A New Method to Copy-Move Forgery Detection in Digital Images Using Gabor Filter

Mostafa Mokhtari Ardakan, Masoud Yerokh and Mostafa Akhavan Saffar

Abstract Copy-move forgery is one of the types of image manipulation which is widely used due to simplicity and effectiveness. In this method, part of the original image is copied and pasted to the desired location in the same image. The goal of detecting copy-move forgery is to find areas of the image that are identical or very similar. One of the important issues that some of the earlier algorithms suffer from is that the forged area is rotated or resized after attachment. In this research, a new approach is presented to detect copy-move forgery in digital images based on discrete wavelet decomposition along with multiple features extracted by Gabor filter to improve the function of detecting similar areas of the image. Experiments have shown that this algorithm recognizes similar areas with relatively good accuracy and is resistant to rotation and change in the scale of the forged area.

Keywords Detection of forgery · Copy-move forgery · Discrete wavelet transform Gabor filter · Feature matrix

1 Introduction

Image forgery or manipulation has a long history. In today's digital world, it's easy to create, modify, and correct information provided by the image (without leaving any obvious traces of this operation) [1]. Image forgery can be done in different ways and for different purposes. An old sample of forged image is the following Fig. 1.

M. Mokhtari Ardakan (✉) · M. Yerokh · M. Akhavan Saffar
Department of Computer and Information Technology, Faculty of Engineering, Payame Noor University, Tehran, Islamic Republic of Iran
e-mail: mostafamokhtari@pnu.ac.ir

M. Yerokh
e-mail: masoud_yerokh@yahoo.com

M. Akhavan Saffar
e-mail: akhavansaffar@pnu.ac.ir

S. Montaser Kouhsari (ed.), *Fundamental Research in Electrical Engineering*, Lecture Notes in Electrical Engineering 480,
https://doi.org/10.1007/978-981-10-8672-4_9

Fig. 1 Removing Nikolai Yezhov's picture

Fig. 2 The original image before forging

In this picture, the image of Nikolai Yezhov, one of the closest advisers of Joseph Stalin, the General Secretary of the Communist Party of the Soviet Union's Central Committee was removed from Stalin's photo after being jailed for corruption. The original image before the forging can be seen in Fig. 2.

Of the latest examples of image forgery, is Fig. 3. After the speech by Mr. Hassan Rouhani, President of Iran at the seventieth meeting of the UN General Assembly in New York, Foreign Minister Mohammad Javad Zarif, who was leaving the Assembly Hall, occasionally faced with President Barack Obama and Secretary of State John Kerry at the entry to the General Assembly and shook hands with them. After the publication of news, an image was published on social networks that claimed to be the photo of the moment that Javad Zarif and Barack Obama were shaking hands. A little care in watching the image shows that the image of Obama shaking hands with Zarif is manipulated in photoshop and it is fake. Studies also show that the original image is related to the visit of President Cavillion Raúl Castro and Barack Obama (Fig. 4).

The purpose of detecting forged image is the authentication of a digital image. Authentication solution is classified into two types:

Fig. 3 A forged image published showing the moment of Zarif's meeting with Barack Obama

Fig. 4 Cuban President Raúl Castro's and Barack Obama

(1) active and
(2) passive or blind.

Active forgery detection techniques (such as digital watermarking or digital signatures) utilize a well-known authentication code embedded in the image content; the authentication process may be proven through the verification of the existence of such an authentication code (by comparing with the original code inserted). In addition, this method requires specific hardware or software to add an authentication code into the image (before the image is published) [2].

Blind or passive forgery detection technique uses the received images only to assess the completeness or accuracy of the images. This method is based on the assumption that while digital forgery measures may leave no visual clues of a distorted image, but most likely they distort the statistic features or image integrity compared to the normal structure of the image, resulting in new adverse effects (leading to various forms of mismatch). This mismatch can be used to identify

forgery. Since this technique does not require any former information about the image, it is a commonly used technique. Existing techniques determine types of traces of manipulation and identify them (separately) by positioning the distorted areas.

2 Copy-Move Forgery (Or Area Copy Forgery)

Copy-move forgery is one of the most common techniques of image distortion, which is used due to its simplicity and effectiveness. In this method, part of the original image is copied and moved to another part in the same image and it is pasted there. This is done in order to hide particular details of the image or reproduce special effects in it. Because the uneven areas of the image have similar properties of color and noise fluctuations (which is imperceptible to the human eye in search of inconsistencies within the statistical properties of the image,) the region is used as the ideal part for cop-move forgery. Usually, fading operations (along the boundary edge of the modified area) are used to reduce the effect of disturbances between the main area and the pasted area [1]. Figure 5 presents examples of this type of forgery.

Copy-move forgery detection methods can be divided into two general categories:

1. Methods based on blocking
2. Non-block method

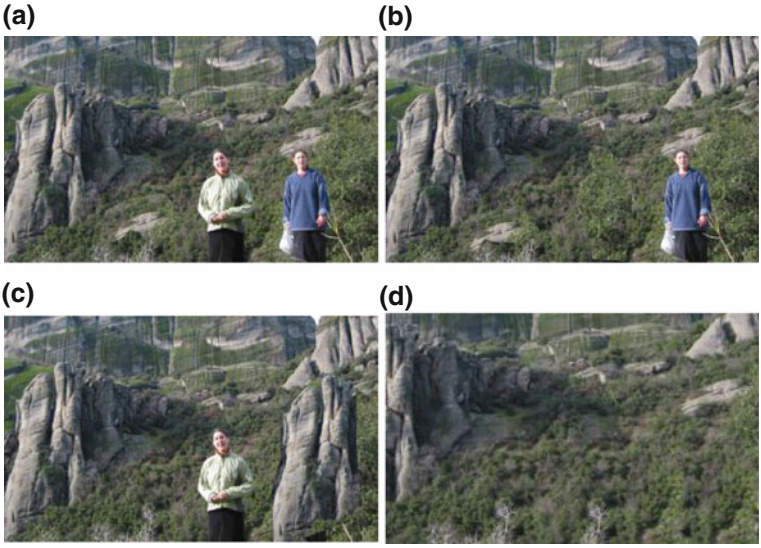

Fig. 5 **a** is the original image; **b**, **c** and **d** are forged images

Detection methods based on blocking

Most blocking methods follow a six-step process according to graph in Fig. 6.

Before the feature extraction process, a series of operations, such as image sorting, conversion of RGB images to black and white images or YCBCR conversion and the use of certain channels of the obtained images, the use of DWT or DCT conversion in order to reduce the size and improve the efficiency of classification, can be enforced on the desired images. To avoid the high computational cost of detailed search of image, comparison is made at the block level. The blocks used for comparison can be square or circle. Of course, square block use is more common [3]. If the image f(x, y) with a size of M × N pixels, and blocks with a size of b × b pixels are considered for comparison, then each block must be compared to the other blocks overlapping in the image by $(M - b + 1) \times (N - b + 1)$. Figure 7 shows the use of the two methods of blocking [4].

Accuracy, speed and complexity of forgery detection algorithm depends heavily on the ability to extract and identify similar features. Different extraction methods have been proposed for the extraction of features, most of which can be summarized in three methods: wavelet [4–7], location [8, 9] and frequency [10–12]. Some of these methods, such as methods that have been proposed in wavelet and frequency, have a good accuracy but are difficult in terms of time complexity, on the other hand, only part of these methods are resistant to factors such as Gaussian flattening and rotation. After the feature is extracted, potential copy-move pairs are identified by searching for similar feature blocks. Extracted features are initially arranged as

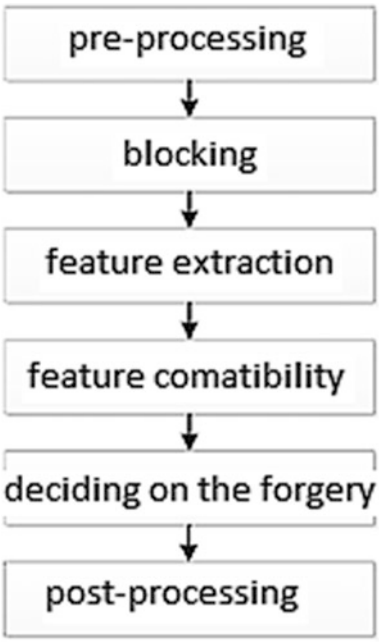

Fig. 6 Forgery detection process based on blocks

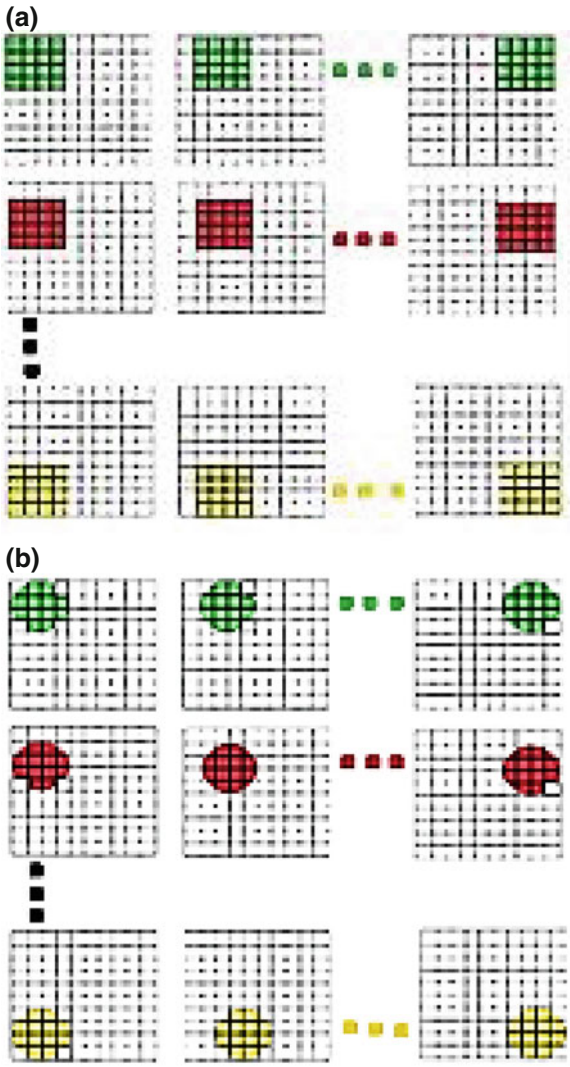

Fig. 7 Types of blocking: **a** square, **b** circular

M-matrix rows, then using trivial approach, each feature is compared with all the other features, but this approach is expensive in terms of computation time. To cope with this challenge, there are many ways to set similar features close together, which prevents useless comparisons and reduces computation time. In fact, each feature will be compared only to a certain number of neighbors. Among the known methods, the most common method is "lexicographic sorting" which uses "radix sorting" to create a matrix with the same features in the neighborhood, and thus make them easier to detect.

In addition to lexicographic sorting, base sorting, sorting by the number of zeros, k-dimensional tree sorting [13], a combination of "lexicographic sorting" and "k-d tree" which is used to improve the time complexity and accuracy in the process of matching the features, Bloom filters counting, sorting based on vector components with the highest variance among all features, comparing the hash values, block linking and block clustering could also be named. As soon as the data are organized to reduce the complexity of the investigation of similarities, search for similar features using various "similarity terms" is done, some of which can be cited as follows: Euclidean distance with the size of $S = 1/(1 + \text{dis})$ where "dis" is the distance measured in Euclidean space; Hamming distance, Hausdorff distance, logical distance, the correlation coefficient, the phase coefficient, cross-spectrum normalized, local sensitive hashing and ratio of absolute error. In the decision-making process on forgery, one can state that, almost always, a single similarity criterion is not enough to decide on the presence or absence of duplicated space. This is due to the fact that most natural images may contain one or more pairs of very similar regions; so, wrong matches may be resulted. Therefore, it is required to identify copy-move features of the areas to distinguish them from false matches. Sometimes, the map of the duplicated areas obtained from the previous step require more processing. Along with the rest (of the methods), post-processing can be performed by methods such as morphological post-processing including opening operations, erosion, dilatation, sliding window, square kernel mean filter and random sample consensus algorithm (RANSAC) which recognize the inliers and eliminate the outliers [3].

3 Introducing the New Method

In this research, a new method is presented for identifying areas of the image that are identical or very similar. The methodology is one of the methods of blind detection based on blocking. The proposed method is shown in Fig. 8. Myna et al. [4], presented a wavelet-based approach in which the use of wavelet transform in detection of copy-move forgery was tested. In the second stage, stored blocks are repeatedly compared in each level of the wavelet transform. Finally, the last match is done on the image. This approach functions properly when the copied area is changed by scaling and rotation. In their method, to resist against the change of scale and rotation, polar logarithmic transformation is used which is a change from the Cartesian to polar coordinates. In the new method in the present paper, to resist to the change in scale and rotation of the attached area, the Gabor filter is used.

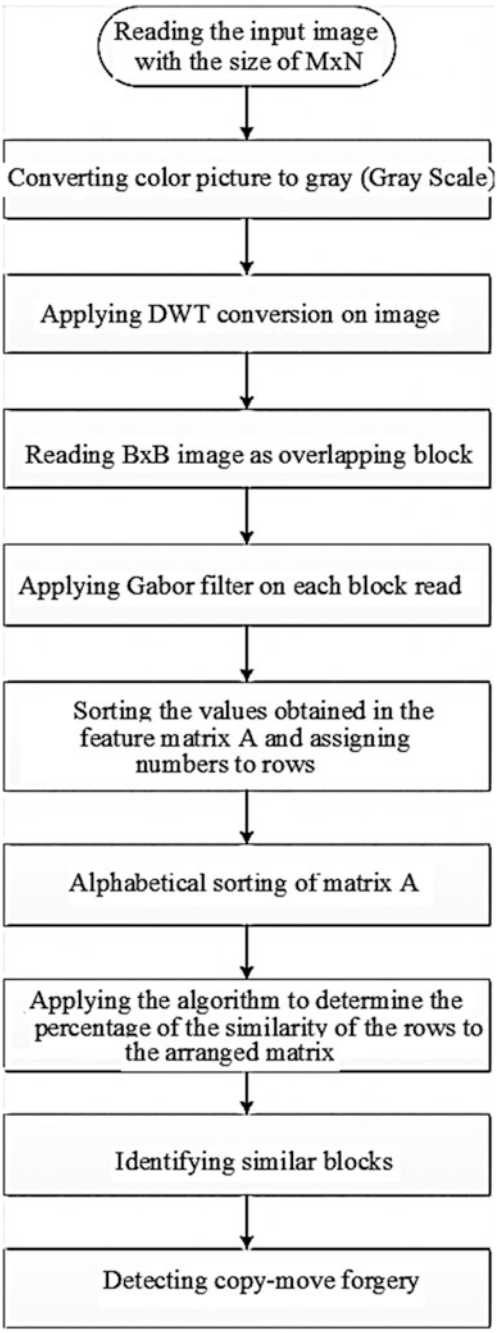

Fig. 8 Steps of the proposed method

3.1 Feature Extraction by Gabor Filter

Since the desired features in the image have different scales and directions, to extract information and directed features in different scales from the image is an essential step. Today, Gabor filters are widely used for this purpose due to suitable properties.

In 1946, Gabor deduced the principle of uncertainty for information on relations in quantum mechanics. According to this principle, simultaneous accuracy of a signal in two domains of time and frequency (the product of its time and frequency bandwidths) is limited by a low limit. Then he introduced a group of one-dimensional functions that achieved the low limit of uncertainty principle; in other words, the minimum simultaneous resolution in both time and frequency. These could be called fundamental (function) signals [14].

In 1980, inspired by Gabor, Dougman presented relations of uncertainty in two dimensions, and introduced a family of two-dimensional functions that reach the minimum value in the principal of uncertainty, and he called them Gabor functions. Two-dimensional Gabor function is obtained by multiplication of two-dimensional Gaussian function by a sinusoidal function in different directions of two-dimensional space. Due to very helpful properties, these functions are used in many applications as a filter in different fields of machine vision such as texture analysis, classification, image retrieval, pen detection, etc. Some of these properties to mention are simplicity, optimal simultaneous focus in location and frequency, and choice of direction and frequency for extracting image data [15, 16].

Using the two-dimensional transform of Gabor wavelet, one can extract the directional properties of the image in different scales. Physiological studies suggest that visual information processing in the visual system is done by a series of parallel mechanisms called channels; so that for each channel to use two-dimensional transform of Gabor wavelet, directional characteristics of the image at various scales could be extracted and each channel is regulated for a low frequency band width with specified direction. Mathematically, each of these channels are modeled with a pair of band-pass Gabor filters. The main advantage of Gabor filters are immutability to clearing up, rotation, scaling and image transfer. In addition, the filters can resist against photometric disorders (such as clearing changes and noise in the picture). Gabor filter in a two-dimensional spatial coordinate is a Gaussian kernel function (modulated by a complex flat sine wave), as formula (1).

$$\begin{aligned} \mathrm{G}(\mathrm{x},\mathrm{y}) &= \frac{f^2}{\pi\gamma\mu}\exp\left(-\frac{x'^2+\delta^2 y'^2}{2\delta^2}\right)\exp\ (j2\pi f x'+\varphi) \\ x' &= x\cos\theta + y\sin\theta \\ y' &= -x\sin\theta + y\cos\theta \end{aligned} \tag{1}$$

where f is the frequency of the sinusoidal factor. θ also shows the orientation of the normal stripe of Gabor's function relative to the parallel striped of the Gabor

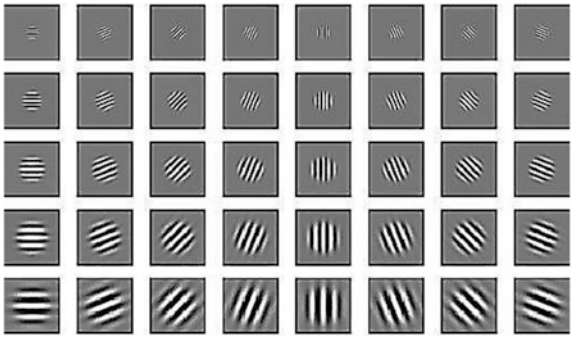

Fig. 9 Gabor filter in 5 sizes and 8 directions

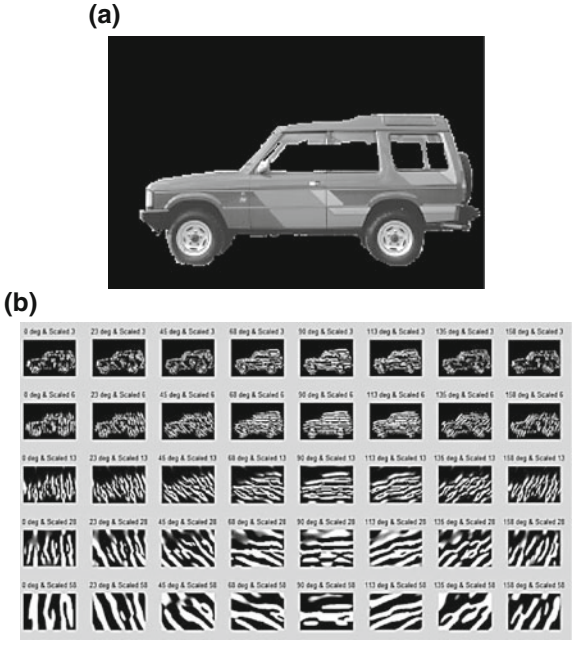

Fig. 10 **a** Vehicle image to apply to the Gabor filter. **b** The Gabor filter output on the vehicle image

function. φ is the offset of phase and σ is equal to the standard deviation of Gaussian cover. γ is the ratio of space visibility that determines the ellipticity of the Gabor function. As shown in Fig. 9, the algorithm can take advantage of forty Gabor filters (on five scales and eight directions) [17].

For example, if we use Gabor filter on Fig. 10a, the output will be the same as Fig. 10b.

Due to the fact that adjacent pixels in the image are correlated to each other, extension information could be removed through the sampling process which is less than the usual images resulting from Gabor filters [17].

3.2 Splitting the Image into Overlapped Blocks and Creating a Feature Matrix

After reading the input image of the size M × N the wavelet transform is done to the "L" level, then blocks of the size b × b pixels continue from the top left corner of the image down to the lower right corner. For each position, the block is mapped to the fifth row of the Gabor filter, then the pixel values are extracted in one row of the two-dimensional A-matrix with 32 columns and (M − b + 1) × (N − b + 1) rows. Each row corresponds to a block position and to better understand the steps involved in implementing the proposed method, this algorithm is described with a small and very simple image like Fig. 11.

Because Fig. 11 is too small, a 4 × 4 window as shown in Fig. 12 is moved by applying Gabor filter on each block. According to Fig. 10, (8 × 8 block was used in the source code) overlapping blocks inserted in the feature matrix as a row vector shown Fig. 13.

3.3 Alphabetical Sorting of Feature Matrix

To ensure the minimum number of comparisons to find the most similar blocks to each other, alphabetical sorting is applied on the feature matrix obtained from the previous step. This will locate the more similar rows next to each other and the execution time of the algorithm will reduce significantly. The result of the alphabetic sorting on the feature matrix of Fig. 13 is visible in Fig. 14.

Fig. 11 An 9 × 8 image

1	1	1	1	3	6	10	4	3
1	1	1	1	4	2	12	11	5
1	1	1	1	9	4	1	9	2
1	1	1	1	5	8	2	7	6
6	4	5	6	1	1	1	1	9
2	10	3	4	1	1	1	1	7
3	5	4	1	1	1	1	1	1
7	9	7	8	1	1	1	1	3

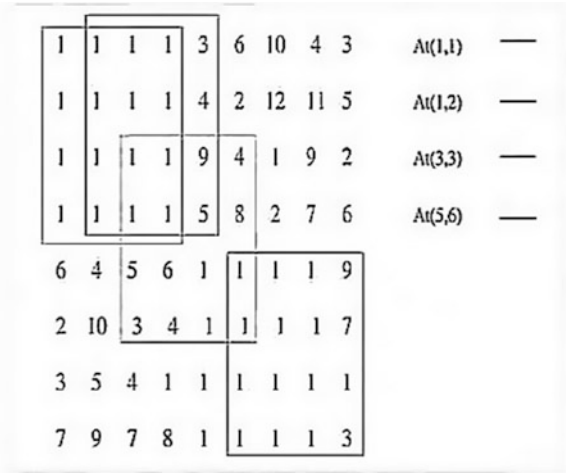

Fig. 12 Overlapping blocks in rows

3.4 Finding the Most Similar Blocks to Each Other Using Fourier Transform and Phase Correlation

Phase relationship is a suitable method for pattern matching. The ratio of R between the two pictures img1 and img2 is calculated according to formula (2) where 'F' is Fourier transform, and 'conj' is mixed conjunction [4, 18].

$$R = \frac{F(img1) \times conj(f(img2))}{F(img1) \times conj(f(img2))} \tag{2}$$

To find forgery in the image, a threshold proportional to the image is defined which the selection of this coefficient will be largely empirical. Surely, the more accurate this coefficient is selected, the more precise will be the locations that are detected as forgeries and also the less the extra points.

4 Investigating the results

The new program for detecting forgery by Gabor filter and the Myna [4] method was implemented in MATLAB environment version R2014a and was tested on a computer with a six gigabyte RAM and a five-core processor and Windows 8.1 operating system.

As mentioned, to resist the rotation and size change of the forged parts, the Gabor and Myna [4] filters used logarithmic-polar transformation. Results on the forged image have been investigated in different sizes and modes that shown in Figs. 15, 16, 17, 18, 19, 20, 21, 22, 23 and 24.

(a) Matrix of feature vectors before sorting																Blocks index
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	3	4	9	5	2
1	1	1	1	1	1	1	1	3	4	9	5	6	2	4	8	3
1	1	1	1	3	4	9	5	6	2	4	8	10	12	1	2	4
3	4	9	5	6	2	4	8	10	12	1	2	4	11	9	7	5
6	2	4	8	10	12	1	2	4	11	9	7	3	5	2	6	6
1	1	1	6	1	1	1	4	1	1	1	5	1	1	1	6	7
1	1	1	4	1	1	1	5	1	1	1	6	4	9	5	1	8
1	1	1	5	1	1	1	6	4	9	5	1	2	4	8	1	9
1	1	1	6	4	9	5	1	2	4	8	1	12	1	2	1	10
4	9	5	1	2	4	8	1	12	1	2	1	11	9	7	1	11
2	4	8	1	12	1	2	1	11	9	7	1	5	2	6	9	12
1	1	6	2	1	1	4	10	1	1	5	3	1	1	6	4	13
1	1	4	10	1	1	5	3	1	1	6	4	9	5	1	1	14
1	1	5	3	1	1	6	4	9	5	1	1	4	8	1	1	15
1	1	6	4	9	5	1	1	4	8	1	1	1	2	1	1	16
9	5	1	1	4	8	1	1	1	2	1	1	9	7	1	1	17
4	8	1	1	1	2	1	1	9	7	1	1	2	6	9	7	18
1	6	2	3	1	4	10	5	1	5	3	4	1	6	4	1	19
1	4	10	5	1	5	3	4	1	6	4	1	5	1	1	1	20
1	5	3	4	1	6	4	1	5	1	1	1	8	1	1	1	21
1	6	4	1	5	1	1	1	8	1	1	1	2	1	1	1	22
5	1	1	1	8	1	1	1	2	1	1	1	7	1	1	1	23
8	1	1	1	2	1	1	1	7	1	1	1	6	9	7	1	24
6	2	3	7	4	10	5	9	5	3	4	7	6	4	1	8	25
4	10	5	9	5	3	4	7	6	4	1	8	1	1	1	1	26
5	3	4	7	6	4	1	8	1	1	1	1	1	1	1	1	27
6	4	1	8	1	1	1	1	1	1	1	1	1	1	1	1	28
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	29
1	1	1	1	1	1	1	1	1	1	1	1	9	7	1	3	30

Fig. 13 Feature matrix before sorting

4.1 Forgery Detection Without Changing Size and Rotation and Different Rows of Gabor Filter

Result 1: The result of the forgery detection algorithm is visible using the Gabor filter in Fig. 16.
Result 2: Test on the second forged image without using discrete wavelet transform (Fig. 17).
Result 3: Test on the second forged image using discrete wavelet transform (Fig. 18).

(b) Matrix of feature vectors after sorting																Blocks index
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	29
1	1	1	1	1	1	1	1	1	1	1	1	3	4	9	5	2
1	1	1	1	1	1	1	1	1	1	1	1	9	7	1	3	30
1	1	1	1	1	1	1	1	3	4	9	5	6	2	4	8	3
1	1	1	1	3	4	9	5	6	2	4	8	10	12	1	2	4
1	1	1	4	1	1	1	5	1	1	1	6	4	9	5	1	8
1	1	1	5	1	1	1	6	4	9	5	1	2	4	8	1	9
1	1	1	6	1	1	1	4	1	1	1	5	1	1	1	6	7
1	1	1	6	4	9	5	1	2	4	8	1	12	1	2	1	10
1	1	4	10	1	1	5	3	1	1	6	4	9	5	1	1	14
1	1	5	3	1	1	6	4	9	5	1	1	4	8	1	1	15
1	1	6	2	1	1	4	10	1	1	5	3	1	1	6	4	13
1	1	6	4	9	5	1	1	4	8	1	1	1	2	1	1	16
1	4	10	5	1	5	3	4	1	6	4	1	5	1	1	1	20
1	5	3	4	1	6	4	1	5	1	1	1	8	1	1	1	21
1	6	2	3	1	4	10	5	1	5	3	4	1	6	4	1	19
1	6	4	1	5	1	1	1	8	1	1	1	2	1	1	1	22
2	4	8	1	12	1	2	1	11	9	7	1	5	2	6	9	12
3	4	9	5	6	2	4	8	10	12	1	2	4	11	9	7	5
4	8	1	1	1	2	1	1	9	7	1	1	2	6	9	7	18
4	9	5	1	2	4	8	1	12	1	2	1	11	9	7	1	11
4	10	5	9	5	3	4	7	6	4	1	8	1	1	1	1	26
5	1	1	1	8	1	1	1	2	1	1	1	7	1	1	1	23
5	3	4	7	6	4	1	8	1	1	1	1	1	1	1	1	27
6	2	3	7	4	10	5	9	5	3	4	7	6	4	1	8	25
6	2	4	8	10	12	1	2	4	11	9	7	3	5	2	6	6
6	4	1	8	1	1	1	1	1	1	1	1	1	1	1	1	28
8	1	1	1	2	1	1	1	7	1	1	1	6	9	7	1	24
9	5	1	1	4	8	1	1	1	2	1	1	9	7	1	1	17

Fig. 14 Feature matrix after sorting

Result 4: Test on the third forged image using discrete wavelet transform (Fig. 19).
Result 5: Test on a the fourth forged image without using a discrete wavelet transform (Fig. 20).
Result 6: Test on the fourth forged image using discrete wavelet transform (Fig. 21).

Fig. 15 The original image on the right, the forged image on the left

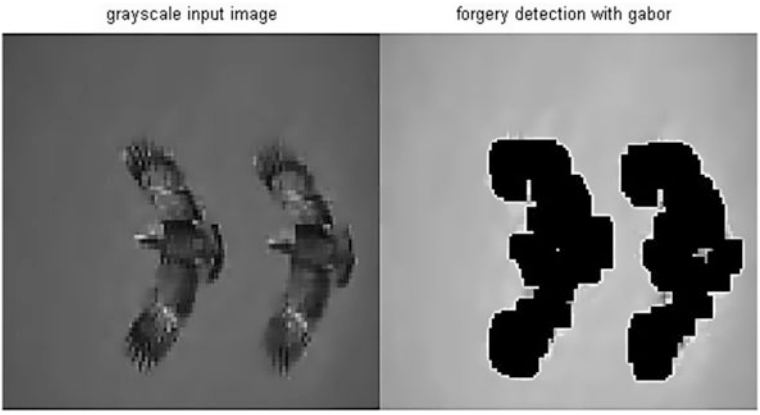

Fig. 16 Resolution: 256 × 256 pixels, block size: 88, diagnosis time: 30.737703 s, the correlation coefficient: 0.8 < R < 0.87, Gabor filter: fifth row, DWT to the first level

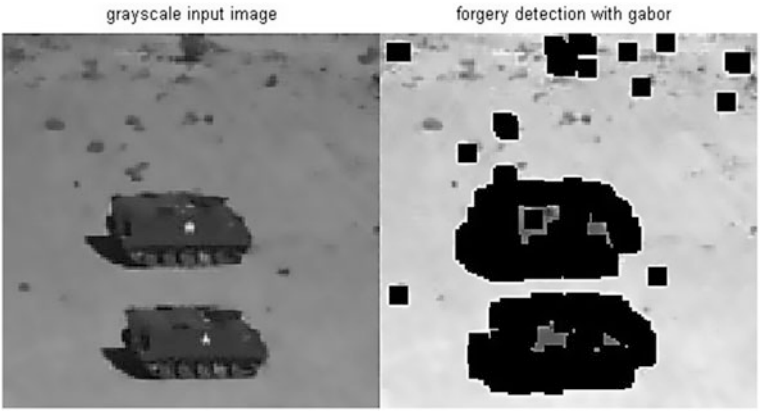

Fig. 17 Resolution: 160 × 160 pixels, block size: 88, diagnosis time: 63.503775 s, the correlation coefficient: 0.87 < R < 0.81, Gabor filter: fifth row, no DWT

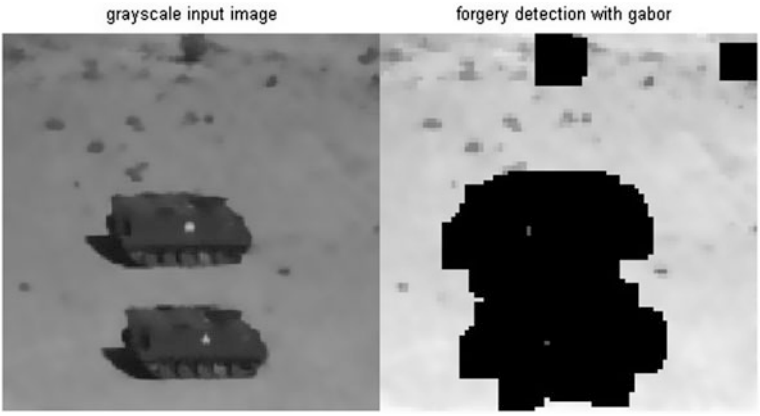

Fig. 18 Resolution: 160 × 160 pixels, block size: 88, diagnosis time: 7.636435 s, correlation coefficient: 0.87 < R < 0.81, Gabor filter: fifth row, DWT to the first level

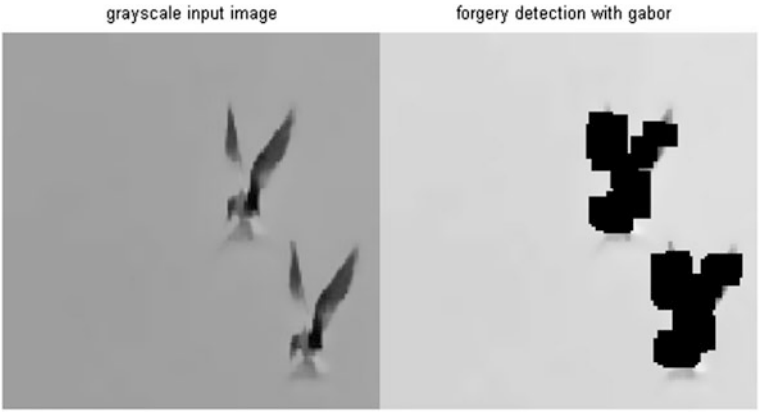

Fig. 19 Resolution: 256 × 256 pixels, block sizes: 88, diagnosis time: 31.899262 s, correlation coefficient: 0.9 < R < 0.85, Gabor Filter: fifth row, DWT to the first level

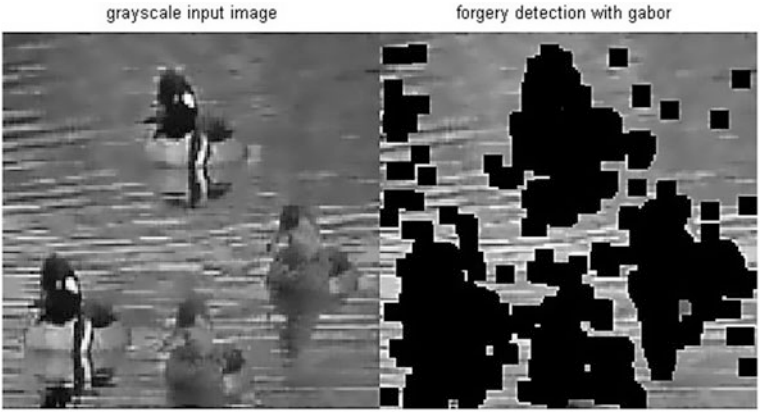

Fig. 20 Resolution: 160 × 160 pixels, block size: 88, diagnosis time: 61.1505862 s, correlation coefficient: 0.95 < R < 0.9, Gabor filter: fifth row, no DWT

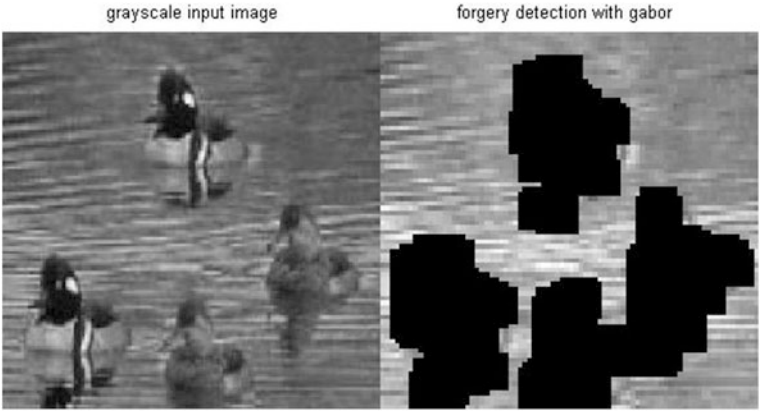

Fig. 21 Image size: 160 × 160 pixels, block size: 88, detection time: 61.1505862 s, correlation coefficient: 0.95 < R < 0.9, Gabor filter: fifth row, DWT to the first level

4.2 Resistance to Rotation

See Figs. 22 and 23.

4.3 Resistance to Resizing

See Fig. 24.

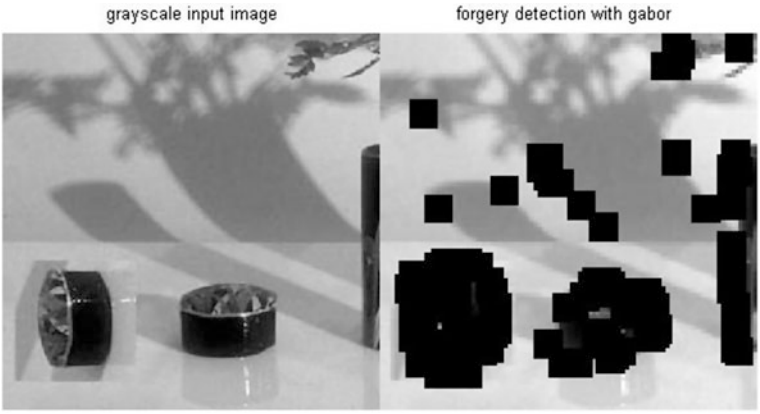

Fig. 22 The original image on the left, the forged image on the right, image size: 412 × 412 pixels, block size: 88, detection time: 15.12938 s, correlation coefficient: 0.86 < R < 0.83, Gabor filter: fifth row, DWT to second level

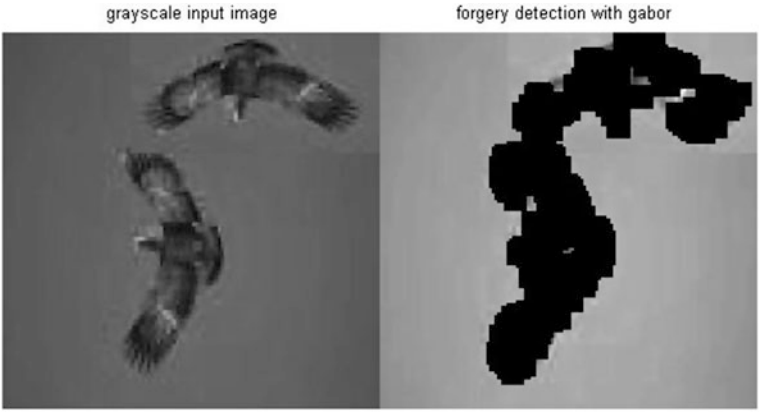

Fig. 23 The original image on the left, the forged image on the right, image size: 256 × 256 pixels, block size: 88, detection time: 30.04619 s, correlation coefficient: 0.9 < R < 0.8, Gabor filter: fifth row, DWT to the first level

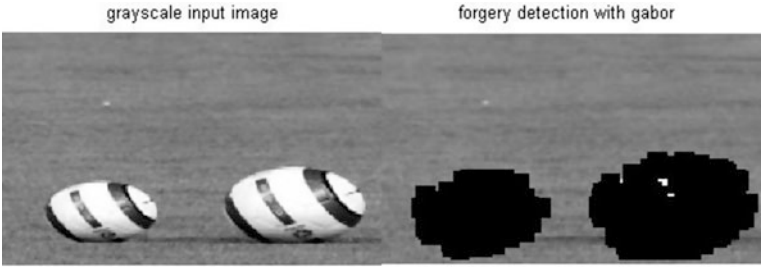

Fig. 24 The original image on the left, the forged image on the right, resolution: 300 × 600 pixels, block sizes: 88, detection time: 25.27208 s, the correlation coefficient: $0.92 < R < 0.87$, Gabor filter: fifth row, DWT to second level

5 Conclusion

The obtained results and their comparison with the results indicated by Myna, it can be concluded that the new method proposed considering the time of performance is suitable, and on some images, in particular, the images in which the forged piece is resized, this method is better than Myna's method. To detect the forged area on images that forgery is not in the form of moving one part, which is not a dominant component of the image, it works well and as expected, it also works well in resize and rotation cases. However, in case of forgeries that part of the image background is used to hide part of the image or object, the performance is reduced. As already mentioned, the main advantage of Gabor filters is their immutability to clearing up, rotation, scaling and image transfer. In addition, the filters can resist against photometric disorders (such as clearing up and noise in the picture). Additional operations such as blurring may be used to eliminate the unevenness of the edge of the copied area. In such cases, the use of DCT and PCA has the advantage of being resistant to such an operation, but direct implementation lacks this advantage. It should be noted that these methods can undergo this type of operation to a certain extent. For example, if blurring is performed with high intensity, other duplicated areas cannot be identified. This occurs when blurring can be detected by eye, in which case there will be no need to search for the duplicated area. In the mentioned methods, the time complexity of the algorithm will also be reduced by reducing the length and size of the blocks.

References

1. Birajdar GK, Mankar VH (2013) Digital image forgery detection using passive techniques: a survey. Digit Invest: 226–245
2. Chauhan A (2015) Digital watermarking-revisit. J Comput Sci Inf Technol 6(1):833–838
3. Diane N, Xingming WNS, Moise FK (2014) A survey of partition-based techniques for copy-move forgery detection. Sci World J 1–13

4. Myna AN, Venkateshmurthy MG, Patil C (2007) Detection of region duplication forgery in digital images using wavelets and log-polar mapping. In: International conference on computing intelligence multimedia application, pp 371–377
5. Li G, Wu Q, Tu D, Sun S (2007) A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD. In: IEEE international conference on multimedia and expo, pp 1750–1753
6. Khan S, Kulkarni A, Khan ES, Kulkarni EA (2010) An efficient method for detection of copy-move forgery using discrete wavelet transform. Int J Comput Sci Eng: 1810
7. Gan Y, Zhong J (2015) Image copy-move forgery blind detection algorithm based on the normalized histogram multi-feature vectors. J Softw Eng: 254–264
8. Luo W, Huang J, Qiu G (2006) Robust detection of region-duplication forgery in digital image. In: 18th international conference pattern recognition, pp 18–21
9. Ryu SJ, Lee MJ, Lee HK (2010) Detection of copy-rotate-move forgery using zernike moments. Lecture notes computing science (including Subseries. Lecture notes artificial intelligence lecture notes bioinformatics), pp 51–65
10. Bayram S, Sencar HT, Memon N (2009) An efficient and robust method for detecting copy-move forgery. In: IEEE international conference on acoustics speech signal process. ICASSP 2009. IEEE, pp 1053–1056
11. AndaJan L, Fridrich J, Soukal D (2008) Detection of copy-move forgery in digital images using sift algorithm. In: Proceedings—2008 Pacific-Asia workshop on computational intelligence and industrial application, PACIIA, pp 272–276
12. Popescu AC, Farid H (2004) Exposing digital forgeries by detecting duplicated image regions. Department Computing Science, Dartmouth College. Technical Report. TR2004-515, no. 2000, pp 1–11, 2004
13. Davarzani R, Yaghmaie K, Mozaffari S, Tapak M (2013) Copy-move forgery detection using multiresolution local binary patterns. Forensic Sci Int: 61–72
14. Gabor D (1946) Theory of communication. Part 1: the analysis of information. J Inst Electr Eng III Radio Commun Eng: 429–441
15. Daugman JG (1985) Uncertainty relation for resolution in space, spatial frequency, and orientation optimized by two-dimensional visual cortical filters. J Opt Soc Am A:1160
16. Seryasat OR, Haddadnia J, Ghayoumi-Zadeh H (2015) A new method to classify breast cancer tumors and their fractionation. Ciência e Nat 37:51–57
17. Haghighat M, Zonouz S, Abdel-Mottaleb M (2013) Identification using encrypted biometrics. In: Computer analysis of images and patterns, pp 440–448
18. Kang X, Li Y, Qu Z, Huang J (2012) Enhancing source camera identification performance with a camera reference phase sensor pattern noise. IEEE Trans Inf Forensics Secur: 393–402