NÖHÜ Müh. Bilim. Derg. / NOHU J. Eng. Sci., 2022; 11(3), 513-521

Niğde Ömer Halisdemir Üniversitesi Mühendislik Bilimleri Dergisi
Niğde Ömer Halisdemir University Journal of Engineering Sciences

Araştırma makalesi / Research article

www.dergipark.org.tr/tr/pub/ngumuh / www.dergipark.org.tr/en/pub/ngumuh

SURF ve MSER kombinasyonu ile kopya taşı sahteciliği algılama

Copy move forgery detection with SURF and MSER combination

Yıldız Aydın[1], Funda Akar[2*]

[1, 2] *Erzincan Binali Yıldırım Üniversitesi, Bilgisayar Mühendisliği Bölümü, 24100, Erzincan, Türkiye*

Abstract

Because digital images may contain a variety of data, they are regarded as an important source for information sharing. Also, images are widely used as evidence in a variety of real-life cases. The rapid rise in popularity of digital photographs is due to the improvement of technologies. Several software programs have been developed in recent years to modify digital images, such as Photoshop and Corel Photo, however these programs are now being used extensively for forgery. Because of technological advancements, it is difficult for people to recognize faked images with their naked eyes Therefore, in this study, the features used in forgery detection problems are combined to ensure accurate labeling of even forgery images that are difficult to detect. Stronger feature is obtained by combining Speeded-Up Robust Features (SURF) and Maximally Stable Extremal Regions (MSER). Considering the experimental results; it has been observed that the use of the proposed method, which is obtained as a result of combining the two methods in copy-move forgery detection problems, is more successful than using the SURF and MSER features separately.

Keywords: Copy-move forgery detection, SURF, MSER, Image forensics

Öz

Sayısal görüntüler çeşitli veriler içerebildiğinden bilgi paylaşımı için önemli bir kaynak olarak kabul edilmektedir. Ayrıca, görüntüler gerçek hayatta birçok vakada kanıt olarak yaygın olarak kullanılmaktadır. Dijital fotoğrafların popülaritesindeki hızlı artış, teknolojilerin gelişmesinden kaynaklanmaktadır. Dijital görüntüleri değiştirmek için Photoshop ve Corel Photo gibi son yıllarda çeşitli yazılım programları geliştirilmiştir, bu programlar sahtecilik için de yaygın olarak kullanılmaktadır. Teknolojik gelişmeler nedeniyle, insanların sahte görüntüleri çıplak gözle tanıması zordur. Bu nedenle, bu çalışmada, tespit edilmesi zor olan sahte görüntülerin doğru etiketlenmesini sağlamak için sahtecilik tespit problemlerinde sık kullanılan öznitelikler birleştirilmiştir. Hızlandırılmış Sağlam Öznitelikler (SURF) ve Maksimum Kararlı Ekstremal Bölgeler (MSER) birleştirilerek daha güçlü öznitelik elde edilmiştir. Deneysel sonuçlara bakıldığında; kopyala-taşı sahtecilik tespit problemlerinde iki yöntemin birleştirmesi sonucu elde edilen önerilen yöntemin kullanılmasının SURF ve MSER özniteliklerinin ayrı ayrı kullanılması durumuna göre daha başarılı olduğu gözlemlenmiştir.

Anahtar kelimeler: Kopyala-taşı Sahtecilik tespiti, SURF, MSER, Görüntü sahteciliği

1 Introduction

Technological developments and the increase in digital image editing tools in recent years have resulted in more frequent use of digital images in various fields. As a result of these developments, forgery operations on images have also become easier. This situation increases the number of manipulated images day by day and focuses researchers on the detection of image forgery [1]. Image forgery causes numerous problems in many areas such as military investigations, medical research, and forensic and judicial processes. For this reason, the verification of digital images and the detection of image forgery are of great importance in many areas.

Image forgery is the deliberate falsification of an image to change the information it carries off. The trick may be to add, remove, or change any of the image properties or content without leaving any hint as to the applied change. Falsification of images has become easier and more difficult to detect with so many free image editing tools and software available. So, this causes less confidence in the reality and completeness of the image. Therefore, the need for robust algorithms for automatic forgery detection is increasing day by day and this is one of the important investigative problems in image processing [2]. In addition to forgery detection, some precautions can also be taken, such as picture encryption, which prevents forgery in pictures [3].

2 Related work

There are two kinds of techniques as active technique and passive technique in digital image forgery detection (Figure 1). In active techniques involving digital signature and watermarking, some information is embedded in the image during creation or before publication [4], [5]. However, the scope of this technique is limited due to the deficiency of information about the watermark in most cases. In addition, active techniques have some constraints as they need specially equipped cameras or human intervention [5], [6]. Passive techniques have been proposed to overcome this problem. The blind or passive forgery detection technique uses the image only to determine its reality or completeness, without the watermark or signature of the original image from the sender. This technique accepts that even though

* Sorumlu yazar / Corresponding author, e-posta / e-mail: fakar@erzincan.edu.tr (F. Akar)
Geliş / Recieved: 18.02.2022 Kabul / Accepted: 17.06.2022 Yayımlanma / Published: 18.07.2022
doi: 10.28948/ngmuh.1075784

digital forgeries may leave no visual traces of having been tampered with image, they may probably extremely disrupt the basic statistics feature or image consistency of a natural image. Thus, it presents new artifacts outcoming in different forms of mismatches. These mismatches can be used to detect the forgery. Because of it does not require any prior information about image, passive technique is popular. Using localization of tampered region, current techniques, define diverse traces of tampering and detect them one by one [7-9].

The most widespread types of image forgery are copy-move forgery, also called cloning, and splicing. A part of an image is copied then pasted into another part of the same image in copy-move forgery. The primary purpose of this forgery category is to secrete unwanted objects, copy some parts of the image or increase the visual effect of the image. Copied areas can be of any dimension and form and can be pasted several times in varied locations within the same image [9]. As seen Figure 1, copy-move forgery detection (CMFD) can be done by both methods as block-based and key-based. The purpose of block-based methods is separating the image into overlapping/nonoverlapping blocks then calculating feature vector for each block. After that alike feature vectors are defined and for finding forged regions they are matched. In key-point based methods, image is screened for key-points and feature vector is computed for each key-points. In this method, feature vectors are matched to discover repeated regions and the image is not sub-divided into blocks [10, 11]. Usually, image segments are chosen for this purpose, which easily merge with the background so that they do not leave any questionable artifacts in the manipulated areas. The fact that the source and target images are the same, will cause the features of the fake regions such as texture, color palette, noise, dynamic range to be harmony with the rest of that image, thus making forgery detection difficult [12]

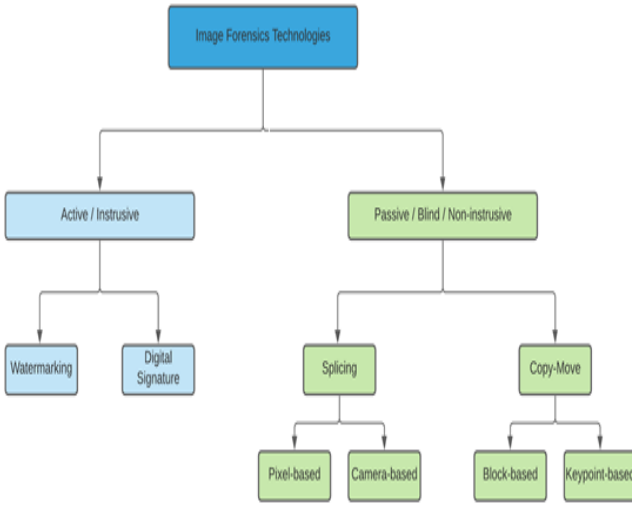


Figure 1. Classification of CMFD methods [13, 14]

First step of CMFD methods is pre-processing (Figure 2). Many methods have been used in the literature for this purpose, as examples:

- Choosing dyadic wavelet transform (DyWT) or Wiener filter for noise elimination,
- Transforming RGB color space into YCrCb color space, grayscale space, HSV space or color local binary pattern (LBP),
- Appling Gaussian pyramid or discrete wavelet transform (DWT) decomposition for size reduction of the image [13].

The key-point approach for feature extraction is most suitable due to their low computation time and well performance. The other benefit of this method is that key-points are very precision to recurrent image content and low-contrast regions [15]. For this reason, the key-point based MSER method was used in this study.

Second step is feature extraction process for CMFD. Fourier-Mellin transform, discrete cosine transform (DCT), polar harmonic transform (PHT), 2D-Fourier transform, LBP, singular value decomposition (SVD), Hu moment, Zernike moment, speeded up robust features (SURF), scale-invariant feature transform (SIFT), maximal stable extremal region (MSER), Harris corner features, FAST, ORB, BRISK and DAISY were used in literature [13].

Third step, feature matching, is the operation of detecting alike feature vectors. Euclidean distance and Manhattan distance are among the methods for finding similarity between feature vectors. The last steps are localization and post-processing. For correcting the detection regions some methods used such as filtering, morphologic operations or random sample consensus (RANSAC) algorithm [16].

In general, there are three classes of feature detectors such as affine invariant, single-scale or multi-scale detectors. Single-scale detectors are invariant for image transformations (translation, rotation, noise addition, illumination changes, etc.). But they fall short of the scaling issue. If there are two images that same scene with a scale modify, it is desired to define whether the same points of interest can be specified. That's why, it is essential to construct multi-scale detectors that can reliably extract distinguished features in case of scale changes. Single and multi-scale detectors partially address the difficult affine invariance problem. Therefore, affine invariant detectors can be used, which is a robust detector against perspective transformations. It can also be said that an affine invariant detector is a generalized model of a scale invariant detector [17].

Examples of single-scale detectors could be Harris, Moravec's, FAST, SUSAN, Hessian detector. As an example of multi-scale detectors; Hessian-Laplace, Harris-Laplace, Difference of Gaussian (DoG), Laplacian of Gaussian (LoG), and Gabor wavelet detector can be given. And finally examples of affine detectors could be Hessian-Affine, Harris-Affine, EBR (edge-based region), IBR (intensity extrema-based region), MSER [18].

In the literature, for each color channel in color images and descriptors for which invariants can be calculated across channels have been shown to be more successful than gray level descriptors [19, 20].

The ORB algorithm utilizes the advanced FAST algorithm to define feature points. If a pixel is significantly dissimilar from the neighborhood pixels this method claims

that it is more probably to be a corner point. First it extracts the Oriented FAST feature points, then applies the improved BRIEF algorithm to compute the descriptors for every point [21].

SIFT and SURF are shape matching based methods, while MSER is based on region analysis. In SURF and SIFT methods, feature vectors are extracted by focusing on prominent regions in the image. The MSER algorithm finds related ellipses in the image. Each MSER consists of ellipses defined as composite points around specified pixels [22]–[25]. SIFT and SURF methods have been extensive used in literature, but the number of studies with MSER is not too much.

In the literature, some studies have been done with the use of SURF and MSER features [26]–[28]. The authors in [26], [27] separate the input images into blocks, then implement CMFD using SURF or MSER features on the blocks that are related to each other. The authors in [28] firstly divide images to nonoverlapping blocks. After the key-points were detected using MSER, they extracted SURF descriptor at these MSER key-point locations and used them in the matching step. The proposed method is different from early studies in that it is not block-based and uses a combination of SURF and MSER features.

3 Material and method

3.1 Proposed method

In pre-processing step, the image is converted to gray level. The SURF and MSER features are extracted from the gray level image separately and then these features are combined to have stronger feature in feature extraction step. The combination of features has been used in various fields in the literature [29], [30] and it has been observed that the rate of true positive rate is higher, and the rate of false positive rate is less than the applications performed with this combined feature compared to the applications performed with the use of these features separately. Therefore, the combination features are used in the proposed method. Thus, it is ensured that images that are fake but not labeled as fake are detected correctly. Flowchart of the proposed method is given in Figure 3.

The suggested CMF identification technique used a key-point based technique, which is thought being more reliable and quicker than block-based CMF recognition approaches. After transforming the original tampering image to gray level, SURF and MSER descriptors are combined in the feature extraction step of the suggested CMF detecting approach.

SURF and MSER were combined for efficient and effective feature use in the matching step, so that the proposed CMFD approach was able to correctly label even the attacked images.

The algorithms used in the proposed method are detailed below.

3.1.1 Extracting MSER (Maximally stable extremal regions) key-points:

MSER is the dependent ingredient of a properly thresholded image. The notion of Maximally Stable Extremal Regions is suggested by Matas et al, in 2004. MSERs indicate a set of prominent regions determined in a grayscale image. Whole regions are described by an extreme property of the density function in the region and its external border. MSERs have features that make up their outstanding performance as a stable local detector. The sequence of MSERs is off in continual geometric transformations and is invariant with affine density changes. In addition, MSERs are defined at distinct scales [24]. MSER has linear complicacy and is fast to determine an affine invariant stable subset of extreme regions.

3.1.2 SURF (Speeded Up Robust Feature) key-points:

The SURF descriptor is both fast and durable to translation and affine transformation also in the presence of noise [31]. Even if after post-processing attacks such as rotation, blur, contrast adjustment, color reduction, SURF features enable detection of fake regions. There are two main steps in SURF, points of interest (POI) detection and POI identification. The detector and descriptor of SURF is both faster, and its detector is more reiterationable, and its descriptor is more distinguishable. SURF converts the original image to the integral image. The total of whole pixels in the input image I inside of the rectangular region created by the origin and x, have shown by the input of an integral image $I_{\Sigma}(x)$ at an $x=(x,y)^T$ [32]:

$$I_{\Sigma(x)} = \sum_{i=0}^{i\leq x} \sum_{j=0}^{j\leq y} I(i,j) \quad (1)$$

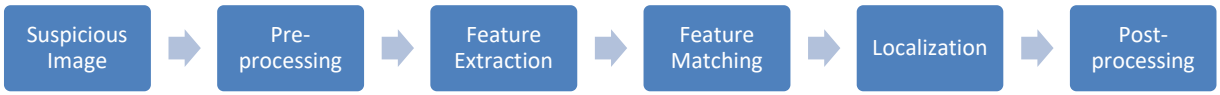


Figure 2. Copy-move forgery detection process

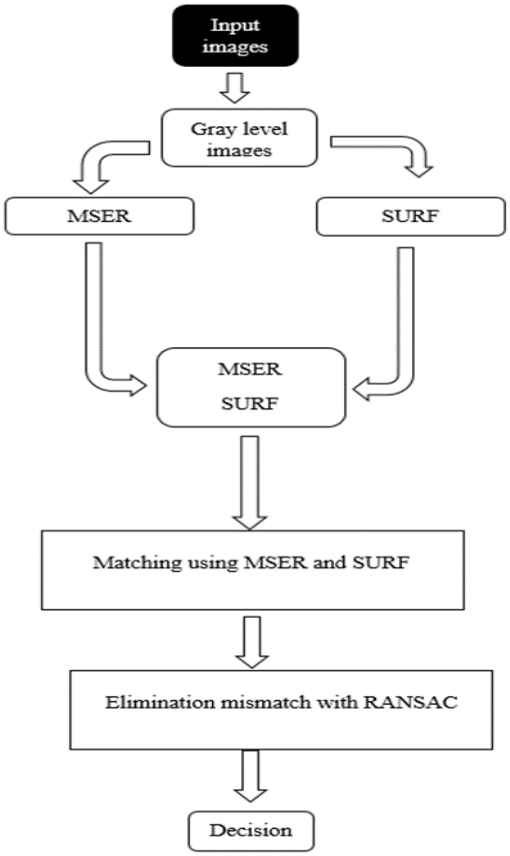


Figure 3. Flowchart of the proposed method

By using the Hessian matrix determinant as a criterion, information about the changes between regions is obtained. H(x,σ) Hessian matrix with σ scale for a point x=(x,y) in the I image given with:

$$H = \begin{bmatrix} L_{xx}(x,\sigma) & L_{xy}(x,\sigma) \\ L_{xy}(x,\sigma) & L_{yy}(x,\sigma) \end{bmatrix} \quad (2)$$

In Equation 2 $L_{xx}(x,\sigma)$ is obtained as a result of the convolution of the I image at x and the second-order derivative of the gaussian filter. $L_{xy}(x,\sigma)$ and $L_{yy}(x,\sigma)$ are obtained similarly [23], [32].

$$L_{xx}(x,\sigma) = I(x) * \frac{d^2}{dx^2} g(\sigma) \quad (3)$$

3.1.3 SURF and MSER (SURF + MSER)

After the image is converted to gray level, firstly, SURF features are extracted from the image. Then, all 64-dimensional feature vectors obtained after extracting the MSER feature from the gray-level image are combined. For example, let the 25x64 size SURF features and 35x64 size MSER features are extracted from the image. In this case, the features are combined in the matching step so 60x64 sized features are used (Figure 4).

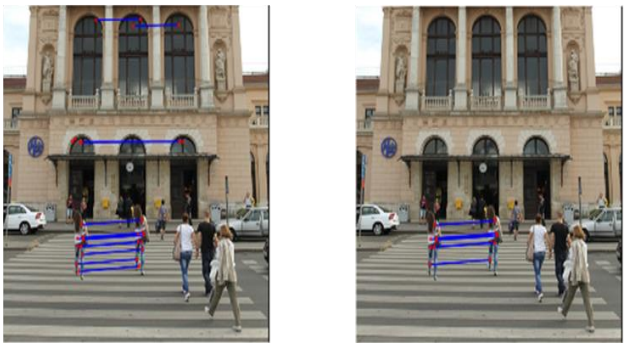
Figure 4. Process steps to obtain the MSER+SURF identifier

3.2 Matching

In the feature matching step, first, the scalar product of each feature descriptor with the other feature descriptors is calculated. The inverse cosine components of the scalar products calculated for all the features are obtained and these values are ordered in ascending order. If the ratio between consecutive neighbors is above the predetermined threshold, this feature pair is labeled as matched.

3.3 Mismatch elimination using RANSAC

It's easy to find erroneous matches, as illustrated in Figure 4. This is why the proposed model was evaluated using Fischler's RANSAC [33] to keep inliers (correct matches) and eliminate outliers. The proposed model has the most correct matches after a specific amount of repetitions. Following the RANSAC algorithm, the false match elimination result can be shown in Figure 5.



(a) (b)

Figure 5. CMFD results a) without RANSAC b) with RANSAC

4 Results and discussion

4.1 Dataset

To evaluate the efficiency of the algorithm, CoMoFoD dataset consisting of 400 images in PNG format (200 tampered images, 200 original images with a resolution of 512x512 pixels) was used in this study. Five categories were formed as a result of geometric transformations (rotation, translation, scaling, deformity and combining two or more transformations) applied to whole images. 40 images are in every class and every class has also six subclasses based on six types of post-processing (noise addition, JPEG compression, brightness changing, image blurring, contrast adjustments and color reducing) that can be applied on an

image. Due to all operations, the CoMoFoD dataset consists of 10400 images in total [34].

4.2 Metrics

The achievement rating of the proposed method was made over three comparison parameters, which are used extensively in the literature: Precision (P) and Recall (R) and F1 scores (Equation 4). TP (true positive) refers that a forged image is detected as fake, TN (true negative) refers that the original image is detected as original, FP (false positive) refers to an image which is not forged but reported as forged, FN (false negative) refers to an image which is not reported as forged even though it is forged. F1 is also a metric that combines Precision and Recall with a single rate [16], [35].

$$P = \frac{TP}{TP + FP}, \quad R = \frac{TP}{TP + FN}, \quad F_1 = 2 * \frac{P * R}{P + R} \qquad (4)$$

4.3 Comparison results

The corresponding authors' applications with best parameter values reported in their respective papers (FMT, PCT-Cart, PCT-Polar, ZM-Cart, ZM-Polar) [36], Alexnet, VGG [37] are used. SURF [38] and MSER [39] methods for CMFD were applied by us, and the results obtained are given in the table. The method proposed in the manuscript was compared with the state-of-the-art methods [37]–[40] . The results of the aforenamed methods and our proposed method on CoMoFod dataset are presented in Table 1.

Table 1. Results of methods on CoMoFod

Dataset	Technique Name	R	P	F1
CoMoFoD	FMT (result taken from [36])	0.522	0.8290	0.6406
	PCT-Cart (result taken from [36])	0.494	0.8480	0.6243
	PCT-Polar (result taken from [36])	0.491	**0.8770**	0.6295
	ZM-Cart (result taken from [36])	0.509	0.8480	0.6361
	ZM-Polar (result taken from [36])	0.489	0.8700	0.6260
	Alexnet (result taken from [37])	**0.835**	0.5105	0.6334
	VGG (result taken from [37])	0.7204	0.4965	0.5875
	SURF	0.725	0.6416	0,6808
	MSER	0.710	0.6256	0.6651
	Proposed Method (MSER+SURF)	0.795	0.6437	**0.7113**

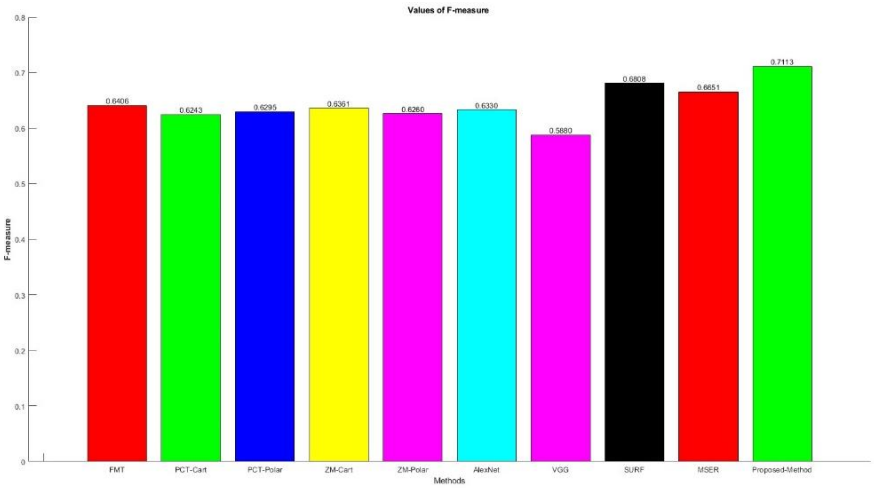


Figure 6. F1 Scores of methods

(a) original image (b) forged image (c) result of proposed method

Figure 7. Image which is applied brightness change attack

Experimental results showed that the proposed method was more successful than both the use of SURF and MSER features separately and other methods. In applications performed with the use of SURF and MSER features separately, F1 score 0.6808 and 0.6651 were obtained, respectively, while F1 score became 0.7113 with the use of these features together. Also, it can be seen from the Table 1, P and R values in some methods were higher than the proposed method. However, in these methods where higher values are obtained, the disproportion between P and R values is striking. As a result, considering the F1 score, which is obtained from P and R values and which is frequently used in the literature, the most successful method has been the recommended method.

To calculate efficiently a high-quality approximate nearest neighbor field for the whole image, Cozzolino et al. used the PatchMatch algorithm (FMT, PCT-Cart, PCT-Polar, ZM-Cart, ZM-Polar) [40]. F1-scores from all methods in table 1 are evaluated using bar graph in Figure 6.

4.4 Experiments on post-processing

On the tampered images described in Dataset section, we test the resilience of our proposed CMFD technique against three forms of post-processing attacks: brightness change, contrast adjustments, color reduction, image blurring, noise adding, JPEG compression. Figure 7, 8, 9, 10, 11 and 12 shows the suggested CMFD results of images with attacks, respectively.

As can be seen from the figures, the proposed method has detected copy-move forgery even in cases where different attacks were applied.

5 Conclusions

On the basis of MSER and SURF, this article offers a unique CMFD technique that combines MSER and SURF. A typical block-based scheme splits images into overlapping blocks, but our suggested technique preserves the superiority of a key-point based scheme, which is effective for native images. In addition, our approach is robust against JPEG compression, noise addition, image blurring, brightness changing, color reduction and contrast adjustments attacks. Although the proposed method is strong according to the compared methods and also considering the attacks, it can be improved and made more robust. In this study, it has been shown that more success can be achieved by applying hybrid methods instead of applying the methods one by one. It would be beneficial for people who will work in this field to take this issue into consideration.

It is important to use strong features in CMFD applications where correct detection as well as false detection is of great importance. In this context, studies can be conducted on different combination methods such as triple hybrid combination with different features in the future.

(a) original image (b) forged image (c) results of proposed method

Figure 8. Image which is applied contrast adjustment attack

(a) original image (b) forged image (c) results of proposed method

Figure 9. Image which is applied color reduction change attack

(a) original image (b) forged image (c) results of proposed method

Figure 10. Image which is applied image blurring attack

(a) original image (b) forged image (c) results of proposed method

Figure 11. Image which is applied noise adding attack

(a) original image (b) forged image (c) results of proposed method

Figure 12. Image which is applied JPEG compression attack

Acknowledgement

The authors would like to thank the editor and anonymous reviewers for their comments that help improve the quality of this work.

Competing interests

The authors declare that they have no competing interests.

Similarity rate (iThenticate): 15%.

References

[1] M. Hassaballah, A. A. Abdelmgeid, and H. A. Alshazly, Image Features Detection, Description and Matching, Image Feature Detectors and Descriptors : Foundations and Applications, A. I. Awad and M. Hassaballah, Eds. Cham: Springer International Publishing, 11–45, 2016.

[2] G. Ulutas and G. Muzaffer, A New Copy Move Forgery Detection Method Resistant to Object Removal with Uniform Background Forgery, Mathematical Problems in Engineering, 2016, https://doi.org/10.1155/2016/3215162.

[3] D. Ozdemir and D. Celik, Analysis of Encrypted Image Data with Deep Learning Models, 14th International Conference on Information Security and Cryptology, ISCTURKEY Proceedings, 121–126, 2021. https://doi.org/10.1109/ISCTURKEY53027.2021.9626.

[4] M. A. Qureshi and M. Deriche, A bibliography of pixel-

based blind image forgery detection techniques, Signal Processing: Image Communication, (39), 46–74, 2015, https://doi.org/10.1016/j.image.2015.08.008.

[5] M. Kashif, T. M. Deserno, D. Haak, and S. Jonas, Feature description with SIFT, SURF, BRIEF, BRISK, or FREAK A general question answered for bone age assessment, Computers in Biology and Medicine, (68), November, 67–75, 2016, https://doi.org/10.1016/j.compbiomed.2015.11.006.

[6] K. Asghar, Z. Habib, and M. Hussain, Copy-move and splicing image forgery detection and localization techniques: a review, Australian Journal of Forensic Sciences, 49, (3), 281–307, 2017, https://doi.org/10.108/00450618.2016.1153711.

[7] T. Mahmood, T. Nawaz, A. Irtaza, R. Ashraf, M. Shah, and M. T. Mahmood, Copy-Move Forgery Detection Technique for Forensic Analysis in Digital Images, Mathematical Problems in Engineering, 2016, https://doi.org/10.1155/2016/8713202.

[8] O. I. Al-Sanjary and G. Sulong, Detection of video forgery: A review of literature, Journal of Theoretical and Applied Information Technology, 74, (2), 207–220, 2015.

[9] N. P. Joglekar and P. N. Chatur, A Compressive Survey on Active and Passive Methods for Image Forgery Detection, International Journal Of Engineering And Computer Science, 4, (1), 10187–10190, 2015.

[10] R. Oommen, M. Jayamohan, and S. Sruthy, A Survey of Copy-Move Forgery Detection Techniques for Digital Images, International Journal of innovations in engineering and technology, 5, (2), 419–426, 2015.

[11] J. A. Redi, W. Taktak, and J. L. Dugelay, Digital image forensics: A booklet for beginners, Multimedia Tools and Applications, 51, (1), 133–162, 2011, https://doi.org/10.1007/s11042-010-0620-1.

[12] B. L. Shivakumar and S. S. Baboo, Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Methods, Global Journal of Computer Science and Technology, 10, (7), 61–65, 2011.

[13] Z. Zhang, C. Wang, and X. Zhou, A survey on passive image copy-move forgery detection, Journal of Information Processing Systems, 14, (1), 6–31, 2018, https://doi.org/10.3745/JIPS.02.0078.

[14] P. C. Sekhar and T. Shankar, Review on Image Splicing Forgery Detection, International Journal of Computer Science and Information Security, 14, (11), 471–475, 2016.

[15] R. Raj and N. Joseph, Keypoint Extraction Using SURF Algorithm for CMFD, Procedia Computer Science, (93), 375–381, 2016, https://doi. org/10.1016/j.procs.2016.07.223.

[16] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, An evaluation of popular copy-move forgery detection approaches, IEEE Transactions on Information Forensics and Security, 7, (6), 1841–1854, 2012, https://doi.org/10.1109/TIFS.2012.2218597.

[17] M. Hassaballah and A. I. Awad, Detection and Description of Image Features: An Introduction, Image Feature Detectors and Descriptors : Foundations and Applications, A. I. Awad and M. Hassaballah, Eds. Cham: Springer International Publishing, 1–8, 2016.

[18] K. Mikolajczyk et al., A comparison of affine region detectors, International Journal of Computer Vision, 65, (1–2), 43–72, 2005, https://doi.org/10.1007/s11263-005-3848-x.

[19] G. J. Burghouts and J.-M. Geusebroek, Performance evaluation of local colour invariants, Computer Vision and Image Understanding, 113, (1), 48–62, 2009, https://doi.org/10.1016/j.cviu.2008.07.003.

[20] I. Abu Doush and S. AL-Btoush, Currency recognition using a smartphone: Comparison between color SIFT and gray scale SIFT algorithms, Journal of King Saud University - Computer and Information Sciences, 29, (4), 484–492, 2017, https://doi.org/10.1016/j.jksuci.2016.06.003.

[21] E. Rublee, V. Rabaud, K. Konolige, and G. Bradski, ORB: An efficient alternative to SIFT or SURF, Proceedings of the IEEE International Conference on Computer Vision, pp. 2564–2571, 2011, https://doi.org/10.1109/ICCV.2011.6126544.

[22] D. G. Lowe, Object recognition from local scale-invariant features, Proceedings of the IEEE International Conference on Computer Vision, 2, pp. 1150–1157, 1999, https://doi.org/10.1109/ICCV.1999.790410.

[23] H. Bay, T. Tuytelaars, and L. Van Gool, LNCS 3951-SURF: Speeded Up Robust Features, Computer Vision–ECCV, pp. 404–417, 2006, [Online]. Avai lable: https://link.springer.com/chapter/10.1007/11744023_32.

[24] J. Matas, O. Chum, M. Urban, and T. Pajdla, Robust wide-baseline stereo from maximally stable extremal regions, Image and Vision Computing, 22, (10) SPEC. ISS., 761–767, 2004, https://doi.org/10.1016/j.imavis.2004.02.006 .

[25] F. Akar and Y. Aydın, Comparison of Interest Point-Based Features in Object Recognition Applications, 8th International Advanced Technologies Symposium (IATS'17), Elazığ, Türkiye, 19-22, pp. 3553-3556, 2017.

[26] K. Ramirez-Gutierrez, Mariko-Nakano, G. Sanchez-Perez, and H. Perez-Meana, Copy-move forgery detection algorithm using frequency transforms, surf and mser, 2019 7th International Workshop on Biometrics and Forensics, IWBF, pp. 4–9, 2019, doi:10.1109/IWBF.2019.8739168.

[27] K. Ramirez-Gutierrez, M. Nakano-Miyatake, G. Sanchez-Perez, Blind Tamper Detection to Copy Move Image Forgery using SURF and MSER, MMEDIA, 9, 2015.

[28] B. Soni and P. K. Das, Geometric Transformation Invariant Improved Block-Based Copy-Move Forgery Detection, in Image Copy-Move Forgery Detection : New Tools and Techniques, Singapore: Springer Singapore, 51–67, 2022.

[29] M. Bansal, M. Kumar, and M. Kumar, 2D object recognition: a comparative analysis of SIFT, SURF and

ORB feature descriptors, Multimedia Tools and Applications, 80, (12), 18839–18857, 2021, https://doi.org/10.1007/s11042-021-10646-0.

[30] C. Lin, W. Lu, et al., Copy-move forgery detection using combined features and transitive matching, Multimedia Tools and Applications, 78, (21), 30081–30096, 2019, https://doi.org/10.1007/s11042-018-6922-4.

[31] K. Mikolajczyk and C. Schmid, A performance evaluation of local descriptors, IEEE Transactions on Pattern Analysis and Machine Intelligence, 27, (10), 1615–1630, 2005, https://doi.org/10.1109/TPAMI.2005.188.

[32] H. Bay, A. Ess, T. Tuytelaars, and L. Van Gool, Speeded-Up Robust Features (SURF), Computer Vision and Image Understanding, 110, (3), 346–359, 2008, https://doi.org/10.1016/j.cviu.2007.09.014.

[33] M. A. Fischler and R. C. Bolles, Random sample consensus: A Paradigm for Model Fitting with Applications to Image Analysis and Automated Cartography, Communications of the ACM, 24, (6), 381–395, 1981, https://doi.org/10.1145/358669.358692.

[34] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, CoMoFoD - New database for copy-move forgery detection, Proceedings Elmar - International Symposium Electronics in Marine, pp. 49–54, 2013.

[35] V. T. Manu and B. M. Mehtre, Copy-move tampering detection using affine transformation property preservation on clustered keypoints, Signal, Image and Video Processing, 12, (3), 549–556, 2018, https://doi.org/10.1007/s11760-017-1191-7.

[36] M. Bilal, H. A. Habib, Z. Mehmood, T. Saba, and M. Rashid, Single and Multiple Copy–Move Forgery Detection and Localization in Digital Images Based on the Sparsely Encoded Distinctive Features and DBSCAN Clustering, Arabian Journal for Science and Engineering, 45, (4), 2975–2992, 2020, https://doi.org/10.1007/s13369-019-04238-2.

[37] A. Kumar, A. Bhavsar, and R. Verma, Syn2Real: Forgery Classification via Unsupervised Domain Adaptation, Proceedings-2020 IEEE Winter Conference on Applications of Computer Vision Workshops, WACVW, 63–70, 2020, https://doi .org/10.1109/WACVW50321.2020.9096921

[38] B. Xu, J. Wang, G. Liu, and Y. Dai, Image copy-move forgery detection based on SURF, Proceedings - 2010 2nd International Conference on Multimedia Information Networking and Security, MINES 2010, pp. 889–892, 2010, https://doi.org/10.1109/MINES.2010. 189.

[39] Kanica Sachdev, A Novel Technique for Detection of Copy Move Forgery Using MSER Features, International Journal of Emerging Technologies in Engineering Research (IJETER), 5, (9), 14–19, 2017, [Online]. Available: https://ijeter.everscie nce.org/Manuscripts/Volume-5/Issue-9/Vol-5-issue-9-M-03.pdf.

[40] D. Cozzolino, G. Poggi, and L. Verdoliva, Efficient Dense-Field Copy-Move Forgery Detection, IEEE Transactions on Information Forensics and Security, 10, (11), 2284–2297, 2015, https://doi.org/10.1109/TIFS.2015.2 455334.