Multimedia Tools and Applications (2019) 78:20655–20678
https://doi.org/10.1007/s11042-019-7277-1

Copy-move forgery detection based on multifractals

Aleksandra Pavlović[1,2] • Natasa Glišović[2] • Ana Gavrovska[1] • Irini Reljin[1]

Received: 4 July 2018 / Revised: 30 November 2018 / Accepted: 24 January 2019 /
Published online: 5 March 2019

Abstract
Digital images and video are the basic media for communication nowadays. They are used as authenticated proofs or corroboratory evidence in different areas like: forensic studies, law enforcement, journalism and others. With development of software for editing digital images, it has become very easy to change image content, add or remove important information or even to make one image combining multiple images. Thus, the development of methods for such change detection has become very important. One of the most common methods is copy-move forgery detection (CMFD). Methods of this type include change detection that occur by copying a part of an image and pasting it to another location within the image. We propose new method for detection of such changes using certain multifractal parameters as characteristic features, as well as common statistical parameters. Before the analysis, images are divided into non-overlapping blocks of fixed dimensions. For each block, the characteristic features are calculated. In order to classify observed blocks, we used metaheuristic method and proposed new semi-metric function for similarity analysis between blocks. Simulation shows that the proposed method provides good results in terms of precision and recall, with low computational complexity.

Keywords Image forensics · CMFD (copy-move forgery detection) · Multifractal spectrum · Hölder exponent · Metaheuristic method · Semi-metric

✉ Aleksandra Pavlović
sandra.pavlo@gmail.com

Natasa Glišović
natasaglisovic@gmail.com

Ana Gavrovska
anaga777@gmail.com

Irini Reljin
irinitms@gmail.com

Extended author information available on the last page of the article

1 Introduction

With development of modern digital cameras and smartphones, the use of multimedia content is increasingly present in everyday life. Distribution of digital images has increased especially on the Internet and social networks. Those images are used in everyday life, as authenticated proofs or corroboratory evidence in areas like: forensic studies, law enforcement, journalism and others. There are many available software applications used for modification of digital image content. Digital photographs can be easily modified, so one cannot be certain about delivered information from the image content. Therefore, it is important to develop methods to be used in checking the image authenticity, which will indicate any changes in the image content.

The methods for change detection in images can be divided into two categories: active and passive. Active methods imply that a digital signature or a watermark is inserted into the original image. It requires additional information to be embedded in the image during the capturing process or, at later, by authorized personnel, which will be a proof that the image is genuine, i.e. the image content can be trusted when delivered. On the other hand, passive methods allow change detection in images without the presence of additional information. They can be used to detect changes in images by extracting natural features within the image or to detect the source of the image generation, based on optical and sensor regularities.

Numerous methods have been proposed for image forensics, where: image splicing, copy move and image recoloring or fake colorizing are analyzed [13, 14, 32]. Image splicing means that a new image is made by combining content from two or more different images. Image recoloring is a technique that can transfer image color or theme, making imperceptible changes. Copy-Move Forgery Detection (CMFD) is one of the most popular methods in image forensics, where content changes are deliberately made by copying a part of an image and pasting it to another location within the image. An example of copy-move forgery is given in Fig. 1, where both the original and the modified image (forgery) are presented. In Fig. 1 the modification is made so that the soldier from the original image is covered by copying a piece of grass found within the image.

The typical aim of the copy-move changes is to duplicate (or multiplicate) an object found in the image or to cover some image parts in order to convey information different from the original image. Thus, the image content is modified all in purpose to deliver erroneous information. Such deliberately made changes, e.g. copied parts, can be: translated, rotated, scaled, filtered, and so on. If parts of the original image are copied somewhere else within the

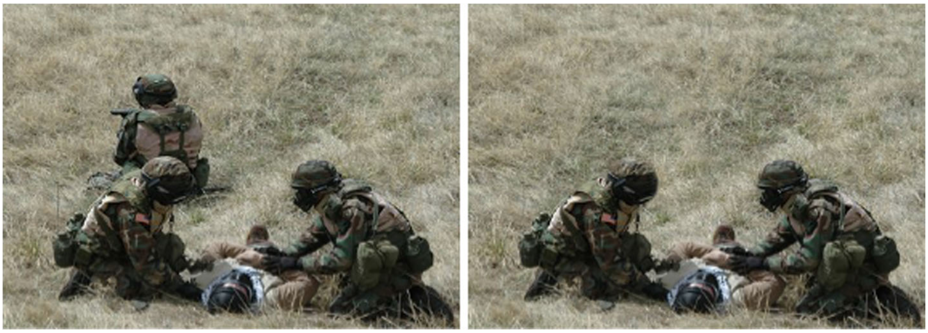

Fig. 1 Copy-move forgery example

same image, noise components, color, dynamic range and other corresponding important features of the copied parts will be compatible with the rest of the image. Consequently, it is not an easy task to detect the changes by methods that seek for incompatibilities according to image statistics, and statistics of various image parts.

CMFD methods can be keypoint-based or block-based.

The keypoint-based methods use characteristic point extraction, where the extraction is made only in particular regions, without any subdivisions of the image. The keypoint features are based on the characteristics such as: corners, blobs, edges. The characteristics should be helpful in increasing the accuracy of matching. The obtained feature vectors are classified and matched to each other in order to find the duplicated regions in the copy-move forgery.

Various techniques and transforms are used in the literature for the region clustering and keypoint-based matching, like: Discrete Radon Polar Complex Exponential Transform (DRPCET), the Radon transform (RT) and the Polar Complex Exponential Transform (PCET) [40], an Adaptive Patch Matching algorithm and Matched Keypoints Merging algorithm [6], Local Bidirectional Coherency Error [3], Scale Invariant Feature Transform (SIFT) [35], FAST (Features from Accelerated Segment Test) and scaled ORB (Oriented FAST and Rotated BRIEF (Binary Robust Independent Elementary Feature)) [36], discrete analytical Fourier–Mellin transform (DAFMT) [38], analytical Fourier–Mellin transform (AFMT) [36], Local Binary Pattern (LBP) and Discrete Cosine Transform (DCT) [1, 19, 21], Speeded-Up Robust Feature (SURF) [15], Multi-Level Dense Descriptor (MLDD) [4], local Gabor wavelets patterns (LGWP) [6], planar homography constraint and graph cut [34]**,** SIFT and overlapping region-based global context descriptor (OR-GCD) [39].

The block-based CMFD methods use overlapping or non-overlapping blocks for forgery image analysis. Descriptors are calculated for individual blocks and used in order to determine similarities among the blocks, i.e. different parts of the analyzed image. The block-based CMFD methods use different descriptors for the similarity matching, where the blocks suspected as forgery are typically the ones where the matching is detected. The algorithms usually applied for block-based approaches use: Radial Harmonic Fourier Moments (RHFMs) and SIFT [9], stationary wavelet transform (SWT) and DCT [21], invariant Quaternion Exponent Moments (QEMs) [31], Discrete Radial Harmonic Fourier Moments (DRHFMs) [38], DCT [2, 30], LBP and DCT [1], DWT and DCT [15], Swarm Intelligence (SI) and SIFT [35], Auto Color Correlogram (ACC) [22], Histogram of Gradients (HOG) [19], PCET and Approximate Nearest Neighbor (ANN) Searching [8], LBP Histogram, Fourier features and Fast Walsh-Hadamard Transform (FWHT) features [29].

In addition to the above-mentioned methods, there were also a few considerations of using fractal and multifractal dimension in order to perform CMFD [17, 26]. In [17], authors use multifractal dimension, block-based mean and variance of pixel values and central moment, while in [26] the authors apply Local Fractal Dimension (LFD) and Singular Value Decomposition (SVD) in order to perform CMFD.

The aim of this research is to develop a multifractal-based method in order to detect changes in the images produced by copy-move and multi-paste methods. Namely, copy-move image forgery detection using multifractal spectrum and its characteristics, as well as some common statistical parameters, has been carried out to show how block size affects the forgery detection accuracy, as well as to analyze the impact of the block size on the precision and recall. Image database used in this paper considers data from a publicly available CoMoFoD and Image Manipulation Dataset [7, 16].

The paper is consisted of six sections. The Introduction section is followed by Section II where the methods from the literature are briefly described. Section III presents some of the main multifractal spectrum image characteristics. The proposed method and mathematical model used for block classification are presented in Section IV. The experimental results followed by discussion are presented in Section V. Section VI represents the main conclusions of the proposed multifractal-based method.

2 Related work

In the last decade different methods were developed for detection of changes in images, especially the ones made in copy-move manipulations. CMFD can be divided into keypoint-based and block-based methods.

2.1 Keypoint-based methods

Zhong, J., Gan, Y., Young, J., Huang, L., & Lin, P.in [38] proposed the method based on color invariance and QPCET (quaternion polar complex exponential transform). The points of interest in an image are extracted using point detector, which involves the Speeded Up Robust Features (SURF) detector and color invariance model. In [6], Bi, X., Pun, C. M., & Yuan, X. C. suggest copy-move forgery detection method using multi-scale feature extraction and adaptive matching. The image is firstly segmented into the non-overlapping patches of irregular shape in different scales, where Scale Invariant Feature Transform (SIFT) is applied to extract feature points from all patches. The method based on a coherency sensitive hashing for establishing the feature correspondences and a local bidirectional coherency in an image is presented in [3], by Bi, X., & Pun, C. M. In [33], Sun, X., Guo, H., Xia, Z., & Chen, X. presented keypoint method based on the modified SIFT-based detector. For keypoints distribution, a novel strategy is developed for interspersing, where the keypoints are described by an improved SIFT descriptor. Zhu, Y., Shen, X., & Chen, H. in [40] proposed the method based on the following steps: establishing a Gaussian scale space, extracting the orientated FAST keypoints and the ORB features in each scale space, reverting the coordinates of the orientated FAST keypoints to the original image and matching the ORB features between each pair of keypoints. The method based on the use of DAFMT was presented in [36] by Zhong, J., & Gan, Y.. The image is firstly converted from RGB to grayscale domain, and then the DAFMT is applied in extracting the characteristics. The characteristics are lexicographically sorted and then compared using the Spearman rank correlation coefficient. In [1], Alahmadi, A., Hussain, M., Aboalsamh, H., Muhammad, G., Bebis, G., & Mathkour, H. presented the method based on steerable pyramid transform (SPT) and Local Binary Pattern (LBP). The color image is firstly converted into the YCbCr system, and then the SPT is applied to the chrominance channels in order to provide multiple and multi-oriented subbands. SVM (Support Vector Machine) is used for the classification. The method based on the analysis of discrete cosine transform coefficients is presented in [20] by Lin, C. S., & Tsay, J. J.. The method was proved to be convenient for change detection in images that have undergone JPEG compression and contain the accompanying artefacts. Kaushik, R., Bajaj, R. K., & Mathew, J. in [18] describe the method based on two-dimensional DCT and statistical moments. The window centered around each pixel slides through the image. DCT is calculated for each window, and a quantization matrix is obtained. In [15], the authors describe a method that uses the SURF algorithm in the opponent's color space. Namely, the color image is firstly converted to the opponent color space. The color gradient is calculated for each pixel, and it is used as the workspace for the SURF algorithm for keypoints extraction. The method based on the application of analytical Fourier Mellin transform (AFTM) is shown [9] by Gan, Y., & Zhong, J.. The idea is to use AFTM in order to provide scaling and rotational invariance for constructing the image geometric invariance. In [4], Bi, X., Pun, C. M., & Yuan, X. C. present the method using Multi-Level Dense Descriptor (MLDD) and Hierarchical Feature Matching. MLDD is calculated for each pixel, and it consists of two parts: the Color Texture Descriptor and the Invariant Moment Descriptor. After calculating the MLDD, Hierarchical Feature Matching is applied to detect suspicious regions. In [34], Zhang, W., Cao, X., Qu, Y., Hou, Y., Zhao, H., & Zhang, C. proposed a method based on the planar homography constraint with automatic extraction using graph cut. Firstly, the fake region is located roughly by using the planar homography constraint. Secondly, the fake object is segmented via graph cut. This method works efficiently as long as there are image regions satisfying the planar homography constraint. In [39], the authors proposed a method based on SIFT algorithm and the overlapping region-based global context descriptor (OR-GCD). The proposed method consists of three main steps: SIFT feature matching, OR-GCD extraction, and verification of SIFT matches**.** In order to filter false matches for copy detection, the authors used a global context verification scheme.

2.2 Block-based methods

The block-based CMFD is popular approach adopted by researchers in recent years, due to its compatibility with various feature extraction techniques and an increased matching performance. Chou, C. L., & Lee, J. C. [8] proposed the block-based passive method for copy-move forgery detection based on LGWP and rotation-invariant ability of uniform LBP. In [11], Gan, Y., Chung, J., Young, J., Hu, Z., & Zhao, J. suggested the block-based method which combines RHFMs and SIFT algorithm. Texture patches are used in segmentation, and the Simple Linear Iterative Clustering (SLIC) is proposed. Mahmood, T., Mehmood, Z., Shah, M., & Saba, T. in [21] proposed the method based on the extracts of SWT, because of its impressive localization properties, in both spectral and spatial domain. For reduction of the feature vector dimension, DCT is applied. Robust copy–move forgery detection approach by using invariant QEMs is presented in [31], by Wang, X. Y., Liu, Y. N., Xu, H., Wang, P., & Yang, H. Y. The tempered color image is firstly preprocessed with Gaussian low-pass filter and then divided into overlapping circular blocks. Then, the descriptor, QEMs modulus, is calculated for each block. A new copy-move method is presented in [37], by Zhong, J., Gan, Y., Young, J., Huang, L., & Lin, P., where an image is firstly divided into overlapped blocks, and then the local image features are extracted by the DRHFMs. The similar feature vectors corresponding to blocks are found by 2 Nearest Neighbors (2NN) test and Euclidean distance. In [2], Alkawaz, M. H., Sulong, G., Saba, T., & Rehman, A. suggested a method based on DCT coefficients. Firstly, RGB image is converted into grayscale domain and, then, the grayscale image is divided into overlying blocks. 2D DCT coefficients are calculated for each block and the duplicated block is located by the Euclidean distance. In [35], Zhao, F., Shi, W., Qin, B., & Liang, B. proposed a method, where the standard deviation is calculated for each block, and then the image is divided into layers according to the standard deviation value. The SIFT algorithm is used to detect each layer. The method with the automatic determination of decision threshold was presented in [30] by Ustubioglu, B., Ulutas, G., Ulutas, M., & Nabiyev, V. The image is firstly converted to the YCbCr color system, and then divided into overlapping blocks. The feature vectors are extracted for each block using DCT and the zig-zag scanning. In [28], Shih, F. Y., & Jackson, J. K. describe a method for CMFD, where the algorithm loads the grayscale image of resolution 256 × 256, then divides it into blocks for which either PCA (Principal Component Analysis) or DCT is performed. The calculated values obtained by PCA or DCT are compared, and the duplicated regions are found. Malviya, A. V., & Ladhake, S. A. in [22] presented a block-based method, where an input image is filtered in order to remove the noise, and then divided into blocks of dimension MxN. Each block is subject to 8Z affine transformation. The characteristics of each block are extracted by Auto Color Correlogram (ACC). In [19], Lee, J. C., Chang, C. P., & Chen, W. K. present a method based on a histogram of orientated gradients. The image is firstly divided into overlapping blocks of fixed size. The characteristics of each block are calculated using the Histogram of Gradient (HOG) descriptor. Similar blocks are searched, and the result is mapped to the image being tested. In [10], the authors Emam, M., Han, Q., & Niu, X., proposed a copy-move detection method with a combination of geometric transformations based on PCET. The image is firstly divided into overlapping blocks, and in each block PCET transformations are used to extract the characteristics. ANN Searching is used to identify similar blocks. In [1], Alahmadi, A., Hussain, M., Aboalsamh, H., Muhammad, G., Bebis, G., & Mathkour, H., proposed a method based on DCT and LBP. Firstly, the color image is converted into the YCbCr system and divided into overlapping blocks with 50% overlap. LBP operator is applied on each block and each LBP encoded block is then transformed into a frequency domain using DCT. The SVM is used to classify the coefficients. Hayat, K., & Qazi, T. [15] suggested a method based on DWT and DCT. The image is firstly converted to grayscale and then the DWT is applied. After applying the DWT, an image is divided into overlapping blocks, where DCT is applied to each block. Soni, B., Das, P. K., & Thounaojam, D. M. [29] proposed two methods based on the Local Binary Pattern Histogram Fourier features and Fast Walsh-Hadamard Transform features. Input image is first converted from RGB to grayscale domain, and divided into overlapping blocks of different size. In order to match similar blocks, the authors used Euclidean distance. In [25], Mohsen Jenadeleh and Mohsen Ebrahim Moghaddam proposed a method based on modified fractal coding and matching characteristic vectors. The image is firstly divided into overlapping blocks, and then the extraction of fractal coding features of each block is performed. These features are used for detection of the copied regions. Rani Susan Oommen, Jayamohan M. and Sruthy S. in [26] proposed a local Fractal Dimension (LFD) approach with applying the SVD. An image is firstly divided into blocks of fixed dimensions and for each block the local fractal dimension is estimated. In order to reduce the complexity, image blocks are arranged in B + tree, according to LFD values.

Although the above-mentioned methods detect forged image regions, their computational complexity is very large. Also, there is a high percentage of false positives that give miss-detection results.

Block-based methods use overlapping or non-overlapping blocks (windows) of a square shape for an image analysis. For each block, a characteristic feature vector is calculated, and then these vectors are compared in order to find duplicates in blocks. Most of the block-based methods work with blocks of size 8 × 8. What results will be obtained if we use blocks of other dimensions, for example 16 × 16 or 32 × 32?

The concepts to be considered when calculating the accuracy of forgery detection of image parts are: the number of correct detections (TP-True Positive), the number regarding incorrect detections as forged (FP-False Positive) and missed forgered regons (FN-False Negative).

In this paper, copy-move image forgery detection using multifractal spectrum and its characteristics, as well as common parameters like mean value and standard deviation corresponding to blocks, has been carried out to show how block size affects the forgery detection accuracy, as well as to analyze the impact of the block size on recall and precision. Having compared with other existing techniques, it is important to obtain two main advantages:

1) better performances in terms of FP and FN, i.e. recall and precision, and
2) lower dimension of the feature vector.

3 Multifractal spectrum

In multifractal process, two matrices are created: the Hölder exponent matrix α, which describes the local regularity of the image (pixels) being analyzed and the distribution matrix of these coefficients - the spectrum $f(\alpha)$ or the multifractal spectrum of the image [27]. The multifractal spectrum gives a global description of an image (or, more generally, the phenomenon being examined). The parameter α gives local signal information. The spectrum $f(\alpha)$ describes a signal globally. A signal from a local and a global point of view can be described based on the pair (α, $f(\alpha)$). The small values α denote poorly modified signal locally. The small values of $f(\alpha)$ indicate a phenomenon with a local value of α which is unlikely (it seldom occurs), and vice versa, for large $f(\alpha)$ [27].

The value of the Hölder exponent depends on the position in the structure and describes the local signal regularity. Namely, different objects in the image have different spectra, different positions of the maximum, which proved to be an interesting method for detecting changes in the images. Figure 2a and b give a simple example of an image and its changes, while Fig. 2c shows their multifractal spectra. In Fig. 2c, it can be clearly seen that there is a difference in the values of the multifractal spectrum and Hölder's exponent for the original image and its modification.

By simply calculating the multifractal spectrum of the original image and its modification and by extracting their characteristic features, it can be seen there is a difference in the calculated spectra, especially in the parts rounded up in the Fig. 2c. By analyzing the multifractal spectra for a large number of original and modified images, we have concluded that such differences are the main indicators that there has been a change in an image content. Therefore, these can be used as descriptors of the image blocks (Section 4).

4 Proposed method

In this paper, Copy-Move image forgery detection based on multifractal spectrum and its characteristics, as nonlinear parameters, as well as mean value and standard deviation of block pixels, has been carried out to explore the posibility of detection of forged parts in images and effect of block size on performance of tampered region detection in terms of FP and FN. We implemented the blocks of sizes 8 × 8, 16 × 16 and 32 × 32, in the proposed method. Figure 3 presents the diagram explaining algorithm proposed in this paper.

The experimental analysis is carried out in five steps.

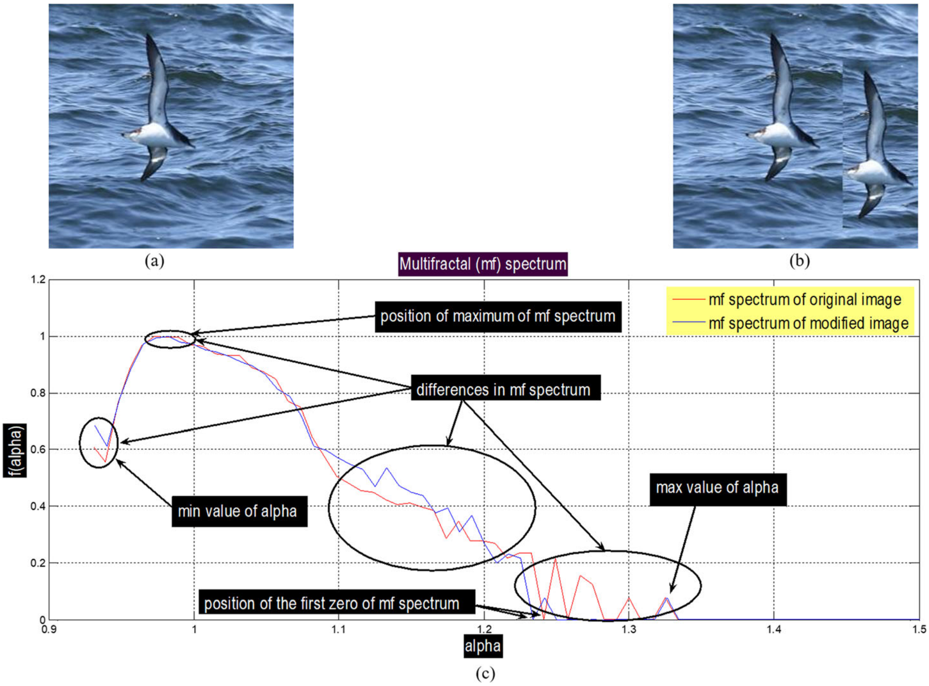

Fig. 2 The example of **a** original, **b** modified image and **c** their multifractal spectrum

Step 1: Preprocessing of an Image

The first step in our experiment is to convert the RGB input into the intensity image. Low frequency component features are considered more useful in the feature matching than high frequency components. Thus, the Gaussian low-pass filter is employed to reduce high frequency components. In this implementation, the filter size is 5 × 5 and the standard deviation of the filter is 0.5.

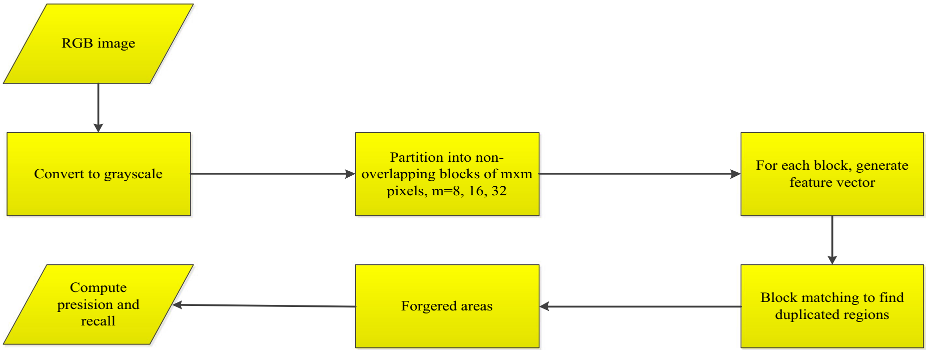
RGB image
Convert to grayscale
Partition into non-overlapping blocks of mxm pixels, m=8, 16, 32
For each block, generate feature vector
Block matching to find duplicated regions
Forgered areas
Compute presision and recall

Fig. 3 The algorithm of the proposed method based on multifractals

Next, the three color components are used to obtain a grayscale image based on the well-known Eq. (1):

$$X_{gray} = 0.299 \times R + 0.587 \times G + 0.114 \times B \tag{1}$$

where R, G and B are red, green and blue components of the image, respectively.

Step 2: Partition into non-overlapping blocks

After RGB to grayscale image conversion, the image is divided into non-overlapping square blocks of dimension mxm, for m = 32, 16, 8. For the purposes of testing, the resolution of the images is 256 × 256, which does not affect the generality, but allows a better transparency of the method. The method can be applied to arbitrary image resolution. Accordingly, each image is divided into 64, 256 and 1024 non-overlapping blocks, respectively. Figure 4 represents the division of an image into non-overlapping blocks.

Step 3: Feature extraction

The next step is feature extraction for each block of the image of interest. In the case of images modified by Copy-Move Method, the copied and pasted parts have similar structure, and a multifractal analysis can be applied, which basically analyzes the self-similarity. For each block, a multifractal spectrum is calculated by histogram method, described in detail in [27]. The descriptors used to generate feature vectors of blocks consist of two parts: multifractal and non-multifractal (or common statistical) descriptors. Multifractal descriptors are characteristics of multifractal spectrum: α_0 (the position of multifractal spectrum maximum), α_{min} and α_{max} (minimum and maximum value of Hölder's exponent), α_1 (the first zero, or the first minimum

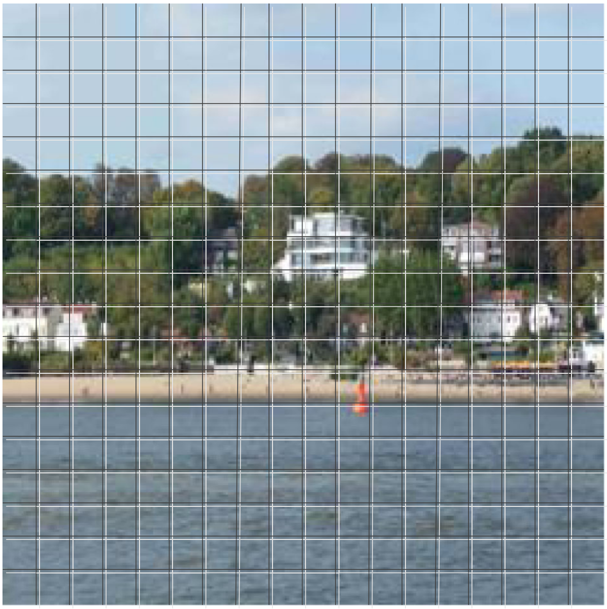

Fig. 4 The image division into non-overlapping blocks

value of $f(\alpha)$), the difference between α_1 and α_{min}, $\Delta = \alpha_1 - \alpha_{min}$ (Fig. 5), while linear descriptors are mean value and standard deviation of block pixels (Eqs. (2), (3) for the blocks of size 32 × 32, Eqs. (4), (5) for the blocks of size 16 × 16 and Eqs. (6) and (7) for the blocks of size 8 × 8).

$$\overline{x}_{32} = \frac{1}{1024}\sum_{i=1}^{1024} x_i \tag{2}$$

$$\sigma_{32}^2 = \frac{1}{1024}\sum_{i=1}^{1024}\left(x_i - \overline{x}_{32}\right)^2 \tag{3}$$

$$\overline{x}_{16} = \frac{1}{256}\sum_{i=1}^{256} x_i \tag{4}$$

$$\sigma_{16}^2 = \frac{1}{256}\sum_{i=1}^{256}\left(x_i - \overline{x}_{16}\right)^2 \tag{5}$$

$$\overline{x}_{8} = \frac{1}{64}\sum_{i=1}^{64} x_i \tag{6}$$

$$\sigma_{8}^2 = \frac{1}{64}\sum_{i=1}^{64}\left(x_i - \overline{x}_{8}\right)^2 \tag{7}$$

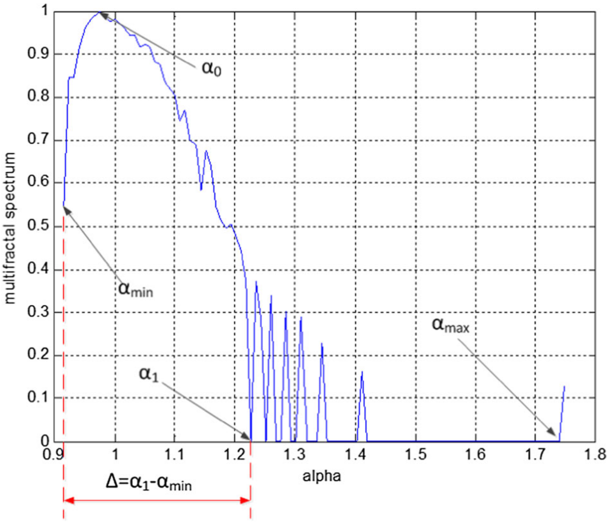

Fig. 5 The parameters of multifractal spectrum used as block descriptors

Step 4: Block matching

For the purpose of this research, a new sem-metric that can be used to compare the objests, has been developed $d : R^n \times R^n \rightarrow [0, +\infty)$, and it can be used to compare the objects (blocks) $x_i, x_j \in R^n$:

$$d(x_i, x_j) = \begin{cases} 0 & , \text{if } i = j \\ \frac{\sum_{k=1}^{n}\left(x_i^k - x_j^k\right)^2}{|i-j|} & . \text{if } i \neq j, i, j = 1, \ldots, m \end{cases} \tag{8}$$

where $x_i \left(x_i^1, x_i^2, \ldots, x_i^n\right)$ is a characteristic feature vector which describes the block with attributes $x_i^1, x_i^2, \ldots, x_i^n$, $i = 1, \ldots, m$, where m is the number of blocks, $n = 7$ is the number of descriptors for each block, and i and j represent the position of the image block.

Lemma: $d : R^n \times R^n \rightarrow [0, +\infty)$ defined with

$$d(x_i, x_j) = \begin{cases} 0 & , \text{if } i = j \\ \frac{\sum_{k=1}^{n}\left(x_i^k - x_j^k\right)^2}{|i-j|} & . \text{if } i \neq j, i, j = 1, \ldots, m, m \in N \end{cases}$$

is semi-metric.

Proof:

We prove the *symmetry* is true.

$\forall x_i, x_j \in R^n$ if $i = j$ the proof is trivial: $d(x_i, x_j) = 0 = d(x_j, x_i)$.

If $i \neq j$ then $d(x_i, x_j) = \frac{\sum_{k=1}^{n}\left(x_i^k - x_j^k\right)^2}{|i-j|} = \frac{\sum_{k=1}^{n}\left(x_j^k - x_i^k\right)^2}{|j-i|} = d(x_j, x_i)$.

Reflexivity: $\forall x_i \in R^n$ because $i = j$, $d(x_i, x_i) = 0$.

Identity of indiscernibles: $\forall x_i, x_j \in R^n d(x_i, x_j) = 0 \Longleftrightarrow i = j \Longleftrightarrow x_i = x_j$.

The lemma has been proved.

Also, we used interval [min, max], where min is the smallest value of all minimum values of semi-metric of changed blocks and both of the image databases [7, 16] (calculated using the formula (8)), and max represents the highest value of all the maximum values of semi-metric of the changed blocks from all the bases (calculated using the formula (8)). More precisely, it is $X_1, X_2, \ldots X_p$ finite number of sets (in this case-datasets of images) with finite elements $x_i \in X_k$, $i = 1, 2, \ldots, m_k$ and $k = 1, 2, \ldots, p$, $p, m_k \in N$. Let $\min = \min_{1 \leq k \leq p} d(x_i, x_j), x_i, x_j \in X_k$, where x_i, x_j are changed block vectors and $\max = \max_{1 \leq k \leq p} d(x_i, x_j), x_i, x_j \in X_k$, where x_i, x_j are changed block vectors. To make a decision, the cluster grouping is used only for blocks whose semi-metrics d from each other are in this interval [min, max].

Step 5: Extraction of forged areas

The Basic Variable Neighborhood Search (BVNS) [23, 24] applied in the problem of detection of changed blocks has been implemented in the following way. Firstly, the distances have been calculated (by using semi-metric) among blocks by applying formula (8). In preprocessing phase, the types of matric distances (and also the appropriate indexes of blocks) have been sorted in a non-declining order [11]. Then, the interval [min, max] is determined based on the process described in Step 4, and the blocks with distances in this interval have only been observed. This data is used for more efficient implementation of the shaking operator. Indeed, since every solution is characterized by the centroid set, the shaking operator is replaced with the appropriate number of centroids. More precisely, shaking in the neighborhood means that centroids are to be replaced by accidently chosen blocks that are not centroids, and they are the most distant from k-th place of the the centroid they change (centroids are actually blocks). In each step replacement of all centroids is considered, and there will not be any replacement if an accidently chosen blocks are the closest to the centroid (actually it is the centroid itself). Local searching consists of a systematic replacement of one centroid with the block that is not a centroid. This starts from the solution gained by shaking, and it is performed in line with the principle of the best improvement, as long as there is an improvement [12].

With a pseudo-code, BVNS can be presented in the following way [12]:

- Initialization. Choose the starting solution $x \in X$ and define the stopping criteria STOP = 0
- Repeat {

- $i = 1$
- Repeat
- {

- Shaking () – Generate the accidental solution $x'y^i$ in the neighborhood from x.
- Local searching () – mark with x'', gained local minimum by applying some of the procedures of the local searching starting from x'.
- Checking of the solution () – If a local minimum is better than the current minimum, it should be moved to the solution, i.e. $x = x''$.
- Continue to the new starting solution in the neighborhood $i = 1$

Otherwise, move to the next surrounding, i.e. $i = i + 1$.

If a stopping criterion is satisfied, set the value STOP = 1.

- } until it is $i = i_{max}$ or STOP = 1

- } until it is STOP = 1

4.1 Performance measurement

The performance measurement focuses on the accuracy, which is described in the following. Precision signifies the probability for the correct forgery of the detected blocks as forgery, whereas recall determines the probability of forged blocks in the set of images being detected (Eqs. (9) and (10)). True positive (TP) represents the number of tampered blocks, which are classified as tampered, false positive (FP) represents the number of authentic blocks, which are classified as tampered, and false negative (FN) represents the number of tampered blocks, which are classified as authentic.

$$\text{Precision} = \text{TP}/(\text{TP} + \text{FP}) \tag{9}$$

$$\text{Recall} = \text{TP}/(\text{TP} + \text{FN}) \tag{10}$$

5 Experimental results and discussion

In this section, the experimental results are presented to verify the accuracy performance of the proposed method. The implemented method is evaluated by utilizing the images from publicly available CoMoFoD dataset and Image Manipulation Dataset [7, 16]. CoMoFoD and Image Manipulation Dataset present common datasets for benchmarking the detection of image tampering artefacts [7, 16]. CoMoFoD dataset consists of 200 images: 100 original images and 100 tampered images, while Image Manipulation Dataset consists of 48 base images [7, 16]. The standard image size has been set as 256 × 256. The tampered images have been generated by copying and pasting image parts. The parts of images can be geometrically transformed before pasting them, by applying scaling and rotation. The pasted regions can vary in size (small, medium and large). In this paper, the results for 10 (of 100 used in the research) images are presented. In each of these images, one or more regions are copied. Also, the size of the copied regions varies among the images. Original and forged images and its ground truth, indicating the forged area, are shown in Figs. 6 and 7.

This research has implemented the block-based copy-move image forgery detection approach using multifractal spectrum for non-overlapping blocks of different size. Figure 8 presents the forgery detection results for the first set of tested images (images from Fig. 6), for different block sizes (32 × 32, 16 × 16 and 8 × 8), while Fig. 9 presents forgery detection results for the second set of tested images (images from Fig. 7), also for different block sizes.

The detection accuracy performance of the implemented method is calculated in terms of precision and recall for images from CoMoFoD and Image Database datasets [7, 16]. Each of

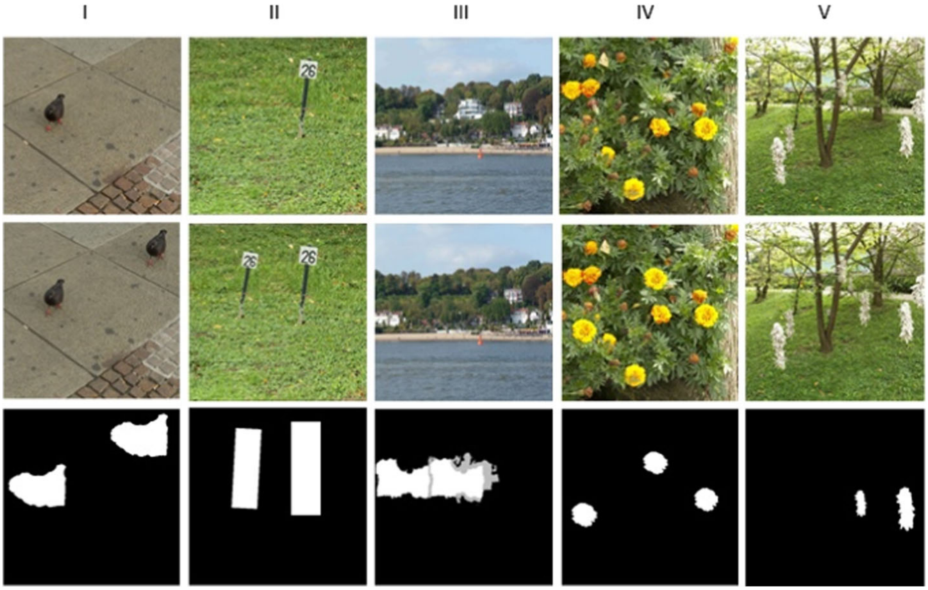

Fig. 6 The first five examples for Copy-Move forgery: original images (the first row), the corresponding tampered images (the second row), and ground truth maps (the third row)

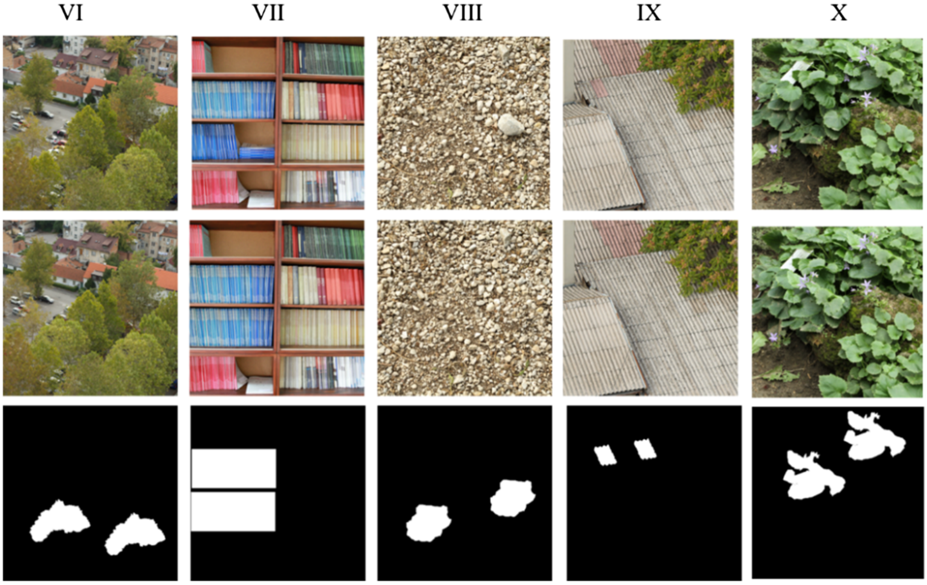

Fig. 7 The second five examples for Copy-Move forgery: original images (the first row), the corresponding tampered images (the second row), and ground truth maps (the third row)

the input images is tested to analyze the effects of different non-overlapping block size on the accuracy performance for the forgery detection, in terms of precision and recall. The described algorithm, along with the proposed semi-metric for the similarity, has been implemented in the C# programming language. Success of the classification of the defined semi-metric is shown by comparing the results with paper [2], for block size of 8 × 8, and for images from CoMoFoD dataset [7] (I, II, IV, V, VI, VII, VIII, IX and X). The success rates are given in Table 1. Table 2 shows the results for the same set of images, only for block size of 16 × 16.

For the purpose of testing our method, an image from the Image Dataset with a more complicated structure (containing sky, forest, sea, sand, buildings) is also tested. The results obtained for the image III are shown in Tables 1 and 2, for different block sizes. The image numeration in Tables 1 and 2 represents the order number associated with images in Figs. 6 and 7, respectively.

From Table 1, we can see that significantly better results are obtained in terms of precision and recall for images denoted by I, IV,V, VI, VII, VIII and X, especially in the term of precision in the case of Images IV,V,VI, VII, IX and X. Also, the results obtained for Image II are relatively satisfying in term of precision, as well as results obtained for image IX, in term of recall.

The results presented in Table 2 show high accuracy percentage for the forgery detection, in terms of precision and recall. In comparison with the results shown in Table 1, we can conclude that greater accuracy is obtained by applying blocks of size 16 × 16, for the same set of tested images.

Considering the results obtained for Image III (Tables 1 and 2), we can conclude that our method gives fairly good results, even when the tested image is of more complex content. In this case, it is better to use blocks of smaller dimensions (higher accuracy is obtained using blocks of size 8 × 8 comparing to size 16 × 16).

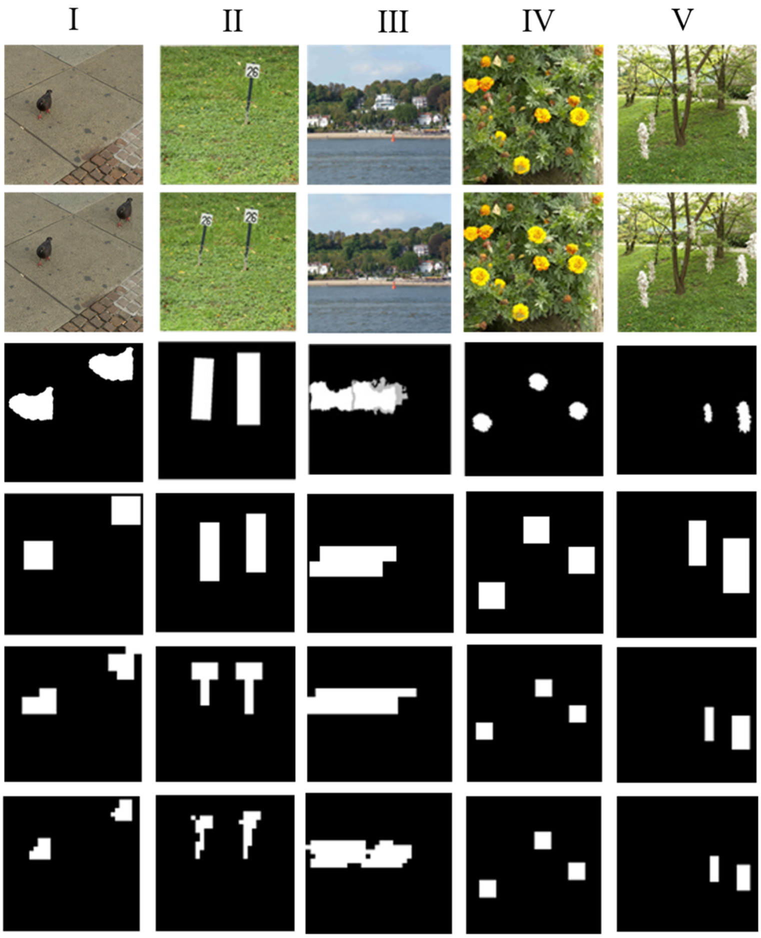

Fig. 8 The first five examples for Copy-Move forgery detection: original images (the first row), the corresponding modified images (the second row), ground truth maps (the third row), forgery detection for 32 × 32 non-overlapping blocks (the fourth row), forgery detection for 16 × 16 non-overlapping blocks (the fifth row) and forgery detection for 8 × 8 non-overlapping blocks (the sixth row)

In order to compare the performance of our method with the performance of other authors' methods, we use- measure performance parameters for the accuracy of the proposed algorithm: correct detection ratio (CDR), used by authors in [6], and defined as follows:

$$\mathrm{CDR} = \frac{\text{The detected tampered region}}{\text{The tampered region}} \tag{11}$$

as well as the correct detection ratio F_C and the false detection ratio F_f, used by autors in [19], and defined as follows:

$$F_C = \frac{\left|\mu \cap \mu^C\right| + \left|\omega \cap \omega^C\right|}{|\mu| + |\omega|} \tag{12}$$

$$F_f = \frac{\left|\mu^C - \mu\right| + \left|\omega^C - \omega\right|}{\left|\mu^C\right| + \left|\omega^C\right|} \tag{13}$$

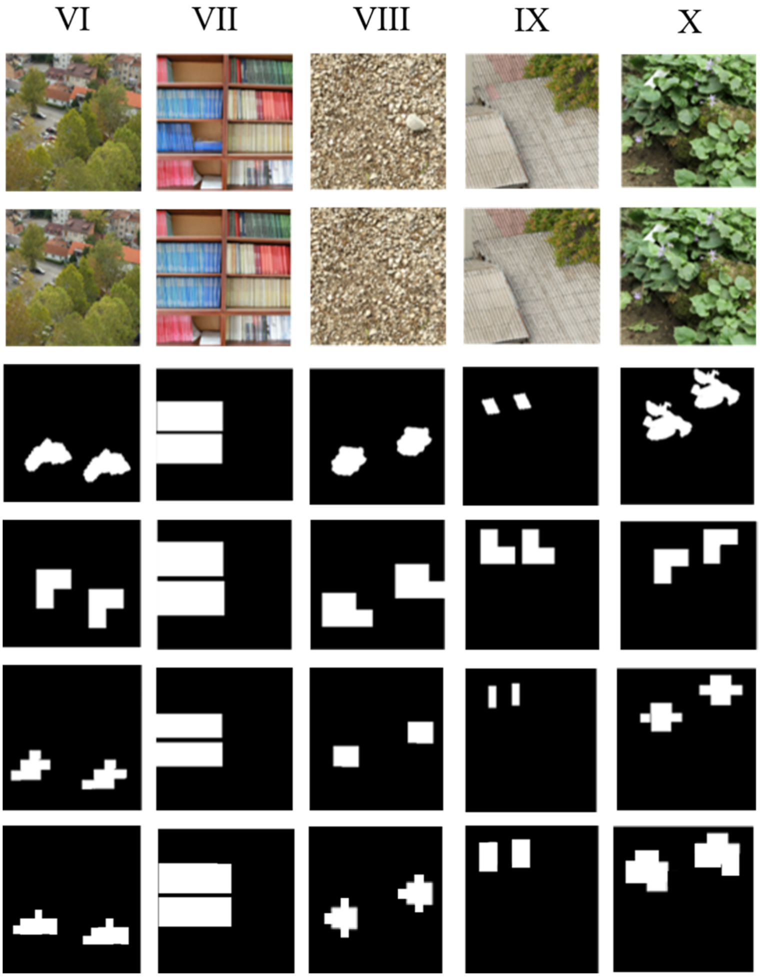

Fig. 9 The second five examples for Copy-Move forgery detection: original images (the first row), the corresponding modified images (the second row), ground truth maps (the third row), forgery detection for 32 × 32 non-overlapping blocks (the fourth row), forgery detection for 16 × 16 non-overlapping blocks (the fifth row) and forgery detection for 8 × 8 non-overlapping blocks (the sixth row)

where μ and ω denote pixels in original region and corresponding forgery region respectively, and μ^C and ω^C denote pixels of original region and forgery region respectively, $|\ \ |$ refers to the area of the region, ∩ refers to the intersection of two regions, and – refers to the difference between two regions [19]. The ratio F_C indicates the performance of the algorithm in correct locating the pixels of copy–move regions in the tampered image, while F_f reflects the percentage of pixels that were false positives (i.e. incorrectly identified as forgeries) [19]. In other words, the two values indicate the precision with which the proposed algorithm locates copy–move regions. The closer F_C is to 1 and F_f is to 0, the more precise the method is [19].

In the Table 3 the comparison results between the results obtained in [6] and the proposed approach are given in the terms of CDR, for Image II in the case of the blocks of size 16 × 16

Table 1 Precision-recall performance of 8 × 8 block size in percentage (%), for images I, II, III, IV, V, VI, VII, VIII, IX and X

Image	Experimental results			
	Results from paper [2]		Obtained results by the proposed approach	
	Precision (%)	Recall (%)	Precision (%)	Recall (%)
I	87.62	99.48	91.67	100
II	100	97.53	95.83	97.87
III	Not available at [2]	Not available at [2]	100	98.33
IV	26.58	94.85	73.08	95
V	63.32	88.47	81.48	95.65
VI	59.25	98.68	86.95	99.56
VII	49.80	100	92.36	100
VIII	95.19	96.25	97.36	97.36
IX	62.53	97.30	89.32	96.35
X	41.49	93.37	95.48	96.65

and 32 × 32. Table 4 shows the results of the comparison with the results obtained in [19], in terms of F_C and F_f, for Images II, V, VI and VII, for the blocks of size 16 × 16, while Table 5 shows the same results for the blocks of size 32 × 32.

From Table 3, we can see that we get better results in terms of CDR in the case of block size 16 × 16. But results obtained in the case of block size 32 × 32 are worst, in comparation with results obtained in [6]. The proposed algorithm gives better results for blocks sizes of 16 × 16 than block sizes 32 × 32 because some portions of the forged regions are so small and they cannot be detected by using larger block sizes. From Table 4, we can see that we get significantly better results in terms of F_C and F_f for Image II, VI and VII, for the block of size 16 × 16. Also, the results obtained for Image V are relatively satisfying in terms of F_C and F_f. From Table 5, we can see we get significantly better results in terms of F_C and F_f for Image II, V and VII, for the block of size 32 × 32.

The computational complexity is one of the most important issues in CMFD, which is affected by the number of descriptors for each block (the dimensionality of selected feature vector). In other words, computational complexity can be minimized by finding a method to reduce the dimensionality of feature vectors.

Table 2 Precision-recall performance of 16 × 16 block size in percentage (%), for images I, II, III, IV, V, VI, VII, VIII, IX and X

Image	Experimental results	
	Precision (%)	Recall (%)
I	93.75	100
II	100	100
III	93.55	96.67
IV	76.74	97.06
V	84.61	91.67
VI	99.19	99.19
VII	99.16	100
VIII	100	99.59
IX	99.60	99.60
X	100	100

Table 3 Accuracy CDR performance in the case of 16 × 16 and 32 × 32 block size, for Image II

Image	Block size	Experimental results	
		Results from paper [6] CDR	Obtained results by the proposed approach CDR
II	16 × 16	0.991	1
II	32 × 32	0.974	0.8

In this paper, we used multifractal spectrum and its parameters, as well as standard statistical parameters, to generate feature vector for each block. In our experiments, feature vector for each block is 7-dimensional. Table 6 shows the efficacy of the proposed technique against other existing methods. Compared with [2, 5, 6, 8, 15, 21, 33], the dimension of the feature vector is lower, which implies that the proposed technique has a lower computational complexity.

The goal of this research is to study the effects of different block size (8 × 8 pixels, 16 × 16 pixels) on the performances in terms of FP and FN. By comparing the results, the results shown in Tables 1 and 2, we can conclude that the block size affects both the precision and the recall. Also, a better accuracy is obtained for the block size of 16 × 16. This is the consequence of using blocks of larger dimension blocks that give more data to calculate the multifractal spectrum, and therefore we get a good representation.

By analyzing the obtained results, it can be seen that our method yields significantly better results in the terms of precision and recall, compared to the results obtained in [2] (Table 1), for images denoted by I, IV, V, VI, VII, VIII, IX and X, especially in term of precision in the case of Images IV, V, VI, VII, IX and X. Also, the results obtained for Images II and IX are relatively satisfying in terms of precision and recall. In the case of a more complicated image structure (containing sky, forest, sea, sand, buildings) the proposed method gave fairly good results (Tables 1 and 2). In that case, it is better to use blocks of smaller dimensions (better accuracy is obtained using blocks of size 8 × 8 comparing to size 16 × 16). Compared to other authors who analyzed the same images [6], we obtained better results in the terms of the CDR, for Image II and the blocks of size 16 × 16 (Table 3). In the terms of F_C and F_f, for Image II, VI and VII, we obtained significantly better results, for the block of size 16 × 16. The results obtained for the Image V are relatively satisfying, in comparison to [19] (Table 4). From Table 5, we can conclude that we get better results in terms of F_C and F_f, for Images II, V and VII, for block of size 32 × 32. Also, reults obtained form image II are relatively good.

Table 4 AccuracyF_C and F_f performance in the case of 16 × 16 block size, for Images II, V, VII and VIII

Image	Experimental results			
	Results from paper [19]		Obtained results by the proposed approach	
	F_C	F_f	F_C	F_f
II	0.898	0.154	1	0
V	0.996	0.003	0.988	0.049
VI	0.976	0.012	0.988	0.004
VII	0.992	0.011	0.993	0.015

Table 5 AccuracyF_C andF_f performance in the case of 32 × 32 block size, for Images II, V, VII and VIII

Image	Experimental results			
	Results from paper [19]		Obtained results by the proposed approach	
	F_C	F_f	F_C	F_f
II	0.922	0.107	0.953	0.625
V	0.976	0.015	100	0
VI	0.966	0.016	0.953	0
VII	0.958	0.06	100	0

Based on Tables 1,2, 3, 4 and 5, we can conclude that the method proposed in this paper gives excellent results for the blocks of size of 8 × 8 and 16 × 16, while the results for the larger blocks are fairly good. We should point out that most of the compression techniques use 8 × 8 or 16 × 16 blocks, which are important for high detailed images. Thus, in order not to lose changes done in small regions, the most important detections should be based on 8 × 8 and 16 × 16 blocks. Results detected by 32 × 32 blocks may be very good as well for detection of changes in large images. By using the small blocks (for instance, 4 × 4), in the detection algorihtm, it is possible that large changes could stay undetected. On the contrary, huge blocks, such as 32 × 32 or larger, may omit very small changes. So, for CMFD we suggest to use 16 × 16 blocks. Additional check could be done by using larger blocks if the image is of extremely high resolution.

The second aspect important for the development of new CMFD methods is computational complexity, which is affected by the number of descriptors for each block (the dimensionality of characteristic feature vector). In our experiments, characteristic vector for each block is 7-dimensional. Compared with other methods (Table 6), the dimension of the feature vector is lower, which implies that our proposed method has a lower computational complexity.

6 Conclusions

Nowdays high-tech but low-cost tehnology enables to easy create and change image content, add and/or remove some information within an image, or even to make a new image out of two or more images. Among artistic and personal use, for creating different contents from existing images, changes in image content can be a part of criminal activities. Thus, the development of methods for detecting such changes has become very important demand. One of the most

Table 6 Comparisonof computational complexity

Methods	Extraction algorithm	Feature vector dimensionality
[6]	LGWP	256
[5, 33]	SIFT	128
[2]	DCT	64
[21]	DWT, DCT	64
[15]	Improved DWT, DCT	10
[8]	PCET	8
Proposed method	Multifractal spectrum and statistic parameters	7

researched methods is the copy-move forgery detection (CMFD) one. In this paper, a novel method for CMFD, based on multifractal spectrum and its parameters, common statistical parameters and the new metaheuristic method and semi-metric is proposed here. Clustering as inherent part of the proposed metahuristic method is experimentaly comfired. The results show high degree of success on the specific issues presented in the paper. Compared with the results in literature, the proposed method has achieved better results in terms of precision and recall as a figure of merits. It should be pointed out that the dimensionality of the feature vector used in our approach is lower compared with those used in other methods, leading to lower computational complexity. In further research, besides the algorithm proposed in this paper, new metaheuristic and supervised learng methods, as well as other multifractal based parameters are going to be developed and compared.

Acknowledgements This work has been supported by the Serbian Ministry of Science, Grant nos. III044006, III44009 and TR32023.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

1. Alahmadi A, Hussain M, Aboalsamh H, Muhammad G, Bebis G, Mathkour H (2017) Passive detection of image forgery using DCT and local binary pattern. SIViP 11(1):81–88. https://doi.org/10.1007/s11760-016-0899-0
2. Alkawaz MH, Sulong G, Saba T, Rehman A (2016) Detection of copy-move image forgery based on discrete cosine transform. Neural Comput & Applic:1–10. https://doi.org/10.1007/s00521-016-2663-3
3. Bi X, Pun CM (2018) Fast copy-move forgery detection using local bidirectional coherency error refinement. Pattern Recogn 81:161–175. https://doi.org/10.1016/j.patcog.2018.03.028
4. Bi X, Pun CM, Yuan XC (2016) Multi-level dense descriptor and hierarchical feature matching for copy–move forgery detection. Inf Sci 345:226–242. https://doi.org/10.1016/j.ins.2016.01.061
5. Bi X, Pun CM, Yuan XC (2018) Multi-scale feature extraction and adaptive matching for copy-move forgery detection. Multimed Tools Appl 77(1):363–385. https://doi.org/10.1007/s11042-016-4276-3
6. Chou CL, Lee JC (2017) Copy-Move Forgery Detection Based on Local Gabor Wavelets Patterns. In: International Conference on Security with Intelligent Computing and Big-data Services (pp. 47-56). https://doi.org/10.1007/978-3-319-76451-1_5
7. CoMoFoD database, available at: http://www.vcl.fer.hr/comofod. Accessed March 2018
8. Emam M, Han Q, Niu X (2016) PCET based copy-move forgery detection in images under geometric transforms. Multimed Tools Appl 75(18):11513–11527. https://doi.org/10.1007/s11042-015-2872-2
9. Gan Y, Chung J, Young J, Hu Z, Zhao J (2018) A Duplicated Forgery Detection Fusion Algorithm using SIFT and Radial-Harmonic Fourier Moments. International Journal of Performability Engineering 14(1): 111. https://doi.org/10.23940/ijpe.18.01.p12.111120
10. Gan Y, Zhong J (2016) Application of AFMT method for composite forgery detection. Nonlinear Dynamics 84(1):341–353. https://doi.org/10.1007/s11071-015-2524-0
11. Glisovic N, Davidovic T, Bojovic N, Kenzevic N Statistical and Mathematical Methods for Solving the Problem of Clustering of Station Data When Data Is Incomplete, Conference: XXXV Symposium on New Technologies in Postal and Telecommunication Vehicles, PosTel 2017. Traffic Faculty, Belgrade
12. Glisovic N, Davidovic T, Raskovic M (2017) Clustering when missing data by using the variable neighborhood search, (in serbian). In: Proc. SYM-OP-IS 2017, pages 158-163, Zlatibor
13. Gong J, Guo J (2016) Image copy-move forgery detection using SURF in opponent color space. Transactions of Tianjin University 22(2):151–157. https://doi.org/10.1007/s12209-016-2705-z
14. Guo Y, Cao X, Zhang W, Wang R (2018) Fake Colorized Image Detection. IEEE Transactions on Information Forensics and Security 13(8):1932–1944. https://doi.org/10.1109/TIFS.2018.2806926
15. Hayat K, Qazi T (2017) Forgery detection in digital images via discrete wavelet and discrete cosine transforms. Comput Electr Eng 62:448–458. https://doi.org/10.1016/j.compeleceng.2017.03.013

16. Image Manipulation Dataset, available at: https://www5.cs.fau.de/research/data/image-manipulation/. Accessed April 2018
17. Jenadeleh M, Ebrahimi Moghaddam M (2016) Blind detection of region duplication forgery using fractal coding and feature matching. J Forensic Sci 61(3):623–636. https://doi.org/10.1111/1556-4029.13108
18. Kaushik R, Bajaj RK, Mathew J (2015) On image forgery detection using two dimensional discrete cosine transform and statistical moments. Procedia Computer Science 70:130–136. https://doi.org/10.1016/j.procs.2015.10.058
19. Lee JC, Chang CP, Chen WK (2015) Detection of copy–move image forgery using histogram of orientated gradients. Inf Sci 321:250–262. https://doi.org/10.1016/j.ins.2015.03.009
20. Lin CS, Tsay JJ (2016) Passive forgery detection using discrete cosine transform coefficient analysis in JPEG compressed images. Journal of Electronic Imaging 25(3):033010. https://doi.org/10.1117/1.JEI.25.3.033010
21. Mahmood T, Mehmood Z, Shah M, Saba T (2018) A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform. J Vis Commun Image Represent 53:202–214. https://doi.org/10.1016/j.jvcir.2018.03.015
22. Malviya AV, Ladhake SA (2016) Pixel based image forensic technique for copy-move forgery detection using auto color correlogram. Procedia Computer Science 79:383–390. https://doi.org/10.1016/j.procs.2016.03.050
23. Mladenović N, Hansen P (1997) Variable neighborhood search. Comput Oper Res 24(11):1097–1100
24. Mladenović N, Sörensen K, Souza M (eds) (2018) Special issue on "Advances in Variable Neighborhood Search". Int Trans Oper Res 25(1):427–427
25. Mohsen J, Mohsen E-M (2016) Blind Detection of Region Duplication Forgery Using Fractal Coding and Feature Matching. J Forensic Sci 61(3). https://doi.org/10.1111/1556-4029.13108
26. Oommen RS, Jayamohan M, Sruthy S (2016) Using Fractal Dimension and Singular Values for Image Forgery Detection and Localization. Procedia Technology 24:1452–1459. https://doi.org/10.1016/j.protcy.2016.05.176
27. Reljin I, Reljin B, Pavlovic I, Rakočevic I (2000). Multifractal analysis of gray-scale images. In: Electrotechnical Conference, 2000. MELECON 2000. 10th Mediterranean (Vol. 2, pp. 490-493). IEEE
28. Shih FY, Jackson JK (2015) Copy-Cover Image Forgery Detection in Parallel Processing. Int J Pattern Recognit Artif Intell 29(08):1554004. https://doi.org/10.1142/S021800141554004X
29. Soni B, Das PK, Thounaojam DM (2018) Dual System for Copy-move Forgery Detection using Block-based LBP-HF and FWHT Features. Eng Lett 26(1). https://doi.org/10.1109/TIFS.2010.2051666
30. Ustubioglu B, Ulutas G, Ulutas M, Nabiyev VV (2016) A new copy move forgery detection technique with automatic threshold determination. AEU-International Journal of Electronics and Communications 70(8): 1076–1087. https://doi.org/10.1016/j.aeue.2016.05.005
31. Wang XY, Liu YN, Xu H, Wang P, Yang HY (2018) Robust copy–move forgery detection using quaternion exponent moments. Pattern Anal Applic 21(2):451–467. https://doi.org/10.1007/s10044-016-0588-1
32. Yan Y, Ren W, Cao X (2019) Recolored Image Detection via a Deep Discriminative Model. IEEE Transactions on Information Forensics and Security 14(1):5–17. https://doi.org/10.1109/TIFS.2018.2834155
33. Yang B, Sun X, Guo H, Xia Z, Chen X (2018) A copy-move forgery detection method based on CMFD-SIFT. Multimed Tools Appl 77(1):837–855. https://doi.org/10.1007/s11042-016-4289-y
34. Zhang W, Cao X, Qu Y, Hou Y, Zhao H, Zhang C (2010) Detecting and extracting the photo composites using planar homography and graph cut. IEEE Transactions On Information Forensics And Security 5(3): 544–555. https://doi.org/10.1109/TIFS.2010.2051666
35. Zhao F, Shi W, Qin B, Liang B (2017) Image forgery detection using segmentation and swarm intelligent algorithm. Wuhan University Journal of Natural Sciences 22(2):141–148. https://doi.org/10.1007/s11859-017-1227-4
36. Zhong J, Gan Y (2016) Detection of copy–move forgery using discrete analytical Fourier–Mellin transform. Nonlinear Dynamics 84(1):189–202. https://doi.org/10.1007/s11071-015-2374-9
37. Zhong J, Gan Y, Young J, Huang L, Lin P (2017) A new block-based method for copy move forgery detection under image geometric transforms. Multimed Tools Appl 76(13):14887–14903. https://doi.org/10.1007/s11042-016-4201-9
38. Zhong J, Gan Y, Young J, Lin P (2017) Copy Move Forgery Image Detection via Discrete Radon and Polar Complex Exponential Transform-Based Moment Invariant Features. Int J Pattern Recognit Artif Intell 31(02):1754005. https://doi.org/10.1142/S0218001417540052
39. Zhou Z, Wang Y, Wu QJ, Yang CN, Sun X (2017) Effective and efficient global context verification for image copy detection. IEEE Transactions on Information Forensics and Security 12(1):48–63. https://doi.org/10.1109/TIFS.2016.2601065
40. Zhu Y, Shen X, Chen H (2016) Copy-move forgery detection based on scaled ORB. Multimed Tools Appl 75(6):3221–3233. https://doi.org/10.1007/s11042-014-2431-2

Aleksandra Pavlović is currently PhD student at the Department of Telecommunications and information technologies, at School (Faculty) of Electrical Engineering, University of Belgrade and Teaching Assistant at State university of Novi Pazar. She received her dipl.ing (four year university) degree in electrotechnical engineering, and her Master degree in electrotechnical engineering and computer science at the Department of Telecommunications and information technologies, at School (Faculty) of Electrical Engineering, University of Belgrade. Her research interest include digital image processing, telecommunications, thermovison, signal and image processing, information theory, audio systems. She is the author of more than thirty research publications.

Natasa Glišović is currently an assistant of the Department of Mathematical Science, State University of Novi Pazar. She received the Ph.D. in the Mathematical Faculty, University of Belgrade. Her research interests include mathematic applied, clustering, metaheuristic, metrics, optimization, fuzzy logic, statistical and numerical methods, time cost tradeoff. She is on the project Mathematical Institute of the Serbian Academy of Sciences and Arts, PROJECT III 044006, Development of new information and communication technologies, based on advanced mathematical methods, with applications in medicine, telecommunications, power systems, protection of national heritage and education.

Ana Gavrovska is currently Assistant Professor at School (Faculty) of Electrical Engineering, University of Belgrade. She received her dipl.ing (five year university) degree in electrotechnical engineering, and her PhD degree in electrotechnical engineering and computer science at the Department of Telecommunications and information technologies, at School (Faculty) of Electrical Engineering, University of Belgrade. Her research interest include linear and nonlinear methods, multimedia, television and telemedicine systems, signal and image processing, video technologies, and telecommunications. She is the author of more than eighty research publications and a book.

Irini Reljin received the degree (5-year university degree), M.S., and the Ph.D. degrees in electrical engineering, all from the Faculty of Electrical Engineering (FEE) University of Belgrade, where she has been selected for full professor. Since 2001 she has been teaching the multimedia and video technologies at undergraduate studies, as well as linear and non-linear signal analysis and multimedia processing at graduate studies. She has published over 350 journal and papers presented on scientific conferences, as well as several book chapters. She has given a number of invited lectures on different aspects of communications, signal and image processing, fractal and multifractal analyses, content-based indexing, and retrieval. She has participated in a number of scientific and research projects in the areas of telecommunications, multimedia, and telemedicine. Her research interests are in video and multimedia analyses, digital image processing, neural networks, statistical signal analysis, fractal and multifractal analyses. She has been responsible for technical issues of transition from analog to digital broadcasting, as well as digital dividend planning in the Republic of Serbia. She is a Member of the IEEE, SMPTE (Society of Motion Pictures and Television Engineers), BSUAE (Trans Black Sea Union of Applied Electromagnetism), Gender Team, as well as several national societies.

Affiliations

Aleksandra Pavlović[1,2] • **Natasa Glišović**[2] • **Ana Gavrovska**[1] • **Irini Reljin**[1]

[1] Telecommunications Department, School of Electrical Engineering, University of Belgrade, Bulevar kralja Aleksandra 73, Belgrade 11020, Serbia

[2] Department of Technical Sciences, State University of Novi Pazar, Vuka Karadzica, Novi Pazar 36300, Serbia