Original Article

The Optimal Model for Copy-Move Forgery Detection in Medical Images

Abstract

Background: Digital devices can easily forge medical images. Copy-move forgery detection (CMFD) in medical image has led to abuses in areas where access to advanced medical devices is unavailable. Forgery of the copy-move image directly affects the doctor's decision. The method discussed here is an optimal method for detecting medical image forgery. **Methods:** The proposed method is based on an evolutionary algorithm that can detect fake blocks well. In the first stage, the image is taken to the signal level with the help of a discrete cosine transform (DCT). It is then ready for segmentation by applying discrete wavelet transform (DWT). The low-low band of DWT, which has the most image properties, is divided into blocks. Each block is searched using the equilibrium optimization algorithm. The blocks are most likely to be selected, and the final image is generated. **Results:** The proposed method was evaluated based on three criteria of precision, recall, and F1 and obtained 90.07%, 92.34%, and 91.56%, respectively. It is superior to the methods studied on medical images. **Conclusions:** It concluded that our method for CMFD in the medical images was more accurate.

Keywords: *Copy-move forgery detection, discrete cosine transform, discrete wavelet transform, equilibrium optimization, medical image*

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

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

Submitted: 10-May-2022 **Revised:** 29-Aug-2022 **Accepted:** 06-Mar-2023 **Published:** 26-Mar-2024

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 (CMF)[5,6] or simulation forgery is one of the most common types of image forgery. In forging copy-move, the part of the image with the appropriate feature is copied and then selected by selecting the appropriate location. It is posted in another part of the same image.[7] The main purpose of forging copy-move is to hide objects and image aspects. The same areas in the CMF 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]

Today's systems are replacing traditional paper-based health records to be more efficient in retrieving, accessing, and transferring data.[9] They have a lot of data about people, such as age, weight, medical history, allergies, magnetic resonance imaging scans, and computed tomography scans.[10] An internal attacker working in health-care systems or an external intruder via the Internet may interfere with the treatment process by altering the patient's health images. Defaming movie stars, politicians, or ordinary people and creating confusion in the patient insurance process is one of the most important reasons. Therefore, one must authenticate such digital records before any treatment or review.

Forgery in medical images[9] is one of the most important issues in forensic medicine. People get insurance benefits by forging medical pictures. It has sometimes been observed that an athlete refuses to perform exercises or competitions by changing medical images. By falsifying their medical images, workers persuade employers to

How to cite this article: Amiri E, Mosallanejad A, Sheikhahmadi A. The optimal model for copy-move forgery detection in medical images. J Med Sign Sens 2024;14:5.

Address for correspondence:
Dr. Ahmad Mosallanejad,
Department of Computer Engineering, Sepidan Branch, Islamic Azad University, Ardakan, Sepidan, Iran.
E-mail: ahmad.upm@gmail.com

Access this article online

Website: www.jmssjournal.net

DOI: 10.4103/jmss.jmss_35_22

Quick Response Code:

grant special benefits. If applied to a medical image, CMF misleads the physician or hospital staff.[10] In CMF, a part of the body is placed in the same part and confuses the doctor.

The motivation of CMF detection (CMFD) of medical image is to detect manipulated images. Image forgery detection is very important, and researchers are focused on CMFD and have achieved excellent results. According to the studies, CMF can be classified into two general methods[7,11] based on block and keypoint.

Block and keypoint methods

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 and Chantaf has been introduced.[12] The PCA method is used to describe blocks of low complexity. Another important method introduced in the past by Lee (2015) is the extracted uniformly positioned binary patterns (BPs) that were based on circular blocks.[13] The block method considered in this article is discrete cosine transformation (DCT), introduced by Vega *et al*. in 2018.[14,15]

Keypoints are extracted from the image in methods that use a keypoint. The most important method among keypoint methods is the scale variable property conversion (scale-invariant feature transform [SIFT]) method,[16] which many studies use as a suitable descriptive method for detecting forgery. Amerini, in 2011, detected CMF based on the SIFT feature, which has obtained very good results.[16,17] The SIFT method has been modified and improved in many studies. In Amiri *et al*., an optimal model of SIFT is introduced.[3]

One of the recently considered methods is evolutionary methods in optimizing the detection answers of fake copy-move images. Agarwal and Verma[18] used the emperor penguin optimization algorithm to optimize the selection of blocks. The results[15] show the superiority of the proposed method in selecting similar blocks over many block methods. Amiri *et al.*[3] used the SIFT optimization method, and Uma and Sathya[19] used the football game optimization method. The balance optimization method is one of the newly introduced evolutionary methods, which can work on images due to its agent-oriented structure. The article[20] is based on the forgery of public images available on the Internet, which has been done with the help of a bat evolution algorithm. The wavelet feature detection method and the bat evolution algorithm are used. The very important point of this article is that its results are not on the medical image database, and general images are used. The results of these two methods on medical images are different, and the present article has a much better answer.

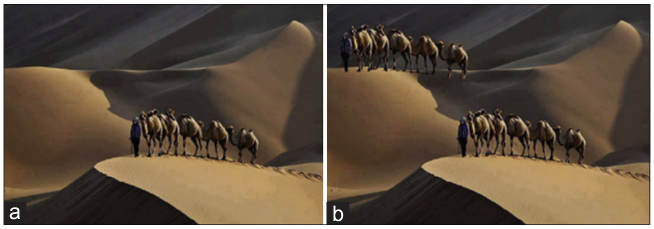

Figure 1: An example of image forgery

Equilibrium optimization

So far, many evolutionary algorithms[18,19] have been introduced. Evolutionary algorithms such as equilibrium optimization (EO) can solve various problems based on intelligent principles.[21] The mass balance equation is obtained according to the amount of mass entered into the system. The mass balance equation to the input equals the sum of the first and second output mass Figure 2.

Sometimes, it occurs in the accumulation system, which must maintain the stable energy equation and the state of general equilibrium. In the case of accumulation, the sides of the equation must be equal.[21]

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

According to Eq. 1, the mass production rate equals the number of changes in the input per second. In Eq. 1, C is mass per cubic meter, Q is the velocity, V is volume, and dc/dt indicates the volume change rate.[22]

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.[21]

Eq. 1 is a first-order differential equation showing the general mass equilibrium equation. In Eq. 1, the mass change over time equals the amount of mass entering.[22]

If there is no change in the system and Vdc/dt is 0, a steady state of equilibrium is achieved. A stable equilibrium is

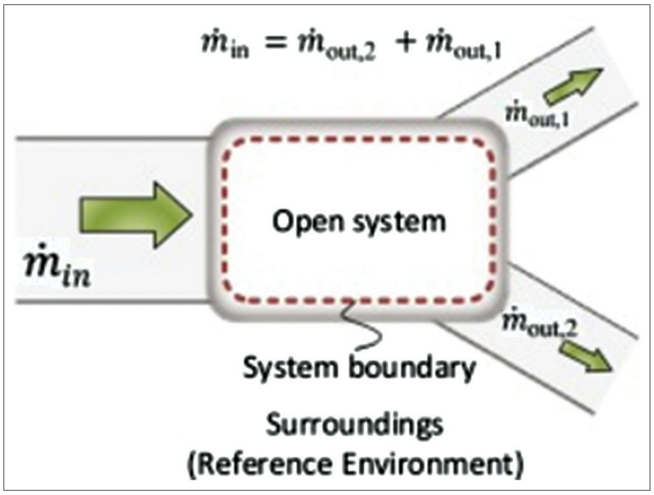

Figure 2: Input and output in the mass balance equation[21]

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.[21]

With the help of an evolutionary algorithm, this article introduces an optimal method for detecting forgery in an image. Section 2 presents a copy-move detection algorithm based on an EO algorithm (EOA). Section 3 presents the experiments, and Section 4 presents the Discussion.

Related work

Today, everything seen in digital medical images can be unreal due to the emergence of advanced systems and image editing software. It is easy to edit digital images without leaving a trace of manipulation, so detecting manipulation is difficult to see. Image falsification has become a major threat to information credibility. Forensic image analysis aims to detect and locate image forgery using multiple clues that allow it to determine whether or not an image is authentic. CMF is the most challenging among the digital image forgery types.

An adaptive forgery detection approach was proposed in 2014.[23] This research used the standard deviation to evaluate the energy of the blocks' frequency coefficients. Jaberi *et al*.[24] discussed the keypoints and used the Kd-tree feature for similarity matching. Liu *et al*.[2] proposed a method that relies on the gradient-oriented histogram.

Among the CMFD methods, keyword-based methods are very popular. In these methods, the keypoints of the image are selected. The situation where two keypoints in the image have the same feature is called forgery. The study[8] in 2018 presents a fast SIFT-based method for detecting CMF. The method introduced in this article is SIFT feature selection along with fuzzy clustering. In the study[25] in 2018, image change detection was done using the JPEG compression model. The main problem with JPEG compression is that pixels have different values after being transferred to a different position and stored in JPEG format. This method has provided low detection ability in cases such as rotated and uncompressed images. In the study[26] in 2019, the use of local fixed symmetry features to detect image forgery is presented. The proposed scheme can detect multiple copy-move forgeries but has obtained inappropriate results in noisy images. In the 2019 study[27] on CMF using SIFT, fixed points and growth strategy are imaged. The proposed scheme effectively identifies copy-move duplicated regions.

Another method of detecting forgery is detecting fake blocks. Most of the studies in this field have used the discrete wavelet transform (DWT) method. In the study[8] in 2018, a suitable technique to detect forgery and fake displacement in digital images is presented through stationary wavelet and discrete cosine transform. This technique extracts features based on stationary wavelet transform to reveal the forgery of digital images. To evaluate the proposed method, two standard datasets, namely CoMoFoD and UCID, have been used for testing. Forgery detection methods are used in forensic applications. This method has low detection in compressed images. The study[28] published in 2015 introduces a CMFD model based on DCT blocking. In this article, a method for authentication of images is presented. The proposed method detects copy-move changes in an image by using a discrete cosine transform. However, the discrete cosine method has a high computational cost. To reduce the computational complexity, Huang *et al*.[29] truncate the feature vector by using a constant to reduce the feature dimensions and present a scheme to check the similarity between feature vectors. Mahmood *et al*.[30] used RBF to reduce the dimensionality of the feature vector, which improved the efficiency of the feature-matching process.

In current studies, combined methods are of interest. The use of deep learning methods, optimization algorithms, and statistical models, along with general detection methods, has increased the accuracy of counterfeit detection. Popescu and Farid[31] have focused on detecting duplicate image regions based on PCA. In the study[32] in 2018, forgery detection was done using binary separation features. This method is a combination of common methods based on block and keyword. The results of the experiments show that the proposed method has better results in terms of accuracy, recall, and F1 criterion. A study[33] in 2019 detected counterfeiting based on density-based clustering. The proposed method has provided a suitable solution in various challenging conditions but has obtained inappropriate solutions on compressed images. The method[34] is fast object recognition with the help of deep learning. This article presents a deep architecture for compressed images for better object detection. In the study[35] in 2019, image segmentation based on the gray wolf optimization algorithm is presented. The study[19] in 2022 studied the optimization of CMFD with the help of a football game optimization algorithm. In the article[18] published in 2021, a forgery detection method is based on superpixel areas. The innovation of this article is the use of the emperor penguin optimization algorithm in optimizing the selection areas.

Subjects and Methods

This section proposes CMFD using an EOA (CMFDEOA) Figure 3. Evolutionary algorithms in the first stage should be initialized with a random amount.

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 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 4a, it should be converted into a grayscale image Figure 4b using the following formula.

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

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, a type of conversion in the frequency domain.

The DCT matrix must be converted to a suitable matrix using a feature discovery method. A DWT is a matrix that can achieve the appropriate EOA property. The DCT matrix is converted to a wavelet matrix using the two-dimensional (2D) wavelet (DWT) function.[36] This matrix has four bands: low-low (LL), low-high (LH), high-low (HL), and high-high (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]) (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 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 ≤ i ≤ (M − b + 1) and 1 ≤ j ≤ (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, we 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[21] has random input segments. This section selects three random blocks 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).[20]

$$fitness\left(m.n\right)=\sum_{x^1=1}^{x^2}\sum_{y^1=1}^{y^2}\left(\left|I_1\left(x^1+m-1.y^1+n-1\right)-I_2(x^1.y^1)\right|\right) \tag{4}$$

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

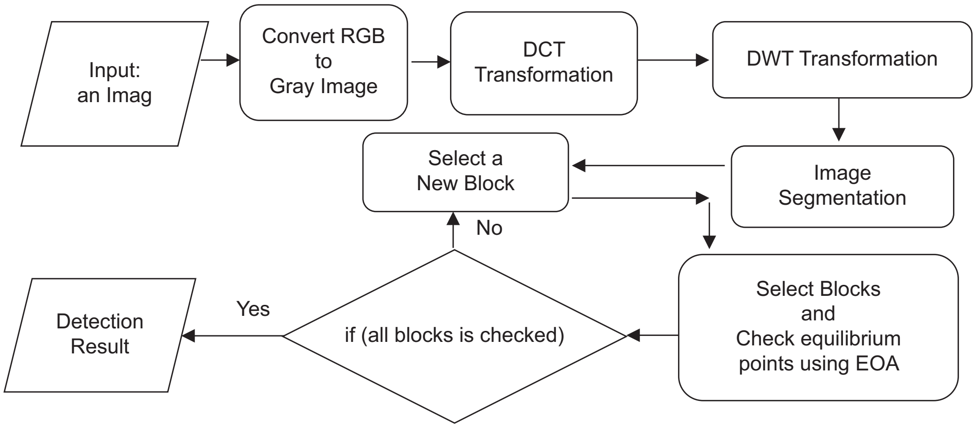

Figure 3: CMFD with EOA, DWT, and DCT. CMFD: Copy-move forgery detection, DWT: Discrete wavelet transform, DCT: Discrete cosine transform, RGB: Red, Green, and Blue

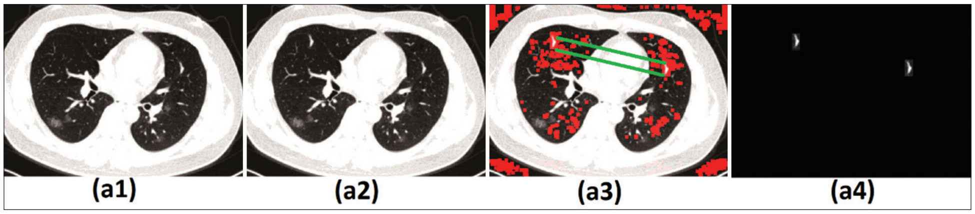

Figure 4: Copy-move with EOM, DWT, and DCT. (a1) RGB, (a2) Grayscale, (a3) Matching, (a4) Detection of forgery. EOM: Equilibrium Optimization Matching, DWT: Discrete wavelet transform, DCT: Discrete cosine transform, RGB: Red, Green, and Blue

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.[20]

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 that 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. Compared to similar block models, the innovation obtained in this model is the selection of better formats and more sensitivity to 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.

Results

Database

The proposed CMFDEOA method is applied to 300 medical images. This dataset, available on https://www.ctisus.com/teachingfiles/chest/285194 website, contains 200 fake and 100 original images.

Fake images are synthetically formed using image editing tools to study the performance of the developed method.[10] Results are given for simple forged, rotating forged (5°, 10°, and 15°), and noisy forged images.

Figure 6 shows applying the proposed model to the existing database. The images of the first group are fake, and the second group detected images. Based on the results, the proposed method can detect fake parts of the images to a large extent and return the appropriate blocks.

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 and pixel levels. 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.

```
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. EOA: Equilibrium optimization algorithm, DWT: Discrete wavelet transform, DCT: Discrete cosine transform

In general, 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:[37]

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

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

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

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.

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.

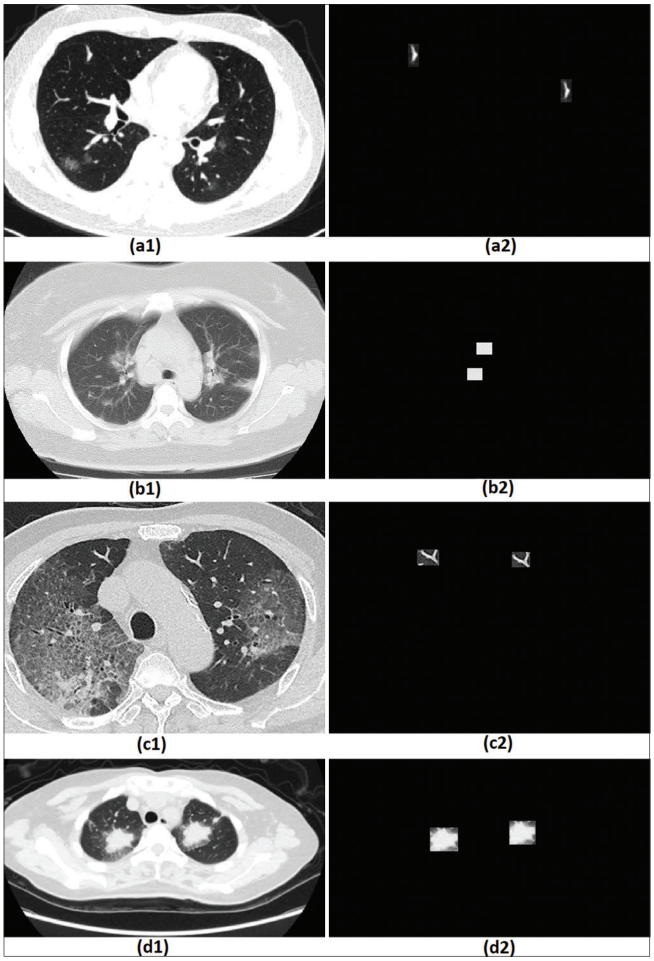

Figure 6: The proposed method in the CMFD on the dataset. (a1, b1, c1, and d1) Main forged image and (a2, b2, c2, and d2) detected forgery region. CMFD: Copy-move forgery detection

The results of comparing the CMFDEOA algorithm with other methods studied on the dataset are given here. The database contains 300 images without forgery, forged images, rotation, and noise. The results are given in Table 1 for the two sections of images without forgery and images with forgery.

Comparison results and analysis

Table 1 shows the performance differences in the types of fake images in the database. The accuracy of detecting nonfake images is excellent. In contrast, it detects fake images with about 95%, which is a very good result. In rotated images, the accuracy is lower as the number of rotations increases. The existing noise images were created using a Gaussian function with a factor of 0.1. The proposed method's image forgery detection accuracy in Gaussian noise images is about 90%.

Table 2 shows the high-performance accuracy of the proposed method on the existing database. In addition to precision, there is excellence in the recall and F1 criteria. The results in Table 2 show that the introduced method (CMFDEOA) has the highest F1 (98.47%), followed by 96.91% in suggested MEVA and GBO-based method (SMGM) and 90.11% in classical SURF-based method (CSM) for the forged images. The results in Table 2 show an improvement of about 2%. Therefore, the proposed method has improved the results in forgery-detecting areas. The most important feature of this method is the selection of optimal blocks that other methods have not been able to detect.

Discussion

Block-based or key-based methods can detect image forgery. The method introduced is an EOA-based algorithm called CMFDEOA, which focuses on detecting CMF. Experimental analysis of the proposed method showed its effectiveness in detecting CMF. This method offers higher precision. The precision in Tables 1 and 2 is better

Table 1: Comparison of the proposed method in the data set

Actual class	Rate of precision (%)	Rate of recall (%)	Rate of F1 (%)
Original	100	100	100
Simple forgery images	100	95.0	97.43
Forgery images with rotation (5°)	94.0	94.0	94.0
Forgery images with rotation (10°)	90.5	90.0	90.24
Forgery images with rotation (15°)	89.0	90.0	89.49
Forgery images with noise	90.5	89.0	89.74

Table 2: Comparison of the proposed method and other methods

Algorithms	Rate of precision (%)	Rate of recall (%)	Rate of F1 (%)
SMGM[10]			
Original image	100	100	100
Forged image	100	94.0	96.91
CSM[10]			
Original image	100	100	100
Forged image	100	82.0	90.11
BAM[20]			
Original image	100	99.0	99.49
Forged image	86.5	90.5	88.45
MROGH[38]			
Original image	-	-	-
Forged image	93.6	91.7	92.6
Gabor filter[39]			
Original image	-	-	-
Forged image	83.3	90.9	86.92
SIFT-ACO[40]			
Original image	-	-	-
Forged image	90.0	89.63	89.81
Proposed method			
Original image	100	100	100
Forged image	100	97.0	98.47

SMGM: Suggested MEVA and GBO-based method, CSM: classical SURF-based method, BAM: bat algorithm with mutation, MROGH: Multiple Region of Gradient Hog feature, SIFT-ACO: scale-invariant feature transform-Ant Colony Optimization

than other algorithms. Tables 1 and 2 also show that the proposed CMF method obtains forged points with 98.47% in the F1 for the medical image dataset. It is possible to improve the accuracy of local point detection and expand the detection area in the future. Fraud detection in medical images can be investigated based on forgery by the operator or transmission interference by the Internet.

Conclusion

Medical data is always at risk of data loss. Due to the increasing development of image editing software, it is possible to forge medical images. If a medical image is intentionally altered, it increases the possibility of physician error. Therefore, detecting forgery in these images is very important. The introduced method is an optimal method based on DCT and DWT. This method has been able to detect forgery image in all kinds of medical images.

Financial support and sponsorship

Nil.

Conflicts of interest

There are no conflicts of interest.

References

1. Abd Warif NB, Wahab AW, Idris MY, Ramli R, Salleh R, Shamshirband S, *et al*. Copy-move forgery detection: Survey, challenges and future directions. J Netw Comput Appl 2016;75:259-78.
2. Liu K, Lu W, Lin C, Huang X, Liu X, Yeung Y, *et al*. Copy move forgery detection based on keypoint and patch match. Multimed Tools Appl 2019;78:31387-413.
3. Amiri E, Mosallanejad A, Sheikhahmadi A. Copy-move forgery detection by an optimal keypoint on SIFT (OKSIFT) method. J Comput Robot 2021;14:11-9.
4. Tahaoğlu G, ULUTAS G. Copy-move forgery detection and localization with hybrid neural network approach. Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi 2022;28:748-60.
5. Deep Kaur C, Kanwal N. An analysis of image forgery detection techniques. Stat Optim Inf Comput 2019;7:486-500.
6. Roy A, Dixit R, Naskar R, Chakraborty RS, Roy A, Dixit R, *et al*. Copy-Move Forgery Detection in Digital Images—Survey and Accuracy Estimation Metrics. Digital Image Forensics: Theory and Implementation 2020:27-56.
7. Songpon T, Uehara T. Copy-move forgery detection: A state-of-the-art technical review and analysis. IEEE Access 2019;7:40550-68.
8. sAlberry HA, Hegazy AA, Salama GI. A fast SIFT based method for copy move forgery detection. Future Comput Inf J 2018;3:159-65.
9. Sharma S, Ghanekar U. A rotationally invariant texture descriptor to detect copy move forgery in medical images. In: 2015 IEEE International Conference on Computational Intelligence & Communication Technology. IEEE; 2015. p. 795-8.
10. Suganya D, Thirunadana Sikamani K, Sasikala J. Copy-move forgery detection of medical images using golden ball optimization. International Journal of Computers and Applications 2022;44:729-37.
11. Rashidi S, Fallah A, Towhidkhah F. Authentication based on pole-zero models of signature velocity. J Med Signals Sens 2013;3:195-208.
12. Hilal A, Chantaf S. Uncovering copy – Move traces using principal component analysis, discrete cosine transform and Gabor filter. Anal Integr Circuits Signal Process 2018;96:283-91.
13. Lee JC. Copy-move image forgery detection based on Gabor magnitude. J Visual Commun Image Represent 2015;31;320-34.
14. Vega EA, Fernández EG, Orozco AL, Villalba LJ. Copy-move forgery detection technique based on discrete cosine transform blocks features. Neural Comput Appl 2021;33:4713-27.
15. Azarianpour S, Sadri AR. A generalized ghost detection and segmentation method for double-joint photographic Experts Group compression. J Med Signals Sens 2019;9:211-20.
16. 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 Process Image Commun 2013;28:659-69.
17. 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 Trans Inf Forensics Secur 2011;6:1099-110.
18. Agarwal R, Verma OP. Robust copy-move forgery detection using modified superpixel based FCM clustering with emperor penguin optimization and block feature matching. Evol Syst 2022;13:27-41.
19. Uma S, Sathya PD. Copy-move forgery detection of digital

images using football game optimization. Aust J Forensic Sci 2022;54:258-79.

20. Amiri E, Mosallanejad A, Sheikhahmadi A. Copy-move forgery detection using a bat algorithm with mutation. Int J Nonlinear Anal Appl 2021;12:1947-55.
21. Faramarzi A, Heidarinejad M, Stephens B, Mirjalili S. Equilibrium optimizer: A novel optimization algorithm. Knowledge Based Syst 2020;191:105190.
22. Shaheen AM, Elsayed AM, El-Sehiemy RA, Abdelaziz AY. Equilibrium optimization algorithm for network reconfiguration and distributed generation allocation in power systems. Appl Soft Comput 2021;98:106867.
23. Zandi M, Mahmoudi-Aznaveh A, Mansouri A. Adaptive matching for copy-move forgery detection. In: 2014 IEEE International Workshop on Information Forensics and Security (WIFS). IEEE; 2014. p. 119-24.
24. Jaberi M, Bebis G, Hussain M, Muhammad G. Accurate and robust localization of duplicated region in copy – Move image forgery. Mach Vis Appl 2014;25:451-75.
25. Novozámský A, Šorel M. Detection of copy-move image modification using JPEG compression model. Forensic Sci Int 2018;283:47-57.
26. Vaishnavi D, Subashini TS. Application of local invariant symmetry features to detect and localize image copy move forgeries. J Inf Secur Appl 2019;44:23-31.
27. Chen CC, Lu WY, Chou CH. Rotational copy-move forgery detection using SIFT and region growing strategies. Multimedia Tools and Applications 2019;78:18293-308.
28. Kumar S, Desai JV, Mukherjee S.Copy move forgery detection in contrast variant environment using binary DCT vectors. Int J Image Graph Signal Process 2015;7:38.
29. Huang Y, Lu W, Sun W, Long D. Improved DCT-based detection of copy-move forgery in images. Forensic Sci Int 2011;206:178-84.
30. Mahmood T, Nawaz T, Irtaza A, Ashraf R, Shah M, Mahmood MT. "Copy-Move Forgery Detection Technique for Forensic Analysis in Digital Images", Mathematical Problems in Engineering, vol. 2016, Article ID 8713202, 13 pages, 2016.
31. Popescu AC, Farid H. Exposing Digital Forgeries by Detecting Duplicated Image Regions; 2004.
32. Raju PM, Nair MS. Copy-move forgery detection using binary discriminant features. Journal of King Saud University-Computer and Information Sciences 2022;34:165-78.
33. Hegazi A, Taha A, Selim MM. An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal. Journal of King Saud University-Computer and Information Sciences 2021;33:1055-63.
34. Deguerre B, Chatelain C, Gasso G. Fast object detection in compressed jpeg images. In2019 ieee intelligent transportation systems conference (itsc) 2019. (pp. 333-338). IEEE.
35. Yao X, Li Z, Liu L, Cheng X. Multi-threshold image segmentation based on improved grey wolf optimization algorithm. In: IOP Conference Series: Earth and Environmental Science. Vol. 252. Russian Federation: IOP Publishing; 2019. p. 042105.
36. Yildiz K, Buldu A. Wavelet transform and principal component analysis in fabric defect detection and classification. Pamukkale Univ Muh Bilim Derg 2017;23:622-7.
37. Lyu Q, Luo J, Liu K, Yin X, Liu J, Lu W. Copy move forgery detection based on double matching. J Vis Commun Image Represent 2021;76:103057.
38. Yu L, Han Q, Niu X. Copy-rotation-move forgery detection using the MROGH descriptor. 2014 IEEE International Conference on Cloud Engineering; 2014.
39. Yohannan R, Manuel M. Detection of copy-move forgery based on Gabor filter. 2016 IEEE International Conference on Engineering and Technology (ICETECH); 2016.
40. Mehak TG. Improve copy move forgery image classification by optimization technique. Int. J. Adv. Eng. Res 2017;13:19-29.