Computer
& Robotics

Copy-Move Forgery Detection by an Optimal Keypoint on SIFT (OKSIFT) Method

Ehsan Amiri [a], Ahmad Mosallanejad [b,*] Amir Sheikhahmadi [a]

[a] *Department of Computer Engineering, Sanandaj Branch, Islamic Azad University, Sanandaj, Iran*
[b] *Department of Computer Engineering, Sepidan Branch, Islamic Azad University, Sepidan, Iran*

Received 15 December 2021, Accepted 23 December 2021

Abstract

Copy-Move is a technique widely used in digital image tampering, meaning Copy Move Forgery Detection (CMFD) is still significant research. This paper proposes an optimal keypoint in SIFT (OKSIFT). The OKSIFT method produces images of different sizes and different sigma's. Then with the help of the Gaussian difference (DoG) method, the maximum and minimum keypoints are calculated. When selecting the optimal keypoints, the absolute value of the second sentence will be used instead of using the Taylor expansion binomial series. First, the keypoints lose their dependence on the blurred regions, and secondly, more keypoints appear at the main edges. In the localization process of the region, considering the cases of multiple copies, method g2NN has been used to compare the keypoints. This method reduces the complexity of keypoint calculations and gives a better answer. Experimental results based on precision, recall, and F1 criteria show that the proposed method, with good robustness, works better than some advanced methods.

Keywords: *Copy-Move Forgery Detection, SIFT, new optimal keypoint in SIFT, Gaussian Filter*

1. Introduction

With the advancement of recent technology in image processing, people can easily modify and manipulate images using image editing software, such as Photoshop. In the last few years, more fake images have appeared in the public media and everyday life. The side effects of these fake images have caused a great deal of concern.

There are several types of image forgery, such as copy-move / copy-transfer / cloning [1]. The copy-move type forgery is a challenging model because it is done by copying part of the image and pasting it into another part (Fig. 1) [2]. This type of forgery can destroy some information or increase the number of objects [3].

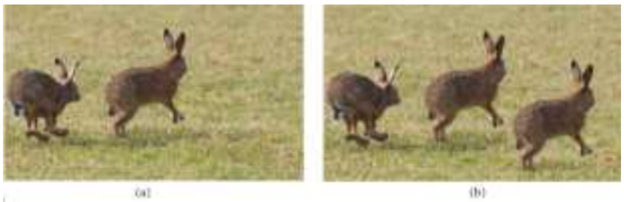

Fig. 1.Example of copy-move forgery [2]

To achieve a realistic fake image, the process of forging a copy by move performs various operations before pasting different areas, including geometric operations and post-processing operations. Geometric operations include rotation and scaling. Post-processing operations include JPEG compression, Gaussian noise, color reduction, contract adjustment, brightness change, and image blur [4].

Many copy-move forgery detection (CMFD) solutions have been proposed to detect counterfeit areas of copy motion in an image, which can be classified into two approaches: keyword-based [1, 5], block-based [6],

[*] Corresponding Author Email:ahmad.upm@gmail.com

and based on deep learning [7]. Keypoint-based and block-based algorithms have similar workflows, such as sequential computational steps, including image feature extraction, feature matching, false-match filtering, and additional processing to detect attacks [5]. Block-based algorithms divide images into overlapping blocks to extract block properties using fixed-moment techniques [6]. Keypoint-based algorithms search for high entropy regions and extract extreme pixels for the whole image [5].

All previous detection algorithms [8] have bugs:

1. These algorithms are inefficient in detecting forgery images with copy-move.
2. These algorithms do not perform well for detecting copy movement areas with various geometric attack operations and after processing.
3. The detection results of these algorithms have many false positive pixels.

This paper proposes a new CMFD algorithm to overcome these drawbacks [9, 10].

Various studies have been performed on detecting this type of image forgery, which is mainly based on scale-invariant feature transform (SIFT) [9] and Speeded Up Robust Features (SURF) [10] methods.

• The most important disadvantage of the SIFT method is its high computational cost, especially in tissue extraction and adaptation. This method has low efficiency. On the other hand, this method has a low ability to detect multiple copies in the image.

• The SURF attribute is efficient but cannot find symmetric pairs of attribute points.

• Both of these methods are very slow and weak in detecting motion-copy forgery in compressed images.

• Other methods used in copy-move forgery have weaker structures than the SURF and SIFT methods.

The proposed algorithm is two-step to detect false positive keypoints using keypoint density based on networks and group pairs and significantly reduce the number of false-positive pixels. In the first step, the SIFT algorithm has been rewritten to increase the number of appropriate keypoints and reduce the number of inappropriate points in the blurred image points. In the second step, an image matching algorithm based on the g2NN method is introduced to examine the calculated keypoints without further calculation and reduce the complexity of the calculations. The proposed algorithm for CMFD works better than other algorithms. In addition, its detection speed is faster than block-based algorithms and other keypoint-based algorithms.

The rest of the article is introduced in Section 2 of previous studies. Section 3 presents a copy motion detection algorithm based on the SIFT algorithm. Section 4 presents the experiments and their results. Section 5 is a general conclusion of the work and offers suggestions for further study.

2. Related Work

Detection of features in real or cloud [11] environments is done in different ways, such as deep neural networks [12], wavelet transform [13]. In copy-move image forgery detection, feature detection methods can be classified into two main categories: block-based and keypoint-based methods. In keypoint-based, SIFT detects the scale-invariant features from a digital image [14]. The detected features [15] are invariant to image scaling [16], rotation, and translation.

Four important steps of the SIFT are scale-space extrema detection, keypoint localization [17], orientation assignment, and keypoint descriptor. We can acquire many SIFT keypoints through these four major steps, each containing orientation and position. These features are partially invariant to illumination changes and are robust to local geometric distortion. Therefore, the proposed scheme adopts SIFT to acquire significant features of image regions.

There are two main problems with using the SIFT method. The first problem is the inability of the SIFT method to withstand the light challenge, and the second problem is the matching of keypoints. Amerini et al. [18] utilized the spatial coordinates of the keypoints to implement agglomerative hierarchical clustering. Because only the coordinates of the matched pairs are taken into account, and the matching constraint between points is ignored. This method fails when the duplicated region is spatially close to the original region. The authors eventually proposed an improved method to overcome this shortcoming using the J-Linkage algorithm [19]. Because the time complexity of the J-Linkage algorithm is quadratic on the number of matched pairs, the clustering time increases significantly as the number of matched pairs increases [20].

In a study [21] in 2018, forgery detection was performed using binary resolution features, and in [4], image change detection was performed using the JPEG compression model. These methods are a combination of common block and keyword-based methods. The key forged locations are first identified, and then, using the area extraction technique, the wrought iron area is localized. Also, image change has a specific pattern called copy-move forging.

The main problem with JPEG compression is that the pixels have different values after being transferred to a different location and stored in JPEG format. Most existing algorithms [22], such as evolutionary algorithms [23], are based on matching pairs of similar patches [24], which causes many errors. A JPEG-based constraint is used to overcome this problem that considers each pair of bits of a valid candidate and proposes an efficient algorithm to examine this constraint.

Copy-move forgery detection [25] was performed using local two-way coherence error modification. In the first step, a coherence-sensitive method is used to obtain the feature in an image. Then, a local bilateral coherence error. When a local two-way coherence error change occurs, the iterative detection process stops [26]. Finally, with the help of the calculated features, the areas of motion forgery are easily identified using a local error.

In a study [27] in 2019, forgery detection was based on density-based clustering. In this type of forgery, an image area is copied and pasted elsewhere in the same image. In this paper, an improved approach to detect copy-based motion forgery is presented. The proposed method is based on density-based clustering.

Local fixed symmetry properties to detect image forgery was proposed in [28]. This paper presents a new scheme for detecting forgery in copy-move using local symmetry-based features. DCT is another video method [29] and image detection. Forgery detection in [26] trains a neural network to detect objects [30] based on DCT coefficients in the compressed image.

Recently, there has been an extensive rise in digital image forensics [23]. Initially, Fridrich et al. [31] proposed four different methods, viz., exact match, autocorrelation, exhaustive search, and full match (based on Discrete Cosine Transform (DCT)) to find the copy-move forged regions in digital images. The robust match method has been proven to be better than the others because it allows finding the duplicate regions more accurately. The drawback of this method is that applying it on large identical texture images may give many false matches. Popescu and Farid [32] developed a forgery detection method based on Principal Component Analysis (PCA). This method does not perform well for loss compression because of the dimensionality reduction feature of PCA. Kang and Wei [33] developed a copy-move forgery detection method utilizing Singular Value Decomposition (SVD) features of the digital images.

This method can detect forgery even image having slight noise with low computational complexity. Zhang et al. [34] applied Discrete Wavelet Transform (DWT) on a forged image by decomposing it into four frequency sub-bands and dividing the approximate sub-band into overlapping blocks. Copy-move regions were detected using correlation values among overlapped blocks. This technique's computational complexity is low compared to the other existing algorithms.

3. Copy Move Forgery Detection With New Sift (CMFNS)

Various ways are presented to explore the problem of CMFD. Most of the introduced algorithms in the feature extraction for revealing and illustrating local visual features often demand two procedures: the first procedure detects the centralized interest points. In contrast, robust local descriptors are constructed to be invariant orientation and scaling [21, 25].

The proposed algorithm consists of two steps. The first step is to discover the keypoints of the image-based Optimal Keypoint SIFT (OKSIFT) algorithm and the second step is a method to check the similarity of the keypoints obtained from the first step. These steps are described in detail below.

3.1. An Optimal Keypoint SIFT (OKSIFT)

In 1999, Lowe first proposed the Scale Invariant Feature Transform local feature [26], robust and highly efficient in rotation, scale change, affine transform, and viewpoint change. The SIFT algorithm has good performance in the gray image feature detection.

The proposed algorithm in discovering the optimal keypoints consists of 3 steps. As shown in Fig. 2, these three steps are Create octaves, Extract keypoints of the image, and Select the optimal keypoints with a new method introduced below.

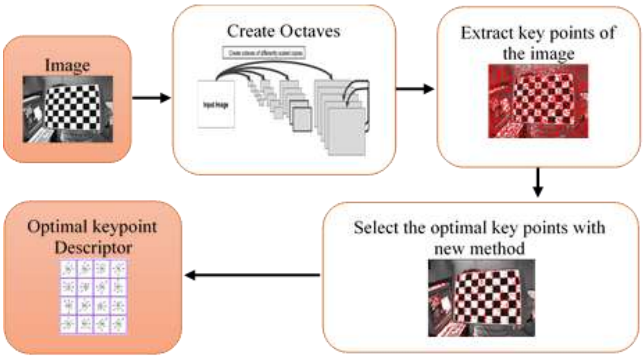
Image
Create Octaves
Input Image
Extract key points of the image
Select the optimal key points with new method
Optimal keypoint Descriptor

Fig. 2. Proposed model based on SIFT algorithm

SIFT algorithm converts image data into local feature vectors named SIFT descriptors. Those features have the power to geometric transformations that are constant to scaling and rotation. This algorithm is divided into four main stages (Fig. 2).

3.1.1. Create Octaves

In the first step, the image is converted into images of different scales. Then with the help of a Gaussian filter [35], the images are completed by applying different sigma's. Here, four images with sizes I, I / 2, I / 4, and I / 8 are obtained. Applying the Gaussian filter with four different sigma's will transform the main image into 16 different scales and transparency. The scale-space image is called L (x, y, σ), created by the convolution process between function and image. In this situation, convolution between Gaussian function, G (x, y, σ), and an image I (x, y) is used [14]:

$$L(x.y.\sigma) = G(x.y.\sigma)*I(x.y) \tag{1}$$

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

3.1.2. Extract Keypoint of the Image

Optimizing a computable approximation of Gaussian Laplacian is used to elicit the keypoints of the image named Difference of Gaussians (DoG) [9], where, a DoG Image D is introduced as follows:

$$D(x.y.\sigma) = L(x.y.k\sigma) - L(x.y.\sigma) \tag{3}$$

Where L (x, y, k σ) is the convolution of the original image, I (x, y) with the Gaussian Blur G (x, y, k σ) at scale k σ.

3.1.3. Select the Optimal Keypoint With New Method

To select the main point from image extrema where the main points are unsettled over image variation, rejecting the points over image edges and those characterized by low contrast. The Taylor expansion of scale-space function D (x, y, σ) shifted such that the sample point is the origin.

Taylor expansion determines the appropriate points in the initial SIFT model [14]. According to the studies that have been done, most researchers have used the first two sentences of Taylor expansion in determining the appropriate points. In contrast, the negative values obtained from Taylor expansion contain points located in the blurred part of the image, and by removing Those values can be achieved at fewer points in the blurred areas of the image. If a threshold is used to remove Taylor's negative values, this hypothesis will fail. In this case, can achieve the desired result by deleting the first sentence of Taylor expansion and the absolute value of the second sentence. This formula is introduced as follows:

$$D(x) = D_0 + \left|\frac{1}{2} x^T \frac{\partial^2 D_0}{\partial x^2} x\right| \tag{4}$$

The removal of keypoints using the two Taylor general expansion methods and the proposed method is shown in Fig. 3.

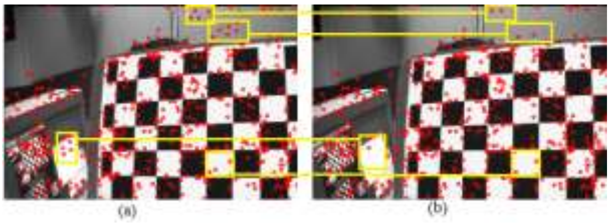

Fig. 3. The removal of keypoints. a) With Taylor general expansion method. b) With new Taylor expansion method

As shown in Fig. 3, it is clear that Taylor's expansion method has not worked well in areas where the image's brightness has caused blurred areas. In addition to removing inappropriate keypoints of the edge, the proposed method has increased the number of important keypoints and reduced the number of keypoints on blurred surfaces.

3.1.4. Keypoint Descriptor Generation

Keypoint Descriptor Generation to ensure that The SIFT descriptors are constant in scaling and rotation, a canonical orientation is specified to each main point. A gradient orientation histogram is computed in the neighborhood of the keypoint to specify the descriptor orientation. Particularly, for an image sample L (x, y, σ) at scale s (the scale in which detect that keypoint), the gradient magnitude m (x, y) and orientation q (x, y) are computed using Eq. (5) and (6) [36]:

$$m(x.y) = \sqrt{\left(L(x+1.y) - L(x-1.y)\right)^2 + \left(L(x.y+1) - L(x.y-1)\right)^2} \quad (5)$$

$$\theta(x.y) = tan^{-1}\left(\frac{L(x.y+1) - L(x.y-1)}{L(x+1.y) - L(x-1.y)}\right) \quad (6)$$

A feature vector with 128 elements is created for each descriptor. This vector is composed of the values of orientation histogram in an image plane and scale-space form with a 4×4 array of histograms and eight orientation bins in each. The results obtained are 4×4×8 = 128 element feature vector.

3.2. Matching of Keypoints

After obtaining the OKSIFT descriptors, we can roughly determine whether there are duplicated regions in the test image via feature matching. In copy-move forgery, a tampered image generally contains two or more duplicated regions, and so the keypoints in these regions have similar descriptor vectors. We adopt the g2NN matching process proposed in [18] in the feature matching stage, which effectively solves the detection problem of multiple cloned regions.

For the sake of clarity, a matched pair, s, is referred to as a source keypoint, and s' is called a corresponding keypoint.

4. Experimental Results

4.1. Database

Here, will examine a series of data to copy-move forgery detection.

The first database contains the IMD (Image Manipulation Dataset) public image data set (Fig. 4) [37] that has been used to evaluate the proposed method. The IMD dataset, sometimes known as CoMoFoD, includes 48 different simple images, rotating images, JPEG compression images, and noise images. The largest image in this dataset is about 3000 × 2300 pixels. In this dataset, about 10% of the areas of each image are manipulated.

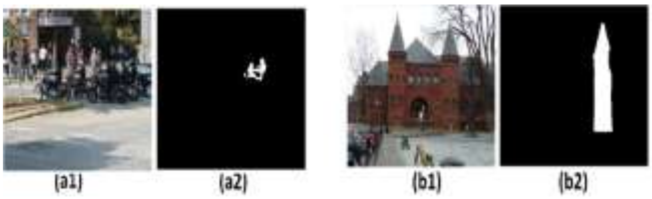

Fig. 4. Example results of the OKSIFT forgery detection algorithm on the IMD dataset. (a1) and (b1) Original image [31]. (a2) and (b2) Detected forged region.

The second database is MICC-F600 [18], containing 1440 images (Fig. 5). This data set has been used to construct test images with more types of area manipulation. The size of the images in this dataset varies from 800 × 533 to 3888 × 2592 pixels. This set includes (1) single copies: forged areas are reproduced once. (2) Multiple copies: Forgery areas have been duplicated two or three times.

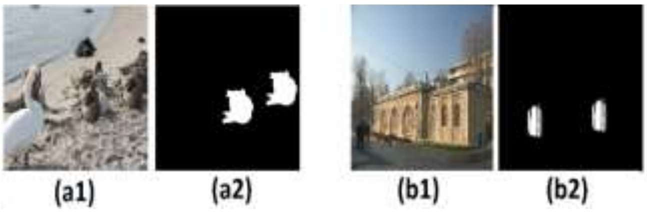

Fig. 5. Example results of the OKSIFT forgery detection algorithm on the MICC-F600 dataset(a1) and (b1) Original image. (a2) and (b2) Detected forged region.

The GRIP database [42] contains 2×80=160 ground truth images and tampered images which tampered regions have arbitrary shape, ranging in size from 4000 pixels (less than 1% of the image) to 50000 pixels.

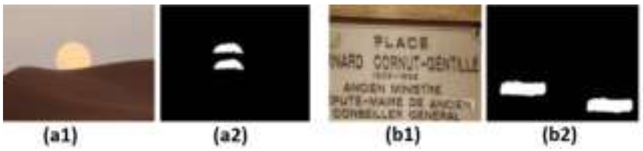

Fig. 6. Example results of the OKSIFT forgery detection algorithm on the GRIP dataset(a1) and (b1) Original image. (a2) and (b2) Detected forged region

4.2. Performance Measures

For certain, CMFD aims to promote detection precision and recall its best to find all the pixels belonging to the tampered region. Generally, three commonly used indexes, $precision$ (Eq. 7), $recall$ (Eq. 8), and $F1$ (Eq. 9), represent the effect of different aspects, which are also applied to our method evaluation. They are calculated as [28]:

$$Precision = \frac{A \cap B}{|A|} \quad (7)$$

$$Recall = \frac{|A \cap B|}{|B|} \quad (8)$$

$$F1 = 2 \times \frac{Precision\,.\,Recall}{Precision + Recall} \quad (9)$$

To calculate these parameters, two factors, A and B, are defined, A as the detected images by the method and B as the forged images of the data set. At the image level, precision is computed as the ratio of the number of correctly detected forged images to the number of totally detected forged images, as shown in Eq. (7) and, recall is computed as the ratio of the number of correctly detected forged images to the total number of forged images in the dataset, as shown in Eq. (8). F1 combines both precision and recall as a weighted average measure. The score is called the F1-Score because it gives equal weights to both precision and recall, as shown in Eq. (9).

4.3. Comparison Results and Analysis

The results of quantitative analysis on the images are taken according to the proposed model, which includes the detection of forgery with the help of OKSIFT. The Keypoint method automatically detects fake images, but the results are incomplete and accurate. Precision in detecting Copy-Move forgery is the possibility of identifying real forgery points, and recall is the possibility of detecting forged images.

4.3.1. Results on IMD

This section compares the identified results with some of the advanced CMFD methods. These methods include: SIFT [18], KAZE (KAZE is a Japanese word that means wind) [38], LIOP (Local Intensity Order Pattern) [24], PCET (Polar Complex Exponential Transform) [39], and MSA (multi-scale analysis) [40]. In this case, the results are shown in the simple copy subset in Table 1.

Table 1
Results of IMD dataset

Methods	Precision (%)	Recall (%)	F1 (%)
SIFT [18]	80.77	43.75	56.75
KAZE [38]	71.43	83.33	76.93
LIOP [24]	73.44	75.41	74.42
PCET [39]	73.65	62.77	67.69
MSA [40]	75.48	73.28	74.36
OKSIFT	**83.22**	**84.16**	**82.76**

Table 1 shows that the OKSIFT method has the highest precision (83.22%), 80.77% in SIFT, and 75.48% in MSA. However, the goal of the CMFD method is to detect as much as possible of all manipulated images. It is more important to detect fake images for a set of images containing real and image forgery.

4.3.2. Results on MICC-F600

This section compares the identified results with some advanced CMFD methods on the MICC-F600 dataset. The methods of introduction in this section, as in the previous section, are: SIFT [18], KAZE [38], PCET [39], MSA [40], and DAFMT (Discrete Analytical Fourier-Mellin Transform) [41]. In this case, the results are shown in the simple copy subset in Table 2.

Table 2
Results of MICC-F600 dataset

Methods	Precision (%)	Recall (%)	F1 (%)
SIFT [18]	77.55	42.21	54.67
KAZE [38]	68.40	51.40	58.70
PCET [39]	71.14	66.34	67.69
MSA [40]	64.58	72.45	68.00
DAFMT [41]	73.86	73.28	74.00
OKSIFT	**83.65**	**83.99**	**83.71**

This table shows that the proposed method is more accurate than the other methods presented in Table 2. According to the recall column, it is clear that the number of image forgery detected by this method is much higher than other methods. The precision of other methods is high because they detect images forgery correctly, but the proposed method detects more image forgery in addition to increasing the precision.

4.3.3. Results on GRIP

This section compares the identified results with some advanced CMFD methods on the GRIP dataset. The methods of introduction in this section, as in the previous section, are: SIFT [18], and Clustering SIFT [42]. In this case, the results are shown in the simple copy subset in Table 3.

Table 3
Results of GRIP dataset

Methods	Precision (%)	Recall (%)	F1 (%)
SIFT [18]	90.32	89.18	89.56
Clustering SIFT [42]	99.79	99.67	99.72
OKSIFT	**98.18**	**99.81**	**98.76**

This table shows that the proposed method is more accurate than the other methods presented. According to the recall column, it is clear that the number of image forgery detected by this method is much higher than other methods. Despite the increased accuracy of the method [42] compared to the proposed method, increasing the number of SIFT layers puts a lot of time load on the system so that a small difference can be overcome.

5. Conclusion and future work

Copy-move is the most common method of image manipulation in which image areas are copied internally. The proposed method focuses on detecting copy-move forgery using the OKSIFT model. Experimental analysis proved the effectiveness of the proposed method in detecting forgery and transmission of forgery. This method offers a higher detection rate and precision. Results show a significant improvement in the precision and value of the F1 Score compared to other algorithms. It has also shown relatively good results for call rates. The results show that the proposed method detects copy-move counterfeiting and achieves a precision of about 83.22% for the IMD dataset and about 83.65% for the MICC-F600 dataset. Future work will focus on improving the localization precision of the area and expanding the method for detecting other types of image forgery.

References

[1] Roy, A., et al., Copy-Move Forgery Detection in Digital Images—Survey and Accuracy Estimation Metrics, in Digital Image Forensics. 2020, Springer. p. 27-56.

[2] Mahmood, T., et al., Copy-move forgery detection technique for forensic analysis in digital images. Mathematical Problems in Engineering, 2016. 2016.

[3] Raju, P.M. and M.S. Nair, Copy-move forgery detection using binary discriminant features. Journal of King Saud

[4] Novozámský, A. and M. Šorel, Detection of copy-move image modification using JPEG compression model. Forensic science international, 2018. 283: p. 47-57.

[5] Abd Warif, N.B., et al., Copy-move forgery detection: survey, challenges and future directions. Journal of Network and Computer Applications, 2016. 75: p. 259-278.

[6] Sun, Y., R. Ni, and Y. Zhao, Nonoverlapping blocks based copy-move forgery detection. Security and Communication Networks, 2018. 2018.

[7] Rao, Y. and J. Ni. A deep learning approach to detection of splicing and copy-move forgeries in images. in 2016 IEEE International Workshop on Information Forensics and Security (WIFS). 2016. IEEE.

[8] Amiri, E., et al., Detection of Topographic Images of Keratoconus Disease Using Machine Vision. International Journal of Engineering Science and Application, 2020. 4(4): p. 145-150.

[9] Alberry, H.A., A.A. Hegazy, and G.I. Salama. A fast SIFT based method for copy move forgery detection. Future Computing and Informatics Journal, 2018. 3(2): p. 159-165.

[10] Shivakumar, B. and S.S. Baboo, Detection of region duplication forgery in digital images using SURF. International Journal of Computer Science Issues (IJCSI), 2011. 8(4): p. 199.

[11] Khaledian, N., Mardukhi, F. CFMT: a collaborative filtering approach based on the nonnegative matrix factorization technique and trust relationships. Journal

of Ambient Intelligence and Humanized Computing. 2021 Jul 14:1-7.

[12] Kazemi A, Shiri ME, Sheikhahmadi A, Khodamoradi M. A new parallel deep learning algorithm for breast cancer classification. International Journal of Nonlinear Analysis and Applications. 2021 Jan 1;12(Special Issue):1269-82.

[13] Amiri S, Mosallanejad A, Sheikhahmadi A. Medical images fusion based on equilibrium optimization and discrete wavelet. International Journal of Nonlinear Analysis and Applications. 2021 Jan 1;12(Special Issue):1337-54.

[14] Jin, G. and X. Wan. An improved method for SIFT-based copy–move forgery detection using non-maximum value suppression and optimized J-Linkage. Signal Processing: Image Communication, 2017. 57: p. 113-125.

[15] Ramezanpour, M., Azimi, M. A., & Rahmati, M., A New Method for Eye Detection in Color Images. Journal of Advances in Computer Research, 2010; 1(2): 55-61.

[16] Fini MR, ZargariAsl F. A fast intra mode decision method based on reduction of the number of modes in HEVC standard. In7'th International Symposium on Telecommunications (IST'2014) 2014 Sep 9 (pp. 839-843). IEEE.

[17] Bilal M, Habib HA, Mehmood Z, Yousaf RM, Saba T, Rehman A. 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. 2021 Jul 4;53(4):459-82.

[18] Amerini, I., et al., A sift-based forensic method for copy–move attack detection and transformation recovery. IEEE transactions on information forensics and security, 2011. 6(3): p. 1099-1110.

[19] Amerini, I., et al., Copy-move forgery detection and localization by means of robust clustering with J-Linkage. Signal Processing: Image Communication, 2013. 28(6): p. 659-669.

[20] Toldo, R. and A. Fusiello, Image-consistent patches from unstructured points with J-linkage. Image and Vision Computing, 2013. 31(10): p. 756-770.

[21] Li, L., et al., An Efficient Scheme for Detecting Copy-move Forged Images by Local Binary Patterns. J. Inf. Hiding Multim. Signal Process., 2013. 4(1): p. 46-56.

[22] Hilal, A. and S. Chantaf. Uncovering copy–move traces using principal component analysis, discrete cosine transform and Gabor filter. Analog Integrated Circuits and Signal Processing, 2018. 96(2): p. 283-291.

[23] Ghodsi, M. and M. Saniee Abadeh, Fraud Detection of Credit Cards Using Neuro-fuzzy Approach Based on TLBO and PSO Algorithms. Journal of Computer & Robotics, 2017. 10(2): p. 57-68.

[24] Lin, C., et al., Copy-move forgery detection using combined features and transitive matching. Multimedia Tools and Applications, 2019. 78(21): p. 30081-30096.

[25] Fujishiro, I. and Y. Takeshima, Coherence-sensitive solid fitting. Computers & Graphics, 2002. 26(3): p. 417-427.

[26] Lowe, D.G., Object Recognition from Local Scale-Invariant Features. Int. Journal of Computer Vision, 2004. 60(2): p. 91-110.

[27] Hegazi, A., A. Taha, and M.M. Selim. An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal. Journal of King Saud University-Computer and Information Sciences, 2019.

[28] Lyu, Q., et al., Copy Move Forgery Detection based on double matching. Journal of Visual Communication and Image Representation, 2021. 76: p. 103057.

[29] Asl, V.F., et al., An Improved Real-Time Noise Removal Method in Video Stream based on Pipe-and-Filter Architecture. Journal of Computer & Robotics, 2021. 14(1): p. 21-32.

[30] Aboutalebi, M. and R. Abasi, Classification of Brain Tumor Grades by MRI Images using Artificial Neural Network. Journal of Computer & Robotics, 2019. 12(2): p. 1-11.

[31] Fridrich, A.J., B.D. Soukal, and A.J. Lukáš. Detection of copy-move forgery in digital images. in in Proceedings of Digital Forensic Research Workshop. 2003. Citeseer.

[32] Popescu, A.C. and H. Farid. Exposing digital forgeries by detecting duplicated image regions. 2004.

[33] Kang, X. and S. Wei. Identifying tampered regions using singular value decomposition in digital image forensics. in International conference on computer science and software engineering. 2008. IEEE.

[34] Zhang, J., Z. Feng, and Y. Su. A new approach for detecting copy-move forgery in digital images. in 2008 11th IEEE Singapore International Conference on Communication Systems. 2008. IEEE.

[35] Iranpour Mobarakeh, S. and M. Emadi, Improving Face Recognition Rate Based on Histogram of Oriented Gradients and Difference of Gaussian. Journal of Computer & Robotics, 2019. 12(2): p. 57-66.

[36] Kasiselvanathan, M., V. Sangeetha, and A. Kalaiselvi, Palm pattern recognition using scale invariant feature transform. International Journal of Intelligence and Sustainable Computing, 2020. 1(1): p. 44-52.

[37] Ardizzone, E., A. Bruno, and G. Mazzola, Copy–move forgery detection by matching triangles of keypoints. IEEE Transactions on Information Forensics and Security, 2015. 10(10): p. 2084-2094.

[38] Yang, F., et al., Copy-move forgery detection based on hybrid features. Engineering Applications of Artificial Intelligence, 2017. 59: p. 73-83.

[39] Emam, M., Q. Han, and X. Niu, PCET based copy-move forgery detection in images under geometric transforms. Multimedia Tools and Applications, 2016. 75(18): p. 11513-11527.

[40] Silva, E., et al., Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale

analysis and voting processes. Journal of Visual Communication and Image Representation, 2015. 29: p. 16-32.

[41] Deng, J., et al., Copy-move forgery detection robust to various transformation and degradation attacks. KSII Transactions on Internet and Information Systems (TIIS), 2018. 12(9): p. 4467-4486.

[42] Chen, H., Yang, X., & Lyu, Y. (2020). Copy-move forgery detection based on keypoint clustering and similar neighborhood search algorithm. IEEE Access, 8, 36863-36875.