Neural Comput & Applic (2018) 30:183–192
https://doi.org/10.1007/s00521-016-2663-3

ORIGINAL ARTICLE

Detection of copy-move image forgery based on discrete cosine transform

Mohammed Hazim Alkawaz[1] · Ghazali Sulong[2] · Tanzila Saba[3] · Amjad Rehman[4]

Received: 8 April 2016 / Accepted: 24 October 2016 / Published online: 16 November 2016

Abstract Since powerful editing software is easily accessible, manipulation on images is expedient and easy without leaving any noticeable evidences. Hence, it turns out to be a challenging chore to authenticate the genuineness of images as it is impossible for human's naked eye to distinguish between the tampered image and actual image. Among the most common methods extensively used to copy and paste regions within the same image in tampering image is the copy-move method. Discrete Cosine Transform (DCT) has the ability to detect tampered regions accurately. Nevertheless, in terms of precision (FP) and recall (FN), the block size of overlapping block influenced the performance. In this paper, the researchers implemented the copy-move image forgery detection using DCT coefficient. Firstly, by using the standard image conversion technique, RGB image is transformed into grayscale image. Consequently, grayscale image is segregated into overlying blocks of $m \times m$ pixels, $m = 4.8$. 2D DCT coefficients are calculated and reposition into a feature vector using zig-zag scanning in every block. Eventually, lexicographic sort is used to sort the feature vectors. Finally, the duplicated block is located by the Euclidean Distance. In order to gauge the performance of the copy-move detection techniques with various block sizes with respect to accuracy and storage, threshold D_similar = 0.1 and distance threshold (N)_d = 100 are used to implement the 10 input images in order. Consequently, 4×4 overlying block size had high false positive thus decreased the accuracy of forged detection in terms of accuracy. However, 8×8 overlying block accomplished more accurately for forged detection in terms of precision and recall as compared to 4×4 overlying block. In a nutshell, the result of the accuracy performance of different overlying block size are influenced by the diverse size of forged area, distance between two forged areas and threshold value used for the research.

Keywords Copy-move image forgery · Digital image forensics · Discrete cosine transform · Statistical moments

1 Introduction

As the old saying goes, a picture is worth a thousand words. Nonetheless, in 'seeing is believing,' one wonders the practicality of the proverb in our current situation [1–3]. At the present time, digital media plays a vibrant role in our daily life with the emergence of advance digital cameras [4–6]. Consequently, image tampering becomes a common phenomenon with the accessibility to powerful digital image editing software such as Photoshop [7–9]. Modification on digital forgeries images is made easier and expedient with the advancement of editing software without leaving any apparent suspicions [10, 11]. It is almost impossible for human to track the tampering of images

✉ Amjad Rehman
a_khan@yu.edu.sa

[1] Faculty of Information Sciences and Engineering, Management and Science University, Shah Alam, Selangor, Malaysia

[2] TM-IRDA Digital Media Centre (MaGIC-X), Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, Johor, Malaysia

[3] College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia

[4] College of Computer and Information Systems, Al-Yamamah University, Riyadh 11512, Saudi Arabia

with their naked eyes. Hence, authenticity verification of images has turned to be a perplexing task [12].

The swift upsurge of digitally manipulated counterfeits in media has resulted in the lack of integrity on digital images [13–16]. Thus, the dire needs to come up with methods to validate the authenticity and the integrity of image became vital, particularly the images presented as evidence or even document used in journalism, criminal, medical and others [17]. Image tampering is a digital art which needs one to comprehend the image properties. An image can be tampered by the usage of a variety of manipulation techniques such as blurring, resampling, filtering, scaling, rotation and cropping. The imitative region may not be the precise copy when pasted directly [18–22].

Various ways to tamper the image include blurring, addition of noise or even when the image is saved with a lower compression [23–26]. Apart from that, the copied region could be applied geometric transformation including rotating, scaling and others. Detection of image tampering deals with investigation on tampered images for possible correlations embedded owing to the tampering operations [27, 28]. Detecting forged image becomes a prominent research field in ensuring the integrity of images [29, 30]. Image forgery detection techniques are needed for copyright protection and forgery prevention. Copy-move attack which manipulates the image forgery by hiding some important information in the image is one of the prominent techniques in image forgery [31–33]. Copy-move manipulates an image by duplicating one portion of the image within the same image on a separate location. Nevertheless, copy move forgery is top challenging falsifications since the region of copy-move attack belongs to the same image. Hence, it is tougher to detect the tampered region within the same image as compared with detecting the areas of some other image statistical methods such as image splicing [34, 35].

2 Related work

It is an inevitable fact that we are exposed to an extraordinary visual images in this innovative era. While we have pledge in the authentic of this digital image, the advent of technology has eroded this belief. There are numerous unscrupulous doctored images growth rate in our daily life until we could not grasp ranging from the advertisement in magazines for the scientific journals, mainstream media outlets or even fashion industry. The multimedia forensics which includes image tampering detection is to verify and authenticate a digital image. Manipulation of a digital image to hide the truth and altering the meaning of the image indicated in it can be misleading when used in a law court [31, 36, 37]. The misled evidence image may influence the verdict. This is similar to the influences that may inflict our interpretation based on the image. Therefore, we need to understand the underlying situation and comprehend what had exactly happened since the image has been manipulated. We need to identify if part of the image has been duplicated, an object has been covered, a combination of object or something has been copied and pasted from another image [38]. Image forensics is a field to detect and analyze images to verify the credibility and authenticity of the digital images. There are three main categories of forgeries in state-of-the-art digital image forensics namely image splicing, copy-move forgery and image retouching [39].

One of the most prevailing methods in image manipulation is by copying and pasting a part of the image once or numerous times elsewhere within the same image known as copy-move forgery. There is diversity of manipulation techniques in manipulating an image so as to have a perfect image without leaving any apparent suspicions. The main intention in copy-move image forgery detection is to detect tampered regions. Exhaustive search technique is an easy apparent approach to detect copy-move attack. The overlapped image and the circularly shifted version is used to look for closely undistinguishable image parts. Though exhaustive search method is relatively costly, it is simple and effective [40].

To resolve the problem of exhaustive approach, robust match detection method is engaged. Discrete Wavelet Transform (DWT) is used to identify forged image in robust match detection process. DWT method has lesser computational complexity as compared to the exhaustive search which only performed the lowest resolution image. Furthermore, this method works even for the images which has noise applied to it and when JPEG quality changes. Nevertheless, this method is not capable to detect the duplication image with geometrical transformation like rotation and scaling [41, 42].

Instead of exhaustive search approach, Discrete Cosine Transform (DCT) approach is used for the copy-move image forgery detection [43]. The detection process is initiated by scanning at upper left corner to lower right corner by sliding B $\times$ B block. Finally, DCT transform and quantized DCT coefficients are calculated for each block.

With the extensive use of powerful editing software currently, even an amateur can easily manipulate the image as they anticipated, hence resulting in the loss of the authenticity for the images. Human beings will not be able to tell apart between the real image and forged images due to the forged image which seems so real [44].

There exist two processing alternatives in copy-move image forgery detection: keypoint-based approach and block-based approach [45, 46]. For block-based techniques, the image is partitioned in a rectangular block depending on the block size such as 8 $\times$ 8 pixels. Then, we are to compute the feature vector and subsequently

matched for the similar feature vectors for each block. In DCT, the discovery procedure starts from checking upper left corner to the lower right corner while sliding a B × B block. For each block, the DCT is applied and the B^2 coefficients are quantized. The special characteristics of DCT are to detect tampered areas with a higher accuracy rate. However, the shortcomings of DCT are if there is a large number of block, extract feature vector's size from the block will also be huge. However, smaller blocks will have smaller variability in DCT coefficients and this is due to high probability of false positive (FP). Since most of the study of DCT copy-move forgery detection only use 8 × 8 pixels block size, what will be the effect of different block size being used on DCT?

The issues need to be concerns when evaluating accuracy of detected tampered region in terms of precision and recall of detected forged areas number correctly (TP-True Positive), areas' number that have been incorrectly detected as forged (FP-False Positive), and forged areas that are falsely missed (FN-False Negative). Therefore, precision (FP) and recall (FN) should be increased in order to achieve good accuracy rate. This research focuses on the investigation on the effect of block size on FP and FN by implementing the block-based copy-move image forgery detection approach using coefficients with various block sizes. Therefore, the main issue is:

- What is the appropriate block size in order to achieve best accuracy (precision and recall)?
- What is the effect of block size on false positive and false negative?

This research aims to implement the block-based copy-move image forgery detection approach using DCT coefficients with various block sizes in order to inspect the effect of block size on FP and FN.

3 Proposed methodology

In this research, copy-move image forgery detection using DCT coefficients has been carried out to investigate the effect of block size on performance of tampered region detection in terms of FP and FN by implementing the block-based detection approach with a variety of block size ranging from 4 × 4 to 8 × 8 pixels. Figure 1 presents the framework for this research.

3.1 RGB image convert to grayscale

To transform RGB image into grayscale, the image conversion technique is deployed[47]. The procedure to convert the RGB image to grayscale-indexed image is shown below.

Step 1 Converting color-indexed images

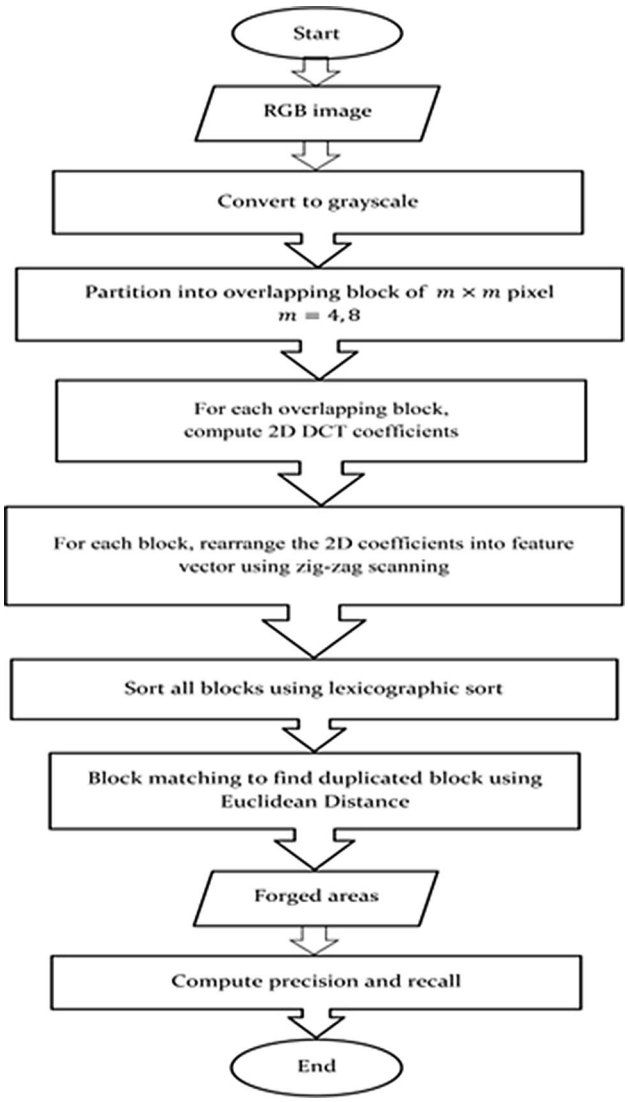

Fig. 1 Research framework

First, the color-indexed image is divided into its RGB components;

R = map (X2, 1); R = reshape (R, size (X2));
G = map (X2, 2); G = reshape (G, size (X2));
B = map (X2, 3); B = reshape (B, size (X2));

Eventually, the three color components, RGB, using the standard perceptual weightings, convert the matrices into a grayscale intensity image based on Eq. (1).

$$X_{\text{rgb}} = 0.2990 \times \text{R} + 0.5870 \times \text{G} + 0.1140 \times \text{B}; \quad (1)$$

3.2 Overlapping block

Following RGB image conversion to grayscale image, the image is partitioned into overlapping block to detect forged area by using block matching to find the duplicated or identical block.

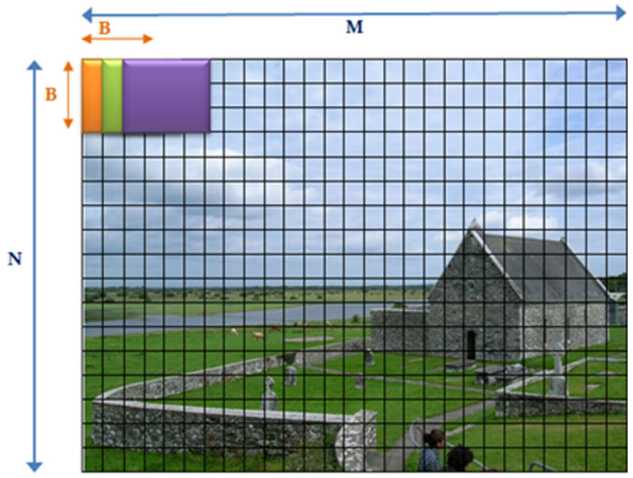

Fig. 2 Image M × N is divided into B × B overlapped blocks

Step 1 Assuming a $n \times n$ grayscale image I, is partitioned into overlapping blocks of $m \times n$ pixels, $m = 4, 8$. The neighboring blocks will only have one different column or row. Each block is indicated as B_{ij}, where i and j signifies the beginning point of the block's row and column, respectively, [Eq. (2)]. Figure 2 shows the 4 × 4 overlapping block with different color block.

$$B_{ij}(x, y) = f(x + j, \quad y + i) \tag{2}$$

where $x, y \in \{0, \ldots, B - 1\}$, $i \in \{1, \ldots, M - B + 1\}$, and $j \in \{1, \ldots, N - B + 1\}$

Hence, obtain N_{blocks} of overlapped sub-blocks from suspicious image using Eq. (3).

$$N_{blocks} = (M - B + 1) \times (N - B + 1) \tag{3}$$

Step 2 Let $N_{blocks} = (M - B + 1) \times (N - B + 1)$, DCT is applied for each block $B_i (i = 1, 2, 3, \ldots, N_{blocks})$. Then, exploit a DCT coefficients framework with an indistinguishable size from the block, which the comparing block could be represented [47]. Applied common quantization mask with same size as the DCT coefficients matrix and rounding to integers result as feature vector for each block.

3.3 Rearrange the coefficient

The feature vector is rearranged into row vector using zig-zag scanning. Zig-zag scanning converts 2D matrix into a 1D array (row vectors). Figure 3 represents the direction of the way of zig-zag scanning arrangement.

3.4 Lexicographically sorting

The A is then sorted using lexicographically sorting and left corner's facilitates every block that is indicated by a circle block is recorded. The sorted set could be characterized as $\widehat{A}$ since each element of A is a vector. In lexicographic sorting, a matrix of feature vectors is developed and each feature vector appears as a row in the matrix. This matrix is further sorted in row-wise fashion and similar features in sequential rows are appeared. Figure 4 shows the feature vector in row before and after sorting.

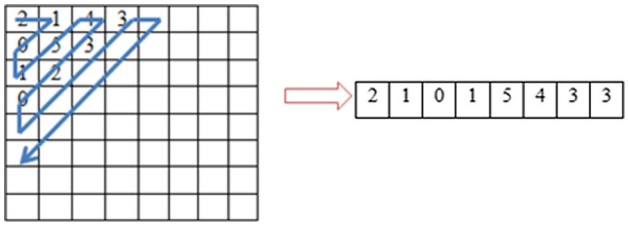

Fig. 3 Zig-zag scanning converting 2D matrix into 1D array

3.5 Block matching

The block using quantized DCT coefficients is represented in robust match method. In calculating DCT coefficients, quantization process is involved decided by a user-specified parameter Q. Higher the values of Q factor means finer quantization so Q factor plays vital role in quantization steps for DCT transform coefficients. The blocks should match intently to recognize as comparable. However, more matching blocks are produced for the lower values of the Q factor and it will lead to false matches. Consequently, it may affect the accuracy of the final result. Based on $\widehat{A}$ after the lexicographically sorting, calculated the Euclidean distance m_match $\left(\widehat{A}_i, \widehat{A}_{i+j}\right)$ between adjacent pairs of $\widehat{A}$. Initialize a black map P with the size M × N and consider the looked blocks as a couple of possibility for the forgery,if the separation is littler than a preset limit $D_{similar}$.

$$\text{m\_match}\left(\widehat{A}_i, \widehat{A}_{i+j}\right) = \sqrt{\sum_{k=1}^{4}\left(v_i^k - v_{i+j}^k\right)^2} < D_{similar} \tag{4}$$

Moreover, due to the neighboring squares might have the comparative component vector, the real distance between two comparable pieces calculated using Eq. (5).

$$\text{m\_distance}\left(\widehat{A}_i, \widehat{A}_{i+j}\right) = \sqrt{(x_i - x_{i+j})^2 + (y_i - y_{i+j})^2} N_d \tag{5}$$

as (x,y) is the circle center of the corresponding block, m_match and m_distance is used to determine the duplicated blocks.

In short, set two thresholds to make the detection: likeness threshold $D_{similar}$ and distance threshold N_d where the amounts of neighboring feature vectors are controlled, only if the test satisfies the following condition [Eq. (6)].

$$\begin{aligned} &\text{m\_match}(V_i, V_j) < D_{similar} \quad \text{and} \\ &\text{m\_distance}(V_i, V_j) > N_d \end{aligned} \tag{6}$$

Fig. 4 **a** Exhibits feature vector in row before sorting and **b** exhibits feature vector in row after lexicographically sort

(a)

-1	0	1	4	-3	-1	0	0	1	1
1	0	-1	-2	2	2	1	4	3	-1
0	1	4	-2	-1	-1	0	-2	-4	1
1	1	2	-2	-1	2	0	0	1	0
0	-1	-1	2	4	0	-1	1	2	3
0	1	2	-1	-3	0	0	1	4	2
2	3	-1	3	2	0	1	-2	1	-1
2	-1	-1	4	0	1	4	2	1	1

Sorting

(b)

-1	0	1	4	-3	-1	0	0	1	1
0	-1	-1	2	4	0	-1	1	2	3
0	1	2	-1	-3	0	0	1	4	2
0	1	4	-2	-1	-1	0	-2	-4	1
1	0	-1	-2	2	2	1	4	3	-1
1	1	2	-2	-1	2	0	0	1	0
2	-1	-1	4	0	1	4	2	1	1
2	3	-1	3	2	0	1	-2	1	-1

where $j \in [i - \mathrm{N}_{\mathrm{number}}]$, for the actual block, denotes a shading map and another guide for the copied block.

3.6 Forgery decision

Since most of the natural images would have many similar blocks, the method of block matching is insufficient to make the forgery decision. In the case, that there are more than a specific number of blocks that are linked to each other within a same distance, the forgery decision could be determined. Meanwhile, the distance between the two blocks those have the similar feature vectors, $\widehat{A}_i$ and $\widehat{A}_j$.

Let (i_1, i_2) and (j_1, j_2) represents matching blocks location. In next step, we calculate shift vector between two blocks to be compared. Refer to Eq. (7).

$$s = (s_1, s_2) = \left(i_{1-j_1}, i_2 - j_2\right) \tag{7}$$

Due to the shift vectors $-s$ and s correspond to the same shift, if necessary, normalize the shift vectors s by multiplying by -1 so that $s1 \geq 0$. Increase the standardized move vector counter C by one for each coordinating pair of blocks using Eq. (8).

$$C(s_1, s_2) = C(s_1, s_2) + 1 \tag{8}$$

At the beginning, initialize the values of C to zero. At least one of the values of $C(s_1, s_2)$ should be more than a threshold value, if there are many blocks which give the similar feature values within the same separation. In the event that these blocks are associated with each other, then the forgery decision can be made.

3.7 Performance measurement

The performance measurement only focuses on the accuracy of the evaluation, which was described as following.

3.7.1 Accuracy evaluation

Appropriate measures are required in order to gauge the performance of the method in a copy-move forgery. The accuracy in the performance of the implemented method with various block sizes in detecting the forged region is being considered in this research.

The accuracy in the performance of the implemented method is evaluated regarding exactness and review as shown in Fig. 5. Precision signifies the probability correct forgery of the detected blocks as forgery, whereas recall determines the probability of forged blocks in the image that are detected. True positive (TP) represents the number of appropriately detected forged areas, false positive (FP) represents the number of regions that have been wrongly distinguished as produced, and false negative (FN) represents the falsely missed forged areas based on Eqs. (9) and (10).

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

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

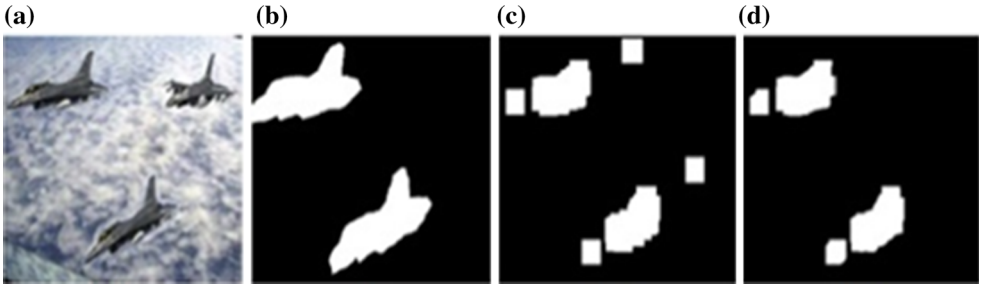

Fig. 5 **a** Forged image, **b** forged region, **c** detected region and **d** (Forged Region ∩ Detected Region)

It could be conclude that low FP rates lead to high precision values, whereas low FN rates will result in high recall values based on the equation to predict the precision and recall equation. As shown in Fig. 5, there is a difference between forged area and detected region when calculating accuracy performance.

The precision in percentage term is computed as below [Eqs. (11 and 12)] [48].

$$\text{Precision} = ((\text{Forged Region} \cap \text{Detected Region})) / (\text{Detected Region}) \times 100 \quad (11)$$

In contrast, recall in percentage is computed as below [48]:

$$\text{Recall} = ((\text{Forged Region} \cap \text{Detected Region})) / (\text{Forged Region}) \times 100\,\% \quad (12)$$

4 Implementation

In this section, experimental result of the proposed approach has been exhibited to verify its performance. The implemented method is evaluated by utilizing the images from the CoMoFoD dataset. The algorithm has been implemented using MATLAB and C++.

4.1 CoMoFoD dataset

CoMoFoD is a standard dataset for benchmarking the detection of image tampering artifacts [49]. This dataset comprises of 200 images: 100 original images and 100 tampered images. The standard image size has been set as 512 × 512. In this research, 10 images will be chosen as experimental images. Each of the images will implement the block-based copy-move image forgery detection approaches using DCT coefficients with 4 × 4 and 8 × 8 pixel block sizes. Figure 6 shows the sample of datasets used as input images.

4.2 Experimental results

This research implemented the block-based copy-move image forgery detection approach using DCT coefficients with 4 × 4 and 8 × 8 overlying block and evaluated performance of forgery detection in terms of precision and recall.

Figure 7a–c presents the forgery detection for 4 × 4 and 8 × 8 overlying block. Detected forged area is displayed in white color block. Threshold $D_{similar}$ and distance threshold N_d where the amounts of neighboring feature vectors are control. Threshold $D_{similar} = 0.1$ and distance threshold $N_d = 100$ are used to examine the effect of different block size on performance of the forgery detection in terms of precision and recall. Obviously, the forgery detection for 8 × 8 overlapping block is more accurate as compared to the 4 × 4 overlapping block. 4 × 4 overlapping block increased the number of areas that have been erroneously detected as forged (FP-False Positive). Therefore, the number of false positive value influenced the precision of the forgery detection.

4.3 Accuracy performance

The detection accuracy performance of the implemented method is evaluated in terms of precision (FP) and recall (FN) for the 10 selected images from CoMoFoD standard datasets. Each of the input images are evaluated on the effects of different overlapping block size 4 × 4 and 8 × 8 pixel on the accuracy performance for the forgery detection in terms of recall and precision.

Table 1 revealed the accuracy precision-recall performance of different overlapping block size in percentage. In general, performance for 4 × 4 overlapping block is low in precision but high in recall. It indicates that using 4 × 4 overlapping block size will result in a higher number of false positive value. Consequently, it decreases the

Fig. 6 Input images used in this experiment

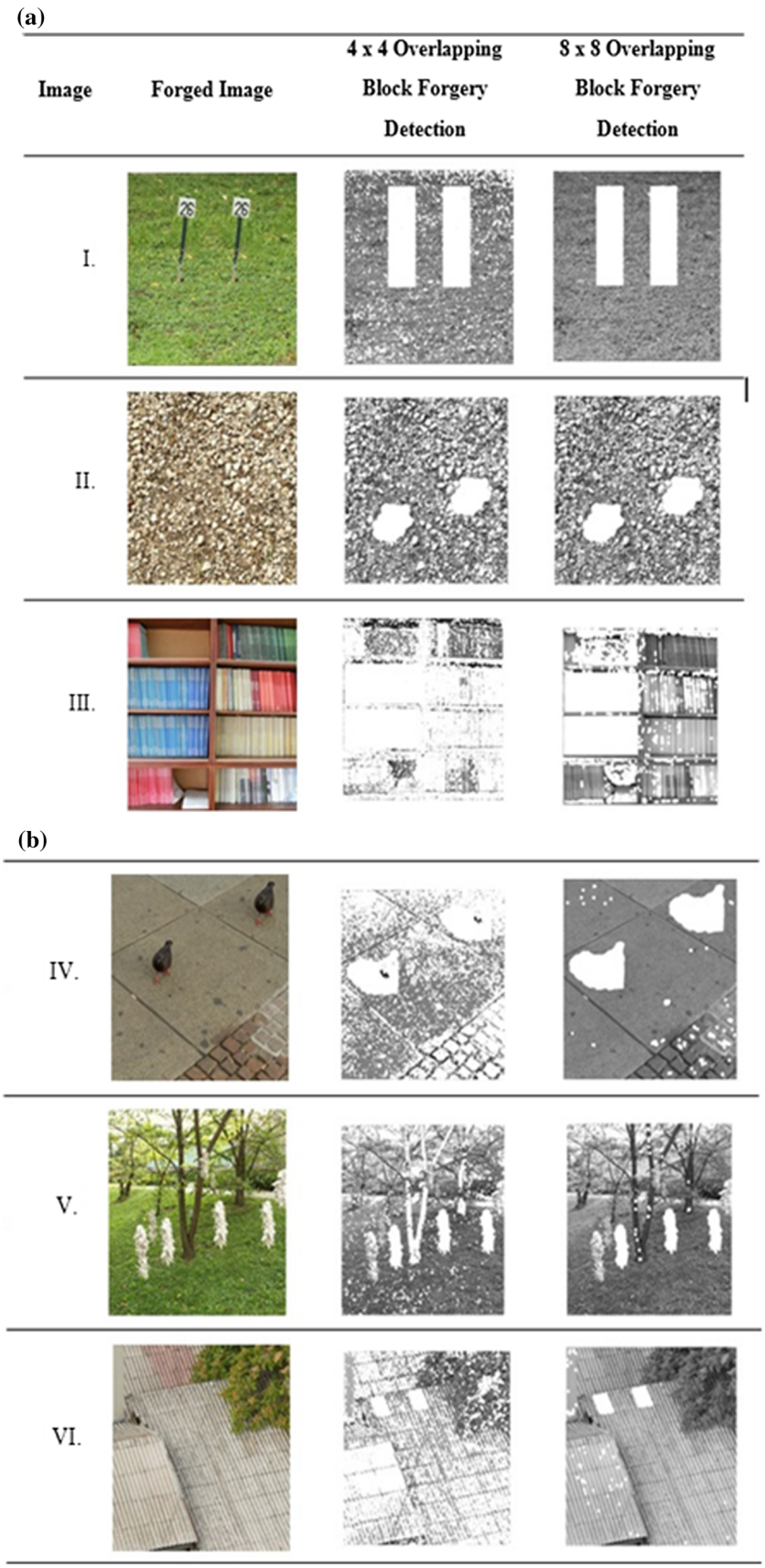

Fig. 7 **a** Forgery detection for 4×4 and 8×8 overlapping block. **b** Forgery detection for 4×4 and 8×8 overlapping block. **c** Forgery detection for 4×4 and 8×8 overlapping block

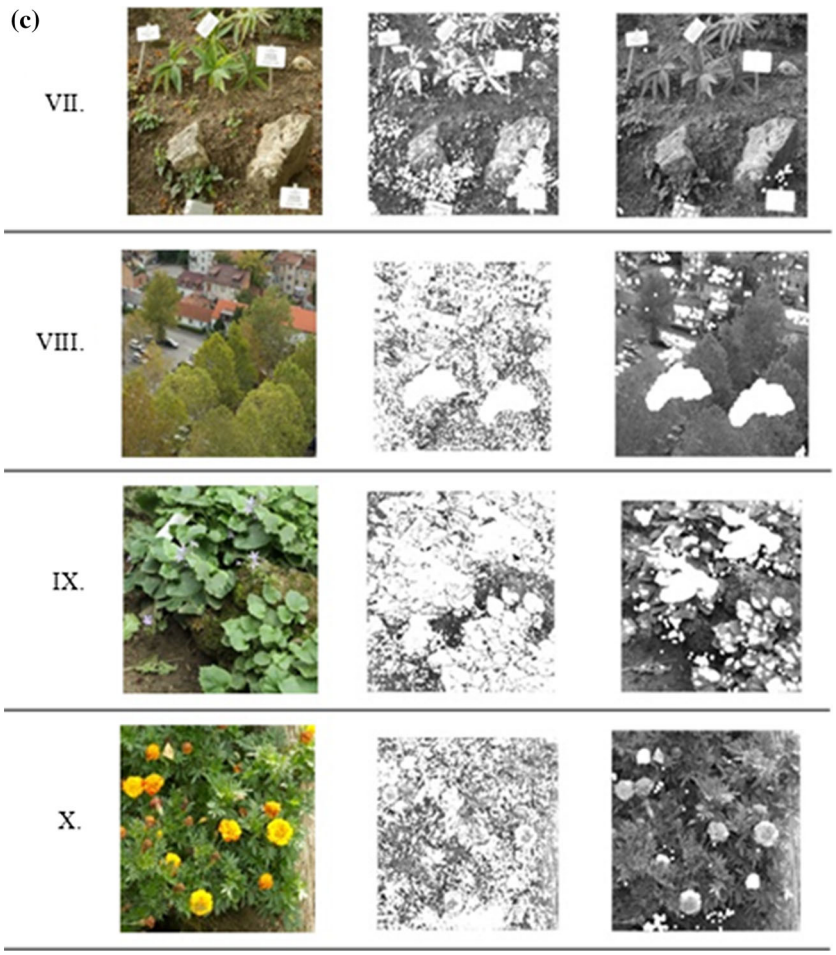

Fig. 7 continued

accuracy performance of precision for the forged detection. For 8×8 overlapping block, as compared to 4×4 overlapping block, it obviously had perform well in accuracy performance in terms of precision and recall.

Implementation method block-based forgery detection using discrete cosine transform (DCT) with different overlapping block size will influence the accuracy performance in terms of precision and recall.

From the research result and accuracy performance result, 8×8 overlapping block achieve good accuracy performance as compared to 4×4 overlapping block. 4×4 overlapping block has successfully detect the forged area accurately. However, a large number of areas have been erroneously detected as forged influence the accuracy performance in terms of precision. Small overlapping block size increased the number of similarity between block, thus increased the number of false positive in forgery detection. For 8×8 overlapping block, it had a lesser number of false positive as compared to 4×4 overlapping block. Therefore, it can perform more accurately for forged area detection in terms of precision. For the area of the forgery detection influenced the accuracy performance in terms of precision and recall as well. For the small area of forgery detection, 4×4 overlapping block can achieve higher performance in terms of recall. Small overlapping block detects smaller area of forgery detection accurately; it decreased the number of false negative which is falsely missed forged areas. However, performance in recall for 8×8 overlapping block is lower than 4×4 overlapping block in a smaller area forgery detection.

Threshold $D_{similar} = 0.1$ and distance threshold $N_d = 100$ are used to implement in the 10 input images. However, the size of the forged area and the distance between two forged areas will influence the accuracy performance. The accuracy performance of the forged image will be influenced by the changes of threshold value. The value of the threshold value can change according to each forged image in order to get most accuracy performance.

Overall, 8×8 overlapping block achieve good accuracy performance in terms of precision and recall as compared to 4×4 overlapping block. Even though 4×4 overlapping block is able to decrease the number of false negative to perform better in recall for small area of forgery detection portion, 8×8 overlapping block can also achieve good accuracy performance in both precision and recall.

Table 1 Accuracy precision-recall performance of different block size in percentage (%)

Image	Experiment results		
	Overlapping block size	Precision (%)	Recall (%)
I.	4 × 4	63.52	97.89
	8 × 8	100	97.53
II.	4 × 4	42.55	95.54
	8 × 8	95.19	96.25
III.	4 × 4	27.44	99.70
	8 × 8	49.80	100
IV.	4 × 4	19.30	98.07
	8 × 8	87.62	99.48
V.	4 × 4	23.02	92.19
	8 × 8	63.32	88.47
VI.	4 × 4	3.52	99.35
	8 × 8	62.53	97.30
VII.	4 × 4	10.37	99.62
	8 × 8	59.51	99.86
VIII.	4 × 4	13.47	99.45
	8 × 8	59.25	98.68
IX.	4 × 4	15.85	95.57
	8 × 8	41.49	93.37
X.	4 × 4	1.73	98.60
	8 × 8	26.58	94.85

5 Conclusion

Digital images are the primary source of information in today's digital era. With the accessibility of various powerful image editing software such as Photoshop, it is simple to influence digital images with no observable signs of exploitation.

Hence, it is almost impossible for one to detect any temperance of an image through naked eyes. Authenticity of image is highly significant in several fields like journalism, criminal, medical and others.

This research is meant to study about the effects of different block size ranging from 4 × 4 and 8 × 8 pixels on the performance in terms of FP and FN. The objectives of the study is to implement the block-based copy-move image forgery detection approach using DCT coefficients with various block size in order to investigate the effect of block size on FP and FN. In general, three objectives are carried out in this study based on the implementation method which is using DCT coefficients with different block size, in order to achieve the accuracy to detect the tampered region. As a result, 4 × 4 overlapping block size had high false positive thus decreased the accurately performance of forged detection in terms of precision. However, as compared to 4 × 4 overlapping block, 8 × 8 overlapping block outperformed for forged detection in terms of precision and recall. In a nutshell, the result of the accuracy performance of different overlapping block size are influenced by the different size of forged area, distance between two forged areas and threshold value are used for the research.

Acknowledgments Authors are grateful to Faculty of Information Sciences and Engineering, Management and Science University (MSU), Shah Alam, Selangor and Faculty of Computing, Universiti Teknologi Malaysia (UTM), Skudai 81310 Johor, Malaysia for their support in this research.

References

1. Pinsky LE, Wipf JE (2000) A picture is worth a thousand words. J Gen Int Med 15:805–810
2. Norouzi A, Rahim MSM, Altameem A, Saba T, Rada AE, Rehman A, Uddin M (2014) Medical image segmentation methods, algorithms, and applications. IETE Tech Rev 31(3):199–213. doi:10.1080/02564602.2014.906861
3. Mundher M, Muhamad D, Rehman A, Saba T, Kausar F (2014) Digital watermarking for images security using discrete slant let transform. Appl Math Inf Sci 8(6):2823–2830. doi:10.12785/amis/080618
4. Belk RW (2013) Extended self in a digital world. J Consum Res 40:477–500
5. Saba T, Rehman A, Sulong G (2011) Cursive script segmentation with neural confidence. Int J Innov Comput Inf Control (IJICIC) 7(7):1–10
6. Rehman A, Saba T (2014) Features extraction for soccer video semantic analysis: current achievements and remaining issues. Artif Intell Rev 41(3):451–461. doi:10.1007/s10462-012-9319-1
7. Karie NM, Venter HS (2014) Toward a general ontology for digital forensic disciplines. J Forensic Sci 59:1231–1241
8. Al-Qershi OM, Khoo BE (2013) Passive detection of copy-move forgery in digital images: state-of-the-art. Forensic Sci Int 231:284–295
9. Rehman A, Saba T (2012) Off-line cursive script recognition: current advances, comparisons and remaining problems. Artif Intell Rev 37(4):261–288. doi:10.1007/s10462-011-9229-7
10. Anand V, Hashmi MF, Keskar AG (2014) A copy move forgery detection to overcome sustained attacks using dyadic wavelet transform and sift methods. In: Intelligent information and database systems. Lecture Notes in Computer Science, vol 8397. Springer, pp 530–542
11. Muhsin ZF, Rehman A, Altameem A, Saba T, Uddin M (2014) Improved quadtree image segmentation approach to region information. Imaging Sci J 62(1):56–62. doi:10.1179/1743131X13Y.0000000063
12. Zhao Y, Sutardja A, Ramadan O (2015) Digital image manipulation forensic. Technical Report No. UCB/EECS-2015-125, Electrical Engineering and Computer Sciences, University of California at Berkeley
13. Sutardja A, Ramadan O, Zhao Y (2015) Forensic methods for detecting image manipulation-copy move. Technical Report No. UCB/EECS-2015-84, Electrical Engineering and Computer Sciences, University of California at Berkeley
14. Yazdani S et al (2015) Image segmentation methods and applications in MRI brain images. IETE Tech Rev 32:413–427
15. Saba T, Rehman A (2012) Machine learning and script recognition. Lambert Academic publisher, pp 39–45. ISBN-13: 978-3659111709

16. Saba T, Rehman A, Altameem A, Uddin M (2014) Annotated comparisons of proposed preprocessing techniques for script recognition. Neural Comput Appl 25(6):1337–1347. doi:10.1007/s00521-014-1618-9
17. Granty REJ, Aditya T, Madhu SS (2010) Survey on passive methods of image tampering detection. In: Communication and computational intelligence (INCOCCI), 2010 international conference on, pp 431–436
18. Mire AV et al (2014) Digital forensic of JPEG images. In: Signal and image processing (ICSIP), 2014 fifth international conference on 2014, pp 131–136
19. Rehman A, Saba T (2014) Evaluation of artificial intelligent techniques to secure information in enterprises. Artif Intell Rev 42(4):1029–1044. doi:10.1007/s10462-012-9372-9
20. Saba T, Rehman A, Al-Dhelaand A, Al-Rodhaand M (2014) Evaluation of current documents image denoising techniques: a comparative study. Appl Artif Intell 28(9):879–887. doi:10.1080/08839514.2014.954344
21. Joudaki S, Mohamad D, Saba T, Rehman A, Al-Rodhaan M, Al-Dhelaan A (2014) Vision-based sign language classification: a directional review. IETE Tech Rev 31(5):383–391. doi:10.1080/02564602.2014.961576
22. Fadhil MS, Alkawaz MH, Rehman A, Saba T (2016) Writers identification based on multiple windows features mining. 3D Res 7(1):1–6. doi:10.1007/s13319-016-0087-6
23. Bayram S, Sencar HT, Memon N (2009) 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
24. Meethongjan K, Dzulkifli M, Rehman A, Altameem A, Saba T (2013) An intelligent fused approach for face recognition. J Intell Syst 22(2):197–212. doi:10.1515/jisys-2013-0010
25. Al-Ameen Z, Sulong G, Rehman A, Al-Dhelaan A, Saba T, Al-Rodhaan M (2015) An innovative technique for contrast enhancement of computed tomography images using normalized gamma-corrected contrast-limited adaptive histogram equalization. EURASIP J Adv Signal Process 32:1–12. doi:10.1186/s13634-015-0214-1
26. Basori AH, Alkawaz MH, Saba T, Rehman A (2016) An overview of interactive wet cloth simulation in virtual reality and serious games. Comput Methods Biomech Biomed Eng Imaging Vis. doi:10.1080/21681163.2016.1178600
27. Mahdian B, Saic S (2010) A bibliography on blind methods for identifying image forgery. Signal Process Image Commun 25:389–399
28. Saba T, Rehman A, Al-Dhelaan A, Al-Rodhaan M (2014) Evaluation of current documents image denoising techniques: a comparative study. Appl Artif Intell 28(9):879–887. doi:10.1080/08839514.2014.954344
29. Pan X, Lyu S (2010) Region duplication detection using image feature matching. Inf Forensics Secur IEEE Trans 5:857–867
30. Ahmad AM, Sulong G, Rehman A, Alkawaz MH, Saba T (2014) Data hiding based on improved exploiting modification direction method and Huffman coding. J Intell Syst 23(4):451–459. doi:10.1515/jisys-2014-0007
31. Amerini I et al (2011) A sift-based forensic method for copy-move attack detection and transformation recovery. Inf Forensics Secur IEEE Trans 6:1099–1110
32. Boato G, Natale F, Zontone P (2010) How digital forensics may help assessing the perceptual impact of image formation and manipulation. In: Proceedings of fifth international workshop on video processing and quality metrics for consumer electronics–VPQM, 2010
33. Nodehi A, Sulong G, Al-Rodhaan M, Al-Dhelaan A, Rehman A, Saba T (2014) Intelligent fuzzy approach for fast fractal image compression. EURASIP J Adv Signal Process. doi:10.1186/1687-6180-2014-112
34. Petitcolas FA, Anderson RJ, Kuhn MG (1999) Information hiding—a survey. Proc IEEE 87:1062–1078
35. Christlein V, Riess C, Angelopoulou E (2010) A study on features for the detection of copy-move forgeries. Sicherheit 2010:105–116
36. Lu W, Wu M (2010) Multimedia forensic hash based on visual words. In: Image processing (ICIP), 2010 17th IEEE international conference on 2010, pp 989–992
37. Verma VS, Jha RK (2015) An overview of robust digital image watermarking. IETE Tech Rev 32:479–496
38. Christlein V et al (2012) An evaluation of popular copy-move forgery detection approaches. Inf Forensics Secur IEEE Trans 7:1841–1854
39. Sunil K, Jagan D, Shaktidev M (2014) DCT-PCA based method for copy-move forgery detection. In: ICT and critical infrastructure: proceedings of the 48th annual convention of computer society of India, vol II, pp 577–583
40. Farid H, Lyu S (2003) Higher-order wavelet statistics and their application to digital forensics. In: IEEE Workshop on Statistical Analysis in Computer Vision (in conjunction with CVPR), 2003
41. Khan S, Kulkarni A (2010) Robust method for detection of copy-move forgery in digital images. In: Signal and image processing (ICSIP), 2010 international conference on 2010, pp 69–73
42. Sridevi M, Mala C, Sanyam S (2012) Comparative study of image forgery and copy-move techniques. In: Advances in computer science, engineering and applications. Advances in Intelligent and Soft Computing, vol 166. Springer, pp 715–723
43. Fridrich AJ, Soukal BD, Lukáš AJ (2003) Detection of copy-move forgery in digital images. In: Proceedings of digital forensic research workshop, 2003
44. Mahmood T, Nawaz T, Irtaza A, Ashraf R, Shah M, Mahmood MT (2016) Copy-Move Forgery Detection Technique for Forensic Analysis in Digital Images. Math Probl Eng 2016(2016) ID 8713202, doi:10.1155/2016/8713202
45. Pun CM, Yuan X-C, Bi X-L (2015) Image forgery detection using adaptive over segmentation and feature point matching. Inf Forensics Secur IEEE Trans 10:1705–1716
46. Yan CP, Pun C-M, Yuan X-C (2016) Multi-scale image hashing using adaptive local feature extraction for robust tampering detection. Signal Process 121:1–16
47. Cao Y, Gao T, Fan L, Yang Q (2012) A robust detection algorithm for copy-move forgery in digital images. Forensic Sci Int 214(1-3):33–34
48. Yavuz F, Bal A, Cukur H (2016) An effective detection algorithm for region duplication forgery in digital images. Proc. SPIE 9845, Optical Pattern Recognition XXVII, 98450O. doi:10.1117/12.2223732
49. Zampoglou M, Papadopoulos S, Kompatsiaris Y (2015) Detecting image splicing in the wild (WEB). In: Multimedia and expo workshops (ICMEW), 2015 IEEE international conference on 2015, pp 1–6