Appl Intell (2018) 48:1791–1801
DOI 10.1007/s10489-017-1038-5

An efficient forensic technique for exposing region duplication forgery in digital images

Toqeer Mahmood[1] · Zahid Mehmood[2] · Mohsin Shah[3,4] · Zakir Khan[3]

Published online: 7 September 2017

Abstract The internet users share a massive amount of digital images daily. The accessibility of powerful image manipulation tools has made the integrity of image contents questionable. The most popular image tampering is to duplicate a region elsewhere in the same image to replicate or conceal some other region. The duplicated regions have identical color and texture attributes that make this artifact invisible to the human eye. Therefore, efficient techniques are required to verify the credibility of image contents by detecting the regions duplicated in the digital images. This paper proposes an efficient technique for exposing region duplication forgery in digital images. The proposed technique divides the approximation (LL) sub-band of shift invariant stationary wavelet transform into overlapping blocks of $w \times w$ (i.e. $w = 4, 8$) sizes. The distinctive features extracted from the overlapping blocks are utilized to expose the region duplication forgeries in digital images. The experimental results of the proposed technique are compared with state-of-the-art techniques that reveal the prominence, and effectiveness of the proposed technique in terms of precision, recall and F_1 score for different block sizes. Therefore, the proposed technique can reliably be applied to identify the counterfeited regions and the benefits of the proposed technique can be achieved in different fields for example crime investigation, news reporting, and judiciary.

Keywords Digital forensics · Region duplication · Copy-move · Image tampering · Passive authentication

✉ Toqeer Mahmood
toqeer.mahmood@uettaxila.edu.pk;
toqeer.mahmood@yahoo.com

Zahid Mehmood
zahid.mehmood@uettaxila.edu.pk

Mohsin Shah
syedmohsinshah@gmail.com; mohsin@mail.ustc.edu.cn

Zakir Khan
zakirk2012@gmail.com

1 Department of Computer Engineering, University of Engineering and Technology, Taxila, Pakistan

2 Department of Software Engineering, University of Engineering and Technology, Taxila, Pakistan

3 Department of Information Technology, Hazara University, Mansehra, Pakistan

4 School of Information Science and Technology, University of Science and Technology of China, Hefei, China

1 Introduction

In the recent years, the internet, multimedia, and imaging technologies are playing an imperative role in our daily life. The internet users share a massive amount of multimedia contents such as text, audios, videos and images over the social media every day. The accessibility of high-resolution, inexpensive digital cameras and user-friendly image manipulation software have made the integrity of image contents questionable. The security concern of digital image contents arose a long time ago. Therefore, numerous techniques have been suggested to determine the truthfulness of image contents [1]. These techniques can be grouped into two classes: active and passive (blind) [2].

Digital watermarking [3] and digital signatures [4] fall into the active class. Watermarking requires embedding of watermark robust to tampering attacks into the image for content verification. Digital signature requires transmission of image signature and a private key generated by an algorithm with the original image. As both the techniques require additional information, they are grouped as active techniques. The requirement of additional information also makes the application of such technique limited in practice [5].

Consequently, passive techniques have gained more attention of the researchers recently. A substantial amount of research is focused on region duplication (or copy-move) forgery detection (RDFD) [1]. In region duplication forgery (RDF), an image region is duplicated onto a different region of the same image, with the aim of concealing or replicating some essential contents [2]. Since the source and destination of duplicated regions are the same image, they have identical color and texture attributes that make the tampering more effective. Figure 1 demonstrates the examples of RDF attack. For the examples presented in the left column of Fig. 1, a region is duplicated to conceal undesirable objects in the authentic image. In the other case, an object is replicated to create contents that are not in the authentic image. The duplicated regions are well blended at the desired locations, and become very difficult to identify visually. To investigate the image RDF, there exist two types of systems: keypoint-based and block-based [6]. The keypoint-based systems compute features only on image regions with high entropy. Subsequently, similar features within the image are matched in order to detect the RDF [7]. In contrast, block-based systems sub-divide an image into square blocks and

Authentic image Tampered image

Fig. 1 Examples showing the RDF attack

extract feature representation for each block. Thereafter, all the features of image blocks undergo a matching process of similarity check.

This paper proposes an efficient technique for RDFD in digital images using the low approximation (LL) sub-band of the stationary wavelet transform (SWT). The proposed technique analyzes the similarity between image regions for tampering detection. The SWT is a translation invariant transform that makes it distinctive over the discrete wavelet transform (DWT) and is more appropriate for detection of duplicated regions. Most of the existing studies mentioned in the related work (Section 2) use an overlapping block of size 8×8 pixels for detection of region duplication image forgeries. However, what if the block size is different? Therefore, different block sizes (4×4, and 8×8) are used to investigate the effects of block size on accuracy detection. The study shows that the selection of block size needs attention while evaluating the accuracy of the system in terms of precision and recall. Thus, the following concerns are considered in this study:

- What is the most suitable block size in order to get higher accuracy performance (precision and recall)?
- What is the effect of block size on block regions that are falsely detected as duplicated (false positive) and the duplicated regions that are falsely missed (false negative) during the comparison and matching step?

In addition, the results of the proposed technique are compared with state-of-the-art techniques [8–10], that shows the prominence and effectiveness of the proposed technique. Compared to [8–10], the key benefits of the proposed technique are:

- Utilization of reduced size feature vectors for blocks representation,
- Lower computational complexity, and
- Unveiling multiple region-duplication forgeries efficiently.

The paper is arranged as follows: Section 2, presents the overview of related work in the domain of RDFD. The proposed technique is described in Section 3. The experiments are discussed in Section 4. Finally, the concluding notes are given in Section 5.

2 Related work

In literature, many techniques have been proposed for RDFD. Fridrich et al. [11], suggested the first technique for RDFD using DCT. The technique divides the image into small overlapping blocks. The DCT coefficients obtained from overlapping blocks forms the features vectors. The drawback of the technique is high computational time.

Popescu and Farid [12], utilized principal components analysis (PCA) to reduce the length of feature vectors of [11] for detecting the duplications. Myna et al. [13] proposed a technique utilizing log-polar coordinates and wavelet transform for RDFD. Exhaustive searching is performed for duplication detection by mapping the similar blocks to log-polar coordinates, however, a phase correlation is adopted for similarity test. Christlein et al. [14], presented a technique using Fourier-Mellin transform (FMT) based features and *kd*-tree are employed for similarity measure. This technique performed excellently in the absence of geometric transformations over the duplicated blocks. Ryu et al. [15] suggested a scheme for duplication detection by using the Zernike moments of the image blocks as rotation invariant features. Huang et al. [16], proposed an improved DCT coefficients based technique to detect the duplicated regions. The length of feature vectors is reduced through truncation process to only [$p \times B^2$] elements. The DCT coefficients are quantized to make the technique effective against the compression attack. Zimba and Xingming [9], proposed a technique by combining the DWT and PCA for duplication detection, however, the technique is not efficient. Muhammad et al. [17], suggested an RDFD technique through the undecimated dyadic wavelet transform (DyWT). The proposed technique employees LL1 and HH1 sub-bands of DyWT for forgery detection. Sekeh et al. [18], exposed the tampering in digital images through a block clustering technique. The algorithm generates clusters of similar blocks and feature matching is performed within the same clusters. Lynch et al. [19], came up with an expanding block algorithm for RDF detection. This technique performed well against image post-processing operations or when the tampered areas are made lighter or darker. YunJie et al. [20], proposed a technique based on dual-tree complex wavelet transform. The method performed better for rotated duplicated regions and JPEG compressed images. Alahmadi et al. [21], suggested a duplication detection method utilizing LBP and DCT based features. The classification of images is performed using SVM. Ulutas et al. [22], proposed a frame and mirroring detection technique through binary features. The technique is shown to be efficient for duplication detection with lower computational time. Hayat and Qazi [10], proposed a masked-based technique using DWT and DCT for region duplication detection. First, the low approximation sub-band of DWT is extracted that followed the application of DCT over the small overlapping image blocks for RDFD.

3 The proposed technique for RDFD

This section presents an efficient block-based forensic technique for exposing RDF in digital images utilizing the translation invariant SWT. Different from existing techniques, the proposed technique further splits image blocks (4×4 and 8×8) into four triangular regions in order to obtain the reduced feature vector length. Hence, the algorithm extracts moment of the first order as features corresponding to each triangular region that is further utilized for duplication detection.

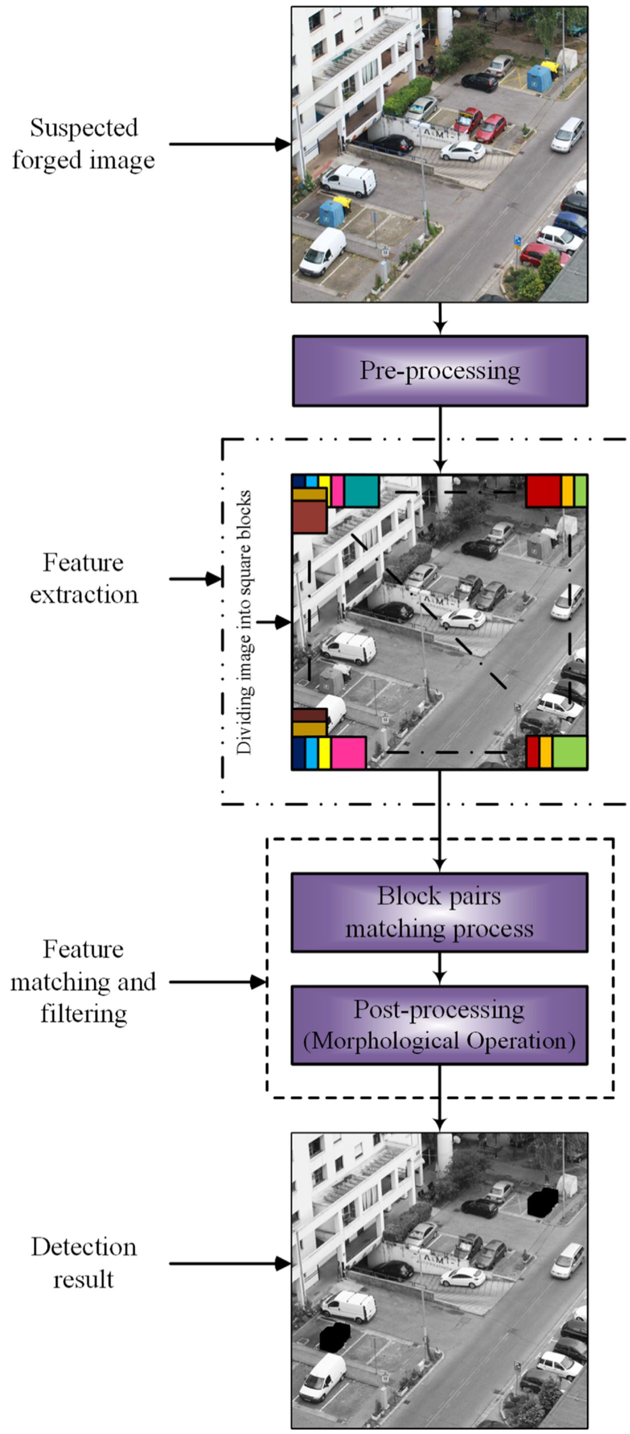

Fig. 2 The framework of the proposed technique based on SWT for RDFD

The discussion above draws forth the framework of the proposed RDFD technique as depicted in Fig. 2. The implementation details of the proposed technique are given in the following sub-sections.

3.1 Pre-processing the question image

We have taken an RGB color image and transformed it into YC_bC_r color space, represented by the following mathematical equations;

$$Y = \left(\frac{77}{256}\right) R + \left(\frac{150}{256}\right) G + \left(\frac{29}{256}\right) B$$
$$C_b = -\left(\frac{44}{256}\right) R - \left(\frac{87}{256}\right) G + \left(\frac{131}{256}\right) B + 128$$
$$C_r = \left(\frac{131}{256}\right) R - \left(\frac{110}{256}\right) G - \left(\frac{21}{256}\right) B + 128 \qquad (1)$$

where R (Red), G (Green) and B (Blue) are the three channels of the color image.

The YC_bC_r color space was adopted as a part of ITU-R BT.601 during the standardization process of digital video encoding. The YC_bC_r color space reflects the fact that the human eye can perceive the brightness of a given color due to variation in the wavelength of the light [23]. Moreover, the YC_bC_r color space contains the information in the form of separate channels that are luminance (grayscale) and chrominance (color) channels. The luminance channel of the YC_bC_r color space holds more spatial information as comparted to the channels of other color spaces such as RGB color space channels. Therefore, the luminance channel (Y) of the YC_bC_r color space is adopted for region duplication forgery detection in digital images that is denoted by GI.

3.2 Feature extraction

The proposed technique decomposes GI into different sub-bands of translation invariant SWT. In SWT, the input 2D image is convolved by applying low (l) and high (h) pass filters to obtain the approximation and detailed coefficients. The detailed discussion on SWT could be found in literatures [24] and [25].

For an image GI, of size $M \times N$, the SWT at ith level is given by:

$$LL_{i+1}(a, b) = \sum_x \sum_y l_x^i l_y^i LL_i(a + x, b + y) \qquad (2)$$

$$LH_{i+1}(a, b) = \sum_x \sum_y l_x^i h_y^i LL_i(a + x, b + y) \qquad (3)$$

$$HL_{i+1}(a, b) = \sum_x \sum_y h_x^i l_y^i LL_i(a + x, b + y) \qquad (4)$$

$$HH_{i+1}(a, b) = \sum_x \sum_y h_x^i h_y^i LL_i(a + x, b + y) \qquad (5)$$

where $a = 1, 2, 3, \ldots, M$; $b = 1, 2, 3, \ldots, N$.

The LL, LH, HL, and HH obtained using (02-05) of an image, represents the approximation, horizontal, vertical and diagonal sub-bands, respectively. The approximation (LL) sub-band of size $M \times N$ is further considered for implementation of the proposed RDFD technique, which is most suitable for detection of duplicated regions.

Therefore, the proposed technique divides LL into overlapping blocks B_i of size $w \times w$ pixels $(w = 4, 8)$. Therefore, we can obtain N_b of overlapping blocks from LL.

$$N_b = (M - w + 1) \times (N - w + 1) \qquad (6)$$

Table 1 Computational complexity comparison in terms of feature length

Techniques	Block size	Feature	Feature length
Proposed technique	4 × 4	Moment of first order	4
	8 × 8		4
Alkawaz et al. [8]	4 × 4	DCT	16
	8 × 8		64
Zimba and Xingming [9]	8 × 8	DWT and PCA	7
Hayat and Qazi [10]	8 × 8	DWT and DCT	10

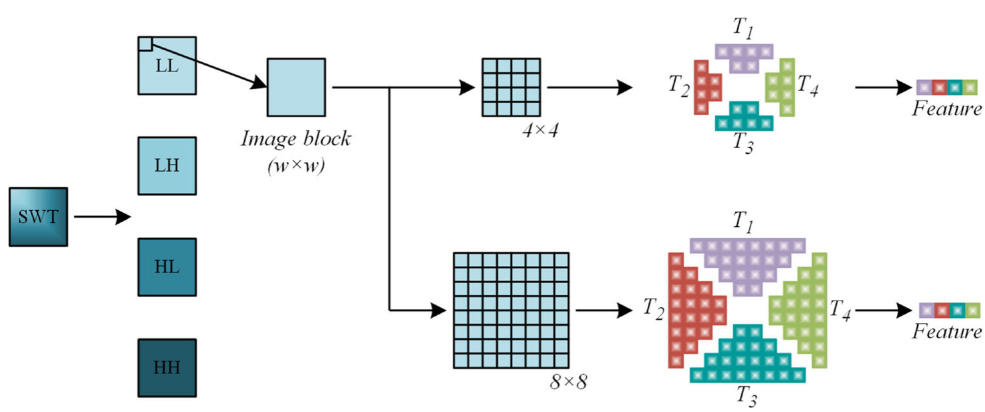

Fig. 3 Proposed triangular feature vector extraction process for different block sizes

Table 2 Computational complexity comparison (in seconds) for feature extraction from an image block

Techniques	Block size	
	4×4	8×8
Proposed technique	0.001	0.011
Alkawaz et al. [8]	0.19	0.023
Zimba and Xingming [9]	–	0.068
Hayat and Qazi [10]	–	.014

For feature extraction, the proposed technique further divides each block $B_i (i = 1, 2, 3 \ldots, N_b)$ into triangular regions T_1, T_2, T_3, T_4, as exemplified in Fig. 3. For each B_i, we represent $\mu_1, \mu_2, \mu_3, \mu_4$ as features of T_1, T_2, T_3, T_4 respectively. Hence, we obtain feature vectors for duplication detection through a mathematical representation, as follows:

$$\mu = \frac{\sum f(x, y)}{n}, (f(x, y) \in T_i, i = 1, 2, 3, 4) \tag{7}$$

where μ represents the moment of first order as features of B_k, corresponding to each T_i. Thus, features extracted from B_k can be arranged in a sequence to produce a feature vector of size 1×4 as described in (8)

$$\hat{\mu} = [\mu_1, \mu_2, \mu_3, \mu_4] \tag{8}$$

One additional problem related to block-based RDFD techniques is the computational complexity that is directly associated with the length of feature vectors and number of overlapping blocks. The feature matrix contains the number of blocks in the form of rows and the number of columns denotes the number of features. The lexicographic sorting, when applied over this matrix, is a major source of computational complexity. Therefore, the techniques with smaller length of feature vectors are computationally efficient compared to the techniques with larger length of feature vectors. A comparison between the proposed technique and state-of-the-art techniques [8–10] in terms of feature length is given in Table 1. In comparison with [8–10], the proposed technique utilizes the same size $w \times w$ pixels ($w = 4, 8$) of overlapping blocks B_i for an input image. However, the length of feature vector of the proposed technique is reduced, which indicates the proposed technique is more efficient and has lower computational complexity. A comparison of computational complexity (in seconds) of feature extraction from an image block B_k of size $w \times w$ pixels ($w = 4, 8$) is also shown in Table 2. Table 2 shows that the proposed technique is computationally efficient for feature extraction process as well compared to other techniques.

3.3 Similar block pairs searching

A feature matrix f_m of size $N_b \times 4$ is created by arranging all the feature vectors extracted according to the details given in Section 3.2, represented by following mathematical equation;

$$f_m = \begin{bmatrix} \widehat{\mu_1} \\ \widehat{\mu_2} \\ \vdots \\ \widehat{\mu_{N_b}} \end{bmatrix} \tag{9}$$

Before instigating the process of similar block pairs searching, the matrix f_m is sorted lexicographically and organizes all the feature vectors of similar blocks closer to each other. Thereby, sorting process reduces the similarity

Fig. 4 Images used in the experiments

search and makes the algorithm computationally more efficient. In the meantime, top left corner coordinates of all the image blocks B_i are recorded. The matrix f_m after sorting is denoted by f_{sm}.

Since the image blocks are overlapping and the duplicated regions are supposed to be non-overlapping, a block distance (T_{bd}) threshold is employed to make a decision, whether a pair of feature vectors corresponds to non-overlapping regions. For this, let us consider (x_i, y_i) and (x_j, y_j) are the top left corner coordinates of two blocks denoted by the feature vectors μ_i and μ_j of f_{sm}, then:

$$\forall\sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2} \geq T_{bd} \tag{10}$$

In addition, if a pair of feature vectors satisfy above block distance criteria (10), the proposed technique consider these feature vectors for similarity test to meet the second requirement of RDFD. Therefore, the proposed technique computes the similarity between two feature vectors using (11). If the distance of similarity is smaller than a preset threshold T_s, then the inquired image blocks will be considered as a candidate for RDF.

$$\widehat{\mu_i} = \left[\mu_i^1, \mu_i^2, \mu_i^3, \mu_i^4\right]$$
$$\widehat{\mu_j} = \left[\mu_j^1, \mu_j^2, \mu_j^3, \mu_j^4\right]$$
$$\forall\sqrt{\sum_{f=1}^{4}\left(\mu_i^f - \mu_j^f\right)^2} < T_s \tag{11}$$

3.4 Post-processing of duplication detection result

Finally, the proposed technique generates the desired output image I_o by highlighting all the duplicated blocks detected during the similar block pairs searching process as described in Section 3.3. The morphological opening operation is also applied to I_o to eliminate the isolated regions and to fill the holes in the highlighted regions of I_o.

4 Experimental results

The experimental results demonstrating the efficacy of the proposed technique are presented in this section. The performance of the technique is evaluated over a publically available image dataset (CoMoFoD [26]) designed for image duplication detection. All the experiments are carried out on a notebook computer with Intel $Ci5$ 2.4 GHz processor 6 GB RAM running $Matlab2015a$. The following sub-sections describe the testing dataset, parameter setup and evaluation metrics, visual results of the proposed technique and the accuracy performance comparison with other techniques.

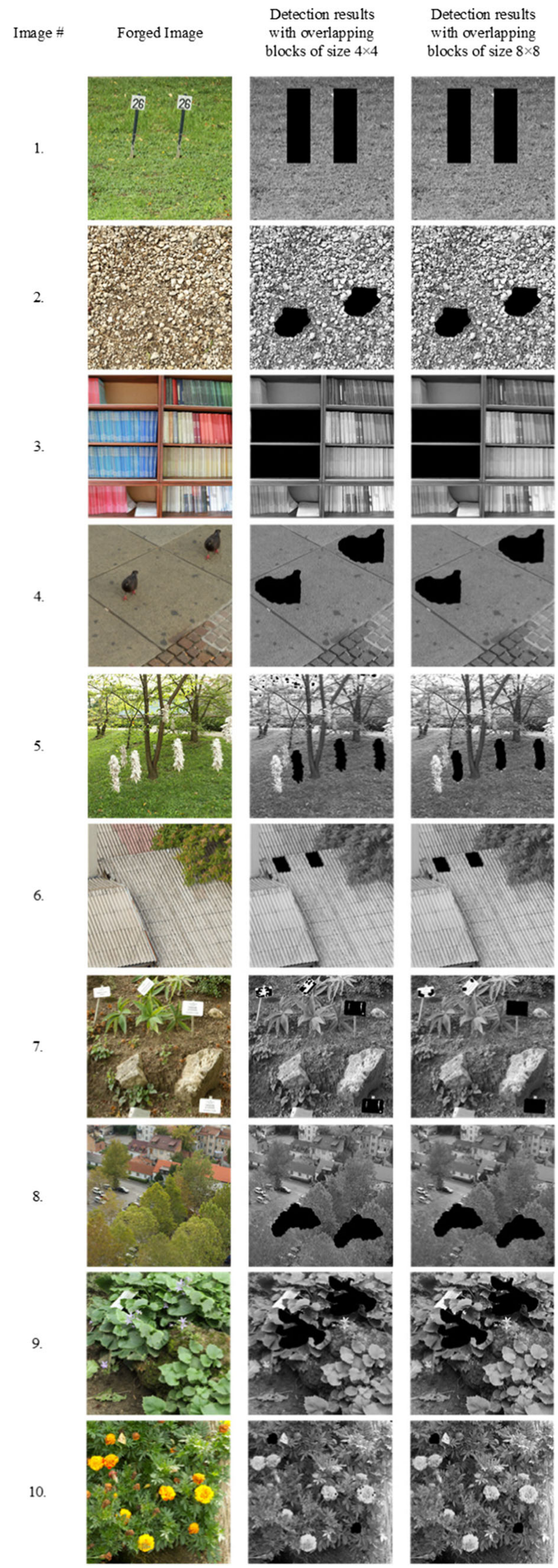

Fig. 5 Visual results of the proposed technique for overlapping blocks of size 4 × 4 and 8 × 8

4.1 Testing dataset

The CoMoFoD dataset comprises 100 original and 100 forged images with the size 512 × 512 pixels. The performance of the proposed technique is measured by comparing the detection results with the ground-truth image available with each forged image in the dataset. Each image implements block-based RDFD technique using the low approximation sub-band (LL) of SWT with the block size 4 × 4 and 8 × 8. The input images used in the experiments are presented in Fig. 4.

4.2 Parameter setup and evaluation metrics

In our experiments, all the parameter values are set as: $w = 4, 8$ (block size), $N_r = 10$ (No. of neighboring feature vectors to compare), $T_s = 0.0015$ (similarity threshold) and $T_{bd} = 40$ (block distance threshold).

The robustness of the proposed technique is evaluated using performance evaluation metrics known as precision 'p' and recall 'r' [8, 27] that are defined as follows:

$$p = \frac{FR \cap DR}{DR} \tag{12}$$

$$r = \frac{FR \cap DR}{FR} \tag{13}$$

where FR is the $forgedregion$ and DR is the $detectedregion$.

In addition, F_1 score is also computed by taking account of both the metrics 'p' and 'r'. Therefore, it reflects the overall accuracy of duplication detection. The F_1 score is defined [27] as follows:

$$F_1 = \frac{2 \times p \times r}{p + r} \tag{14}$$

4.3 Visual results of the proposed technique

In the proposed technique, we implemented a block based RDFD technique using the low approximation (LL) sub-band of SWT with overlapping blocks of size 4×4 and 8×8. In order to show the efficacy of the proposed technique, different experiments are realized with regular and irregular shaped forged regions. The RDF detection results of the proposed technique with overlapping blocks of size 4 × 4 and 8 × 8 are shown in Fig. 5. The visual results shown in Fig. 5 are demonstrating the algorithm is capable of unveiling forgeries in digital images precisely. However, the visual results presented in Fig. 5(5), (7), and (10), exhibit the block size 4 × 4 produces more false detection compared to block size 8 × 8. Here, it is important to note that false detection effects the accuracy of the duplication detection technique in terms of 'p' and 'r'.

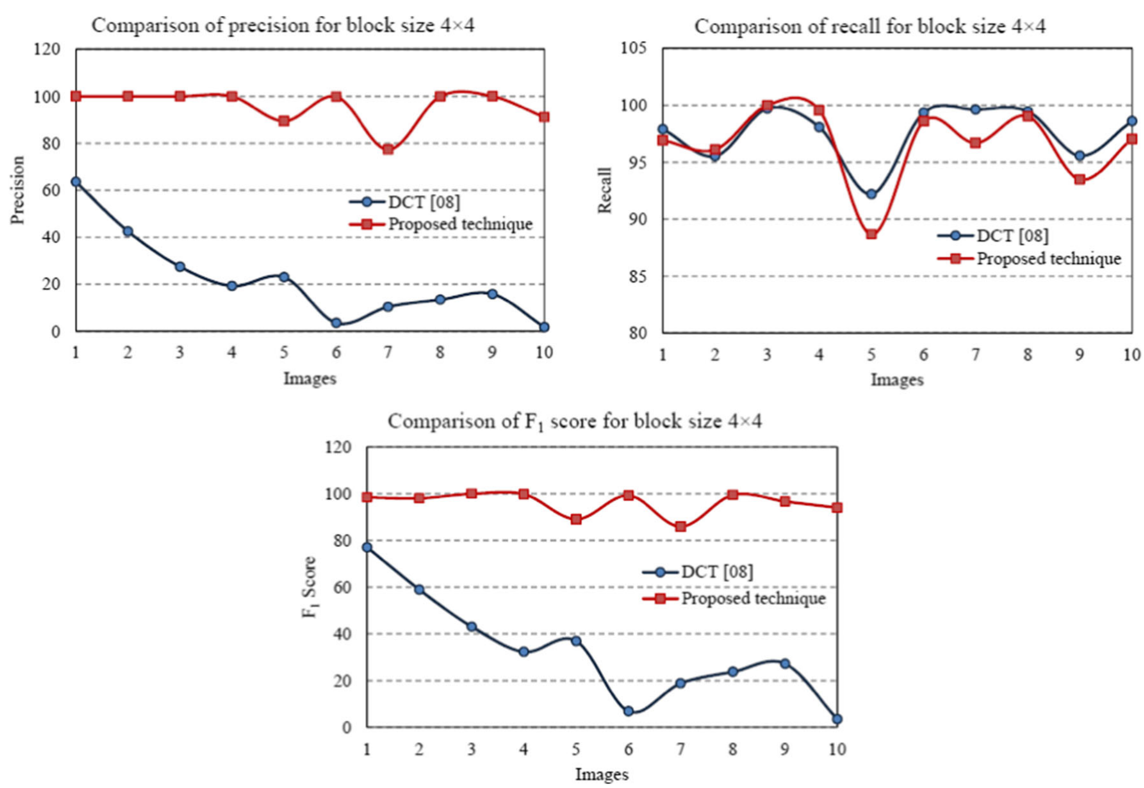

Fig. 6 Detection accuracy of forged images with state-of-the-art technique [8] for block size 4 × 4

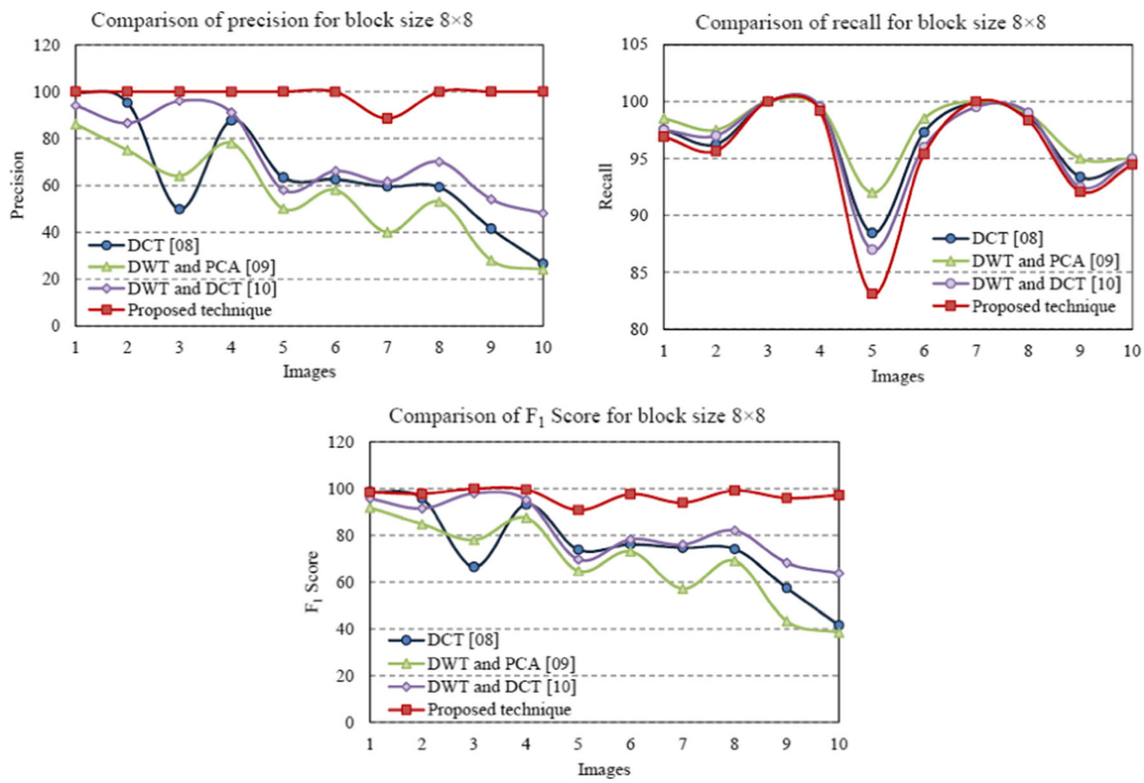

Fig. 7 Detection accuracy of forged images with state-of-the-art techniques [8–10], for block size 8 × 8

4.4 Comparison of accuracy performance

The duplication detection results of the proposed technique are compared with state-of-the-art techniques [8–10], for tampered images from the CoMoFoD dataset as described in Section 4.1. The accuracy of the proposed technique is measured through 'p' and 'r' and to visualize the overall accuracy of the proposed technique F_1 score is also computed as shown in Figs. 6 and 7. In our experiments, all the input images are tested to evaluate the effect of different overlapping blocks (4 × 4 and 8 × 8) for detecting the forgeries. The experimental results demonstrate that the performance of block size 4 × 4 is lower in terms of 'p' and 'r' as compared to block size 8 × 8.

The overlapping block size 4 × 4 identified the duplicated regions precisely. While a large number of image regions have been identified incorrectly as duplicated, it is also observed that the smaller block size increases similarity between image blocks, thereby increasing false matches during the detection process. Therefore, smaller block size affects the detection accuracy of the RDFD technique in terms of 'p'. On the contrary, overlapping block size 8 × 8 produced lower number of false matches as compared to block size 4 × 4. Therefore, block size 8 × 8 can perform more precisely for detecting the duplicated regions in terms of 'p'.

The detection of duplicated regions also affects the detection accuracy in terms of 'r'. It is observed that the overlapping block size 4 × 4 can produce larger accuracy in terms of 'r'. Due to the fact that small sized overlapping block can identify duplicated regions accurately. Moreover, small sized overlapping block decreases the number of false negative that is duplicated regions falsely missed in the process of duplication detection. The detection accuracy in terms of

Table 3 Comparison of average detection accuracy for block size 4 × 4

Techniques	Precision		Recall		F_1 scores	
	Average	Standard deviation	Average	Standard deviation	Average	Standard deviation
Proposed technique	95.763	7.644	96.606	3.389	96.05	4.911
DCT [8]	22.077	18.804	97.598	2.448	32.796	22.633

Table 4 Comparison of average detection accuracy for block size8×8

Techniques	Precision		Recall		F_1 scores	
	Average	Standard deviation	Average	Standard deviation	Average	Standard deviation
Proposed technique	98.835	3.621	95.518	5.053	97.028	2.839
DCT [8]	64.529	20.871	96.579	3.588	75.166	17.727
DWT and PCA [9]	55.600	20.871	97.490	2.650	68.764	18.168
DWT and DCT [10]	72.500	17.873	96.300	4.029	81.801	12.600

'r' for block size 8×8 is relatively lower than the block size 4×4 where if the regions are smaller in size than block size 8×8. For the analysis of overall detection accuracy, F_1 score is adopted for 4×4 and 8×8 overlapping block sizes. F_1 scores indicated that the overall accuracy of overlapping block size 8×8 is higher as compared to overlapping block size 4×4.

Figure 6 exhibit that the proposed technique has higher accuracies in detecting the duplicated regions in comparison to the technique of Alkawaz et al. [8] for block size 4×4. Furthermore, the plot of F_1 scores in Fig. 6 illustrate that the overall accuracy is greater than 86% in most of the cases. Figure 7 also demonstrates the similar response that the proposed technique has higher accuracies in detecting the duplicated regions in comparison to the techniques of Alkawaz et al. [8], Zimba and Xingming [9], and Hayat and Qazi [10] for block size 8×8. The plot of F_1 scores in Fig. 7 shows that the overall accuracy is greater than 91% for all the cases.

It is evident from the results given in Figs. 6 and 7 that the proposed technique outperformed DCT [8], DWT and PCA [9], and DWT and DCT [10] in terms of both the 'p' and 'r', due to the following reasons: a) the first order moment based features computed over the low approximation (LL) components of SWT are more discriminative compared to DCT [8], DWT and PCA [9], and DWT and DCT [10] based features, for that reason, decreases the occurrence of false positive and false negative, b) the post-verification process of the proposed technique is more capable of filtering out falsely matched identical block pairs. The superiority of the proposed technique is quite obvious with respect to the overall accuracy (F_1 scores) as can be observed from Figs. 6 and 7. The prominence of the proposed technique is also quite glaring with respect to the statistical results tabulated in Tables 3 and 4. As can be seen from the tables, the recall values of the proposed technique and the reference techniques are comparable for different block sizes. However, the precision values for different block sizes of the proposed technique are higher than that of DCT, DWT and PCA, and DWT and DCT, that demonstrates the strength of the proposed technique as the false detection rate is very low.

5 Conclusion

This paper has presented an efficient and effective technique for detecting duplicated regions in digital images through stationary wavelet transform based features. This paper mainly investigates the affect of different block sizes such as 4×4 and 8×8 for RDFD in digital images. The results of the experiments showed that the overlapping block size 4×4 produce more false detection thereby r affecting the accuracy performance of the algorithm. On the contrary, the overlapping block size 8×8 impressively performed better for RDFD in terms of 'p', 'r' and F_1 score. The proposed technique not only reduces the false detection, but also uses reduced length of feature vector which helps in improving the execution time of the algorithm. The experimental results are also compared with state-of-the-arts [8–10] in the domain of RDFD. The results demonstrate that the DCT [8], DWT and PCA [9], and DWT and DCT [10] based features performed poorly, while the proposed moment of first order based features exhibited good performance as discussed in Section 4.4. It is also concluded that accuracy performance of the size of overlapping blocks is influenced by the size of the duplicated regions, the distance measure between the duplicated regions represented by feature vectors and the threshold value used in the algorithm.

Compliance with Ethical Standards

Conflict of interests All authors declare that there are no conflict of interests regarding the publication of this paper.

References

1. Qureshi MA, Deriche M (2015) A bibliography of pixel-based blind image forgery detection techniques. Signal Process Image Commun 39:46–74
2. Asghar K, Habib Z, Hussain M (2017) Copy-move and splicing image forgery detection and localization techniques: a review. Aust J Forensic Sci 49(3):281–307
3. Qi X, Xin X (2015) A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization. J Vis Commun Image Represent 30:312–327
4. Bausvs R, Kriukovas A (2008) Digital signature approach for image authentication. Electron Electr Eng 6(86):65–68

5. Qazi T, Hayat K, Khan SU, Madani SA, Khan I, Kołodziej J, Li H, Lin W, Yow K, Xu C-Z (2013) Survey on blind image forgery detection. IET Image Process 7(7):660–670
6. Pan X, Lyu S (2010) Region duplication detection using image feature matching. IEEE Trans Inf Forensics Secur 5(4):857–867
7. Amerini I, Barni M, Caldelli R, Costanzo A (2013) Counter-forensics of SIFT-based copy-move detection by means of keypoint classification. EURASIP J Image Video Process 2013(1):18
8. Alkawaz MH, Sulong G, Saba T, Rehman A (2016) Detection of copy-move image forgery based on discrete cosine transform. Neural Comput Appl. https://doi.org/10.1007/s00521-016-2663-3
9. Zimba M, Xingming S (2011) DWT-PCA(EVD) based copy-move image forgery detection. Int J Digital Content Technol Appl 5(1):251–258
10. Hayat K, Qazi T (2017) Forgery detection in digital images via discrete wavelet and discrete cosine transforms. Comput Electr Eng. https://doi.org/10.1016/j.compeleceng.2017.03.013
11. Fridrich AJ, Soukal BD, Lukáš AJ (2003) Detection of copy-move forgery in digital images. In: Proceedings of digital forensic research workshop. Citeseer
12. Popescu AC, Farid H (2004) Exposing digital forgeries by detecting duplicated image regions. TR2004-515, Technical Report, Dartmouth College
13. Myna A, Venkateshmurthy M, Patil C (2007) Detection of region duplication forgery in digital images using wavelets and log-polar mapping. In: International conference on computational intelligence and multimedia applications, 2007. IEEE, pp 371–377
14. Christlein V, Riess C, Angelopoulou E (2010) A Study on Features for the Detection of Copy-Move Forgeries. In: Sicherheit, pp 105–116
15. Ryu S-J, Lee M-J, Lee H-K (2010) Detection of copy-rotate-move forgery using zernike moments. In: 12th international conference on information hiding. Springer, Berlin, pp 51–65
16. Huang Y, Lu W, Sun W, Long D (2011) Improved DCT-based detection of copy-move forgery in images. Forensic Sci Int 206(1):178–184
17. Muhammad G, Hussain M, Bebis G (2012) Passive copy move image forgery detection using undecimated dyadic wavelet transform. Digit Investig 9(1):49–57
18. Sekeh MA, Maarof MA, Rohani MF, Mahdian B (2013) Efficient image duplicated region detection model using sequential block clustering. Digit Investig 10(1):73–84
19. Lynch G, Shih FY, Liao H-YM (2013) An efficient expanding block algorithm for image copy-move forgery detection. Inf Sci 239:253–265
20. Wu Y, Deng Y, Duan H, Zhou L (2014) Dual tree complex wavelet transform approach to copy-rotate-move forgery detection. Sci China Inf Sci 57(1):1–12
21. Alahmadi A, Hussain M, Aboalsamh H, Muhammad G, Bebis G, Mathkour H (2017) Passive detection of image forgery using DCT and local binary pattern. Signal Image Video Process 11(1): 81–88
22. Ulutas G, Ustubioglu B, Ulutas M, Nabiyev V (2017) Frame duplication/mirroring detection method with binary features. IET Image Process 11(5):333–342
23. Lee J-C (2015) Copy-move image forgery detection based on Gabor magnitude. J Vis Commun Image Represent 31:320–334
24. Nason GP, Silverman BW (1995) The stationary wavelet transform and some statistical applications. Lecture notes in statistics. Springer, New York, pp 281–281
25. Pesquet J-C, Krim H, Carfantan H (1996) Time-invariant orthonormal wavelet representations. IEEE Trans Signal Process 44(8):1964–1970
26. CoMoFoD dataset. http://www.vcl.fer.hr/comofod/
27. Li Y (2013) Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching. Forensic Sci Int 224(1):59–67

Toqeer Mahmood, is serving as a senior researcher at University of Engineering and Technology (UET), Taxila, Pakistan. He has been completed his MS Computer Engineering in 2010 from Center for Advanced Studies in Engineering (CASE), Islamabad, Pakistan. He has been completed his Ph.D. Computer Engineering in 2016 from UET, Taxila, Pakistan. His research interests are image forensic, image processing, image retrieval, computer vision, and computer networks.

Zahid Mehmood is serving at Department of Software Engineering, University of Engineering and Technoly (UET), Taxila, Pakistan. He has been completed his BS(Hons) Computer Engineering in 2009 from COMSATS University of Sciences and Technology, Pakistan, and MS Electronic Engineering in 2012 with specialization in Signal and Image Processing from International Islamic University (IIU), Islamabad, Pakistan. He has been completed his Ph.D. Computer Engineering in 2016 from UET, Taxila, Pakistan. He is a reviewer for international journals and conferences such as Pattern Recognition, Computer & Electrical Engineering, PAMI, CVPR, Neurocomputing etc. His research interests are content-based image retrieval (CBIR), medical imaging, image forensic, computer vision, and machine learning.

Mohsin Shah is serving as Assistant Professor at the Department of Telecommunication, Hzara University Mansehra, Pakistan. He has completed his BS in Telecommunication Engineering from the University of Engineering and Technology (UET), Peshawar, Pakistan in 2007 and MS Telecommunication Engineering from the University of Engineering and Technology (UET), Taxila, Pakistan in 2012. Currently, he is working toward his PhD degree on CAS-TWAS President Fellowship at the School of Information Science and Technology, University of Science and Technology of China (USTC), Hefei, China. His research interests include Information hiding, multimedia security, and image processing.

Zakir Khan has been completed his BS Computer Science and MS Computer Science from Hazara University Mansehra, Pakistan in 2011, 2015 respectively. Currently, he is pursuing his PhD at Hazara University Mansehra, Pakistan since 2016. He is a skilled programmer and his research interests include image and signal processing, optical fiber communication, network security and computer networks.