Journal of Visual Communication and Image Representation 53 (2018) 202–214

Contents lists available at ScienceDirect

Journal of Visual Communication and Image Representation

journal homepage: www.elsevier.com/locate/jvci

A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform☆

Toqeer Mahmood[a,*], Zahid Mehmood[b], Mohsin Shah[c], Tanzila Saba[d]

[a] Department of Computer Science, University of Engineering and Technology, Taxila 47050, Pakistan
[b] Department of Software Engineering, University of Engineering and Technology, Taxila 47050, Pakistan
[c] School of Information Science and Technology, University of Science and Technology of China, Hefei 230027, China
[d] College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia

ARTICLE INFO

Keywords:
Copy-move forgery
Tampered images
Forgery detection
Authenticity
Passive authentication

ABSTRACT

In this era, due to the widespread availability of digital devices, various open source and commercially available image editing tools have made authenticity of image contents questionable. Copy-move forgery (CMF) is a common technique to produce tampered images by concealing undesirable objects or replicating desirable objects in the same image. Therefore, means are required to authenticate image contents and identify the tampered areas. In this paper, a robust technique for CMF detection and localization in digital images is proposed. The technique extracts stationary wavelet transform (SWT) based features for exposing the forgeries in digital images. SWT is adopted because of its impressive localization properties, in both spectral and spatial domains. More specifically approximation subband of the stationary wavelet transform is utilized as this subband holds most of the information that is best suited for forgery detection. The dimension of the feature vectors is reduced by applying discrete cosine transform (DCT). To evaluate the proposed technique, we use two standard datasets namely, the CoMoFoD and the UCID for experimentations. The experimental results reveal that the proposed technique outperforms the existing techniques in terms of true and false detection rate. Consequently, the proposed forgery detection technique can be applied to detect the tampered areas and the benefits can be obtained in image forensic applications.

1. Introduction

In this era, the users not only share many digital images in social media over the Internet but also in courtrooms as evidence, news reports, for insurance claims etc. The development of commercially available image editing tools are the basis of increasing use of digital images in our daily life. Ease of use of such tools has made manipulation of image contents easier. Image manipulation techniques can be classified as image steganography and image forgery. Both image steganography and image forgery manipulate an image but they differ from one another according to their practices [1–3]. Steganography manipulates a subject digital image for hiding secret information whereas image forgery changes the original semantic meaning of an image.

There have been a large number of steganographic techniques that utilize digital image for covert communication [4,5]. At the same time, various steganalysis techniques have been devised to unveil secret messages in digital images [6]. The embedded data is restored during the authentication process by comparing the reference data. Thereafter, in the forensic investigation, the authenticated data is used to ensure the integrity of digital media whether forged or not [7]. Various existing stenographic tools have also been used to help forensic experts for the analysis of multimedia contents [8–10].

The tampering of digital images is very easy due to the accessibility of sophisticated and easy to use image manipulation and editing software. The tampered images can be used as a deceiving tool for hiding the actual facts. For instance, tampered images presented in digital media (TV and newspapers) mislead the people, as important objects may be replicated or concealed from the images [11]. This exhibits that image forgery is a serious threat, therefore, it has become a key concern for the researchers of digital image forensics in the recent times [12–15]. In literature, we can find various tampering detection techniques that may be categorized as active techniques and passive (blind) techniques [16–18].

The active techniques like watermarking, digital signature and

☆ This paper has been recommended for acceptance by Zicheng Liu.

* Corresponding author.
E-mail addresses: toqeer.mahmood@uettaxila.edu.pk (T. Mahmood), zahid.mehmood@uettaxila.edu.pk (Z. Mehmood), mohsin@mail.ustc.edu.cn (M. Shah), tsaba@psu.edu.sa (T. Saba).

https://doi.org/10.1016/j.jvcir.2018.03.015
Received 12 September 2017; Received in revised form 13 March 2018; Accepted 24 March 2018
Available online 27 March 2018

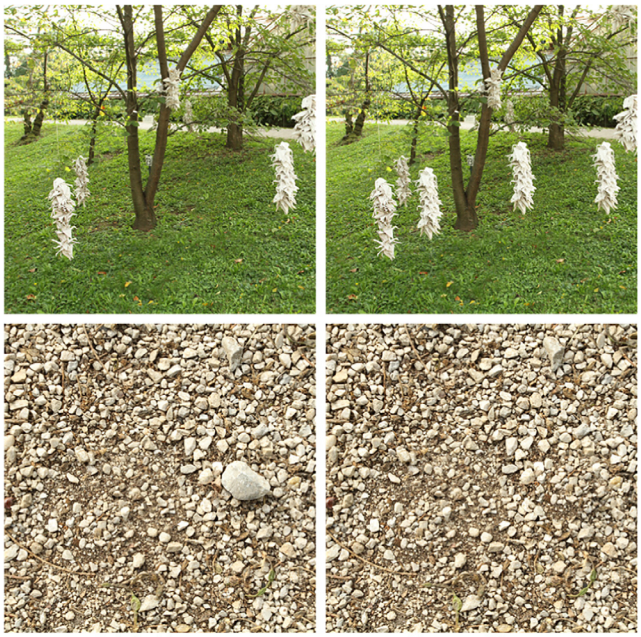

Fig. 1. Image forgery examples [20].

image steganography embed data into the original image. In forensic analysis, the embedded data is used to establish the integrity of image contents by validating if the embedded data matches the extracted information. The active techniques require specialized hardware and software for processing of the images as well [16–18]. The constraints of active techniques adjured the evolution of passive techniques for forensic applications in images.

In literature, the passive techniques proposed for image forensic applications work totally in the absence of any embedded data [16–18]. However, the techniques in this class examine the local information to identify tampered areas in the questioned image. The researchers describe two types of tampering that may be applied to the digital images are image splicing and image copy-move forgery (CMF). In image splicing, areas from multiple images are obtained to generate a feigned image. On the contrary, in CMF, areas of the same image are utilized to replicate or conceal some important contents [19]. Fig. 1 exemplifies the applications of CMF in images. For the cases given in the first column, the object (plant) is replicated to produce the contents that are unavailable in the original image. In the other example, an area is replicated to conceal unwanted object (big sized stone) in the original image. The tampered objects in Fig. 1 are well blended at the desired locations, and become very hard to differentiate through the human eye.

The output of a digital image forgery detection technique could be of two types: (a) classifying a digital image as original or tampered (no localization), and (b) localization of the tampered areas within the same image, if the image is counterfeited [21]. In the current paper, we propose a passive CMF detection technique with the goal of localization to show the input image as original or tampered. To detect CMF reliably our technique relies on both the translation invariant stationary wavelet transform (SWT) and the discrete cosine transform (DCT). The major reason for utilizing the SWT is its impressive localization properties, in both spectral and spatial domains. The proposed technique first applies SWT on the image in question to get the approximation subband. This is followed by segmenting the approximation subband into fixed sized overlapping blocks. The dimension of the feature vectors is reduced by applying DCT to the individual blocks. Thereafter, a few numbers of DCT coefficients are selected that are further utilized to investigate the similarity between tampered areas. Experimental results indicate that the proposed technique has higher accuracy as compared to state-of-the-art techniques even after post-processing attacks on digital images. The contributions of the proposed approach for the CMF detection are:

- Utilization of reduced sized feature vectors which lowers the computational complexity for tampering detection.
- Ability to unveil multiple CMFs in digital images efficiently.
- Robustness against post-processing attacks like translation, blurring, JPEG compression, color reduction, and, brightness change.

The structure of the current paper is as follows: Section 2 presents the related work from various tampering detection techniques. In Section 3 the proposed technique is presented in detail including feature extraction, feature dimension reduction, matching and filtering processes. The experimental setup, results and a comparison with other techniques are given in Section 4. Finally, Section 5 concludes the current paper.

2. Related work

Owing to the simplicity, the CMF is the most common technique for image tampering. Over the past, various techniques have been carried out for detection of CMF in digital images. The first technique to detect CMF is presented by Fridrich et al. [22]. The technique extracts DCT coefficients based features from small overlapping image blocks. The features are sorted lexicographically before similarity check between feature vectors to detect tampered areas. In [23], a related technique is presented that extracts DCT coefficients as features for different block sizes. The main limitations of both the techniques are high computational complexity and improper detection of tampered areas when post-processing operations are applied to the tampered images. In [24], Popescu and Farid utilized principal components analysis (PCA) for CMF detection. The authors obtained the block representation using half of the number of features utilized by [22]. In [25], Bayram et al. utilized Fourier Mellin Transform based features for representing the image blocks. To minimize the comparison time *kd*-tree and counting bloom filters are employed in the block matching process. The results exhibit that this technique is able to identify slightly rotated tampered areas. In [26], Li proposed a forgery detection system using the orthogonal polar cosine transform (PCT) as a feature of the image blocks. The author also developed a Locality-sensitive hashing (LSH) based mechanism for image blocks matching. The results show that the algorithm is effective for a few post-processing operations. In [27], Zhao and Guo proposed a solution using singular value decomposition (SVD) with DCT for detecting forgeries in digital images. The technique applies DCT to each overlapping block extracted from the input image. The quantized DCT coefficients blocks are further subdivided into non-overlapping blocks. The SVD is applied to each sub-blocks and highest singular value is extracted to construct the feature vector that represents the current DCT coefficients block. The technique is shown to be robust in terms of accuracy and false negatives to other techniques in the literature based on DCT. In [28], Mahmood et al. came up with a technique that is based on DCT and KPCA features. The technique exhibits the robustness against a few post-processing image operations. Hayat and Qazi [12], suggested a DWT and DCT based technique for detecting duplicated areas in digital images. The authors extracted the approximation subband of DWT thereafter the DCT is applied to the overlapping image blocks extracted from the approximation subband of DWT for detecting the forgeries. However, the detection performance for different image operations is missing in the study.

In [29], Zandi et al. suggested a technique using an adaptive similarity threshold. The algorithm identifies forged areas using thresholds proportional to the standard deviation of the image block. In [30], Lee et al. came up with a scheme using histogram of orientated gradients (HOG) for CMF detection. The authors extracted the statistical features for representing the overlapping image blocks. The results show that

the scheme performed well for some of the post-processing image operations. In [31], Silva et al. proposed a method to detect copy-move forgeries in digital images utilizing point of interest and blocks of pixels at the same time to detect forgeries with voting in a multiscale space. In [32], Liu et al. presented a solution for duplication detection. The authors first decomposed the input image in question through the Gaussian pyramid and Hu moments extracted from the circular overlapping image blocks. In [33], Mahmoud and Abu-AlRukab presented a comparative study of Zernike and Pseudo Zernike moments based CMF detection technique. The study shows that Pseudo Zernike moments perform better as compared to Zernike moment-based features for some of the image post-processing operations. However, the quantitative analysis is missing in the study. In [14], Al-Qershi and Khoo proposed a comparative study utilizing four matching techniques based on lexicographical sorting, lexicographical sorting and grouping, *kd*-tree and locality sensitive hashing. Their scheme is capable of detecting tampered areas in the presence of scaling, rotation, JPEG compression, Gaussian noise, and blurring. In [15], Fadl and Semary proposed a solution for CMF detection by converting each image blocks to the polar system. The authors applied the Fourier transform to each column of the converted block for extracting the features. The matching of the features is achieved after sorting all the feature of the image using the radix sort. The technique is shown to be robust against some of the image post-processing operations but the images used for experiments are of very small size (128 × 128 pixel).

In recent years, convolutional neural networks (CNN) based techniques have been presented in the area of image forensics. CNNs have the ability to extract complex high dimensional features and make effective representations [34]. In [35], a CNN based approach with the spatial rich model (SRM) [36] is proposed for the first convolutional layer to a set of high-pass filters in order to suppress the image contents. However, the authors utilized CNNs for image binary classification (original/tampered), without localization. In [37], a special blocking strategy is suggested for image splicing tampering detection. In this paper, the authors utilized rich model convolutional neural networks (rCNN) which serve as the block descriptor for tampering detection. However, the complexity of the method is very high. In [38], a multi-domain based CNN method is suggested again to solve the image tampering detection. This study explores the combined use of CNNs trained on spatial domain patches (RGB) and on DCT histograms as input for detecting the image splicing task.

3. The proposed technique

In this paper, a key contribution is proposed based on SWT and DCT for CMF detection and localization. The reason for selecting the SWT is its translation invariance and localization properties in both spectral and spatial domains [39]. The proposed technique decomposes the input image in question into four subbands (approximation, horizontal, vertical and diagonal) through the translation invariant SWT. The technique further divides the approximation subband into overlapping blocks for feature extraction. A reduced dimension of the feature is obtained by applying DCT to each overlapping block. The motivation to use DCT over the overlapping blocks of approximation subband of SWT is its robustness for post-processing operations, e.g. scaling, compression, and blurring [19,40], as these operations are commonly applied to the tampered images to make the tampering detection difficult [41]. Therefore, the combination of SWT and DCT makes the representation of features more diverse and also appears as a better choice for CMFD.

The architecture of the proposed CMFD technique is shown in Fig. 2. The steps of the proposed CMFD technique are outlined in the succeeding subsections:

3.1. Pre-processing

In order to implement the proposed CMFD technique, the input *RGB* image in question is transformed into YC_bC_r color space using the following mathematical expression:

$$
\begin{aligned}
Y &= \left(\tfrac{77}{256}\right)R + \left(\tfrac{150}{256}\right)G + \left(\tfrac{29}{256}\right)B \\
C_b &= -\left(\tfrac{44}{256}\right)R - \left(\tfrac{87}{256}\right)G + \left(\tfrac{131}{256}\right)B + 128 \\
C_r &= \left(\tfrac{131}{256}\right)R - \left(\tfrac{110}{256}\right)G - \left(\tfrac{21}{256}\right)B + 128
\end{aligned}
\tag{01}
$$

The key motivation for transforming input image into YC_bC_r color space is that the luminance channel (Y) holds more spatial information than other color spaces [42]. Therefore, the proposed technique utilizes Y for CMFD in digital images.

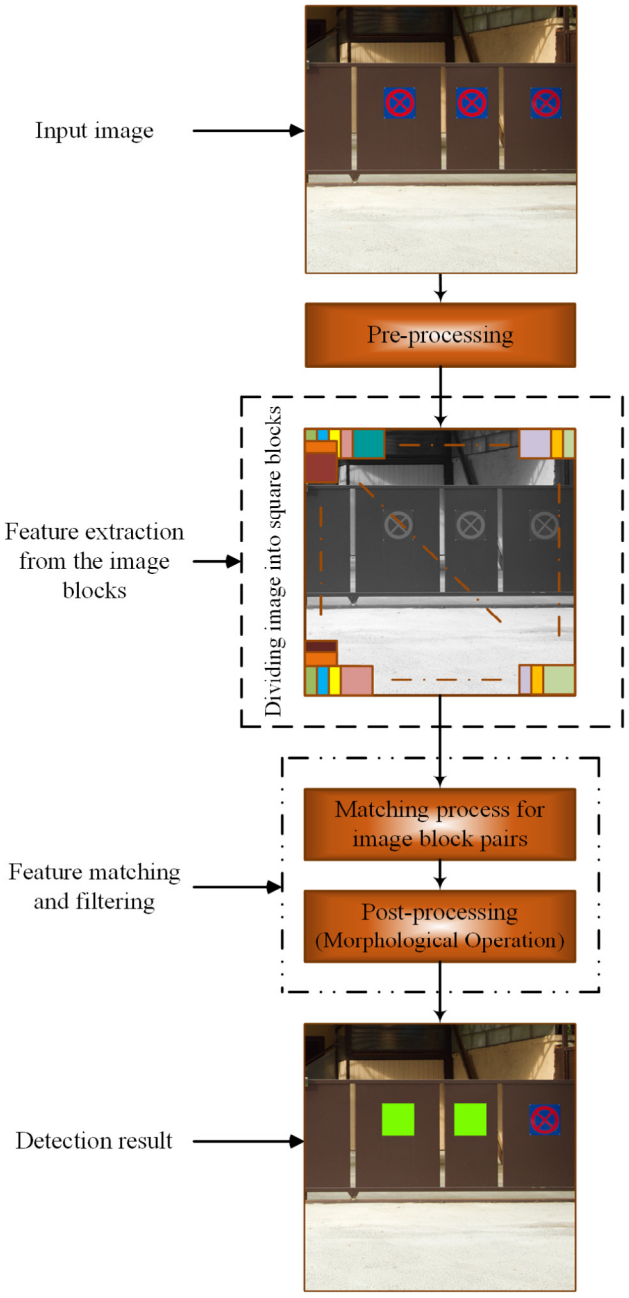

Fig. 2. The architecture of the proposed CMFD technique.

3.2. Feature extraction

This section defines the procedure for feature extraction in detail as follows:

3.2.1. SWT

In order to compress the input image, existing techniques [12,43–45], have employed discrete wavelet transform (DWT) that inherently lacks the shift invariance property. Thus, DWT shows pseudo-Gibbs phenomena around the singularities thereby produces unimpressive results for signal analysis applications like edge detection, denoising and texture analysis [46]. In [47], it is proved that the shift-invariant wavelet transform provides better detection performance and texture analysis than the shift variant transform. A slight shift in the input image may result in a great difference in DWT coefficients at different scales, which may produce different feature vectors for copied and moved areas with little spatial shift [48]. Therefore, to avoid the drawbacks of shift-variant DWT, we utilized the shift invariant SWT that is more suitable for pattern recognition, feature extraction, and tampering detection. In DWT, the input image is convolved with the low pass $l[m]$ and high pass $h[m]$ filters and decimate by a factor of 2 to obtain the wavelet coefficients. On the contrary, in SWT the input image is convolved with the low pass $l[m]$ and high pass $h[m]$ filters in a similar way, however, to obtain the wavelet coefficients no decimation is performed [49]. Therefore, for a luminance image Y of size $W \times H$, the SWT at j^{th} level can be expressed in mathematical Eqs. (02)–(05) as follows:

$$LH_{j+1}(M,N) = \sum_{x=-\infty}^{+\infty} \sum_{y=-\infty}^{+\infty} l_x^j h_y^j LL_j(M+x,N+y) \tag{02}$$

$$HL_{j+1}(M,N) = \sum_{x=-\infty}^{+\infty} \sum_{y=-\infty}^{+\infty} h_x^j l_y^j LL_j(M+x,N+y) \tag{03}$$

$$HH_{j+1}(M,N) = \sum_{x=-\infty}^{+\infty} \sum_{y=-\infty}^{+\infty} h_x^j h_y^j LL_j(M+x,N+y) \tag{04}$$

The sub-images LH, HL, and HH obtained using (02)–(04) denote the horizontal, vertical and diagonal subbands, respectively. However, the LL subband can be expressed as:

$$LL_{j+1}(M,N) = \sum_{x=-\infty}^{+\infty} \sum_{y=-\infty}^{+\infty} l_x^j l_y^j LL_j(M+x,N+y) \tag{05}$$

where $M = 1,2,...,W, N = 1,2,...,H$, l is a low pass filter and h is a high pass filter. The approximation subband (LL) obtained through Y is further considered for the evaluation of the proposed forgery detection technique.

First level decomposition of a $2D$ image through SWT is shown in Fig. 3 as well. Fig. 3 clearly states that an image of size $W \times H$ decomposed into four (04) subbands: approximation (LL), horizontal (LH), vertical (hL) and diagonal (HH), where all the subbands have same size $W \times H$ as of the input image.

3.2.2. Feature dimension reduction through DCT

The proposed technique further divides the LL of an image obtained

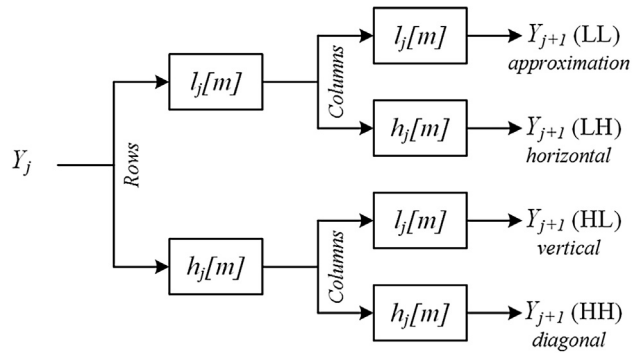

Fig. 3. Decomposition process of an image through SWT into four subbands.

by applying SWT as described in the preceding Section 3.2.1 into overlapping image blocks $B_i (i = 1,2,...,T_b)$ using a sliding window of size $w \times h = 8 \times 8$. Therefore, LL can be divided into T_b of overlapping blocks as given in (06);

$$T_b = (W-w+1) \times (H-h+1) \tag{06}$$

where W, H indicates the total number of columns and rows of LL, $w = 8$ and $h = 8$.

Considering all the coefficients of an image block B_k extracted from LL produces a feature vector larger in dimension. However, in forgery detection systems, the reduction of feature dimension is one of the main issues [49,50]. Consequently, in order to produce a reduced dimension of feature vector some mechanism is required. In the proposed forgery detection technique, a reduced dimension of feature vector is obtained by applying 8×8 block DCT to each B_i. The 8×8 block DCT applied to each B_i is computed as:

$$F_{uv} = \frac{1}{4} C_u C_v \sum_{w=0}^{7} \sum_{h=0}^{7} B_{wh} \cos\left(u\pi \frac{2w+1}{16}\right) \cos\left(v\pi \frac{2h+1}{16}\right) \tag{07}$$

where

$$C_u = \begin{cases} \frac{1}{\sqrt{2}} & u = 0 \\ 1 & 1 \leqslant u \leqslant 2 \\ 0 & 3 \leqslant u \leqslant 7 \end{cases}$$

$$C_v = \begin{cases} \frac{1}{\sqrt{2}} & v = 0 \\ 1 & 1 \leqslant v \leqslant 2 \\ 0 & 3 \leqslant v \leqslant 7 \end{cases}$$

It is the property of DCT that the most significant information concentrates in just a few low-frequency coefficients, therefore, all the DCT coefficients are not equally important. To extract the most informative frequency coefficients in the form of a feature vector from the DCT coefficients block a zigzag scan is followed starting from the DC coefficient. The proposed forgery detection technique is implemented utilizing first six (06) the most informative coefficients to form a feature vector from each B_i as represented by the mathematical equation (08). The process of feature vector extraction through SWT and DCT following a zigzag order is exemplified in Fig. 4 as well.

$$f = [f_1 f_2 f_3 f_4 f_5 f_6] \tag{08}$$

In block-based CMFD techniques, the computational complexity is a major concern which is directly related to the dimension of features [42] and overlapping blocks of the image. A feature matrix of the image comprises of the feature vectors corresponding to each B_i. Applying the lexicographical sorting in a high dimensional feature matrix is the main cause of computational complexity [49]. Thus, the techniques with reduced dimension of feature vectors are computationally proficient in comparison with the techniques having larger dimension of the feature vectors. Table 1 presents a comparison of computational complexity in terms of feature dimension between proposed and other techniques. Compared to [12,23–25,28,31], the proposed technique uses the same size of sliding window (i.e. $w \times h = 8 \times 8$) for extracting the overlapping image blocks B_i. However, the proposed technique utilizes a reduced dimension of feature vectors that specifies the presented technique is computationally more efficient.

3.3. Feature matching and filtering

3.3.1. Formation of the feature matrix

A feature matrix $\mathscr{F}_m$ of size $T_b \times 6$ is formed by placing all the feature vectors corresponding to each B_i extracted in accordance with the procedure described in Section 3.2, as:

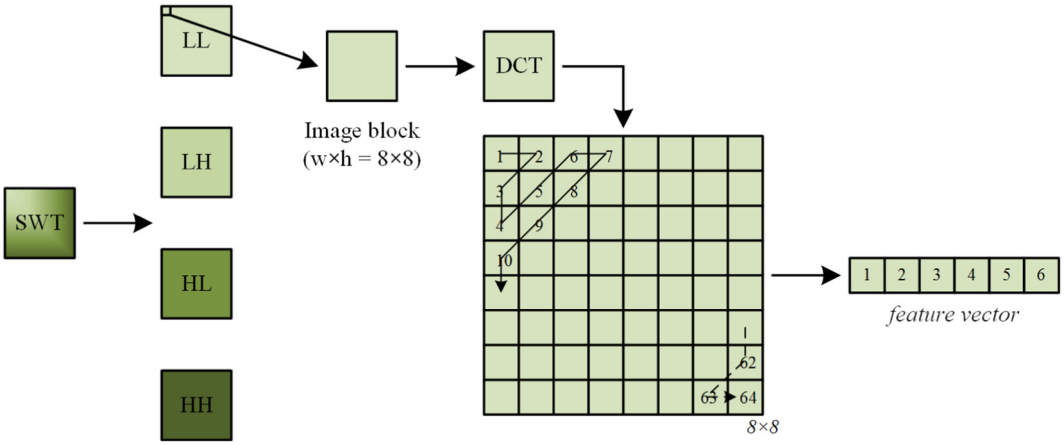

Fig. 4. Proposed feature extraction procedure for an image block of size 8 × 8 through SWT and DCT.

Table 1
Comparison of computational complexity in terms of feature dimension.

Techniques	Type of feature	Feature dimension
Alkawaz et al. [23]	DCT	64
Silva et al. [31]	SURF	64
Bayram et al. [25]	FMT	45
Popescu and Farid [24]	PCA	32
Mahmood et al. [28]	DCT & KPCA	10
Hayat and Qazi [12]	DWT & DCT	10
Proposed technique	SWT & DCT	6

$$\mathscr{F}_m = \begin{bmatrix} f_{1,z} \\ f_{2,z} \\ \vdots \\ f_{T_b,z} \end{bmatrix} \tag{09}$$

where $z = 1,2,\ldots,6$.

Before activating the procedure for matching the image block pairs, the feature matrix $\mathscr{F}_m$ is lexicographically sorted that re-arranges all the feature vectors of similar blocks closer to one another. Hence, lexicographic sorting helps in reducing the computational time and makes the technique more efficient in terms of searching of similar block pairs. For further processing, the proposed CMFD technique records top left corner coordinates of each B_i during the process of sorting. The $\mathscr{F}_m$ after lexicographical sorting is denoted as $\mathscr{F}_s$.

3.3.2. Matching of similar block pairs

Since tampered areas are believed to be non-intersecting and the image blocks in our approach are overlapping, to meet the requirements of the CMFD technique we employ the following constraints: (a) block distance threshold, and, (b) block similarity threshold.

3.3.2.1. Block distance threshold. In order to match the identical block pairs and identify areas that are likely to have been tampered. Using the matrix $\mathscr{F}_s$, the proposed CMFD technique computes block distance between the adjacent pair of blocks as defined in (10).

$$\forall \sqrt{(x_i - x_{i+j})^2 + (y_i - y_{i+j})^2} \tag{10}$$

where (x,y) is top left corner coordinate of the blocks.

If the block distance exceeds a predetermined block distance threshold (B_{th}) then the proposed CMFD technique will compute the block similarity threshold between the pair of blocks.

3.3.2.2. Block similarity threshold. If a pair of blocks holds the criteria given in (10), the proposed CMFD technique further computes block similarity between the feature vectors of corresponding blocks as defined in (11).

$$\mathscr{F}_{s_i} = [f_i^1 f_i^2 f_i^3 f_i^4 f_i^5 f_i^6]$$

$$\mathscr{F}_{s_j} = [f_j^1 f_j^2 f_j^3 f_j^4 f_j^5 f_j^6]$$

$$\forall \sqrt{\sum_{l=1}^{6} (f_i^l - f_j^l)^2} \tag{11}$$

If the distance of similarity is lesser than a predetermined block similarity threshold (S_{th}) thereafter the pair of blocks will be considered a candidate for forgery.

The process of feature matching and filtering is repeated for all the feature vectors of $\mathscr{F}_s$ corresponding to each B_i. The proposed CMFD technique using (10) and (11) determines whether the image blocks are tampered and stores all the filtered block pairs in a set Ω. The whole process of feature matching and filtering is also shown in Fig. 5.

3.4. Post-processing the visual detection results

The proposed CMFD technique finally produces the required output O_i through filtered block pairs stored in the set Ω. The morphological opening operation with a structural element of width 8 is also applied to O_i for eliminating the falsely detected areas in O_i. In general, all the detected pair of blocks comprising of original as well as tampered are

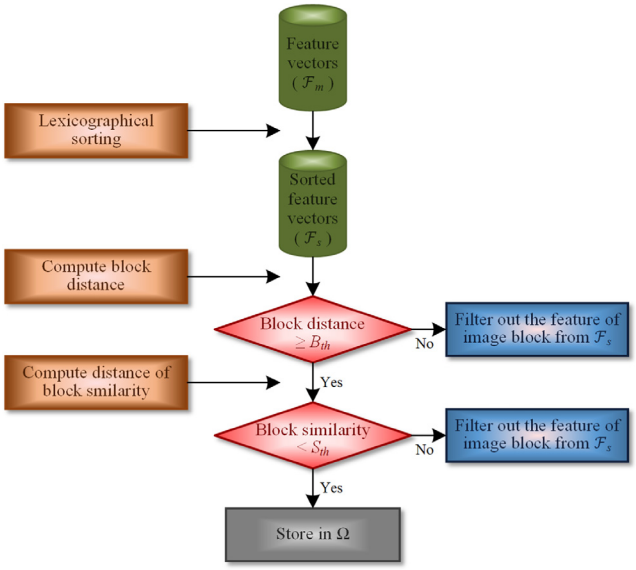

Fig. 5. Proposed process of feature matching and filtering.

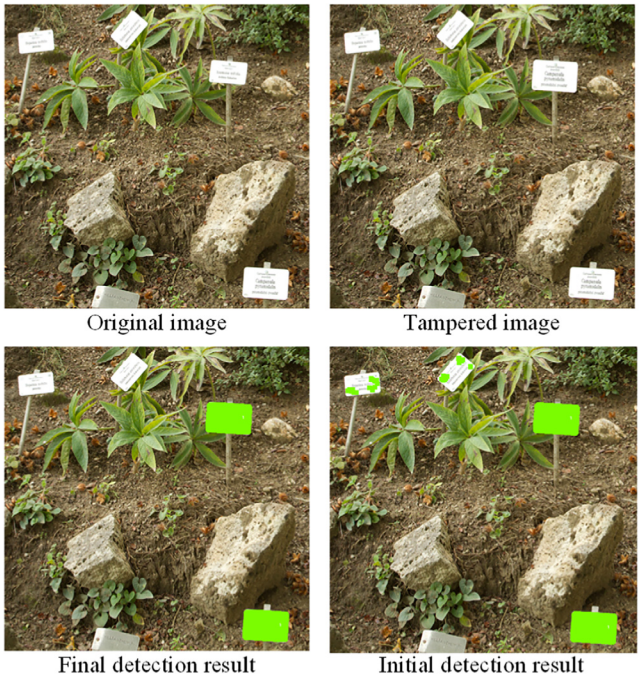

Fig. 6. Visual detection results using the proposed technique.

highlighted to show the final detection results. Fig. 6 is exemplifying the visual detection results using the proposed CMFD technique.

4. Experimental setup

This section demonstrates various experiments performed to demonstrate the usefulness of the technique. To evaluate the proposed CMFD technique, we considered two publically available standard image collections namely (CoMoFoD [20] and UCID v2 [51]). The CoMoFoD image collection contains 200 images of size 512×512 pixels, while UCID v2 image collection consists of 1338 digital images of size 512×384 pixels. The images tampered by CMF operation were generated through image manipulation and edition tool, Adobe Photoshop. All experiments are performed on a platform having *Ci5 2.4GHz* Intel processor *6GB* RAM running *Matlab2015a*. The experimental details and the visual detection results are provided in the succeeding subsections.

4.1. Parameter settings

In the experiments, values of the parameters are set as $b = 8$ (size of the image block), $N_r = 5$ (No. of neighboring features to compare), $D_{th} = 40$ (block distance threshold) and $S_{th} = 0.0005$ (block similarity threshold).

The usefulness of the technique is gauged through two metrics true and false detection rate. True detection rate (TDR) and false detection rate (FDR) are computed using the following mathematical equations:

$$TDR = \frac{|C \cap \overline{C}| + |T \cap \overline{T}|}{|C| + |T|} \tag{12}$$

$$FDR = \frac{|\overline{C} - C| + |\overline{T} - T|}{|\overline{C}| + |\overline{T}|} \tag{13}$$

where C is the copied area, T is the tampered area, $\overline{C}$ is the detected copied area, and $\overline{T}$ is the detected tampered area.

The TDR reflects the performance of the proposed technique in terms of localizing the elements of the duplicated areas in the manipulated image. Whereas, FDR indicates the elements that are not part of the tampered area but wrongly detected by the technique. Thus, both the performance metrics demonstrate that how accurately the technique is able to detect the tampered areas in an image.

4.2. Effectiveness and accuracy test

In order to evaluate the effectiveness and accuracy test, various experiments are performed to detect the images tampered by translation operation. In translation tampering operation, the desired area is simply copied and pasted to a different area in the same image. In literature, the block-based techniques split the input image into overlapping blocks to detect the tampered areas. It is important to mention here that irregular shaped and multiple duplicated areas affect the values of TDR and FDR. Therefore, three different experiments of translation operation for regular shaped, irregular shaped and multiple duplicated areas are performed to analyze the performance of the proposed CMFD technique. In these experiments, all the manipulated images are devoid of any image and post-processing operations. The first experiment is performed for regular shaped tampered areas of size 32×32, 64×64, and 96×96 pixels. The experimental results of the proposed technique are presented in Fig. 7. The forged images shown in the top row of Fig. 7(a–c), are with a duplicated area of size 32×32, 64×64, and 96×96 pixels respectively whereas the bottom row of Fig. 7(d–f), is showing the duplication revealing results of the technique. The value of TDR = 1 and FDR = 0 for Fig. 7(d–f), reveal that the proposed CMFD technique has the ability to unveil the tampering effectively and accurately.

The second experiment is carried out to show the results of the proposed technique when the tampered areas have irregular shapes. The experimental results using three different sample images are presented in Fig. 8, where the first forged image is selected from the CoMoFoD dataset and the remaining two images are taken from the UCID dataset to create forged images. The forged images are given in the top row of Fig. 8(a–c) whereas the detection results are presented in Fig. 8(d–f). The TDR = 1 for Fig. 8(e–f) and FDR = 0.001, 0.015 indicate that the proposed technique identifies the tampered areas in a true manner. However, TDR for Fig. 8(a) is approximately 0.99 because the proposed technique marks some area as forged erroneously and FDR is 0.009, which is almost negligible.

The third experiment is performed to present the usefulness of the technique when images have multiple tampered areas. The detection results using three sample images are presented in Fig. 9, where again the first forged image is selected from the CoMoFoD dataset and the remaining two images are taken from the UCID dataset to create forged images. The forged images are given in the upper row of Fig. 9(a–c) whereas Fig. 9(d–f) is presenting the detection results. The TDR = 1 for Fig. 9(e–f) and FDR = 0.003, 0.001 indicate that the proposed technique identifies the tampered areas in a true manner. However, TDR for Fig. 9(a) is 0.997 because the proposed technique marks some area as forged erroneously and FDR is 0.003, which is almost negligible.

4.3. Robustness test

Usually, a counterfeiter applies different post-processing operations to conceal the visual marks of the tampering attacks. Therefore, the capability to resist against the post-processing operations is important for CMFD techniques. The most commonly used post-processing operations are image blurring, JPEG compression, color reduction and brightness change. In this section, we present experimental details in which different post-processing operations are applied to the tampered images.

Visual experimental results exhibit that the proposed technique can detect tampered areas efficiently even if the manipulated images have undergone post-processing operations. The CoMoFoD dataset contains tampered images with blurring operation that are produced using three different averaging filters (3×3,5×5, and 7×7). The same averaging filters are used to produce blurred images taken from the UCID dataset as well. Detection results of the tampered images using 7×7 averaging

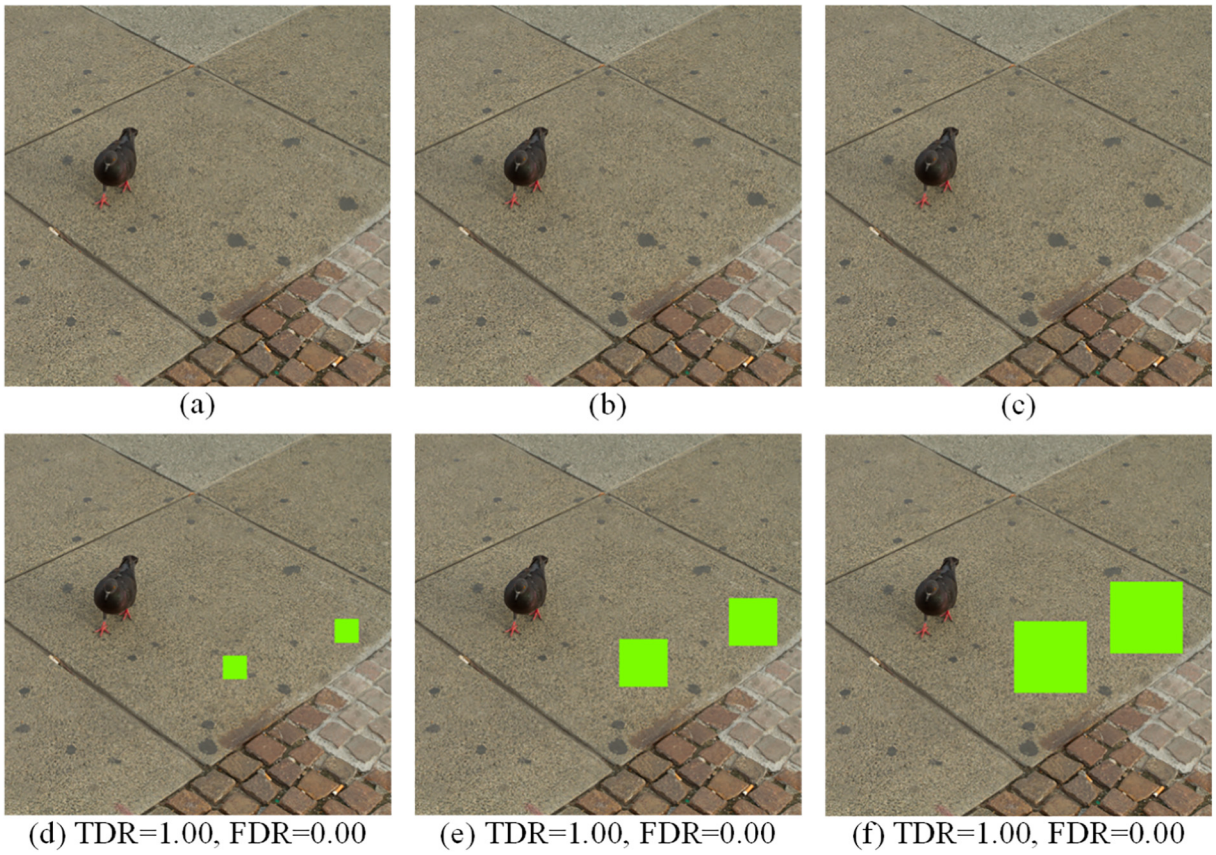

Fig. 7. Visual results for translation operation with regular shaped tampered areas.

filter are given in Fig. 10(c) and (f). Fig. 10(b) and (e) are showing that the tampered images that are noticeably altered due to the 7×7 averaging filter.

The experiments conducted to demonstrate the accuracy of the proposed technique under JPEG compression (quality levels = 80 and 85) are exemplified in Fig. 11. The results are showing that the proposed CMFD technique is also robust to JPEG compression attack.

The effectiveness of the proposed technique is also evaluated for the

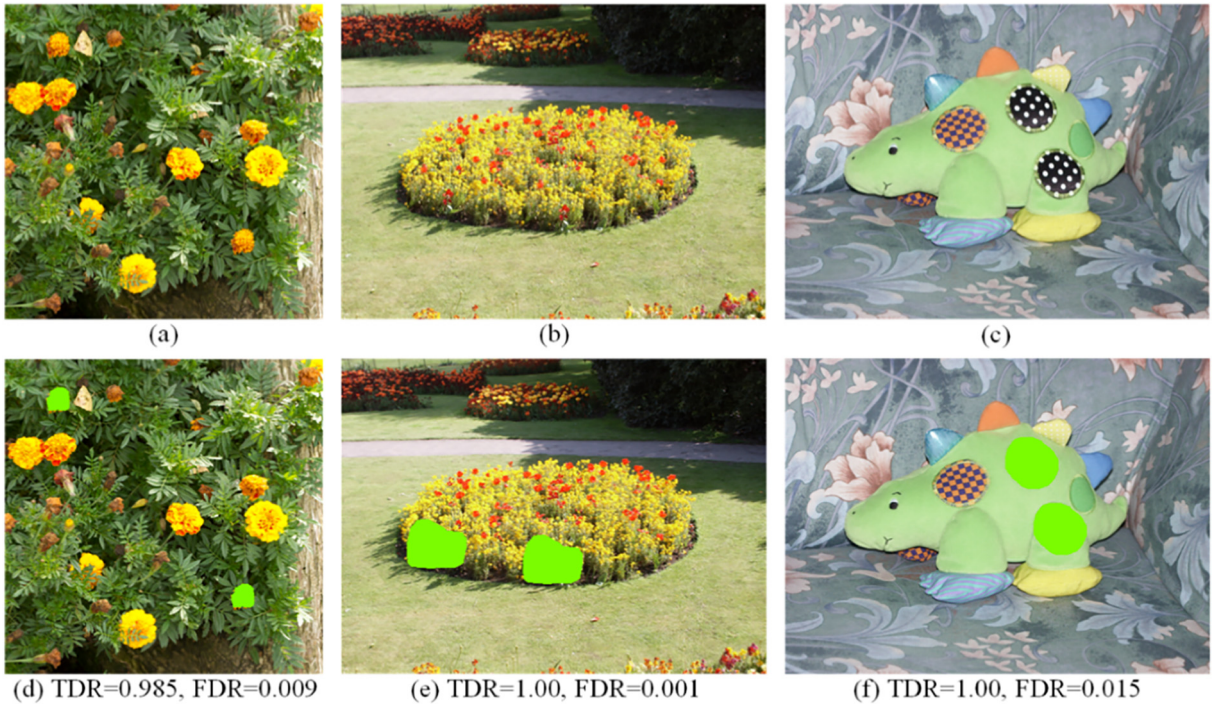

Fig. 8. Visual results for translation operation with irregular shaped tampered areas.

Fig. 9. Visual results for translation operation with multiple tampered areas.

manipulated images contaminated with color reduction operation. In this test, the manipulated images from the CoMoFoD dataset are used that are generated through uniform quantization of the image intensity values. The channels of all the forged images were uniformly reduced in different channels such as 256–128, 64, 32 respectively. The images manipulated using the color reduction operation have approximately imperceptible degradation as compared to the original images. Fig. 12 is showing the detection results of the proposed CMFD technique when color reduction operation is applied to the forged image. The visual results indicate that the proposed CMFD technique performed well when color reduction operation is applied to the forged images.

In the last test, we gauged the efficacy of the proposed CMFD technique for the images selected from the CoMoFoD dataset as well. The brightness change operations on the forged images contained in the CoMoFoD dataset are applied in the range $[0, 1]$. Hence, three different manipulated images with brightness ranges ($[0.01, 0.95]$, $[0.01, 0.9]$

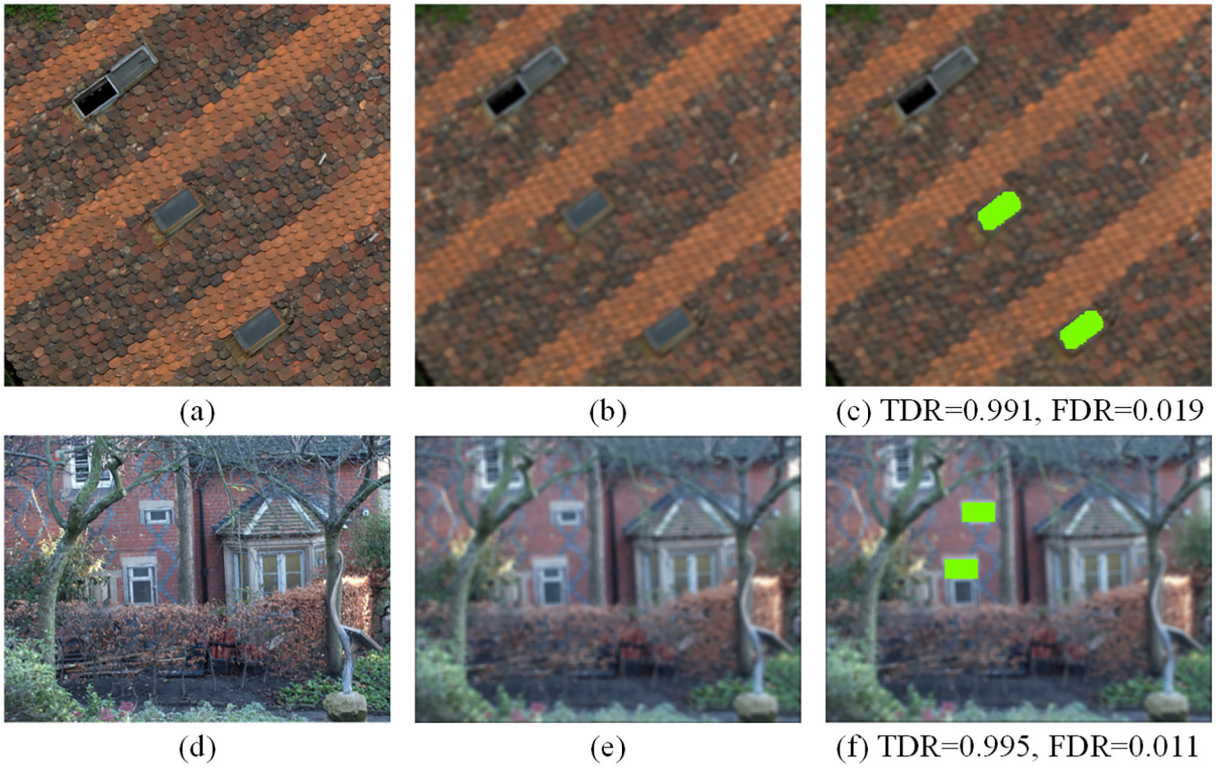

Fig. 10. Visual results for blurring operation using averaging filter of size (7×7).

Fig. 11. Visual results for JPEG compression operation.

Fig. 12. Visual results for color reduction operation.

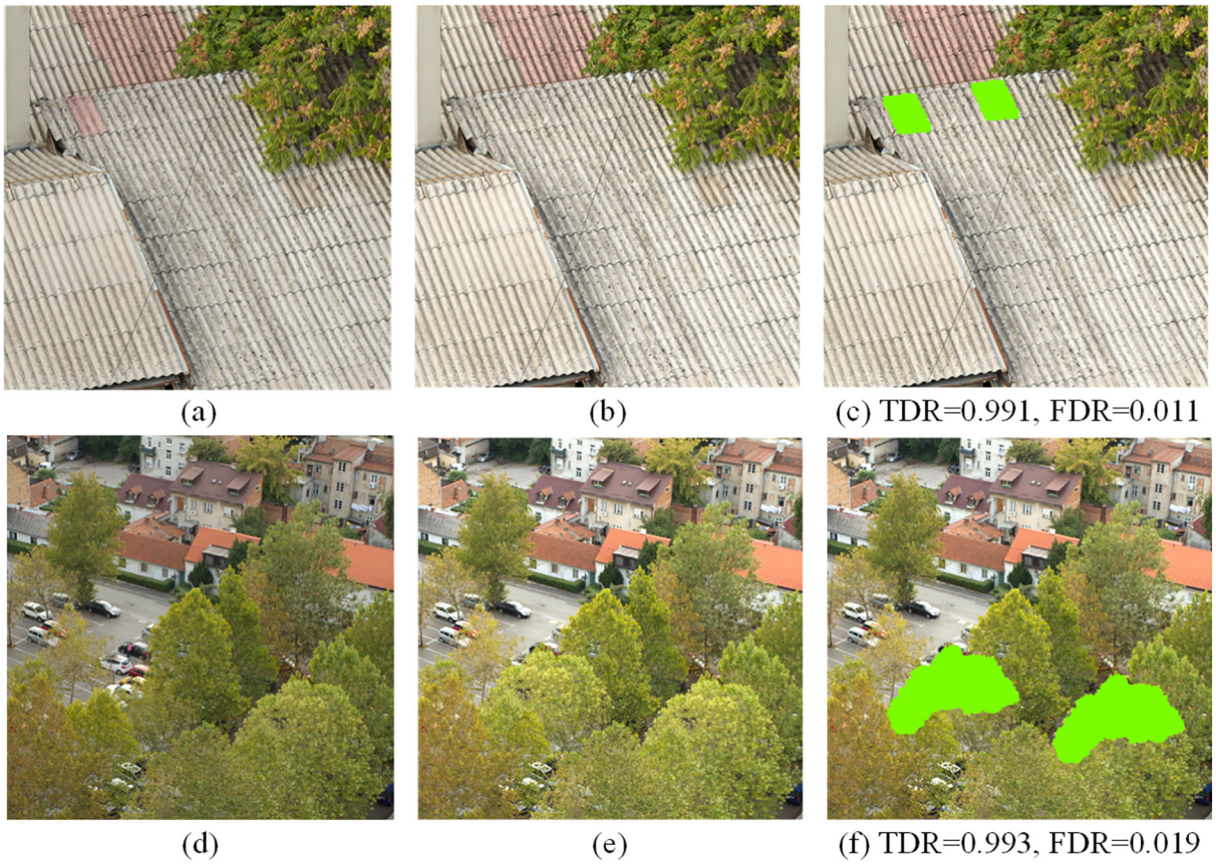

Fig. 13. Visual results for brightness change operation.

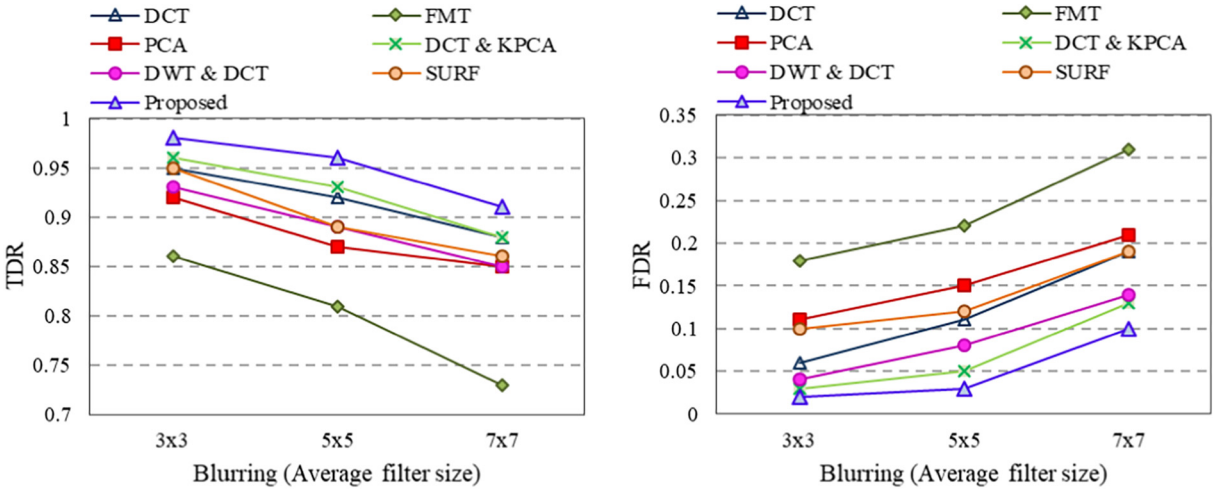

Fig. 14. Average detection rates for blurring operation using different averaging filters.

and [0.01, 0.8]) are produced. To demonstrate the effectiveness of the technique, the forgery detection results with brightness change operation in the range [0.01, 0.9] (Row 1) and [0.01, 0.8] (Row 2) are represented in Fig. 13(c) and (f), respectively. The detection results reveal that the proposed technique is capable of detecting the image forgeries precisely.

4.4. Comparison test

Experimental results given in Sections 4.2 and 4.3 reveal the effectiveness of the proposed CMFD technique. This section finally compares the proposed CMFD technique with existing state-of-the-art techniques: DCT-based [23], FMT-based [25], PCA-based [24], DCT& KPCA-based [28], and, DWT&DCT-based [12]. In order to test the performance of the technique, the experiments are conducted over more than 250 images selected from the CoMoFoD and UCID datasets.

The overall average performance comparison with blurring (averaging filter), JPEG compression, color reduction and brightness change operations is shown in Figs. 14–17, respectively. In the case of blurring, Fig. 14 is showing the results where the manipulated images are blurred through different averaging filters. It is observed from the experimental results that reducing the kernel of averaging filter results in higher TDR and lower FDR for all the techniques. Furthermore, the TDR curve of the proposed CMFD technique achieves higher accuracy than other

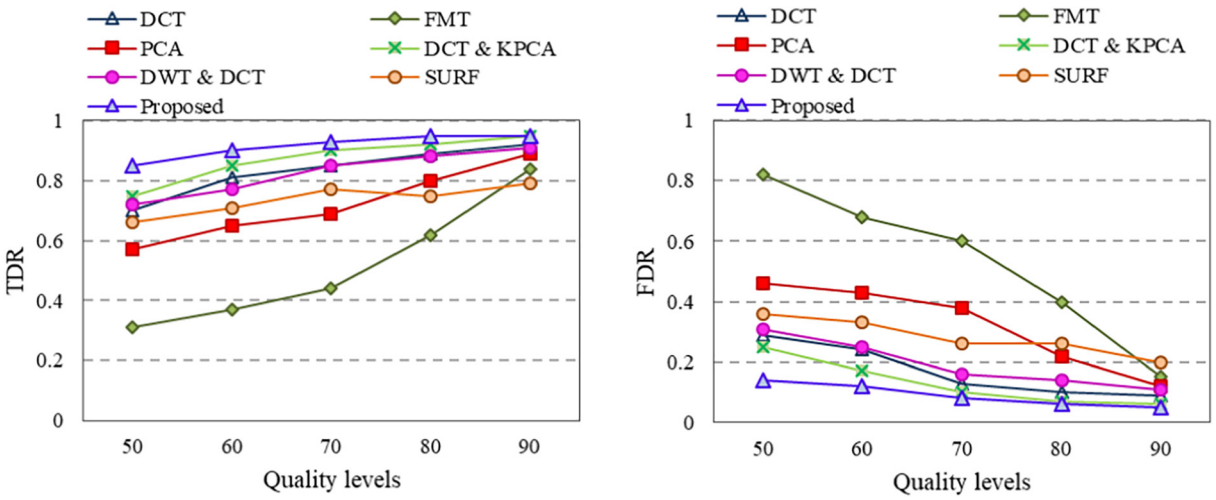

Fig. 15. Average detection rates for JPEG compression operation with different quality levels.

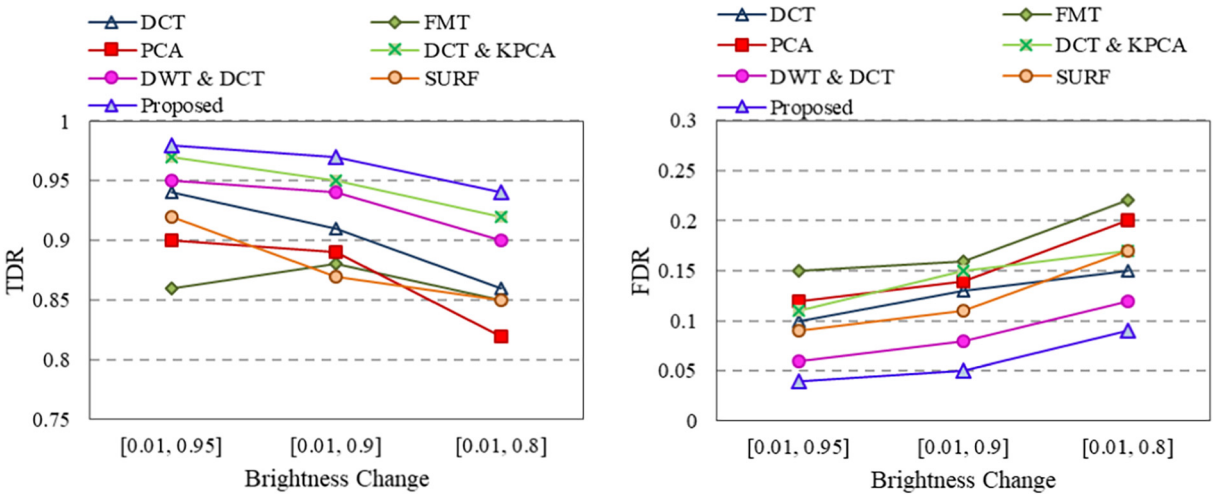

Fig. 16. Average detection rates for brightness change operation.

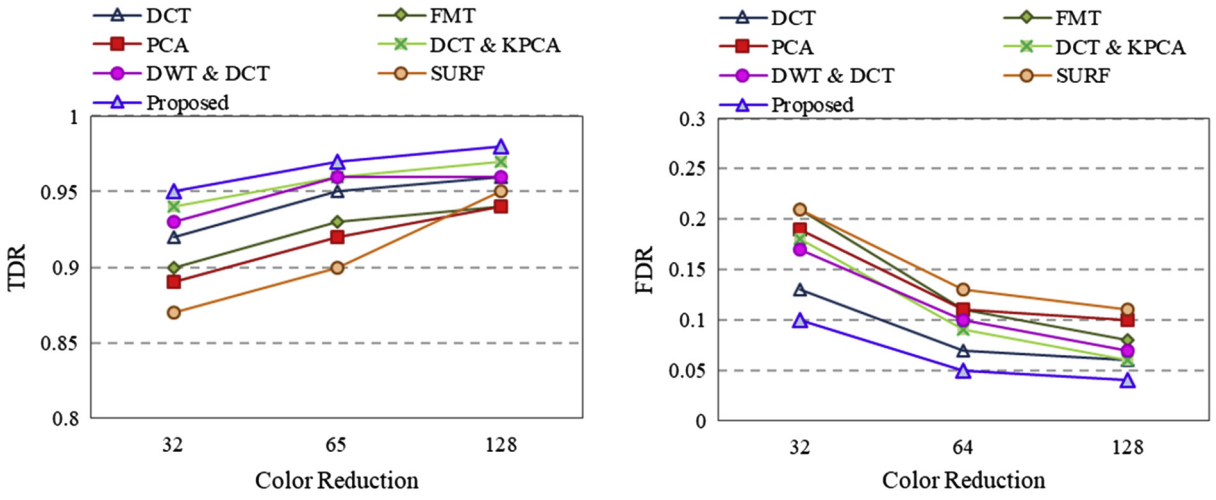

Fig. 17. Average detection rates for color reduction operation.

techniques with TDR > 90%, even when the kernel of averaging filter is increased. The FDR curve also gives a satisfactory performance that the proposed CMFD technique has lower FDR even with the larger averaging filter kernel of size (7 × 7). In the case of JPEG compression, Fig. 15 is showing the detection results when the tampered images are contaminated with different compression levels (Q = 50, 60, 70, 80 and 90). The TDR and FDR curves are presenting that the proposed CMFD technique shows better accuracy rate compared to other techniques

when the images were compressed slightly. Fig. 16 is depicting the detection performance for the tampered images when brightness change is achieved in different ranges ([0.01, 0.95], [0.01, 0.9] and [0.01, 0.8]). The TDR and FDR curves show that the proposed technique outperformed the other technique even when the brightness level is increased with TDR ≥ 94%. The FDR curve also exhibits that the proposed technique has lower FDR as compared to other techniques. A similar behavior is observed for the color reduction operation as well. Fig. 17 is indicating the results when the color of the tampered images was reduced in three different intensity ranges (256 to 128, 64 and 32). The average detection results indicate that the proposed CMFD technique provides better detection even at the higher intensity level.

5. Conclusion

We have proposed a robust technique for exposing CMF detection and localization in digital images for forensic applications. CMF detection in the digital images is investigated through the use of approximation subband of shift-invariant SWT based features. The SWT does not involve decimation procedure, which results in a larger length of the feature vector. Thus, DCT is applied to obtain a reduced length of feature vectors. The results of the proposed CMFD technique reveals significant improvement against other techniques in the presence of different forms of tampering and image operations e.g. translation, blurring, JPEG compression, brightness change, color reduction, and translation operation with multiple tampered areas. The experimental results reveal that the proposed CMFD technique outperforms the existing techniques in terms of TDR and FDR. As the proposed technique is capable of detecting image forgeries under different image operations. Therefore, the proposed technique can play a vital role in various proof centric image forensic applications.

Nevertheless, image tampering can be obscured by adopting other means such as larger scaling, rotation, inpainting, additive noise, contrast adjustment or a blend thereof. The post-processing operations make the detection of CMF even far more challenging. Therefore, we are in the process of developing new techniques to handle these issues in efficient manners.

Acknowledgments

This work was partially supported by the Machine Learning Research Group; Prince Sultan University Riyadh; Saudi Arabia [RG-CCIS-2017-06-02]. The authors are grateful for this financial support.

References

[1] M. Islam, M. Shah, Z. Khan, T. Mahmood, M.J. Khan, A new symmetric key encryption algorithm using images as secret keys, in: 2015 13th International Conference on Frontiers of Information Technology (FIT), 2015, pp. 1–5.
[2] D.M. Uliyan, H.A. Jalab, A.W.A. Wahab, P. Shivakumara, S. Sadeghi, A novel forged blurred region detection system for image forensic applications, Expert Syst. Appl. 64 (2016) 1–10.
[3] A.U. Islam, F. Khalid, M. Shah, Z. Khan, T. Mahmood, A. Khan, et al., An improved image steganography technique based on MSB using bit differencing, in: 2016 Sixth International Conference on Innovative Computing Technology (INTECH), 2016, pp. 265–269.
[4] G. Kessler, An Overview of Steganography for the Computer Forensics Examiner. An edited version, issue of Forensic Science Communications, Technical Report, 62004.
[5] Z. Khan, M. Shah, M. Naeem, D. Shahzad, T. Mahmood, LSB steganography using bits complementation, in: International Conference on Chemical Engineering and Advanced Computational Technologies (ICCEACT), 2014.
[6] Z. Khan, M. Shah, M. Naeem, T. Mahmood, S.N.A. Khan, N.U. Amin, et al., Threshold based steganography: a novel technique for improved payload and SNR, Int. Arab J. Inform. Technol. 13 (2016) 380–386.
[7] C.S. Rao, S.T. Babu, Image authentication using local binary pattern on the low frequency components, in: Microelectronics, Electromagnetics and Telecommunications, Springer, 2016, pp. 529–537.
[8] P. Hayati, V. Potdar, E. Chang, A survey of steganographic and steganalytic tools for the digital forensic investigator, in: Workshop of Information Hiding and Digital Watermarking, 2007, pp. 1–12.
[9] A. Almohammad, R.M. Hierons, G. Ghinea, High capacity steganographic method based upon JPEG, in: Third International Conference on Availability, Reliability and Security, 2008. ARES 08, 2008, pp. 544–549.
[10] S. Khan, T. Khan, T. Mahmood, N. Ahmad, Analysis of data hiding in R, G and B channels of color image using various number of LSBs, in: 2016 Sixth International Conference on Innovative Computing Technology (INTECH), 2016, pp. 270–274.
[11] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra, A sift-based forensic method for copy–move attack detection and transformation recovery, Inform. Forensics Secur. IEEE Trans. 6 (2011) 1099–1110.
[12] K. Hayat, T. Qazi, Forgery detection in digital images via discrete wavelet and discrete cosine transforms, Comput. Electr. Eng. 62 (2017) 448–458.
[13] A. Ferreira, S.C. Felipussi, C. Alfaro, P. Fonseca, J.E. Vargas-Muñoz, J.A. dos Santos, et al., Behavior knowledge space-based fusion for copy-move forgery detection, IEEE Trans. Image Process. 25 (2016) 4729–4742.
[14] O.M. Al-Qershi, B.E. Khoo, Comparison of matching methods for copy-move image forgery detection, in: 9th International Conference on Robotic, Vision, Signal Processing and Power Applications, 2017, pp. 209–218.
[15] S.M. Fadl, N.A. Semary, Robust copy-move forgery revealing in digital images using polar coordinate system, Neurocomputing 265 (2017) 57–65.
[16] M.A. Qureshi, M. Deriche, A bibliography of pixel-based blind image forgery detection techniques, Signal Process. Image Commun. 39 (2015) 46–74.
[17] T. Mahmood, T. Nawaz, R. Ashraf, M. Shah, Z. Khan, A. Irtaza, et al., A survey on block based copy move image forgery detection techniques, in: 2015 11th International Conference on Emerging Technologies (ICET), 2015, pp. 1–6.
[18] K. Asghar, Z. Habib, M. Hussain, Copy-move and splicing image forgery detection and localization techniques: a review, Aust. J. Forensic Sci. 49 (2017) 281–307.
[19] V. Christlein, C. Riess, J. Jordan, C. Riess, E. Angelopoulou, An evaluation of popular copy-move forgery detection approaches, Inform. Forensics Secur. IEEE Trans. 7 (2012) 1841–1854.
[20] D. Tralic, I. Zupancic, S. Grgic, M. Grgic, CoMoFoD—new database for copy-move forgery detection, in: ELMAR, 2013 55th international symposium, 2013, pp. 49–54.
[21] G. Muhammad, M.H. Al-Hammadi, M. Hussain, G. Bebis, Image forgery detection using steerable pyramid transform and local binary pattern, Mach. Vis. Appl. 25 (2014) 985–995.
[22] A.J. Fridrich, B.D. Soukal, A.J. Lukáš, Detection of copy-move forgery in digital images, in: Proceedings of Digital Forensic Research Workshop, 2003.
[23] M.H. Alkawaz, G. Sulong, T. Saba, A. Rehman, Detection of copy-move image forgery based on discrete cosine transform, Neural Comput. Appl. (2016) 1–10, http://dx.doi.org/10.1007/s00521-016-2663-3.
[24] A.C. Popescu, H. Farid, Exposing digital forgeries by detecting duplicated image regions, TR2004-515, Technical Report, Dartmouth College, 2004.
[25] S. Bayram, H.T. Sencar, N. Memon, An efficient and robust method for detecting copy-move forgery, in: Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on, 2009, pp. 1053–1056.
[26] Y. Li, Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching, Forensic Sci. Int. 224 (2013) 59–67.
[27] J. Zhao, J. Guo, Passive forensics for copy-move image forgery using a method based on DCT and SVD, Forensic Sci. Int. 233 (2013) 158–166.
[28] T. Mahmood, T. Nawaz, A. Irtaza, R. Ashraf, M. Shah, M.T. Mahmood, Copy-move forgery detection technique for forensic analysis in digital images, Math. Probl. Eng. 2016 (2016) 1–13.
[29] M. Zandi, A. Mahmoudi-Aznaveh, A. Mansouri, Adaptive matching for copy-move forgery detection, in: Information Forensics and Security (WIFS), IEEE International Workshop on, 2014, pp. 119–124.
[30] J.-C. Lee, C.-P. Chang, W.-K. Chen, Detection of copy–move image forgery using histogram of orientated gradients, Inform. Sci. 321 (2015) 250–262.
[31] E. Silva, T. Carvalho, A. Ferreira, A. Rocha, Going deeper into copy-move forgery detection: exploring image telltales via multi-scale analysis and voting processes, J. Vis. Commun. Image Represent. 29 (2015) 16–32.
[32] G. Liu, J. Wang, S. Lian, Z. Wang, A passive image authentication scheme for detecting region-duplication forgery with rotation, J. Network Comput. Appl. 34 (2011) 1557–1565.
[33] K. Mahmoud, A. Abu-AlRukab, Copy-move forgery detection using zernike and pseudo zernike moments, Int. Arab J. Inform. Technol. 13 (2016) 930–937.
[34] Y. Yao, Y. Shi, S. Weng, B. Guan, Deep learning for detection of object-based forgery in advanced video, Symmetry 10 (2017) 3.
[35] Y. Rao, J. Ni, A deep learning approach to detection of splicing and copy-move forgeries in images, in: Information Forensics and Security (WIFS), 2016 IEEE International Workshop on, 2016, pp. 1–6.
[36] J. Fridrich, J. Kodovsky, Rich models for steganalysis of digital images, IEEE Trans. Inform. Forensics Secur. 7 (2012) 868–882.
[37] J. Zhou, J. Ni, Y. Rao, Block-based convolutional neural network for image forgery detection, in: International Workshop on Digital Watermarking, 2017, pp. 65–76.
[38] I. Amerini, T. Uricchio, L. Ballan, R. Caldelli, Localization of JPEG double compression through multi-domain convolutional neural networks, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2017, pp. 53–59.
[39] S. Chaplot, L. Patnaik, N. Jagannathan, Classification of magnetic resonance brain images using wavelets as input to support vector machine and neural network, Biomed. Signal Process. Control 1 (2006) 86–92.
[40] T. Mahmood, T. Nawaz, Z. Mehmood, Z. Khan, M. Shah, R. Ashraf, Forensic analysis of copy-move forgery in digital images using the stationary wavelets, in: Innovative Computing Technology (INTECH), 2016 Sixth International Conference on, 2016, pp. 578–583.
[41] T. Mahmood, A. Irtaza, Z. Mehmood, M.T. Mahmood, Copy–move forgery detection through stationary wavelets and local binary pattern variance for forensic analysis

in digital images, Forensic Sci. Int. 279 (2017) 8–21.
[42] J.-C. Lee, Copy-move image forgery detection based on Gabor magnitude, J. Vis. Commun. Image Represent. 31 (2015) 320–334.
[43] G. Li, Q. Wu, D. Tu, S. Sun, A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD, in: Multimedia and Expo, 2007 IEEE International Conference on, 2007, pp. 1750–1753.
[44] M. Zimba, S. Xingming, DWT-PCA(EVD) based copy-move image forgery detection, Int. J. Digital Content Technol. Appl. 5 (2011) 251–258.
[45] T. Mahmood, T. Nawaz, M. Shah, Z. Khan, R. Ashraf, H.A. Habib, Copy-move forgery detection technique based on DWT and Hu Moments, Int. J. Comput. Sci. Inform. Secur. 14 (2016) 156–161.
[46] R.R. Coifman, D.L. Donoho, Translation-invariant De-noising, Springer, New York, 1995.
[47] J.-L. Starck, J. Fadili, F. Murtagh, The undecimated wavelet decomposition and its reconstruction, Image Process. IEEE Trans. 16 (2007) 297–309.
[48] G. Muhammad, M. Hussain, G. Bebis, Passive copy move image forgery detection using undecimated dyadic wavelet transform, Digital Invest. 9 (2012) 49–57.
[49] T. Mahmood, Z. Mehmood, M. Shah, Z. Khan, An efficient forensic technique for exposing region duplication forgery in digital images, Appl. Int. (2017) 1–11.
[50] Y. Cao, T. Gao, L. Fan, Q. Yang, A robust detection algorithm for copy-move forgery in digital images, Forensic Sci. Int. 214 (2012) 33–43.
[51] G. Schaefer, M. Stich, UCID: an uncompressed color image database, Electron. Imag. 2003 (2004) 472–480.