signal Processing*,
Smart Innovation, Systems and Technologies 216,
https://doi.org/10.1007/978-981-33-4676-5_8

Fig. 8.1 Copy–move image forgery example [5]

used for hiding the underlying truth or to improve the visual features in the image. However, the process which alters the visual features of the image changes original metadata in the image [4].

A large number of tempered images exist now; one of such, which is example of copy–move forgery from CMFD dataset [5] is presented in Fig. 8.1. A large number of image forgery detection algorithms have been developed over the years, and the efficiency of the existing image forgery detection algorithm is low.

The efficiency of these algorithms is improved with the advent of key-point-based feature detection such as SIFT [6] and speeded-up robust features (SURF) [7] algorithms. The main algorithms for active forgery detection use key-point-based features detection, such as SIFT, algorithms combine with some clustering algorithms, such as K-means. This work is about the improvement of the existing state-of-the-art active image forensics with improved key-point mechanism and improved clustering procedure. For the key points, we have used the Harris key-point detector to improve the computation efficiency and the CLA clustering to improve the clustering procedure.

8.2 Related Works

The existing research in image forensics mainly focuses on improving the feature extraction and clustering stages [6]. Image forensics uses combined methods involving different kinds of key point and feature descriptors; one such example is presented in [7], where Harris corner and SIFT descriptor are used. The key points and feature vectors can be extracted in different color spaces; one of such example of extracting the feature by using the SURF in the opponent color space is presented in [8]. Adaptive non-maximal suppression algorithm is used for smooth tampered regions to select Harris corners and extracted DAISY descriptors in [9]. A two-stage

detection method to detect tempering by using Harris corners and extracted multi-support regions order-based gradient histogram (MROGH) and hue histogram (HH) descriptors is presented in [10]. Both methods using extracted DAISY descriptor and extracted MROGH and HH descriptors have poor owing to the adoption of the Harris corner and poor robustness to scaling. Some methods that integrated block-based and key-point-based methods have been proposed in the last two years. A method based on multi-scale analysis and voting processes determining the range of suspicious feature regions for matching and clustering by using SURF and then block-based method to detect tampered regions in the multi-scale space is presented in [11]. Adaptive over-segmentation and the forgery region extraction algorithm are presented in [12] to detect tampered regions. Feature extraction by DCT, clustering by using k-means and feature matching done by radix sort in [13]. Guaranteed outlier removal is clubbed with key-point-based algorithm to improve the efficiency and robustness in [14]. Techniques for uniformly scattered key-points are adopted with Laplace of Gaussian in [15] for improving the results in smooth areas. A combination of image segmentation and iterative nearest neighborhood methods for detecting suspected tempering and then to gradually improve the detection precision is used in [16]; however, the computational cost of this method is prohibitive for large images.

8.3 SIFT K-Means Algorithm

The SIFT-based image forgery detection approach uses the key-point detector. The scale space S of image $I(x, y)$ is $S(x, y, \sigma)$

$$S(x, x, \sigma) = I(x, y) * G(x, y, \sigma) \tag{8.1}$$

where $G(x, y, \sigma)$ is variable scale Gaussian

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{\frac{-(x^2+y^2)}{2\sigma^2}} \tag{8.2}$$

where σ is standard deviation of $G(x, y, \sigma)$.

Hessian matrix-based Hessian operator is used for key-point detection. The Hessian matrix $H(x, s)$ for x at scale s for a given image point $x = (x, y)$ in the image I(x, y) is defined by its Laplacian of Gaussian (LoG) as

$$H(x, \sigma) = \begin{bmatrix} L_{xx}(x, \sigma) & L_{xy}(x, \sigma) \\ L_{xy}(x, \sigma) & L_{yy}(x, \sigma) \end{bmatrix} \tag{8.3}$$

where $L_{xx}(x, \sigma)$ is the convolution of the Laplacian of Gaussian (LoG) which is the second-order derivative $\frac{\partial^2 G}{\partial x^2}$ in point x for image $I(x, y)$, and similarly for $L_{xy}(x, \sigma)$, and $L_{yy}(x, \sigma)$.

To suppress the noise before using Laplace for edge detection

$$\Delta[G_\sigma(x, y) * f(x, y)] = [\Delta G_\sigma(x, y)] * f(x, y) = LoG * f(x, y) \tag{8.4}$$

The first equal is due to the fact

$$\begin{aligned} \frac{\mathrm{d}}{\mathrm{d}t}[h(t) * f(t)] &= \frac{\mathrm{d}}{\mathrm{d}t} \int f(\tau) h(t - \tau) \mathrm{d}\tau \\ &= \int f(\tau) \frac{\mathrm{d}}{\mathrm{d}t} h(t - \tau) \mathrm{d}\tau = f(t) * \frac{\mathrm{d}}{\mathrm{d}t} h(t) \end{aligned} \tag{8.5}$$

First, consider Laplacian of Gaussian (LoG)

$$\begin{aligned} \frac{\partial^2}{\partial x^2} \left(\frac{1}{2\pi\sigma^2} \mathrm{e}^{\frac{-(x^2+y^2)}{2\sigma^2}} \right) &= \frac{x^2}{\sigma^4} \mathrm{e}^{\frac{-(x^2+y^2)}{2\sigma^2}} - \frac{1}{\sigma^2} \mathrm{e}^{\frac{-(x^2+y^2)}{2\sigma^2}} \\ &= \frac{x^2 - \sigma^2}{\sigma^4} \mathrm{e}^{\frac{-(x^2+y^2)}{2\sigma^2}} \end{aligned} \tag{8.6}$$

For simplicity, normalizing coefficient $1/\sqrt{2\pi\sigma^2}$ is omitted and the convolution of Laplace of Gaussian (LoG) is done by using Eq. 8.7.

$$\begin{aligned} \Delta G_\sigma(x, y) &= \frac{\partial^2}{\partial x^2} G_\sigma(x, y) + \frac{\partial^2}{\partial y^2} G_\sigma(x, y) \\ &= \frac{x^2 + y^2 - 2\sigma^2}{\sigma^4} \mathrm{e}^{\frac{-(x^2+y^2)}{2\sigma^2}} \end{aligned} \tag{8.7}$$

All key points are checked for the presence of local extreme, i.e., either lowest or highest. The extreme key points are used to localize the key-point localization edge. Low contrast points and poorly localized points along edges are removed to discard noise and instability of local minima maxima points, which is done by discarding the functional value of $L(\hat{x})$ above a threshold (usually 0.5). The functional value of $L(\hat{x})$ is computed by using equation

$$L(\hat{x}) = L + \frac{1}{2} \frac{\partial L^T}{\partial x} (\hat{x}) \tag{8.8}$$

where $\hat{x}$ is the location of extremum and is determined by

$$\hat{x} = \frac{\partial^2 L^{-1}}{\partial x^2} \frac{\partial L}{\partial x} \tag{8.9}$$

With scale-space function, $L(x, y, \sigma)$ can be shifted to compute the origin of the sample point by

$$L(x) = L + \frac{\partial L^T}{\partial x}x + \frac{1}{2}x^T\frac{\partial^2 L}{\partial x^2}x \tag{8.10}$$

where L and its derivatives are evaluated at the same point and $x = (x, y, \sigma)^T$ is offset from this point.

The key points are clustered by using the k-means clustering with minimization problem of two parts.

$$J = \sum_{i=1}^{m}\sum_{k=1}^{K}\omega_{ik}\left|\left|x^i - \mu_k\right|\right|^2 \tag{8.11}$$

where $\omega_{ik} = 1$ for all points belonging to cluster k; else 0 with μ_k as centroid of cluster.

$$\frac{\partial J}{\partial \omega_{ik}} = \sum_{i=1}^{m}\sum_{k=1}^{K}\left|\left|x^i - \mu_k\right|\right|^2 \tag{8.12}$$

$$\omega_{ik} = \begin{cases} 1 \text{ if } k = \arg\min_j \left|\left|x^i - \mu_k\right|\right|^2 \\ 0 \text{ otherwise} \end{cases} \tag{8.13}$$

$$\frac{\partial J}{\partial \mu_k} = 2\sum_{i=1}^{m}\omega_{ik}\left(x^i - \mu_k\right) = 0 \tag{8.14}$$

$$\mu_k = \frac{\sum_{i=1}^{m}\omega_{ik}x^i}{\sum_{i=1}^{m}\omega_{ik}} \tag{8.15}$$

The SIFT k-means algorithm involves.

- Transformation of RGB image to grayscale.
- Calculation of Hessian matrix of grayscale image.
- Key-point-based feature extraction using SIFT algorithm.
- Select strongest matching key points for matching forgery features.
- Key-point clustering by using k-means algorithm.
- Localize and mark each as clustered region with more than pre-specified group of pixels as forged.
- Show forged regions.

The flowchart of the proposed SIFT k-means algorithm for the detection of tempering is presented in Fig. 8.2.

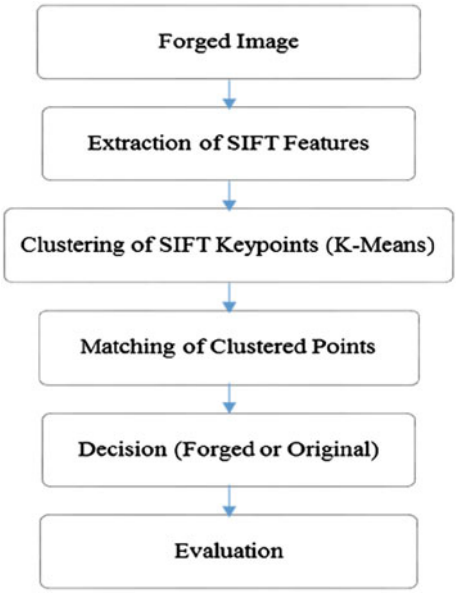

Fig. 8.2 SIFT k-means forgery detection algorithm

8.4 Proposed Key-Point-Based Harris CLA Clustering Scheme

The Harris key-point detection algorithm works with extracting point features of the images. Harris algorithms utilize the work window ω to search key points (u, v) in any direction of the image. In order to improve the noise capabilities of the Harris algorithm, we have selected the Gaussian window

$$E(u, v) = \sum_{x,y} \omega(x, y)[I(x + u, y + v) - I(x, y)]^2 \tag{8.16}$$

where $\omega(x, y)$ is the window function and u, v are small displacements used to search, $I(x, y)$ is the intensity function of the image, and $I(x + u, y + v)$ is the shifted intensity of the image using Taylor expansions

$$E(u, v) \approx [uv]M\begin{bmatrix} u \\ v \end{bmatrix} \tag{8.17}$$

where M is given by

$$M = \sum_{x,y} \omega(x, y)\begin{bmatrix} I_x I_x & I_x I_y \\ I_y I_x & I_y I_y \end{bmatrix} \tag{8.18}$$

where I_x and I_y are image derivatives.

CLA-based clustering is used to calculate the forged regions. The objective of CLA-based clustering is to group features into homogeneous classes by using a set of conditions. Each key point in the class is very similar in terms appearance, and different features usually belong to other groups. It is inspired by Newton's gravitational theory for reflecting the relation of a data point to its neighbors.

$$\overrightarrow{F_{12}} = G\frac{m_1 m_2}{D_{12}^2}\widehat{D_{12}} \tag{8.19}$$

where $\overrightarrow{F_{12}}$ is the attractive force between two points of mass m_1 and m_2 located at distance D_{12}, G is gravitational constant, and $\widehat{D_{12}}$ is unit vector specifying the direction of force.

The distance between the neighbors does not vary significantly in a local region, so,

$$\overrightarrow{F_{12}} = Gm_1 m_2\widehat{D_{12}} \tag{8.20}$$

Therefore, the total local resultant force at a point i from its k neighbors is

$$\overrightarrow{F_i} = Gm_i\sum_{j=1}^{k} m_j\widehat{D_{ij}} \tag{8.21}$$

The number of cluster will be dependent on the threshold value of centrality with lower bound 0 and upper bound $m_i\sum_{j=1}^{k} m_j D_{ij}$.

The proposed key-point-based Harris CLA clustering scheme involves the following steps.

- Initialize the number of clusters to be used usually for image forgery, 8 to 10 points are used.
- Select input features for which clustering of key points will be done.
- Using the Euclidian similarity measure find distances
- Stepwise cluster/group the key points using hierarchical clustering involving a combination and division of the features into a set of clusters.
- If cluster group contains enough neighbors, then validate and select the cluster as a forged region.

The brief flowchart of the Harris CLA clustering scheme is presented in Fig. 8.3.

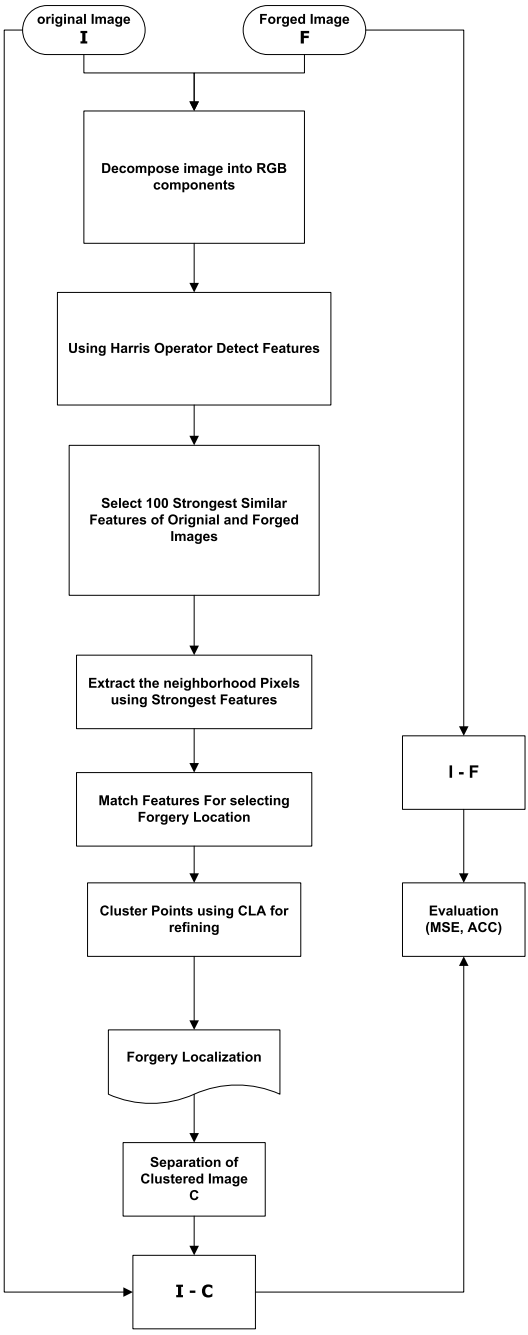

Fig. 8.3 Proposed key-point based-Harris CLA clustering scheme

8.5 Experimental Analysis

An Intel Core i3 central processing unit having 8 GB random-access memory and operating system raring at 2.4 GHz by using Windows 7 and 64-bit operating system is used for executing the proposed methodology. The proposed methodology is implemented in MATLAB 2016a. The dataset used for analyzing the SIFT k-means and the proposed algorithm is copy–move forgery. The copy–move forgery dataset [5] has four subsets $D0$, $D1$, $D2$, and $D3$ consisting of 1020 image with image size 1000 $\times$ 700 to 700 $\times$ 1000 pixels in JPEG format. It has attacks in the form of plain copy, scaling, and rotation with availability of ground truth. The dataset is freely downloadable [17]. A sample of the results by the proposed algorithm is presented below in Fig. 8.4.

Average accuracy, PSNR, and SSIM are used as metric for performance evaluation on various images. Accuracy (ACC) of the proportions of correctly identified predicted pixels is:

$$\text{Accuracy(ACC)} = \frac{T_p + T_n}{T_p + T_n + F_p + F_n} \tag{8.22}$$

PSNR is measurement of quality between the original forgery from ground truth and retrieved forgery in image. It is calculated in decibels by using the PSNR block from mathworks, which uses the mean square error (MSE). The mean square error is cumulative squared error between ground truth and retrieved forgery. The higher PSNR value represents the better quality of identified forgery [17]. For MxN size image I_1 and I_2.

$$\text{MSE} = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M \times N} \tag{8.23}$$

$$\text{PSNR} = 10\ \log_{10}\left(\frac{R^2}{\text{MSE}}\right) \tag{8.24}$$

Fig. 8.4 Sample of CMFD by using the proposed Harris corner CLA clustering algorithm (original, forged, and detected from left to right)

R is image dependent, R for image having double-point floating data is 1, and R for unassigned 8-bit image is 255.

SSIM is the weighted combination of contrast, luminance, and structure [18].

$$\mathrm{SSIM}(I_1, I_2) = \left[l(I_1, I_2)^{\alpha}.c(I_1, I_2)^{\beta}.s(I_1, I_2)^{\gamma}\right] \tag{8.25}$$

The SSIM with α, β, and γ weights as 1 is below.

$$\mathrm{SSIM}(I_1, I_2) = \frac{\left(2\mu_{I_1}\mu_{I_2} + c_1\right)\left(2\sigma_{I_1 I_2} + c_2\right)}{\left(\mu_{I_1}^2 + \mu_{I_2}^2 + c_1\right)\left(\sigma_{I_1}^2 + \sigma_{I_2}^2 + c_2\right)} \tag{8.26}$$

μ, σ^2, and c are average, variance, and variables for stabilizing denominator.

For experimental analysis, various images were considered for the evaluation. The average of each examining parameter was calculated. The average accuracy, PSNR and SSIM rates of SIFT k-means and key-point-based Harris CLA clustering scheme are presented in Table 8.1 and Fig. 8.5.

It is clear from the results that the proposed key-point-based Harris CLA clustering scheme performs better. The proposed key-point-based Harris CLA clustering scheme achieves average accuracy of 98.51%, which is 6.24% higher than SIFT k-means whose average accuracy performance is 92.27%. The average PSNR for the proposed key-point-based Harris CLA clustering scheme is 48.63%, which has still huge potential for improvement, but the proposed scheme out performed which is about 65% more than SIFT k-means at 29.34. The average structural similarity (SSIM) for the proposed key-point-based Harris CLA clustering scheme is 95.90%, which is again about 4% higher than SIFT k-means whose average SSIM is 95.90%.

Table 8.1 Performance of SIFT k-means and the proposed key-point-based Harris CLA clustering scheme on accuracy, PSNR and SSIM metric

Metric	SIFT k-means	Proposed Harris CLA
Accuracy	92.27	98.51
PSNR	29.34	48.63
SSIM	95.90	99.13

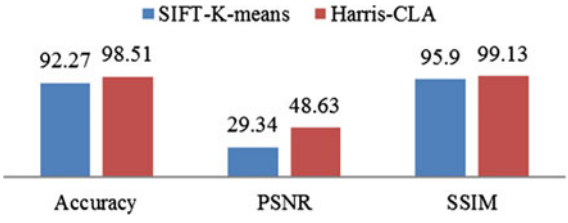

Fig. 8.5 Results of image forgery detection performance of SIFT k-means and the proposed key-point-based Harris CLA clustering scheme on accuracy, PSNR, and SSIM metric

8.6 Conclusion and Future Scope

Copy–move forgery is performed to improve the visual features or to cover the underlying truth in the image. A new key-point-based Harris CLA clustering scheme is proposed which combines the efficiency of a key-point-based scheme and clustering of these key points to further produced better results. Experimental results established that the proposed key-point-based Harris CLA clustering scheme has improved the efficiency of detection process over the key-point detection scheme, namely SIFT k-means. In future work, parallel programming can be tried to improve the detection speed of the proposed scheme. Researchers can also focus on other types of image forgeries.

Acknowledgements This work is part of bilateral Indian-Bulgarian cooperation research project between Technical University of Sofia, Bulgaria, and Deenbandhu Chhotu Ram University of Science and Technology, Murthal, Sonepat, India, under the title "Contemporary Approaches for Processing and Analysis of Multidimensional Signals in Telecommunications," financed by the Department of Science and Technology (DST), India, and the Ministry of Education and Science, Bulgaria.

References

1. Farid, H.: Image forgery detection. IEEE Signal Process. Mag. **26**(2), 16–25 (2009). https://doi.org/10.1109/MSP.2008.931079
2. Birajdar, G.K., Mankar, V.H.: Digital image forgery detection using passive techniques: a survey. Digit. Investig. **10**(3), 226–245 (2013). https://doi.org/10.1016/j.diin.2013.04.007
3. 3Qureshi, M.A., Deriche, M.: A review on copy move image forgery detection techniques. In: 2014 IEEE 11th International Multi-Conference Systems Signals Devices, SSD 2014, pp. 1–5 (2014). https://doi.org/10.1109/SSD.2014.6808907
4. Shivakumar, B.L., Baboo, S.S.: Detecting copy-move forgery in digital images: a survey and analysis of current methods. Glob. J. Comput. Sci. Technol. **10**(7), 61–65 (2010)
5. 5E. Ardizzone, Bruno, A., and Mazzola, G., Copy-Move Forgery Detection by Matching Triangles of Keypoints, IEEE Trans. Inf. Forensics Secur., 10(10), 2084–2094, (2015), doi: https://doi.org/10.1109/TIFS.2015.2445742.
6. Shivakumar, B.L., Baboo, S.S.: Detection of region duplication forgery in digital images using SURF. Int. J. Comput. Sci. **8**(4), 199–205 (2011)
7. Shivakumar, B.L., Baboo, S.S.: Automated forensic method for copy move forgery detection based on Harris interest points and SIFT descriptors. Int. J. Comput. Appl. **27**(3), 9–17 (2011). https://doi.org/10.5120/3283-4472
8. Gong, J., Guo, J.: Image copy-move forgery detection using SURF in opponent color space. Trans. Tianjin Univ. **22**(2), 151–157 (2016). https://doi.org/10.1007/s12209-016-2705-z
9. Guo, J.M., Liu, Y.F., Wu, Z.J.: Duplication forgery detection using improved DAISY descriptor. Expert Syst. Appl. **40**(2), 707–714 (2013). https://doi.org/10.1016/j.eswa.2012.08.002
10. Yu, L., Han, Q., Niu, X.: Feature point-based copy-move forgery detection: covering the non-textured areas. Multimed. Tools Appl. **75**(2), 1159–1176 (2014). https://doi.org/10.1007/s11042-014-2362-y
11. Silva, E., Carvalho, T., Ferreira, A., Rocha, A.: Going deeper into copy-move forgery detection: exploring image telltales via multi-scale analysis and voting processes. J. Vis. Commun. Image Represent. **29**, 16–32 (2015). https://doi.org/10.1016/j.jvcir.2015.01.016

12. Pun, C.M., Yuan, X.C., Bi, X.L.: Image forgery detection using adaptive oversegmentation and feature point matching. IEEE Trans. Inf. Forensics Secur. **10**(8), 1705–1716 (2015). https://doi.org/10.1109/TIFS.2015.2423261
13. Parveen, A., Khan, Z.H., Ahmad, S.N.: Block-based copy–move image forgery detection using DCT. Iran J. Comput. Sci. **2**(2), 89–99 (2019). https://doi.org/10.1007/s42044-019-00029-y
14. 14Hegazi, A., Taha, A., Selim, M.M.: An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal. J. King Saud Univ. Comput. Inf. Sci. (2019). https://doi.org/10.1016/j.jksuci.2019.07.007
15. Wang, X.Y., Wang, C., Wang, L., Jiao, L.X., Yang, H.Y., Niu, P.P.: A fast and high accurate image copy-move forgery detection approach. Multidimens. Syst. Signal Process. **31**(3), 857–883 (2019). https://doi.org/10.1007/s11045-019-00688-x
16. Li, J., Li, X., Yang, B., Sun, X.: Segmentation-based image copy-move forgery detection scheme. IEEE Trans. Inf. Forensics Secur. **10**(3), 507–518 (2015). https://doi.org/10.1109/TIFS.2014.2381872
17. Mathworks, compute peak signal-to-noise ratio (PSNR) between images. MathWorks India (2020). https://in.mathworks.com/help/vision/ref/psnr.html. Accessed Jul 04 2020
18. Wang, Z., Simoncelli, E.P., Bovik, A.C.: Multi-scale structural similarity for image quality assessment. Conf. Record Asilomar Conf. Signals Syst. Comput. **2**, 1398–1402 (2003). https://doi.org/10.1109/acssc.2003.1292216