An Enhanced Hybrid Method based on Local and Frequency Feature Extraction for Image Copy Move Forgery Detection

Shirin Nayerdinzadeh[1], Mohammad Reza Yousefi[2*]
1- Department of Computer Engineering, Najafabad Branch, Islamic Azad University, Najafabad, Iran.
Email: sh.nayerdin@gmail.com
2- Department of Electrical Engineering, Najafabad Branch, Islamic Azad University, Najafabad, Iran.
Email: mr-yousefi@iaun.ac.ir (Corresponding author)

Received: September 2020 Revised: November 2020 Accepted: March 2021

ABSTRACT:
Today, due to the advent of the powerful photo editing software packages, it has become relatively easy to create forgery images. Recognizing the correctness of digital images becomes important when those images are used as evidence in legal, forensic, industrial, and military applications. One of the most common ways to forge images is copy move forgery, in which one part of the image is copied and pasted in another part of the same image. So far, various methods have been proposed for detecting copy move forgery, but these methods are not able to detect copy move forgery with different challenges of noise, rotation, scale, and detection of symmetrical images with high accuracy. In this paper, an enhanced hybrid method based on local and frequency feature extraction is presented for image copy move forgery detection, which has a very high resistance to above challenges, both individually and simultaneously and has provided good identification accuracy. In this method, the combination of Discrete Wavelet Transform, Scale Invariant Feature Transform and Local Binary Pattern are used simultaneously. The forged area is chosen in such a way that at least both methods used in this proposed method have consensus about the forgery of that area. Various experiments and analyses on the MICC database show that the proposed methods, despite the above challenges, have reached the accuracy of 98.81% both separately and simultaneously, which shows significant improvement compared to other methods used in this field.

KEYWORDS: Copy Move Forgery Detection, Scale Invariant Feature Transform, Discrete Wavelet Transform, Local Binary Pattern, Symmetrical Images.

1. INTRODUCTION

One of the most common ways for forging images is copy move forgery, in which one part of the image is copied and then pasted in another part of the same image. Many detection copies move forgery methods are capable of detection if no change has been made to the copied area prior to paste. Most people apply a series of geometric transformations to the copied area to make the copied area match the around area and make the image look more natural. Since in some cases it is necessary to confirm the truth of an image (military, criminal and social applications), many researchers have sought to find a way to examine the image and recognize its truth. The result of researches has been creation of many software and methods for forgery detection, which are based on image processing algorithms. A good forgery detection method must be resistant to different geometric changes and transformations. Fig. 1 shows a sample of copy move forgery.

So far, various methods have been designed to counter images forgery, which are divided into active and passive groups. Most active methods are marked based on digital signatures, which require data pre-processing, which has its own complexities. Passive methods for image analysis do not use previous information. Today, more passive methods are used, and there are broader and used more generally for detection of image forgery. The following are the works in which a variety of passive methods are used. Fig. 2 displays the classification of detection of image forgery systems.

Huang et al.[1], proposed an improved Discrete Cosine Transform (DCT)-based detection of copy-move forgery in images. Experimental results showed that the presented method is resistant to JPEG compression, blurring.

Paper type: Research paper
DOI: https://doi.org/10.52547/mjee.15.3.69
How to cite this paper: Sh. Nayerdinzadeh, M. R. Yousefi, **"An Enhanced Hybrid Method based on Local and Frequency Feature Extraction for Image Copy Move Forgery Detection"**, *Majlesi Journal of Electrical Engineering*, Vol. 15, No. 3, pp. 69-80, 2021.

(a) (b)

Fig. 1. (a) original image (b) forged image.

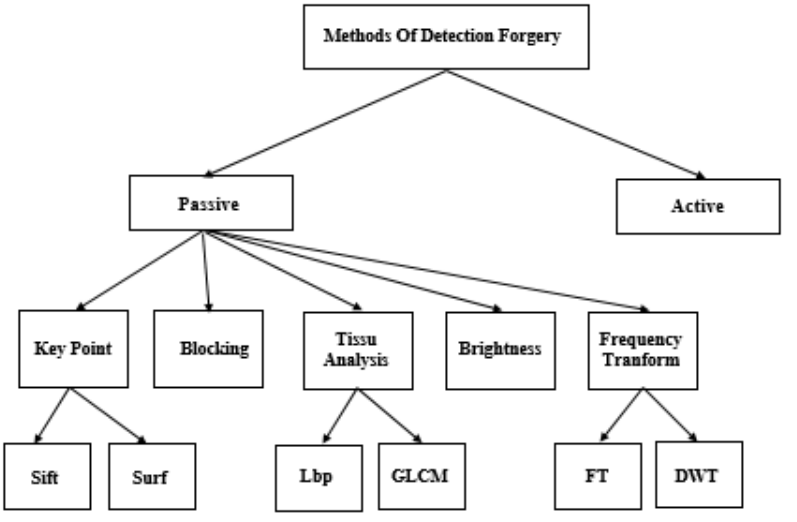


Fig. 2. Classification of detection image forgery systems.

Also, Gaussian noise. Davarzani et al.[2], provided an efficient method for copy-move forgery detection using Multiresolution Local Binary Patterns (MLBP)

In this method, the algorithm of Random Sampling Consensus (RANSAC) was used to eliminate false matches. Experimental results showed that the presented method was able to precisely detect duplicated regions even after distortions such as rotation, scaling, JPEG compression, blurring, and noise addition. Lynch et al.[3], presented an efficient present block algorithm for detecting copy-move forgery and identifying the duplicated regions in an image. It was found that the expanding block algorithm was able to detect specific types of forgeries, such as JPEG compression, the effect of Gaussian blurring, or when the duplicated region was made lighter or darker. Jen et al.[4], presented an effective method for detecting duplicated regions based on the Histogram of Gabor Magnitude (HOGB). The results showed that the proposed method is resistant well in the presence of rotation, scaling, JPEG compression, and blurring. Silva et al.[5], proposed a method of detection copy move forgery using scale independent features. This provides a new approach for detecting copy move forgery based on multi-scale analysis and voting processes from a digital image. This method is able to deal with rotation, resize, and compression simultaneously. Ashwini et al.[6], proposed a method that uses a content-based image retrieval feature extraction technique for detection of forgery. In this method, the Auto Color Correlogram (ACC) algorithm was used. Experimental results revealed that the presented method is resistant well in the presence of different attacks such as scaling, translation, and rotation. Bi et al.[7], offered a Multi-Level Dense Descriptor (MLDD) extraction method and a Hierarchical Feature Matching method to detect copy–move forgery in digital images. Experimental results showed that the presented method functioned well in the presence of challenges of JPEG compression and noise. Yang et al.[8], proposed a copy-move forgery detection method based on hybrid features. In this method, a strong detector and an adaptation algorithm were used to

deal with copy move. The research showed that the proposed method can detect duplicated areas after changes such as rotation, scale, JPEG compression, and noise. Ahmed et al.[9], provided an effective algorithm to indicate Copy Move Forgery in digital image. In this method, The Scale Invariant Feature Transform (SIFT) and Fuzzy C-means (FCM) for clustering are utilized in the presented algorithm. Research shows that the proposed method can detect duplicated areas after changes such as rotation and scale. Pun et al.[10], presented a two-stage localization for Copy-Move Forgery Detection (CMFD). In this method, Discrete Analytic Fourier–Mellin Transform (DAFMT) is used. Experimental results show that the proposed method is resistant to Gaussian noise, JPEG compression, rotation, and scale challenges. Bi et al.[11], proposed an algorithm that could accurately and robustly detect regions of copy-move forgery. Experimental results showed that the proposed method is resistant to noise, JPEG compression, rotation, and scale challenges. Mahmood et al.[12], presented the method of copy move forgery detection in digital images through Stationary Wavelet Transform (SWT) and Discrete Cosine Transform (DCT). Experimental results showed that the presented method was well resistant in the presence of different attacks such as blurring, JPEG compression, brightness change, and color reduction. Soni et al.[13], presented an enhancement of block-based copy-move forgery detection using hybrid local features extraction. In this method, the Speed up Robust Feature algorithm (SURF) was used. The results showed that the proposed method was resistant well in the presence of different geometric attacks such as rotation, scaling, and composition of these attacks. Hegazi et al.[14], proposed an improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal. In this method, the Scale Invariant Feature Transform (SIFT) was used. Experimental results revealed that the method functioned well in the existence of various attacks such as scaling, rotation, JPEG compression, and Gaussian noise. Zhong et al. [15], provided Two-pass hashing feature representation and searching method for copy-move forgery detection. In this method, the Two-pass hashing searching algorithm was used. The results showed that the proposed method is resistant well in the presence of different attacks such as rotation, scaling, JPEG compression, and noise. Meena et al.[16], presented a copy-move image forgery detection technique based on Tetrolet transform. The results indicated that the proposed method is resistant to rotation, scaling, and JPEG compression.

2. REVIEW OF THE LBL ALGORITHM, SIFT ALGORITHM AND DWT

In the proposed method, we have used 3 algorithms simultaneously, including Local Binary Pattern, Scale Invariant Feature Transform algorithm, and Discrete Wavelet Transform. In the following, we will explain each of the algorithms.

A. Local Binary Pattern algorithm (LBP)

This algorithm is a local feature extraction and one of the most powerful feature extraction algorithms in car vision. This operator produces a binary number of each pixel according to the label of the neighboring 3×3 pixels. Tags are obtained based on the threshold the value of neighboring pixels with the value of the central pixel. In this way, for pixels with a larger value or equal to the value of the central pixel, label 1 is assigned, while for pixels with values smaller than the value of the central pixel, label 0 is placed. The labels are then rotated to from an 8-bit number. This operation is shown in Fig. 3[2].

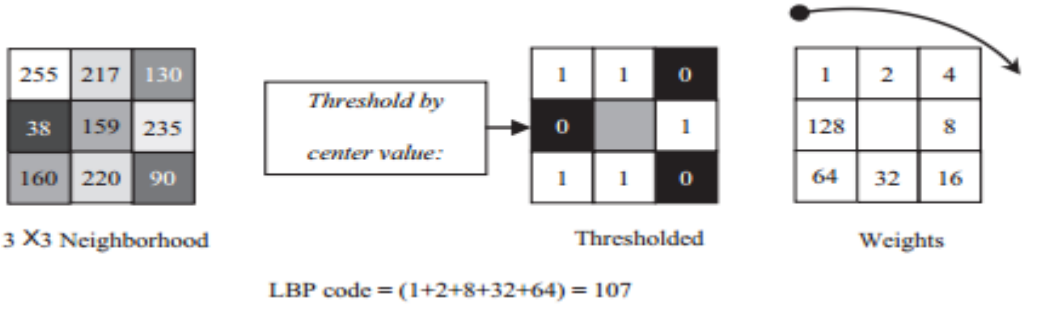
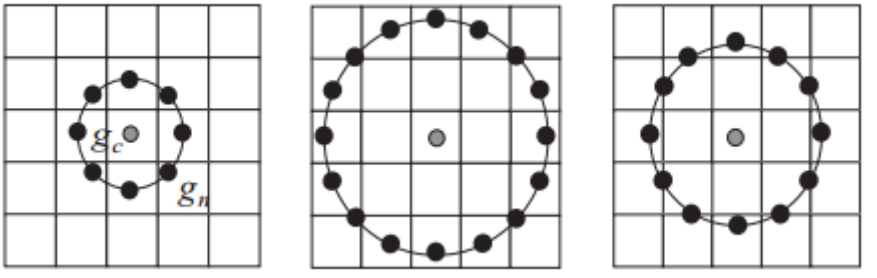


Fig. 3. Operation of local binary patterns.

The LBP operators' limit on the small neighbor base is 3×3, which makes it impossible to control large scale images. For this purpose, the neighborhood size is 2, which is shown as a circle with a radius of pixel R on the pixel P. This operator is represented as LBP and can produce a maximum of 2^P different values, according to the 2^P binary pattern generated by the pixel P on

the neighborhood radius. Fig. 4 [2] displays how to select neighboring pixels in this type of local binary pattern for three different radius After tagging an image by the LBP operator, the histogram of the tags is defined as Eq. 1[2]:
.



P=8,R=1 P=16,R=2 P=12,R=1.5

Fig. 4. LBP operator with different radius and number of neighbors.

$$H(t)=\left(\frac{1}{M\times N}\right)\sum_{i=1}^{m}\sum_{j=1}^{n} f\left(LBP_{P,R}(i,j),t\right),t\in[0,T],$$
$$f(x,y)=\begin{cases}1, & x=y\\ 0, & otherwise\end{cases} \quad (1)$$

Where, T is the maximal LBP pattern value.

B. Scale Invariant Feature Transform algorithm (SIFT)

The algorithm first finds the key points and assigns 128 attributes to each. The key points of these algorithms are usually the important points of the image objects. There are 4 steps in this algorithm:

1. Building a scale space and finding local extremes: it first blurs the original image with smoothing cow filters to varying degrees. Then, it halves the size of the image and makes the faded versions the same size as before. It reduces each image created from the image above and differentiates the Gaussians. The process of Gaussians difference is shown in Fig. 5 [17].

At the intermediate levels, each pixel of Gaussian difference image is compared to 8 pixels of its neighbor, 9 pixels of the neighboring image of the upper gossip difference, and 9 pixels of the neighboring image of the lower Gaussian difference (26 neighbors). In Fig. 6 [17], each point, such as X, is compared to its 26 neighboring neighbors.

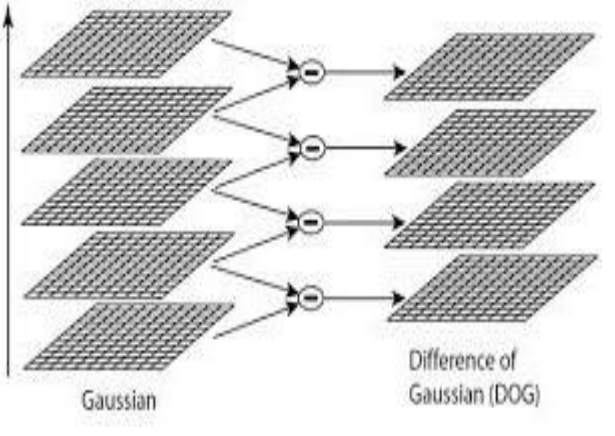


Fig. 5. Difference of Gaussian.

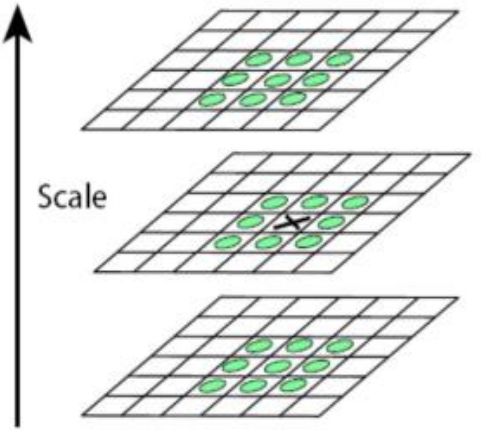


Fig. 6. Comparison of any point in Gaussian difference with his neighbors.

2. Finding the location of the key points: candidates that are on the edge, or have little difference with their neighbors, are the first to speak. The exact location and scale of each key point are then estimated. In steps 1 and 2, the main points of the image are obtained.
3. A window is placed around each key point such that the key point itself is in the center. Then, the direction and size of the gradient of all points in this window are obtained. Finally, the angle whose total size is greater than the total block is assigned to that key point.
4. Extracting features: first, the origin of the coordinates is rotated by the angle of the key points and scaled to the extent that the properties obtained are independent of the rotation and size. Then, as in the previous step, it considers a 16×16 window on any key point. As shown in Fig. 7 [18], this window is divided into 4×4 squares. In each of these squares, calculating the gradient and makes a histogram from the angle of the gradient. Every 45 degrees, a column will appear in the corresponding histogram. In other words, angles 0 to 44 are in the first column, 45 to 89 are in the second column, and so on. That is, the histogram has 8 columns. So, a total of 128 bin values are available.

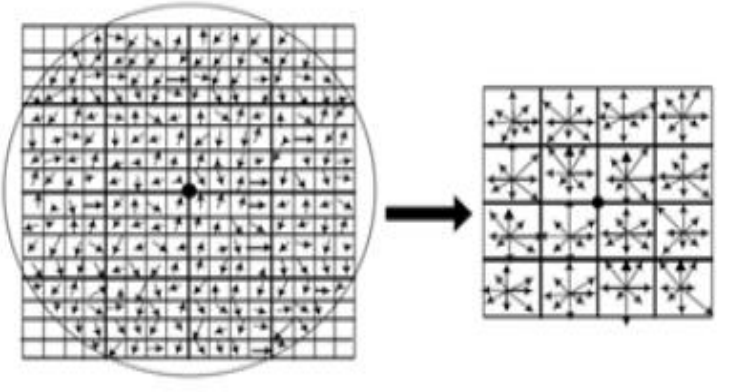


Fig. 7. Extraction of the characteristics of each key point based on the surrounding areas.

C. Discrete Wavelet Transform (DWT)

Wavelet is one of the frequency domain transformers that provides a time-frequency display of the image and offers a multi-spiral design to display the image for different resolutions using different commands. The image is broken down into four sub-bands LL, LH, HL, and HH. The LL sub band is low frequency sub-band, HL and LH are intermediate frequency sub-bands, and HH is high frequency sub-band. To obtain higher levels of decomposition, wavelet transform is applied to low frequency sub-bands. To extract the feature, a two-stage violet conversion is applied by discrete wavelet transform on each 8×8 image block. This process divides each block into 7 sub-blocks. Figs. 8 [19] and 9 [20] depict a block of two-stage discrete wavelet transform.

Fig. 8. Block view of two stage violet sub-bands on 8×8 block.

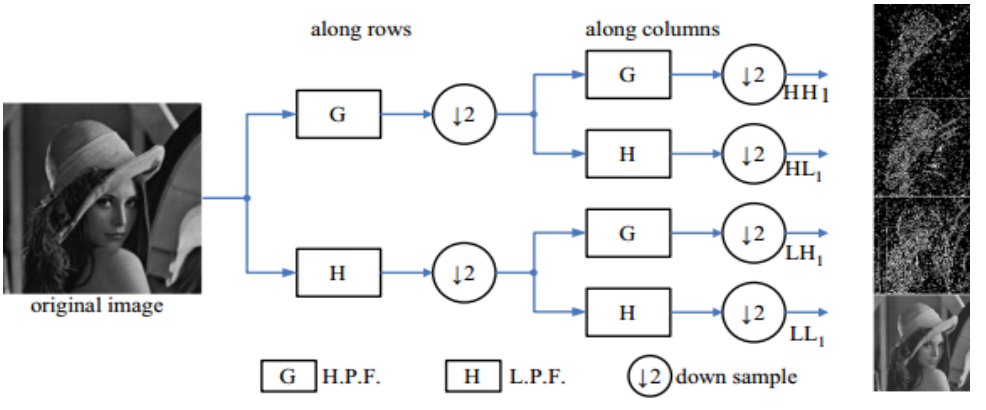


Fig. 9. Flows of the DWT image decomposition.

The DWT function is obtained from the following eq.2 [21]:

$$W_{m,n} = \left\langle f(t), \varphi_{m,n}(t) \right\rangle = a_0^{\frac{m}{2}} \int f(t)\varphi(a_0^m(t) - nb_0)dt \quad (2)$$

Where, $W_{m,n}$ is the wavelet coefficient and $\varphi_{m,n}$ is the mother wavelet [21].

3. PROPOSED MODEL

The copy move forgery detection system consists of six steps, which include pre-processing, area extraction, feature extraction, comparison of feature vector, extraction of suspicious area, and decision-making. The system input data include a digital image, and its output is a standardized mathematical model that contains the information required to use the system software. In recent years, various methods have been proposed due to the challenges in images in the field of copy move forgery detection, but they are not efficient as they cannot properly perform forgery detection with the presence of such high accuracy challenges. Thus, in this paper, to improve accuracy, symmetrical images and copied regions even after distortions such as rotation, scaling, and adding noise were detected. In this method, in order to increase the accuracy, three different methods of Discrete Wavelet Transform, Scale Invariant Feature Transform and Local Binary Pattern have been used simultaneously. The output percentage and final suspicious area are selected where at least both methods used in this method have the same opinion about the forgery of that area. Fig. 11 indicates the flowchart proposed in this paper.

A. Pre-processing

In the proposed method, the per-processing step, as shown in Fig. 10, first uses the Gaussian filter algorithm, which can normalize the pixel values of the image using the Gaussian filter and smooths the image relative to sharp points that exist. Then, using the histogram adjustment algorithm, the normalized light intensity values in the whole image have been normalized, as a result of which the accuracy of the algorithms can be enhanced in the next steps.

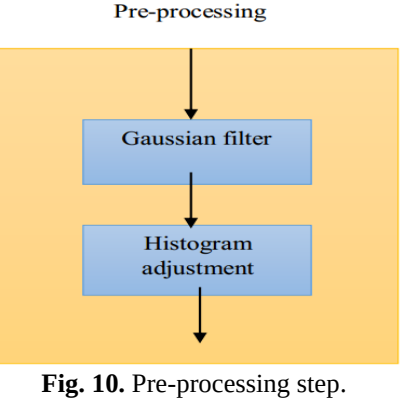


Fig. 10. Pre-processing step.

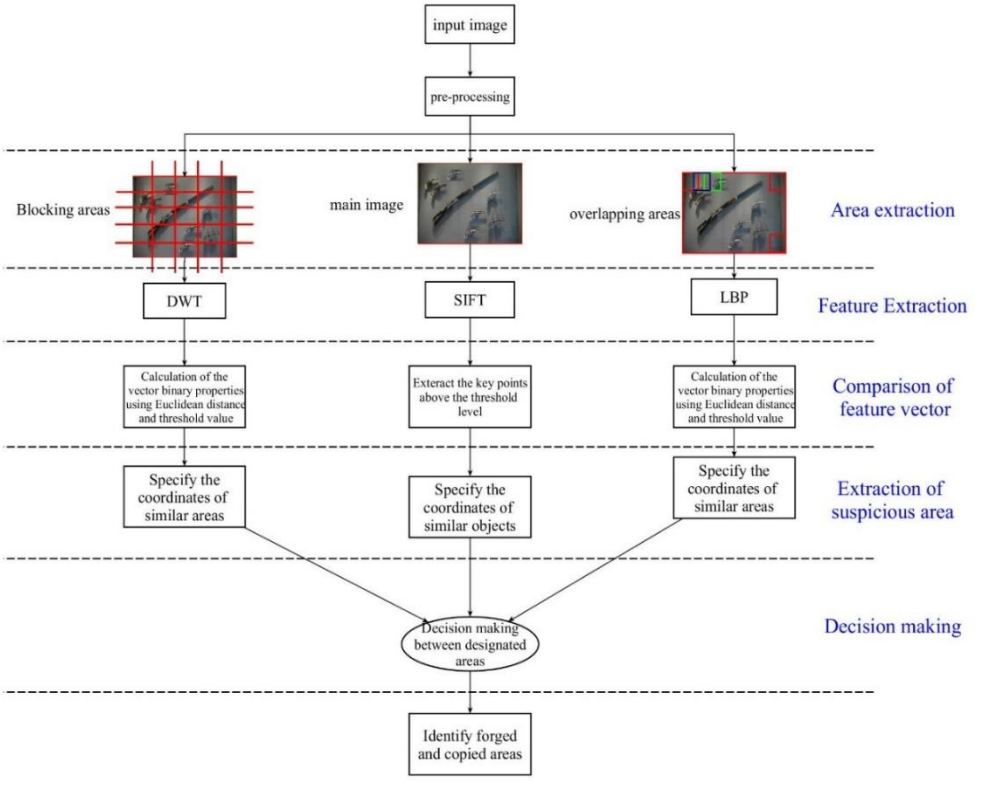


Fig. 11. Flowchart of the suggested method.

B. Area extraction

At this step, an image is divided into several areas. In this algorithm, three different types of functions are used, which include blocking areas, main image, and overlapping areas.

1. Blocking areas

The image is divided into $n \times n$ blocks and the properties of each block are extracted. Fig. 12 displays an example of a blocked image.

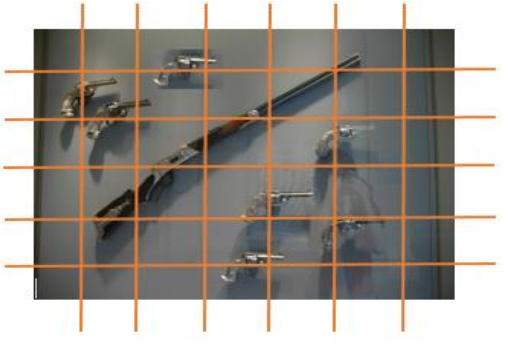


Fig. 12. Blocked image.

2. Overlapping areas

A $n \times n$ dimension cut is designed. This cut is given a shift of X in each step of survey and the features of each step are extracted. Fig. 13 reveals an example of an image with overlapping areas.

Fig. 13. Image with overlapping areas.

C. Feature Extraction

Once the image is separated into different areas, the feature is taken separately from each area; in the Local Binary Pattern algorithm and Discrete Wavelet Transform, the features of the image are extracted. It repeats this until the image areas are finished. Using the Scale Invariant Feature Transform algorithm, the key points of the image are extracted.

D. Comparison of feature vector

This step is performed based on the number of separated areas from the image. In each step, one of the areas is selected as the test areas and is compared with

the feature vector of all other areas. If the Euclidean distance of the two vectors is less than threshold level, that area is selected as the copied area, with this comparison made to the number of available areas. In the Scale Invariant Feature Transform algorithm, once the key points of the image are extracted, the key points in each part of the image are examined, and if the number of key points matched in the part of the image is greater than the threshold level, that area is considered as a copied area.

E. Extraction of suspicious area

At this step, all areas are compared and similar areas are selected as suspicious areas and in all three methods, suspicious areas have been extracted.

F. Decision-making

Once each of the three parallel procedures was answered, the output percentage and final suspicious area were selected; at least both methods used in this method have the same opinion about the forgery of that area.

4. EXPERIMENTAL RESULTS

In this paper, the MICC database, which contains 800 images with different color scales and sizes, has been used[9]; 200 images were used for parameter setting experiments and 600 images for final experiments. The images in this database include challenges such as noise, rotation, change of scale and images that have symmetrical parts. The following is an example of images in this database.

Fig. 14. Challenge of noising.

Fig. 15. Challenge of rotating.

Fig. 16. Challenge of resizing.

Fig. 17. Challenge of symmetrical images.

In this section, in order to increase the efficiency of the proposed method, the parameters used in it have been adjusted and evaluated. In this section, using the 200 images in the database and the algorithms used in this method, experiments have been performed to adjust the parameters as follows:

A. Adjustment of the number of surfaces parameters and function type in the Discrete Wavelet Transform

In this section, for better performance of the proposed method, the values of the number of surfaces and the type of function for discrete wavelet transform are tested. The purpose of these experiments is to improve the detection accuracy by performing various experiments as shown in Tables 1 and 2, the number of the surfaces selected for use in the final experiments is 3 and the function is Daubechies, which has the best performance. Their detection accuracy is 91.70% and 92.83%, respectively.

Table 1. The number of the surfaces in Discrete Wavelet Transform.

Number of the surfaces	Identification accuracy (%)
1	90.42
2	88.67
3	**91.70**

Table 2. The function in Discrete Wavelet Transform.

Function	Identification accuracy (%)
Haar	92.36
Daubechies	**92.83**
Symlets	87.93
Gaussian	90.63
Complex Gaussian	90.42

B. Adjustment of the sigma parameter in the Scale Invariant Feature Transform

In this section, the value of sigma parameters in the Scale Invariant Feature Transform used to blur the image in this algorithm is tested. The purpose of these experiments is to improve the detection accuracy by performing various experiments as shown in Table 3, the best set of sigma parameter for the Scale Invariant Feature Transform is 3.5, which has the best performance. Their detection accuracy is 94.13%.

Table 3. The sigma parameter in the Scale Invariant Feature Transform.

The average value of sigma	Identification accuracy (%)
1.5	92.50
2.5	86.20
3.5	**94.13**
4.5	89.23

C. Adjustment of the radius of parameters and neighbors' number in the local binary pattern algorithm

In this section, the values of radius and neighbors number in the local binary algorithm are tested. The purpose of these experiments is to improve the detection accuracy by performing various experiments as shown in Tables 4 and 5, the radius selected for use in the final experiments is 1 and the number of neighbors is 8, which has performance best. Their detection accuracy is 93.18% and 91.46%, respectively.

Table 4. The radius in the local binary pattern algorithm.

Radius	Identification accuracy (%)
1	**93.18**
2	89.11
3	92.56

Table 5. The number of neighbors in the local binary pattern algorithm.

The number of neighbors	Identification accuracy (%)
4	86.13
8	**91.46**
16	88.57
24	91.14

D. Adjusting number of neighbors and the type of distance calculation in the nearest neighbor algorithm

In this section, the classification algorithm of nearest neighbor with the metrics of cosine distance, Euclidean and block city, as well as the number of selected neighbors have been evaluated. The proposed method of accuracy has been examined by considering each of criteria for measuring the mentioned distance. Finally, the criterion causing the highest accuracy was considered as the main parameter. As can be seen in Tables 6 and 7, the number of neighbors selected for use in the final experiments is 3 and the type of distance calculation is equal to Euclidean distance criterion, which has performed well.

Table 6. The performance of system upon changing the distance calculation criteria.

Distance criteria	Identification accuracy (%)
Cosine	95.13
Euclidean	**97.16**
block city	96.45

Table 7. The performance of system upon altering the parameter of neighborhood number.

K	Identification accuracy (%)
1	90.01
3	**97.66**
5	91.56
7	89.34
9	93.54

E. Adjusting the number of blocks in the blocked image

In this section, the number of blocks in the blocked image is tested. The purpose of these experiments is to improve the detection accuracy; after different experiments as shown in Table 8, the best value is 9×9, which has the best performance and its detection accuracy is 90.75%.

Table 8. Adjusting the number of blocks in the blocked image.

Number of blocks	Identification accuracy (%)
3×3	86.35
5×5	87.56
9×9	**90.75**
11×11	85.67

F. Adjusting the cutting dimension of parameters in the image with overlapping areas

In this section, the cut dimensions in the image with overlapping areas are tested. The purpose of these experiments is to improve the detection accuracy; after

performing several experiments as shown in Table 9, the best value is 9×9 which has the best performance and its detection accuracy is 91.54%.

Table 9. Adjustment of the cutting dimension of parameters in the image with overlapping areas.

Cutting dimensions	Identification accuracy (%)
3×3	84.87
5×5	84.43
9×9	**91.54**
11×11	89.16

5. DISCUSSION

In this study, MICC databases were used to evaluate the results, where there are 600 images with different challenges for the final experiments. Next, the proposed method is compared with the following methods:

- Speed Up Robust Feature algorithm[22]
- Scale Invariant Feature Transform algorithm[9]
- Stationary wavelet and discrete cosine transform[12]

The results of the proposed method performance based on independent variables as well as the results obtained of comparison with the methods mentioned above will be expressed further.

A. Comparison and evaluation of the proposed method performance with other methods mentioned when noising the copied area

One of the challenges in this area is reducing the proposed methods of efficiency; the higher the extent of noise in the image, the harder it is to identify the copied area. In this section, the proposed method of efficiency in dealing with noise challenge will be examined by adding salt and pepper noise images with different intensities. Then, their accuracy will be evaluated with the best methods available in this field. The experimental results of the proposed methods and other methods are shown in Table 10.

Table 10. Performance comparison of the proposed method for noise challenge in the copied area.

Noise / Method	Identification rate (%)			
	0.01	0.05	0.1	0.5
Speed Up Robust Feature algorithm	97.34	97.15	96.69	96.42
Scale Invariant Feature Transform algorithm	96.21	95.78	95.64	95.43
Stationary wavelet and discrete cosine transform	97.56	97.21	96.86	96.24
Suggested method	**98.65**	**98.34**	**97.87**	**96.59**

According to the values shown in Table 10, the higher noise intensity, the lower accuracy. Also, by comparing methods, it is clear that the accuracy of stationary wavelet transform is better than that of strong Speed up Robust Feature algorithm and the Scale Invariant Feature Transform algorithm. As a result, the proposed method, which uses three feature extractors simultaneously, has outperformed the other three methods in different noise modes.

B. Comparison and evaluation of the proposed method performance with other methods mentioned when rotating the copied area

One of the challenges in the proposed method is the rotation challenge. In this section, the detection rate of forgery images during rotation is examined in such a way that the images are rotated at different angles and their accuracy is evaluated with the best methods available in this field. The results of proposed methods of experiment and other methods are reported in Table 11.

Table 11. Comparison of the proposed method performance when the challenge of rotating the copied area occurs.

Rotation rate / Method	Identification rate (%)			
	45	90	135	180
Speed Up Robust Feature algorithm	96.27	96.64	96.15	97.15
Scale Invariant Feature Transform algorithm	97.61	98.01	97.89	98.10
Stationary wavelet and discrete cosine transform	93.24	94.51	93.35	94.62
Suggested method	**98.32**	**98.56**	**98.41**	**98.69**

As can be seen in Table 11, the Scale Invariant Feature Transform algorithm is more accurate than the other two methods. as can be seen, the proposed method is more accurate than the other three methods when rotating.

C. Comparison and Evaluation of the proposed method performance with other methods mentioned when resizing the copied area

In this section, the forged image recognition rate is checked when the input images are changed. The rate of change in the input image of scale in these experiments is considered to be 0.5, 1.5, and 2. This section examines the rate of identification of forged images during the scale change and evaluates their accuracy with the best methods available in this field. The results of the proposed methods of experiment and other methods are reported in Table 12.

Table 12. Comparison of the proposed method performance for challenge of resizing the copied area.

Change of scale / Method	Identification rate (%)		
	0.5	1.5	2
Speed Up Robust Feature algorithm	94.57	94.55	93.02
Scale Invariant Feature Transform algorithm	96.88	96.87	95.34
Stationary wavelet and discrete cosine transform	94.76	94.78	93.89
Suggested method	**98.72**	**98.74**	**97.87**

As can be seen in Table 12, the Scale Invariant Feature Transform algorithm is more accurate than the other two methods since it has fixed scale change; as can be seen, the proposed method is more accurate than the other three methods.

D. Comparing and evaluating of the proposed method performance with other methods mentioned in the symmetrical images

One of the challenges in the proposed method is the symmetrical images challenge. In this section, the rate of identification of forged images in symmetrical images has been examined and their accuracy has been evaluated with the best methods available in this field. The results of proposed methods of experiment and other methods are reported in Table 13.

As can be seen in Table 13, the Speed up Robust Feature algorithm is more accurate than the other two methods. As the number of symmetrical images increases, so does the error in detection, where these images are usually identified as forged images. For this reason, the higher the number of symmetrical images, the lower the detection accuracy. As can be seen, the prediction method is more accurate than the other three methods.

Table 13. Comparing the proposed method performance for challenge of symmetrical images.

Number of symmetrical images / Method	Identification rate (%)			
	1	2	3	4
Speed Up Robust Feature algorithm	95.75	95.12	94.91	93.12
Scale Invariant Feature Transform algorithm	94.35	93.79	93.23	91.34
Stationary wavelet and discrete cosine transform	94.89	93.99	93.57	92.93
Suggested method	**98.78**	**98.32**	**97.88**	**96.55**

E. Comparison and evaluation of the proposed method performance with other methods mentioned when all 4 challenges occur simultaneously

Since the occurrence of noise, rotation, scale and symmetrical image challenges simultaneously has a significant impact on the performance of forged image recognition systems, in this section, the identification rate of forged images when all four challenges occur simultaneously is examined. The extent of changes is 0.01 for noise, 180 for rotation, 1.5 for scale change, and 1 for symmetrical images, which is maximum change in image counterfeiting detection systems. The results of experiments can be seen in Table 14.

Table 14. Comparison of the proposed method performance when all four challenges occur simultaneously.

Method	Identification rate (%)
Speed Up Robust Feature algorithm	91.56
Scale Invariant Feature Transform algorithm	94.28
Stationary wavelet and discrete cosine transform	93.34
Suggested method	**98.81**

Based on the results shown in Table 14, the Scale Invariant Feature Transform algorithm is more accurate than the other two methods. As can be seen, the proposed method is more accurate than the other three methods.

5. CONCLUSION

In this paper, we provided an improved hybrid method for copy move forgery detection which a very high resistance to noise, rotation, scale and symmetrical images detection both individually and simultaneously, with also a detection accuracy were achieved. This method used a combination of Discrete Wavelet Transform, Scale Invariant Feature Transform algorithm, Local Binary Pattern simultaneously, and finally the suspicious area was selected in such a way that at least both methods used in this proposed method have the same opinion about the forgery of that area. This method, as several feature extractors were used simultaneously, was able to achieve acceptable accuracy compared to other methods presented in this field so far.

REFERENCES

[1] Y. Huang, W. Lu, W. Sun, and D. Long, **"Improved DCT-based detection of copy-move forgery in images,"** *Forensic Science International,* Vol. 206, pp. 178-184, 2011/03/20/ 2011.

[2] R. Davarzani, K. Yaghmaie, S. Mozaffari, and M. Tapak, **"Copy-move forgery detection using multiresolution local binary patterns,"** *Forensic*

Science International, Vol. 231, pp. 61-72, 2013/09/10/ 2013.

[3] G. Lynch, F. Y. Shih, and H.-Y. M. Liao, "**An efficient expanding block algorithm for image copy-move forgery detection,**" *Information Sciences*, Vol. 239, pp. 253-265, 2013/08/01/ 2013.

[4] J.-C. Lee, C.-P. Chang, and W.-K. Chen, "**Detection of copy–move image forgery using histogram of orientated gradients,**" *Information Sciences*, Vol. 321, pp. 250-262, 2015/11/10/ 2015.

[5] 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, 2015/05/01/ 2015.

[6] A. V. Malviya and S. A. Ladhake, "**Pixel Based Image Forensic Technique for Copy-move Forgery Detection Using Auto Color Correlogram,**" *Procedia Computer Science*, Vol. 79, pp. 383-390, 2016/01/01/ 2016.

[7] X. Bi, C.-M. Pun, and X.-C. Yuan, "**Multi-Level Dense Descriptor and Hierarchical Feature Matching for Copy–Move Forgery Detection,**" *Information Sciences*, Vol. 345, pp. 226-242, 2016/06/01/ 2016.

[8] 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, 2017/03/01/ 2017.

[9] 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, pp. 159-165, 2018/12/01/ 2018.

[10] C.-M. Pun and J.-L. Chung, "**A two-stage localization for copy-move forgery detection,**" *Information Sciences*, Vol. 463-464, pp. 33-55, 2018/10/01/ 2018.

[11] X. Bi and C.-M. Pun, "**Fast copy-move forgery detection using local bidirectional coherency error refinement,**" *Pattern Recognition*, Vol. 81, pp. 161-175, 2018/09/01/ 2018.

[12] T. Mahmood, Z. Mehmood, M. Shah, and T. Saba, "**A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform,**" *Journal of Visual Communication and Image Representation*, Vol. 53, pp. 202-214, 2018/05/01/ 2018.

[13] B. Soni, P. K. Das, and D. M. Thounaojam, "**Geometric transformation invariant block based copy-move forgery detection using fast and efficient hybrid local features,**" *Journal of Information Security and Applications*, Vol. 45, pp. 44-51, 2019/04/01/ 2019.

[14] A. Hegazi, A. Taha, and M. M. Selim, "**An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal,**" *Journal of King Saud University - Computer and Information Sciences*, 2019/07/24/ 2019.

[15] J.-L. Zhong and C.-M. Pun, "**Two-pass hashing feature representation and searching method for copy-move forgery detection,**" *Information Sciences*, vol. 512, pp. 675-692, 2020/02/01/ 2020.

[16] K. B. Meena and V. Tyagi, "**A copy-move image forgery detection technique based on tetrolet transform,**" *Journal of Information Security and Applications*, vol. 52, p. 102481, 2020/06/01/ 2020.

[17] X. Chao-jian and G. San-xue, "**Image Target Identification of UAV Based on SIFT,**" *Procedia Engineering*, Vol. 15, pp. 3205-3209, 2011/01/01/ 2011.

[18] A. Batur, G. Tursun, M. Mamut, N. Yadikar, and K. Ubul, "**Uyghur Printed Document Image Retrieval Based on SIFT Features,**" *Procedia Computer Science*, Vol. 107, pp. 737-742, 2017/01/01/ 2017.

[19] Y. Ji, L. Sun, Y. Li, and D. Ye, "**Detection of bruised potatoes using hyperspectral imaging technique based on discrete wavelet transform,**" *Infrared Physics & Technology*, Vol. 103, p. 103054, 2019/12/01/ 2019.

[20] C.-H. Hsia and J.-M. Guo, "**Efficient modified directional lifting-based discrete wavelet transform for moving object detection,**" *Signal Processing*, Vol. 96, pp. 138-152, 2014/03/01/ 2014.

[21] K. Gopala Krishnan and P. T. Vanathi, "**An efficient texture classification algorithm using integrated Discrete Wavelet Transform and local binary pattern features,**" *Cognitive Systems Research*, Vol. 52, pp. 267-274, 2018/12/01/ 2018.

[22] D. Vaishnavi and T. Subashini, "**Application of local invariant symmetry features to detect and localize image copy move forgeries,**" *Journal of information security and applications*, Vol. 44, pp. 23-31, 2019.