Pamukkale Univ Muh Bilim Derg, 30(2), 222-227, 2024

Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi

Pamukkale University Journal of Engineering Sciences

Copy-Move forgery detection using EOA, DWT and DCT

EOA, DWT ve DCT kullanarak kopyalama-taşıma sahtecilik tespiti

Ehsan AMIRI[1], *Ahmad MOSALLANEJAD*[2*], *Amir SHEIKHAHMADI*[1]

[1]Department of Computer Engineering, Sanandaj Branch, Islamic Azad University, Sanandaj, Iran.
ehsan.amiri@iausdj.ac.ir, asheikhahmadi@iausdj.ac.ir

[2]Department of Computer Engineering, Sepidan Branch, Islamic Azad University, Sepidan, Iran.
ahmad.upm@gmail.com

Received/Geliş Tarihi: 31.03.2022 Revision/Düzeltme Tarihi: 15.01.2023 doi: 10.5505/pajes.2023.94395
Accepted/Kabul Tarihi: 13.04.2023 Research Article/Araştırma Makalesi

Abstract

Copy-move forgery (CMF) is a new challenge because it reduces the accuracy of image forgery detection. In CMFD, we have selected and pasted similar points. The proposed method based on the Equilibrium Optimization Algorithm (EOA), Discrete Wavelet Transform (DWT), and Discrete Cosine Transform (DCT) helps image forgery detection. The method includes feature detection, image segmentation, and detection of forgery areas using the EOA, DWT, and DCT. In the first step, the image converts to a grayscale. Then, with the help of a discrete cosine transform algorithm, it is taken to the signal domain. With the help of discrete wavelet transform, its appropriate properties are introduced. In the next step, the image is divided into blocks of equal size. Then the similarity search is performed with the help of an equilibrium optimization algorithm and a suitable proportion function. Copy-move forgery detection using the Equilibrium Optimization Algorithm can find areas of forgery with a precision of about 86.21% for the IMD data set and about 83.98% for the MICC-F600 data set.

Keywords: Forgery detection, Copy-Move image forgery, EOA algorithm.

Öz

Kopyala-taşı sahteciliği (CMF), görüntü sahteciliği tespitinin doğruluğunu azalttığı için yeni bir zorluktur. CMFD'de benzer noktaları seçip yapıştırdık. Denge Optimizasyon Algoritması (EOA), Ayrık Dalgacık Dönüşümü (DWT) ve Ayrık Kosinüs Dönüşümü (DCT) tabanlı önerilen yöntem, görüntü sahteciliğini tespit etmeye yardımcı olur. Yöntem, özellik tespiti, görüntü segmentasyonu ve EOA, DWT ve DCT kullanılarak sahte alanların tespitini içerir. İlk adımda, görüntü gri tonlamaya dönüştürülür. Daha sonra ayrık bir kosinüs dönüşüm algoritması yardımıyla sinyal alanına alınır. Ayrık dalgacık dönüşümü yardımıyla uygun özellikleri tanıtılır. Bir sonraki adımda, görüntü eşit büyüklükte bloklara bölünür. Daha sonra bir denge optimizasyon algoritması ve uygun bir orantı fonksiyonu yardımıyla benzerlik araştırması yapılır. Denge Optimizasyon Algoritması kullanılarak kopyala-taşı sahtecilik tespiti, IMD veri seti için yaklaşık %86.21 ve MICC-F600 veri seti için yaklaşık %83.98 hassasiyetle sahtecilik alanlarını bulabilir.

Anahtar kelimeler: Sahtecilik tespiti, Görüntüyü kopyala-taşıt sahtekarlığı, EOA algoritması.

1 Introduction

Intentional manipulation of an image to change its information is called image forgery [1], [2]. The most important forgeries are adding, deleting, or identifying objects in the image. Changing any feature or content of the image will result in forgery if it leaves no trace of the change in the result [3]. The number of software that edits the image for free is very large. Therefore, image forgery is very common. In contrast to image forgery, image forgery detection algorithms must be strong enough to detect image forgery [3],[4].

Copy-move forgery [5],[6] or simulation forgery is one of the most common types of image forgery. In forging copy-move, the part of the image that has the appropriate feature is copied and then selected by selecting the appropriate location. It is pasted in another part of the same image [7]. The main purpose of forging copy-move is to hide objects and some image aspects. The duplicate areas in the copy-move forgery can have different sizes and shapes and can be pasted the forged part of the image one or more times in different places (Figure 1) [8].

The motivation of CMFD detection is to detect manipulated images [9]. Image forgery detection is very important, and researchers are focused on CMFD and have achieved excellent results. According to the studies, copy-move forgery can be classified into two general methods [10] based on block and key-point.

Figure 1. An example of image forgery [8].

In block-based image forgery detection methods, the image is divided into several blocks, and the main features are obtained according to the selected blocks. Several different properties are selected from blocks in a block-based method. For example, the principal component analysis (PCA) method by Hilal et al. (2018) has been introduced [11]. The PCA method is used to describe blocks of low complexity.

In methods that use a key-point, key points are extracted from the image. The most important method among key-point methods is the scale variable property conversion (SIFT)

*Corresponding author/Yazışılan Yazar

method [14], which many studies use as a suitable descriptive method for detecting forgery. Amerini, in 2011 detected copy-move forgery based on the SIFT feature, which has obtained very good results [15],[16]. The SIFT method has been modified and improved in many studies. In Amiri et al., an optimal model of SIFT is introduced [4].

With the help of an evolutionary algorithm, this paper introduces an optimal method for detecting forgery in an image. This method is based on an equilibrium optimization algorithm (EOA).

The structure of this article consists of 5 main sections. Section 2 introduces the Evolutionary Algorithm (EOA). Section 3 presents a copy motion detection algorithm. Section 4 presents the experiments, and Section 5 presents the conclusions.

2 Literature review

Copy-move forgery detection (CMFD) methods are used in various applications such as image processing and news media. The CMFD is not just copying and pasting. A few transformations and processing are done that it significantly more challenging visually and by forensic strategies. Numerous methodologies have been proposed to take care of these cloning techniques.

Copy-Move Forgery Detection (CMFD) is classified into passive and active techniques. Active techniques require special hardware and software. Passive doesn't require any prior information about the image to be verified [5]. Passive techniques are keypoints and blocks. For example, some algorithms use the technique of Speeded Up Robust Features (SURF) [4], while some algorithms use the technique of Scale Invariant Feature Transform (SIFT) [15]. For keypoint-based CMFD techniques, the feature extraction phase consists of two steps: feature detection and description step [5]. Feature detection is to localize a set of keypoints/regions inside an image that is stable for geometric transformation [26]. In the description phase, key points are described by coding. SIFT and SURF are the most popular algorithms utilized in CMFD which can perform the features detection and description [26]. Another important method introduced in the past by Lee et al. (2013) is the extracted uniformly positioned binary patterns (LBPs) that were based on circular blocks [12]. The block method considered in this article is Discrete Cosine Transformation (DCT), introduced by Vega et al. in 2018 [13]. In this category, the features are stored in the form of quantized coefficients, extracted through discrete cosine transform, which contains the maximum information of image within the small number of coefficients. These quantized coefficients are sorted lexicographically and put into row of a matrix. Matching blocks are found using normalized movement vectors among all rows of matrix. The matching blocks, for which the value of the normalized movement vector is greater than the user-defined value, are considered as forged [13].

In the literature exist several optimization algorithms, one of the first is the Genetic Algorithm [19]. The first metaheuristics group utilizes evolution-inspired operators, such as mutation, recombination, and selection of the fittest. The second block of the metaheuristic algorithm is Swarm Intelligence (SI). This group has many approaches, like Particle Swarm Optimization (PSO), which possess operators based on the behavior of bird flocks or fish schools [20]. Several optimization algorithms have been proposed to obtain optimal solutions for various applications. In 2017, a spotted hyena optimizer (SHO) was proposed. The basic process of SHO is prey search, encircling, and prey attack. This SHO is utilized to solve several engineering problems such as optical buffer design and airfoil design and can be extended to solve multiple objective optimization problems [31]. Another evolutionary algorithm is the equilibrium optimization (EO) algorithm, inspired by control volume mass balance models used to estimate both dynamic and equilibrium states. In EO, each particle (solution) with its concentration (position) acts as a search agent. The search agents randomly update their concentration concerning best-so-far solutions [19].

3 Equilibrium optimization algorithm (EOA)

So far, many evolutionary algorithms [17],[18] have been introduced. Evolutionary algorithms such as Equilibrium Optimization (EO) can solve various problems based on intelligent principle [19]. The mass balance equation is obtained according to the amount of mass entered into the system. The mass balance equation with respect to the input is equal to the sum of the first output mass and the second output mass (Figure 2).

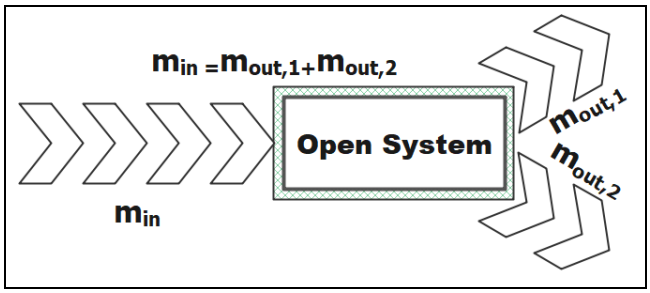

Figure 2. Input and output in the mass balance equation [19].

Sometimes it occurs in the accumulation system, in which case the stable energy equation and the state of general equilibrium must be maintained. In the case of accumulation, the sides of the equation must be equal [19].

$$V\frac{dC}{dt} = QC_{eq} - QC + G \quad (1)$$

According to Equation 1, the mass production rate equals the number of changes in the input per second. In Equation 1, C is mass per cubic meter, Q is the velocity, V is volume, and dc/dt indicates the rate of volume change [20].

According to these cases, $Q * C$ will be the system's input, and its unit is in kilograms in seconds. QC is also the concentration that goes out of control volume [19].

Equation 1 is a first-order differential equation showing the general mass equilibrium equation. In Equation 1, the change in mass over time is equal to the amount of mass entering [20].

If there is no change in the system and Vdc/dt is zero, a steady state of equilibrium is achieved. A stable equilibrium is a state in which a change in an equation does not occur during the period of stability. Therefore, the parameters of the stable equation do not change over time. In general, a constant equilibrium state is obtained when the input and output of the equation are constant [19].

4 Proposed approach

This section proposes Copy-Move Forgery Detection using an Equilibrium Optimization Algorithm (CMFDEOA) (as shown in

Figure 3). Evolutionary algorithms in the first stage should be initialized with a random amount.

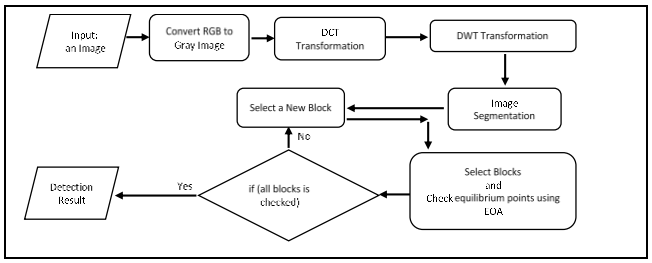

Figure 3. Copy-Move forgery detection with EOA, DWT and DCT.

As a result, one of the major challenges in solving this problem is the initialization of the EOA algorithm. Another issue is how to optimize based on the type of input features of the algorithm. Choosing the right feature impacts optimizing the algorithm and thus detecting forgery.

In the first step, an image is received as input. If the input image is a color image Figure 4(a), it should be converted into a grayscale image Figure 4(b) using the following formula.

$$Y = 0.298R + 0.582G + 0.117B \quad (2)$$

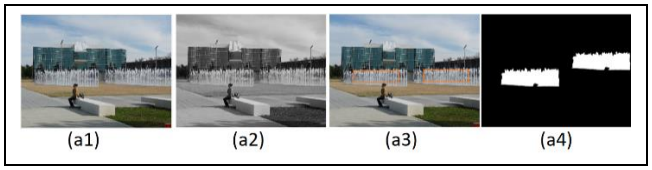

Figure 4. Copy Move using EOM, DWT and DCT. (a1): RGB. (a2): Grayscale. (a3): Matching. (a4): Detection of forgery.

The proposed method will convert The gray image obtained from the previous step to a new matrix with the Discrete Cosine Transform (DCT) function [21]. Converting an image to a DCT matrix will result in a matrix of image size. This operation is performed with the help of a discrete cosine function, which is a type of conversion in the frequency domain.

The Copy-Move detection method will convert the gray image obtained from the previous step to a new matrix with the Discrete Cosine Transform (DCT) function. Converting an image to a DCT matrix will result in a matrix of image size. This operation is performed with the help of a discrete cosine function, which is a type of conversion in the frequency domain.

The DCT matrix must be converted to a suitable matrix using a feature discovery method. The matrix that can achieve the appropriate EOA property is discrete wavelet transform. The DCT matrix is converted to a wavelet matrix using the two-dimensional wavelet (DWT) function [22]. This matrix has four bands LL, LH, HL, and HH. The band to be transferred to the next stage will be the LL band. The LL band will have the most connection with the main image. The conversion of a gray image into a wavelet is done according to Eq. (3).

$$[LL, LH, HL, HH] = 2D\ DWT\ function\ (DCT\ function\ (Gray\ Image)) \quad (3)$$

At this step, the converted LL matrix with the size MxN is divided into $(M - b + 1)x(N - b + 1)$ overlapping blocks by sliding the window of 10 x 10 pixels along from the upper-left corner right down to the lower-right corner. The size of each image block is b × b pixels. Bij represents the image blocks, where $1 \leq i \leq (M - b + 1)$ and $1 \leq j \leq (N - b + 1)$.

The most important part of the Copy-Move detection method is the selection of equilibrium points and forgery detection with the EOA evolutionary algorithm. At this stage, will select each of the blocks in order. These blocks are entered as input to the EOA algorithm, and the equilibrium determination operation begins. Like evolutionary algorithms, the EOA algorithm [19] has random input segments. In this section, three random blocks are selected from all other blocks as equilibrium blocks.

The balance check is performed by Eq. (1) and the input block. A very important point in using this method is to check the similarity of the blocks. The similarity of the blocks is investigated using the fitness function (Eq. (4)) [23].

$$fitness(m.n) = \sum_{x1=1}^{x2} \sum_{y1=1}^{y2} (|I_1(x1 + m - 1.y1 + n - 1) - I_2(x1.y1)|) \quad (4)$$

Fitness (m, n) shows the position in the block of the original, and I1 and I2 are values of the pixel for the original block and another block. The best fitness value is the minimum matching point. Fitness calculation requires calculation $(x1 - x2 + 1) * (y1 - y2 + 1)$ values of fit, and this item cannot detect all suitable forging blocks well. Here should be an optimal algorithm for a better selection of search areas. The proposed algorithm is an EOA algorithm, which results in good answers according to its equilibrium structure.

The maximum similarity is the best fitness function values in each round. The desired equilibrium parameters in each round will select a row of blocks and balance them. This process is done in two rounds for rows and columns of blocks to ensure the balance is achieved. The CMFDEOA (Figure 5) model compares all the image parts and returns the part with the most similarity.

Start Algorithm
f=input image;
f1=grayscale image(f) by **Eq. 2**;
Dctmatrix= DCT function in Gray Image;
[LL, LH, HL, HH] = 2D DWT function in Dctmatrix;
Select LL in output DWT function;
I1=segmentation section with 10 × 10 in LL matrix;
***for** k=1 to all section*
I2=select a segmentation in I1
Begin *EOA algorithm*
Step 1: Initialization. *Initialize random the population with two section and select row and column; Assign free parameter a_1=2, a_2=1, GP=0.5*
Step 2: while *Iteration < Max Iteration* ***do***
Step 3: *Evaluate the fitness by* **Eq. 2** *for each particle in section image by* **Eq. 4**, *C_i is row or column section, and $C_{eq1}$and C_{eq2} are two section of the population.*
if (fit(C_i)<fit(C_{eq1}) then
Replace ***C_i with C_{eq1}***
else if (fit(C_i)>fit(C_{eq1})) & (fit(C_i)<fit(C_{eq2})) then
Replace ***C_i with C_{eq2}***
end if
$C_{avg}=(C_1+C_2)/2$;
Change C_{eq1} and C_{eq2} with C_{avg};
Step 4: end while
Step 5: *Convert the selected blocks to the image with discovered areas.*
End *EOA algorithm*
End for k;
End Algorithm.

Figure 5. Copy move detection algorithm with EOA, DWT, and DCT.

The number of steps of this algorithm depends on the number of blocks obtained. After completing all the steps, the blocks with the most balance are selected as the forgery samples. Using the CMFDEOA model, the model's sensitivity in selecting

blocks increases. The innovation obtained in this model compared to similar block models is the selection of better molds and more sensitivity on the blocks.

The studies found that the CMFDEOA algorithm could not correctly detect about 45% of images in the first round. Still, the modified process was in other periods due to its evolutionary structure and obtained satisfactory results.

5 Experimental results

5.1 Databases

The first data set of IMD (Figure 6) [24] data sets contains 48 different simple images, rotates, noise images, and JPEG images. In the IMD data set, there are different sizes. The largest image in the IMD data set is about 3000 x 2300 pixels. The amount of manipulation in this data set is about 10%.

Figure 6. The proposed method in the copy-move forgery detection on the IMD dataset. Main image and Detected forgery region.

The second database, which contains 1440 images, is MICC-F600 [15], [16] (Figure 7). This dataset has more areas of manipulation, which is considered to be a lot of articles.

The size of the images in this dataset has a large variety and varies from 533×800 to 3888×2592 pixels. This collection includes forging in an area and several areas.

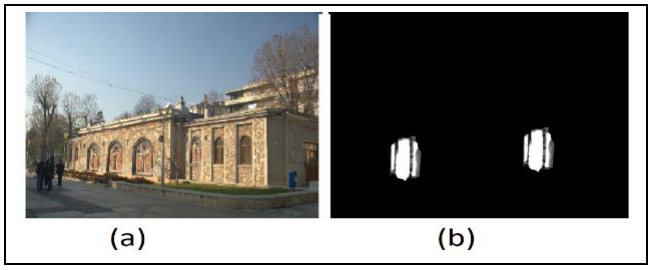

Figure 7. Results of the CMFDA algorithm on the MICC-F600 dataset. (a): Main image. (b): Detected forgery region.

CoMoFoD database (Figure 8) for a copy-move forgery detection consist of 260 forged image sets in two categories (small 512x512, and large 3000x2000). Images are grouped in 5 groups according to applied manipulation: translation, rotation, scaling, combination and distortion. Different types of postprocessing methods, such as JPEG compression, blurring, noise adding, color reduction etc., are applied to all forged and original images [32].

5.2 Performance measures

The image forging system aims to increase the accuracy of detecting and finding all pixels belonging to the tampered area. The function of forgery detection systems is tested on image level and pixel level. The function of forgery detecting areas at the image level is emphasized on whether an image is manipulated or not. In contrast, the forgery detection function at the pixel level focuses on the correct location of the manipulated areas.

Figure 8. Results of the CMFDA algorithm on the CoMoFoD dataset. (a): Main image. (b): Detected forgery region [32].

Generally, three commonly used indexes, $precision$ (Eq. 5), $recall$ (Eq. 6), and $F1$ (Eq. 7), indicate the effectiveness of the method in discovering the image forging. They are calculated as [25]:

$$Precision = \frac{A \cap B}{|A|} \tag{5}$$

$$Recall = \frac{|A \cap B|}{|B|} \tag{6}$$

$$F1 = 2 \times \frac{Precision\ .\ Recall}{Precision + Recall} \tag{7}$$

Two factors, A and B, are defined to calculate these parameters. The first factor, A, is forgery images identified by the CMFDEOA, and B is defined as forgery images available in the data set.

F1 includes two precision and recall benchmarks defined as a weighted average criterion because Precision Weights and Recall are used according to Formula 7.

5.3 Comparison results and analysis

In this section, some of the results of image forgery detection are examined with the help of various methods. One of the discussed algorithms is forgery detection with the help of the CMFDEOA algorithm. Keypoint-based methods can automatically detect fake images, but their results are inaccurate. The higher the accuracy of image forgery detection, the more powerful the proposed algorithm is compared to other methods.

5.3.1 Comparison of different aspects of the proposed method

DCT and DWT methods are used in image forgery detection. In the proposed method, the combination of these two methods is used along with the EO method. To check the importance of this composition, Table 1 has been prepared. Table 1 shows the accuracy of each DWT and DCT method on the IMD dataset.

The comparative results of the CMFDEOA method are given in Table 1 and show that it is better than other methods. The results of Table 1 show a 30% superiority between the combined method and the non-combined method. The reason for this superiority is the importance of balance optimization input data.

Table 1. Comparison of different aspects of the proposed method on the IMD, MICC-F600, and CoMoFoD datasets.

Algorithms	Precision of IMD (%)	Precision of MICC-F600 (%)	Precision of CoMoFoD (%)
DCT	45.12	40.77	31.94
DWT	59.01	53.41	37.21
EOA	51.77	46.21	42.94
DCT-EOA	44.10	46.99	40.08
DWT-EOA	66.38	63.02	60.28
DCT-DWT-EOA	86.21	86.12	86.18

5.3.2 Image forgery detection on IMD

The results of comparing the CMFDEOA algorithm with other methods studied on the IMD dataset are in the Table 2. The methods discussed are: SIFT [16], KAZE [26], LIOP [27], PCET [28], BAM [23] and MSA [29]. The type of images discussed in this comparison (Table 2) is simple images with up to 10% fraud.

Table 2. Comparison of the proposed method in the IMD data set.

Algorithms	Rate of Precision (%)	Rate of Recall (%)	Rate of F1 (%)
SIFT [16]	81.36	44.75	56.74
KAZE [26]	70.42	82.30	75.92
LIOP [27]	72.45	74.40	75.43
PCET [28]	72.64	63.78	68.70
MSA [29]	74.47	74.30	73.35
BAM [23]	81.39	83.79	82.19
CMFDEOA	86.21	86.12	86.18

The results in Table 2 show that the introduced method (CMFDEOA) has the highest accuracy (86.21%), followed by 81.39% in BAT and 81.36% in SIFT. The results in Table 2 show an improvement of about 5%. In forgery detecting areas, therefore, the proposed method has improved the results. The most important feature of this method is the selection of optimal blocks that other methods have not been able to detect.

5.3.3 Image forgery detection on MICC-F600

The results of comparing the CMFDEOA algorithm with other methods studied on the MICC-F600 dataset are in the Table 3. The methods discussed are: SIFT [16], KAZE [26], PCET [28], MSA [29], and BAM [23]. The type of images discussed in this comparison (Table 3) is simple images of different sizes.

Table 3. Comparison of the proposed method in the MICC-F600 dataset.

Algorithms	Rate of Precision (%)	Rate of Recall (%)	Rate of F1 (%)
SIFT [16]	77.54	42.22	54.66
KAZE [26]	68.41	51.41	58.71
PCET [28]	71.15	66.35	67.70
MSA [24]	64.57	72.44	68.01
BAM [23]	81.04	81.36	81.15
CMFDEOA	83.98	83.04	83.21

The comparative results of the CMFDEOA method are given in Table 3 and show that it is better than other methods. According to the Precision, Recall, and F1 columns shown in Table 3, it is clear that the number of forged images detected with this method is much higher than in other methods.

5.3.4 Image forgery detection on CoMoFoD

The results of comparing the CMFDEOA algorithm with other methods studied on the CoMoFoD dataset are in the Table 4. The methods discussed are: SIFT [16], KAZE [26], PCET [28], and DAMFT [30]. The type of images discussed in this comparison (Table 4) is simple images of different sizes.

Table 4. Comparison of the proposed method in the CoMoFoD dataset

Algorithms	Rate of Precision (%)	Rate of Recall (%)	Rate of F1 (%)
SIFT [16]	79.36	56.23	67.79
KAZE [26]	61.03	57.12	59.07
PCET [28]	72.09	62.33	67.21
DAMFT [30]	74.39	79.27	76.83
CMFDEOA	82.13	82.75	82.44

The comparative results of the CMFDEOA method are given in Table 4 and show that it is better than other methods. According to the Precision, Recall, and F1 columns shown in Table 4, it is clear that the number of forged images detected with this method is much higher than in other methods.

6 Conclusion and future work

Block-based or key-based methods can detect image forgery. The method introduced is an EOA-based algorithm called CMFDEOA, which focuses on detecting copy-move forgery. In CMFDEOA, the images are first converted to the gray image, then a DCT transformation is applied to the image to reduce the amount of calculations. The DWT method, which is generally considered to detect forgery in block form, is used and forgery blocks are identified. An Equilibrium optimization method has been used to improve the results of forgery detection. Experimental analysis of the proposed method showed its effectiveness in detecting copy-move forgery. This method offers higher precision. The precision in Table 2, Table 3 and Table 4 is better than other algorithms. Table 2, Table 3 and Table 4 also show that the proposed copy-move forgery method obtains forged points with 86.21% in the precision for the IMD dataset, about 83.98% for the MICC-F600 dataset and 83.21 for the CoMoFoD dataset. It is possible to improve the accuracy of local point detection and expand the detection area in the future.

7 Author contribution statements

In the scope of this study, Ehsan AMIRI, in the formation of the idea, the design of the system, performing analyzes and writing the article; Ahmad MOSALLANEJAD, in the formation of the idea and checking the article; Amir SHEIKHAHMADI the assessment of obtained results and checking the article, were contributed.

8 Ethics committee approval and conflict of interest statement

"There is no need to obtain permission from the ethics committee for the article prepared".

"There is no conflict of interest with any person/institution in the article prepared".

9 References

[1] Abd Warif NB, Wahab AW, Idris MY, Ramli R, Salleh R, Shamshirband S, Choo KK. "Copy-move forgery detection: survey, challenges and future directions". *Journal of Network and Computer Applications*, 75, 259-78, 2016.

[2] Ulutas G, Ustubioglu B, Ulutas M, Nabiyev V. Video forgery detection method based on local difference binary. Pamukkale University Journal of Engineering Sciences. 26(5):983-92, 2020.

[3] Liu K, Lu W, Lin C, Huang X, Liu X, Yeung Y, Xue, Y. "Copy move forgery detection based on keypoint and patch match". *Multimedia Tools and Applications*, 78(22), 31387-31413, 2019.

[4] Amiri E, Mosallanejad A, Sheikhahmadi A. "Copy-Move forgery detection by an optimal keypoint on SIFT (OKSIFT) Method". *Journal of Computer & Robotics*, 14(2), 11-19, 2021.

[5] Tahaoğlu G, Ulutas G. "Copy-move forgery detection and localization with hybrid neural network approach". *Pamukkale University Journal of Engineering Sciences*, 28(5), 748-760, 2022.

[6] Deep Kaur C, Kanwal N. "An analysis of image forgery detection techniques". *Statistics, Optimization & Information Computing*, 7(2), 486-500, 2019.

[7] Roy A, Dixit R, Naskar R, Chakraborty RS. "Copy-Move forgery detection in digital images-survey and accuracy estimation metrics". *In Digital Image Forensics*, 27-56, Springer, 2020.

[8] Alberry HA, Hegazy AA, Salama GI. "A fast SIFT based method for copy move forgery detection". *Future Computing and Informatics Journal*, 3(2), 159-165, 2018.

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

[10] Teerakanok, Songpon, Tetsutaro Uehara. "Copy-move forgery detection: A state-of-the-art technical review and analysis". *IEEE Access*, 7, 40550-40568, 2019.

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

[12] Lee JC. "Copy-move image forgery detection based on Gabor magnitude". *Journal of Visual Communication and Image Representation*, 31, 320-334, 2015.

[13] Vega EAA, Fernández EG, Orozco ALS, Villalba LJG. "Copy-move forgery detection technique based on discrete cosine transform blocks features". *Neural Computing and Applications*, 33(10), 4713-4727, 2021.

[14] Lowe DG. "Object Recognition from Local Scale-Invariant Features". *International Journal of Computer Vision*, 60(2), 91-110, 2004.

[15] Amerini I, Ballan L, Caldelli R, Del Bimbo A, Del Tongo L, & Serra G. "Copy-move forgery detection and localization by means of robust clustering with J-Linkage". *Signal Processing: Image Communication*, 28(6), 659-669, 2013.

[16] Amerini I, Ballan L, Caldelli R, Del Bimbo A, Serra G. "A sift-based forensic method for copy–move attack detection and transformation recovery". *IEEE Transactions on Information Forensics and Security*, 6(3), 1099-1110, 2011.

[17] Üstün O. "Determination of activation functions in a feedforward neural network by using genetic algorithm". *Pamukkale University Journal of Engineering Sciences*, 15(3), 395-403, 2009.

[18] Başkan Ö, Ceylan H. "Differential evolution algorithm based solution approaches for solving transportation network design problems". *Pamukkale University Journal of Engineering Sciences*, 20(9), 324-31, 2014.

[19] Faramarzi A, Heidarinejad M, Stephens B, Mirjalili S. "Equilibrium optimizer: a novel optimization algorithm". *Knowledge-Based Systems*, 191, 1-21, 2020.

[20] Shaheen AM, Elsayed AM, El-Sehiemy RA, Abdelaziz AY. "Equilibrium optimization algorithm for network reconfiguration and distributed generation allocation in power systems". *Applied Soft Computing*, 98, 1-19, 2021.

[21] Şahin Y, Ulutaş G, İmamoğlu M. "A fragile zero watermarking schema to check integrity of relational databases based on discrete cosines transform". *Pamukkale University Journal of Engineering Sciences*, 24(5), 887-897, 2018.

[22] Yildiz K, Buldu A. "Wavelet transform and principal component analysis in fabric defect detection and classification". *Pamukkale University Journal of Engineering Sciences*, 23(5), 622-627, 2017.

[23] Amiri E, Mosallanejad A, Sheikhahmad, A. "Copy-move forgery detection using a bat algorithm with mutation". *International Journal of Nonlinear Analysis and Applications*, 12(Special Issue), 1947-1955, 2021.

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

[25] Lyu Q, Luo J, Liu K, Yin X, Liu J, Lu W. "Copy Move Forgery Detection based on double matching". *Journal of Visual Communication and Image Representation*, 76, 1-14, 2021.

[26] Yang F, Li J, Lu W, Weng J. "Copy-move forgery detection based on hybrid features". *Engineering Applications of Artificial Intelligence*, 59, 73-83, 2017.

[27] Lin C, Lu W, Huang X, Liu K, Sun W, Lin H, Tan Z. "Copy-move forgery detection using combined features and transitive matching". *Multimedia Tools and Applications*, 78(21), 30081-30096, 2019.

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

[29] Silva E, Carvalho T, Ferreira A, Rocha A. "Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes". *Journal of Visual Communication and Image Representation*, 29, 16-32, 2015.

[30] Deng J, Yang J, Weng S, Gu G, Li Z. "Copy-move forgery detection robust to various transformation and degradation attacks". *KSII Transactions on Internet and Information Systems (TIIS)*, 12(9), 4467-4486, 2018.

[31] Dhiman G, Vijay K. "Spotted hyena optimizer: a novel bio-inspired based metaheuristic technique for engineering applications". *Advances in Engineering Software*, 114, 48-70, 2017.

[32] Tralic D, Zupancic I, Grgic S, Grgic M. "CoMoFoD-New database for copy-move forgery detection". *55th International Symposium ELMAR-2013*, Zadar, Croatla, 25-27 September 2013.