Digital image forgery detection techniques: a survey

Article · December 2016

DOI: 10.19101/TIS.2017.25003

CITATIONS
5

READS
8,509

2 authors:

Shwetha B Basavarajappa
Jawaharlal Nehru National College of Engineering
2 PUBLICATIONS **7** CITATIONS
SEE PROFILE

S. V. Sathyanarayana
Jawaharlal Nehru National College of Engineering
29 PUBLICATIONS **170** CITATIONS
SEE PROFILE

Review Article

ACCENTS Transactions on Information Security, Vol 2(5)
ISSN (Online): 2455-7196
http://dx.doi.org/10.19101/TIS.2017.25003

Digital image forgery detection techniques: a survey

Shwetha B[1*] and S V Sathyanarayana[2]
Research Scholar, Department of Electronics and Communication Engineering Research Center JNNCE, Shimoga, Karnataka, India[1]
Professor, Department of Electronics and Communication Engineering, JNNCE, Shimoga[2]

Abstract
From the early days, images are being generally accepted as a proof of occurrence of the past events. The availability of low cost hardware and software tools makes easy to create and manipulate digital images with no obvious traces. With this consequence the Digital Image Forgeries are growing at an alarming rate in different application fields and have made negative marking to accept the integrity and authenticity of the digital images. Technology has been innovated to check the originality of the digital images. Researchers have proposed various techniques in this field in recent years. This survey attempts to cover the techniques that have been proposed for exposing digital image forgeries.

Keywords
Digital image forgery (DIF), Active and passive authentication, Copy move, Splicing, Source camera identification.

1.Introduction
Now days, images have become very useful in communication media. There is a belief that the image speaks more truth about the incident or the situation captured than the words. In the past, professional knowledge was required to manipulate the images generated by traditional film cameras with sophisticated dark-room equipment, which is difficult to do so for average users. The images are easy to acquire nowadays with the inexpensive devices. The process of recording, storing and sharing of large number of images is possible by everyone. With the era of digital images most of the image processing techniques have been proposed. In this context, the image editing software tools increased day by day leading to the forgery of digital images.

Images edited using the software tools are subjected to several processing stages and are so photorealistic that, the forgery in an image can never be detected by the human vision. As a consequence, the manipulated images are appearing at an increasing rate leading to the decrease of trust in the visual content. Hence, the authenticity of the image is not taken as granted. With the development of forgery tools, technology has been innovated to check the originality of the image information.

*Author for correspondence

So the research community has found an alternative way of authenticating the images and named it as digital image forensics. Forgery detection technique is one of the authentication methods, which assumes that the original image has some inherent patterns, which are introduced by the various imaging devices or processing. These patterns are always consistent in the original image and altered after some forgery operations. The image forgery detection has become complex, because of the advanced and sophisticated processing tools. In this view, researchers have proposed various techniques to detect the forgery in an image.

Existing techniques for Digital Image forgery can be broadly classified into two major domain categories [1]:

a. Active/ intrusive/non-blind method
Examples for active forgery methods are digital signature and watermarking. These methods have been proposed as means to authenticate the contents of digital images. These methods require certain digital information to be embedded with the original image, such as signature generation and watermark embedding when creating the images, which would limit their applications in practice.

b. Passive/ non-intrusive/ blind method
The original image has some inherent patterns, which are introduced by the various imaging devices or

processing. These patterns are always consistent in the original image and altered after some tampering operations. The original image is said to be forged when it is tampered. With the detection of the patterns, identification of the source of the digital image and its authenticity is obtained. Comparing it with prior active methods, this new technology does not need any extra information such as a watermark or a signature. Example forgery methods are copy-move, image splicing, Re-sampling and compression.
The remainder of this paper is organized as follows. Section 2 reviews the related literatures on active and passive image authentication techniques. The section also presents detailed study of works carried out so far in the field of passive technology for digital image forgery detection has been dealt. Section 3 deals with the comparison of digital image forgery detection techniques. Section 4 concludes the survey along with the future works that can be carried out in this research field.

2.Literature review

Digital image authentication or forgery detection techniques are broadly classified into two categories namely active and passive methods. The classification is based on whether the original image is available or not.

A. Active authentication

Number of tools exists to create or manipulate the digital image, so one can't easily trust on any digital document which is provided as legal evidences. Hence the authenticity of the image is to be checked. Image is said to be manipulated if the operation like scaling, rotating, blurring, brightness adjusting, change in contrast, etc. or combination of these operations are performed on an image. In active authentication techniques prior information about the image is indispensable to the process of authentication. It is concerned with data hiding where some code is embedded into the image at the time of generation. Verifying this code authenticates the originality of image. Active authentication methods are further classified into two types: digital signature and digital watermarking.

1) Digital signature: Digital signature is one among the active method used for detecting image forgery or tampering. Demonstrating the authenticity of digital document using a sort of mathematical scheme is called as digital signature. In digital signature a robust bits are extracted from the original image. An image is divided into blocks of 16*16 pixels. A secret key k is used to generate N random matrices with entries uniformly distributed in interval [0, 1]. A low pass filter is applied on each random matrix repeatedly to obtained N random smooth pattern [2]. System generate digital signature by applying signing process on digital image. Image Signing process contain following steps [3]:

1) Decompose the image using parameterized wavelet feature.
2) Extract the SDS
3) Cryptographically hash the extracted SDS, generate the crypto signature by the image senders private key.
4) Send the image and its associated crypto signature to the recipient.

Digital signature is simple and basic approach for digital image authentication.

2) Digital watermarking: Watermarking is also used for image forgery detection. Several watermarking techniques have been proposed. One uses a checksum schema in that it can add data into last most significant bit of pixels [4]. Others add a maximal length linear shift register sequence to the pixel data and then identify the watermark by computing the spatial cross-correlation function of the sequence and the watermarked image. These watermarks are designed to be invisible, or to blend in with natural camera or scanner noise. Visible watermarks also exist. In addition to this, a visually undetectable watermarking schema is also available which can detect the change in single pixels and it can locate where the change occur [4]. Embedding watermarks during creation of digital image it may limits its application where digital image generation mechanism have built-in watermarking capabilities. These active techniques have some limitation because they required some human intervention or specially equipped cameras. To overcome this problem a passive authentication has been proposed.

B. Passive authentication

Passive or blind forgery detection technique uses the received image only for assessing its authenticity or integrity, without any signature or watermark of the original image from the sender. It is based on the assumption that although digital forgeries may leave no visual clues of having been tampered with, they may highly disturb the underlying statistics property or image consistency of a natural scene image which introduces new artifacts resulting in various forms of inconsistencies. These inconsistencies can be used to detect the forgery. This technique is popular as it

does not need any prior information about the image. Existing techniques identify various traces of tampering and detect them separately with localization of tampered region. The Passive image authentication techniques are mainly classified into five groups [1]:

1. Pixel based techniques-involves the detection of forgeries at the pixel level.
2. Format based technique-involves the statistical correlation.
3. Camera based techniques-involves artifacts detection of camera components.
4. Physically based techniques - involves the detection of forgeries in the 3D interaction between the lights, objects and the camera.
5. Geometric based techniques-involves the detection of measurements of objects in the world and their positions relative to the camera.

The detailed survey of the related works regarding the passive authentication/passive forgery detection technique is as follows:

1) Pixel based techniques: Pixel based forgery detection techniques are broadly classified into three categories:

1. Copy move

Copy-move is the most popular and common photo tampering technique because of the ease with which it can be carried out. It involves copying of some region in an image and moving the same to some other region in the image. Since the copied region belong to the same image therefore the dynamic range and color remains compatible with the rest of the image [5]. Along with the copy move operation, image editing related operations such as rotation, color, scaling, blurring, compression and noise addition are added to the original image. This is done in order to make the forged part unnoticed to the human vision. The detection of some parameters like noise, color from the forged is not possible to differentiate. From the previous studies copy- move forgery can be classified as [6]:

a. Block based algorithms

In the block based methods surveyed till now, the input image is divided (segmented) into overlapping and regular image blocks. The tampered region is then obtained by matching the blocks of image pixels or transform coefficient.

The block based methods involve:

- Quantized Discrete Cosine Transform (DCT) coefficients of blocks matched to detect the tampered regions.
- Principal Component Analysis (PCA) to reduce the block feature dimensions.
- RGB color components and direction information as block features.
- Calculation of 24 blur invariant moments as block features.
- Fourier-Mellin Transform (FMT) for block feature calculation.
- Gray average results of each block and sub-blocks used as block features.
- Zernike moments for block feature.
- Information entropy used as block feature.

Apart from the above mentioned process the image feature calculation is also important to meet the rotation, scaling, compressions and time complexity improvements in image forgery detection. Hence the feature key-point based techniques were developed to achieve the accuracy even with the forgery subjected to rotation and scaling.

b. Feature key-point based

The feature key-point detection involves the following method

- SIFT- Scale invariant feature transform to extract host image feature transform to match for forgery or duplication detection.
- SURF- Speed up Robust Feature for feature extraction.

Although these feature results in locating matched key-points, they fail to locate the forgery. Fast and robust copy move forgery detection methods are developed with the combination of block based and feature based algorithms. Although these techniques can improve the computational complexity and detect the forgery accurately, they have a drawback of low recall rate because of the regularity in blocking methods.

In order to overcome this problem recent technique based on an adaptive over - segmentation and feature point matching was developed [6]. In this method segmentation of blocks are non-overlapping and irregular blocks called image blocks (IB). The recall rate was improved compared to the previous works because of the irregularity in the blocks.

2. Image splicing

Image splicing is a method of combining two or more im-ages to make it a composite (single) image. When images are spliced, resulting image shows lines, edges, regions and blur at the point where the images have been spliced. Development of the editing tools have made the lines, edges, regions and blur to merge in the image so that the human vision is not able to detect the forgery. Hence the image splicing detection has become one of the challenging topics for the researchers.

Steganography and Image Splicing have different approaches but still both the process create a new tampered image. Both the method makes an alteration in image smoothness, regularity, continuity and periodicity. Hence, statistical approaches are applied to detect these traces [7]. As steganalysis and Image Splicing detection make use of statistical approaches, some of the statistical natural models applied for steganalysis can be applied for Image Splicing detection.

Image splicing technique involves dimensional feature vectors. Four general methods applied for steganalysis were applied to image splicing detection with the accuracy of less than 80% [7].

The methods applied are:

- 72- Dimensional (72-D) feature vector composed of higher-order statistical moments of wavelet with the ac-curacy of 73.78%.
- 78-Dimensional (78D) feature vector- first three moments of characteristics and the prediction error applied for each four sub-bands in the three-level wavelet decomposition. This method has detection accuracy of 75.83%.
- 2-D Markov chain - for threshold prediction-error image. Features are extracted from three directions (horizontal, vertical, and main diagonal). The accuracy obtained is 76.25%.
- Singular Value Decomposition (SVD) - SVD based 50-Dimensional feature vector merged with Discrete Cosine Transform (DCT). This method has a detection accuracy of 78.82%.
- Combination of 1-D and 2-D - statistical moments of 1-D and 2-D characteristic functions extracted from the spatial domain and multi block discrete cosine transform (MB-DCT) are combined. This method provides an accuracy of 87.07%.

3. Image retouching

Image retouching is one more type of image forgery tool which is most commonly used for commercial and aesthetic applications. Retouching operation is carried out mostly to enhance or reduce the image features. Retouching is also done to create a convincing composite of two images which may require rotation, resizing or stretching of one of the image.

Image retouching detection is carried out by trying to find the blurring, enhancements, color changes and illumination changes in the forged image. Detection is easy if the original image is available. However, blind detection is a challenging task. For this type of forgery two type of modification is done either global or local [8]. Local modification is done usually in copy-move and in splicing forgery. Contrast enhancement that is carried out in case of retouching is done at global level and for detection of tampering these is investigated. For illumination and changes in contrast global modification is carried out.

In [9], a classifier is designed to measure distortion between the doctored and original image. The former may consist of many operations as change in blurring and brightness. Again the classifier performs well in case a number of operations are carried out on the image.

Algorithm in [10], describes a method that not only detect global enhancements but also suggests methods for histogram equalization. A similar model based on the probabilistic model of pixel values is detailed in [11] that approximate the detection of contrast enhancement. Histograms for entries that are most likely to occur with corresponding artifacts due to enhancement are identified. This technique provides very accurate results in case the enhancement is not standard. A number of enhancement and gamma correction localization algorithms are available that can easily detect the image modification and enhancement both globally and locally [10][12].

Authors in [8] Presents a technique that detects contrast changes making use of global modification by detecting positive or negative changes in the image based on Binary similarity measure and IQM. IQMs may provide substantial traces to detect the changes in the statistics. On the other hand, binary similarity measures features provide the differences. Appreciably accurate and effective results are produced in case image is highly modified.

Cao et al. [13] developed a method for detection of gamma correction for image forgery detection. Then technique is based on estimation of histogram characteristics that are calculated by patterns of the

peak gap features. These features are discriminated by the pre-computed histogram for the gamma correction detection in images. Results propose that this technique is very effective for both global and local gamma correction modifications.
In [14] a technique for detection of retouching is suggested based on the bi-Laplacian filtering .This technique looks for matching blocks on the basis of a KD tree for each block of the image. This technique works well on uncompressed images and compressed high-resolution images. Accuracy also depends on area of the tampered region for high-level compressed images.

Two novel algorithms were developed in [15] to detect the contrast enhancement involved manipulations in digital images. It focuses on the detection of global contrast enhancement applied to JPEG-compressed images. The histogram peak/gap artifacts incurred by the JPEG compression and pixel value mappings are analyzed theoretically, and distinguished by identifying the zero-height gap fingerprints. Another algorithm in same paper proposes to identify the composite image created by enforcing contrast adjustment on either one or both source regions. The positions of detected block wise peak/gap bins are clustered for recognizing the contrast enhancement mappings applied to different source regions. Both algorithms are very effective.

Techniques based on the photo-response non-uniformity (PRNU) that detect the absence of the camera PRNU, a sort of camera fingerprint, are explored in [16]. This algorithm detects image forgeries using sensor pattern noise. A Markov random field take decisions jointly on the whole image rather than individually for each pixel. This algorithm shows better performance and a wider practical application.

Number of methods have been proposed and discussed for retouching forgery. Limitation is that most of the methods work well if the image is greatly modified in comparison to the original image. Moreover, the human intervention required to interpret the result makes them non blind techniques.

2)Format based technique: Image alteration does not prove malicious tampering, as in the cases of color/contrast adjustment for image enhancement, and file format conversion for saving storage space. These manipulations do not fundamentally change the contents of the original image, while malicious tampering will alter the meaning of the image, such as removing, adding and modifying an object in a scene [17]. Malicious manipulations, in collaboration with subsequent operations such JPEG compression, contrast adjustment, blurring, etc., would make forgeries hard to detect. Therefore image-alteration detection can determine whether the images are original and help us with further analysis.

In [17], [18], authors have proposed a method to identify the bitmap compression history. In this method, given an image which is saved in bitmap format, to determine whether it has been previously JPEG-compressed, and further to estimate which quantization matrix has been used. The original intention of the paper was not for tampering detection. However, it can provide us indirect evidence for image forensics. The method assumes that if there is no compression the pixel differences across blocks should be similar to those within blocks, while they should be different due to block artifacts if the image has been JPEG-compressed.

Another issue about JPEG forgeries is the detection of double JPEG compression. In [19], authors have proposed a method to estimate the primary (previous) quantization matrix from a double-compressed JPEG image. In [20], authors have presented a method to determine whether the image has been double JPEG-compressed. Both works are based on the periodicity in the histogram of DCT coefficients that is introduced by double JPEG compression.

3)Camera based techniques: High-resolution and low-cost digital cameras have been rapidly replacing the typical film cameras. Now, most images in our daily life are acquired by various brands of digital cameras, such as Canon, Nikon, Sony, Olympus, etc. One of the main problems related to source identification is the classification of the different camera models or individuals for a given image.

The most straightforward solution for camera identification is to check the exchangeable image file (EXIF) format header of the output image. Some settings of an image are stored in the headers, and the settings are constrained by a given camera, such as the manufacturer, the model of the camera, image size, exposure time, and the quantization matrix used in JPEG compression [21], etc. If the given image settings are out of the range of the given camera, it can be concluded that the image did not come from the camera or it was not the original one at least. However, it is difficult to distinguish among the cameras of the same or similar model whose images

contain the same header information. Furthermore, the header information can be easily replaced or made consistent by JPEG recompression or other operations.

There are some defect pixels in the charge coupled device (CCD) inside the low-cost digital cameras. These defects pixels are at the different places of the CCD according to the different sensors, and thus can be used as the unique evidence for the cameras. As mentioned in [22], there are some restrictions when using this method. For example, the defects in pixels are visible only in the regions that are darker or the lighter areas if a surface has the same intensity lighting. These defects pixels also depend on the temperature. Furthermore, some post-processing operations such as JPEG compression, etc., may remove or suppress the defective pixels. For the expensive cameras which have better CCDs with fewer errors, the method cannot be applied.

Due to cost considerations, many manufactures employ a single sensor instead of multiple sensors to capture the color scene. Thus the color filter array (CFA) is always applied in front of the sensor to control the band of wavelengths arriving at the CCD array.

In order to reconstruct the full-resolution color scene, some interpolation algorithms will be employed. The estimations are usually carried out by interpolating neighboring pixel values using a weighting matrix around the missing pixel, which are called demosaicking techniques [23].

The correlations may be linear, nonlinear or adaptive. And these different techniques are employed in different models of cameras, which will inevitably introduce a different statistical correlation between the original values and the interpolation values. The simplest demosaicking methods are kernel-based ones that act on each channel independently. More sophisticated algorithms interpolate edges differently from uniform areas to avoid blurring salient image features. Regardless of the specific implementation, CFA interpolation introduces specific statistical correlations between a subset of pixels in each color channel.

To estimate the pattern of the correction between the samples, the EM (expectation/maximization) algorithm has been applied. The algorithm includes two steps: E-step and M-step. In the E-step, the probability of each pixel belonging to an original pixel or to the interpolated one is evaluated. Then in the M-step, the estimation is optimized and updated.
The pattern noise is defined as any noise component that survives frame averaging [24], which is another important characteristic of imaging sensors. The pattern noise described in [24], include two main components: the fixed pattern noise (FPN) and the photo-response non-uniformity noise (PRNU). Fixed pattern noise (FPN) is mainly caused by the dark current on a CCD chip. The dark current is due to thermal activity in the photocathode and the dynodes. And it is present whether the shutter is open or closed. However, the magnitudes of the dark current on a CCD are always non-uniformity as different pixels may have different generation rates of dark current. The millions of non-uniformity pixels are arranged regularly on each CCD, and therefore can create the unique pattern for each sensor. In [24], the authors used FPN to identify the video camera from videotape images. They recorded 100 black images with each camera by covering the lens, and then the images were accumulated to suppress the effect of the random noise. The results show that some bright dots are observed in the accumulated images, and these bright dots are at different positions for each camera. However, FPN is visible only in the dark frames. Furthermore, the noise can be alleviated at a low temperature.

Another main source of the pattern noise in imaging sensor is PRNU. Unlike FPN, which is generated thermally in the sensor even when no light arrives, PRNU is the pixel variation under illumination. FPN is an offset, while PRNU is a gain. Therefore, the primary source of pattern noise remaining in nature images may be PRNU. Two sources contribute to PRNU. The main source is pixel non-uniformity (PNU), and the other source is low frequency defects, which is caused by light refraction on dust particles and optical surfaces, etc. This source is low spatial frequency in nature. In [24], the authors used PNU as an inherent pattern of the imaging sensor for camera identification. To verify that a given image p was taken with a specific camera C; they first extracted the camera reference pattern P_c, which is an approximation of PNU.

4)Physically based techniques: Images that are combined during tampering are taken in different lighting conditions. It becomes difficult to match the lighting condition from combining photographs. This lighting inconsistency in the composite image can be used for detection of image tampering. Initial attempt in this regard was made by Johnson and Farid [25].

They proposed a technique for estimating the direction of an illuminating light source within one degree of freedom to detect forgery. By estimating direction of light source for different objects and people in an image, inconsistencies in lighting are uncovered in the image and tampering can be detected.

Johnson and Farid [26] proposed a model based on lighting inconsistencies because of presence of multiple light sources. This model is motivated from earlier model [25] but it generalizes this model by estimating more complex lighting and can be adapted to a single lighting source.

Johnson and Farid [27] estimated 3-D direction to a light source by means of the lights reflection in the human eye. These reflection called specular highlights are a powerful clue as to the location and shape of the light sources. Inconsistencies in location of the light source can be used to detect tampering.

Chen et al., [28] proposed a method for authentication of image with infinite light source based on inconsistencies in light source direction. Hestenes-Powell multiplier method was employed to calculate the light source direction of different objects and their background in infinite light source images. Authenticity is determined on the basis of consistency between the light source direction of the object and its background with detection rate of 83.7%.

Kee and Farid [29] described a method to estimate a 3-D lighting environment with a low dimensional model and to approximate the model's parameters from a single image. Inconsistencies in the lighting model are used as indication of forgery. In [30], the authors present a forgery detection technique which is based on inconsistency in light source direction. The method called as neighborhood was used to calculate surface normal matrix of image in the blind identification algorithm with detection rate of 87.33%.

Fan et al., [31] proposed a technique which infers that methods based on forgery detection using 2D lighting system can be fooled easily and gave a promising technique based on shape from shading. This approach is more general but the issue of estimation of 3D shapes of objects remains.

The authors of [32] describe a method for image forgery detection based on inconsistencies in the color of the illumination. Information from physics and statistical based illuminate estimators on image regions of similar material are used. From these texture and edge based features are extracted. SVM meta fusion classifier is used and detection rate of 86% obtained. This approach requires minimal user interaction. The advantage of these methods is that they make the lighting inconsistencies in the tampered image very difficult to hide.

5) Geometric based techniques: In authentic images, the principal point (the projection of the camera center onto the image plane) is near the center of the image. When a person or object is translated in the image, the principal point is moved proportionally. Differences in the estimated principal point across the image can therefore be used as evidence of tampering. The authors in [33], has described how to estimate a cameras principal point from the image of a pair of eyes (i.e., two circles) or other planar geometric shapes. They showed how translation in the image plane is equivalent to a shift of the principal point. Inconsistencies in the principal point across an image can then be used as evidence of tampering.

In [34], the authors have analyzed the physical differences in generation between CG and photographic images, e.g., the sharp structures in CG images and gamma correction in photographic. They then proposed a geometry-based image model that reveals the differences. For source identification, the method extracts the geometry features based on the rigid body moments. Finally, an SVM classifier is employed. The experimental results show the effect of the proposed method with a classification accuracy of 83.5%, which outperforms the prior methods. Another contribution of their work is that they created an image benchmark for the classification problem of CG and photographic images.

3.Comparison of Dif detection techniques

With the image processing techniques developing at increasing rate, tampering the digital images without leaving any clues has become an easy task. This leads to the problem like image authentication. Digital image forensics has evolved as a solution to image tampering.

Passive technology for image forensics is a new research area. Unlike the signature-based and watermark-based methods, the new method is blind without extra side information in detection. The inherent pattern of the image can be served as a non-

intrusive watermark for source identification and alternation detection. Therefore pattern selection is crucial in this technology. Although some of the existing methods succeed in reaching a relatively high accuracy, the proposed methods in the survey carried out exhibits limitation and drawbacks which has to be improved.

As passive technology is mainly based on detection of the inherent pattern, pattern removal and pattern reinsertion would prevent detection. For example, in source-camera identification based on pattern noise [24], there are some ways to prevent identification, such as removing the pattern noise from the image, extracting the pattern noise from another camera and then adding it to an image to confuse identification, etc. However, some of these operations are beyond the ability of average users, such as pattern noise extraction, Re-JPEG artifacts removal, CFA re-interpolation, chromatic aberration reparation, make the lighting consistency by virtual light source(s) and so on, which require the attacker mastering some professional knowledge about digital cameras, image processing, computer graphics, etc. Furthermore, any post-processing performed on the tampered image may introduce new or more inconsistencies into the image and thus may leave other traces for detection. Therefore new methods have to be proposed to provide more accuracy detection in these situations.

Standard image dataset and benchmark are in urgent demand for evaluating the proposed methods. For example, the estimation of the parameters employed inside a digital camera requires an image dataset including various models of camera with different acquisition settings. For the splicing detection evaluation, the image dataset with more realistic operations has to be created. For the problem of identifying computer-generated and digital-camera images, the dataset should include higher photorealism computer graphics with the same scenes as photographic images. To reduce the effects of the software and physics apparatus, the CG images should be generated by different software programs, and the photographic images should be captured by different models of cameras, etc. Some of the proposed methods are under too many constraints. For example, the methods for the image-splicing detection do not consider post-processing at all. However, when creating a forged image, the attacker could apply some operations such as edge blurring, adding noise, and lossy compression, etc., after the simple joining of image regions. And such post-processing will inevitably decrease the detection accuracy.

In double JPEG detection, the method assumes repeated JPEG compression with different quantization matrices. Thus, all the prior methods may fail when recompressing with the same quantization matrix. Furthermore, most of the passive technologies are dependent on statistical features of the image. If a small portion of an image has been manipulated, the statistical features may not be altered. Thus the tampered region should be large enough to be detected when using some of the passive technologies.

There are many open issues. For example, finding more robust statistical features to resist the various post-processing and creating image benchmarks to set up a fair evaluation system. Apart from this, when tampering with an image or creating a CG, editing software is to be used. However, such software programs are diverse due to the different implements inside them. For instance, when editing JPEG images, IJG, Adobe Photoshop, GIMP and MATLAB may be used.

According to our experiments, even in decompressing the same image, the outputs are different. The inherent patterns introduced by editing software may be used as signature for image forensics. Furthermore, most the prior literatures focus on the forgery detection. However, the forgery detection and tampering technology are interactional, just like the relationship between steganalysis and Steganography. The advanced image manipulation technologies combining with image processing, computer vision and computer graphics need to be further investigated for making the forgery more realistic and harder to detect. The passive method in collaboration with the active approach may play an important role in the field of image forensics.

4.Conclusion

In the last decades many forgery detection techniques have been proposed. In this paper, a brief survey of Digital image forgery classification and its detection methods have been presented. An attempt is made to bring in various potential algorithms that signify improvement in image authentication techniques. From the knowledge of the image authentication techniques it is inferred that Passive or blind techniques which need no prior information of the image under consideration have a significant advantage of no requirement of special equipment's

to embed the code into the image at the time of generation, when compared to active techniques.

As discussed earlier, the techniques which have been developed till now are cable of detecting the forgery and only a few can localize the tampered area. There are a number of drawbacks with the presently available technologies. Firstly all systems require human interpretation and thus cannot be automated. Second being the problem of localizing the forgery. Next problem is of robustness to common image processing operations like blurring, JPEG compression, scaling, and rotation.

In practice since an image forgery analyst may not be able to know which forgery technique is used to tamper the image, using a specific authentication technique may not be reasonable. Hence there is still an utmost need of a forgery detection technique that could detect any type of forgery. There is also a setback of no established benchmarks which makes performance analysis and comparison of results of current algorithms difficult. As such there is need to develop common benchmark for image data set and image forgery detection techniques that could detect any type of forgery with lesser computational complexity and high robustness.

Acknowledgment
None.

Conflicts of interest
The authors have no conflicts of interest to declare.

References
[1] Farid H. Image forgery detection. IEEE Signal Processing Magazine. 2009; 26(2):16-25.
[2] Fridrich J. Robust bit extraction from images. IEEE international conference on in multimedia computing and systems 1999 (pp. 536-40). IEEE.
[3] Doke KK, Patil SM. Digital signature scheme for image. International Journal of Computer Applications. 2012; 49(16):1-6.
[4] Zhao X, Li J, Li S, Wang S. Detecting digital image splicing in chroma spaces. In international workshop on digital watermarking 2010 (pp. 12-22). Springer Berlin Heidelberg.
[5] Bravo-Solorio S, Nandi AK. Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics. Signal Processing. 2011; 91(8):1759-70.
[6] Pun CM, Yuan XC, Bi XL. Image forgery detection using adaptive over segmentation and feature point matching. IEEE Transactions on Information Forensics and Security. 2015; 10(8):1705-16.
[7] Moghaddasi Z, Jalab HA, Noor RM. SVD-based image splicing detection. In international conference on information technology and multimedia 2014 (pp. 27-30). IEEE.
[8] Boato G, Natale FG, Zontone P. How digital forensics may help assessing the perceptual impact of image formation and manipulation. In proceedings of fifth international workshop on video processing and quality metrics for consumer electronics 2010.
[9] Avcibas I, Bayram S, Memon N, Ramkumar M, Sankur B. A classifier design for detecting image manipulations. In image processing international conference on 2004 (pp. 2645-8). IEEE.
[10] Stamm M, Liu KR. Blind forensics of contrast enhancement in digital images. In IEEE international conference on image processing 2008 (pp. 3112-15). IEEE.
[11] Stamm MC, Liu KR. Forensic estimation and reconstruction of a contrast enhancement mapping. In ICASSP 2010 (pp. 1698-1701).
[12] Stamm MC, Liu KR. Forensic detection of image manipulation using statistical intrinsic fingerprints. IEEE Transactions on Information Forensics and Security. 2010; 5(3):492-506.
[13] Cao G, Zhao Y, Ni R. Forensic estimation of gamma correction in digital images. In IEEE international conference on image processing 2010 (pp. 2097-2100). IEEE.
[14] Li XF, Shen XJ, Chen HP. Blind identification algorithm for retouched images based on Bi-Laplacian. Jisuanji Yingyong/ Journal of Computer Applications. 2011; 31(1):239-42.
[15] Cao G, Zhao Y, Ni R, Li X. Contrast enhancement-based forensics in digital images. IEEE Transactions on Information Forensics and Security. 2014; 9(3):515-25.
[16] Chierchia G, Poggi G, Sansone C, Verdoliva L. A Bayesian-MRF approach for PRNU-based image forgery detection. IEEE Transactions on Information Forensics and Security. 2014; 9(4):554-67.
[17] Fan Z, de Queiroz R. Maximum likelihood estimation of JPEG quantization table in the identification of bitmap compression history. In international conference on image processing proceedings 2000 (pp. 948-51). IEEE.
[18] Fan Z, De Queiroz RL. Identification of bitmap compression history: JPEG detection and quantizer estimation. IEEE Transactions on Image Processing. 2003; 12(2):230-5.
[19] Lukáš J, Fridrich J. Estimation of primary quantization matrix in double compressed JPEG images. In proceedings of digital forensic research workshop 2003 (pp. 5-8).
[20] Popescu AC. Statistical tools for digital image forensics (Doctoral dissertation, Dartmouth College).
[21] Hany F. Digital image ballistics from JPEG quantization. Technical report TR2006-583, department of computer science, dartmouth college; 2006.

[22] Geradts ZJ, Bijhold J, Kieft M, Kurosawa K, Kuroki K, Saitoh N. Methods for identification of images acquired with digital cameras. In international society for optics and photonics enabling technologies for law enforcement 2001 (pp. 505-12).
[23] Popescu AC, Farid H. Exposing digital forgeries in color filter array interpolated images. IEEE Transactions on Signal Processing. 2005; 53(10):3948-59.
[24] Lukas J, Fridrich J, Goljan M. Digital camera identification from sensor pattern noise. IEEE Transactions on Information Forensics and Security. 2006; 1(2):205-14.
[25] Johnson MK, Farid H. Exposing digital forgeries by detecting inconsistencies in lighting. In proceedings of the 7th workshop on multimedia and security 2005 (pp. 1-10). ACM.
[26] Johnson MK, Farid H. Exposing digital forgeries in complex lighting environments. IEEE Transactions on Information Forensics and Security. 2007; 2(3):450-61.
[27] Johnson MK, Farid H. Exposing digital forgeries through specular highlights on the eye. In international workshop on information hiding 2007 (pp. 311-25). Springer Berlin Heidelberg.
[28] Chen H, Shen X, Lv Y. Blind identification method for authenticity of infinite light source images. In fifth international conference on frontier of computer science and technology 2010 (pp. 131-5). IEEE.
[29] Kee E, Farid H. Exposing digital forgeries from 3-D lighting environments. In IEEE international workshop on information forensics and security 2010 (pp. 1-6). IEEE.
[30] Lv Y, Shen X, Chen H. An improved image blind identification based on inconsistency in light source direction. The Journal of Supercomputing. 2011; 58(1):50-67.
[31] Fan W, Wang K, Cayre F, Xiong Z. 3D lighting-based image forgery detection using shape-from-shading. In proceedings of the European signal processing conference 2012 (pp. 1777-81). IEEE.
[32] De Carvalho TJ, Riess C, Angelopoulou E, Pedrini H, de Rezende Rocha A. Exposing digital image forgeries by illumination color classification. IEEE Transactions on Information Forensics and Security. 2013; 8(7):1182-94.
[33] Johnson MK, Farid H. Detecting photographic composites of people. In international workshop on digital watermarking 2007 (pp. 19-33). Springer Berlin Heidelberg.
[34] Ng TT, Chang SF, Hsu J, Xie L, Tsui MP. Physics-motivated features for distinguishing photographic images and computer graphics. In proceedings of the ACM international conference on multimedia 2005 (pp. 239-48). ACM.

This paper is selected from proceedings of National Workshop on Cryptology-NWC 2016 organized at JNN College of Engineering Shimoga, Karnataka, India during 11-13, August 2016.