



# BRISK and SIFT-based Copy-Move Forgery Detection of Digital Images

Sundar Uma<sup>1\*</sup>, and P. D. Sathya Sakhivel

<sup>1</sup> Department of Electronics and Communication Engineering, Annamalai University, Tamil Nadu-608002, INDIA.

\*Corresponding Author (Tel: +91-7845453223, Email: [umasumi13@gmail.com](mailto:umasumi13@gmail.com)).

**Paper ID: 12A3H**

**Volume 12 Issue 3**

Received 01 October 2020

Received in revised form 14  
December 2020

Accepted 23 December  
2020

Available online 12 January  
2021

## Keywords:

Copy-move forgery  
(CMF); BRISK algorithm;  
K-means clustering;  
Key-point technique;  
Image forgery; SIFT  
algorithm; CMFD.

## Abstract

This paper presents a simple method for copy-move forgery detection (CMFD) of digital images with a view of enhancing the computational speed. The method employs BRISK, which is based on the FAST corner detector, for identifying the key points (KPs), and then uses SIFT for evaluating the feature descriptors at the identified KPs. It also applies wavelet transform for feature reduction and K-means clustering for transforming from feature space into cluster space. It eliminates false matches by using RANSAC. The paper exhibits the superior performances of the developed method over existing methods by presenting results on 500 digital images.

**Disciplinary: Electronics and Digital Engineering.**

©2021 INT TRANS J ENG MANAG SCI TECH.

## Cite This Article:

Uma, S., and Sakhivel, P. D. S. (2021). BRISK and SIFT-based Copy-Move Forgery Detection of Digital Images. *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies*, 12(3), 12A3H, 1-12. <http://TUENGR.COM/V12/12A3H.pdf> DOI: 10.14456/ITJEMAST.2021.50

## 1 Introduction

Copy-move forgery (CMF) is a commonly used technique for doctoring digital images by simply copying a part of an image and pasting it on the same image. Such forged images must be detected before using them as evidence in the law of court, insurance claim, and so on. Due to the flexible and easily available image editing tools, everyone with little knowledge tampers the images either with malicious intent or for creating fun, thereby causing damage to the credibility of the images. Besides, such tampering in images cannot be detected by naked eyes. Image forgery detection has turned out to be a hot topic among researchers and has become a tool for detecting the authenticity of the given digital images (Warif *et al.*, 2016).

Several techniques were suggested in recent decades for forgery detection and categorized into block-based and key-point (KP) based techniques (Zhang *et al.*, 2018). The former ones divide

the image into several small blocks and extract features from each block, and then perform feature matching among the blocks for forgery detection. The block-based techniques are computationally inefficient and fail to detect geometrically altered images. The KP-based techniques identify a small number of KPs and evaluate features at these KPs, and are preferred due to their computational efficiency and invariant to geometrical transformations. Singular value decomposition (SVD) and discrete wavelet transform (DWT) were applied to each cascaded block to obtain reduced features, and Lexicographical sorting was performed before performing the matching among the blocks for forgery detection (Li *et al.*, 2007). The dyadic wavelet transform was applied on features of each cascaded block for obtaining reduced sub-bands and feature matching was performed on these reduced sub-bands for forgery detection (Muhammad *et al.*, 2012). MROGH descriptors were evaluated at KPs, obtained by Harris Corner Detector, with a view of achieving uniform distribution of features and robustness against geometrical transformations (Yu *et al.*, 2014). KD-Tree was applied on the evaluated SURF features for multidimensional data matching in performing forgery detection (Shivakumar and Baboo, 2017). The agglomerative hierarchical clustering was applied on the evaluated SURF features and 2NN feature matching was performed for avoiding false matches (Kiruthika *et al.*, 2019). The SURF descriptors were evaluated and the K-nearest neighbour search was performed for forgery detection with a view of getting better reproducibility and robustness (Paul *et al.*, 2019). Discrete Cosine Transformation (DCT), SVD, and SVM were employed in detecting image forgery at the frequency domain with a view of lowering the dimension of features and enhancing the classification accuracy (Priyanka *et al.*, 2020). The KP-based SURF descriptors were evaluated and dynamic histogram equalization was applied for effective forgery detection even on images with smooth forged regions (Bilal *et al.*, 2020a). A SURF-based technique was suggested for detecting forgeries with geometrical transformations (Bilal *et al.*, 2020b). The block and KP-based forgery detection techniques were surveyed while outlining various feature extraction and matching techniques and mentioning the research gaps (Warif *et al.*, 2016). A few forgery detection techniques were reviewed besides narrating the several performance measures for assessing the forgery detection methods and showing the research gaps (Zhang *et al.*, 2018).

Although, the SIFT and SURF-based forgery detection methods yield successful results in forgery detection and are robust to geometric transformations in the forged regions. Still, these approaches are computationally inefficient involving large computations for both identifying the KPs and computing the descriptors.

The KP detector should find prominent image regions in such a way that they are repeatedly identified and robust to different image transformations and viewpoints. Similarly, the KP descriptor should represent the most significant and unique features at the identified KPs, in such a way that the same image region can be detected if encountered. Moreover, the speed of such detection and description needs to be optimized to make it suitable for online applications in addition to producing high-quality results.

Recently, BRISK descriptors were suggested for KP identification and feature extraction (Warif *et al.*, 2016; Zhang *et al.*, 2018). As the KP identification is based on the FAST corner detector, BRISK has the advantage of higher speed but has poor reliability and robustness as it is sensitive to image distortions and transformations. This paper thus attempts to exploit the superior features of both BRISK and SIFT in obtaining fast KPs and robust feature descriptors respectively. The proposed method has been applied on 500 test images and the results are presented in this paper.

## 2 Proposed Method

The proposed CMFD (PCMFD) involves a series of functions. Initially, it converts the RGB colour scale image into grayscale and removes the noise. It identifies the KPs by BRISK and extracts the features by SIFT. It clusters the features by K-means clustering and performs feature matching and removal of false matches by Random Sample Consensus (RANSAC). The block diagram of the PCMFD is shown in Figure 1, and the various blocks are explained in this section:

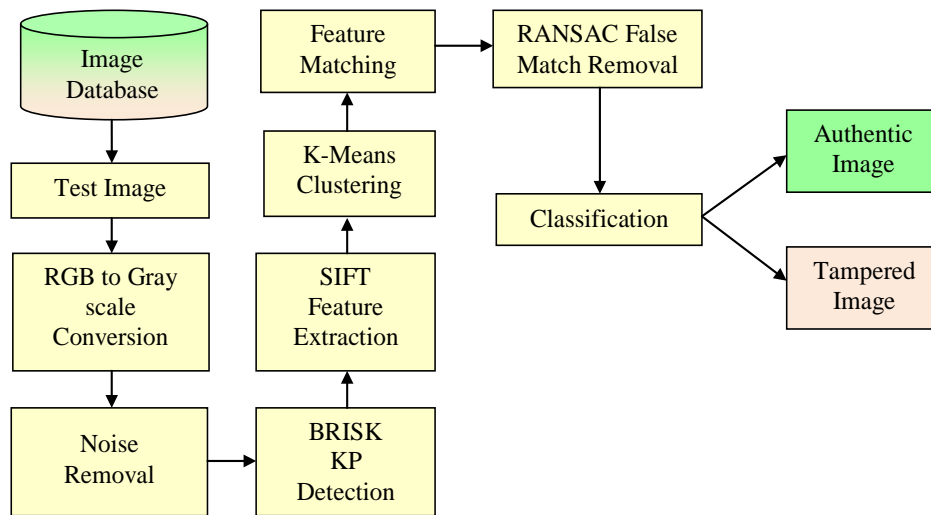


Figure 1: Block diagram of PCMFD

### 2.1 Identification of KPs

SIFT is an algorithm for evaluating both the KPs and their feature descriptors. SIFT uses a time consuming procedure involving Difference of Gaussian (DoG) images in scale space to identify scale-invariant KPs. Instead of evaluating the SIFT KPs, the proposed method uses the fast BRISK algorithm for identifying KPs. BRISK is based on the FAST corner detector involving a Bresenham circle to classify whether a candidate pixel is a corner or not. It performs a test at a pixel-  $m$  by forming a Bresenham circle of radius 3 and examining the 16 pixels around that circle  $n \in \{1 \dots 16\}$  as illustrated in Figure 2. It detects  $m$  as a corner if 9 contiguous pixels in the circle are darker than  $(I_m - q)$  or brighter than  $(I_m + q)$ , where  $q$  is a chosen threshold.

$$Q_{bright} = \{n | I_{m \oplus n} \geq I_m + q\}$$

$$Q_{dark} = \{n | I_{m \oplus n} \leq I_m - q\}$$

(1),

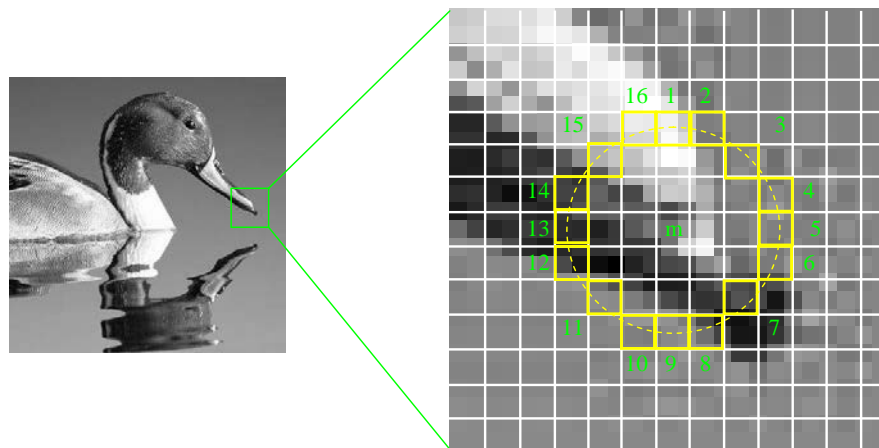
where

$I_{m@n}$  indicates the intensity of point-  $m$  in the circle around pixel-  $n$ .

$Q_{bright}$  is a set of points in the circle, which are brighter.

$Q_{dark}$  is a set of points in the circle, which are darker.

BRISK is insensitive to scale changes as it identifies corner pixels in different scale space using 9-16 masks. FAST identification is adapted at four octave levels, and the interest regions are computed from neighboring pixels. All the points in the chosen regions are subjected to non-maximum suppression, and identified as corner points, if they satisfy the maximum condition with respective to their neighbours.



**Figure 2:** Bresenham circle around point-m.

## 2.2 Feature Extraction and Reduction

SIFT descriptors are computed at each identified BRISK KPs. The procedure involving the formation of a 16x16 window around each KP and partitioning the window into sixteen 4x4 patches. It then evaluates the gradients and orientations and arranges them into an 8 bin histogram using a "Gaussian weighting function" for each 4x4 patch, thereby resulting in 128 (4x4x8) unique descriptors. It finally normalizes the 128 values and represents them as descriptors to the respective KP. The length of each feature vector is so large and increases the time involved in matching. The size of each feature vector can be reduced by applying DWT, which uses the dyadic positions and scales and is powerful in yielding good results. The feature vector is arranged into a matrix of (16 x 8) and the DWT is applied to obtain the reduced approximation components of (8 x 4) LL sub-band matrix, which is rearranged to have a (1 x 32) sized reduced feature vector.

## 2.3 K-means Clustering

K-means clustering is an unsupervised learning algorithm for classifying the feature space into a K-number of clusters by grouping similar objects based on features. It partitions the points in the feature matrix  $[x]$  of size  $(N \times D)$  into K number of clusters  $[c_1, c_2, \dots, c_k]$ . Rows of the feature matrix correspond to feature points and columns correspond to variables. This algorithm exploits the approximation of the nearest neighbour method in finding the nearest neighbouring features

and the cluster centre. The clustering is thus performed by minimizing the sum of squares of Euclidean distances between observed features and the corresponding cluster centroids.

$$\text{Minimize } F = \sum_{m=1}^K \sum_{n=1}^N \|x_n - c_m\|^2 \quad (2),$$

where

$$\|x_n - c_m\| = \sqrt{\sum_{i=1}^D (x_{ni} - c_{mi})^2} \quad (3)$$

represents Euclidean distance

$x_n$  represents the  $n$ -th row of the feature matrix, representing  $n$ -th feature

$x_{ni}$  denotes the  $i$ -th variable of the  $n$ -th feature.

$c_m$  represents the  $m$ -th cluster.

$c_{mi}$  denotes the  $i$ -th variable of the  $m$ -th cluster centre.

$N$  denotes the number of feature points

$D$  represents the number of values in each feature vector

The steps involved in the K-means algorithm are outlined below:

1. Select the value for  $K$ , that is, the number of clusters.
2. Randomly generate values for  $K$  number of cluster centres  $\{c_{mi}\}, m = 1: K, i = 1: D$
3. Assign each feature point to the nearest cluster point by computing the Euclidean distance.
4. Compute new values for cluster centres that minimize Equation (2).
5. Repeat the steps (3) and (4) till there is no change between subsequent cluster centre values.

All cluster centers, obtained by the K-means algorithm, form the visual word vocabulary, wherein each visual word represents a cluster centre. The visual vocabulary has to be formed through learning from a given feature database. The procedure for building the visual vocabulary and assignment of the visual word is pictorially depicted in Figure 3.

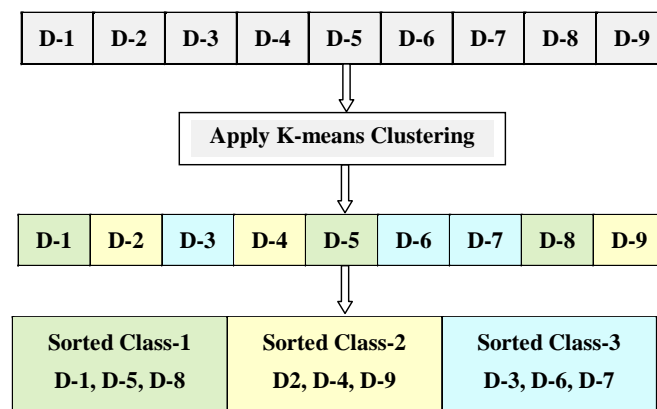


Figure 3: K-means Clustering and Sorting.

## 2.4 Feature Matching and False Match Elimination

The matching between two features  $p$  and  $q$  can be performed by checking whether their Euclidean distance  $d(p, q)$ , computed for 32-dimensional descriptors, is less than a certain

threshold. If the number of matching is larger than three, then that image is classified as a forged one in this paper. The Euclidean distance (Liwei *et al.*, 2005) is evaluated by

$$d(p, q) = \sqrt{\sum_{i=1}^3 (p_i - q_i)^2} < T_d \quad (4).$$

The false matches can be eliminated through the affine geometry model, known as RANSAC (Fischler and Bolles, 1981). The model randomly selects a set of matched KPs and estimates a transformation matrix  $T$ :

$$\begin{bmatrix} \hat{x}_p \\ \hat{y}_p \end{bmatrix} = \begin{bmatrix} T_1 \\ T_2 \\ T_3 \end{bmatrix} \begin{bmatrix} \hat{x}_q \\ \hat{y}_q \end{bmatrix} \quad \hat{U} = [T] \begin{bmatrix} \hat{x}_q \\ \hat{y}_q \end{bmatrix} \quad (5).$$

Then, each KP  $(x_q, y_q)$  is transformed by  $T$  and the distance with its matching KP is computed. If the distance is smaller, the pair is considered as a perfect match (denoted as inliers), otherwise, considered as a false match (represented as an outlier) and discarded.

### 3 Results and Discussion

The PCMFD was applied to an image database comprising 350 tampered images and 150 authentic images. To validate the performances of the PCMFD, the classical CMFD (CCMFD) method involving complete SIFT without feature reduction was also developed. The height and width of the images in the database were not altered during the study. The results of four tampered and one authentic image was presented in this section.

The five test images along with their originals are shown in Table 1, which also gives the dimensions of the images. The widths and heights of these images are proportionally reduced and presented in the table so as to portray the correct shape of the images. After identifying the BRISK and SIFT KPs, they are marked in the respective images and displayed in Table 2. The table also includes the number of identified KPs by the BRISK and SIFT techniques. It can be seen that the number of SIFT KPs is 2-3 times greater than those of BRISK KPs, except for the fourth image. The excessively large number of KPs though increases the quality of the diagnosis, it increases the computational cost.


After performing the KP matching and applying the RANSAC for false KP eliminations, the PCMFD identifies the KPs in the forged regions as marked on images in Table 3. The most important question here is whether the PCMFD is able to produce correct results. It is seen from the table that both the methods were able to identify the first four images as forged ones and the last one as an authentic image, thereby exhibiting that the PCMFD is as accurate as of the CCMFD in diagnosing the images. Though the number of matched KP pairs of the CCMFD is larger than the PCMFD, the computation time taken by the CCMFD is large and may not be suitable for online diagnosis of a large image database, while the PCMFD is able to produce quick and accurate

diagnostic results. Moreover, the number of matched KPs differ due to the nature, smoothness, and gradients of the images.

**Table 1: Original and Forged Images**

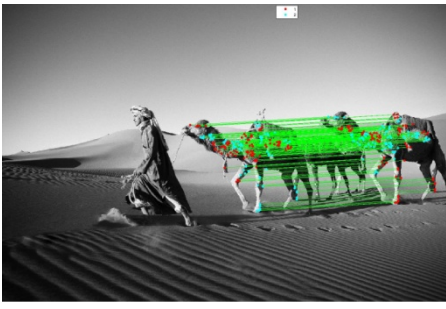
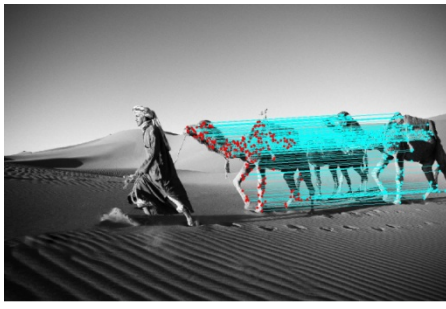

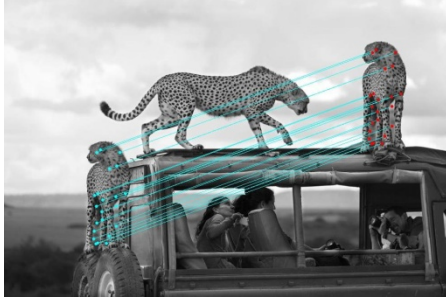
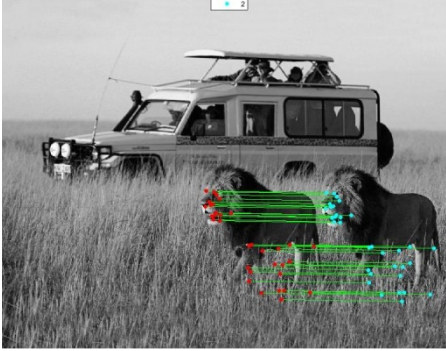

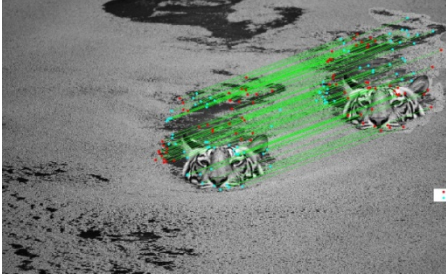
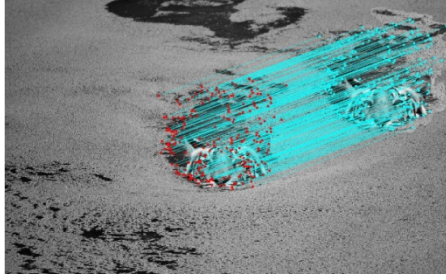


Image No.	Original	Forged	Size
1			1508*984
2			1164*755
3			954*727
4			1454*895
5		Authentic Image	1454*815

**Table 2: Images with clustered KPs**

Image No.	Image with BRISK KPs	No. of KPs	Image with SIFT KPs	No. of KPs
1		3842		7218
2		936		1220
3		687		2196
4		9007		7665
5		2840		4283



**Table 3: Image with Matched KPs.**

Image No.	PCMFD	No. of Matches	CM	No. of Matches
1		165		204
2		10		22
3		33		55
4		85		221
5		0		0

In order to study the performances on a large variety of images, the confusion matrix is formed for the entire image database comprising of 500 images as in Table 4. Both the PCMFD and the CCMFD are able to diagnose the forgery correctly for tampered images 324 and 321 images respectively, thereby indicating that the PCMFD is able to correctly classify 92.57% of the given images, while the CCMFD classifies 91.71%. This indicates that the PCMFD is much better than

CCMFD and the wrong diagnosis of the CCMFD is mainly due to a larger number of KPs leading to false matches. However, both methods correctly categorize the original images as authentic ones.

**Table 4: Confusion Matrix**

				Detected Result	
				Authentic (150)	Tampered (350)
Actual Result	PCMFD	Authentic (150)	TN 150 (100%)	FP 0 (0%)	
		Tampered (350)	FN 26 (7.43%)	TP 324 (92.57%)	
	CCMFD	Authentic (150)	150 (100%)	0 (0%)	
		Tampered (350)	29 (8.29%)	321 (91.71%)	

**Table 5: Comparison of performances**

Method	Accuracy	Sensitivity	Specificity	Precision	F1
PCMFD	94.8	92.57	100.0	100.0	96.14
CCMFD	94.2	91.71	100.0	100.0	95.68
Li et al. (2007)	91.03	--	--	--	--
Yu et al. (2014)	--	91.7	--	93.6	92.6
Shivakumar and Baboo (2017)	--	85.4	--	91.1	88.2
Kiruthika et al. (2019)	--	94	--	--	93

**Table 6: Comparison of NET**

Method	NET (seconds)
PCMFD	10.21
CCMFD	11.96
Yang et al. (2017)	12.4
Huang et al. (2011)	135.12
Fischler et al.(1981)	294.69

The accuracy, sensitivity, specificity, precision, and FI performance indices are also computed for the PCMFD and CCMFD, and compared with a few of the existing published methods in Table 5. It is very clear that all the performances of the PCMFD are better than the CCMFD and existing published results.

The normalized execution time (NET) of the PCMFD, which was run in Matlab 2016 platform using 2.67 GHz Intel Core-i5, 4 GB RAM desktop computer, is compared in Table 6, which clearly indicates that the PCMFD is faster than the other methods. The overall performances of the PCMFD are found to be much better than the literature results, thereby making it suitable for practical online applications.

## 4 Conclusion

A new methodology for performing CMFD of digital images was developed to improve the computational speed. It employed the BRISK algorithm for identifying the KPs and used SIFT for computing the descriptors at identified KPs. As the BRISK is based on fast corner detection, it becomes the prime reason for improved computational speed. Moreover, the number of BRISK KPs is comparatively lower than that of SIFT KPs. The method used K-means clustering and performed Euclidean distance-based KP matching. It then removed the false KP pairs by employing RANSAC.

The study on 500 digital images clearly indicated that the proposed method was able to detect the forgery effectively with a lower computational burden. The comparison of performance indices also indicated superior performances over other methods.

## 5 Availability of Data and Material

Data can be made available by contacting the corresponding author.

## 6 References

- Bilal, M., Habib, H. A., Mehmood, Z., Saba, T., and Rashid, M. (2020b). Single and Multiple Copy–Move Forgery Detection and Localization in Digital Images Based on the Sparsely Encoded Distinctive Features and DBSCAN Clustering. *Arab J Sci Eng.* 45, 2975-2992. DOI: 10.1007/s13369-019-04238-2.
- Bilal, M., Habib, H. A., Mehmood, Z., Yousaf, R. M., Saba, T., and Rehman, A. (2020a). A robust technique for copy-move forgery detection from small and extremely smooth tampered regions based on the DHE-SURF features and mDBSCAN clustering. *Australian Journal of Forensic Sciences.* DOI: 10.1080/00450618.2020.1715479
- Fischler, M., and Bolles, R. (1981). Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography. *Commun ACM.* 24(6), 381-395. DOI: 10.1145/358669.358692.
- Huang, Y., Lu, W., Sun, W., and Long, D. (2011). Improved DCT-based detection of copy-move forgery in images. *Forensic Science International.* 206(1-3), 178-184.
- Kiruthika, K., Mahalakshmi, S. D, and Vijayalakshmi K. (2019). Detecting multiple copies of copy-move forgery based on SURF. *International Journal of Innovative Research in Science, Engineering & Technology,* 8(6S), 676-680.
- Li, G., Wu, Q., Tu, D., and Sun, S. J. (2007). A Sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD. *Proceedings of IEEE International Conference on Multimedia and Expo.* 1750-1753. DOI: 1750-1753. 10.1109/ICME.2007.4285009.
- Liwei, W., Yan, Z., and Jufu, F. (2005). On the Euclidean distance of images. *IEEE Trans Pattern Anal Mach Intell.* 27(8), 1334-1339. DOI: 10.1109/tpami.2005.165.
- Muhammad, G., Hussain, M., and Bebis, G. (2012). Passive copy move image forgery detection using undecimated dyadic wavelet transform. *Digit Investig.* 9(1), 49-57. DOI: 10.1016/j.diin.2012.04.004
- Paul, K. H, Akshatha K. R, Karunakar A. K, and Seshadri S. (2019). Forgery Detection based on KNN Classifier using SURF Feature Extraction. *International Journal of Recent Technology & Engineering.* 8(2), 1600-1607.
- Priyanka, Singh G, and Singh K. (2020). An improved block based copy-move forgery detection technique. *Multimed Tools Appl.,* 79(19-20), 13011-13035.
- Shivakumar, B. L, and Baboo, S. S. (2017). Detection of region duplication forgery in digital images using SURF. *International Journal of Computer Science Issue,* 4(6), 1-7.
- Warif, N, Wahab, A., and Idris, M. (2016). Copy-move forgery detection: Survey, challenges and future directions. *Journal of Network and Computer Applications,* 75, 259-278. DOI: 10.1016/j.jnca.2016.09.008.
- Yang, F., Li, J., Lu, W., and Weng, J. (2017). Copy-move forgery detection based on hybrid features. *Eng*

Yu, L., Han, Q., and Niu, X. (2014). Feature point-based copy-move forgery detection: covering the non-textured areas. *Multimed Tools Appl.* 75(2), 1159-1176. DOI: 10.1007/s11042-014-2362-y

Zhang, Z., Wang, C., and Zhou, X. (2018). A Survey on Passive Image Copy-Move Forgery Detection. *Journal of Information Processing Systems.* 14(1), 6-31. DOI: 10.3745/JIPS.02.0078.

---



**S. Uma** received a B.E (Electronics and Communication Engineering) and an M.E (Applied Electronics) from Bharathiyar University and Sathyabama University respectively. She is working towards her Ph.D at Annamalai University, Chidambaram, Tamilnadu, India. She is a Life membership in I.S.T.E. Her research interests are in the areas of Image Compression, Image Segmentation, Image Enhancement and Fuzzy related to Digital Image Processing.



**Dr.P.D. Sathya** is an Assistant Professor in the Department of Electronics and Communication Engineering at Annamalai University, India. She obtained a B.E. (Electronics and Communication), an M.E. (Applied Electronics) and a Ph.D. degree from Periyar University, Anna University and Annamalai University, respectively. Her research interests include Signal Processing, Image and Video Processing, Antenna Design and Optimization Techniques applied to various Image Processing Applications.

---