A copy-move image forgery detection technique based on Gaussian-Hermite moments

Kunj Bihari Meena[1] · Vipin Tyagi[1]

Abstract

Images are one of the most prominently used digital information sharing medium now a days. Due to availability of state-of-the-art image editing tools it has become very easy to forge an image. Among various types of image forgeries, copy-move (region-duplication) forgery cases are emerging very frequently. In copy-move image forgery one or more regions of an image are replicated within the same image. In this paper, a new robust copy-move image forgery detection technique is proposed using Gaussian-Hermite Moments (GHM). The proposed technique divides the input image into overlapping blocks of fixed size and then the Gaussian-Hermite moments are extracted for each block. The matching of similar blocks is done by sorting all the features lexicographically. The experimental results show that the proposed technique can locate the copy-move forged regions in a forged image very accurately. The proposed technique shows promising results in the presence of various post-processing operations scaling, blurring, color reduction, adjustment of brightness, rotation, and JPEG compression.

Keywords Gaussian-Hermite moments · Image forgery · Image forgery detection · Copy-move forgery · Key-point · Passive forgery detection · Post-processing · Tampering detection

1 Introduction

The image editing tools are developed with the intention of helping the human society. However, some ill intentioned people misuse these tools by manipulating the digital images for wrong motives. The manipulation of digital images to change their semantic meaning is known as digital image forgery. In the last few years several image forgery detection techniques have been proposed by researchers. These techniques can be broadly classified as: active and passive image forgery detection techniques. In active image forgery detection

✉ Vipin Tyagi
dr.vipin.tyagi@gmail.com

[1] Jaypee University of Engineering and Technology, Raghogarh, Guna, MP, India

techniques, some prior information about the image (such as digital watermarking and digital signature) is required to detect the image forgery. However, the passive or blind image forgery detection techniques detect the forgery based on the changes in the intrinsic features of the image without any prior information. It is not very difficult to comprehend that active forgery detection techniques are becoming less practical as Internet is flooded with spurious images for which it is almost impossible to have some prior information. Hence, the passive forgery detection techniques are most appropriate way to identify the image forgery in real life scenarios. The passive forgery detection methods are broadly classified into four ways [4, 42]: copy-move forgery detection, image splicing detection, retouching detection and re-sampling detection. The copy-move image forgery is done by replicating a part of the image on the other location of the same image. In general, there may be two motives for such forgeries: one is to hide the some suspicious objects such as gun etc. by pasting the other object or part from the same image; second is to replicate the objects, such as in many instances fake crowd is created by region replication in the image. The latest multimedia tools provide ease of editing the digital images. An expert forger can create a forged image where it becomes almost impossible to differentiate between a fake and authentic image just by seeing the image with human eyes. The researchers have suggested various techniques to detect forgery in images.

Existing passive region-duplication forgery detection techniques can be grouped into two broad classes namely keypoint-based and block-based techniques. The keypoints in an image are defined as the high entropy distinctive local features used to describe an image. In the keypoint-based copy-move forgery detection, keypoints of the input image are extracted using various techniques like SIFT [2, 30], SURF [46], and Harris corner detector [12, 54]. Then the forgery is detected by matching similar keypoints using a suitable matching techniques such as nearest neighbor search and clustering based matching etc. The block-based detection techniques are the alternative to the keypoint based detection techniques which split the whole image into overlapping or non-overlapping sub-images (blocks). Each block is represented using a suitable transform. Finally the detection of forged or genuine image is done on the basis of some feature matching technique. The selection of appropriate feature extraction technique determines the robustness and detection accuracy of the forgery detection technique. The computational time of the detection technique also depends on the type and number of features extracted per block. In the literature, several feature extraction techniques have been proposed which include Discrete Cosine Transform (DCT) [1], Singular Value Decomposition (SVD) [53], geometric moments [23, 32, 35], Fast Walsh-Hadamard Transform (FWHT) [48], Fourier-Mellin Transform (FMT) [55] etc.

The main contributions of this paper are: Firstly, this paper analyzed and summarized the various issues with the existing copy-move forgery detection techniques. To deal with these issues a novel technique to detect copy-move forgery is proposed based on Gaussian-Hermite moments. Secondly, Gaussian-Hermite moments are used to represent each block in the image. The rotation and scale invariance properties make GHM, a promising feature extraction tool for copy-move forgery detection. To the best of our knowledge, this is the first time when Gaussian -Hermite moments are applied in the area of digital image forensics. Thirdly, morphological operations are utilized in an innovative way such that the proposed method is able to detect forgery in very small regions (upto 16 pixels), at the same time overall accuracy also improved significantly. Finally, the robustness and detection accuracy of the proposed technique is exhibited by conducting a number of experiments on three popular image datasets. The results of the proposed technique are compared with the available forgery detection techniques.

The organization of rest of the paper is as follows: Section 2 presents related work in this field. Introduction to Gaussian-Hermite Moment is presented in section 3. Detailed description about the proposed technique is given in section 4. Section 5 describes the experimental results. The work is concluded in the section 6.

2 Related work

Over the past few years, several researchers have shown their keen interest toward image forensics [29]. First time, Fridrich et al. [17] introduced a block-based copy-move image forgery detection technique. This technique extracts features of each overlapped block using discrete cosine transform (DCT). These features are lexicographically sorted and similarity is matched using Euclidean distance. This technique was not able to detect duplicated image regions when regions are rotated or scaled before pasting. Later several authors also employed DCT with various transforms and matching techniques to improve the detection accuracy and reduce computation time [27]. Another DCT based image forgery detection technique was suggested by Luo et al. [25], in which blocks are divided further into four sub-blocks. The kernel principal component analysis (KPCA) and discrete wavelet transform (DWT) are taken together as a feature to detect copy-move image forgery [6]. Multi-scale analysis and voting processes are taken into consideration by Silva et al. [38], in their approach of image forgery detection. Ardizzone et al. [5] developed a copy-move image forgery detection approach based on matching triangles. Cozzolino et al. [15] described a robust image region duplication detection technique by employing dense-field techniques and Zernike moments.

Pun et al. [34] introduced a technique to detect image forgery by merging keypoint features and block-based features. Lee et al. [21] suggested a new copy-move image forgery detection technique based on histogram of orientated gradients. Gürbüz et al. [18] introduced an approach for copy-move image forgery detection using circular projection. A copy-move forgery detection technique was given by Zandi et al. [52], based on interest point detector. Zhu et al. in [56] introduced a copy-move forgery detection technique that employs scaled ORB with RANSAC algorithm. A multi-level dense descriptor (MLDD) based copy-move image forgery detection algorithm was given by Bi et al. in [9]. The super-pixel content based adaptive feature point detector are used by Wang et al. [44] to detect the duplication forgery in digital image. Tralic et al. [41] combined cellular automata (CA) and local binary patterns (LBP) to detect copy-move image forgery. By employing polar complex exponential transform (PCET) moments features, Hosny et al. [19] introduced a copy-move image forgery detection technique. In this technique, initially objects are enclosed in bounding boxes, and then each such sub-image is matched with remaining sub-images. In this technique, the time required to detect image forgery reduced significantly. This technique was robust against common post-processing operations. In [20] an algorithm to detect copy-move image forgery has been given by combining region and texture features. The local bidirectional coherency error refinement based copy-move forgery detection technique was introduced by Bi et al. [8]. In this technique, image tampering is detected on the basis of stability of iteratively calculated feature correspondences. By employing discrete analytic Fourier–Mellin transform and Weber Local Descriptor, Pun et al. [33] introduced a copy-move image forgery detection technique. They used Locality-Sensitive Hashing (LSH) as a matching tool in this technique.

After reviewing several papers main limitations of existing copy-move forgery detection techniques are summarized as: (1) higher computational complexity [43]; (2) less accuracy

when a small region is copy-moved; (3) sometimes keypoint-based techniques fail to differentiate between duplicated regions vs. naturally identical regions; (4) keypoint-based techniques are less accurate in locating the shapes and sizes of duplicated regions; (5) most of the block-based methods can detect forgery within scaling factors [91% -109%] only.

This paper proposes a new robust region-duplication image forgery detection technique that can overcome the above mentioned issues. On the basis of a number of experiments it is demonstrated that the proposed technique is very effective while detecting the copy-move image forgery (including multiple copy-move forgery cases). The proposed technique is able to detect copy-move image forgery in the presence of common post-processing operations: blurring, contrast adjustment, noise addition, color reduction, brightness change and JPEG compression. The experiments performed at pixel level indicate that the proposed technique can identify copy-move image forgery with high accuracy. More specifically, the proposed technique shows good image forgery detection results even if duplicated regions are very small (upto 16 pixels). Apart from these, promising results are also obtained by the proposed technique while detecting the copy-move image forgery in case, copied region is resized or rotated significantly before pasting it.

3 The Gaussian-Hermite moments

The Gaussian-Hermite Moments (GHM) are the set of moments whose basis are the Gaussian-Hermite polynomials. The concept of GHM was introduced by J. Shen in 1997 [36]. GHM has been used in 3D face recognition [7], moving object recognition [45], and license plate character recognition [26] etc. In [47], Yang et al. exhibited the rotation and translation invariant properties of the GHM. Recently Yang et al. [49] showed experimentally that the GHM can be utilized for representing scale invariant features of any image. GHM can be used as a robust tool to extract features from the image which are rotation, translation and scale invariant in nature. These three invariant properties are the basic requirements for any reliable copy-move forgery detection technique. This is because, frequently used geometric transforms in typical copy-move forgeries include translation, rotation and scaling, i.e. in copy-move forgery, copied part either is simply translated without any geometric transformation (generally known as plain copy-move forgery) or translated after rotating or scaling. Along with rotation, translation and scale invariant properties, GHM are also having following favorable properties: (1) GHM are more robust tool for feature representation as compared to Legendre and discrete Tchebichef moments, due to better distribution of zero-crossings in GHM [47]; (2) less sensitive to the noise due to Gaussian smoothing effect [36].

3.1 The Hermite polynomial

The Hermite polynomial of pth degree is defined as:

$$H_p(x) = (-1)^p e^{x^2} \frac{d^p}{dx^p} e^{-x^2} \qquad (1)$$

Eq. (1) can be expressed in the series form as:

$$H_p(x) = \sum_{k=0}^{\frac{p}{2}} \frac{(-1)^k p!}{k!(p-2k)!} (2x)^{p-2k} \qquad (2)$$

Hermite polynomials follow the orthogonal property corresponding to the weight function e^{-x^2}:

$$\int_{-\infty}^{\infty} e^{-x^2} H_p(x) H_q(x) dx = 2^p p! \sqrt{\pi} \delta_{pq} \qquad (3)$$

where δ_{pq} is the Kronecker delta and is defined as:

$$\delta_{pq} = \begin{cases} 1; & p = q \\ 0; & \text{otherwise} \end{cases} \qquad (4)$$

The orthonormal form of the Hermite polynomial is:

$$\hat{H}_p(x) = \left(2^p p! \sqrt{\pi}\right)^{-\frac{1}{2}} e^{\left(-x^2\right)/2} H_p(x) \qquad (5)$$

which also maintains the orthonormal property:

$$\int_{-\infty}^{\infty} \hat{H}_p(x) \hat{H}_q(x) dx = \delta_{pq} \qquad (6)$$

To adjust the scale of Hermite polynomials, substitute the value of x by x/σ in Eq. (5):

$$\hat{H}_p\left(\frac{x}{\sigma}\right) = \left(2^p p! \sqrt{\pi}\right)^{-\frac{1}{2}} e^{-\left(\frac{x}{\sigma}\right)^2} H_p\left(\frac{x}{\sigma}\right) \qquad (7)$$

where σ is the scale parameter or standard deviation of the Gaussian envelop. Eq. (7) represents the generalized orthonormal Hermite polynomials which is commonly known as Gaussian-Hermite polynomial.

3.2 The Gaussian-Hermite moments

The 2D Gaussian-Hermite moments of order (p,q) p, q $\in$ Z is obtained by taking 2D Gaussian-Hermite polynomials as a basis functions as follows:

$$\mu_{pq} = \iint I(x, y) \hat{H}_p\left(\frac{x}{\sigma}\right) \hat{H}_q\left(\frac{y}{\sigma}\right) dx dy \qquad (8)$$

where I(x,y) is the intensity function of a digital image. The image can be reconstructed by using the GHM of order (0,0) to (n,n) as:

$$\hat{I}(x, y) = \sum_{p=0}^{n} \sum_{q=0}^{n} \mu_{pq} \hat{H}_p\left(\frac{x}{\sigma}\right) \hat{H}_q\left(\frac{y}{\sigma}\right) \qquad (9)$$

The translation invariance can be achieved by shifting the Gaussian-Hermite polynomials from the coordinate origin to the centroid of the image. The rotation and scale invariants of the GHM can be obtained using Yang's theorem [49].

4 Proposed image forgery detection technique

This section describes the complete mechanism of the proposed copy-move image forgery detection technique. As mentioned earlier, copy-move forgery involves replication of some parts of the image within the same image. Hence, some kind of correlation is present between the duplicated regions. Most of the forgery detection algorithms take this correlation as a basis

for forgery detection. When replication of the region is done without any post-processing or geometric transformation (known as plain copy-move forgery), then high similarity is exhibited between copy and pasted regions. Therefore, plain copy-move forgery can be detected easily; however expert forger may perform some post-processing operations on the copied regions such as noise addition, color reduction, retouching, blurring, contrast enhancement and JPEG compression in order to make forgery more realistic. At the same time, some kind of geometric transformation such as scaling, rotation and distortion also can be applied during or after the creation of the image forgery. The presence of these post-processing operations and geometric transformations make the image forgery detection very much challenging. In the proposed technique, features of an image are represented using robust GHM. Then the extracted features are lexicographically sorted. After that sorted features are matched using threshold based Euclidian distance. RANdom SAmple Consensus (RANSAC) algorithm [16] and morphological opening operations are used for filtering the outliers. Each of the step of the proposed technique is described in subsequent section 4.1 through section 4.6.

4.1 Computational complexity reduction using pre-processing

To reduce the computational complexity, most common pre-processing step is the conversion of RGB image to the grayscale image using:

$$Y = 0.299R + 0.587G + 0.114B \tag{10}$$

where color components corresponding to red, green and blue are represented by R, G and B respectively.

4.2 Splitting the input image into overlapping blocks

The input image is divided into overlapped blocks (small sub-images) of size $b \times b$ pixels. Therefore, total of $(m-b+1) \times (n-b+1)$ blocks are obtained from an image of size $m \times n$ pixels. The proper selection of block size determines the computational complexity of the technique and smallest detectable regions. If the input image is divided into very small block size then the total number of blocks becomes large, hence more time required to process the image; however in this case copy-move image forgery with very small duplicated regions can be detected. Conversely, large block size reduces the computational complexity in general; but small duplicated image regions may remain undetected.

4.3 Obtaining Gaussian-Hermite moments from a block

Feature extraction is a crucial step in any copy-move forgery detection technique. The selection of better feature extraction technique determines the detection accuracy of the copy-move forgery detection technique. In the proposed technique, three Gaussian-Hermite moments of order 1, order 3 and order 5 are extracted from each block. The proposed technique uses odd order Gaussian-Hermite moments because more information is represented using the odd order moments [51].

Each block is represented using a feature vector of size three. Hence the total numbers of such feature vectors are equal to the number of blocks in the image. All the feature vectors are then stored in the matrix form as:

$$M = \begin{bmatrix} \nu_1 \\ \nu_2 \\ \nu_3 \\ \cdots \\ \cdots \\ \nu_{(m-b+1)\times(n-b+1)} \end{bmatrix} \tag{11}$$

where ν_1, ν_2, ν_3, ... $\nu_{(m-b+1)\times(n-b+1)}$ are feature vectors each of size three.

4.4 Feature matching (searching of similar blocks)

As discussed earlier, some sort of correlation exists between the duplicated regions in the forged image. Even after applying the common post-processing operations the correlation cannot be disturbed completely. Therefore, it is possible to detect such duplicated regions by using suitable feature matching algorithm. First of all, feature vector matrix M obtained using Eq. (11) is lexicographically sorted to arrange all the rows in lexicographic order. Due to lexicographical sorting similar rows become adjacent. Therefore it becomes computationally efficient to find similar features, as feature vectors with similar characteristic are located adjacent to each other in the sorted feature vector matrix M. The Euclidian distance is computed between two feature vectors x and y as follows:

$$D(x,y) = \sqrt{\sum_{r=0}^{N}(x_r - y_r)^2} \tag{12}$$

where N is the number of GHM calculated per block (we have considered $N = 3$ for all the experiments). Since neighboring blocks will produce similar GHM, therefore, these blocks should not be considered as copy-move blocks. To filter out such neighboring blocks, actual distance between two blocks is computed using Eq. (13).

$$\Delta = \sqrt{(i-k)^2 + (j-l)^2} \tag{13}$$

where (i,j) and (k,l) are the co-ordinates of two blocks $B_{i,j}$ and $B_{k,l}$ in the image.

Two blocks are considered similar if $D(x,y) < Similarity\_Threshold$ and $\Delta > Distance\_Threshold$; where $Similarity\_Threshold$ and $Distance\_Threshold$ are two thresholds whose values are set on the basis of experiments.

4.5 Removal of falsely matched blocks

The set of matching features obtained based on the value of $Similarity\_Threshold$ and $Distance\_Threshold$ may contain falsely matched features which surely affect the detection accuracy. Hence, to remove outliers the mutual coordinate positions of each matching block pairs are considered.

The regions are identified as copy-pasted only when certain number ($Frequency\_Threshold$) of matching block pairs with same mutual positions are detected. However, mutual position based outlier removing technique is not suitable for copy-move forgery in which copied region is resized or rotated before pasting. To make the proposed technique robust against rotation and scaling transformations, RANSAC algorithm is also employed. RANSAC algorithm [16] is used to estimate the affine transformations between duplicated regions in order to filter the outlier (falsely matched features) from the inliers

(correctly matched features). The estimated transformation associated with maximum number of inliers is selected after performing certain number of iterations. The proposed technique empirically uses the number of iteration as 1000 and threshold value as 0.5, as this parameter combination produces best performance.

4.6 Post-processing of detection result

The results obtained after applying RANSAC algorithm are considered as final matching blocks. The matching blocks are then marked with two different colors to locate the exact forgery in the image. However, located regions may contain some isolated pixels or holes due to the effect of post-processing operations applied on the image. To fill these small holes surrounded by group of pixels and to discard the isolated pixels, the proposed technique uses morphological opening operation which is dilation followed by erosion. The complete flow-chart of the proposed technique is depicted in Fig. 1.

5 Experimental results

The proposed technique is tested using MATLAB using various datasets.

5.1 Image datasets used and performance evaluation parameters

The proposed technique has been tested using three popular image datasets; GRIP [15], CoMoFoD [39] and CMF dataset [5]. The reason behind the selection of these datasets is that all these datasets contain the ground truth images corresponding to each forged image, as ground truth images are required to evaluate the performance at pixel level. The image size is 768 × 1024 pixels in both GRIP and CMF dataset; however the size of each image is 512 × 512 pixels in CoMoFoD dataset.

The GRIP dataset is composed of 80 true color primary images saved in PNG format. In GRIP dataset, the smallest copied region is of about 4000 pixels, whereas, the size of largest copied region is 50,000 pixels. Figure 2 shows sample images from GRIP dataset. The second dataset is CoMoFoD that includes 200 primary images captured with different views and sites such as nature, buildings, parking areas, city etc. with different backgrounds such as grass, sky, walls, roads, floors, roofs etc. These 200 images are categorized into five groups: (1) 40 forged images are created by applying simple translation (2) 40 forged images are created by rotating the copied regions with different angles (3) 40 images are tampered by scaling the copied region before pasting (4) fourth set of images is created by distorting the copied regions before pasting (5) last set of 40 images are the combinations of two or more geometric transformations. Six post-processing operations (color reduction, JPEG compression, noise addition, image blurring, brightness change, and contrast adjustments) are also applied on each of the image. Therefore, by considering all the five transformations and six post-processing operations, there are total 10,400 images in the CoMoFoD dataset. The size of smallest copy-pasted region is 360 pixels (0.14% of total image size),whereas the largest copy-pasted region comprises 1037 pixels (14.32% of total image size).
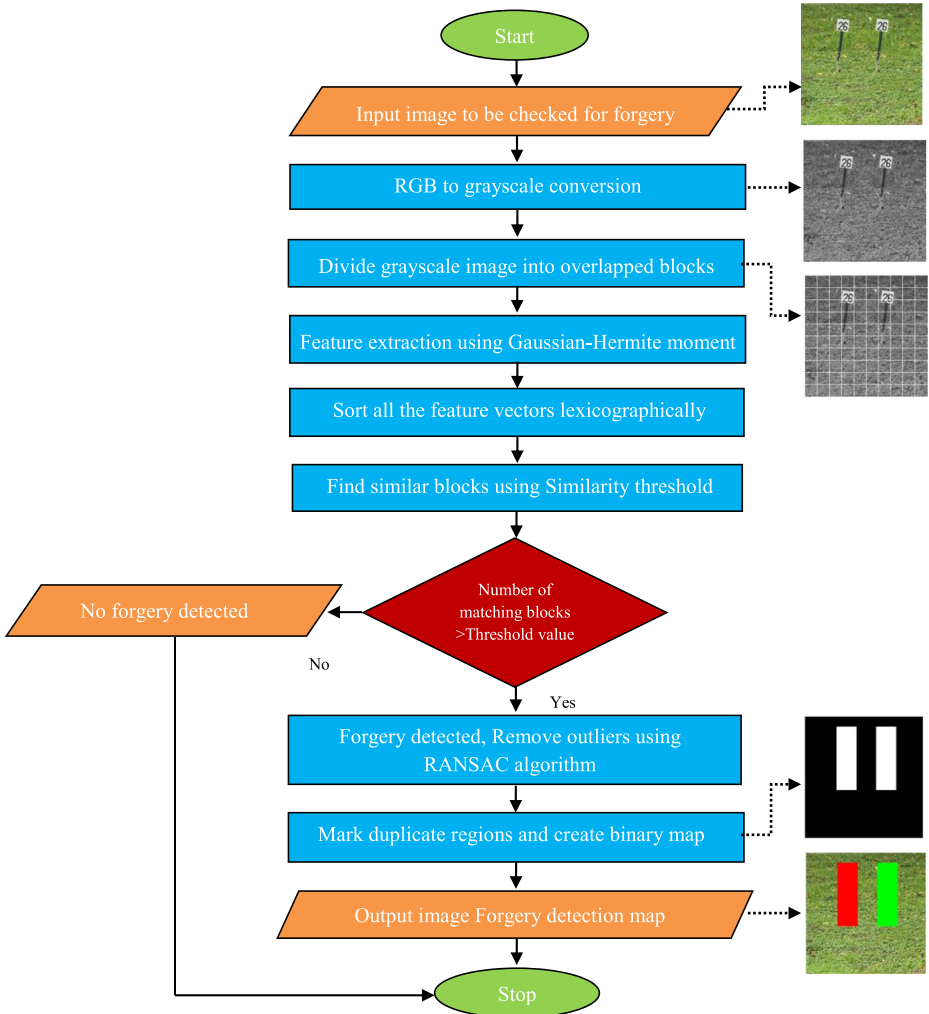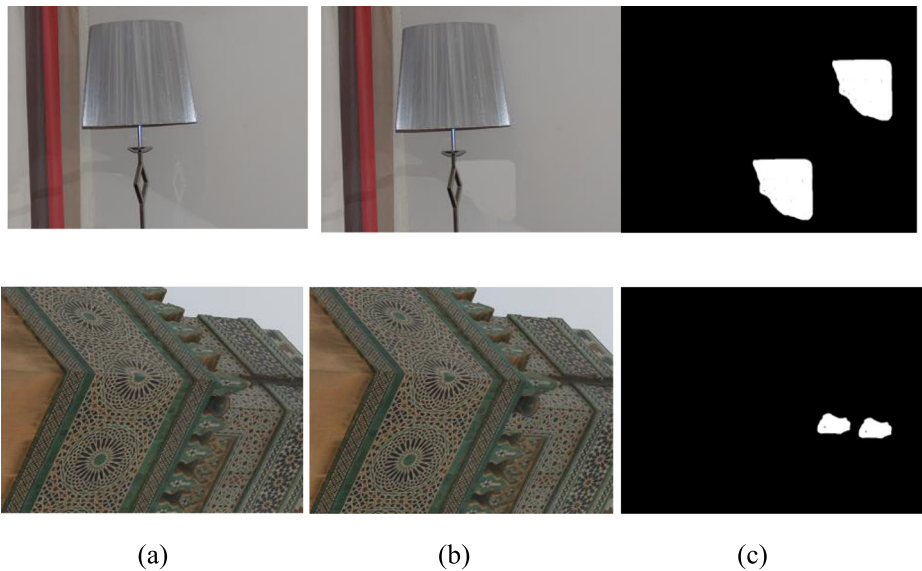
Fig. 1 Flowchart of the proposed technique

The effectiveness of the proposed technique is evaluated based on parameters which are commonly employed by several authors ([13, 34]) for evaluating the copy-move forgery detection technique. These evaluation parameters are; precision, recall and F-measure (Eq.(14)–(16)):

$$\text{Precision } P = \frac{T_p}{T_p + F_p} \tag{14}$$

$$\text{Recall } \quad R = \frac{T_p}{T_p + F_n} \tag{15}$$

Fig. 2 GRIP dataset (top row: forgery in smooth region; bottom row forgery in texture region): (a) Original image (b) Forged image (c) Ground truth image

$$\text{F-measure } F = \frac{2PR}{P+R} \tag{16}$$

where,

T_p is the true positive and defined as the total number of images that are correctly detected as forged. At pixel level, T_p is defined as the total number of pixels that are correctly detected as forged.

F_p is the false positive and defined as the total number of original images that are mistakenly identified as forged. At pixel level, F_p is defined as the number of original pixels that are mistakenly identified as forged.

F_n is the false negative and defined as the total number of forged images that have erroneously not identified. At pixel level, F_n is defined as the total number of forged pixels that are erroneously missed.
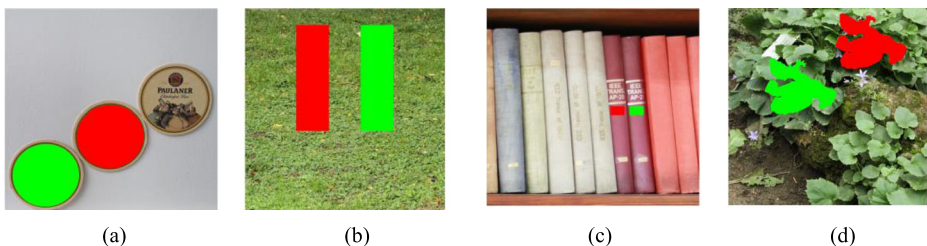
Fig. 3 Detection results of the proposed technique in the presence of plain copy-move image forgery with copied regions of various shapes and sizes

Table 1 Detection results of the proposed technique in the presence of plain copy-move image forgery (including multiple forgeries)

| CoMoFoD Dataset			GRIP dataset			CMF Dataset		
(A) Results at image level								
P (%)	R (%)	F-measure (%)	P (%)	R (%)	F-measure (%)	P (%)	R (%)	F-measure (%)
100	100	100	100	100	100	100	100	100
(B) Results at pixel level								
P (%)	R (%)	F-measure (%)	P (%)	R (%)	F-measure (%)	P (%)	R (%)	F-measure (%)
95.44	95.67	95.55	97.99	98.11	98.05	98.06	92.07	94.97

Higher values of these three parameters indicate the better performance of the detection technique.

5.2 Experimental results of the proposed technique

The evaluation of the proposed copy-move forgery detection technique is carried out at two different levels; at image level and at pixel level. The performance evaluation at image level is merely to evaluate the ability of whether the image is original or forged, and the performance evaluation at pixel level is carried out to check the ability of locating or marking the size and shape of the copy-pasted image regions. It is obvious that performance evaluation at pixel level is possible only when ground truth images are available along with the tampered images. The image level and pixel level experiments have been performed on the CoMoFoD, GRIP, and CMF datasets. The set of experiments are performed by considering all possible post-processing and geometric transformations.

5.2.1 Performance evaluation of the proposed technique under plain copy-move (translation duplication) image forgery

In the plain copy-move image forgery some part of the image is copied and pasted without applying any geometric transformation. The detection results of the proposed technique in presence of plain copy-move forgery are shown in Fig. 3. For image level experiments, 80 forged images and 80 original images are considered from GRIP
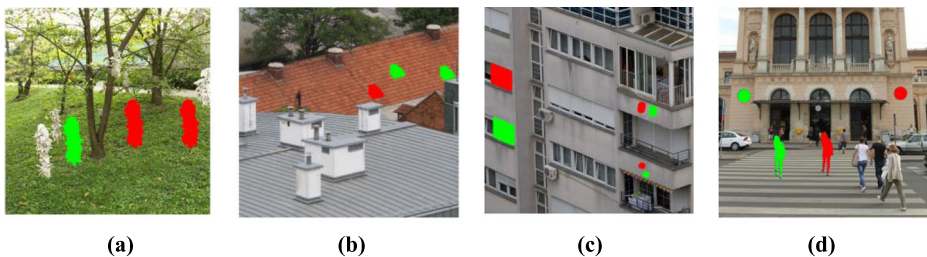
Fig. 4 Detection results of the proposed technique in the presence of multiple copy-move image forgeries: (**a**), (**b**) forgery where one copied region pasted at two separate locations; (**c**) three regions copied and pasted at three different locations; (**d**) two regions are replicated at two separate locations

Table 2 Image forgery detection results of the proposed technique in the presence of image blurring (CoMoFoD dataset)

| Averaging filter size	At image level			At pixel level		
	P (%)	R (%)	F-measure (%)	Average P (%)	Average R (%)	Average F-measure (%)
3 × 3	100	100	100	98.28	87.24	92.43
5 × 5	100	100	100	98.09	78.95	87.49
7 × 7	97.56	100	98.76	96.00	70.71	81.44

dataset. We have also performed image level experiments on CMF dataset by considering all 50 original and all 50 forged images from the dataset. All 40 images numbered from 001_F to 040_F are taken from CoMoFoD dataset for pixel level evaluation. The detection results are shown in Table 1. The proposed technique obtained 100% F-measure value at image level on all three datasets viz. CoMoFoD, GRIP, and CMF datasets (Table 1A), whereas at pixel level the obtained values of F-measures are 95.55%, 98.05%, and 94.97% on CoMoFoD, GRIP, and CMF datasets respectively (Table 1B). By performing a series of experiments the threshold values are set as: *Block_size* = 4, *Similarity_Threshold* = 0.000001, *Distance_Threshold* = 4 and *Frequency_Threshold* = 80.

5.2.2 Performance evaluation of the proposed technique in the presence of multiple copy-move (multiple translation duplication) image forgery detection

Multiple copy-move forgery can be created in two different manners; in first type, one region of the image is copied and then pasted multiple times at various places within the image (Figs. 4a,b); in second type, more than one regions are copied and pasted at various locations within the image (Figs. 4c, d). The experimental results on a set of images taken from CoMoFoD dataset show the robustness of the proposed technique while dealing with multiple image forgeries.

5.2.3 Performance evaluation of the proposed technique when image is post processed with averaging filters (blurring)

To measure the detection accuracy of the proposed technique in the presence of blurring effect, a set of 120 images (numbered from 001_F_IB1 to 040_F_IB3) is considered from the CoMoFoD

(a)   (b)   (c)   (d)
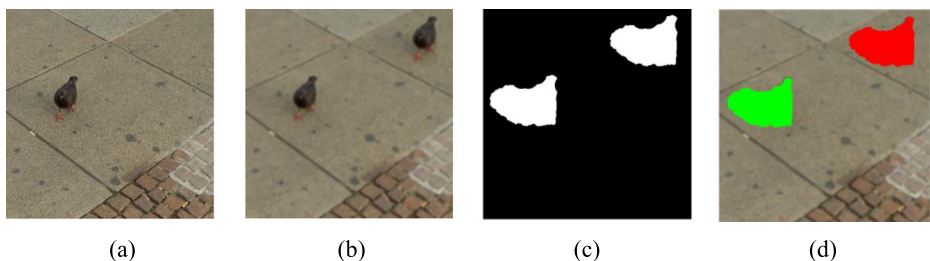
Fig. 5 Image forgery detection results in blurred images: (**a**) Original image (**b**) Forged image after post-processing using 7 × 7 averaging filter (**c**) Ground truth image (**d**) Detection result of the proposed technique

| (a) | (b) | (c) | (d) |
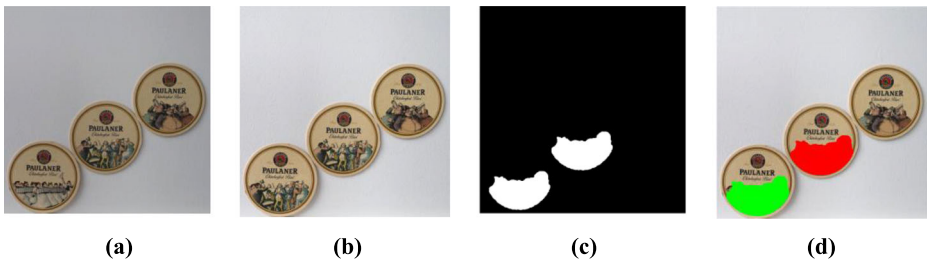
Fig. 6 Image forgery detection results in the presence of brightness change: (**a**) Original image, (**b**) Forged image after post-processing using brightness change [0.01, 0.8], (**c**) Ground truth image, (**d**) Detection result of the proposed technique

dataset. These images are post-processed by three types of averaging filters of size 3×3, 5×5 and 7×7. The image forgery detection results of the proposed technique are shown in Table 2 and Fig. 5. By performing a series of experiments the threshold values are set as: *Block_size* = 8, *Similarity_Threshold* = 0.00000001, *Distance_Threshold* = 4 and *Frequency_Threshold* = 80.

### 5.2.4 Performance evaluation of the proposed technique under brightness change

The evaluation of the performance of the proposed technique in the presence of brightness change post-processing operation is carried out by taking 120 images (numbered from 001_F_BC1 to 040_F_BC3) from the CoMoFoD dataset. Brightness change in the range [0.01, 0.95] does not make much visual difference. However, brightness change in the range [0.01, 0.8] produces much brighter image. Visual detection results of the proposed technique in the presence of changed brightness by [0.01, 0.8] is shown in Fig. 6. Table 3 shows the detection results of the proposed technique with different changes in brightness. It can be observed that the performance of proposed technique is not much affected by the changes in the brightness. Hence the proposed technique is robust against brightness change. By performing a series of experiments the threshold values are set as: *Block_size* = 6, *Similarity_Threshold* = 0.000001, *Distance_Threshold* = 4 and *Frequency_Threshold* = 80.

5.2.5 Performance evaluation of the proposed technique against color reduction (CoMoFoD dataset)

To evaluate the proposed technique in the case of color reduction, the experiments are carried out by considering 120 images (numbered from 001_F_CR1 to 040_F_CR3) from CoMoFoD

Table 3 Image forgery detection results with different alterations in brightness (CoMoFoD dataset)

Range of brightness change	At image level			At pixel level		
	P (%)	R (%)	F-measure (%)	Average P (%)	Average R (%)	Average F-measure (%)
[0.01, 0.95]	100	100	100	93.25	94.25	93.75
[0.01, 0.9]	100	100	100	91.67	93.56	92.61
[0.01, 0.8]	97.56	100	98.76	90.04	90.76	90.40
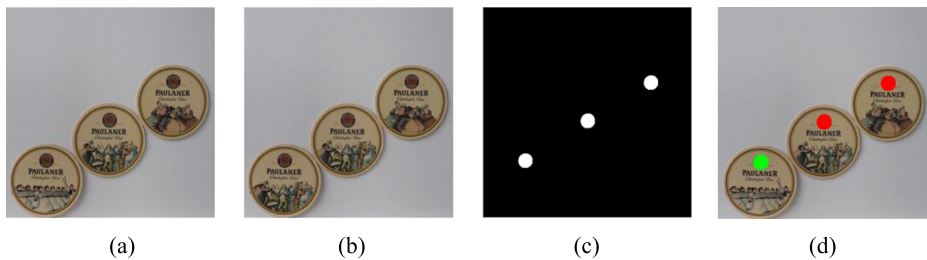
Fig. 7 Image forgery detection results with image color reduction: (**a**) Original image (**b**) Forged image after post-processed using color reduction, intensity levels per each color channel by 128 (**c**) Ground truth image (**d**) Detection result of the proposed technique

dataset. Image forgery detection results obtained with reduced color are shown in Fig. 7. Image forgery detection results in Table 4 show that the proposed technique works well even when colors are reduced significantly. By performing a series of experiments the threshold values are set as: *Block_size* = 6, *Similarity_Threshold* = 0.000001, *Distance_Threshold* = 4 and *Frequency_Threshold* = 80.

### 5.2.6 Performance evaluation of the proposed algorithm against contrast adjustment (CoMoFoD dataset)

The proposed technique is evaluated for image forgery detection against contrast adjustment by considering 120 images (numbered from 001_F_CA1 to 040_F_CA3) from CoMoFoD dataset. Visual results with image that have been contrast adjusted are shown in Fig. 8. Image forgery detection results in Table 5 show that the proposed technique is robust against contrast adjustment. By performing a series of experiments, the threshold values are set as: *Block_size* = 3, *Similarity_Threshold* = 0.000001, *Distance_Threshold* = 4 and *Frequency_Threshold* = 80.

5.3 Performance evaluation of the proposed technique in the presence of JPEG compressions and additive noise

The experiments were also carried out to evaluate the performance of the proposed technique in the presence of additive white Gaussian noise and JPEG compression. Most of the images available over the Internet and social media are in the JPEG format. The JPEG compression uses the lossy compression mechanism; that makes the forgery

Table 4 Results of the proposed technique with various level of color reduction in image (CoMoFoD dataset)

Number of colors per channel	At image level			At pixel level		
	P (%)	R (%)	F-measure (%)	Average P (%)	Average R (%)	Average F-measure (%)
32	100	100	100	95.07	92.73	93.89
64	100	100	100	94.69	92.64	93.65
128	100	100	100	95.00	92.70	93.84

<div align="center">(a)   (b)   (c)   (d)</div>
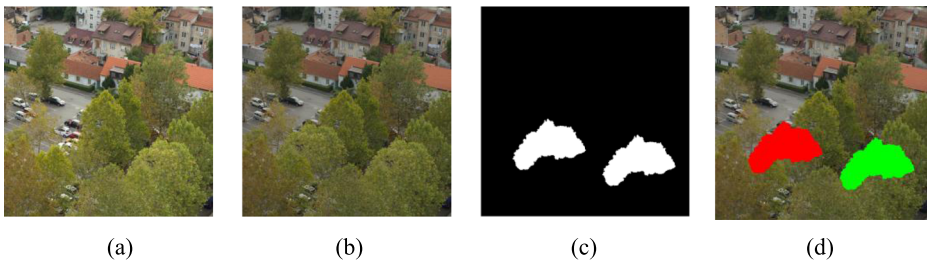
Fig. 8 Image forgery detection results when contrast of the forged image is adjusted as post-processing: (**a**) Original image (**b**) Forged image after post-processing using contrast adjustment with [0.01, 0.8] (**c**) Ground truth image (**d**) Detection result of the proposed technique

detection more challenging. Further, it becomes more difficult to detect forgery when image is stored in the lower quality (JPEG quality factor less than 70%) of the JPEG format. Similarly, adding Gaussian noise also deteriorates the quality of the image that creates the problem in forgery detection. To reduce the effect of noise and data loss introduced by JPEG compression; the input image is smoothed by Gaussian filter. Then the proposed copy-move forgery detection technique is applied on the image. The proposed technique is able to detect the forgery in JPEG and noisy images. Experimentally, the parameters are set as *Block_size* = 4, *Similarity_Threshold* = 10 and *Distance_Threshold* = 4.

5.4 Performance evaluation of the proposed technique in the presence of scaling and rotation

The rotation and scaling are two commonly applied geometric transformations in the copy-move forgery. The performance of the proposed technique is evaluated on the own dataset. We have created a dataset of 50 PNG forged images each of size 200 × 200 pixels using Microsoft Paint software, the forgery is created by applying the scaling (70% to 150%) on the copied region before pasting on the other part of the same image. Figure 9 shows the detection results that prove the robustness of the proposed technique. Proposed technique can detect copy-move forgery even when region is scaled-down upto 80% and scaled-up upto 140% of its original size. Experimentally, the parameters are set as *Block_size* = 4, *Similarity_Threshold* = 10 and *Distance_Threshold* = 4.

Table 5 Image forgery detection results of the proposed technique under various conditions of contrast adjustments (CoMoFoD dataset)

Contrast range	At image level			At pixel level		
	P (%)	R (%)	F-measure (%)	Average P (%)	Average R (%)	Average F-measure (%)
[0.01, 0.95]	100	100	100	95.31	95.80	95.55
[0.01, 0.9]	100	100	100	95.00	95.80	95.40
[0.01, 0.8]	100	100	100	94.54	95.82	95.18

(a) 80%   **(b) 90%**   **(c) 110%**

(d) 120%   **(e) 130 %**   **(f) 140%**
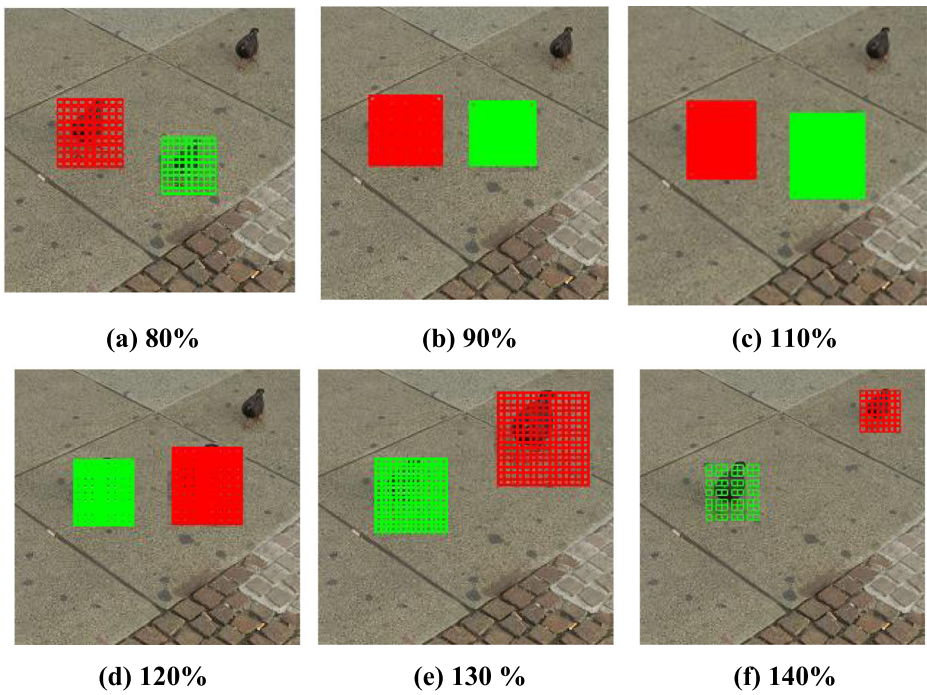
Fig. 9 Image forgery detection results of the proposed technique under various scaling transformations

(a) 90º rotation   **(b) – 90º (270º) rotation**   **(c) 180º rotation**

(d)   **(e)**   **(f)**
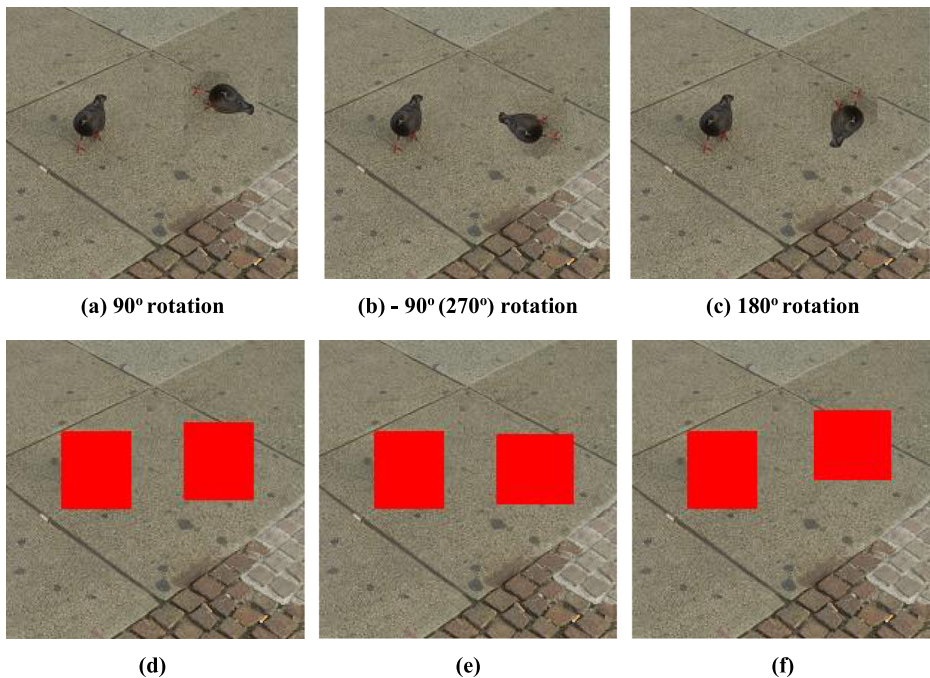
Fig. 10 Image forgery detection results of the proposed technique in the presence of rotation transformations: (**a**), (**b**), (**c**) are forged images; (**d**), (**e**) and (**f**) are respective forgery detection results of the proposed technique

Table 6 Comparison of forgery detection results under plain copy-move forgery at image level on GRIP dataset

| Technique	F-measure (%)
Amerini et al. [3]	67.72
Cozzolino et al. [14]	94.85
Bravo et al. [11]	95.81
Cozzolino et al. [15]	95.92
Bi et al. [10]	92.77
Yang et al. [50]	89.52
Bi et al. [8]	96.63
Proposed technique	**100**

To estimate the robustness of the proposed technique in the presence of rotation transformation separate experiments were performed on a set of images that are created by tampering with the rotations of 90º, 270º and 180º. The experimental results (Fig.10) show that the proposed technique can detect the copy-move image forgery while regions are rotated before pasting it onto other location in the image. The parameters are set as: *Block_size* = 4, *Similarity_Threshold* = 10 and *Distance_Threshold* = 4, empirically.

5.5 Performance comparison of the proposed technique with existing techniques

In this section the proposed technique is compared with the available copy-move forgery detection techniques. A number of researchers have evaluated their copy-move forgery detection techniques on the GRIP dataset. Hence, we have selected GRIP dataset to compare the performance of the proposed technique with existing techniques at image level. As mentioned in Table 1A the proposed technique achieves; P = 100%, R = 100%, and F-measure =100%. Table 6 shows the comparative results in terms of F-measure along with seven copy-move forgery detection techniques viz. Amerini et al. [3], Cozzolino et al. [14], Bravo et al. [11], Cozzolino et al. [15], Bi et al. [10], Yang et al. [50], and Bi et al. [8]. Results in Table 6 show that the proposed technique is superior in comparison to other techniques. Furthermore, it can be observed that the proposed technique achieves 100% F-measure, indicating that the technique is very accurate while detecting forgery.

Table 7 Comparison of forgery detection results under plain copy-move forgery at pixel level on CoMoFoD dataset

Technique	Feature used	F-measure(%)
Tralic et al. [40]	Cellular automata	94.28
Fridrich et al. [17]	DCT	92.72
Ryu et al. [35]	Zernike	90.36
Popescu et al. [31]	PCA	77.15
Shivakumar et al. [37]	SURF	71.81
Silva et al. [38]	Multi-scale analysis	54.93
Liu et al. [24]	Convolutional kernel network	52.46
Li et al. [22]	Segmentation-based	47.98
Manu et al. [28]	Affine transformation property	77.27
Proposed technique	**Guassian Hermite Moments**	**95.55**
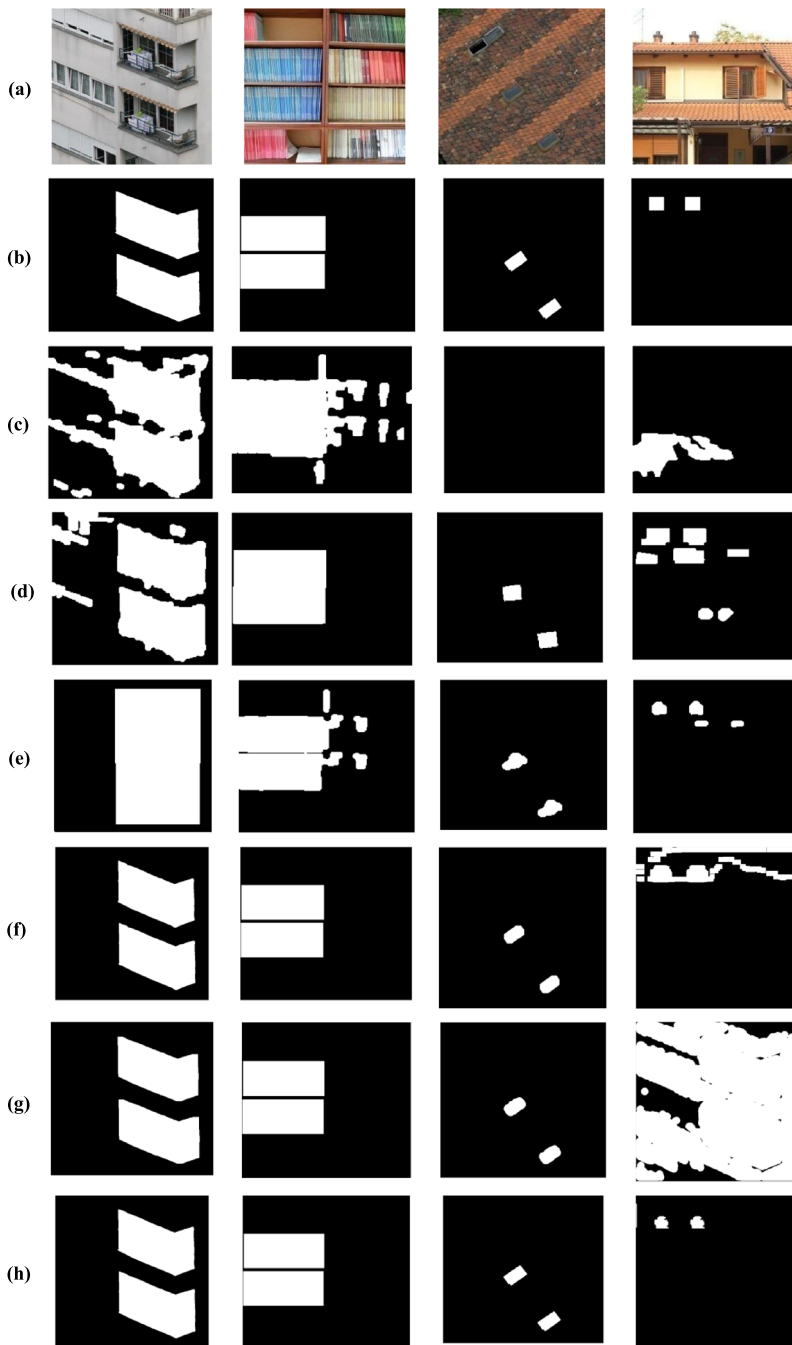
Fig. 11 Visual comparison of image forgery detection results: (**a**) Forged images (**b**) Ground truth images (**c**) Li et al. [22] (**d**) Silva et al. [38] (**e**) Liu et al. [24] (**f**) Fridrich et al. [17] (**g**) Ryu et al. [35] (**h**)Proposed technique

Table 8 Average CPU-time (in seconds) taken by the proposed technique

	Average image size	
	512 × 512 pixels	768 × 1024 pixels
CPU-time (in seconds)	57.79	148.64

The identification of forged or original image is one of the aspects of any forgery detection technique. However, many practical situations require exact shape and size of the duplicated regions. In order to examine forgery locating capability of the proposed technique, different set of experiments (described in section 5.2.1 through 5.2.6) were carried out on the images taken from CoMoFoD dataset. The results at pixel level are compared with nine copy-move forgery detection techniques viz. Tralic et al. [40], Fridrich et al. [17], Ryu et al. [35], Popescu et al. [31], Shivakumar et al. [37], Silva et al. [38], Liu et al. [24], Li et al. [22], and Manu et al. [28]. Table 7 shows the comparative results at pixel level on CoMoFoD dataset.

From Table 7 it can be observed that the proposed technique outperforms referenced copy-move forgery detection techniques. Figure 11 shows the visual forgery detection results of the proposed technique along with the results of techniques of Silva et al. [38], Liu et al. [24], Li et al. [22], and Fridrich et al. [17], and Ryu et al. [35]. These results also show that the proposed technique can mark the forged regions with better accuracy as compared to other copy-move forgery detection techniques. Table 8 shows the average CPU-time taken by the proposed technique to process images of various sizes. The proposed technique is simulated using MATLAB R2016a on a computer with 8 GB RAM.

6 Conclusion

In this paper a technique is proposed to detect and locate the copy-move forgery in digital images. The proposed technique employs Gaussian-Hermite moments to extract the image features. The Gaussian-Hermite moments are moments whose bases are Gaussian-Hermite polynomials. Experimental results show that the proposed technique can detect copy-move forgery with almost 100% accuracy. Furthermore, it is also shown that the proposed technique can locate the copy-pasted regions very accurately. The values of average F-measure at pixel level are also very high. Experimental results show that the proposed technique outperforms other referenced techniques at image level as well as at pixel level. Furthermore, the proposed technique is able to detect forgery when copied region is scaled by any factor within the range of [80% -140%]. The proposed technique can also detect very small (upto 16 pixels) copy-pasted region.

References

1. 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

2. Amerini G, Ballan I, Caldelli L, Bimbo R, Del Serra A (2011) A SIFT-based forensic method for copy – move attack detection and transformation recovery. IEEE Trans. Inf. Forensics Secur. 6(3):1099–1110

3. Amerini I, Ballan L, Caldelli R, Del Bimbo A, Del Tongo L, Serra G (2013) Copy-move forgery detection and localization by means of robust clustering with J-linkage. Signal Process Image Commun 28(6):659–669

4. Ansari MD, Ghrera SP, Tyagi V (2014) Pixel-based image forgery detection: a review. IETE J Educ 55(1): 40–46

5. Ardizzone E, Bruno A, Mazzola G (2015) Copy-move forgery detection by matching triangles of Keypoints. IEEE Trans. Inf. Forensics Secur. 10(10):2084–2094

6. Bashar M, Noda K, Ohnishi N, Mori K (2010) Exploring duplicated regions in natural images. IEEE Trans Image Process 99:1–40

7. Belghini N, Kharroubi J (2012) 3D face recognition using Gaussian Hermite moments. Int J Comput Appl 0975(888):3–6

8. Bi X, Pun CM (2018) Fast copy-move forgery detection using local bidirectional coherency error refinement. Pattern Recogn 81:161–175

9. Bi X, Pun CM, Yuan XC (2016) Multi-level dense descriptor and hierarchical feature matching for copy-move forgery detection. Inf. Sci. (Ny). 345:226–242

10. Bi X, Pun C, Yuan X (2016) Multi-level dense descriptor and hierarchical feature matching for copy – move forgery detection. Inf. Sci. (Ny). 345:1–17

11. Bravo SS and Nandi AK (2011) Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics, in *Proc. Int.Conf. Acoustics, Speech and Signal Processing*, pp. 1880–1883

12. Chen L, Lu W, Ni J, Sun W, Huang J (2013) Region duplication detection based on Harris corner points and step sector statistics. J Vis Commun Image Represent 24(3):244–254

13. Christlein V, Riess C, Jordan J, Riess C, Angelopoulou E (2012) An evaluation of popular copy-move forgery detection approaches. IEEE Trans Inf Forensics Secur 7(6):1841–1854

14. Cozzolino D, Poggi G, and Verdoliva L (2014) Copy-move forgery detection based on PatchMatch, in *IEEE International Conference on Image Processing*, pp. 5312–5316

15. Cozzolino D, Poggi G, Verdoliva L (2015) Efficient dense-field copy-move forgery detection. IEEE Trans. Inf. Forensics Secur. 10(11):2284–2297

16. Fischler MA, Bolles RC (1981) Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography. Commun ACM 24(6):381–395

17. Fridrich J, Soukal D, Lukáš J (2003) Detection of copy-move forgery in digital images. Digit Forensic Res Work 3:652–663

18. Gürbüz E, Ulutaş G, and Ulutaş M (2015) Rotation Invariant Copy Move Forgery Detection Method, in *Proceedings of the 9th International Conference on Electrical and Electronics Engineering (ELECO)*, pp. 202–206

19. Hosny KM, Hamza HM, Lashin NA (2018) Copy-move forgery detection of duplicated objects using accurate PCET moments and morphological operators. Imaging Sci J 66(6):1–16

20. Isaac MM, Wilscy M (2018) Image forgery detection using region - based rotation invariant co-occurrences among adjacent LBPs. J Intell Fuzzy Syst 34(3):1679–1690

21. Lee JC, Chang CP, Chen WK (2015) Detection of copy-move image forgery using histogram of orientated gradients. Inf. Sci. (Ny). 321:250–262

22. Li J, Li X, Yang B, Sun X (2015) Segmentation-based image copy-move forgery detection scheme. IEEE Trans. Inf. Forensics Secur. 10(3):507–518

23. Liu XWY, Xu H, and Wang P (2016) Robust copy – move forgery detection using quaternion exponent moments, *Pattern Anal. Appl.*

24. Liu Y, Guan Q, Zhao X (2017) Copy-move forgery detection based on convolutional kernel network. Multimed Tools Appl 77:1–25

25. Luo W, Jiwu H (2006) Robust detection of region-duplication forgery in digital image. 18th Int Conf Pattern Recognit 4:746–749

26. Ma X, Pan R, and Wang L (2010) License plate character recognition based on Gaussian-Hermite moments, *2nd Int. Work. Educ. Technol. Comput. Sci. ETCS 2010*, vol. 3, no. c, pp. 11–14

27. Mahmood T, Mehmood Z, Shah M, Saba T (2018) A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform. J Vis Commun Image Represent 53:202–214

28. Manu VT, Mehtre BM (2018) Copy-move tampering detection using affine transformation property preservation on clustered keypoints. Signal, Image Video Process. 12(3):549–556

29. Meena KB and Tyagi V (2019) Image Forgery Detection : Survey and Future directions, in *Data, Engineering and applications, vol.2*, Springer Singapore, pp. 163–194, https://doi.org/10.1007/978-981-13-6351-1_14

30. Pan X, Lyu S (2010) Region duplication detection using image feature matching. IEEE Trans. Inf. Forensics Secur. 5:857–867
31. Popescu A and Farid H (2004) Exposing Digital Forgeries by Detecting Duplicated Image Regions, Dartmouth College, Computer Science, Tech. Rep. TR2004–515
32. Prakash CS, Kumar A, Maheshkar S, and Maheshkar V (2018) An integrated method of copy-move and splicing for image forgery detection, *Multimed. Tools Appl.*, pp. 1–25
33. Pun CM, Chung JL (2018) A two-stage localization for copy-move forgery detection. Inf Sci (Ny) 463–464: 33–55
34. Pun C, Member S, Yuan X, Bi X (2015) Image forgery detection using adaptive Oversegmentation and feature point matching. IEEE Trans. Inf. Forensics Secur. 10(8):1705–1716
35. Ryu SJ, Kirchner M, Lee MJ, Lee HK (2013) Rotation invariant localization of duplicated image regions based on zernike moments. IEEE Trans. Inf. Forensics Secur. 8(8):1355–1370
36. Shen J (1997) Orthogonal Gaussian–Hermite moments for image characterization. In: SPIE intelligent robots computer vision XVI, Pitts- burgh, pp 224–233
37. Shivakumar BL, Baboo S (2011) Detection of region duplication forgery in digital images using SURF. Int J Comput Sci Issues 8(4):199–205
38. Silva E, Carvalho T, Ferreira A, Rocha A (2015) Going deeper into copy-move forgery detection: exploring image telltales via multi-scale analysis and voting processes. J Vis Commun Image Represent 29:16–32
39. Tralic D, Zupancic I, Grgic S, and Grgic M (2013) CoMoFoD - New Database for Copy-Move Forgery Detection, in *Proceedings of 55th International Symposium ELMAR-2013*, pp. 25–27
40. Tralic D, Rosin PL, Sun X and Grgic S (2014) Detection of Duplicated Image Regions using Cellular Automata, in *Proceedings of the International Conference on Systems, Signals and Image Processing (IWSSIP)*, pp. 167–170
41. Tralic D, Grgic S, Sun X, Rosin PL (2016) Combining cellular automata and local binary patterns for copy-move forgery detection. Multimed Tools Appl 75(24):16881–16903
42. Tyagi V (2018) *Understanding Digital Image Processing*. CRC Press
43. Ustubioglu B, Ulutas G, Ulutas M, Nabiyev VV (2016) A new copy move forgery detection technique with automatic threshold determination. AEU - Int J Electron Commun 70(8):1076–1087
44. Wang X, Li S, Liu Y (2016) A new keypoint-based copy-move forgery detection for small smooth regions. Multimed Tools Appl 76(22):23353–23382
45. Wu Y, Shen J (2004) Moving object detection using orthogonal Gaussian-Hermite moments. Vis Commun Image Process 5308:841–849
46. Xu B, Wang J, Liu G, and Dai Y (2010) Image copy-move forgery detection based on SURF, in *Proceedings - 2nd International Conference on Multimedia Information Networking and Security, MINES 2010*, pp. 889–892
47. Yang B, Li G, Zhang H, Dai M (2011) Rotation and translation invariants of Gaussian-Hermite moments. Pattern Recogn Lett 32(9):1283–1298
48. Yang B, Sun X, Chen X, Zhang J, Li X (2013) An efficient forensic method for copy-move forgery detection based on DWT-FWHT. Radioengineering 22(4):1098–1105
49. Yang B, Kostková J, Flusser J, Suk T (2017) Scale invariants from Gaussian–Hermite moments. Signal Process 132:77–84
50. Ying Yang H, Niu Y, Xian Jiao L, Nan Liu Y, Yang Wang X, and Li Zhou Z (2017) Robust copy-move forgery detection based on multi-granularity Superpixels matching, *Multimed. Tools Appl.*, pp. 1–27
51. Youfu W, Jun S (2005) Properties of orthogonal Gaussian-Hermite moments and their applications. EURASIP J Appl Signal Processing (4):588–599
52. Zandi M, Mahmoudi-Aznaveh A, Talebpour A (2016) Iterative copy-move forgery detection based on a new interest point detector. IEEE Trans. Inf. Forensics Secur. 11(11):2499–2512
53. Zhao J, Guo J (2013) Passive forensics for copy-move image forgery using a method based on DCT and SVD. Forensic Sci Int 233:158–166
54. Zhao J, Zhao W (2013) Passive forensics for region duplication image forgery based on Harris feature points and local binary patterns. Math Probl Eng 4:1–12
55. Zhong J, Gan Y (2016) Detection of copy – move forgery using discrete analytical Fourier – Mellin transform. Nonlinear Dyn 84(1):189–202
56. Zhu Y, Shen X, Chen H (2016) Copy-move forgery detection based on scaled ORB. Multimed Tools Appl 75(6):3221–3233

Kunj Bihari Meena is working as Asst. Prof. in the Dept. of CSE at Jaypee University of Engg and Technology, Raghogarh, Guna (MP) India. He has completed his M. Tech in Computer Science from IIT Kharagpur in 2013. Now he is working for PhD under the guidance of Prof. Vipin Tyagi in the area of image forgery detection.

Vipin Tyagi is working as Prof. in Dept. of CSE and Head of Faculty of Mathematical Sciences at Jaypee University of Engg and Technology, Raghogarh, Guna (MP) India. He was President of Engineering Sciences Section of the Indian Science Congress Association for the term 2010-11, and recorder for the term 2008 - 2010. He is a Fellow of the Institution of Electronics and Telecommunication Engineers, New Delhi. He was Vice President - Region 3 of Computer Society of India for two terms. He is an expert in the area of Cyber Security, Cyber Forensics and Image Processing. He has authored a number of papers in reputed journals, conferences and books published by Springer Publishers and CRC Press, Taylor and Francis Publishers.