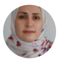
State of the art in passive digital image forgery detection: copy-move image forgery

Article *in* Pattern Analysis and Applications · May 2018

DOI: 10.1007/s10044-017-0678-8



Somayeh Sadeghi
University of New Brunswick
21 PUBLICATIONS **613** CITATIONS
SEE PROFILE

Sajjad Dadkhah
University of New Brunswick
62 PUBLICATIONS **2,338** CITATIONS
SEE PROFILE

Hamid A Jalab
Al-Ayen Iraqi University
159 PUBLICATIONS **3,318** CITATIONS
SEE PROFILE

Giuseppe Mazzola
University of Palermo
40 PUBLICATIONS **746** CITATIONS
SEE PROFILE

Pattern Analysis and Applications
https://doi.org/10.1007/s10044-017-0678-8

SURVEY

State of the art in passive digital image forgery detection: copy-move image forgery

Somayeh Sadeghi[1] · Sajjad Dadkhah[2] · Hamid A. Jalab[1] · Giuseppe Mazzola[3] · Diaa Uliyan[1]

Received: 7 September 2015 / Accepted: 13 December 2017

Abstract

Authenticating digital images is increasingly becoming important because digital images carry important information and due to their use in different areas such as courts of law as essential pieces of evidence. Nowadays, authenticating digital images is difficult because manipulating them has become easy as a result of powerful image processing software and human knowledge. The importance and relevance of digital image forensics has attracted various researchers to establish different techniques for detection in image forensics. The core category of image forensics is passive image forgery detection. One of the most important passive forgeries that affect the originality of the image is copy-move digital image forgery, which involves copying one part of the image onto another area of the same image. Various methods have been proposed to detect copy-move forgery that uses different types of transformations. The goal of this paper is to determine which copy-move forgery detection methods are best for different image attributes such as JPEG compression, scaling, rotation. The advantages and drawbacks of each method are also highlighted. Thus, the current state-of-the-art image forgery detection techniques are discussed along with their advantages and drawbacks.

Keywords Digital forensic · Copy-move forgery · Duplicated detection · Passive authentication · Manipulation detection

1 Introduction

Due to the availability of powerful image processing software and the usage of digital images in different areas, the authenticity of digital images increasingly becomes a critical issue. Nowadays, digital images are used as incontestable evidence for crimes in courts of law; they are also used in medical imaging, journalism, digital forensics and scientific publications [2, 42]. Modifying a digital image by cloning some part of the image and creating a new forged image is very critical because the content of the image will have been changed. Thus, the image cannot play its important role as evidence. Therefore, authenticating digital images is very important and makes forensic science essential [9].

Forensics is the use of technology and science to inspect and determine reality in courts of law for criminal cases [11, 56]. It is categorized into two main groups: analogue forensic and digital forensics. Figure 1 illustrates the ontology of forensics.

Analog forensics, also known as classical forensics, focuses on finding traces of physical evidence in reality, which can neither be wrong nor perjure itself [18]. The main focus of forensic research today is on digital forensics, which is classified into either computer forensics and multimedia forensics [78].

Computer forensics is used when computers are used in criminal actions that take place in the real world, and investigators attempt to extract evidence from the computers. As

✉ Sajjad Dadkhah
dadkhah.sajjad197@mail.kyutech.jp

Somayeh Sadeghi
sasomayeh1@gmail.com

Hamid A. Jalab
hamidjalab@um.edu.my

Giuseppe Mazzola
giuseppe.mazzola@unipa.it

Diaa Uliyan
diaa_uliyan@siswa.um.edu.my

[1] Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia

[2] Kyushu Institute of Technology, 680-4 Kawazu, Iizuka, Fukuoka 820-8502, Japan

[3] Dipartimento di Ingegneria Chimica, Gestionale, Informatica, Meccanica Universit degli Studi di Palermo, viale delle Scienze bd.6, Palermo, Italy

Published online: 26 December 2017

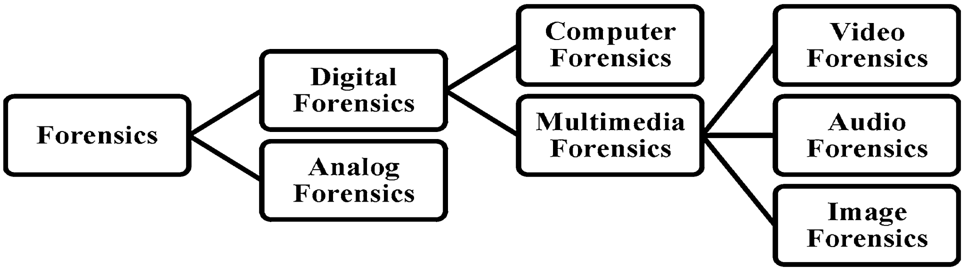


Fig. 1 Ontology of forensics

such, this evidence must be sufficiently trustworthy to be acceptable in a court of law [80]. *Multimedia forensics* is the same as computer forensics in terms of digital evidence, but digital evidence in multimedia forensics is connected to the outside world and cannot be replicated using computers. Its aim is to restore part of the lost reliability of digital media by creating instruments to manifest obvious traces of any change that occurred [18, 21].

Image Forensics seeks to identify the evidence of forgeries and mainly involves enhancing the credibility of digital images. It addresses the issue of authenticating images or their origins and provides credible answers about the origin and authenticity of digital images [53]. *Video forensics* identifies video manipulation, which is then used to create fake videos for illegal purposes. Forging digital video is destructive because videos have always been an integral weapon in the fight against crime [90]. *Audio forensics* is the area of forensic science that relates to the acquisition, analysis, and evaluation of sound recordings. They can finally be accepted as evidence for investigating and setting up facts in criminal courts of law or as part of official investigations into accidents, fraud, or some other civil cases [71].

1.1 Image forgery

Everyday, an assortment of apparatuses creates a huge number of advanced archives, which are then dispersed by daily papers, television, magazines, and the Internet. Images play an influential role in the communication in all these channels; moreover, by increasing the power of image processing tools, manipulating these images becomes very simple [23]. For instance, after the Los Angeles Times event spread a tampered image from the Iraqi front, Professor Russell Frank, a Journalism Ethics professor at Penn State University, said: Whoever said the camera never lies was a liar [79].

Image forgery is the creation of a fake image by changing the content of the original image and producing it as the original photograph for illegitimate goals. Image forgery is an essential topic because the significance of digital image authentication has gained a great amount of attentions recently because digital multimedia is now commonly used in different security applications or organizations. Therefore, appropriate actions for detecting altered images are now being investigated. This effort is important because such detection techniques can be used for high security organizations, such as immigration organization, where digital images and e-passports interact and images stored on passport chips, or in less vital cases such as smart cards, must be authenticated.

1.2 Image forgery creation

Just within a few years after the invention of photography, different techniques were developed for the manipulation of photographs. One of the forgeries that aided in the creation of photographs was combination prints, where darkrooms were used to print many parts of an image in a single page of photographic paper. The first famous combination prints are found in Oscar G. Reijlanders The Two Ways of Life (1857), which used up to 30 separate negatives and took six weeks to produce [15, 77].

In the early twentieth century, the use of copy and paste composite images increased and was mainly used for political quips or in art [97]. An example of earlier image forgeries is presented here. Figure 2 shows a forgery sample from 1939. The right side shows the original image, and left side is the tampered image. It is a photograph of Queen Elizabeth and Canadian prime minister William Lyon Mackenzie King in Banff, Alberta. King George VI was eliminated from the original image, and tampered image has been used in an election advertisement for the prime minister. Some hypothesize that the image had manipulated by the prime minister to show his power by illustrating a photograph of only him and the Queen [34].

The process of creating image forgeries starts by extracting a portion of the image or a 3D object model from the input image. Then, attackers can combine parts of the image or segments of the image that are created from the transformed 2D or 3D model into a different image. Finally, the combined image is retouched to eliminate specific objects from the image or to hide some elements [99].

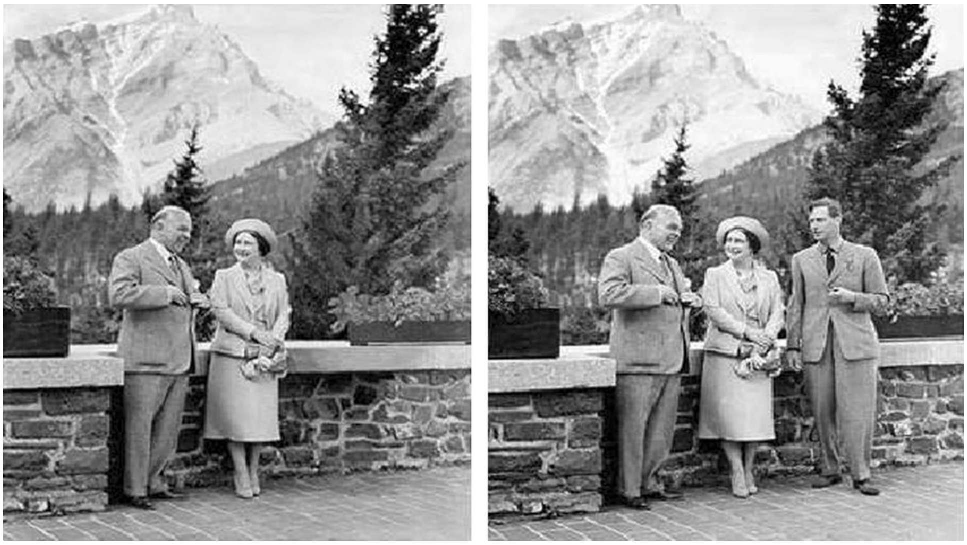


Fig. 2 Image forgery sample (1939)

2 Image forgery detection classification

Image forgery detection refers to the authentication of images and the detection of which part of the image has been tampered. When a digital image is forged, the statistical characteristics of the image are shown to have changed. Thus, the statistical characteristics of the tampered region are likely distinct from the original one. To detect forged areas, the statistical characteristics of every section of the image is computed and compared with each other [99]. Image forgery detection is generally divided into two categories:

1. Active detection [27, 56].
2. Passive detection [6, 59].

Active detection is based on digital signatures or watermarking [91]. Active detection is focused on digital signatures or watermarking. Watermarking is the process of inserting particular data in the image by a person or with an equipped camera [8, 30, 35, 66]. A digital signature may be used for authentication of an image. The exclusive features are extracted from the image as a signature, and then the signature is recreated with the same technique for comparison with the original signature. The trustworthiness of a digital signature can be used as valid evidence [29, 33, 53].

Passive detection refers to detection of forgery by using only the features of the image itself exclusive of extra information. It is a new and important task in image processing. Passive detection has two main categories: forgery detection and source identification [99]. *Source identification* refers to determining the source of digital equipments, such as scanners or cameras. *Forgery detection* concentrates on the authentication of digital images and the location of manipulated areas. It is divided into three types: image splicing forgery, image retouching, and copy-move forgery [92].

Image splicing is the process of creating a forged image by copying one part of an image and pasting it to a different image [45, 59, 70, 74]. It creates a forged image by combination of few images [32, 39, 69, 100].

Image retouching does not clearly alter the image. Thus, it can be regarded as a less damaging kind of digital image forgery. It only enhances few features of the image and is widely known among magazine photography editors [54, 64].

Copy-move forgery copies some part of the image and pastes it to a different part of the same image to hide a significant scene in the image and create another forged image [63]. This kind of forgery is famous because detecting it is more complicated. It is harder because some image features such as colour and noise are same with the rest of the image, and the source and destination of the tampered image are same which makes it more difficult [13, 28].

The detection of copy-move forgery has increased since 2003, and many studies have been published in numerous conferences and journals about it. Figure 3 illustrates the number of papers published in conferences and journals as indexed by Web of Science and SCOPUS since 2007. The data were collected from the Web of Science and SCOPUS website.

Figure 4a shows an example of image splicing forgery, which was released during the 2004 presidential election campaign. It shows Kerry and Jane Fonda speaking simultaneously at an anti-Vietnam war objection to taint Kerry's war record by linking him with Fonda [82]. Figure 4b shows image retouching forgery, which was released on June 1994, in which a darkened mug shot of troubled football star O.J. Simpson appeared on the cover of TIME Magazine. His skin

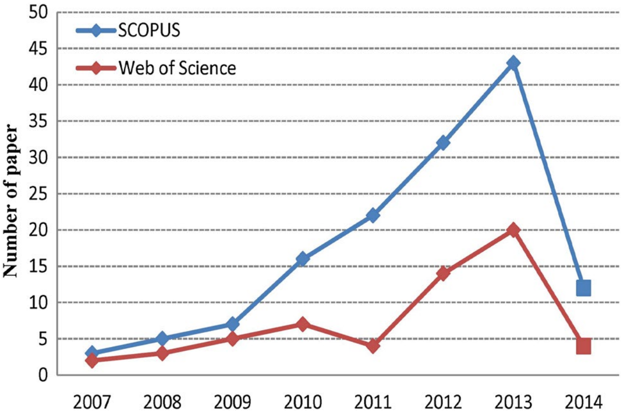


Fig. 3 Copy-move forgery detection publication indexed by Web of Science and SCOPUS

was darkened to make the image incite racial sentiments. However, during the same week, an unchanged photograph of Simpson appeared on a Newsweek cover [67].

Figure 5 shows an obvious example of crime scene image forgery. The copy-move procedure was applied on the original image, as shown in the left side, and the forged image on the right side was created by copying a part of the floor and pasting it on the blood to cover it [64].

Figure 6 illustrates another example of copy-move forgery detection [4]. In this forgery, a car has been copied and pasted to another part of the image. Forged image in Fig. 6b is tested to detect duplicated areas, and Fig. 6c shows the detection result which illustrates which areas has been copied and duplicated areas connected together with lines.

In copy-move forgery, most images undergo some image processing operations, such as the addition of Gaussian noise, rotation, resizing, or scaling. These image processing operations are categorized into two parts. The first type provides a type of spatial harmonization between the copied region and its neighbours, such as rotation or scaling.

The second type focuses on post-processing operations, such as JPEG compression or blurring [60, 81]. Rotation is when the copied area is rotates into various angles from 5 to

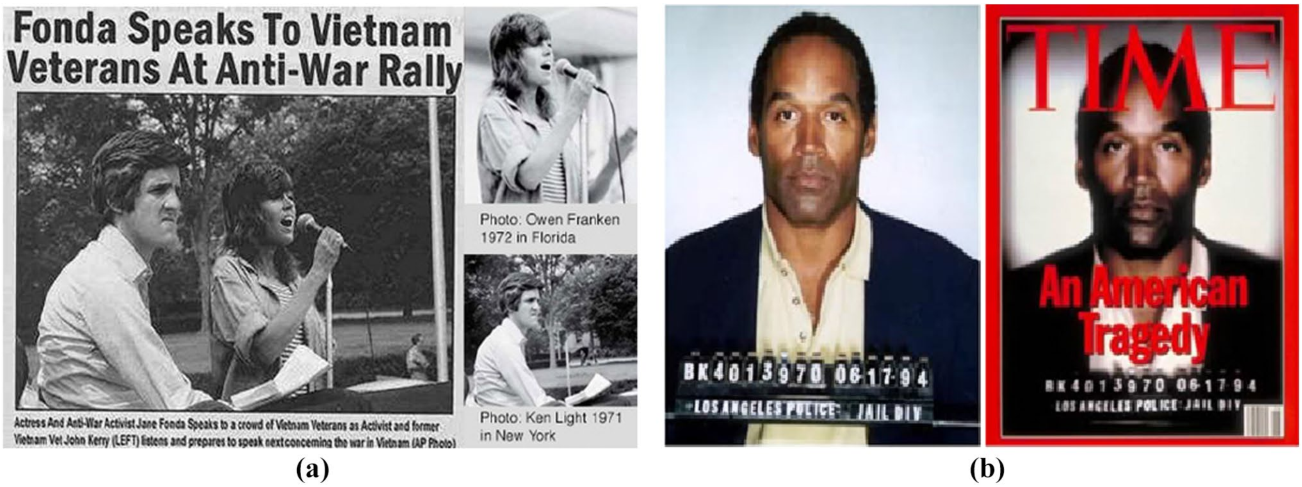
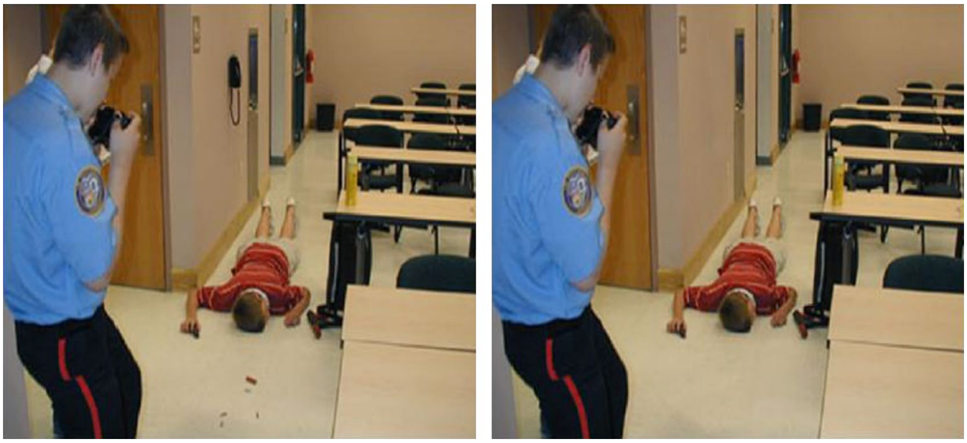

Fonda Speaks To Vietnam Veterans At Anti-War Rally
Actress And Anti-War Activist Jane Fonda Speaks to a crowd of Vietnam Veterans as Activist and former Vietnam Vet John Kerry (LEFT) listens and prepares to speak next concerning the war in Vietnam (AP Photo)
Photo: Owen Franken 1972 in Florida
Photo: Ken Light 1971 in New York
BK 4013970 061794
LOS ANGELES POLICE JAIL DIV
TIME
An American Tragedy
BK 4013970 061794
LOS ANGELES POLICE JAIL DIV
(a)
(b)

Fig. 4 **a** Image splicing forgery, **b** image retouching forgery

Fig. 5 Copy-move crime scene image forgery



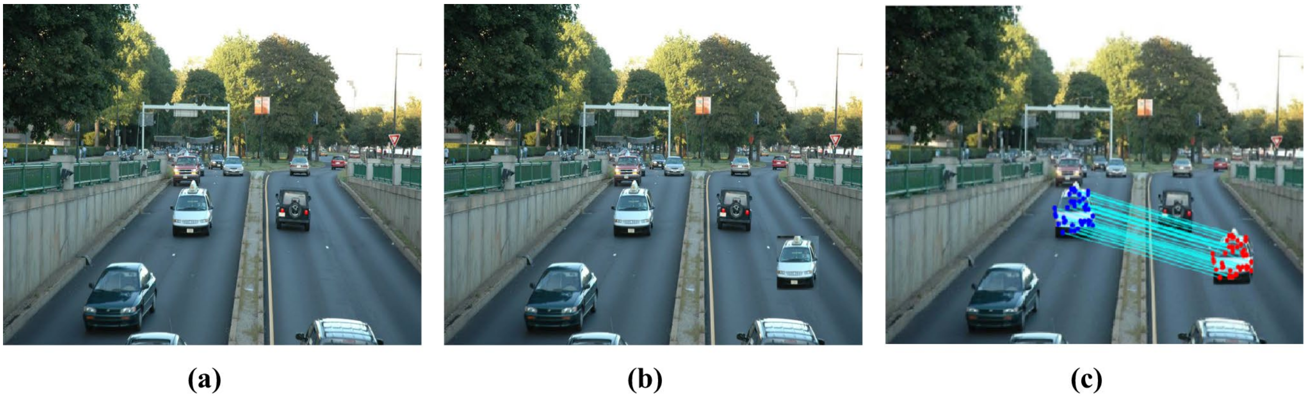


Fig. 6 Digital image forgery detection. **a** Original image, **b** tampered image, **c** detection result

360, before it is pasted to another part of the image. Scaling is a linear transformation that increases or decreases object by a scale factor that is the same in all directions. Gaussian noise is statistical noise that uses the probability density function for the normal distribution. The amount of noise is consistent across the entire original image; by adding noise to the image, it causes inconsistencies in the noise present in the image [1, 65].

JPEG compression is a method generally used for lossy data compression in digital images. The degree of compression, which is the quality factor, can be adjusted. Storage size and image quality are traded off within a range from 5 to 100. When an image is compressed using JPEG, it uses a lossy form of compression file based on a discrete cosine transform (DCT). And it will affect image quality because some original image information is lost and cannot be restored [96].

2.1 Copy-move forgery detection techniques

Copy-move is the most common technique for tampering with images because of its effectiveness. Currently, numerous copy-move forgery detection methods are available; these methods focus on increasing the detection rate and on being robust to any transformations, such as blur filtering, Gaussian noise, or rotation [73, 86]. The main steps in copy-move forgery detection are: feature extraction, similarity checking, and matched pair connection and outlier removal. Feature extraction varies in each method. Generally, they can be classified to two main criteria:

1. Block generation methods [5, 36, 51, 73, 76].
2. Keypoint-based methods [4, 42, 52, 86, 87].

In the matching step, different approaches are used; one such approach is lexicographic sorting, which is used in most block generation methods [10, 20, 33, 36, 46, 50, 98]. In keypoint-based methods, Best-Bin-First is used to find similar keypoints [42]. Connecting match points is the last step in forgery detection. Some authors use morphological operations [50, 94, 98], and some applied thresholds to assign match points if the detected area has at least a minimum number of points [94].

By growing the popularity of copy-move forgery in recent years, different papers published to detect copy-move forgery. Hence, it has put considerable need on realizing the problems and advantages of existing methods, a survey paper published to analysis the current methods, but only few methods have been evaluated [85]. The goal of this paper is to determine which methods for detecting copy-move are best under different image attributes, such as JPEG compression, scaling, rotation. The advantages and drawbacks of each method are also highlighted. The remainder of the paper is organized as follows: Sect. 3 reviews the principle of copy-move forgery detection and gives brief summaries and closing remarks. The conclusion is given in Sect. 4.

2.1.1 Block generation methods

The first stage in block generation methods is to segment digital images into same size overlapping blocks. The size of the block is vary for different methods; if the size of block is $c \times c$, then each image has $(M - c + 1) \times (N - c + 1)$ blocks, where M and N represent image size. The second step is to compute feature vectors of each sub-block, which could be done using different methods such as singular value decomposition, Fourier transform, and DCT. Finally, similar feature vectors are sorted and subsequently matched and the location of tampered area identified. Most of the proposed techniques use lexicographic sorting to classify similar feature vectors. The general procedure of forgery detection is illustrated in Fig. 7.

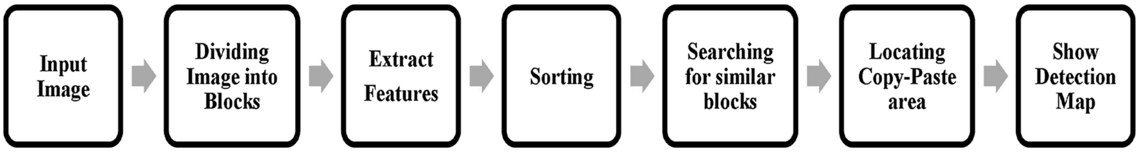


Fig. 7 Block generation forgery detection general procedure

Most of these methods present blocks in a concise way to decrease computational complexity and improve robustness. However, detection time is high because it takes long time for features to be extracted from millions of blocks and then sorted. Block generation methods can be categorized into six groups:

1. Frequency domain-based features [14, 36]
2. Dimensionality reduction-based [49]
3. Moment-based [60, 64, 81]
4. Intensity-based [5, 93]
5. Transform domain [7]
6. Radix Sort [57].

For instance, various image and video processing techniques apply the DCT to convert an image to the frequency domain. Fridrich et al. [36] used 256 coefficients of the discrete cosine transform as features. However, Bayram et al. [14] used FourierMellin Transform (FMT) to generate feature vectors. A method based on dimensionality reduction is achieved by applying wavelet transform, such as singular value decomposition [49] or detection based on DWT and SVD [51], on the image. Next, similar blocks are identified using an exhaustive search. Mahdian and Saic proposed one of the current moment-based methods according to blur moment invariants [64]. Two feature vectors are considered matched if their Euclidean distance is below a certain threshold and if the neighbourhood around their spatial locations consists of similar features. Wang et al. proposed an intensity-based forgery detection method using models using round blocks. It uses the mean intensities of circles with different radii around the block centre [93].

Frequency domain-based features Copy-move forgery is used to manipulate digital images by cloning a part of the image to fulfil illegal purposes. Fridrich *et al.* [36] suggested one of the barest and earliest block generation methods for detecting copy-move forgery. They believed that original image parts and pasted ones contain similarities. These similarities can be used to successfully detect copy-move forgery. Given that the forged image will probably be saved in the JPEG format, the image segments may match approximately rather than exactly. As a result, they discovered that the detection algorithm has some requirements, which are:

1. The algorithm should allow for an approximate match between small image sections.
2. When false positives are a possibility, the algorithm should work for a reasonable amount of time.
3. Duplicated parts in the image should be a connected components rather than a set of single pixels.

However, this approach is computationally very costly and would take $MN\log2\ (MN)$ steps for an image that is sized $M \times N$. Moreover, it might not work if the original part is modified, such as through blurring or scaling. In addition, it could only detect duplicated regions where a large portion of the image has been tampered. This method is not appropriate because it uses exhaustive search, which is not very efficient when post-processing is applied to the copied part. The main computational cost of this algorithm is due to sorting because exhaustive searches are very time consuming [85].

We proposed a block generation method based on Fourier transform [83]. Detection starts by converting the image to grayscale image, and converted image is divided to same size blocks, and then Fourier transform is applied on image to extract features of each blocks. When Fourier transform of the image is calculated, a function is created with the intensity signal across the image, and function is decomposed into a sum of orthogonal basis functions by using Fourier transform.

Fourier transform is applied on the image blocks to perform correlation, and subsequently the correlation of the blocks is computed to locate features within image. Then, correlation is sorted in a lexicographically order because it can make matching more effective. After all blocks sorted properly, the algorithm continues into the matching step by testing each pair of blocks whether they are matching. When similar blocks detected, then the inverse of a transform is performed on a transformed image to produce the original image. Detection time of proposed method enhanced compared to [64]. Detection time for a 256 × 256 grayscale image reduced from 60 to 8 s compared to Kangs method.

Bayram et al. [14] proposed a copy-move detector based on applying FMT on the blocks in the image. The FMT is invariant with respect to blurring, scale, noise, and rotation. However, it works only with rotation angles of 0°, 5°, and 10° and slightly resized and copied regions. This method is robust in case the rotation is only slight because extracted features based on FMT are not rotational invariant theoretically.

Najah et al. [72] proposed an efficient non-intrusive method based on using dyadic wavelet transform. Same as other block generation methods, image is divided into sub-blocks, and then by using a noise pattern of each sub-block, a separate noise image is generated. To approximate the noise of the image and to guess the noise pattern of different blocks, generated noise images are used. At the end, blocks with similar noise histograms are suspicious to be in copy-move areas. This technique can divide an image into complete objects more precisely compared to earlier techniques. However, it is not working on various images. It can only detect forgeries if the image is not complex.

Detection based on Discrete Cosine Transform (DCT) was proposed by [43]. In this method, the method by Fridrichs based on DCT was improved by minimizing the false matching rate. This method compares image sub-block features and determines whether the number of matched blocks in a specific area is more than a defined threshold. To enhance matching accuracy, they have proposed a lexicographical sorting algorithm based on distance. This DCT-based method is not robust to rotation, but it is robust to noise addition and blurring [41].

Li et al. [51] presented a copy-move forgery detection method based on wavelet transform and singular value decomposition (SVD). DWT is applied to the image. Afterwards, SVD is applied on image blocks of the low-frequency element in the wavelet sub-band to generate a brief dimension sign. Then, the singular value features are lexicographically sorted to determine tampered image blocks. Duplicated areas are detected through lexicographically sorting over all image block features and finding similar blocks.

This proposed method reduces computational difficulty and localizes duplicated areas even when the image is compressed. Moreover, the disadvantage of this method is its high computation time, which is due to using lexicographically sorting on the entire image to find similar blocks. The other problem is that it is ineffective when used on highly textured images and on smooth regions in the image.

The authors in [40] proposed a copy-move detection algorithm by using phase correlation within an image. The advantage of this method is its low computational complexity. It is also able to detect small tampered areas because it uses a larger overlap ratio. Phase correlation is computed to obtain the typical distribution that is applied to produce a pulse diagram. Subsequently, the spatial offset between the copied and the pasted portions is estimated according to the pulse position. Thus, the forged area can be located quickly. Detection based on phase correlation is able to detect small areas; however, if the image contains multiple forged regions, it cannot detect copy-move areas; this disadvantage is critical.

The authors in [22] proposed a method where blocks represented DCT. This method is robust to multiple copy-move forgeries, and its computational complexity is smaller than similar existing methods [36, 43, 76] because the dimension of feature vectors is reduced. It works similar to other block generation methods.

At the first stage, the image is divided into blocks of the same size. Then, DCT is applied to each block to generate quantized coefficients. Subsequently, each cosine-transformed block is represented by a round block, to be used to extract valuable features from each block. To be able to have a good detection rate, these extracted features should be robust. Finally, lexicographically sorting is used to sort feature vectors and search for similar blocks. Consequently, similar image blocks will be matched according to a pre defined threshold value.

Dimensionality reduction-based A different approach for copy-move detection is presented in [49] based on SVD. Detection is easy even when the attacker manipulates the photograph further, such as through rotation or additional noise. It also works well for JPEG compression. Detection based on SVD begins by applying SVD on each overlapping block by using:

$$A = USV^{\mathrm{T}} \tag{1}$$

where A is an image matrix, U and V are orthogonal matrixes, and S is a diagonal matrix $(m \times n)$ with singular values (SV) on the diagonal. According to SVD, singular values are extracted and ordered in a matrix. Then, features in each block must be sorted into a k–d tree and similar blocks for each query must be searched using (2). In this formula, u and v values are n-dimensional feature vectors, and D(UV) is the Euclidean distance between these vectors.

$$D(UV) = \left(\sum_{i=1}^{r} (U_i - V_i)^2 \right)^{\frac{1}{2}} \tag{2}$$

Then, matching the similarity of blocks continues to detecting similar blocks. It defines a duplicated area contains many neighbouring copied blocks. Two blocks are suspected as similar if they can be found in the tested space, the similarity of their neighbourhoods to each other is high. Finally, the location of similar blocks and their neighbours confirmed as tampered area.

Their experimental results illustrate its robustness against post-processing operations because singular values are robustness against algebraic and geometric invariance, rotation, scaling, noise, and blurring. For a 256 × 256 colour image, the detection time for this method is 120 s, which is better compared to the method in [64]. It has lower computational time and robustness to noise, unlike the methods in [36, 62, 64, 76].

Authors in [31] presented an efficient block generation forgery detection using multiresolution local binary patterns (MLBP). Image is divided into overlapping blocks and feature vectors extracted using LBP operators for each block. Then, the feature vectors are sorted lexicographically. For reducing detection time, authors used *k–d* tree to determine duplicated blocks in the image, and for eliminating possible false matches, RANSAC algorithm was used. Based on their experimental results, their method is robust to geometric distortions and illumination variations and it can detect duplicated areas even under different post-processing operations such as JPEG compression, rotation or noise. The drawback of this method is its weakness to detect duplicated regions with arbitrary rotation angles.

Moment-based Liu et al. [60] proposed a passive image authentication method that is able to detect duplicated area under rotation. It uses round blocks and Hu moments to find forged areas. In this method, the image is decomposed using a Gaussian pyramid and created sub-images. Low-frequency sub-images are chosen to solve the possible distortion caused by noise contamination and JPEG compression.

Subsequently, each sub-image is divided into many overlapping round blocks. From these blocks, Hu moment features are extracted and used to match features. Finally, forged areas are located by the comparison of shift vectors and copy-paste areas. This method mainly concerns post-processing, such as rotation, blurring, JPEG compression, and noise. However, it is not robust to resizing or cropping images before it is pasted to another area. It has low computational complexity and good accuracy because of its reliance on fewer selected features.

Ryu et al. [81] proposed detection based on Zernike moments. Zernike moments are used to extract the feature vectors of an image block. Then, features are sorted lexicographically and adjacent vectors are located. This method works well in terms of robustness to noise and rotation because Zernike moments are algebraically invariant against rotation, noise, and information content. However, it is weak against other transformations, such as scaling or JPEG compression.

Intensity-based Ardizzone et al. [5] proposed detection of copy-move forgery via texture description. In this method, the authors compared several texture descriptors, using a standard block generation approach to find out which is best for the copy-move forgery detection problem. The inspected descriptors are: statistical, Edge Histogram, Tamura, Gabor, and Haralick. Based on their experiment, the best descriptor is the simplest one which is statically, in terms of precision vs. execution time, but none of them is robust against geometrical transformations.

The authors in [93] used a model with round blocks to detect duplicated areas. The authors improved its detection rate in [36, 76] using round blocks instead of square blocks. The main problem with using square blocks is: when the copy region is rotated or scaled, the method for selecting square blocks fails. Thus, the circle region is used as features to solve the rotation and scale problem in their proposed method. Detection begins by reducing the image dimension by Gaussian pyramid, and four features are accepted for each circle block. Euclidian distance was calculated to compare similarity between two feature vectors. This method is robust to post-processing operations as well as to JPEG compression and the addition of Gaussian white noise. Using Gaussian pyramid, decomposition reduces computational time. Thus, the dimension of the search space is reduced to 1/4 of its original value.

Table 1 shows the computation complexity of their method compared to previous methods [93]. Number of blocks in the table indicates the computational time reduced with lower number of blocks. The size of images for testing is 512 × 512.

Transform domain Ardizzone and Mazzola [7] proposed a copy-move detection method that uses Bit-Plane Analysis. In this method, the image is analysed in the bit-plane domain. For each bit-plane, blocks of bits are encrypted using ASCII code, and the direction of strings is tested rather than the original bit-plane. The cycle is classed, and same groups of bits are removed as suspect regions, which are then transferred to the following plane to be processed. The output of the previous planes shows where the image is altered. Its advantage is detection time which is not excessive. However, Bit-Plane Analysis does not work with JPEG images because bit-plane representation and JPEG compression are not related. It is also not robust to rotation or scale [7].

Radix sort Lin et al. [59] proposed a method using radix sort. It works in a similar manner as other block generation methods. It divides the image into similar-sized blocks, and the features of each block are extracted. Finally, these

Table 1 Computation complexity comparisons

Methods	Extraction domain	Number of blocks	Feature dimension
Fridrich et al. [36]	DCT	255,025	64
Popescu et al. [76]	PCA	255,025	32
Huang et al. [62]	Spatial domain	247,009	5
Wang et al. [93]	Low-frequency part	62,001	4

features are sorted using radix sort. Afterwards, for every pair of adjacent vectors, the differences between vectors are computed by sorting a list. Authors proposed the use of radix sort rather than lexicographic sorting to enhance time complexity. They also enhanced the capability of resisting various forgery methods, such as Gaussian noise and JPEG compression. However, it does not deal with rotation arbitrary angles, and copied regions that were small in size were not successfully detected.

2.1.2 Keypoint-based methods

Keypoint-based methods are completely different from block generation methods. Features in these methods are computed only on image itself without any division, and extracted features vectors per keypoint are compared with each other to find similar keypoints. Finally, forgery is detected if areas of such matches gather into larger areas. The advantage of keypoint-based methods is its computational complexity which is low compared to block generation methods because of its lower post-processing threshold. These methods do not work properly when the source area of the copy-move tampering is homogenous, as no keypoints can be extracted in that area and no matching can be done.

Two well-known keypoint-based feature extractions are scale-invariant feature transform (SIFT) [4, 42, 52, 86] and speeded up robust features (SURF) [87]. SIFT and SURF, as local visual features, have been commonly used for object recognition and image retrieval. Due to their robustness to many geometrical transformations, they have been used in digital forensics as well.

SIFT extraction is used in different criteria, such as shoeprint image retrieval [89], fingerprint detection [88], and in copy-move detection algorithms [3, 75]. In these methods, the best-bin-first search method and k–d tree are used to find nearest neighbours efficiently. Compared to lexicographic sorting in block generation methods, it has better matching results. However, it requires more memory compared to lexicographic sorting [26]. Euclidean distance is also used as a matching measure in most keypoint-based methods. The general procedure of forgery detection in keypoint-based methods is shown in Fig. 8.

SURF is a feature detector based on a Hessian matrix, which uses simple approximation [68]. It depends on integral images to decrease the computation time, because integral images permit the computation of rectangular box filters in constant time. The SURF descriptors refer to the allocation of Haar-wavelet responses within the interest point area. Furthermore, only 64 dimensions are utilized to decrease the time for feature extraction and matching, and concurrently increasing the systems robustness [12].

Different methods based on SIFT and SURF are proposed to detect forgery. Hailing Huang et al. [42] proposed the first method based on SIFT. Only the feature-matching SIFT algorithm is used to detect duplicated regions in the image using best-bin-first nearest neighbour identification. This method has good performance on various kinds of post image processing such as scaling and rotation. However, it is unable to detect tampered regions that are small in size.

Another method presented in [86] is based on SIFT and Grey Level. The detection procedure starts by extracting SIFT keypoints and establishing SIFT feature vectors for every keypoint. Then for locating a feature vector, the grey level feature is extracted and mixed with SIFT features. Finally, the extracted feature vectors are matched with every two different keypoints and location of duplicated area detected. The advantage of this method is its robustness to Gaussian blur and its false match rate is reduced, and one of the primary drawbacks is high time complexity because SIFT and grey level features must be extracted.

The authors improved detection rates by creating a new grey level because the image will change a little when changes are applied to the grey levels. Thus, the new grey level should be created again. The features matching process starts by normalization of SIFT feature vectors because it can decrease the impact of uneven illumination. Based on their results, this method has high time complexity, but they decreased the false matching rate [86].

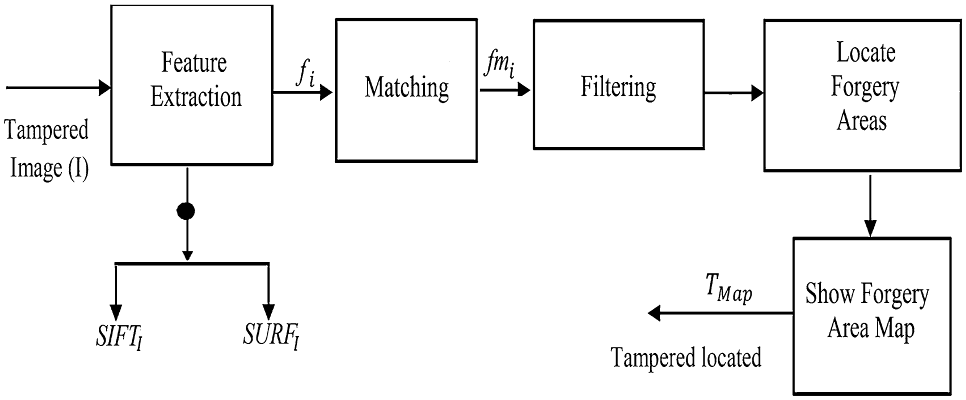


Fig. 8 General procedure of forgery detection in keypoint-based methods

Hussain et al. [44] proposed a detection method based on multiresolution Weber law descriptors (WLD). This method is able to extract features from chrominance components and provide information that human eyes cannot see. For classification points, they used a support vector machine. The important advantage of this method is its ability to reach a WLD descriptor with up to 91% multi-resolution on the hue space of the images. It is also robust to noise and illumination with capability of edge detection. Naked eyes are less sensitive to hue component rather than brightness. Thus, even though forged images appear normal, several altered traces remain in hue channels. Thus, detection starts by converting the input colour image into the YCbCr colour mode using $\mathrm{Y} = 0.299\mathrm{R} + 0.587\mathrm{G} + 0.114\mathrm{B}, \mathrm{Cr} = 0.701\mathrm{R} - 0.587\mathrm{G} -0.114\mathrm{B}, \mathrm{Cb} = -0.299\mathrm{R} - 0.587\mathrm{G} + 0.886\mathrm{B}$.

The YCbCr colour mode is used because it stores colour according to brightness and hue. These components are used to extract image features because they are more sensitive for detecting forgery areas in forged images. To extract features from the image, a multi-resolution WLD, a texture descriptor is used. For tamper detection, a machine learning technique (SVM) that includes training and testing stages is used [26].

The proposed method was evaluated based on specificity, sensitivity, and accuracy. Sensitivity measures the classification accuracy of true cases to determine if the input image is authenticated or forged. It is measured using the following formula: $(100 \times \mathrm{TP}/(\mathrm{TP} + \mathrm{FN}))$. Specificity measures the classification accuracy of false cases and is computed using $(100 \times \mathrm{TN}/(\mathrm{FP} + \mathrm{TN}))$. Percentage accuracy is the percentage ratio among properly classified images over the total number of images and is calculated as:

$$\text{Accuracy} = 100 \times (\mathrm{TP} + \mathrm{TN})/(\mathrm{TP} + \mathrm{TN} + \mathrm{FN} + \mathrm{FP}) \quad (3)$$

where TP (true positive) is the number of forged images that are detected as forged, FN (false negative) is the number of forged images detected as original images. FP (false positive) is the number of original images detected as forged images, and TN (true negative) is the number of original images that are exactly detected as original images. The authors concluded that hue components are very accurate in comparison with brightness and grey image.

The method based on Webers law descriptors is better compared to the method in [95] because hue components and SVM are used in this method. Moreover, they use edge information to extract feature vectors, which are derived by using a filter on the image hue components. The detection result shows that the proposed method detection rate is 91%, which is an increase of 33.9% compared to previous methods.

Amerini et al. [4] proposed a novel method based on SIFT, which is able to detect copy-move forgery and image splicing. It has high reliability when detecting forged images and is capable of detecting and estimating geometric transformations, such as scaling factors or rotation angles. This detection procedure has four principal steps: SIFT feature extraction, keypoint matching, keypoint clustering, and geometric transformation estimation. After the SIFT feature was extracted to match the keypoints, the g2NN test was used to generate a 2NN test. The 2NN test is the first matching procedure for clarifying whether the distance value of the candidate match with respect to the second nearest neighbour is lower than the particular threshold. It is calculated by:

$$\frac{d_1}{d_2} < T \quad (4)$$

where d_1 and d_2 are Euclidean distances with respect to the other descriptors, and T is the threshold $\in (0,1)$. The 2NN test has a drawback: it is unable to detect multiple keypoint matching. To overcome this problem, the authors proposed generalizing the 2NN test. The g2NN generates the 2NN test to clarify the matching whether the distance value of the candidate match with respect to the second nearest neighbour is higher than the particular threshold. The g2NN test is capable of detecting multiple copies, which is computed using:

$$\frac{d_i}{d_i + 1} > T \quad (5)$$

where d is Euclidean distances in the range $(d_1, \ldots, d_k)$. Moreover, k is considered a match. Inspected keypoints in the range of $1 \le k < n$. $d_1, \ldots, d_k$ are Euclidean distances with respect to the other descriptors, and T is the threshold, which is defined as 0.5 in this method. In the clustering stage, keypoints classified using an agglomerative hierarchical tree cluster and a matrix of Euclidean distance is created between each point coordinates. And for the linkage method, weighted centre of mass distance is used. This method performed excellently in terms of having a high true positive (TPR) ratio and a low false positive ratio (FPR). The results in Table 2 illustrate that the SIFT-based method improves upon the methods by Fridrich et al. [36] and Popescu et al. [76] in terms of computational time, TPR, and FPR [4].

Unlike other SIFT-based methods, Bharamagoudar et al. proposed a detection method based on SIFT which is dividing image to overlapping blocks and using Color

Table 2 Performance evaluation of method in [4] with similar methods

Method	FPR (%)	TPR (%)	Time (s)
Fridrich et al. [36]	84	89	294.69
Popescu et al. [76]	86	87	70.97
Amerini et al. [4]	8	100	4.94

Coherence Vector (CCV) as feature extraction method. Searching for similar regions is like block generation method. They have used lexicographically sorting to find similar blocks [16]. Then, image is rotated to the desired angel, and then it will ask the user to crop the suspected regions and remove them from original image. Then, SIFT is applied on the rotated image and features of the image are extracted and the extracted keypoints are compared with the first image to identify which part of the image is tampered. By combining block generation method with SIFT, this method is very time consuming.

Chihaoui et al. proposed a new detection method based on SIFT and Singular Value Decomposition (SVD). SIFT is used to extract image descriptors, and in matching phase SVD is used to identify matched regions. Equation (6) describes the similarity matrix calculation [25].

$$A_{i}j = \sqrt{\sum\nolimits_{ij}^{n}(D_i - D_j)^2} \tag{6}$$

where D_i, D_j are two different descriptors vectors. Two selected vectors are matched if A_{ij} is the minimum along rows and columns at the same time. The main drawback of this method is its limitation for big size images: if the number of features extracted from the image is more than 3000, then it is not possible to authenticate and locate tampered areas.

SURF is another keypoint-based method that is used to extract features in copy-move forgery detection methods. Bo et al. [17] proposed a SURF-based method that can detect matched keypoints. This method is robust to rotation and scaling with high computation time. Quantitative measures were not included in their results and only visual results shown.

Detection speed is important independently of the detection goal. Lin and Wu presented a splicing and copy-move forgery detection method based on SURF and DCT [58]. Detection was performed by analysis of the dual compression effect in the DCT and spatial domain. Then, SURF descriptor used to extract features descriptor to make it robust to scaling and rotation. This method is able to localize duplicated areas, but detection time is high. Table 3 illustrates their experimental results in terms of detection.

Table 3 Detection method based on SURF and DCT experimental result

Image resolution	Block size	Time (s)
2272 × 1704	109	235.4
512 × 384	99	279.31
1500 × 2100	99	227.7

Shivakumar et al. [87] proposed a technique based on SURF that is used to extract image features. Then, keypoint matching is accomplished by filtering a base according to a general pattern. This method is robust to noise, rotation, and scaling.

3 Comparison and discussion

An effort has been made to present different copy-move forgery techniques to enhance forgery detection methods. However, these enhancements are a long way from being excellent and have some disadvantages that must be eliminated to acquire efficient results. This survey of copy-move forgery detection methods was presented to help scientists investigate new concepts and give them new ideas for better detection results. Different methods were evaluated with various detection algorithms based on two main criteria: keypoint-based and block generation. Each of these categories has their own advantages and drawbacks.

Based on our proposed block generation method [83] and the advantages of keypoint-based methods presented in previous sections, keypoint-based methods perform better compared to block generation methods.

In block generation methods, the feature size can result in high memory use and the computation time depends on the size and complexity of feature set. For instance, Zernike, DWT, DCT, and SVD have high computational complexity and do not have viable accuracy rates. As discussed in previous sections, SVD [49]- and DCT [22]-based methods are only robust to noise. However, Zernike performs better compared to the other block generation methods because it requires less memory and the computational time is low. This method also works well in terms of robustness to noise and rotation because Zernike moments are algebraically invariant against rotation, noise, and information content. Therefore, based on its characteristics it is a good choice between block generation methods.

Results in [4, 42, 86, 87] show that keypoint-based methods have better performance compared to block generation methods. Computational time is reduced, and almost all of them are robust to transformations such as rotation and scaling. They are robust to all transformations and post-processing because features extracted using keypoints are robust to these kinds of manipulations. The authors in [41] improved the Fridrich method in [56] by reducing the false matching rate.

The issue of high computational complexity in [36, 52, 76] has been solved by authors in [22], which was similar to previous methods. Detection time for a 256 × 256 colour image improved in [49] compared to the proposed method in [64]. However, the computational time remained high compared to other methods. Their method improved forgery detection in case of forgery with uniform areas, such as when the sky or ocean is manipulated. Computational complexity is also lower, and noise robustness is increased compared to [36, 62, 64, 76]. In [64], detection time is high because lexicographical sorting has been used for sorting singular values feature vectors.

The detection rate in [44] is 91%, which is an increase of 33.9% compared to [95]. Multi-resolution WLD was used, which is a robust image texture descriptor with its extension to various scales. This method is capable of edge detection as well because it is robust to noise and illumination.

Detection based on SURF in [17] is robust to scaling, rotation, and noise blurring but the duplicated area, and its boundary should be automatically located. Authors in [93] improved the efficiency of methods in [36, 76] by reducing the amount of blocks used and feature dimension to narrow the block matching searching space. The proposed method in [51] improved detection time compared to methods in [36, 76] by reducing the number of blocks from 255,025 to 62,001. Feature dimension was also reduced to 8 from 64 and 32.

Keypoint-based techniques perform well in terms of memory utilization, robustness and computation time. In terms of memory utilization, although feature size and the number of extracted keypoints are large, they are less than the number of image blocks used in block generation methods. Thus, the detection procedure is very lightweight and it will reduce computation time which is very important factor for copy-move detection methods. In terms of robustness, keypoints extracted from the image are robust to image processing manipulations such as rotation, noise, scale and JPEG compression.

SIFT and SURF are two approaches for detection and extraction of local image features to find image keypoints and collect image features. They are remarkable because the features extracted by these methods are relatively invariant to changes in scaling, image noise and rotation.

A comprehensive research was done to compare these two feature extraction methods in terms of processing time, robustness to scale changes and image rotation. All the techniques were evaluated based on the same measurements, such as RANSAC, which is used to reject inconsistent matches. An evaluation was carried out on the same image dataset, which includes general deformations, such as rotation, scale changes, and illumination changes. Different evaluations are explained in order to verify the best method for feature extraction in terms of different criteria. To identify the computational cost of the methods, processing time is evaluated in [47], and different factors such as type and size of the images are evaluated.

The authors utilized the Graffiti dataset which consists of images of 300 × 240 pixels. They used the same parameters as used in the original papers [12, 61]. The detection time was computed for the processes of feature extraction and matching. Table 4 illustrates the result of the time evaluation, and the results show that SURF is faster than SIFT (however, it also finds the most matches) [47].

In terms of image rotation robustness, as it is illustrated in Fig. 9, SIFT has better performance as it can detect most matches with rotation remaining invariant.

In terms of scale robustness, another experiment evaluates the performance of these two methods. The results in Table 5 illustrates number of matches in case of scale attack. The results show that when the size of the scale is larger, SIFT and SURF have almost same performance, but in small scale size SIFT has better performance.

As results illustrated in Tables 4, 5 and Fig. 9, SURF is much faster compared to SIFT because it uses a Fast-Hessian detector, which is five times faster than DOG, used in SIFT. In case of robustness to rotation, the results show that SURF needs improvement if the degree of rotation is large. Based on the results, it is concluded that SIFT works

Table 4 Processing time comparison. The item named total time in the table is the time spent to find all the matches

Items	SIFT	SURF
Total matches	271	168
Total time (ms)	2.15378e+007	3362.86
10 matches time (ms)	2.14806e+007	3304.97

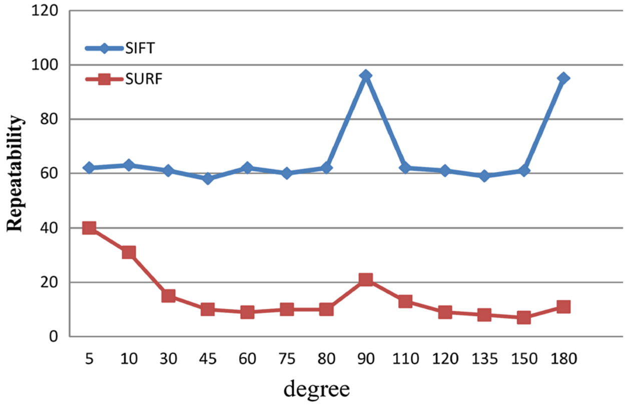


Fig. 9 Rotation comparison, data represents the repeatability of rotation

Table 5 Scale robustness comparison. Data show the total number of matches for each method

Data	SIFT	SURF
1–2	41	10
3–4	35	36
5–6	495	298
7–8	303	418

Table 6 Results of all experiments

Method	Time	Scale	Rotation
SIFT	Common	Best	Best
SURF	Best	Good	Common

very well in all cases except time, because it detects so many keypoints compared to SURF. Table 6 illustrates the results of all experiments [47].

SIFT as a widely used algorithm for feature extraction has better performance compared to other similar algorithms such as SURF. It is clearly obvious that SIFT is significant because of its desired properties, which are Invariant to scale change, rotation change, illumination change. And they are robust to addition of noise, substantial range of affine transformation.

Tables 7 and 8 show conducted comprehensive study on several copy-move detection methods from year 2005 to 2014 in terms of their characteristics.

Table 7 Comparison between the copy-move forgery detection methods

Method	Rotation	Scaling	JPEG compression	Noise	Detection rate (%)
SIFT [42]	√	√	N/A	√	N/A
Radix sort [56]	√	N/A	√	√	94–98
Stationary distribution of Markov chain [13]	√	√	N/A	N/A	65.40
SIFT [4]	√	√	√	√	99–100
Invariant moments [60]	√	×	√	√	N/A
Wavelets and log-polar mapping [73]	√	√	N/A	×	N/A
SVD [49]	×	×	×	√	N/A
Circle block [93]	√	N/A	√	√	N/A
Bit-plane analysis [7]	N/A	×	×	×	99.60
Dyadic wavelet transform [72]	√	√	√	N/A	81.18
DCT [43]	×	×	√	√	85
DCT [41]	×	N/A	N/A	√	98.2–100
Phase correlation [40]	√	√	N/A	N/A	80
DCT [22]	×	×	×	√	90
Block generation [62]	N/A	N/A	√	√	N/A
Feature matching [75]	√	√	√	√	89.95
Multi-resolution Weber law descriptors [44]	√	×	N/A	√	91
Counting bloom filters [55]	×	×	√	√	98
Harris corner points and step sector statistics [24]	√	√	√	√	92.15

Table 8 Comparison between the copy-move forgery detection methods

Method	Rotation	Scaling	JPEG compression	Noise	Detection rate (%)
DWT-PCA [101]	×	×	√	√	N/A
DWT [102]	90°, 180°, 270°	×	√	√	N/A
Log-polar [19]	√	√	×	×	98
DWT and SIFT [38]	√	√	N/A	×	88
Block generation [37]	√	√	√	×	N/A
SIFT and MHJ [84]	√	√	√	√	N/A
SURF [87]	√	√	N/A	√	N/A
Orthogonal wavelet transforms [48]	×	×	×	×	N/A

4 Conclusion

Nowadays, digital forensics is growing very fast and copy-move forgery is one of the new issues that are encountered widely in the field of digital image forensics. Therefore, having an excellent algorithm for authenticating digital images and locating duplicated areas in forged images is very important. Several researchers investigated different algorithms to propose a robust method that is able to detect copy-move forgery even under different transformations. We evaluated the performance of different proposed methods and presented the advantages and drawbacks of current methods. Their common steps were also explained. Almost all of these methods are able to authenticate the image and find duplicated areas without being affected by regular transformations, such as rotation, scale, or noise addition. Based on the categorization of all methods according to keypoint-based and block generation methods, the results show that keypoint-based methods are much better because their computational time is low and their detection performance is good. We believe that the presented results can support proposals for novel crossover-methods. One of the main drawbacks of existing copy-move forgery detection methods is that there is no way to find out the difference between copy-move forgery and retouching forgery such as artistic manipulation or red eye correction. We hope that a perfect copy-move forgery detection algorithm can be created in the future to cover all the weaknesses of current methods which is failure to resist to various post-processing operations. And will be able to detect the other two passive forgeries, which are image splicing and image retouching forgery.

Funding Funding was provided by Universiti Malaya (UM) (Grant No. RG312-14AFR).

References

1. Agarwal R (2012) Bit plane average filtering to remove Gaussian noise from high contrast images. In: 2012 international conference on computer communication and informatics (ICCCI). IEEE, Washington, pp 1–5
2. 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
3. Amerini I, Ballan L, Caldelli R, Del Bimbo A, Serra G (2010) Geometric tampering estimation by means of a sift-based forensic analysis. In: 2010 IEEE international conference on acoustics speech and signal processing (ICASSP). IEEE, Washington, pp 1702–1705
4. Amerini I, Ballan L, Caldelli R, Del Bimbo A, Serra G (2011) A sift-based forensic method for copy-move attack detection and transformation recovery. IEEE Trans Inf Forensics Secur 6(3):1099–1110
5. Ardizzone E, Bruno A, Mazzola G (2010) Copy-move forgery detection via texture description. In: Proceedings of the 2nd ACM workshop on multimedia in forensics, security and intelligence. ACM, New York, pp 59–64
6. Ardizzone E, Bruno A, Mazzola G (2010) Detecting multiple copies in tampered images. In: 2010 17th IEEE international conference on image processing (ICIP). IEEE, Washington, pp 2117–2120
7. Ardizzone E, Mazzola G (2009) Detection of duplicated regions in tampered digital images by bit-plane analysis. In: Image analysis and processing-ICIAP 2009. Springer, Berlin, pp 893–901
8. Barni M, Bartolini F (2004) Watermarking systems engineering: enabling digital assets security and other applications. CRC Press, Boca Raton
9. Barni M, Costanzo A (2012) A fuzzy approach to deal with uncertainty in image forensics. Signal Process Image Commun 27(9):998–1010
10. Bashar M, Noda K, Ohnishi, N, Mori, K (2010) Exploring duplicated regions in natural images. IEEE Trans Image Process 99
11. Battiato S, Farinella GM, Messina E, Puglisi G (2012) Robust image alignment for tampering detection. IEEE Trans Inf Forensics Secur 7(4):1105–1117
12. Bay H, Tuytelaars T, Van Gool L (2006) Surf: speeded up robust features. In: Computer vision-ECCV 2006, pp 404–417
13. Bayram S, Avcibas I, Sankur B, Memon N (2005) Image manipulation detection with binary similarity measures. In: Proceedings of 13th European signal processing conference, vol 1, pp 752–755
14. Bayram S., Sencar HT, Memon N (2009) An efficient and robust method for detecting copy-move forgery. In: IEEE international conference on acoustics, speech and signal processing, 2009. ICASSP 2009. IEEE, Washington, pp 1053–1056
15. Becker D (2013) The father of art photography. http://petapixel.com/2013/07/01/oscar-gustav-rejlander-1813-1875-the-father-of-art-photography/. Accessed Feb 2015
16. Bharamagoudar SR, Mudaraddi NV (2014) Forgery detection in image using CCV and SIFT. Int J Res Innov Eng Technol 1(02)
17. Bo X, Junwen W, Guangjie L, Yuewei D (2010) Image copy-move forgery detection based on surf. In: 2010 international conference on multimedia information networking and security (MINES). IEEE, Washington, pp 889–892
18. Böhme R, Freiling FC, Gloe T, Kirchner M (2009) Multimedia forensics is not computer forensics. In: Geradts ZJMH, Franke K, Veenman CJ (eds) Computational forensics. Springer, Berlin, pp 90–103
19. Bravo-Solorio S, Nandi AK (2011) Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics. Signal Process 91(8):1759–1770
20. Bravo-Solorio S, Nandi AK (2011) Exposing duplicated regions affected by reflection, rotation and scaling. In: 2011 IEEE international conference on acoustics, speech and signal processing (ICASSP). IEEE, Washington, pp 1880–1883
21. Caldelli R, Amerini I, Picchioni F, De Rosa A, Uccheddu F (2009) Multimedia forensic techniques for acquisition device identification and digital image authentication. In: Handbook of research on computational forensics, digital crime and investigation: methods and solutions, pp 130–154
22. 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):33–43
23. de Carvalho TJ, Riess C, Angelopoulou E, Pedrini H, de Rezende Rocha A (2013) Exposing digital image forgeries by

illumination color classification. IEEE Trans Inf Forensics Secur 8(7):1182–1194

24. 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
25. Chihaoui T, Bourouis S, Hamrouni K (2014) Copy-move image forgery detection based on sift descriptors and svd-matching. In: 2014 1st international conference on advanced technologies for signal and image processing (ATSIP). IEEE, Washington, pp 125–129
26. Christlein V, Riess C, Angelopoulou E (2010) A study on features for the detection of copy-move forgeries. Sicherheit 2010:105–116
27. Cox IJ, Miller ML, Bloom JA, Honsinger C (2002) Digital watermarking, vol 53. Springer, Berlin
28. Dadkhah S, Kppen M, Jalab HA, Sadeghi S, Manaf AA, Uliyan D (2017) Electromagnetismlike mechanism descriptor with fourier transform for a passive copy-move forgery detection in digital image forensics. In: Proceedings of the 6th international conference on pattern recognition applications and methods—Volume 1: ICPRAM, pp 612–619
29. Dadkhah S, Manaf AA, Hori Y, Hassanien AE, Sadeghi S (2014) An effective svd-based image tampering detection and self-recovery using active watermarking. Signal Process Image Commun 29(10):1197–1210
30. Dadkhah S, Manaf AA, Sadeghi S (2014) Efficient image authentication and tamper localization algorithm using active watermarking. In: Bio-inspiring cyber security and cloud services: trends and innovations. Springer, Berlin, pp 115–148
31. Davarzani R, Yaghmaie K, Mozaffari S, Tapak M (2013) Copy-move forgery detection using multiresolution local binary patterns. Forensic Sci Int 231(1):61–72
32. Dong J, Wang W, Tan T, Shi YQ (2009) Run-length and edge statistics based approach for image splicing detection. In: Kim HJ, Katzenbeisser S, Ho ATS (eds) Digital watermarking. Springer, Berlin, pp 76–87
33. Dybala B, Jennings B, Letscher D (2007) Detecting filtered cloning in digital images. In: Proceedings of the 9th workshop on multimedia and security. ACM, pp 43–50
34. Farid H (2008) Digital image forensics. Sci Am 298(6):66–71
35. Farid H (2009) Image forgery detection. IEEE Signal Process Mag 26(2):16–25
36. Fridrich AJ, Soukal BD, Lukáš AJ (2003) Detection of copy-move forgery in digital images. In: Proceedings of digital forensic research workshop. Citeseer
37. Gan Y, Zhong J (2014) Image copy-move tamper blind detection algorithm based on integrated feature vectors. J Chem Pharmaceut Res 6(6):1584–1590
38. Hashmi MF, Hambarde AR, Keskar AG (2013) Copy move forgery detection using dwt and sift features. In: 2013 13th international conference on intelligent systems design and applications (ISDA). IEEE, Washington, pp 188–193
39. He Z, Lu W, Sun W, Huang J (2012) Digital image splicing detection based on markov features in DCT and DWT domain. Pattern Recognit 45(12):4292–4299
40. Hou DM, Bai ZY, Liu SC (2012) A new algorithm for image copy-move forgery detection. Adv Mater Res 433:5930–5934
41. Hu J, Zhang H, Gao Q, Huang H (2011) An improved lexicographical sort algorithm of copy-move forgery detection. In: 2011 second international conference on networking and distributed computing (ICNDC). IEEE, Washington, pp 23–27
42. Huang H, Guo W, Zhang Y (2008) Detection of copy-move forgery in digital images using sift algorithm. In: Pacific-Asia workshop on computational intelligence and industrial application, 2008. PACIIA'08, vol 2. IEEE, Washington, pp 272–276
43. 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
44. Hussain M, Muhammad G, Saleh SQ, Mirza AM, Bebis G (2012) Copy-move image forgery detection using multi-resolution weber descriptors. In: 2012 eighth international conference on signal image technology and internet based systems (SITIS). IEEE, Washington, pp 395–401
45. Ibrahim RW, Moghaddasi Z, Jalab HA, Noor RM (2015) Fractional differential texture descriptors based on the machado entropy for image splicing detection. Entropy 17(7):4775–4785
46. Ju S, Zhou J, He K (2007) An authentication method for copy areas of images. In: Fourth international conference on image and graphics, 2007. ICIG 2007. IEEE, Washington, pp 303–306
47. Juan L, Gwun O (2009) A comparison of sift, PCA-SIFT and surf. Int J Image Process (IJIP) 3(4):143–152
48. Sarode TK, Vaswani N (2014) Copy-move forgery detection using orthogonal wavelet transforms. Int J Comput Appl 88(8):41–45
49. Kang XB, Wei SM (2008) Identifying tampered regions using singular value decomposition in digital image forensics. In: International conference on computer science and software engineering, 2008, vol 3. IEEE, Washington, pp 926–930
50. Langille A, Gong M (2006) An efficient match-based duplication detection algorithm. In: The 3rd Canadian conference on computer and robot vision, 2006. IEEE, p 64
51. Li G, Wu Q, Tu D, Sun S (2007) A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD. In: 2007 IEEE international conference on multimedia and expo, pp 1750–1753
52. Li S, Zhang A, Zheng Y, Zhu T, Jin B (2009) Detection of copy-move image forgeries based on sift. J PLA Univ Sci Technol (Nat Sci Ed) 10(4):339–343
53. Li Y (2013) Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching. Forensic Sci Int 224(1):59–67
54. Li Y, Wang H (2012) An efficient and robust method for detecting region duplication forgery based on non-parametric local transforms. In: 2012 5th international congress on image and signal processing (CISP). IEEE, Washington, pp 567–571
55. Lin HJ, Wang CW, Kao YT, Chen S (2009) An efficient method for copy-move forgery detection. In: WSEAS international conference. Proceedings. Mathematics and computers in science and engineering, vol 8. World Scientific and Engineering Academy and Society
56. Lin HJ, Wang CW, Kao YT et al (2009) Fast copy-move forgery detection. WSEAS Trans Signal Process 5(5):188–197
57. Lin SD, Huang YH et al (2009) An integrated watermarking technique with tamper detection and recovery. Int J Innov Comput Inf Control 5(11):4309–4316
58. Lin SD, Wu T (2011) An integrated technique for splicing and copy-move forgery image detection. In: 2011 4th international congress on image and signal processing (CISP), vol 2. IEEE, Washington, pp 1086–1090
59. Lin Z, He J, Tang X, Tang CK (2009) Fast, automatic and fine-grained tampered jpeg image detection via DCT coefficient analysis. Pattern Recognit 42(11):2492–2501
60. Liu G, Wang J, Lian S, Wang Z (2011) A passive image authentication scheme for detecting region–duplication forgery with rotation. J Netw Comput Appl 34(5):1557–1565
61. Lowe DG (2004) Distinctive image features from scale-invariant keypoints. Int J Comput Vis 60(2):91–110
62. Luo W, Huang J, Qiu G (2006) Robust detection of region–duplication forgery in digital image. In: 18th international conference on pattern recognition, 2006. ICPR 2006, vol 4. IEEE, Washington, pp 746–749

63. Lynch G, Shih FY, Liao HYM (2013) An efficient expanding block algorithm for image copy-move forgery detection. Inf Sci 239:253–265
64. Mahdian B, Saic S (2007) Detection of copy-move forgery using a method based on blur moment invariants. Forensic Sci Int 171(2):180–189
65. Mahdian B, Saic S (2009) Using noise inconsistencies for blind image forensics. Image Vis Comput 27(10):1497–1503
66. Mahdian B, Saic S (2010) A bibliography on blind methods for identifying image forgery. Signal Process Image Commun 25(6):389–399
67. Mediabistro (2009) News photos that took retouching. http://www.mediabistro.com/10000words/10-news-photos-that-took-photoshop-too_b328
68. Mikolajczyk K, Schmid C (2001) Indexing based on scale invariant interest points. In: Proceedings. Eighth IEEE international conference on computer vision, 2001. ICCV 2001, vol 1. IEEE, Washington, pp 525–531
69. Moghaddasi Z, Jalab HA, Md Noor R, Aghabozorgi S (2014) Improving RLRN image splicing detection with the use of PCA and kernel PCA. Sci World J 2014:10
70. Moghaddasi Z, Jalab HA, Noor RM (2015) A comparison study on svd-based features in different transforms for image splicing detection. In: 2015 IEEE international conference on consumer electronics-Taiwan (ICCE-TW). IEEE, Washington, pp 13–14
71. Muhammad G (2013) Alghathbar K (2013) Environment recognition for digital audio forensics using mpeg-7 and mel cepstral features. Int Arab J Inf Technol (IAJIT) 10(1):43–50
72. Muhammad N, Hussain M, Muhammad G, Bebis G (2011) Copy-move forgery detection using dyadic wavelet transform. In: 2011 eighth international conference on computer graphics, imaging and visualization (CGIV). IEEE, Washington, pp 103–108
73. Myrna A, Venkateshmurthy M, Patil C (2007) Detection of region duplication forgery in digital images using wavelets and log-polar mapping. In: International conference on conference on computational intelligence and multimedia applications, 2007, vol 3. IEEE, Washington, pp 371–377
74. Ng TT, Chang SF (2004) A model for image splicing. In: 2004 international conference on image processing, 2004. ICIP'04, vol 2. IEEE, Washington, pp 1169–1172
75. Pan X, Lyu S (2010) Region duplication detection using image feature matching. IEEE Trans Inf Forensics Secur 5(4):857–867
76. Popescu AC, Farid H (2004) Exposing digital forgeries by detecting duplicated image regions. Department of Computer Science, Dartmouth College, Tech. Rep. TR2004-515
77. Qureshi MA, Deriche M (2015) A bibliography of pixel-based blind image forgery detection techniques. Signal Process Image Commun 39:46–74
78. Reith M, Carr C, Gunsch G (2002) An examination of digital forensic models. Int J Digital Evid 1(3):1–12
79. Rocha A, Scheirer W, Boult T, Goldenstein S (2011) Vision of the unseen: current trends and challenges in digital image and video forensics. ACM Comput Surveys (CSUR) 43(4):26
80. Rogers M (2003) The role of criminal profiling in the computer forensics process. Comput Secur 22(4):292–298
81. Ryu SJ, Lee MJ, Lee HK (2010) Detection of copy-rotate-move forgery using Zernike moments. In: Böhme R, Fong PWL, Safavi-Naini R (eds) Information hiding. Springer, Berlin, pp 51–65
82. Saban (2013) Imgur image splicing forgery samples. http://imgur.com/gallery/lo7vP
83. Sadeghi S, Jalab HA, Dadkhah S (2012) Efficient copy-move forgery detection for digital images. World Acad Sci Eng Technol 71:543–546
84. Saleem M (2014) A key-point based robust algorithm for detecting cloning forgery. In: IEEE international conference on control system, computing and engineering (ICCSCE), vol 4. 2775–2779
85. Sencar H, Memon N (2008) Overview of state-of-the-art in digital image forensics. Algorithms Archit Inf Syst Secur 3:325–348
86. Shen XJ, Zhu Y, Lv YD, Chen HP (2013) Image copy-move forgery detection based on sift and gray level. Appl Mech Mater 263:3021–3024
87. Shivakumar B, Santhosh Baboo S (2011) Detection of region duplication forgery in digital images using surf. Int J Comput Sci Issues (IJCSI) 8(4):199–205
88. Shuai X, Zhang C, Hao P (2008) Fingerprint indexing based on composite set of reduced sift features. In: 19th international conference on pattern recognition, 2008. ICPR 2008. IEEE, Washington, pp 1–4
89. Su H, Crookes D, Bouridane A, Gueham M (2007) Local image features for shoeprint image retrieval. In: British machine vision conference
90. Su Y, Nie W, Zhang C (2011) A frame tampering detection algorithm for mpeg videos. In: 2011 6th IEEE Joint international information technology and artificial intelligence conference (ITAIC), vol 2. IEEE, Washington, pp 461–464
91. 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. Springer, Berlin, pp 577–583
92. Uliyan DM, Jalab HA, Abdul Wahab AW, Sadeghi S (2016) Image region duplication forgery detection based on angular radial partitioning and Harris key-points. Symmetry 8(7):62
93. Wang J, Liu G, Li H, Dai Y, Wang Z (2009) Detection of image region duplication forgery using model with circle block. In: International conference on multimedia information networking and security, 2009. MINES'09, vol 1. IEEE, Washington, pp 25–29
94. Wang JW, Liu GJ, Zhang Z, Dai Y, Wang Z (2009) Fast and robust forensics for image region-duplication forgery. Acta Autom Sin 35(12):1488–1495
95. Wang W, Dong J, Tan T (2010) Image tampering detection based on stationary distribution of Markov chain. In: 2010 17th IEEE international conference on image processing (ICIP). IEEE, Washington, pp 2101–2104
96. Yang ZC, Li ZH (2012) An anti-jpeg compression digital watermarking technology with an ability in detecting forgery region for color images. In: 2012 international conference on computer distributed control and intelligent environmental monitoring (CDCIEM). IEEE, Washington, pp 93–97
97. Zeng W, Yu H, Lin CY (2011) Multimedia security technologies for digital rights management, vol 18. Academic Press, London
98. Zhang J, Feng Z, Su Y (2008) A new approach for detecting copy-move forgery in digital images. In: 11th IEEE Singapore international conference on communication systems, 2008. ICCS 2008. IEEE, Washington, pp 362–366
99. Zhang Z, Ren Y, Ping XJ, He ZY, Zhang SZ (2008) A survey on passive-blind image forgery by doctor method detection. In: 2008 international conference on machine learning and cybernetics, vol 6. IEEE, Washington, pp 3463–3467
100. Zhang Z, Wang G, Bian Y, Yu Z (2010) A novel model for splicing detection. In: 2010 IEEE fifth international conference on bio-inspired computing: theories and applications (BIC-TA). IEEE, Washington, pp 962–965
101. Zimba M, Xingming S (2011) DWT-PCA (EVD) based copy-move image forgery detection. Int J Digital Content Technol Appl 5(1):251–258
102. Zimba M, Xingming S (2011) Fast and robust image cloning detection using block characteristics of DWT coefficients. JDCTA Int J Digital Content Technol Appl 5(7):359–367