Multimedia Tools and Applications (2023) 82:1431–1456
https://doi.org/10.1007/s11042-022-12391-4

An improved reduced feature-based copy-move forgery detection technique

Shubham Kumar[1] · Soumya Mukherjee[1] · Arup Kumar Pal[1]

Received: 20 March 2021 / Revised: 20 December 2021 / Accepted: 25 January 2022 /
Published online: 18 March 2022

Abstract

With Widespread malpractice of copy-move image forgery, enforcing image forensics becomes imperative. In this approach, objects can be added into or removed from the same image to hide the truth with malicious intention. In order to address this issue, passive copy move forgery localization and detection has been playing a crucial rule in image forensics arena. The paper proposed a reduced feature-based algorithm which is robust as well as highly accurate in terms of detecting forged area. In this proposed scheme, stationary wavelet transform is employed on subject image to obtain low approximation band, and then significant features are extracted from it using block-based Discrete Cosine Transformation (DCT) and singular value decomposition (SVD) accordingly. Traditional block-based approach suffers from computational overhead especially for large images. Proposed scheme, extracts only three feature vectors, one DC component applying DCT on LL bands and two singular value components extracted employing SVD from the remaining AC components of each transformed block. These reduced features are further utilized for analysing and matching to detect identical regions in an image. In spite of having a smaller number of features, experimental results exhibit, this proposed scheme detects the forged area precisely as well as exhibits quality robustness against different post- processing attacks.

Keywords Copy-move forgery · Image forensics · SWT · SVD planes

✉ Soumya Mukherjee
mukhsoumya@gmail.com

Shubham Kumar
kumarshub18@gmail.com

Arup Kumar Pal
arupkrpal@gmail.com

[1] Department of Computer Science and Engineering, Indian Institute of Technology (Indian School of Mines), Jharkha, Dhanbad nd-826004, India

1 Introduction

Image has profound importance in our life. The Evolvement of computation and widespread use of hand-held devices make photography easier. But the abundance of various image-editing tools makes image forgery an easygoing even for the newbies. As photography editing [4] becomes a new normal, image forgery turns invasive and makes it difficult to judge the genuineness of the image. A single image may contain huge information as well as stating a factor describing an incident flawlessly in various spheres of life like newspaper reporting, judiciary, insurance claim, research result, etc. On the other hand, doctored image act to the contrary and jeopardized the innocence and importance of photography. In order to restore the faith of images, image forensics is a pressing need to deal with the image forgery and trace out tampered area of the subject image successfully.

Image forgery is broadly classified into three categories: i. Splicing ii. Copy Move Forgery iii. Image Retouching. In splicing [15, 18] a composite image is generated by copying a part of an image and pasted into another image. On the other hand, copy move forgery [6, 22] is an image manipulation process in which single or multiple areas of an image are moved into the other parts to hide or exaggerate objects present in the same image. This type of forgery has a higher degree of sophistication as the changes in the underlying statistics and entropy of the image is very little. These changes are also imperceptible to the human eyes. Figure 1 illustrates image duplication using copy-move forgery. Image retouching [22] is an image manipulation technique in which image properties or attributes are changed by some post processing technique. Therefore, to cope with this type of forgery, passive image forgery techniques become immensely popular and challenging. To unveil copy-move forgery in an efficient way, a novel method has been proposed.

Image forensic technique is categorized into two ways: 1. Active Image forensics 2. Passive image forensics. In active image forensics [22], pre-set data like digital signature or digital watermark has been embedded into the image and extracted from the image at the time of requirement and further the watermark can be checked whether the image has undergone any manipulation or not. The main challenge lies in active image forensics is that watermark or digital signature must be inserted into the image at the time of image capturing.

But there are thousands of images which was taken earlier and no watermark was embedded into it. In this scenario, active forensics fail to judge the integrity and authenticity

Fig. 1 Copy-Move Forgery Example, (**a**) *Original Image* (**b**) *Forged Image*

of the same. To prevail over this situation, passive forensics [15, 18], which requires no pre-employed data, has been engineered for image forgery detection. In passive image forensics (also known as blind image forensics), the underlying anomalies and statistics of the subject image are investigated and tampered region is localized. In view of its unparalleled advantage, passive forensics become a much-coveted research area among scientific communities.

Owing to the might and efficiency of the blind image forensics technique, the authors proposed a passive forensics scheme that aims to bring out copy move forgery using block-based technique. In this approach, stationary wavelet transform (SWT) is utilized with discrete cosine transform (DCT) along with singular value decomposition (SVD) in order to extract DC coefficients and most significant singular values from the image. Later on, these features are exploited to detect copy move forged region from the subject image. The proposed algorithm reduces the feature vector size significantly by choosing salient but reduced number of features from each block while preserve robustness against any post-processing attack.

The primary contributions of this proposed research work are as follows. First, various issues and limitations in copy move forgery detection techniques are hashed out and to surmount the problem, a new hybrid but substantially reduced feature-based image forensic method has been proposed proosed. In order to produce the coveted feature vectors, SWT, DCT and SVD transformations are applied. Due to shift invariant property of SWT, energy compaction nature of DCT and high stability of SVD; the extracted features exhibit a greater degree of robustness despite low number of feature vectors. It's worth mentioning that only three feature vectors are extracted per block which successfully localizes the forged area and using such a reduced number of feature vectors is the first of the kind. Second, the proposed algorithm can detect forged region successfully irrespective of its number i.e. single or multi forged area as well as irrespective of the size of the forged area specially if the area is small, can be detected successfully. Third, from various experimental results and comparative analyses display the robustness and accuracy of the proposed scheme is sufficiently good.

The reaming part of this paper is structured as follows. Section 2 introduces the state of art techniques for copy move forgery techniques. Section 3 gives an overview of various transformation techniques applied in this paper in the preliminary section. Section 4 describes the details of the proposed work and the algorithmic approach. Experimental results and performance evaluation along with robustness and comparative analysis are described in section 5. Finally, the conclusion of the proposed scheme is drawn in section-6.

2 State of the art

The copy-move forgery detection methods [28] are mainly categorized as (a) Block based technique and (b) Keypoint based technique. In block-based technique [10], an image is partitioned into overlapping or non-overlapping blocks which are further exploited to extract features and analysis, and after that identical features are used to find the forged area. Key point based [16] approaches scanned the high entropy regions of an image in order to extract feature vectors from these areas only. These feature vectors have gone through proper processing for identification of duplicate regions. Keypoint based approaches have the advantage of taking less processing time but with a shortfall of less accuracy. On the other hand, block-based approaches are more time consuming but have the greater accuracy rate. A brief description of various forgery detection techniques is presented here.

It has been stated that copy-move forgery detection process widely used block-based technique. In order to detect forged region in an image, Fridrich et al. [10] pioneered the block-based method using two approaches, named exact match and robust match. Exact match used exact pixel value from the images to form feature vectors, which suffers from lossy compression. While robust match used quantized DCT based feature vector collecting approach, which overcomes the lossy image compression problem. In Alkawaz et al. [1], the author proposed a solution by following same features used by Fridrich et al. [10] but with.

8 × 8 block size. Both the algorithms have limitations of high computational complexity. Later on, Popescu and Fraid [9], proposed a feature extraction method from block using principal component analysis (PCA) coefficients to achieve robustness. Xiao Bing Kang and Wei [13] proposed an SVD based technique to extract singular values from the image. For similarity matching and filtering process, the author utilized Euclidian distance and Chebyshev distance. The technique displayed robustness under post processing attacks like compression, Gaussian blurring and Bayram et al. [3] also gave a feature extraction process using SVD. This method reduced the computational complexity required for matching after lexicographical sorting. This proposed method proved its robustness against noise distortion, lossy JPEG compression and Gaussian blur. Zhang et al. Zhang et al. [15] used DWT to extract sub-bands from the forged image. The Proposed method uses phase correlation to test similarity. In Zhao and Guo [30], utilized DCT and SVD transformation accordingly to extract most significant feature vectors from the image to achieve robustness. In Hayat and Qazi [12], implement DWT-DCT based forgery detection technique. This process extracted approximation band by applying DWT on image thereafter DCT is applied to extracted overlapping block of approximation subband. Zandi et al. [29] proposed a solution using adaptive similarity threshold. This method successfully detects forged regions applying thresholds proportional to standard deviation. In Lee et al. [14], designed a technique using Histogram Oriented Gradients (HOG) for copy move forgery detection. The method depends upon the statistical feature for overlapping blocks. The experiment results show effectiveness against some post-processing operation as well as robustness against slight rotation attack. Mahmood et al. [17] proposed a very effective approach by using SWT which has shift invariant property and reduce the dimensions by deploying DCT. This technique extracted only six feature vectors which demonstrates good result under various post processing attacks. Singh et al. [23] devised a DCT-SVD based technique for feature vector extraction and further support vector machine classifier is employed for classification and K- means clustering is employed to localize copy move forged area. Meena and Tyagi [19] designed a tetrolet based CMFD algorithm for feature extraction and used the filter outlier technique to detect tampered regions with robustness and accuracy. Dixit et al. [8] devised a blur invariant forgery detection technique utilizing SWT-SVD. A colour-based segmentation technique is used to attain blur invariant. Soni et al. [24] suggested a SURF (Speeded Up Robust Feature) and MSER based image forensics which is geometric transformation invariant. Recently Al-Qershi and Khoo [2] designed a *k*-means clustering -based forgery detection algorithm. Nonetheless, it's a challenge for the scientific community and researchers to find a solution to trade- off between robustness and time complexity to produce optimum results. To surpass this challenge, in this paper authors proposed an effective and robust image forensics technique that utilizes SWT, DCT, and SVD techniques which successfully defends the principal cause of image forensic technique.

3 Preliminaries

The proposed technique in this paper requires the basic knowhow for the concepts of DCT, SWT, and SVD. The details of these techniques are given below.

3.1 Discrete cosine transform (DCT)

DCT [21] is a mathematical technique by which an image can be transformed from spatial to transform domains by generating DCT coefficients. DCT has enormous applications in various science and engineering domain (like JPEG, MPEG etc.). The most significant attribute of DCT is, it has energy compaction property that signifies the salient information of a signal is stored in lower frequency band which further can be exploited to compress any multimedia file. As most of the salient features are intact, the quality of data still maintained. This makes it worthy in scientific application where trade- off between dimension reduction and quality maintenance is crucial. For $M \times N$ pixels block of image: where (x, y) represents image coordinates in the spatial domain and (r, s) represents coordinates in transform domain such that x, y ∈ [0....M − 1] r, s∈ [0....N − 1].

$$H(r,s) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} h(x,y)[\alpha(r)]\,[\alpha(s)] cos\left[\frac{(2x+1)r\pi}{2M}\right] \cos\left[\frac{(2y+1)s\pi}{2N}\right]$$

$$where$$

$$\alpha(r) = \sqrt{\frac{1}{M}}\, if\ r = 0, \sqrt{\frac{2}{M}}\, if\ r = 1, 2, \ldots..M{-}1 \tag{1}$$

$$\alpha(s) = \sqrt{\frac{1}{N}}\, if\ s = 0, \sqrt{\frac{2}{N}}\, if\ s = 1, 2, \ldots..N{-}1$$

3.2 Singular value decomposition (SVD)

SVD [5] is an immensely popular matrix factorization technique with its wide range of application areas in image processing. SVD refactors the image into three matrices, using which various algebraic and geometric features can be extracted easily. SVD features in the form of a matrix. Let A be a matrix of an image with $A \in R^{m \times n}$ of rank r, which has m rows and n columns ($m \times n$). Using SVD the image can be factorized into U, S, and V, and is represented as

$$A = USV^T \tag{2}$$

where, U represents a $m \times m$ orthogonal matrix contains orthonormal Eigenvectors of AA^T which can be represented as $U \in R^{n \times n}$, S is a $m \times n$ diagonal matrix contains the diagonal matrix of the singular values, which represents square roots of Eigenvalues of AA^T, and V represents $n \times n$ orthogonal matrix contains the orthonormal Eigenvectors of A^TA *which can be represented as* $V \in R^{m \times m}$.

$$\mathrm{U} = [u_1\ u_2 \cdots u_\mathrm{n}] \tag{3}$$

where, column vectors u_i form an orthonormal set and $i = 1, 2, 3...m$ and matrix V depicts an n × n orthogonal matrix

$$V = \begin{bmatrix} {v_1}^T \\ {v_2}^T \\ \vdots \\ {v_n}^T \end{bmatrix} \tag{4}$$

where, column vectors from v_i from an orthonormal set and $i = 1,2,3,\ldots n$.

$$A = [u_1 u_2 \cdots u_n] \begin{bmatrix} \sigma_1 & 0 \cdots & 0 \\ 0 & \sigma_2 \cdots 0 \\ \vdots & \vdots \ddots & \vdots \\ 0 & 0 & \cdots \sigma_n \end{bmatrix} \begin{bmatrix} {v_1}^T \\ {v_2}^T \\ \vdots \\ {v_n}^T \end{bmatrix} \tag{5}$$

The singular value of SVD is consistent and can represent an image with lesser dimension. From several experiments, it has been observed that larger singular values can represent the significant features of an image and smaller ones has less significant features. In Eq. (5), σ_1, $\sigma_2 \ldots \sigma_n$ are singular values, constitutes square roots of Eigenvalues forming the diagonal of S. The singular values in the matrix A arranged in a descending order i.e. $\sigma_1 > \sigma_2 > \ldots > \sigma_n$. Analyzing the attributes, SVD successfully used for dimension reduction as well as maintains its energy substantially. It also has less computational complexities compare to other transformation technique. Considering the quality attributes of SVD, proposed technique equipped with it and utilized to extract quality feature vectors from AC coefficients.

3.3 Stationary wavelet transformation (SWT)

Wavelet transformation has huge potential application in various image processing operations. But the wavelet transforms suffer from the decimation of coefficients in each stage of decomposition which leads to shift variance problem. Due to the shift variance property, even a little change in the image makes a huge impact on the Discrete Wavelet Transform (DWT) coefficients. This phenomenon may bring set back in forgery investigation as it generates different feature vectors from the same copy moved area due to shift variance by post processing attack. Hence, to overcome this lacuna, SWT has been introduced. SWT [7, 20, 25] has shift invariant property, which exhibits greater degree of pattern recognition, edge detection, and feature extraction capacities, which are further exploited by the investigator for copy, move forgery detection. SWT coefficients are obtained in a similar fashion of DWT decomposed by low pass *l[x]* and high pass filter *h[x]* illustrated in Fig. 2. Lowpass filter *l[x]* generates *LL* and *LH* sub bands, on the other hand, filter *h[x]* produced *HL* and HH sub bands. But, unlike DWT no decimation operation is performed on it hence, all the sub bands contain same size of the original image I_i. Hence, an image of size$N \times M$, N × Mwhere $E = 1, 2, 3 \ldots \ldots, N$ and $F = 1, 2, 3 \ldots, M$. The sub image *LH*, *HL*, *HH*, and *LL* denote horizontal, vertical, diagonal and approximation sub-band of equal size respectively got by the image of size $N \times M$ the SWT decomposition at i^{th} level is expressed from Eqs. (6)–(9). After obtaining the aforementioned sub-bands, approximation *LL* sub-band has been chosen for feature extraction in order to form feature vectors, which are further utilized to find copy move forgery. It's worth mentioning that the feature extracted from approximation sub-band has not only reduced dimensions but provides greater saliency which leads to higher withstanding capacity against various post-processing attacks.

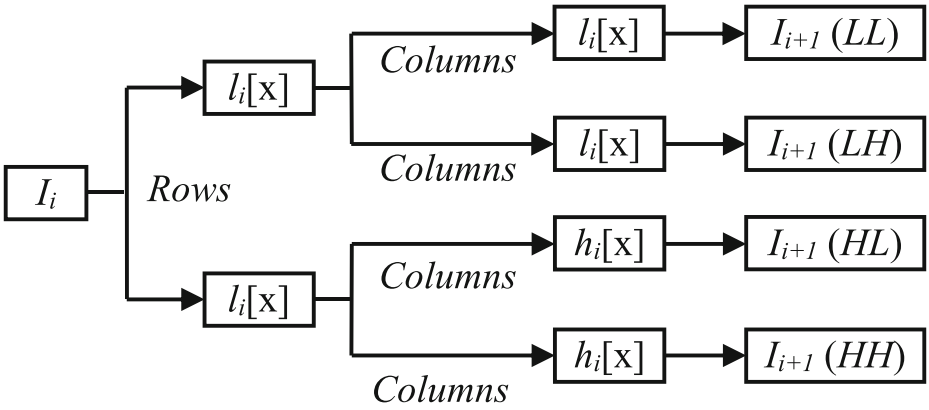

Fig. 2 Decomposition Process of an image through SWT

$$LH_{i+1}(E,F) = \sum_{x=-\infty}^{+\infty} \sum_{y=-\infty}^{+\infty} l_x^i h_x^i LL_i(E+x, F+y) \tag{6}$$

$$HH_{i+1}(E,F) = \sum_{x=-\infty}^{+\infty} \sum_{y=-\infty}^{+\infty} h_x^i h_y^i LL_i(E+x, F+y) \tag{7}$$

$$LL_{i+1}(E,F) = \sum_{x=-\infty}^{+\infty} \sum_{y=-\infty}^{+\infty} l_x^i l_y^i LL_i(E+x, F+y) \tag{8}$$

$$HL_{i+1}(E,F) = \sum_{x=-\infty}^{+\infty} \sum_{y=-\infty}^{+\infty} h_x^i l_y^i LL_i(E+x, F+y) \tag{9}$$

where E = 1,2,3……, N and F = 1,2,3…., M. The sub image *LH*, *HL*, *HH*, and *LL* denote horizontal, vertical, diagonal and approximation sub-band of equal size respectively generated from image of size $N \times M$.

4 Proposed work

The procedure proposed in this research work detects and localize copy-move forged area in digital images using hybrid features and utilizing only three feature vectors in order to reduce the computational overhead. This approach utilizes of SWT, DCT, and SVD for the feature extraction process from the pre-processed image. After conversion of colour image, applying the SWT decomposition on the luminance channel (Y). Then, the approximation band is selected from four sub-bands (approximation, horizontal, diagonal, vertical) for block-based CMF detection method. The reason for adopting SWT is, it has impressive localization and shift invariance properties in both spectral and spatial domains [20]. DCT is employed to each overlapping block on approximation band to select salient features and to reduce the feature

dimensionality. The reason behind picking the DC coefficient of a transformed block is, it contains significant information. This feature has been exploited and used as a first feature of a block as DCT concentrates information in lower spatial frequency domain. Further, SVD is deployed on each transformed block to extract the second feature on the next four AC coefficients through a zigzag scan on the transformed block. To obtain the second feature of the block, the first diagonal value of the singular matrix has been selected. The third feature is the first diagonal value of the singular matrix, which is obtained by applying the SVD on zigzag scanned next sixteen AC coefficients of transformed block. These three feature vectors are extracted from each block and considered for further process of CMF detection and localization. The algorithmic details are described in section 5.1.

4.1 Algorithmic steps

The essence of various steps involved in detecting and localization of copy-move forgery is described in this section. Figure 3 shows the overview of the entire algorithm. Input: *I*-Colour image or grayscale image of size $M \times N$. Output: *BI*- Binary image.

Step 1: Convert *I* into *Y* using the using below formula if *I* colour image else mark *I* as *Y*.

$$Y = \left(\frac{77}{256}\right)R + \left(\frac{150}{256}\right)G + \left(\frac{29}{256}\right)B \tag{10}$$

Step 2: Apply SWT decomposition on Y gives four sub bands: - approximation, horizontal, diagonal, vertical.
Step 3: Divide approximation band into $b \times b$ size overlapping blocks and generate $t = (M - b + 1) \times (N - b + 1)$ blocks.

$$F_m = \begin{bmatrix} f_1^1 f_2^1 f_3^1 x^1 y^1 \\ f_1^2 f_2^2 f_3^2 x^2 y^2 \\ \ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots \\ f_1^t f_2^t f_3^t x^t y^t \end{bmatrix} \tag{11}$$

Step 4: For each block B_i apply Feature Extraction algorithm which gives three features and (x, y) top left spatial location of block B_i, let it call $f_1^i, f_2^i, f_3^i, x_i, y_i$and construct feature matrix F_m of size t × 5 and each row represents i^{th} block's feature extracted from block B_i where ($1 \leq i \leq t$). Depicted at Fig. 4.
Step 5: Apply column normalization by formula giving in Eq. (12) on first, second and third column of feature matrix F_m get converted into F'_m. In Eq. (12), X_{min}, X_{max} and X represents minimum, maximum and real value of corresponding column. For each value it transforms to the new value X in range of [0, 1].

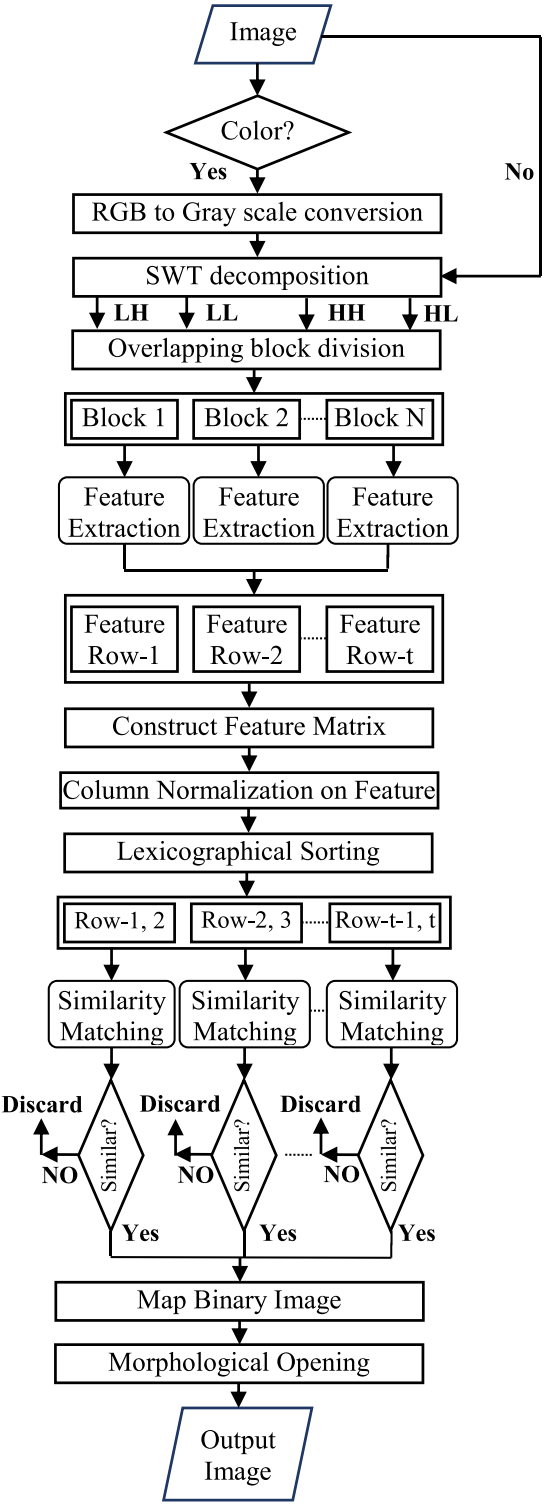

Fig. 3 Workflow of the proposed Algorithm

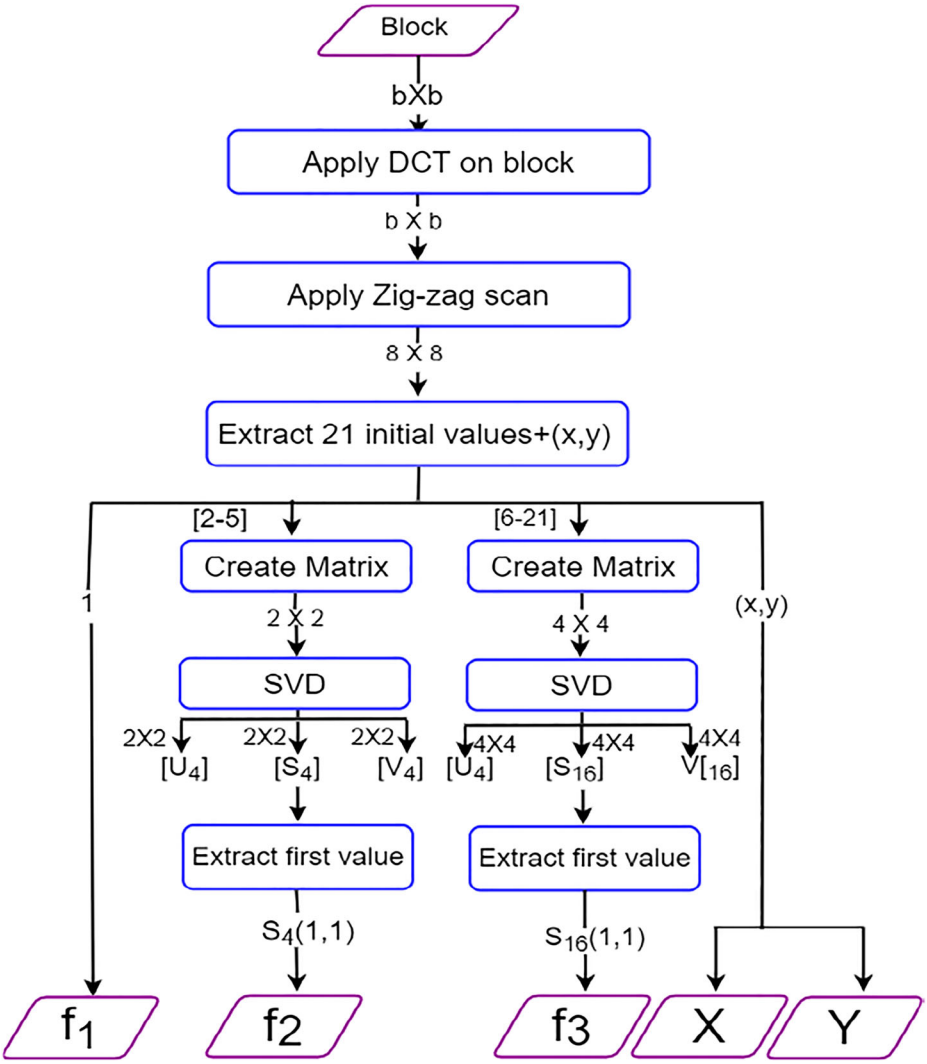

Fig. 4 Feature extraction process from a block

$$X' = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \tag{12}$$

Step 6: Apply lexicographical sorting on F'_m to obtain the transformed matrix F_s.
Step7: Apply Similarity Matching algorithm for each consecutive row pair of matrix F_s and find x and y coordinates of matching block pair's (B_k, B_l). Store the results obtained from Similarity Matching algorithm in another matrix O_s. Detail is illustrated in Fig. 5.
Step 8: For each row O_s consist two blocks top left corner x and y coordinates, let it say (B_k, B_l). Generate the binary image BI of size $M \times N$ by labeling the pixels corresponding to both block pairs (B_k, B_l) with:

$$B_i^{(x_g, y_h)} = \{1\} \forall x_i \leq x_g < x_{i+b} \text{ and } y_i \leq y_g < y_{i+b}$$

where x_i top left x coordinate of block B and $y_{i.}$ top left corner of y coordinate of block $B_i B_i$.

Step 9: Apply Morphological opening operation on BI with structural element sphere of radius b if suspicious regions in mapped binary image BI.
Step10: Output BI as result.

4.2 Feature extraction

Input: $\boldsymbol{B_f}$ Block of size $b \times b$. (x, y): coordinate of top left corner block.
Output: Feature f_1, f_2, f_3 and block left corner location (x, y).

Step1: Apply DCT on $\boldsymbol{B_f}$ gives $B_{DCT} B_{DCT}$ of same size.
Step 2: Follow zigzag scan on B_{DCT} and extract initial twenty one values for further, naming it $DC, AC_1, AC_2, AC_3, AC_{20}$.
Step 3: Create matrix M_4 of size 2×2 and matrix M_{16} of size 4×4.

$$M_4 = \begin{bmatrix} AC_1 AC_2 \\ AC_3 AC_4 \end{bmatrix} M_{16} = \begin{bmatrix} AC_5 AC_6 AC_7 AC_8 \\ AC_9 AC_{10} AC_{11} AC_{12} \\ AC_{13} AC_{14} AC_{15} AC_{16} \\ AC_{17} AC_{18} AC_{19} AC_{20} \end{bmatrix} \tag{13}$$

Step 4: Apply SVD on M_4 and M_{16} gives $U_4, V_4, S_4, U_4, S_4, V_4$ and U_{16}, V_{16}, S_{16} matrices respectively.
Step 5: Declare outputs DC as f_1, $S_4(1, 1)$ as f_2 and S_{16} (1, 1) as f_3, top left of x-coordinate and y coordinate of block B_f as x and y.

4.3 Similarity matching

Input: K_i- i^{th} Feature row of 1×5. K_j-j^{th} Feature row of 1×5, $i \neq j$ and $j = i + 1$. D_b-Block distance threshold,
S_b-Similarity threshold. Output: x_i, y_i, x_j, y_j - x and y coordinates of matching pairs.

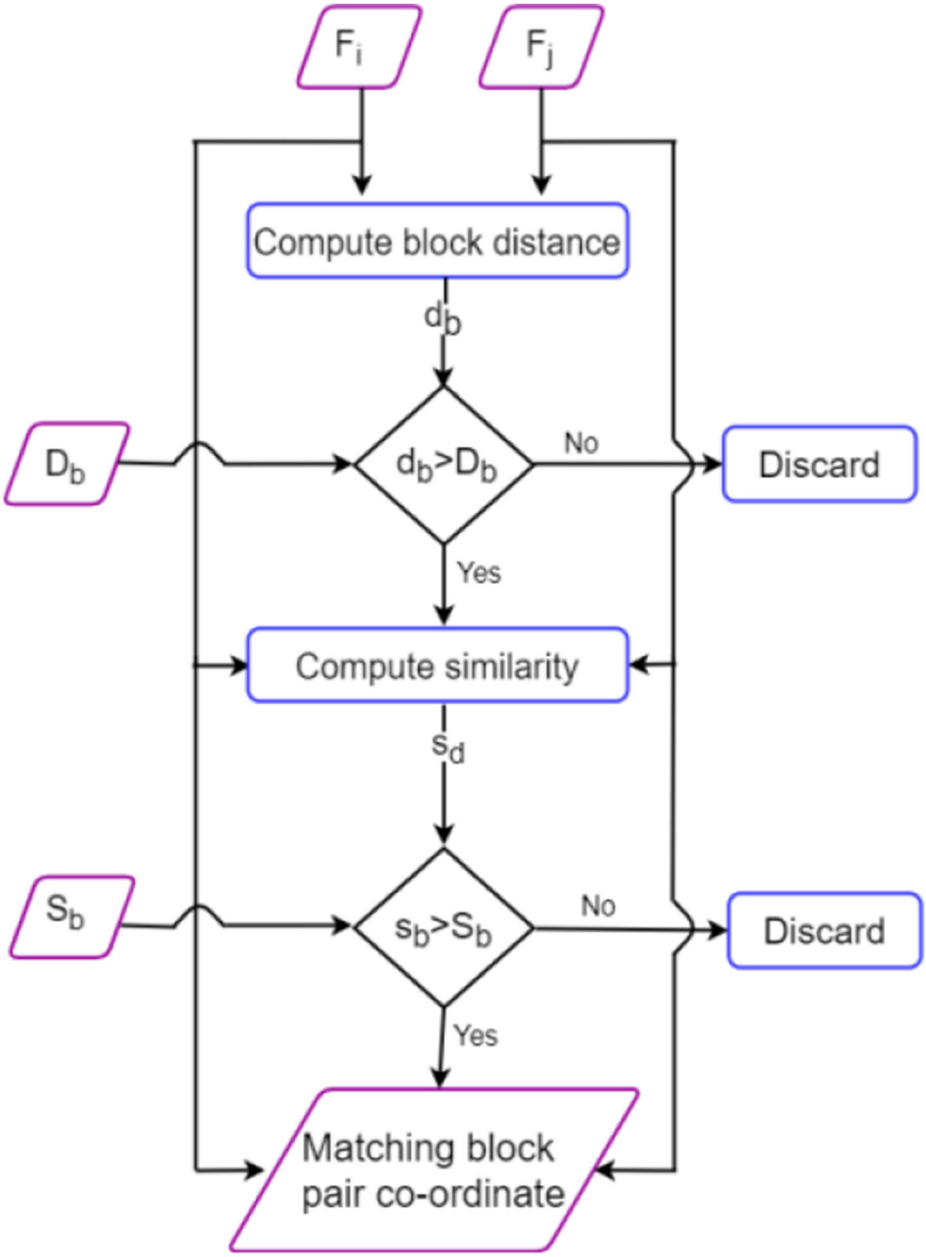

Fig. 5 Feature Similarity Algorithm Process

Step 1: Compute block distance using Eq. (14):

$$d_b = \sqrt{\left(K_{(i,4)} - K_{(j,4)}\right)^2 + \left(K_{(i,4)} - K_{(j,4)}\right)^2} \tag{14}$$

Step 2: If $d_b > D_b$ then go to Step 3 else go to Step 6.

Step 3: Compute similarity between feature using Eq. (15):

$$S_b = \sqrt{\sum_{g=1}^{3} \left(K_{(\mathrm{i,g})} - K_{(\mathrm{j,g})}\right)^2} \tag{15}$$

Step 4: If $s_b < S_b$ then go to step 5 else go to Step 6.
Step 5: Declare outputs $K_{(i,4)}$ as x_i, $K_{(i,5)}$ as y_i, $K_{(j,4)}$ as x_j and $K_{(j,4)}$ as y_j.
Step 6: Abort.

5 Experimental results and discussion

This segment is devoted to discussing various experiments performed on the proposed algorithm. To assess the robustness and exhibit the effectiveness of the developed solution for CMF, CoMoFD [27] image database has been utilized as well as forgery on natural image was created by the authors, comprising both the forged images with its ground truth. CoMoFD comprises 200 images of size 512 × 512 pixels. The experiments were accomplished on Intel® Core™ i-54,210 U CPU @ 1.70GHz processor with 4GB RAM running MATLAB 2018b.In order to measure the performance of the proposed forgery detection and localization some images have been forged and created ground truth of the same. To check the result, authors forged images with irregular and regular shaped tampered regions. To evaluate the robustness of the proposed technique, some post processing operation was employed on it.

Section 5.1 states the parameter set up for the proposed method. Section 5.2 and 5.3 demonstrate the performance evaluation metrics and simulation results respectively. Section 5.4 describes the effectiveness test. Testing of robustness and comparisons has been illustrated in sections 5.5 and 5.6 respectively.

5.1 Parameter setup

In section 4.1 and 4.2, b describes block size. In the similarity matching algorithm, D_b and S_b were used for block distance threshold and block feature similarity threshold respectively.

In the experiments, these parameters were set to $b = 8$, $D_b = 40$, and $S_b = 0.000001$. Various experiments were carried out using these parameters for the proposed method. The morphological opening operation is used as optional for images because sometimes image may not need post- processing. Morphological opening operation suggested using if suspicious regions found in the mapped binary image. The structural element used in the proposed method is sphere to reduce FPR.

5.2 Performance evaluation metrics

The proposed algorithm's performance is analyzed in this paper using various metrics at pixel level [26] are computed by the following mathematical Eqs. (17), (18), (19), (20), and (21).

True Positive (TP): Actually, altered detected pixels.

True Negative (TN): Actually, original pixel detected.

False Negative (FN): Pixels detected as original but that are actually altered
False Positive (FP): Pixels detected as altered but that are actually original

3.1.1 ***Forgery Detection Accuracy (ACC):*** This metric is used to determine the extent correct localization of forged pixels. Higher accuracy value (close to 1) indicates that the method has the capability to differentiate the altered and unaltered pixels of an image.

$$\mathrm{ACC} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FN} + \mathrm{FP}} \tag{16}$$

3.1.2 ***False Positive Rate (FPR) [31]:*** This metric depicts the rate of detecting the unaltered image pixels as forged is entitled as false positive rate. Lower value of FPR (close to zero) is favored.

$$FPR = \frac{FP}{FP + TN} \tag{17}$$

3.1.3 ***Precision [31]:*** Precision indicates the correctness of the detected portion of an image. The higher value (close to 1) implies greater degree of correctly classification of localized block.

$$Precision = \frac{TP}{TP + FP} \tag{18}$$

3.1.4 ***Recall [31]:*** Recall implies the magnitude of rightly identification of forged blocks in an image. A higher value (close to 1) indicates the most of the actual forged blocks are identified as forged.

$$Recall = \frac{TP}{TP + FN} \tag{19}$$

3.1.5 ***F1-measure:*** F1- measure demonstrates harmonic mean of precision and recall. It is used to strike a balance between precision and recall specially when there is large number of true negatives. The value of F1-Measure lies between 0 and 1 and the higher

value of it indicates higher precision of tampered region and proper discern between original and forged region.

$$F1\text{–}Measure = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{20}$$

5.3 Simulation results

Experiments were conducted on various natural images of different size 512 × 512, 1024 × 1024. Simulations were done on these images which are forged using GIMP2.10.12 (GNU Image Manipulation Program). Three of some reproduced images tampering localization results are displayed in Fig. 6(d)-(f) on applying the proposed method. Fig. 6(a)-(c) shows the altered images of "Tree", "Grass" and "Pole" of size 512 × 512, 512 × 512, and 1024× 1024 using the GIMP editing tool. Fig. 6(d)-(f) shows the localization results obtained by employing the proposed CMFD scheme on the tampered images of "Tree", "Grass" and "Pole" respectively. Fig. 6(d) is an image of duplicate tree shows accuracy = 0.9899 and FPR = 0, Fig. 6(e) shows the localization result on irregular shaped tampered area with accuracy = 0.9965 and FPR = 0 and Fig. 6(f) localization result with accuracy = 0.9988 and FPR = 0.0001, however, "pole" image is the size of 1024 × 1024.The localization achieved when no morphological opening operation was applied, shows effective results with only three feature vector size even when the size of the image increased. Image "Tree" displays the forgery with

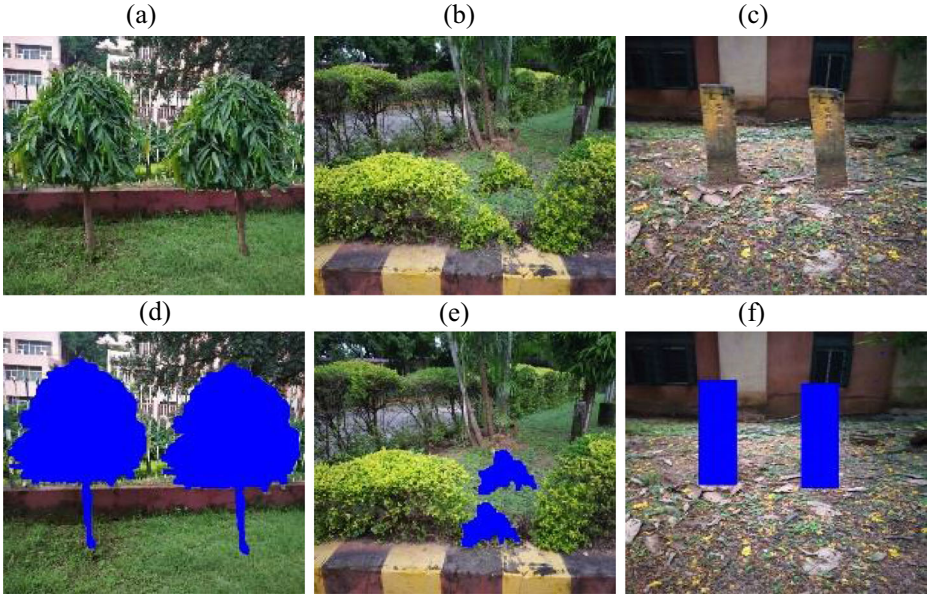

Fig. 6 Localization results on regular shaped region images

the large irregular area; image "grass" shows the forgery with the small irregular area, and image "pole" shows the forgery with the regular shaped area.

5.3.1 Effectiveness and accuracy results

In order to check the effectiveness and accuracy of the proposed algorithm, various experiments were done on translation tampering from CoMoFoD [27] dataset images. In translation operation, the copied region easily moves from one to another location of the image.

It is important in block-based forgery detection method to evaluate the performance on regular shaped, irregular shaped and multiple duplicated regions because it impacts the accuracy as well as false positive rate. In this part, three experiment results are carried out without any post-processing operation on tampered image. The first experiment is done to visualize the results of a regular-shaped copied region forgery. In Fig. 7(a-c) upper row showing the forged image of the regular shaped region whereas bottom row Fig. 7(d-f) showing duplicate regions with their accuracy and false positive rate.

The second experiment was performed on irregular shaped copied region fraud images to check the impact of the developed algorithm. The experimental results are shown in three different irregular shaped regions. Figure 8(a)-(f) shows tampered images and forgery localization respectively with their accuracy and false positive rate.

The third experiment is done on multiple tampered regions. This type of forgery localization is one of the core issues in CMFD algorithm. The detection results are shown in three different images. Figure 9(a)-(c) displays the tampered images when a copied region is pasted in multiple places in the same image whereas Fig. 9(d)-(f) illustrates the results of forgery detection with their accuracy and false positive rate.

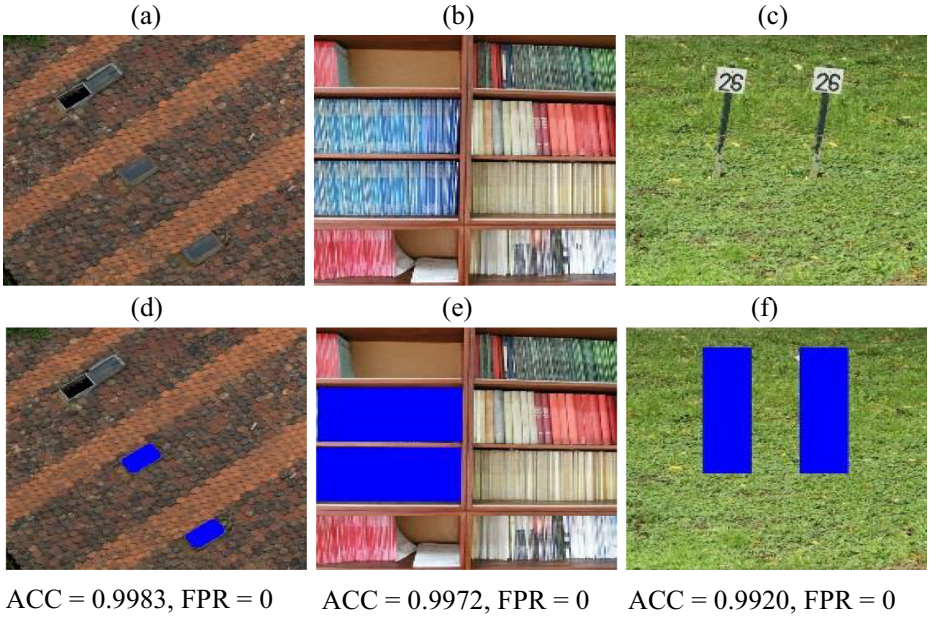

Fig. 7 Localization results on regular shaped region tampered images

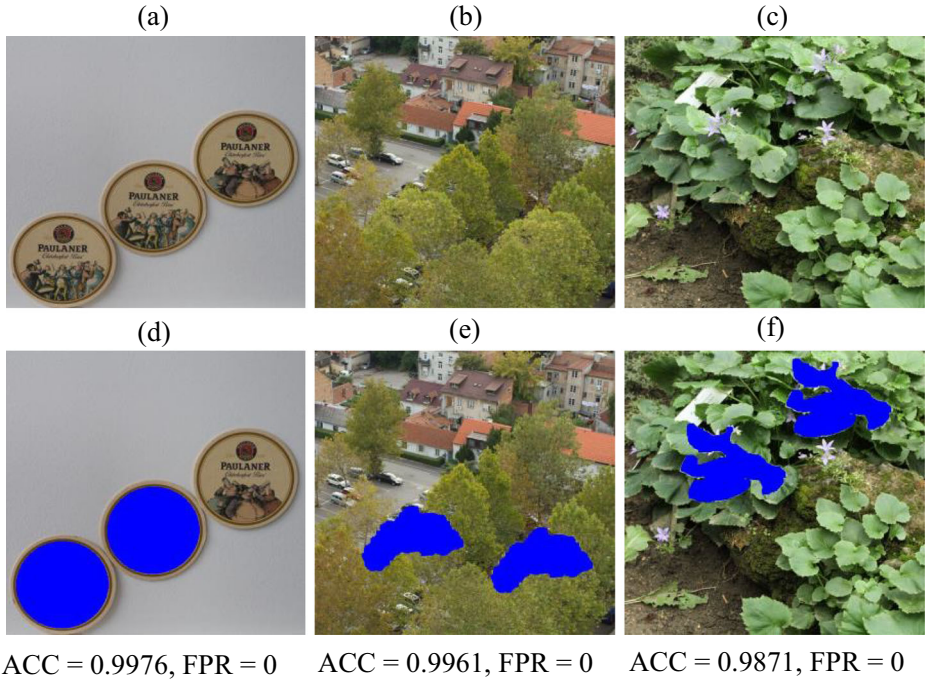

Fig. 8 Localization results on irregular shaped region tampered images

Final experiment conducted on all forty-plain copy-move forged images of CoMoFoD dataset. The average accuracy, FPR, precision, recall, and F1-measure achieved under plain copy move forgery are 0.9890, 0.0066, 0.9100, 0.8175, and 0.8442 respectively achieved in

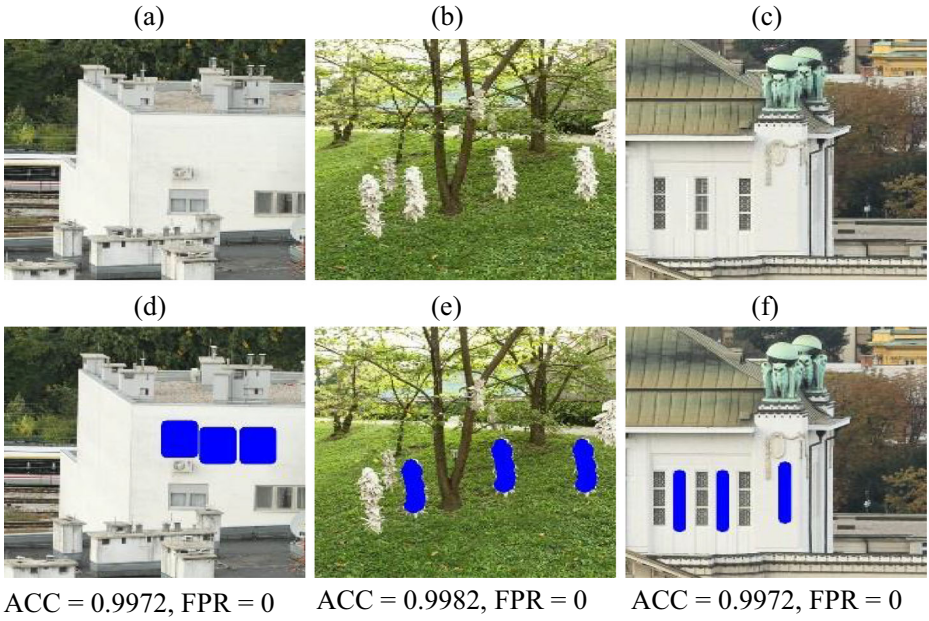

Fig. 9 Localization results on multiple cloning tampered images

Table 1 Performance evaluation on mean filtering operation

Filter Size	Image	Accuracy	FPR
3×3	Tree	0.9648	0
	Grass	0.9907	0
	Pole	0.9968	0
5×5	Tree	0.9569	0
	Grass	0.9877	0
	Pole	0.9947	0.0003
7×7	Tree	0.9495	0
	Grass	0.9843	0
	Pole	0.9928	0

CoMoFoD dataset images that contains 40 images. This balanced performance at pixel level shows the effectiveness and reliability of proposed method.

5.3.2 Robustness analysis

The copy move forgery usually follows by post-processing operation [11]. The objective of these attacks is to make it hard to find out the doctored locations. Therefore, it is necessary to evaluate the resistance of the developed algorithm against post-processing operation. In this section, experiments are carried out on image "tree", "Grass", "pole" and CoMoFoD dataset. The proposed algorithm can resist various post-processing attacks including mean filtering, histogram equalization, image sharpening, Gaussian blurring, and median filtering. The Tables 1, 2, 3 and 4 portray the detailed analysis of effectiveness against these attacks on "tree", "grass" and "pole" test images.

Results displayed from Tables 1, 2, 3 and 4 represent that the proposed solution has the ability to perform efficiently even when the tampered image suffers excessive blurring, sharpening or other operations. It is found that the developed solution is competent enough in detecting and localizing the altered regions significantly with low false positive rate and greater accuracy rate and. Thus, the proposed CMFD method is found to be robust against the attacks mentioned in Tables 1, 2, 3 and 4.

The next experiment conducted on the CoMoFoD dataset. The CoMoFoD dataset contains forged images with six types of post-processing attacks. In this study, the evolved algorithm tested on four attacks. The visual results further show that the proposed solution exhibits impressive forgery localization even after these post-processing operations were applied.

The brightness change operations were applied in the range [0,1] in the CoMoFoD dataset. Hence, CoMoFoD dataset contains tampered images after applying brightness with ranges ([0.01, 0.95], [0.01, 0.9)] and [0.01, 0.8]). Figure 10(a)-(c) is showing the tampered image with different parameters and Fig. 10(d)-(f) showing the localizing results on applying the proposed solution. Thus, the proposed method is robust enough against brightness change operation even when more brightness is applied in the forged image. The next experiments on colour

Table 2 Performance evaluation on Histogram equalization

Image	Accuracy	FPR
Tree	0.9753	0.0003
Grass	0.9940	0
Pole	0.9966	0.0025

Table 3 Performance Evaluation on Image Sharpening Operation

Image	Accuracy	FPR
Tree	0.9598	0.0056
Grass	0.9891	0
Pole	0.9949	0

reduction attacked images reproduced using a uniform quantization process. The values of intensity went through this process. It carried out for a uniform decrease in channels of an image. The operation carried out on all fraud images. It reduces from 256 to 128, 256 to 64 and 256 to 32 this reduction process outcome low-quality fraud images as the number of bits required to represent a channel has reduced. Fig. 11(a)-(c) displays the manipulated images with degradation parameters. Figure 11(d)-(f) shows the tracing outcome on these images when the developed algorithm applied. The visual results show the robustness against colour reduction even when the tampered images are unnoticeable degradation vis-à-vis the original image.

The effectiveness of the proposed algorithm further examined on contrast adjustment attack from the images CoMoFoD dataset. Figure 12(a-c) show the manipulated image after applying the contrast adjustment operation. Figure 12(d-f) unfolding the fraud pixels on applying the proposed algorithm along with their accuracy and false positive rate. The accuracy and false

Table 4 Performance evaluation on Gaussian blurring operation

Kernel Size	Standard Deviation	Image	Accuracy	FPR
3×3	0.5	Tree	0.9962	0
		Grass	0.9913	0
		Pole	0.9968	0
	1	Tree	0.9650	0
		Grass	0.9908	0
		Pole	0.9968	0
	2	Tree	0.9648	0
		Grass	0.9908	0
		Pole	0.9968	0
	4	Tree	0.9648	0
		Grass	0.9909	0
		Pole	0.9968	0
	8	Tree	0.9648	0
		Grass	0.9909	0
		Pole	0.9968	0
5×5	0.5	Tree	0.9663	0
		Grass	0.9911	0
		Pole	0.9967	0
	1	Tree	0.9956	0
		Grass	0.9878	0
		Pole	0.9948	0
	2	Tree	0.9574	0
		Grass	0.9818	0
		Pole	0.9945	0.003
	4	Tree	0.9572	0
		Grass	0.9879	0
		Pole	0.9941	0.0007
	8	Tree	0.9572	0
		Grass	0.9879	0
		Pole	0.9938	0.0011

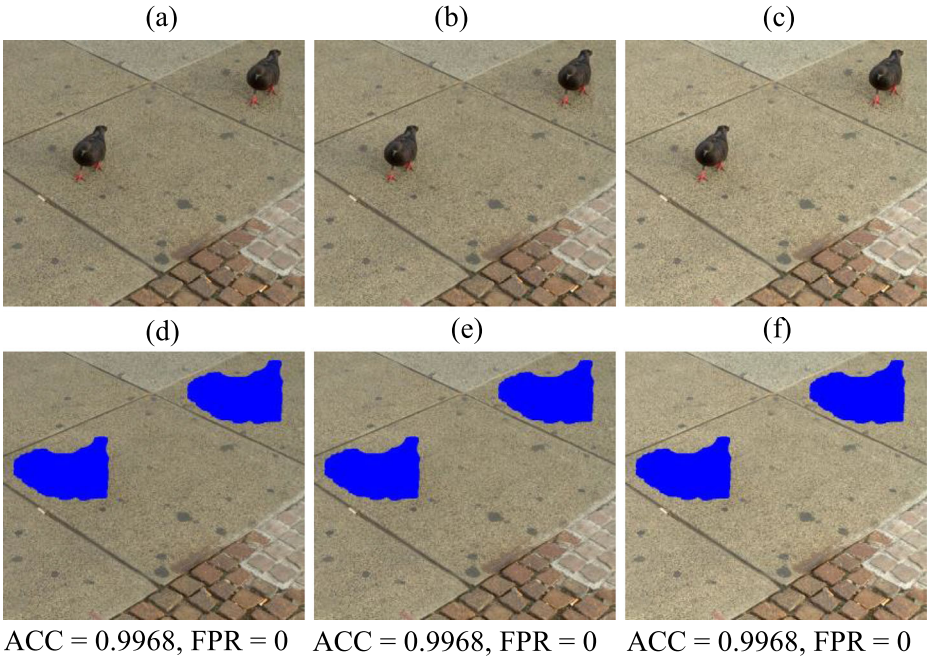

Fig. 10 Localization results for brightness change operation

positive rate need to be close to 1 and approximately to zero respectively. Hence, visual results in Fig. 12(d-f) depicts that the proposed solution has an impressive capability to localize duplicate region even when the high contrast adjustment operation was applied. In the last

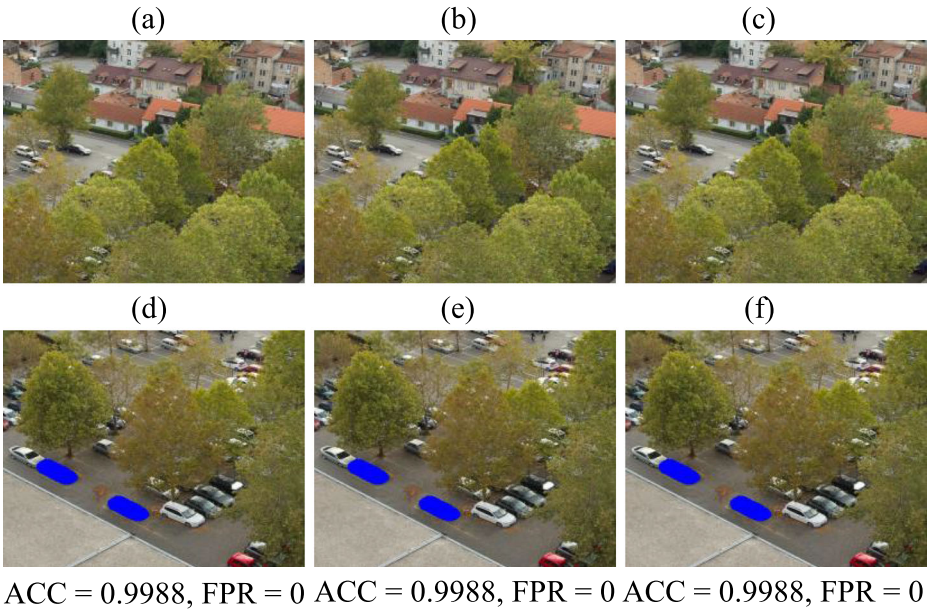

Fig. 11 Localization results on colour reduction operation

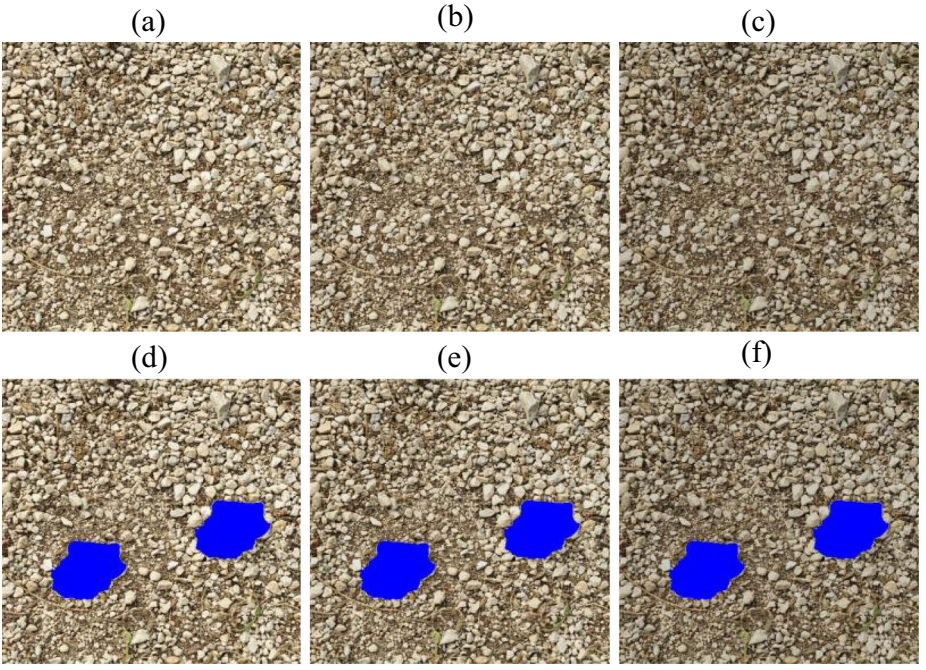

Fig. 12 Localization results on contrast adjustment operation

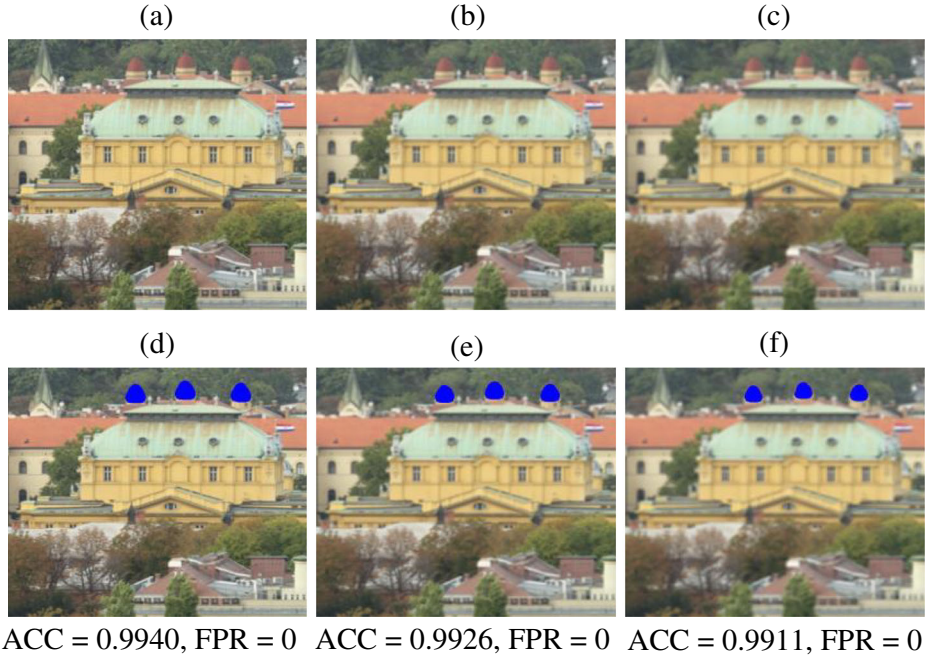

Fig. 13 Localization results on image blurring operation

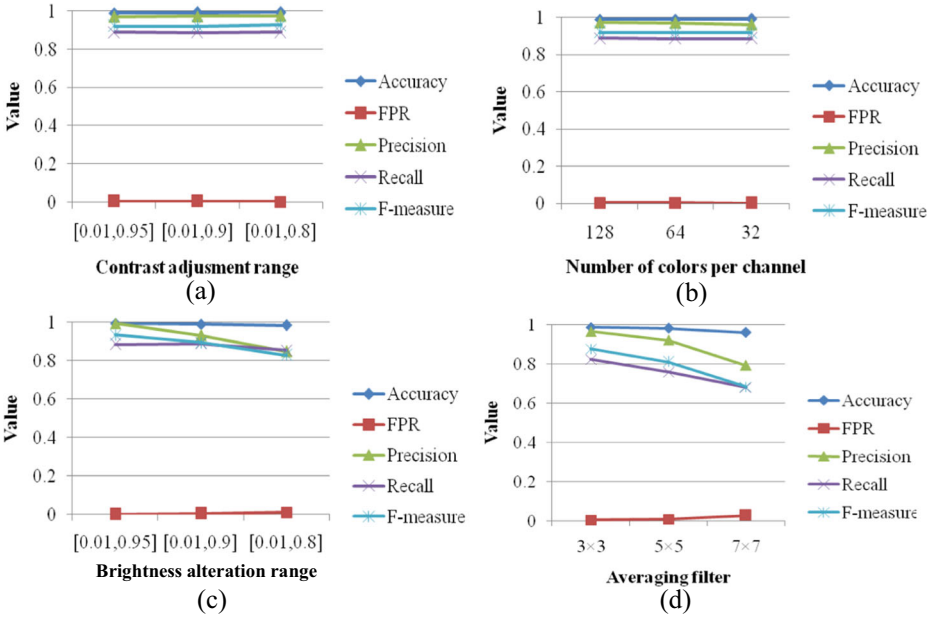

Fig. 14 Average accuracy, FPR, precision, recall and F1-measure of 27 images under (**a**) contrast adjustment (**b**) color reduction (**c**) brightness change(**d**) image blurring post-processing operations

experiment, we indexed the efficiency against blurred image of the CoMoFoD dataset. These images were generated using three kernel-averaging filters (3 × 3, 5 × 5, and 7 × 7). Figure 13(a)-(c) show noticeable tampered image after applying blurring filters along with their parameter. Figure 13(d)-(f) showing the efficiency of the proposed algorithm, even filter size increases. Thus, unfolding forge pixel outcomes are confirming that the developed CMFD algorithm has the ability to stand against image blurring operation. Thus, results shown in Fig. 13 portray the robustness of the proposed technique even the high parameter is applied for post-processing operations with high accuracy nearest to 1 and very low false positive rate nearest to zero. The strength of these features against the above conventional post processing operation has shown in Fig. 14. The analysis of twenty-seven images on colour reduction, contrast adjustment, brightness change and image blurring show that the proposed method with three features

Table 5 Performance Evaluation on Median Filtering Operation

Filter Size	Image	Accuracy	FPR
3×3	Tree	0.9790	0
	Grass	0.9928	0
	Pole	0.9968	0
5×5	Tree	0.9678	0
	Grass	0.9896	0
	Pole	0.9951	0
7×7	Tree	0.9580	0
	Grass	0.9868	0
	Pole	0.9927	0

Table 6 Comparison Results on Colour Reduction Operation

Method	Accuracy on parameter			FPR on parameter		
	3×3	5×5	7×7	3×3	5×5	7×7
DCT (Exact) [10]	0.9695	0.9540	0.9236	0.0266	0.0403	0.0708
DCT (Robust) [10]	0.9297	0.9259	0.9154	0.0758	0.0684	0.0753
SVD-based [13]	0.8530	0.8025	0.7557	0.1516	0.2035	0.2509
DCT & SVD-based [30]	0.9538	0.9265	0.9057	0.0410	0.0678	0.0833
SWT &DCT-based [17]	0.9862	0.9776	0.9469	0.0066	0.0137	0.0444
Proposed	0.9879	0.9821	0.9634	0.0044	0.0081	0.0259

5.3.3 Comparison analysis

Experiment's result outlined in section 6.3, elaborate that the developed solution is an impressive approach for tracing and localization of copy move forgery with an accuracy rate exceeding 90% for images of the CoMFoD dataset. This section finally compares with existing related schemes: DCT (Exact match) Fridrich et al. [10], DCT (Robust match) Fridrich et al. [10], SVD-based Kang and Wei [13], DCT &SVD- based Zhao and Guo [30], SWT & DCT - based Mahmood et al. [17]. To testify, along with examining the proposed scheme, the experiments carried out over 35 forged images of the CoMoFoD dataset operated through translation. The dataset contains forged images that were altered after copy-move forgery through different post-processing techniques, for instance, contrast adjustment, brightness change, colour reduction, blurring, and with different parameters. Suppose an image has undergone blurring operation of filter size 3 × 3, 5 × 5 and 7 × 7 then we have 3 forged images. The comparison results are shown on four post-processing operation with three parameters for each operation. So, Tables 5, 6, 7, 8 and 9) contains the results obtained on 420 images. In this section, the comparison results are given on average of the selected images for each post-processing operation colour reduction, contrast adjustment, brightness change, blurring in Tables 5, 6, 7, 8 and 9. For comparison analysis, the morphological opening operation has operated on all images.

The comparison parameters used in Tables 5, 6, 7, 8 and 9, are false-positive rate and forgery detection accuracy. Higher accuracy and lower false positive rate show an impressive scheme. In the case of colour reduction, Table 6 is showing the results obtained on applying the proposed scheme, where the colour reduction process reduces the intensity from 256 to 128, 256 to 64 and 256 to 64 for reproducing the image. The outcome portray that the developed scheme gives satisfactory accuracy even when the higher intensity parameter is

Table 7 Comparison results on Image Blurring operation

Method	Accuracy on parameter			FPR on parameter		
	128	64	32	128	64	32
DCT (Exact) [10]	0.9736	0.9731	0.9658	0.0249	0.0256	0.0332
DCT (Robust) [10]	0.9172	0.9156	0.9188	0.0853	0.0872	0.0832
SVD-based [13]	0.9334	0.9406	0.9640	0.0662	0.0587	0.0335
DCT & SVD-based [20]	0.9649	0.9592	0.9516	0.0334	0.0390	0.0475
SWT &DCT-based [17]	0.9854	0.9890	0.9851	0.0097	0.0063	0.0103
Proposed	0.9875	0.9907	0.9907	0.0075	0.0041	0.0041

Table 8 Comparison results on brightness change operation

Method	Accuracy on Parameter			FPR on Parameter		
	[0.01, 0.95]	[0.01, 0.9]	[0.01, 0.8]	[0.01, 0.95]	[0.01, 0.9]	[0.01, 0.8]
DCT (Exact) [10]	0.9707	0.9600	0.9220	0.0279	0.0390	0.0786
DCT (Robust) [10]	0.9200	0.9186	0.9357	0.0821	0.0820	0.0640
SVD-based [13]	0.9437	0.9376	0.9290	0.0550	0.0611	0.0679
DCT & SVD-based [30]	0.9585	0.9563	0.9557	0.0402	0.0417	0.0418
SWT &DCT-based [17]	0.9914	0.9842	0.9777	0.0035	0.0108	0.0164
Proposed	0.9928	0.9890	0.9834	0.0017	0.0055	0.0102

used for colour reduction operation. The proposed scheme has a lower false-positive rate in comparison to other schemes. In the case of blurring, Table 7 depicts that average accuracy surpasses other schemes and, average false positive rates are low than other schemes in all averaging filters for blurring operation. Table 8 represents the similar comparison results on brightness change operation with the following change in brightness with ranges: ([0.01, 0.95], [0.01, 0.9] and [0.01, 0.8]). Results demonstrate that the proposed technique has an average accuracy of 98% in all ranges while comparing without methods with a low average false positive rate than other methods.

Results presented in the Table 9 represents that proposed method having average accuracy of 98% when the images have tampered through contrast adjustment operation with ranges: ([0.01, 0.95], [0.01, 0.9] and [0.01, 0.8]). The results also depict that it performed better than other methods, even when the contrast adjustment range is [0.01, 0.8]. Table 8, it observed that the developed technique performed satisfactorily than the other techniques even when pre-processing parameter increased to wipe out traces of forgery. One surplus issue in CMFD methods is the computational power required allied along with block features matching. The Table 10 demonstrates a comparison of the proposed method with other relevant methods. The lexicographical sorting of feature a matrix is a major concern Feature matrix rows indicate the entire name of blocks, and the columns of the matrix mark it as the size of the feature with the top left corner spatial location of the block. The feature number in proposed methods are 3-dimensional, while in other methods Fridrich et al. (Exact match) Fridrich et al. (Robust match) [10], Xiao Bing KANG et al. Kang and Wei [13], Zhao et al. Zhao and Guo [30], Mahmood et al. [17] are 64 dimensional, 64-dimensional, k- dimensional ($k \leq 20$), 16-dimensional and 6-dimensional respectively. As shown in the table, the feature dimension in the proposed method is evidently smaller than other methods. Another common limitation in feature matching process is searching for nearest feature comparison and matching for similar

Table 9 Comparison results on contrast adjustment operation

Method	Accuracy on Parameter			FPR on Parameter		
	[0.01, 0.95]	[0.01, 0.9]	[0.01, 0.8]	[0.01, 0.95]	[0.01, 0.9]	[0.01, 0.8]
DCT (Exact) [10]	0.9753	0.9745	0.9742	0.0232	0.0240	0.0243
DCT (Robust) [10]	0.9079	0.9142	0.9132	0.0955	0.0877	0.0881
SVD-based [13]	0.9265	0.9227	0.9064	0.0740	0.0781	0.0962
DCT & SVD-based [30]	0.9588	0.9581	0.9620	0.0392	0.0388	0.0063
SWT &DCT-based [17]	0.9871	0.9876	0.9891	0.0085	0.0078	0.0134
Proposed	0.9867	0.9872	0.9889	0.0083	0.0076	0.0060

Table 10 Comparison of computational complexity in terms of feature dimensions

Method	Feature Based on	Block Size	Feature Dimension
Fridrich et al. [10]	Intensity	8	64
Fridrich et al. [10]	DCT	8	64
Xiao Bing et al. [13]	SVD	20	$k \leq 20$
Zaho et al. [30]	DCT & SVD	8	16
Mahmood et al. [17]	SWT & DCT	8	6
Proposed	SWT & DCT & SVD	8	3

blocks to probe and detect forged region, which is tedious and time consuming. It influences significantly on computational complexity in the feature-matching step. In the proposed method after lexicographical sorting consecutive features, matching is required to obtain matching block pair. Proposed approach reduces the computational overhead to obtain the matching block pairs. Nonetheless, the proposed method gives better detection proficiency.

6 Conclusion

Copy move forgery detection becomes a dire need in present scenario. In this paper a passive forensics scheme has been proposed which is potent enough to detect any kind of CMF successfully with negligible false positive results. As it has been found that most of the conventional CMFD scheme lack of either robustness or efficiency, our proposed scheme established a proper trade-off between these two coveted properties. To attain the objective, DCT and SVD transformation are employed accordingly to select DC and most significant singular value components from the overlapping blocks. This approach ensures a smaller number of feature vectors, which carries most significant information of an image, has been selected. As a result, the computational overhead of CMFD has been reduced significantly. Therefore, the proposed scheme not only computationally efficient but also possess great withstanding capability against many types of post processing attacks like Gaussian blurring, histogram equalization, sharpening, mean and median filtering, colour reduction, brightness change, contrast adjustment, image blurring, etc. Experiment results and comparative analysis exhibits the efficiency, robustness, and accuracy of the proposed method under various hostile situation and keep false positive results at bay.

Declarations

Conflict of interest The authors declare that there is no actual or potential conflict of interest regarding the publication of this article.

References

1. Alkawaz MH, Sulong G, Saba T, Rehman A (2018) Detection of copy-move image forgery based on discrete cosine transform. Neural Comput & Applic 30(1):183–192
2. Al-Qershi OM, Khoo BE (2019) Enhanced block-based copy-move forgery detection using k-means clustering. Multidim Syst Sign Process 30(4):1671–1695

3. Bayram S, Sencar HT, Memon TN (2009) An efficient and robust method for detecting copy-move forgery. IEEE Int. Conf. on Acoustics, Speech and Signal Processing, pp 1053–1056
4. Bovik AC (2010) 'Handbook of Image and Video Processing'. Academic Press,.
5. Cao L (2006) Singular value decomposition applied to digital image processing. Arizona State University polytechnic Campus, Division of Computing Studies, Arizona State University Polytechnic Campus, Mesa pp.1-15
6. Christlein V et al (2012) An evaluation of popular copy-move forgery detection approaches. IEEE Trans Inform Forensics Secur 7(6):1841–1854
7. Coffman RR, Donoho DL (1995) Translation-invariant de-noising. In Wavelets and statistics, Springer, New York, NY, pp 125–150
8. Dixit R, Naskar R (2017) Review, analysis and parameterisation of techniques for copy–move forgery detection in digital images. IET Image Process 11(9):746–759
9. Farid AP, Popescu AC (2004) Exposing digital forgeries by detecting duplicated image region. Technical Report, Hanover, Department of Computer Science, Dartmouth College, USA
10. Fridrich AJ, Soukal BD, Luk AJ (2003) 'Detection of copy-move forgery in digital images'. Proc. of Digital Forensic Research Workshop
11. Gonzalez RC, Woods RE (2017) Digital image processing. Pearson, Global Edition
12. Hayat K, Qazi T (2017) Forgery detection in digital images via discrete wavelet and discrete cosine transforms. Compu Electrical Eng 62:448–458
13. Kang X, Wei S (2009) Identifying tampered regions using singular value decomposition in digital image forensics. Int Conf Comput Sci Software Eng 3:926–930
14. Lee JC, Chang CP, Chen WK (2015) Detection of copy–move image forgery using histogram of orientated gradients. Inf Sci 321:250–262
15. Lin X et al (2018) Recent advances in passive digital image security forensics: a brief review. Engineering 4(1):29–39
16. Lowe DG (2004) Distinctive image features from scale-invariant key points. Int J Comput Vis 60(2):91–110
17. 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
18. Meena KB, Tyagi V (2019) Image forgery detection: survey and future directions. Data Engineering and applications, Springer, Singapore, pp 163–194
19. Meena KB, Tyagi V (2020) A copy-move image forgery detection technique based on tetrolet transform. J Inform Secur Appl 52:102481
20. Nason GP, Silverman BW (1995) The stationary wavelet transforms and some statistical applications. Wavelets and statistics. Springer, New York, NY, pp 281–299
21. Rao KR, Yip P Discrete cosine transform: algorithms, advantages, applications, 2014, Academic press
22. Schlesinger V et al (2017) Image forgery detection confronts image composition. Comput Graphics 68:152–163
23. Singh G, Singh K (2020) An improved block-based copy-move forgery detection technique. Multimedia Tools Appl:1–25
24. Soni B, Das PK, Thounaojam DM (2019) Geometric transformation invariant block based copy-move forgery detection using fast and efficient hybrid local features. J Inform Secur Appl 45:44–51
25. Starck JL, Fadili J, Murtagh F (2007) The undecimated wavelet decomposition and its reconstruction. IEEE Trans Image Process 16(2):297–309
26. Tharwat A (2018) 'Classification assessment methods'. Appl Comput Inform
27. Tralic D, Zupancic I, Grgic S, Grgic M (2013) CoMoFoD—New database for copy-move forgery detection. IEEE Proceedings ELMAR:49–54
28. Warif NBA et al (2016) Copy-move forgery detection: survey, challenges and future directions. J Network Comput Appl 75:259–278
29. Zandi M, Mahmoudi-Aznaveh A, Mansouri A (2014) Adaptive matching for copy-move forgery detection'. In 2014 IEEE international workshop on information forensics and security (WIFS). IEEE:119–124
30. Zhao J, Guo J (2013) Passive forensics for copy-move image forgery using a method based on DCT and SVD. Forensic Sci Int 233(1–3):158–166