STATISTICS, OPTIMIZATION AND INFORMATION COMPUTING
Stat., Optim. Inf. Comput., Vol. **11**, June 2023, pp 677–684.
Published online in International Academic Press (www.IAPress.org)

Copy-Move Forgery Detection Using an Equilibrium Optimization Algorithm (CMFDEOA)

Ehsan Amiri [1], Ahmad Mosallanejad [2,*], Amir Sheikhahmadi [1]

[1] *Department of Computer Engineering, Sanandaj Branch, Islamic Azad University, Sanandaj, Iran*
[2] *Department of Computer Engineering, Sepidan Branch, Islamic Azad University, Sepidan, Iran*

Abstract Image forgery detection is a new challenge. One type of image forgery is a copy-move forgery. In this method, part of the image is copied and placed at the most similar point. Given the existing algorithms and processing software, identifying forgery areas is difficult and has created challenges in various applications. The proposed method based on the Equilibrium Optimization Algorithm (EOA) helps image forgery detection by finding forgery areas. The proposed method includes feature detection, image segmentation, and detection of forgery areas using the EOA algorithm. In the first step, the image converts to a grayscale. Then, with the help of a discrete cosine transform (DCT) algorithm, it is taken to the signal domain. With the help of discrete wavelet transform (DWT), 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 (CMFDEOA) can find areas of forgery with an accuracy of about 86.21% for the IMD data set and about 83.98% for the MICC-F600 data set.

Keywords Image Forgery; Copy-Move Forgery; EOA Algorithm; Discrete Cosine Transform; Discrete Wavelet Transform

DOI: 10.19139/soic-2310-5070-1511

1. Introduction

Image forgery is the process of deliberately manipulating an image to alter its information [1]. This manipulation can be done by adding, removing, or detecting. Image forgery is modifying any feature of the image or content, leaving no trace of the resulting change [2]. Due to many free image editing tools and software, forgery has become easier difficult. It has eroded confidence in the accuracy and integrity of an image. Therefore, robust algorithms for automatic forgery detection are essential and are an important research problem in image processing [2, 3].

Among the types of image forgery, *copy-move forgery* (CMF) [4, 5], also called cloning, is the most common model. In this type of image forging, part of an image is copied and pasted into another part of the same image [6]. The main purpose of this type of forgery is to hide unwanted objects, copy some aspects of the image or enhance the visual impact. Copied areas can be of any size and shape and can be pasted one or more times in different places in the same image (Figure 1) [7].

The motivation of *Copy-Move Forgery Detection* (CMFD) is to detect manipulated images [8]. Image forgery detection is very important, and many researchers have focused on CMFD and have achieved excellent results. According to the studies, copy-move forgery can be classified into two general methods based on block and key-point [9].

In block-based CMFD methods, most images are divided into several blocks, and the required properties are

[*] Correspondence to: Ahmad Mosallanejad (Email: ahmad.upm@gmail.com). Department of Computer Engineering, Islamic Azad University of Sepidan. Ardakan City, University Street, Iran.

ISSN 2310-5070 (online) ISSN 2311-004X (print)

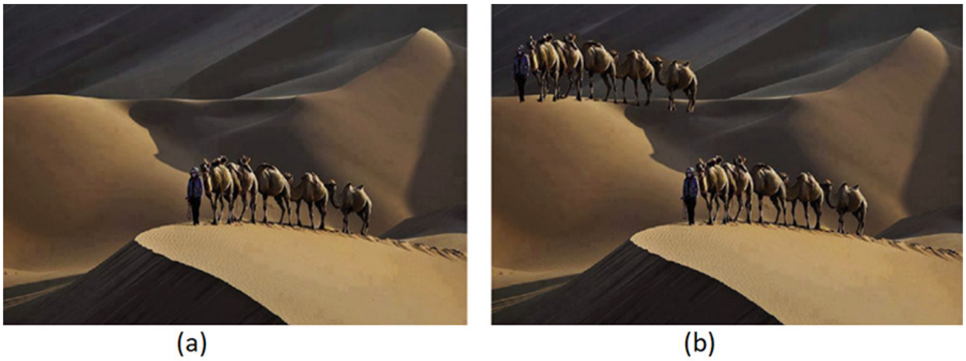


Figure 1. Example of copy-move forgery[7].

obtained according to the selected blocks of the image. In the block-based method, several different properties of the blocks are selected after obtaining the required blocks. For example, Hilal et al. (2018) used *principal component analysis* (PCA) [10] to describe blocks of low complexity, and in (2013), Lee et al., extracted uniform *localized binary patterns* (LBP) were from circular blocks [11]. One method that has been considered the block method is the *discrete cosine transform* (DCT), which was introduced by Vega et al. in 2018 [12].

In key-point methods, key points are extracted from the image. The *scale-invariant feature transform* (SIFT) [3] is used in many studies as a key and descriptive point in CMFD. For example, Amerini et al. (2011) proposed copy motion detection based on the SIFT feature and provided a good start in counterfeiting detection [14, 15]. Despite the suitability of the SIFT method, various methods have improved its performance. In Amiri (2021), an optimal model of SIFT is introduced [3].

This article introduces an optimal way to identify different and similar parts of an image. This method will be based on an *Equilibrium Optimization Algorithm* (EOA). Due to the challenges in detecting fake points, the proposed method has tried to get the most connection between fake pixels.

The rest of the paper is organized as follows: Section 2 introduces the equilibrium optimization algorithm. Section 3 presents a copy motion detection algorithm. Section 4 presents the experiments, and Section 5 presents the conclusions.

2. Equilibrium Optimization Algorithm (EOA)

Equilibrium Optimization (EO) [16] is a swarm intelligence optimization method. For a mass balance equation written on a system, it can be said that the amount of mass entering the system is equal to the amount of the first output masses plus the amount of the second output masses if there is no accumulation or storage in the system (Figure 2).

In the cases that arise in the accumulation system, must maintain the stable energy equation and the general equilibrium state on the other side, i.e., the sides of the equation must be equal again [16].

$$V\frac{dc}{dt} = QC_{eq} - QC + G. \tag{1}$$

In the above equation (Eq. 1), the algebraic sum minus the input minus the output plus the mass generation rate equals how many changes occur per second on the input. In this equation on the first side, V is the unit of volume, and its unit is cubic meters, dc is the differential derivative of concentration changes. Its unit is kilograms per volume, dt is the differential derivative of time changes that $\frac{dc}{dt}$ is the rate of volume change for us, C The mass is in one cubic meter, and since factors, V and C are cubic meters, V * dc is equal to kilograms and the whole unit to the left is equal to kilograms per second [17].

On the other side and to the right of this equation is C equilibrium and its unit in kilograms per cubic meter, Q

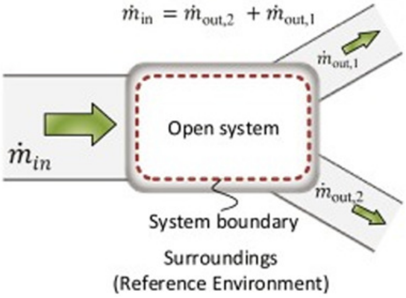


Figure 2. Input and output in the mass balance equation [16].

flow rate (flow rate passing through a system point per unit time) and its unit in cubic meters per second, then Q * C as input and its unit in kilograms in Counts as seconds. Should note that the input of the problem is initially considered in equilibrium. QC is the concentration that leaves the control volume, G is the mass production within the control volume [16].

With the above explanations, it can be said that the above equation is a first-order differential equation, which is, in fact, the general equation of mass equilibrium, in which the change in mass in time is equal to the amount of mass entering the system plus the changes produced. Alternatively, deleted within the control volume minus the value logged out [17].

If there are no changes in the system, i.e., V$\frac{dc}{dt}$ reaches zero, and a stable equilibrium state is achieved. Stable equilibrium means that no change in an equation occurs over time, and the parameters of the equation do not change over time. So, in general, when the input and output of the equation are fixed and do not change, a steady state of equilibrium is achieved [16].

3. Proposed approach

This section proposes *Copy-Move Forgery Detection using an Equilibrium Optimization Algorithm* (CMFDEOA) (as shown in Figure 3). Swarm algorithms must have random initial values to execute and optimize. 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.

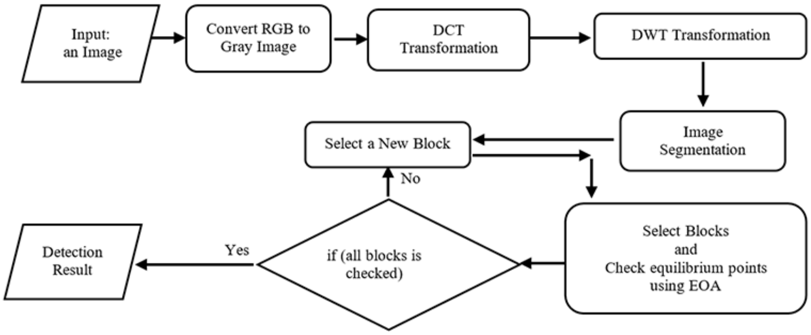


Figure 3. Copy-Move forgery detection with EOA.

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 (Eq. 2).

$$GrayImage = 0.298R + 0.582G + 0.117B. \tag{2}$$

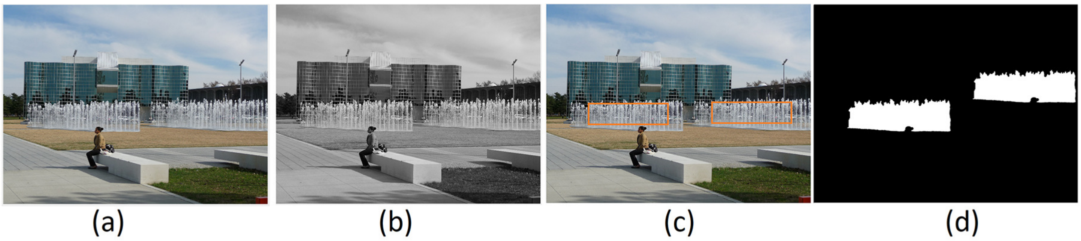


Figure 4. Copy Move with EOM, (a) Main Image, (b) Gray Image, (c) Image Matching, (d) Detection Result.

The proposed 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 a *discrete wavelet transform* (DWT). The DCT matrix is converted to a wavelet matrix using the two-dimensional wavelet function. 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.

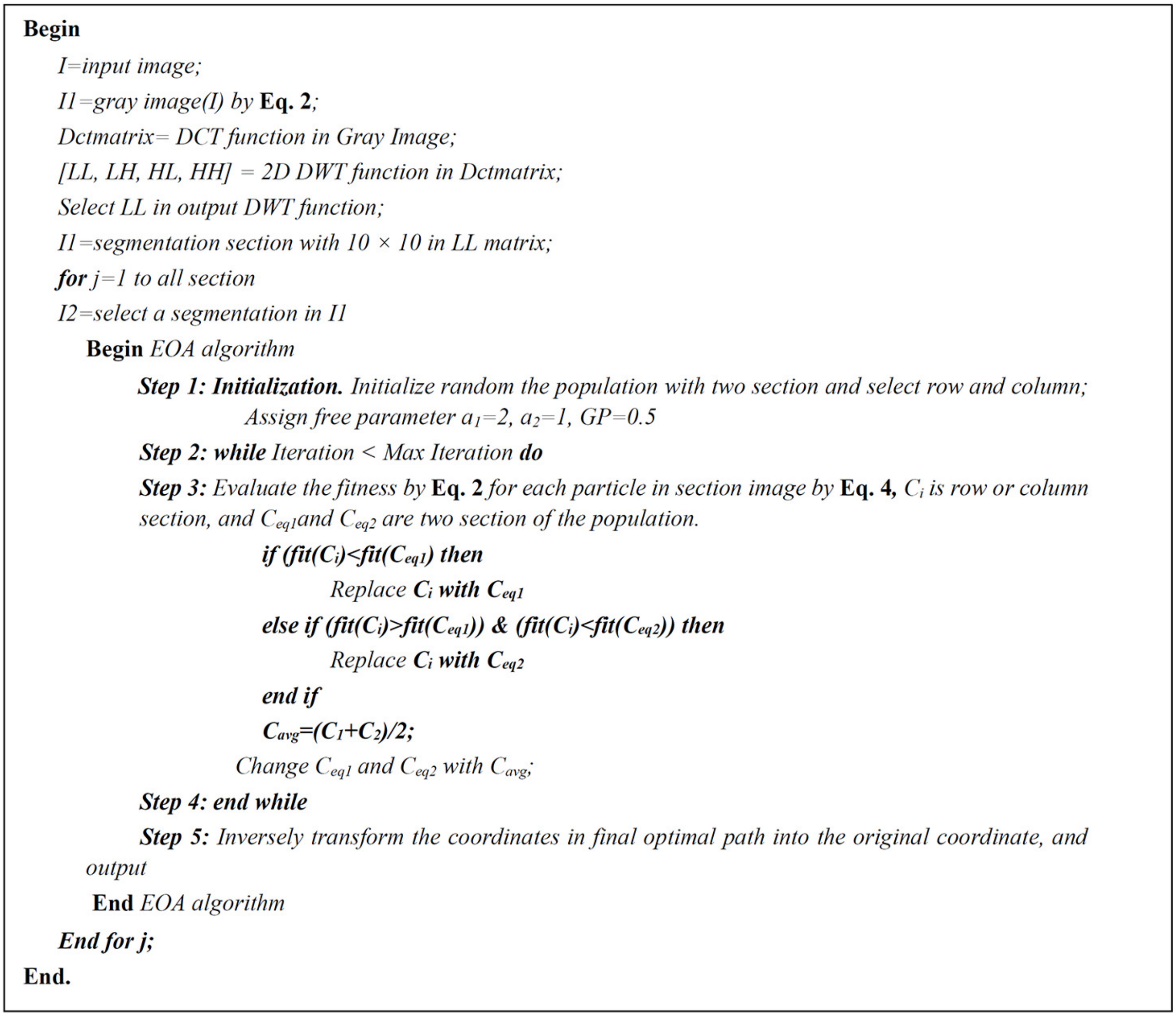
$$[LL, LH, HL, HH] = 2DDWTfunction(DCTfunction(GrayImage)). \tag{3}$$

At this step, the converted LL matrix with the size M×N is divided into $(M - b + 1)(N - b + 1)$ overlapping blocks by sliding the window of 10 × 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 proposed 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 (Afshin Faramarzi et al.) 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].

$$Fitness(C_i) = \sum_{i=1}^{M2} \sum_{j=1}^{N2} (|I_1(i + x - 1, j + y - 1) - I_2(i, j)|) \tag{4}$$

Where (x, y) represents the position in the original section, I1 and I2 are the pixel values for the original section and object section, respectively. Among many definitions for fitness (x, y), the best fitness (the minimum fitness) is the matching point. For timely implementation, it needs to calculate $(M1 - M2 + 1) * (N1 - N2 + 1)$ fitness values, and it is so time-consuming to compute that it cannot satisfy the real-time application. Therefore, the paper uses an EOA algorithm to accelerate searching speed. Each round is updated according to the maximum similarity between the balance parameters. 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. 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 CMFDEOA algorithm could not find a suitable section on 45% of the images in the first round based on the investigations. However, this operation was completed in other rounds and found similar sections.



```
Begin
    I=input image;
    I1=gray image(I) 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 j=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: Inversely transform the coordinates in final optimal path into the original coordinate, and
        output
        End EOA algorithm
    End for j;
End.
```

Figure 5. Copy Move detection algorithm using EOA.

4. Experimental results

4.1. Databases

The first database contains the IMD (*Image Manipulation Dataset*) public image data set (Figure 6) [18] 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.

The second database is known as MICC-F600 [14, 15], which contains 1440 images (Figure 7). 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 x 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.

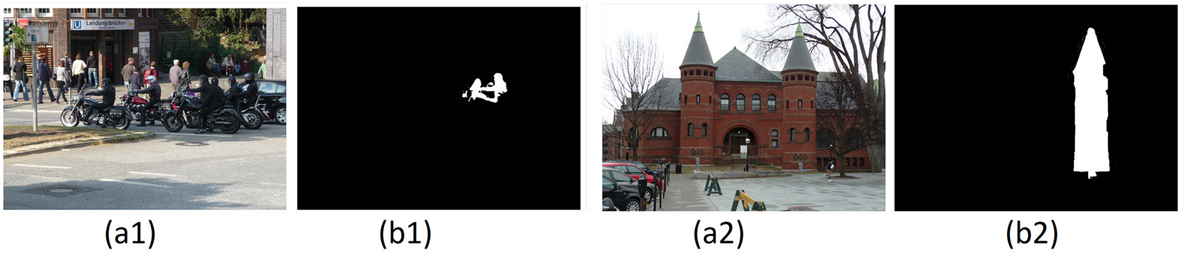


Figure 6. Example results of the EOA forgery detection algorithm on the IMD dataset. (a1) and (b1) Original image. (a2) and (b2) Detected region.

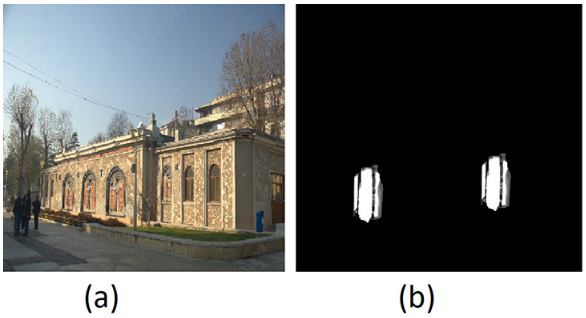


Figure 7. Example results of the EOA forgery detection algorithm on the MICC-F600 dataset. (a) is an Original image. (b) is a Detected region.

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. The performance of the CMFD schemes is tested at two levels: the image level and the pixel level. At the image level, whether an image has been tampered with or not is emphasized, while the pixel-level focuses on correctly locating the tampered regions. Generally, three commonly used indexes, *precision* (Eq. 5),*recall* (Eq. 6) and *F1* (Eq. 7), represent the effect of different aspects, which are also applied to our method evaluation. They are calculated as [19]:

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

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

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

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. (5) 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. (6). 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. (7).

4.3. Comparison results and analysis

The results of the quantitative analysis of the images are taken according to the proposed model, which includes the detection of forgery with the help of EOA. The Keypoint method automatically detects fake images, but the

Table 1. Results of the IMD dataset.

Methods	Precision [%]	Recall [%]	F1 [%]
SIFT[15]	80.77	43.75	56.75
KAZE[20]	71.43	83.33	76.93
LIOP[21]	73.44	75.41	74.42
PCET[22]	73.65	62.77	67.69
BAM[23]	81.39	83.79	82.19
MSA[24]	75.48	73.28	74.36
CMFDEOA	86.21	86.12	86.18

Table 2. Results of the MICC-F600 dataset.

Methods	Precision [%]	Recall [%]	F1 [%]
SIFT[15]	77.55	42.21	54.67
KAZE[20]	68.40	51.40	58.70
PCET[22]	71.14	66.34	67.69
BAM[23]	81.04	81.36	81.15
MSA[24]	64.58	72.45	68.00
DAMFT[25]	73.86	73.28	74.00
CMFDEOA	83.98	83.04	83.21

results are not complete 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 In this section, the identified results are compared with some of the advanced CMFD methods. These methods include SIFT [15], KAZE [20], LIOP [21], PCET [22], BAM [23], and MSA [24]. In this case, the results are shown in the simple copy subset in Table 1.

Table 1 shows that the CMFDEOA method has the highest precision (86.21%), followed by 81.39% in BAT and 80.77% in SIFT. 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 of the advanced CMFD methods on the MICC-F600 dataset. The methods of introduction in this section, as in the previous section, are SIFT [15], KAZE [20], PCET [22], MSA [24], BAM [23], and DAMFT [25]. In this case, the results are shown in the simple copy subset in Table 2.

Table 2 shows that the CMFDEOA method is better than the other methods. According to the Precision, recall, and F1 column, it is clear that the number of image forgeries detected by this method is much higher than by other methods.

5. Conclusion and future work

The CMFDEOA method focuses on detecting copy-move forgery using the EOA 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 86.21% for the IMD dataset and about 83.98% 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. A. Warif, N. Bakiah, A. W. A. Wahab, M. Y. I. Idris, R. Ramli, R. Salleh, S. Shamshirband, and K. R. Choo, *Copy-move forgery detection: survey, challenges and future directions*, Journal of Network and Computer Applications vol. 75, pp. 259–278, 2016.
2. K. Liu, W. Lu, C. Lin, X. Huang, X. Liu, Y. Yeung, and Y. Xue, *Copy move forgery detection based on keypoint and patch match*, Multimedia tools and applications vol. 78, no. 22, pp. 31387–31413, 2019.
3. A. Amiri, A. Mosallanejad, and A. Sheikhahmadi, *Copy-Move Forgery Detection by an Optimal Keypoint on SIFT (OKSIFT) Method*, Journal of Computer & Robotics, vol. 14, no. 2, pp. 11–19, 2021.
4. R. P. Mariam, and M. S. Nair, *Copy-move forgery detection using binary discriminant features*, Journal of King Saud University-Computer and Information Sciences, vol. 34, no. 2, pp. 165–178, 2018.
5. D. K. Chandan, and N. Kanwal, *An analysis of image forgery detection techniques*, Statistics, Optimization & Information Computing, vol. 7, no. 2, pp. 486–500, 2019.
6. R. Aniket, R. Dixit, R. Naskar, and R. S. Chakraborty, *Copy-Move Forgery Detection in Digital Images—Survey and Accuracy Estimation Metrics*, In Digital Image Forensics, Springer, Singapore, pp. 27–56, 2020.
7. H. A. Alberry, A. A. Hegazy, and G. I. Salama, *A fast SIFT based method for copy move forgery detection*, Future Computing and Informatics Journal, vol. 3, no. 2, pp. 159–165, 2018.
8. Y. Sun, R. Ni, and Y. Zhao, *Nonoverlapping blocks based copy-move forgery detection*, Security and Communication Networks, no. Special Issue, 2018.
9. S. Teerakanok, and T. Uehara, *Copy-move forgery detection: A state-of-the-art technical review and analysis*, IEEE Access, vol. 7, pp. 40550–40568, 2019.
10. A. Hilal, and S. Chantaf, *Uncovering copy–move traces using principal component analysis, discrete cosine transform and Gabor filter*, Analog Integrated Circuits and Signal Processing, vol. 96, no. 2, pp. 283–291, 2018.
11. J. C. Lee, *Copy-move image forgery detection based on Gabor magnitude*, Journal of visual communication and image representation, vol. 31, pp. 320–334, 2015.
12. E. A. A. Vega, E. G. Fernández, A. L. S. Orozco, and L. J. G. Villalba, *Copy-move forgery detection technique based on discrete cosine transform blocks features*, Neural Computing and Applications, vol. 33, no. 10, pp. 4713–4727, 2021.
13. D. G. Lowe, *Object Recognition from Local Scale-Invariant Features. Int*, Journal of Computer Vision, vol. 60, no. 2, pp. 91–110, 2004.
14. I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, L. D. Tongo, and G. Serra, *Copy-move forgery detection and localization by means of robust clustering with J-Linkage*, Signal Processing: Image Communication, vol. 28, no. 6, pp. 659–669, 2013.
15. I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, and G. Serra, *A sift-based forensic method for copy–move attack detection and transformation recovery*, IEEE transactions on information forensics and security, vol. 6, no. 3, pp. 1099–1110, 2011.
16. A. Faramarzi, M. Heidarinejad, B. Stephens, and S. Mirjalili, *Equilibrium optimizer: A novel optimization algorithm*, Knowledge-Based Systems, vol. 191, pp. 105190, 2020.
17. A. M. Shaheen, A. M. Elsayed, R. A. El-Sehiemy, and A. Y. Abdelaziz, *Equilibrium optimization algorithm for network reconfiguration and distributed generation allocation in power systems*, Applied Soft Computing, vol. 98, pp. 106867, 2021.
18. E. Ardizzone, A. Bruno, and G. Mazzola, *Copy–move forgery detection by matching triangles of keypoints*, IEEE Transactions on Information Forensics and Security, vol. 10, no. 10, pp. 2084–2094, 2015.
19. Q. Lyu, J. Luo, K. Liu, X. Yin, J. Liu, and W. Lu, *Copy Move Forgery Detection based on double matching*, Journal of Visual Communication and Image Representation, vol. 76, pp. 103057, 2021.
20. F. Yang, J. Li, W. Lu, and J. Weng, *Copy-move forgery detection based on hybrid features*, Engineering Applications of Artificial Intelligence, vol. 59, pp. 73–83, 2017.
21. C. Lin, W. Lu, X. Huang, K. Liu, W. Sun, H. Lin, and Z. Tan, *Copy-move forgery detection using combined features and transitive matching*, Multimedia Tools and Applications, vol. 78, no. 21, pp. 30081–30096, 2019.
22. M. Emam, Q. Han, and X. Niu, *PCET based copy-move forgery detection in images under geometric transforms*, Multimedia Tools and Applications, vol. 75, no. 18, pp. 11513–11527, 2016.
23. E. Amiri, A. Mosallanejad, and A. Sheikhahmadi, *Copy-move forgery detection using a bat algorithm with mutation*, International Journal of Nonlinear Analysis and Applications, vol. 12, no. Special Issue, pp. 1947–1955, 2021.
24. E. Silva, T. Carvalho, A. Ferreira, and A. Rocha, *Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes*, Journal of Visual Communication and Image Representation, vol. 29, pp. 16–32, 2015.
25. J. Deng, J. Yang, S. Weng, G. Gu, and Z. Li, *Copy-move forgery detection robust to various transformation and degradation attacks*, KSII Transactions on Internet and Information Systems (TIIS), vol. 12, no. 9, pp. 4467–4486, 2018.