A Robust Method for Image Copy-Move Passive Forgery Detection with Enhanced Speed

Asif Hassan and V. K. Sharma

Abstract Forgery detection of images is presently one of the fascinated research fields. Copy-move forgery is the most commonly used methods for image forgery. A novel method is proposed in this paper, which is an effective and advanced method for detecting copy-move forgery. The proposed method is a block matching technique with reduced computational speed and less computational complexities. The efficiency of outcome is also improved. The image is segmented into fixed dimensions of overlying blocks and then discrete cosine transform (DCT) is applied to each block to extract its features. Then, the mean of each block is obtained. The mean of each block is compared with other blocks to find the similarity between the blocks. The computational outcomes are shown that indicates the proposed method is robust to detect copy-move forgery efficiently with enhanced speed.

1 Introduction

An image is an artifact that represents visual insight of an event. We live in a digital world where digital images are used as a means of communication. Images are everywhere, on the Internet, social media, newspapers, etc. The authenticity of images is in question because it is very easy to edit any image using easily available image manipulating tools [1–4]. Hence, digital image forgery detection is important to authenticate the images. Image authentication methods can be classified into two modules such as active methods and passive methods. Active method is the technique in which prior information about the original image such as watermarking or signature [5–7] which is embedded inside the image is known for forgery detection. It is a drawback because in various situations prior information about the image is not available [8–11].

A. Hassan (✉) · V. K. Sharma
Bhagwant University, Ajmer, Rajasthan, India
e-mail: asif.43hassan@gmail.com

V. K. Sharma
e-mail: viren_krec@yahoo.com

D. Pandian et al. (eds.), *Proceedings of the International Conference on ISMAC in Computational Vision and Bio-Engineering 2018 (ISMAC-CVB)*, Lecture Notes in Computational Vision and Biomechanics 30,
https://doi.org/10.1007/978-3-030-00665-5_136

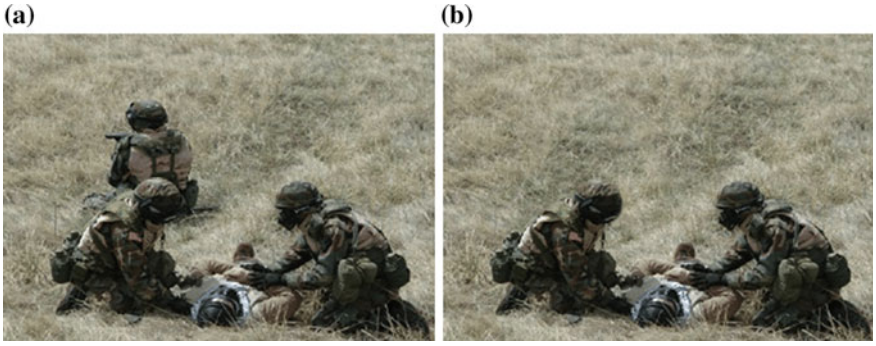

Fig. 1 Copy-move forgery: **a** Original image, **b** Copy-move forged image

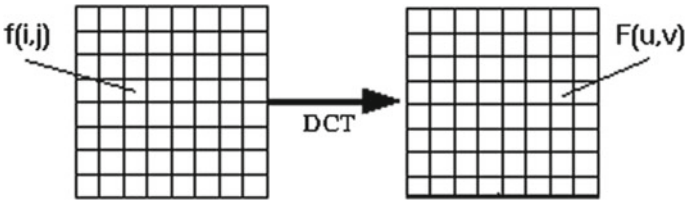

Fig. 2 Discrete cosine transforms

The Passive method is also known as the *blind technique* in which information regarding the image is not available [12, 13]. Hence, this method authenticates the image without the existence of the original information.

One of the most commonly used methods of image altering is hiding a region in the image and distorting the image information. Copy-move forgery is the most common image forgery used to hide the portion of the image. In copy-move forgery, some portions of an image are copied and posted on another area of the same image. An example of copy-move forgery is shown in Fig. 1.

The most frequently used method for image copy-move detection is block matching in which the image is divided into the same size overlying blocks then feature of each block is extracted and then each block is compared with other blocks in the same image. At last, the outcome of forgery detection is decided based on matched block features. During the feature extraction process, the essential features are chosen from the blocks using a discrete cosine transform (DCT)[1, 3]. These essential features are used to compare the blocks. DCT helps to segment the image or spectral sub-bands of differing importance corresponding to the image visual quality. The DCT is like the discrete Fourier transform which transforms the image into the frequency domain from the spatial domain as shown in Fig. 2.

Fadl and Semary (accelerated method) [1] proposed a method using K-means classifier and images of 128 $\times$ 128-pixel grayscale images. The proposed method

works on direct computation, without using the classifier, for an image size of any pixel with reduced computational steps.

The paper is organized as follows: Sect. 2 presents the proposed system in details. Section 3 presents the test and results and Sect. 4 is the conclusion.

2 Proposed Method

The core of the proposed method is to examine whether the input image contains copied regions or not and to identify the region from where it is copied from the same image.

The proposed method is explained in the following steps:

Step 1 The color image or gray image of any pixel value is taken as input for which copy-move detection must be performed.

Step 2 The Color image is converted from RGB to gray. Gray image is retained as it is.

Step 3 Images are segmented into equal size overlaying blocks. The total number of blocks depends on the pixel of the image. It is calculated using the following equations:

$$\textbf{Block size} = \textbf{2t} \tag{1}$$

where $\mathbf{t} = \mathbf{log2}\ (\mathbf{M} \times \mathbf{N}) - \mathbf{12}$, "M" is the number of rows, and "N" is the number of columns.
Therefore,

$$\textbf{the total number of blocks} = ((\mathbf{M} * \mathbf{N}))/(\textbf{Block size}) \tag{2}$$

The minimum value of $t = 2$

Step 4 Calculate the DCT for each block.
The general for DCT is

$$F(u, v) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \left(\frac{2}{M}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \Lambda(i) \cdot \Lambda(j) \cdot \cos\left[\frac{\pi.u}{2.N}(2i+1)\right] \cos\left[\frac{\pi.v}{2.M}(2j+1)\right] \cdot f(i, j) \tag{3}$$

For the input image N by M, $f(i, j)$ is the intensity of the pixel in row i and column j; $F(u, v)$ is the DCT coefficient in row $k1$ and column $k2$ of the DCT matrix.

Step 5 Calculate the mean of obtained DCT of each block.

Step 6 Then, the mean of each block is matched with all other blocks in the same image.

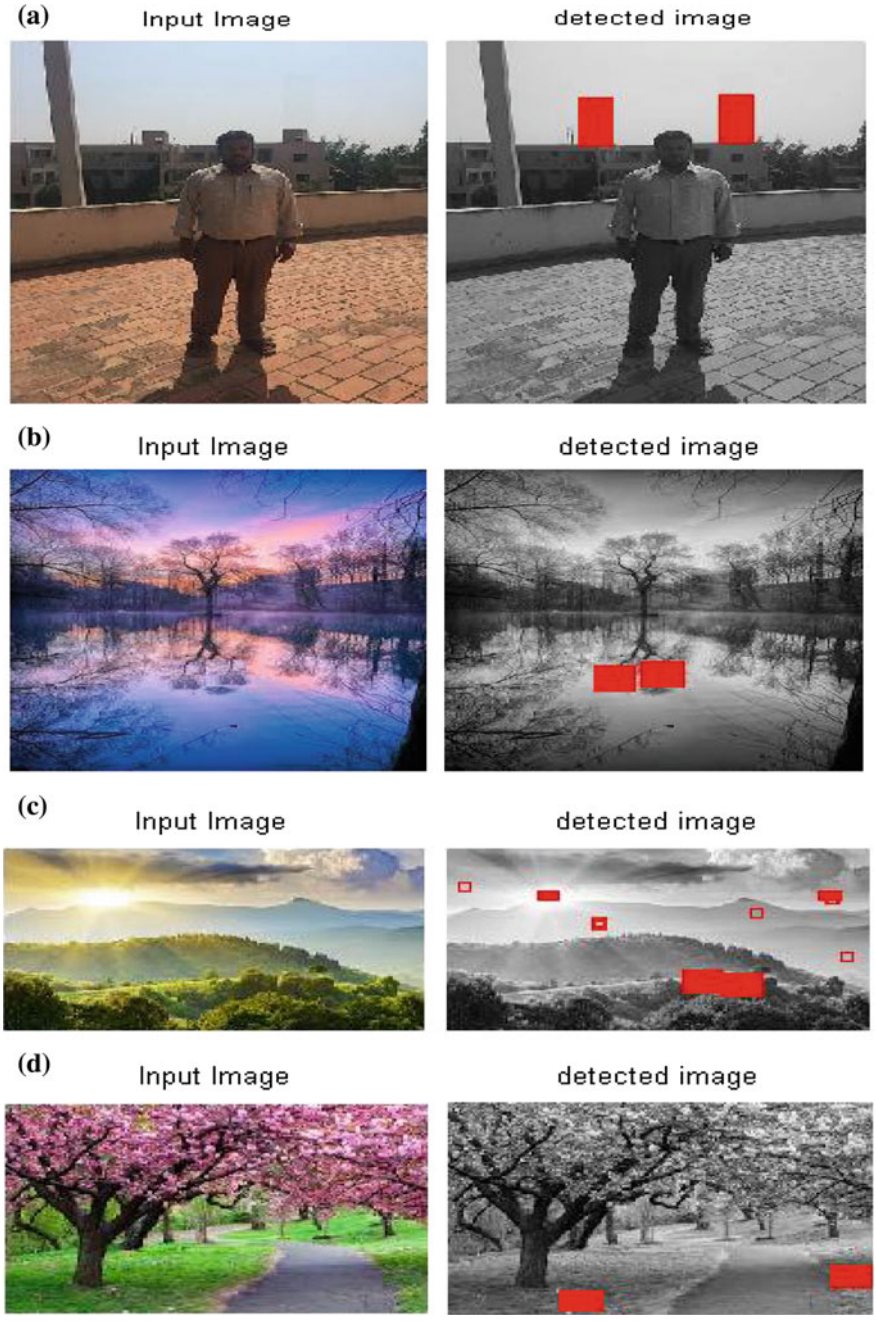

Fig. 3 **a**–**g** Random rectangular region detected

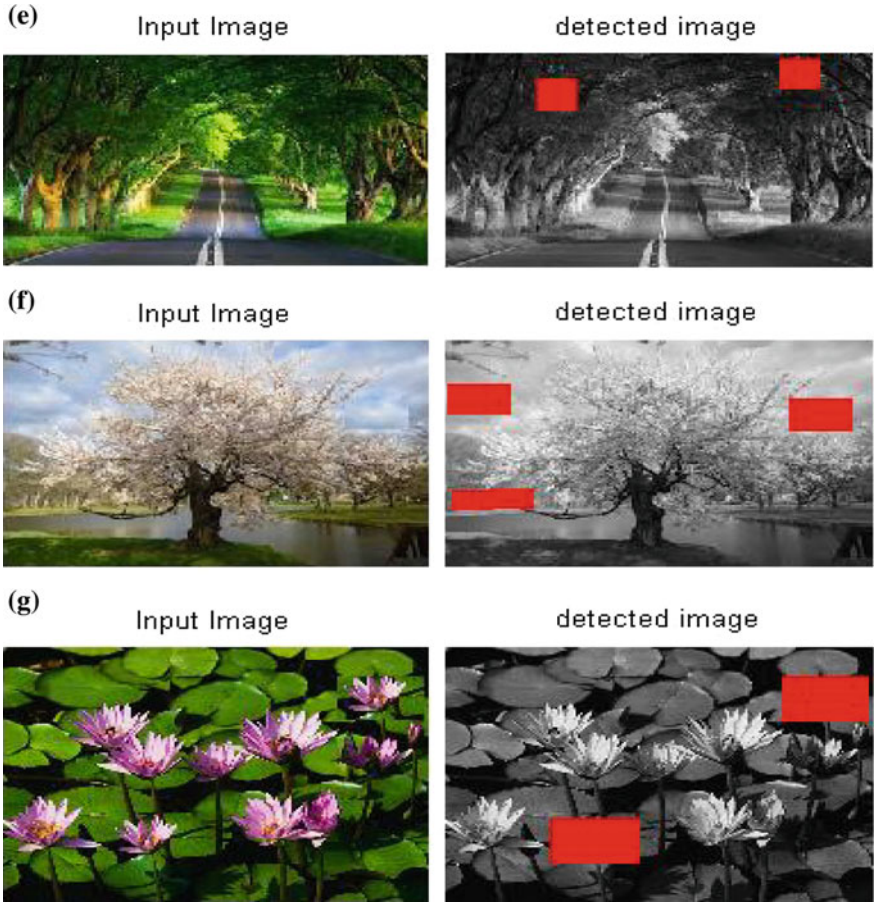

Fig. 3 (continued)

Step 7 If the similarity is found then the block is highlighted (considered as a copied block).

3 Simulation and Results

The experimental results are discussed in this section. The tests were carried out on the MATLAB R2013a, RAM 2 GB, and processor 2.90 GHz, the images with the different pixel values, saved in BMP format, are tested to check the computational speed and robustness of the proposed algorithm.

Figure 3 shows two images: The input image and detected the image. The random rectangular region is copied and pasted onto the same image. The highlighted region

represents the copied region and pasted region. The test conducted without having prior knowledge of the images with different pixel values.

Table 1 shows the computational time of forgery detection of random rectangular regions applied on images using the proposed method and method proposed by Fadl and Semary [1] (the accelerated method). As per the table, the proposed method is improved with enhanced speed compared to the accelerated method.

Figure 4 shows that the performance of the accelerated method, which produces noise while detecting higher pixel value images, and hence its performance is reduced compared to the proposed method. As the pixel values are more, the accelerated method produces noise. The proposed method is more accurate even for higher pixel value. This is highlighted in the first row and last row of Table 1.

Table 1 Comparison of computational time between the proposed method and the accelerated method

Figure	Image pixels	Proposed method (s)	Accelerated method (s)
3a	304 × 408	44.99	78.70 (with noise)
3b	183 × 275	13.07	23.76
3c	300 × 168	14.09	21.09
3d	284 × 177	13.09	22.09
3e	284 × 177	13.95	22.60
3f	276 × 183	14.17	22.03
3g	400 × 300	42.23	84.96 (with noise)

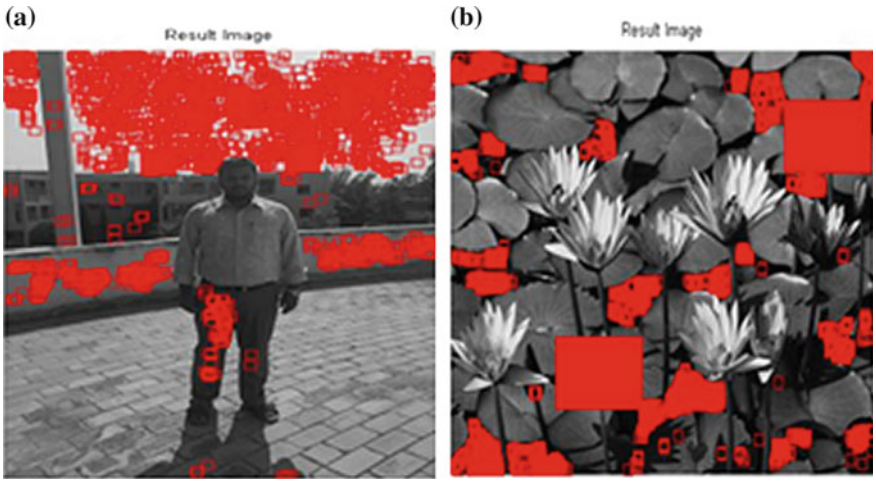

Fig. 4 **a**, **b** Noise during detection in the accelerated method

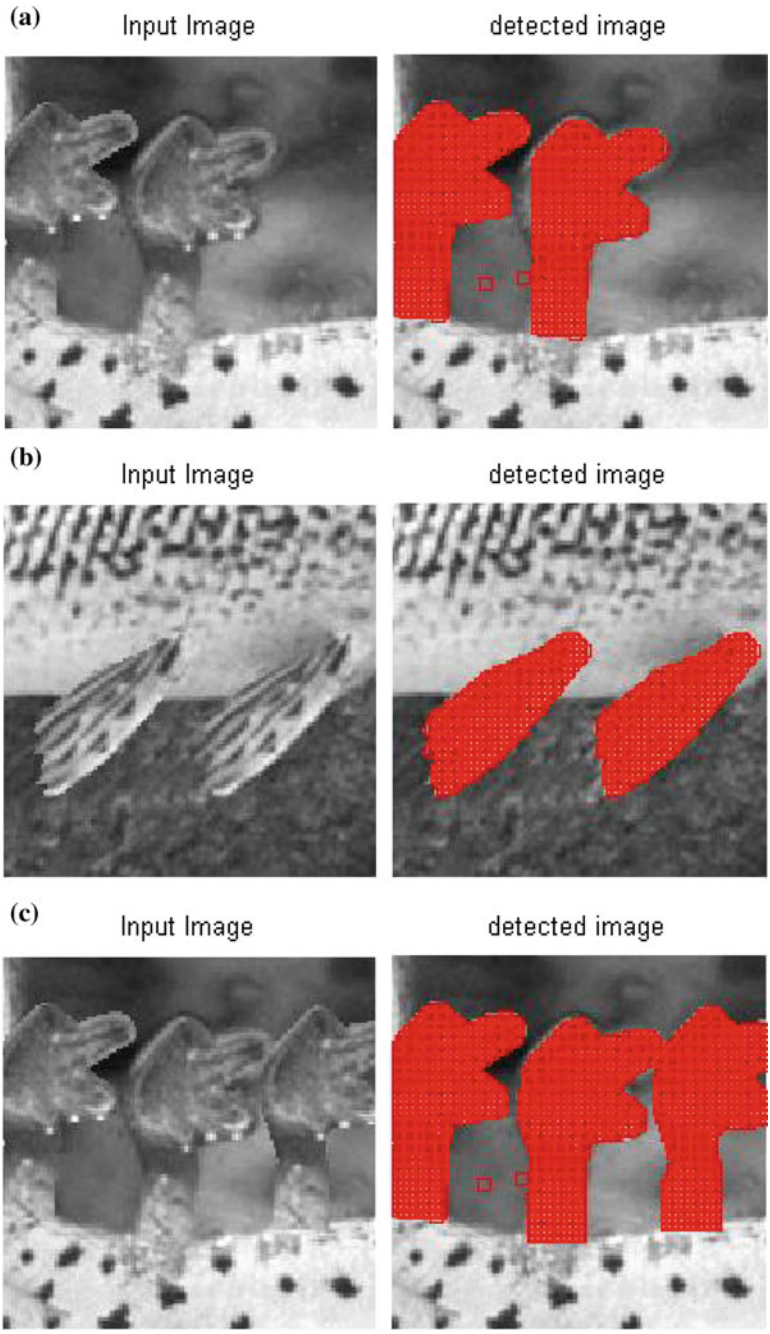

Fig. 5 **a–c** Copy-move detection for irregular regions

Table 2 Comparison of computational time between the proposed method and the accelerated method

Figure	Image pixels	Proposed method (s)	Accelerated method (s)
5a	128×128	3.17	9.46
5b	128×128	3.00	6.42
5c	128×128	3.34	6.86

Figure 5 shows an irregular region that is copied and pasted onto the image. The test shows the detection for the single region and multi-regions. All the images are 128×128 pixel values.

Table 2 shows the computational time of forgery detection of random rectangular regions applied on images using the proposed method and method proposed by Fadl and Semary [1] (the accelerated method). As per the table, the proposed method is improved with enhanced speed compared to the accelerated method.

4 Conclusion

This work is robust to detect copy-move forgery efficiently, by means of DCT features and taking the mean of DCT of blocks and comparing with other blocks of the same image. It works without any prior information about the image. The proposed work is fast and more effective for any pixel values compared to existing methods.

References

1. Fadl SM, Semary NA (2014) A proposed accelerated image copy-move forgery detection. In: Visual communications and image processing conference, IEEE
2. Lynch G, Shih FY, Liao HYM (2013) An efficient expanding block algorithm for image copy-move forgery detection. Inf Sci 239:253–265
3. 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
4. Lin HJ, Wang CW, Kao YT (2009) Fast copy-move forgery detection. WSEAS Trans Sig Process (World Sci Eng Acad Soc) 5(5):188–197
5. Bhargava N, Sharma MM, Garhwal AS (2012) An improved image authentication technique using random-sequence based secret-sharing scheme. In: 2012 International conference on radar, communication and computing (ICRCC), 21–22 Dec. 2012. IEEE 07 Feb 2013
6. Katzenbeisser S, Petitcols FAP (2000) Information techniques for stenography and digital watermarking. Norwood, A, Artec House
7. Alam S, Jamil A, Saldhi A (2015) Digital image authentication and encryption using digital signature. In: 2015 international conference on advances in computer engineering and applications (ICACEA), 19–20 Mar 2015. IEEE 23 July 2015
8. Singh VK, Tripathi RC (2011) Fast and efficient region duplication detection in digital images using sub-blocking method. Int J Adv Sci Technol 35:93–102

9. Liu G, Wang J, Lian S, Wang Z (2010) A passive image authentication scheme for detecting region duplication forgery with rotation. J Netw Comput Appl 34(5):1557–1565
10. Sebe N, Liu Y, Zhuang Y, Huang T, Chang S-F (2007) Blind passive media forensics: motivation and opportunity. In: Multimedia content analysis and mining. Springer, Berlin, pp 57–59
11. Chen C-H, Tang Y-L, Hsieh W-S (2014) Color image authentication and recovery via adaptive encoding. In: 2014 international symposium on computer, consumer and control (IS3C), 10–12 June 2014. IEEE 30 June 2014
12. Zhang Z, Ren Y, Ping XJ, He ZY, Zhang SZ (2008) A survey on passive-blind image forgery by doctor method detection. In: Proceedings of seventh international conference on machine learning and cybernetics, pp 3463–3467
13. Kou G, Ma Y (2015) Color image authentication method based on triple-channel spiking cortical model. In: 2015 10th international conference on broadband and wireless computing, communication and applications (BWCCA), 4–6 Nov 201. IEEE 03 Mar 2016
14. Cox IJ, Miller ML, Bloom JA (2002) Digital watermarking San Francisco. Morgan Kaufmann, Burlington