International Journal of Advanced Science and Technology
Vol.73 (2014), pp.15-32
http://dx.doi.org/10.14257/ijast.2014.73.02

Digital Image Forgeries and Passive Image Authentication Techniques: A Survey

Saba Mushtaq and Ajaz Hussain Mir

Department of Electronics and Communication Engineering, National Institute of Technology Srinagar, India-190006
sab.mushtaq@gmail.com, ahmir@rediffmail.com

Abstract

Digital images are present everywhere on magazine covers, in newspapers, in courtrooms as evidences, and all over the Internet signifying one of the major ways for communication nowadays. The trustworthiness of digital images has been questioned, because of the ease with which these images can be manipulated in both its origin & content as a result of tremendous growth of digital image manipulation tools. Digital image forensics is the latest research field which intends to authorize the genuineness of images. This survey attempts to provide an overview of various digital image forgeries and the state of art passive methods to authenticate digital images.

Keywords: *Digital image forensics, Image authentication, Image forgery, Image tampering*

1. Introduction

From time to time images have been generally accepted as evidence of events of the depicted happenings. Because of dominance of computer in field of education, business and other field, acceptance of digital image as authorized document has become frequent .The ease of use and accessibility of software tools [1] and low-cost hardware, makes it very simple to forge digital images leaving almost no trace of being subjected to any tampering . As such we cannot take the authenticity and integrity of digital images for granted [2]. This challenges the reliability of digital images offered as medical diagnosis, as evidence in courts, as newspaper items or as legal documents because of difficulty in differentiating original and modified contents.

Digital forensics field has developed significantly to combat the problem of image forgeries in many domains like legal services, medical images, forensics, intelligence and sports [3, 4]. Substantial amount of work is carried out in the field of image forgery detection. This is evident from figure 1 which shows the number of papers that addressed image forgery detection in IEEE and science direct over last 10 years. In this context this paper presents a review of blind/passive image forgery detection techniques and attempt is made to survey most recent literature available on the subject.

ISSN: 2005-4238 IJAST

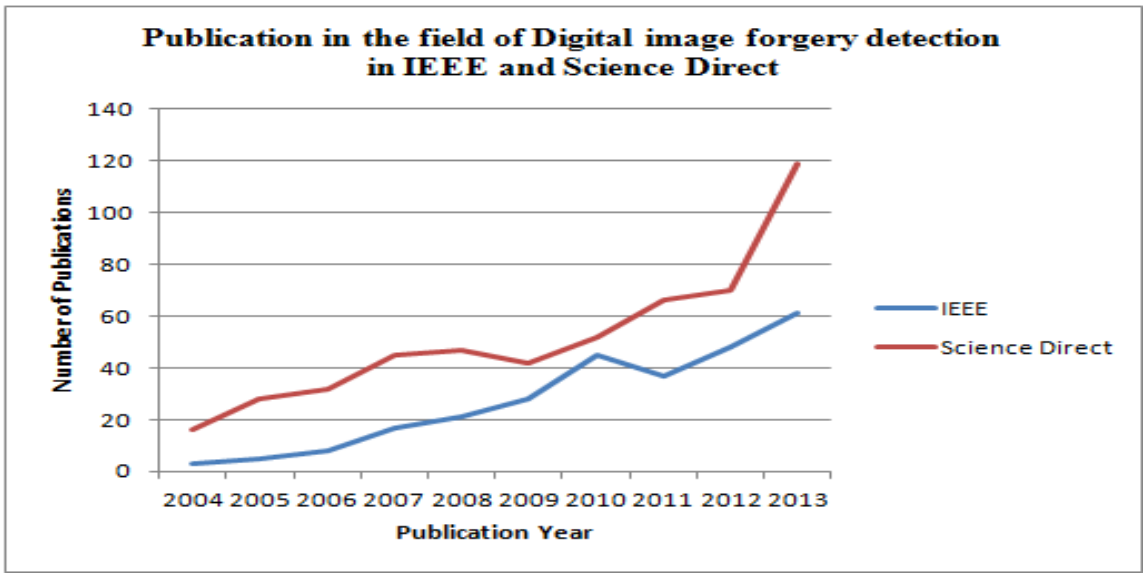

Figure 1. Number of IEEE and Science Direct publications in the field of digital image forgery detection over the last 10 years. Data was retrieved from IEEE explore website, http://ieeexplore.ieee.org and Science Direct website, http://www.sciencedirect.com by submitting the query image forgery detection

2. Classification of Image Authentication Techniques.

Forgery detection intends to verify the authenticity of images [5]. For authentication of images several methods have been developed. In this paper we broadly classify these methods into two classes: Active authentication and Passive authentication. The classification is based on the fact whether the original image is available or not. Under each class the methods are further sub divided. The hierarchy is shown in Figure 2.

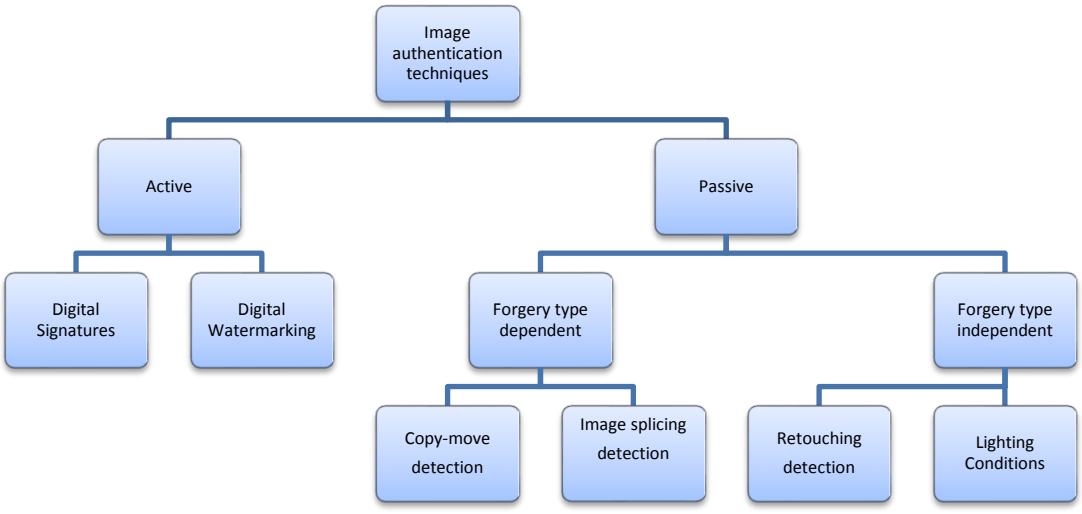

Figure 2. Image Authentication Techniques

2.1. Active Authentication

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 watermarking and digital signatures [6-8]. Digital water marks are embedded into the images at the time of image acquisition or in processing stage and digital signatures embed some secondary information, usually extracted from image, at the acquisition end into the image .A lot of work has been carried in both digital signatures [9-13] and digital watermarking[14-18]. The main drawback of these approaches remains that they are to be inserted into the images at the time of recording using special equipments thus prior information about image becomes indispensable.

2.2. Passive Authentication

Passive authentication also called image forensics is the process of authenticating images with no requirement of prior information just the image itself [19, 20]. Passive techniques are based on the assumption that even though tampering may not leave any visual trace but they are likely to alter the underlying statistics. It is these inconsistencies that are used to detect the tampering. Exhaustive research survey has been carried out in this field of passive image forensics [21-23]. Passive techniques are further classified as forgery dependent methods and forgery independent methods.

Forgery dependent detection methods are designed to detect only certain type of forgeries such as copy-move and splicing which are dependent on the type of forgery carried out on the image while as forgery independent methods detect forgeries independent of forgery type but based on artifact traces left during process of re-sampling & due to lighting inconsistencies [24].

3. General Framework for Forgery Detection

Forgery detection in images is a two class problem. The main objective of passive detection technique remains to classify a given image as original or tampered. Most of the existing techniques extract features from image after that select a suitable classifier and then classify the features. Here we describe a general structure of image tampering detection consisting of following steps shown in Figure 3.

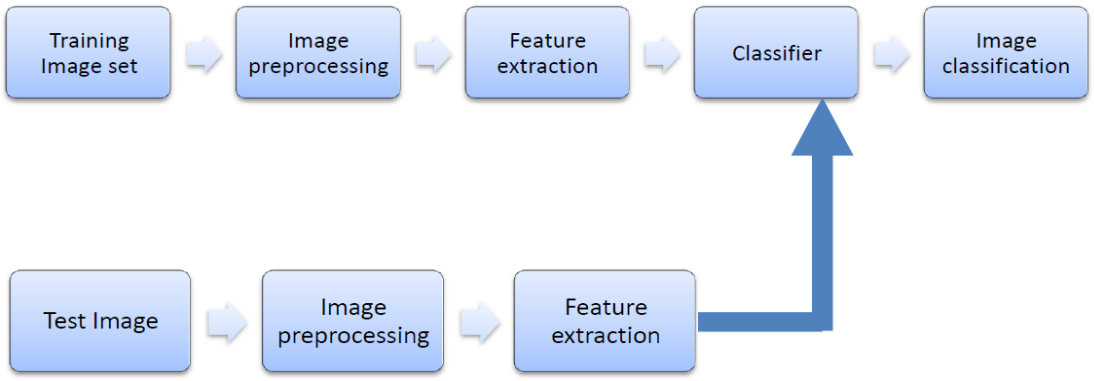

Figure 3. Framework for Image Forgery Detection

Image preprocessing is the first step. Before image could be subjected to feature extraction operation some preprocessing is done on the image under consideration such as enhancement, filtering, cropping, DCT transformation, conversion from RGB to grayscale. Algorithms discussed here after may or may not involve this step depending on the algorithm. After this comes feature extraction. Feature set for each class which differentiates it from other classes but at the same time remains invariant for a particular class are selected. The most desirable feature of the selected feature set is to have a small dimension so that computational complexity is reduced and have a large interclass difference. This is the most important step and all algorithms rely mainly on this step for forgery detection. This step for all aforementioned algorithms is discussed individually with the algorithms. After this is Classifier selections. Based on extracted feature set appropriate classifier is either selected or designed. Most likely a large training set gives a better performing classifier. The extracted features may also require some preprocessing so as to reduce their dimension and as such the computational complexity without affecting the machine learning [44]. The sole purpose of classifier is to classify an image either as original or forged. Various classifiers have been used such as neural networks [25],SVM[26,27,28] and LDA[29].Finally some forgeries like copy move and splicing may require post processing which involve operations like localization of duplicate regions [30,31,32,33].

4. Copy-move Forgery Detection

Copy-move is the most popular and common photo tampering technique because of the ease with which it can be carried out [34]. 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 [35]. An example of copy-move forgery is shown in Figure 4.

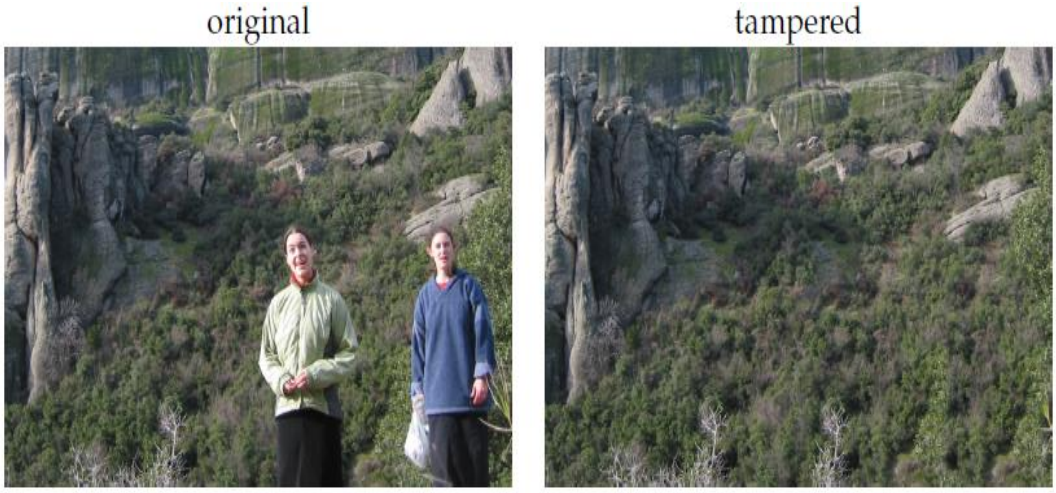

Figure 4. Copy- move Forgery (People in the Image are Masked by Pasting a Region Copied from same Image) [41]

The original image is forged to obtain the tampered image; persons have been masked by copying a region from the same image and pasting it over them. Post processing operation like blurring is used to decrease the effect of border irregularities between the two images.

Among the initial attempts Fredrich [36] proposed methods to detect copy-move forgery. Discrete cosine transform (DCT) of the image blocks was used and their lexicographical sorting is taken to avoid the computational burden. Once sorted the adjacent identical pair of blocks are considered to be copy-moved blocks. Block matching algorithm was used for balance between performance and complexity. This method suffers from the drawback that it cannot detect small duplicate regions.

Popescu and Farid [37] suggested a method using principal component analysis (PCA) for the overlapping square blocks. The computational cost and the number of computations required are considerably reduced $O(N_tN \log N)$, where N_t is the dimensionality of the truncated PCA representation and N the number of image pixels. Detection accuracy of 50% for block size of 32x32 and 100% for block size of 160x160 was obtained. Although this method has reduced complexity and is highly discriminative for large block size but accuracy reduces considerably for small block sizes and low JPEG qualities. To combat computational complexity Langille and Gong [38 proposed use of k-dimensional tree which uses a method that searches for blocks with similar intensity patterns using matching techniques. The resulting algorithm has a complexity of $O(N_aN_b)$ where N_a is neighbourhood search size and N_b is the number of blocks. This method has reduced complexity as compared to the earlier methods.

Gopi *et al.*, [39] developed a model that used auto regressive coefficients as feature vector and artificial neural network (ANN) classifier to detect image tampering. 300 feature vectors from different images are used to train an ANN and the ANN is tested with another 300 feature vectors. Percentage of hit in identifying the digital forgery is 77.67% in experiment in which manipulated images were used to train ANN and 94.83% in experiment in which a database of forged images was used.

Myna *et al.*, [40] proposed a method which uses log polar coordinates and wavelet transforms to detect and also localize copy-move forgery. Application of wavelet transform to input image results in dimensionality reduction and exhaustive search is carried out to identify the similar blocks in the image by mapping them to log-polar coordinates and for similarity criterion phase correlation is used. The advantage of this method is reduced image size and localization of duplicate regions.

XiaoBing and ShengMin [41] developed a technique for localization of copy-move image forgery by applying SVD which provides the algebraic and geometric invariant feature vectors. The proposed method has reduced computational complexity and strong against retouching operation. Method suggested in [42]) applies radix sort technique to the overlapping block which is followed by median filtering and CCA (connected component analysis) for tamper detection this method localizes detection without effecting image quality and is simple and efficient too. This method has used radix sort as an alternative to lexographical sorting which has considerably improved the time efficiency.

Bashar *et al.*, [43] developed a technique that detects duplication using two robust features based on DWT and kernel principal component analysis (KPCA). KPCA-based projected vectors and multi resolution wavelet coefficients subsequent to image-blocks are arranged in the form of a matrix on which lexicographic sorting has been carried out. Translation Flip and translation Rotation are also identified using global geometric transformation and the labeling technique to detect the forgery. This method eliminates the off-set frequency threshold which otherwise is to be manually adjusted as in other detection methods.

Sutthiwan *et al.*, [44] presented a method for passive-blind color image forgery detection which is a combination of image features extracted from image luminance by applying a rake – transform and from image chroma by using edge statistics. The technique results in 99% accuracy.

Liu *et al.*, [45] proposed use of circular block and Hu moments to detect the regions which have been rotated in the tampered image. Sekeh *et al.*, [46] suggested a technique based on clustering of blocks implemented using local block matching method. Huang *et al.*, [47] worked on enhancing the work done by Fridrich *et al.*, [36] in terms of the processing speed. The algorithm is shown to be straightforward, simple, and has the capability of detecting duplicate regions with good sensitivity and accuracy. However there is no mention of robustness of the algorithm against geometric transformation.

Xunyu and Siwei [48] presented a technique that uses region duplication by means of estimating the transform between matched SIFT key points that is invariant to distortions that occurs due to image feature matching. The algorithm results in average detection accuracy of 99.08% but the method has one limitation duplication in smaller region is hard to detect as key points available are very few.

Kakar and Sudha [49] developed a new technique based on transform-invariant features which detecting copy-paste forgeries but requires some post processing based on the MPEG-7 image signature tools. Feature matching that uses the inherent constraints in matched feature pairs so as to improve the detection of cloned regions is used which results in a feature matching accuracy of more than 90%.

Muhammad *et al.*, [50] proposed a copy-move forgery detection method based on dyadic wavelet transform (DyWT). DyWT being shift invarient is more suitable than DWT. Image is decomposed into approximate and detail subbands which are futher divided into overlapping blocks and the similarity between blocks is calculated. Based on high similarity and dissimilarity pairs are sorted. Using thresholding, matched pairs are obtained from the sorted list.

Hong shao *et al.*, [51] proposed a phase correlation method based on polar expansion and adaptive band limitation. Fourier transform of the polar expansion on overlapping windows pair is calculated and an adaptive band limitation procedure is applied to obtain a correlation matrix where peak is effectively enhanced. After estimating the rotation angle of the forgery region, a searching algorithm in the sense of seed filling is executed to display the whole duplicated region. This approach can detect duplicated region with high accuracy and robustness to rotation, illumination adjustment, and blur and JPEG compression.

Gavin Lynch [52] developed expanding block algorithm for duplicate region detection. In this method image is divided into overlapping blocks of size SxS. For each block grey value is calculated to be its dominant feature. Based on the comparison of this dominant factor a connection matrix is created. If the connection matrix has a row of zeros, then the block corresponding to this row is not connected to any other block in the bucket. This way duplicate regions are detected. This method is good at identifying the location and shape of the forged regions and direct block comparison can be done without sacrifice in performance time.

Copy-move detection proposed by Sekeh [53] offers improved time complexity by using sequential block clustering. Clustering results in reduced search space in block matching and improves time complexity as it eliminates several block-comparing operations. When number of cluster is greater than threshold, local block matching is more efficient than lexicographically sorting algorithm.

Detection and localization method for copy-move forgery is proposed in [54] based on SIFT features. Novelty of the work consists in introducing a clustering procedure which operates in the domain of the geometric transformation and deal with multiple cloning too.

A robust method based on DCT and SVD is proposed in [55] to detect copy-move forgery. The image is divided into fixed-size overlapping blocks and 2D-DCT is applied to each block, then the DCT coefficients are quantized to obtain a more robust representation of each

block followed by dividing these quantized blocks into non overlapping sub-blocks and SVD is applied to each sub-block, then features are extracted to reduce the dimension of each block using its largest singular value, feature vectors are lexicographically sorted, and duplicated image blocks will be matched by predefined shift frequency threshold.

All methods discussed above that are able to detect and localize copy move forgery and cloned regions in an image are computationally complex and require human interpretation of the results. Table 1 below gives comparison of various copy-move forgery detection algorithms.

Table 1. Comparison of Copy-move Forgery Detection Methods

Method	Extracted Feature	Classifier	Detection Accuracy
Popescu & Farid [37]	PCA of overlapping block	Lexographical sorting	50% for small block size 100% for 16x16 block size
Gopi et al. [39]	Auto regressive coffecients	ANN	94.83%
Myan et al. [40]	Log polar co-ordinates	Phase correlation	-
Xiaibing & Shengmin[41]	Singular value decomposition and algebraic and geometric feature invariant	Lexographical sorting	-
Lin et al. [42]	Average intensity of image blocks.	Radix sort followed by shift vector calculation	98%
Basher et al. [43]	DWT & KPCA	Point based duplication detection algorithm	95.55% (DWT) 90.94%(KCPA)
Sutthiwan et al.[44]	Image luminance using RAKE model & image chroma using edge statistics	SVM	99%
Xunyu & Siwei [48]	Matched SIFT Keypoints	K-mean Clustring	99.08%
Muhammad et al. [50]	Dyadic wavelet transform	Thresholding Classification	98.34%
Zhao & Guo[55]	DCT & SVD	Lexographical sorting of blocks and frequency thresholding.	96.1 %

5. Image Splicing

Image splicing forgery technique involves composition or merging of two or more images changing the original image significantly to produce a forged image. In case images with differing background are merged then it becomes very difficult to make the borders and boundaries indiscernible. Figure 5 below shows an example of image splicing where the face of two different people is combined to form a forged image.

Figure 5. Osama Bin Ladin's Spliced Image which Became Viral on the Net [http://www.theguardian.com/world/2011/may/02/osama-bin-laden-photo-fake]

Splicing detection is a complex problem whereby the composite regions are investigated by a variety of methods. The presence of abrupt changes between different regions that are combined and their backgrounds, provide valuable traces to detect splicing in the image under consideration. Farid [56] suggested a method based on bi-spectral analysis to detect introduction of un-natural higher-order correlations into the signal by the forgery process and is successfully implemented for detecting human-speech splicing.

Ng and Chang [57] suggested an image-splicing detection method based on the use of bi-coherence magnitude features and phase features. Detection accuracy of 70% was obtained. Same authors later developed a model for detection of discontinuity caused by abrupt splicing using bi-coherence [58].

Fu *et al.*, [59] proposed a method that implemented use of Hilbert-Huang transform (HHT) to obtain features for classification. Statistical natural image model defined by moments of characteristic functions was used to differentiate the spliced images from the original images.

Chen *et al.*, [60] proposed a method that obtains image features from moments of wavelet characteristic and 2-D phase congruency which is a sensitive measure of transitions in a spliced image, for splicing detection. Zhang *et al.*, [61] developed a splicing detection method that utilizes moment features extracted from the multi size block discrete cosine transform (MBDCT) and image quality metrics (IQMs) which are sensitive to spliced image. It measures statistical difference between spliced and original image and has a broad area of application.

Ng and Tsui [62] and Ng T.T. [63] developed a method that uses linear geometric invariants from the single image and thus extracted the CRF signature features from surfaces linear in image irradiance. In [63] authors developed an edge-profile based method for extraction of CRF signature from a single image. In the proposed method the reliable extraction depends on the fact that edges should be straight and wide.

Qing Zhong and Andrew [64] explained a technique based on extraction of neighboring joint density features of the DCT coefficients, SVM classifier is applied for image splicing detection. The shape parameter of generalized Gaussian distribution (GGD) of DCT coefficients is utilized to measure the image complexity.

Wang *et al.*, [65] developed a splicing detection method for color images based on gray level co-occurrence matrix (GLCM). GLCM of the threshold edge image of image chroma is used. Zhenhua et al. [66] developed a splicing detection method based on order statistic filters

(OSF). Feature extraction is guided by edge sharpness measure and a visual saliency. Fang et al. [67] gives an example that makes use of the sharp boundaries in color images. The technique looks for the consistency of color division in the neighborhood pixels of the boundary. The author suggests that the irregularity at the color edge is significant evidence that the image has been tampered.

In [68] a method based on extraction of features by Hilbert–Huang transform (HHT) and a statistical model based on the moments of characteristic functions on application of wavelets to detect spliced region is explained. This method gives high accuracy results for passive splicing detection.

Zhang *et al.*, [69] developed a technique that makes use of planar homography constraint to identify the fake region roughly and an automated method for extraction using graph cut with automated feature selection to isolate the fake object.

Zhao *et al.*, [70] developed a method based on chroma space. Gray level run length texture feature is used. Four gray level run-length run-number (RLRN) vectors along different directions obtained from de-correlated chroma channels were used as unique features for detection of image splicing and for classification SVM was employed as classifier. Liu et al. [71] developed a method based on photometric consistency of illumination. Photometric consistency was employed in shadows by formulating color characteristics of shadows which is measured by shadow matte value.

Image splicing detection method proposed in [72] uses illuminant color inconsistency. Given color image is divided into many overlapping blocks. Based on the content of blocks a classifier is used to adaptively select illuminant estimation algorithm. Illuminant color is estimated for each block, and the difference between the estimation and reference illuminant color is measured. If the difference is larger than a threshold, the corresponding block is labeled as spliced block.

Method based on run length is proposed in [73] to detect splicing. Edge gradient matrix of an image is computed, and approximate run length is calculated along the edge gradient direction. Some features are constructed from the histogram of the approximate run length. To further improve the detection accuracy, the approximate run length is applied on the error image and the reconstructed images based on DWT to obtain more features. SVM is employed to classify the authentic and spliced images. An improvement was obtained in [74] where a Markov based approach is proposed. Markov features are expanded to capture not only the intra- block but also the inter-block correlation between block DCT coefficients. To handle a large number of developed features, feature selection method SVM-RFE is utilized and SVM is exploited as a classifier.

A novel scheme was proposed by Rimba *et al.*, [75] which exploits a group of similar images, to verify the source of tampering. Membership function and the correlation-based alignment method is used to automatically identify the spliced region in any fragment of the reference images. The proposed scheme is efficient in revealing the source of spliced regions.

Subtle inconsistencies in the color of the illumination of images are exploited in [76]. The technique is applicable to images containing two or more people and requires no expert interaction for the tampering decision. Texture and edge based features are extracted from illuminant estimators which are then provided to a machine-learning approach for automatic decision-making. SVM is used for classification and detection rates of 86% on a dataset consisting of 200 images and 83% on 50 images collected from the Internet was achieved. Another detection scheme based on blur as a clue is proposed in [77]. This method expose the presence of splicing by evaluating inconsistencies in motion blur even under space-variant blurring situations.

The methods discussed above have a few limitations such as the detection methods fail when measures such as blur are used to conceal the sharp edges disturbances after splicing. The requirement of edges to be wide for reliable extraction is also a limitation. Moreover minor and localized tampering may go undetected. Table 2 below gives comparison of few image splicing detection methods.

Table 2. Comparison of Splicing Detection Methods

Method	Extracted Feature	Classifier	Detection Accuracy
Ng et al.[58]	Higher order bi-coherence features	SVM	70%
Fu et al. [59]	Hilbert-Huang Transform & wavelet decomposition based features.	SVM	80.15%
Chen et al. [60]	Moments of wavelet characteristics & 2D phase congruency.	SVM	82.32%
Zhang et al. [69]	moment features from multi size block features(MBDCT) & Image quality Metrics	SVM	87.10%
Zhen Hua et al. [66]	Edge sharpness measure and visual saliency	SVM	96.33%
Fang et al. [67]	sharpness in color edges	LDA	90%
Zhao et al.[70]	Grey level run length number vectors	SVM	94.7%

6. 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. Example is shown below in figure 6; this photograph was released by Iran army to exaggerate their army strength by simply showing four missile in place of three in the original image.

Figure 6. Re-sampled image: Iran army's Missile Launch [http://latimesblogs.latimes.com/babylonbeyond/2008/07/iran-doctored-m.html]

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 challenging task. For this type of forgery two type of modification is done either global or local [78]. 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 are investigated. For illumination and changes in contrast global modification is carried out.

In [79] 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 [80] describes a method that does 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 [81] 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 [80, 82].

[78] 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 & 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. [83] 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 [84] 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 [85] 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 [86]. 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.

Given below in Table 3 a comparison of methods for detection of image retouching is shown.

Table 3. Comparison of Methods for Detection of Retouching Forgery

Method	Extracted Feature	Classifier	Detection Accuracy
Avcibas et al.[79]	First order moment of angular co relation & first order moments of czenakowrki measure.	Linear regression classifier	80.0%
Stamm & Liu[81]	Contrast enhancement, histogram equalization & additive noise	Thresholding classifier	99%
Cao et al. [83]	zero value probability on first order difference map using median filter statistical finger print	Threshold classifier	TP > .85 & >95
Li et al.[84]	Bi-Laplacian filtering	KD- tree matching	-
Cao et al. [85]	zero height gap fingerprints and contrast enhancement mapping	thresholding classifier	100%

Many methods have been proposed and discussed for retouching forgery. Again the limitation here remain that most 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.

7. Lighting Condition

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 [87]. 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 [88] proposed a model based on lighting inconsistencies because of presence of multiple light sources. This model is motivated from earlier model [87] but it generalizes this model by estimating more complex lighting and can be adapted to a single lighting source.

Johnson and Farid [89] estimated 3-D direction to a light source by means of the light's 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.*, [90] 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 [91] described how to estimate a 3-D lighting environment with a low-dimensional model & to approximate the model's parameters from a single image. Inconsistencies in the lighting model are used as indication of forgery. Yingda *et al.*, [92]described a method based on inconsistency in light source direction. The method called as neighborhood method was used to calculate surface normal matrix of image in the blind identification algorithm with detection rate of 87.33%.

Fan *et al.*, [93] proposed a method that described 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.

Carvalho [94] described a method for image forgery detection based on inconsistencies in the color of the illumination. Information from physics and statistical based illuminant 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% is 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. A table of comparison for few of these methods is given below.

Table 4. Comparison of Methods for Detection of Forgeries based on Lighting Conditions

Method	Extracted Feature	Classifier	Detection Accuracy
Chen et al. [90]	Inconsistencies in light source direction using Hesten- Powell multiplier method	Thresholding	83.7%
Yingda et al. [92]	Surface normal matrix of image, light source directions.	Difference between light source direction of local and infinite light source	87.33 %
De Carvalho et al . [94]	Texture and edge features	SVM Metafusion classifier	86%

8. Conclusion

In the last decade many forgery detection techniques have been proposed. In this paper a brief survey of image tampering and forgery detection is presented and the methods have been categorized in Figure 2. 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 we infer that Passive or blind techniques which need no prior information of the image under consideration have a significant advantage of no requirement of special equipments to embed the code into the image at the time of generation, over active techniques.

Aforesaid techniques which have been developed till now are mostly 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. Third is the

problem 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.

References

[1] G. Liu, J. Wang, S. Lian and Z. Wang, "A passive image authentication scheme for detecting region-duplication forgery with rotation", Journal of Network and Computer Applications, vol. 34, no. 5, **(2010)**, pp. 1557–1565.
[2] N. Sebe, Y. Liu, Y. Zhuang, T. Huang and S.-F. Chang, "Blind passive media forensics: motivation and opportunity", Multimedia Content Analysis and Mining, Springer, Berlin/Heidelberg, **(2007)**, pp. 57–59.
[3] B. Mahdian and S. Saic, "Blind methods for detecting image fakery", IEEE Aerosp. Electron. Syst. Mag., vol. 25, **(2010)**, pp. 18–24.
[4] B. L. Shivakumar and S. S. Baboo, "Detecting copy-move forgery in digital images: a survey and analysis of current methods", Global J. Comput. Sci. Technolgy, vol. 10, **(2010)**, pp. 61–65.
[5] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey", Digital investigations, **(2013)**, pp. 226-245.
[6] S. Katzenbeisser and F. A. P. Petitcols, "Information Techniques For Stenography And Digital Watermarking", Norwood, MA: Artec House, **(2000)**.
[7] I. J. Cox, M. L. Miller and J. A. Bloom, "Digital watermarking San Fransisco", CA: Morgan Kaufmann, **(2002)**.
[8] Z. Zhang, Y. Ren, X. J. Ping, Z. Y. He and S. Z. Zhang, "A survey on passive-blind image forgery by doctor method detection", Proc. Seventh Int. Conf. on Machine Learning and Cybernetics, **(2008)**, pp. 3463–3467.
[9] C.-Y. Lin and S.-F. Chang, "Generating Robust Digital Signature for Image/Video Authentication", Multimedia and Security Workshop at ACM Multimedia '98, Bristol, U.K.
[10] C.-S. Lu and H.-Y. Mark Liao, "Structural Digital Signature for Image Authentication: An Incidental Distortion Resistant Scheme", IEEE transactions on multimedia, vol. 5, no. 2, **(2003)**.
[11] H. Bin Zang, C. Yang and X. Mei Quan, "Image Authentication based on digital signature and semi fragile watermarking", Comput and technol, vol. 9, no. 6, **(2004)** November.
[12] X. Wang, J. Xue, Z. Zheng, Z. Liu and N. Li, "Image forensic signature for content authenticity analysis", Vis. Commun. Image R., vol. 23, **(2012)**.
[13] M. Sengupta and J. K. Mandal, "Authentication through Hough transformation generated Signature on G-Let D3 Domain (AHSG)", International Conference on Computational Intelligence: Modeling Techniques and Applications, **(2013)**.
[14] J.-M. Shieh, D.-C. Lou and T. Ming-Chang Chang, "A semi-blind digital watermarking scheme based on singular value decomposition", Computer Standards & Interfaces, vol. 28, **(2006)**, pp. 428–440.
[15] R. Chamlawi, A. Khan and I. Usman, "Authentication and Recovery of images using multiple watermarks", Computers and Electrical Engineering, vol. 36, **(2010)**, pp. 578–584.
[16] Y.-S. Chen and R.-Z. Wang, "Reversible authentication and cross-recovery of images using (t, n)-threshold and modified-RCM watermarking", Optics Communications, vol. 284, **(2011)**, pp. 2711–2719.
[17] G. SchirripaSpagnolo and M. DeSantis, "Holographic watermarking for authentication of cut images", Optics and Lasers in Engineering, vol. 49, **(2011)**, pp. 1447–1455.
[18] L. Rosales-Roldan, M. Cedillo-Hernandez, M. Nakano-Miyatake, H. Perez-Meana and B. Kurkoski "Watermarking-based image authentication with recovery capability using halftoning technique", Signal Processing: Image Communication, vol. 28, **(2013)**, pp. 69–83.
[19] T. T. Ng, S. F. Chang, C. Y. Lin and Q. Sun, "Passive-blind image forensics", Zeng, W., Yu, H., Lin, C.Y., (Eds.), 'Multimedia security technologies for digital rights management', **(2006)**, pp. 383–412.
[20] Z. Zhou and X. Zhang, "Image splicing detection based on image quality and analysis of variance", 2010 Second Int. Conf. on Education Technology and Computer (ICETC), vol. 4, **(2001)**, pp. 242–246.
[21] T.-T. Ng, S.-F. Chang, C.-Y. Lin and Q. Sun, "Passive-blind image forensics", Multimedia security technologies for digital rights. USA: Elsevier, **(2006)**.

[22] W. Luo, Z. Qu, F. Pan and J. Huang, "A survey of passive technology for digital image forensics", Front Comput Sci China, vol. 1, no. 2, **(2007)**, pp. 166–79.
[23] H. Farid, "A survey of image forgery detection", IEEE Signal Proc Mag., vol. 2, no. 26, **(2006)**, pp. 6–25.
[24] J. A. Redi, W. Taktak and J. L. Dugelay, "Digital image forensics: a booklet for beginners", Multimedia Tools Appl., vol. 51, no. 1, **(2011)**, pp. 133–162.
[25] W. Lu, W. sun, J.-W. huang and H.-T. Lu, "Digital image forensics using statistical features and neural network classifiers", Proceedings of seventh international conference on machine learning and cybernetics, Kunming, **(2008)** July 12-15.
[26] D. Fu, Y. Shi and W. Su, "Detection of image splicing based on Hilbert-Huang transform and moments of characteristic functions with wavelet decomposition", Proc. of International workshop on digital watermarking, **(2006)**, pp. 177–87.
[27] W. Chen, Y. Shi and W. Su, "Image splicing detection using 2-d phase congruency and statistical moments of characteristic function", Proc. Of SPIE electronic imaging: security, steganography, and watermarking of multimedia contents, **(2007)**.
[28] N. Khanna, GT-C. Chiu, J. P. Allebach and E. J. Delp, "Forensic techniques for classifying scanner, computer generated and digital camera images", Proc. IEEE International conference on acoustics, speech and signal processing, **(2008)**, pp. 1653–6.
[29] Z. Fang, S. Wang and X. Zhang, "Image splicing detection using camera characteristic inconsistency", Proc. of International conference on multimedia information networking and security, **(2009)**, pp. 20–4.
[30] G. Muhammad, M. Hussain, K. Khawaji and G. Bebis, "Blind copy move image forgery detection using dyadic uncedimated wavelet transform", Proc. of 17th International conference on digital signal processing, **(2011)**, pp. 1–6.
[31] E. Gopi, N. Lakshmanan, T. Gokul, S. Ganesh and P. Shah, "Digital image forgery detection using artificial neural network and auto regressive coefficients", Proc. Canadian conference on electrical and computer engineering, **(2006)**, pp. 194–7.
[32] M. Ghorbani, M. Firouzmand and A. Faraahi, "DWT-DCT (QCD) based copy-move image forgery detection", Proc. of 18th International conference on systems, signals and image processing (IWSSIP), **(2011)**, pp. 1–4.
[33] J. Fridrich, D. Soukal and J. Lukas, "Detection of copy-move forgery in digital images", Proc. of digital forensic research workshop, **(2003)**, pp. 55–61.
[34] E. Ardizzone, A. Bruno and G. Mazzola, "Copy-move forgery detection via texture description", MiFor'10 – Proceedings of the 2010 ACM Workshop on Multimedia in Forensics, Security and Intelligence, Co-located with ACM Multimedia, **(2010)**, pp. 59–64.
[35] S. Bravo-Solorio and A. K. Nandi, "Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics", Signal Proc., vol. 91, no. 8, **(2011)**, pp. 1759–1770.
[36] J. Fridrich, D. Soukal and J. Lukas, "Detection of copy-move forgery in digital images", Proc. of digital forensic research workshop, **(2003)**, pp. 55–61.
[37] A. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions", Technical Report TR2004-515. Department of Computer Science, Dartmouth College, **(2004)**.
[38] A. Langille and M. Gong, "An efficient match-based duplication detection algorithm", Proc. of the 3rd Canadian conference on computer and robot vision, **(2006)**, pp. 64.
[39] E. Gopi, N. Lakshmanan, T. Gokul, S. Ganesh and P. Shah, "Digital image forgery detection using artificial neural network and auto regressive coefficients", Proc. Canadian conference on electrical and computer engineering, **(2006)**, pp. 194–7.
[40] A. Myna, M. Venkateshmurthy and C. Patil, "Detection of region duplication forgery in digital images using wavelets and log-polar mapping", Proc. of the International conference on computational intelligence and multimedia applications ICCIMA, **(2007)**, pp. 371–7.
[41] K. XiaoBing and W. ShengMin, "Identifying tampered regions using singular value decomposition in digital image forensics", Proc. of International conference on computer science and software engineering, **(2008)**, pp. 926–30.
[42] H. Lin, C. Wang and Y. Kao, "An efficient method for copy-move forgery detection", Proc. Eighth WSEAS Int. Conf. on Applied Computer and Applied Computational Science, **(2009)**, pp. 250–253.
[43] M. Bashar, K. Noda, N. Ohnishi and K. Mori, "Exploring duplicated regions in natural images", IEEE Trans Image Process, **(2010)**, pp. 1–40.
[44] P. Sutthiwan, Y. Q. Shi, S. Wei and N. Tian-Tsong, "Rake transform and edge statistics for image forgery detection", Proc. IEEE International conference on multimedia and Expo (ICME), **(2010)**, pp. 1463–8.
[45] G. Liu, J. Wang, S. Lian and Z. Wang, "A passive image authentication scheme for detecting region-duplication forgery with rotation", J Netw. Comput. Appl., vol. 34, **(2011)**, pp. 1557–1565.
[46] M. A. Sekeh, M. A. Marof, M. F. Rohani and M. Motiei, "Sequential straightforward clustering for local image block matching", World Acad. Sci. Eng. Technol., vol. 50, **(2011)**, pp. 774–778.

[47] Y. Huang, W. Lu, W. Sun and D. Long, "Improved DCT-based detection of copy-move forgery in images", Forensic Sci. Int., vol. 3, **(2011)**, pp. 178–184.
[48] P. Xunyu and L. Siwei, "Region duplication detection using image feature matching", IEEE Trans Inf Forensics Security, vol. 5, no. 4, **(2011)**, pp. 857–67.
[49] P. Kakar and N. Sudha, "Exposing postprocessed copy-paste forgeries through transform-invariant features", IEEE Trans Inf Forensics Security, vol. 7, no. 3, **(2012)**, pp. 1018–28.
[50] G. Muhammad, M. Hussain and G. Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform", Digital Investigation, vol. 9, **(2012)**, pp. 49–57.
[51] H. Shao, T. Yu, M. Xu and W. Cui, "Image region duplication detection based on circular window expansion and phase correlation", Forensic Science International, vol. 222, **(2012)**, pp. 71–82.
[52] G. Lynch, F. Y. Shih and H.-Y. Mark Liao, "An efficient expanding block algorithm for image copy-move forgery detection", Information Sciences, vol. 239, **(2013)**, pp. 253–265.
[53] M. Akbarpour Sekeh, M. Aizaini Maarof, M. Foad Rohani and B. Mahdian, "Efficient image duplicated region detection model using sequential block clustering", Digital Investigation, vol. 10, **(2013)**, pp. 73–84.
[54] I. Amerini, L. Ballan, R. Caldelli, A. DelBimbo, L. DelTongo and G. Serra, "Copy-move forgery detection and localization by means of robust clustering with J-Linkage", Signal Processing: Image Communication, vol. 28, **(2013)**, pp. 659–669.
[55] J. Zhao and J. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD", Forensic Science International, vol. 233, **(2013)**, pp 158–166.
[56] H. Farid, "Detecting digital forgeries using bispectral analysis", Technical Report AIM-1657. AI Lab, Massachusetts Institute of Technology, **(1999)**.
[57] T. Ng and S. Chang, "A model for image splicing", Proc. of IEEE International conference on image processing (ICIP), **(2004)**, pp. 1169–72.
[58] T. Ng, S. Chang and Q. Sun, "Blind detection of photomontage using higher order statistics", Proc. IEEE International symposium on circuits and systems (ISCAS), **(2004)**, pp. 688–91.
[59] D. Fu, Y. Shi and W. Su, "Detection of image splicing based on Hilbert-Huang transform and moments of characteristic functions with wavelet decomposition", Proc. of International workshop on digital watermarking, **(2006)**, pp. 177–87.
[60] W. Chen, Y. Shi and W. Su, "Image splicing detection using 2-d phase congruency and statistical moments of characteristic function", Proc. Of SPIE electronic imaging: security, stegnography, and watermarking of multimedia contents, **(2007)**.
[61] Z. Zhang, J. Kang and Y. Ren, "An effective algorithm of image splicing detection", Proc. International conference on computer science and software engineering, **(2008)**, pp. 1035–9.
[62] T. Ng and M. Tsui, "Camera response function signature for digital forensics - part I: theory and data selection", Proc. IEEE workshop on information forensics and security, **(2009)**, pp. 156–160.
[63] T.-T. Ng, "Camera response function signature for digital forensics – part II: signature extraction", Proc. IEEE workshop on information forensics and security, **(2009)**, pp. 161–5.
[64] L. Qingzhong and H. Andrew, "A new approach for JPEG resizes and image splicing detection", Proc. ACM multimedia and security workshop, **(2009)**,pp. 43–8.
[65] W. Wang, J. Dong and T. Tan, "Effective image splicing detection based on image chroma", Proc. IEEE International conference on image processing, **(2009)**, pp. 1257–60.
[66] Q. Zhenhua, Q. Guoping and H. Jiwu, "Detect digital image splicing with visual cues", Proc. International workshop on information hiding, **(2009)**, pp. 247–61.
[67] Z. Fang, S. Wang and X. Zhang, "Image splicing detection using color edge inconsistency", 2010 Int. Conf. on Multimedia Information Networking and Security (MINES), **(2010)**, pp. 923–926.
[68] X. Li, T. Jing and X. H. Li, "Image splicing detection based on moment features and Hilbert-Huang transform", 2010 IEEE Int. Conf. on Information Theory and Information Security (ICITIS), **(2010)**, pp. 1127–1130.
[69] W. Zhang, X. Cao, Y. Qu, Y. Hou, H. Zhao and C. Zhang, "Detecting and extracting the photo composites using planar homography and graph cut", IEEE Trans Inf Forensics Security, vol. 5, no. 3, **(2010)**, pp. 544–55.
[70] X. Zhao, J. Li, S. Li and S. Wang, "Detecting digital image splicing in chroma spaces", Proc. International workshop on digital watermarking, **(2010)**, pp. 12–22.
[71] Q. Liu, X. Cao, C. Deng and X. Guo, "Identifying image composites through shadow matte consistency", IEEE Trans Inf Forensics Security, vol. 6, no. 3, **(2011)**, pp. 1111–22.
[72] X. Wu and Z. Fang, "Image Splicing Detection Using Illuminant Color Inconsistency", International Conference on Multimedia Information Networking and Security (MINES), **(2011)**, pp. 600-603.
[73] Z. He, W. Sun, W. Lu and H. Lu c, "Digital image splicing detection based on approximate run length", Pattern Recognition Letters, vol. 32, **(2011)**, pp. 1591–1597.

[74] Z. He, W. Lu, W. Sun and J. Huang, "Digital image splicing detection based on Markov features in DCT and DWT domain", Pattern Recognition, vol. 45, **(2012)**, pp. 4292–4299.
[75] R. Whidiana Ciptasari, K. Hyune Rhee and K. Sakurai, "Exploiting reference images for image splicing verification", Digital Investigation, vol. 10, **(2013)**, pp. 246–258.
[76] R. De Carvalho, P. Angelopoulou and R. de Rezende Rocha, "Exposing Digital Image Forgeries by Illumination Color Classification", IEEE Transactions on Information Forensics and Security, **(2013)**, pp 1182–1194.
[77] R. Rao and S. Rajagopalan, "Harnessing Motion Blur to Unveil Splicing", IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, **(2014)**, pp. 583-595.
[78] G. Boato, F. G. B. D. Natale and P. Zontone, "How digital forensics may help assessing the perceptual impact of image formation and manipulation", Proc. Fifth Int. Workshop on Video Processing and Quality Metrics for Consumer Electronics – VPQM 2010, **(2010)**.
[79] I. Avcibas, S. Bayram, N. Memon, M. Ramkumar and B. Sankur, "A classifier design for detecting image manipulations", Proc. IEEE Int. Conf. on Image Processing, **(2004)**, pp. 2645–2648.
[80] M. C. Stamm and K. J. R. Liu, "Blind forensics of contrast enhancement in digital images", Proc. 15th IEEE Int. Conf. Image Processing 2008, (ICIP'2008), **(2008)**, pp. 3112–3115.
[81] M. C. Stamm and K. J. R. Liu, "Forensic estimation and recnstruction of a contrast. Enhancement mapping", Proc. IEEE Int. Conf. Acoustics speech and signal processing (ICASSP), **(2010)**, pp. 1698-1701.
[82] M. Stamm and K. J. R. Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints", IEEE Trans. Inf. Forensics Secur., vol. 5, no. 3, **(2010)**, pp. 492–506.
[83] G. Cao, Y. Zhao and R. Ni, "Forensic estimation of gamma correction in digital images", Proc. 17th IEEE Int. Conf. on Image Processing, (ICIP'2010), **(2010)**, pp. 2097–2100.
[84] X. F. Li, X. J. Shen and H. P. Chen, "Blind identification algorithm for the retouched images based on bi-Laplacian", Comput. Appl., vol. 31, **(2011)**, pp. 239–242.
[85] G. Cao, Y. Zhao, R. Ni and X. Li, "Contrast Enhancement-Based Forensics in Digital Images", IEEE Transactions on Information Forensics and Security, vol. 9, no. 3, **(2014)**, pp. 515-525.
[86] G. Chierchia, G. Poggi, C. Sansone and L. Verdoliva, "A Bayesian-MRF Approach for PRNU-Based Image Forgery Detection", Information Forensics and Security, IEEE Transactions, vol. 9, no. 4, **(2014)**, pp. 554-567.
[87] M. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting", Proc. ACM multimedia and security workshop, **(2005)**, pp. 1–10.
[88] M. Johnson and H. Farid, "Exposing digital forgeries in complex lighting environments", IEEE Trans Inf Forensics Security, vol. 3, no. 2, **(2007)**, pp. 450–61.
[89] M. Johnson and H. Farid, "Exposing digital forgeries through specular highlights on the eye", Proc. International workshop on information hiding, **(2007)**, pp. 311–25.
[90] H. Chen, S. Xuanjing and Y. Lv, "Blind Identification Method for Authenticity of Infinite Light Source Images", Fifth International Conference on Frontier of Computer Science and Technology (FCST), **(2010)**, pp. 131-135.
[91] E. Kee and H. Farid, "Exposing digital forgeries from 3-D lighting environments", IEEE International Workshop on Information Forensics and Security (WIFS), **(2010)**, pp. 1-6.
[92] L. Yingda, S. Xuanjing and C. Haipeng, "An improved image blind identification based on inconsistency in light source direction", Supercomput, vol. 58, no. 1, **(2011)**, pp. 50–67.
[93] W. Fan, K. Wang, F. Cayre and Z. Xiong, "3D Lighting-Based Image Forgery Detection Using Shape-From-Shading", 20th European Signal Processing Conference EUSIPCO, **(2012)**, pp. 1777-1781.
[94] T. J. De Carvalho, C. Riess, E. Angelopoulou and H. Pedrini, "Exposing Digital Image Forgeries by Illumination Color Classification", IEEE Transactions on Information Forensics and Security, vol. 8, no. 7, **(2013)**, pp. 1182–1194.

Authors

Saba Mushtaq received her B.E. degree in Electronics and Communications Engineering from Kashmir University, India in 2008. She obtained her M. Tech. degree in Communication and Information Technology from National Institute of Technology, Srinagar, India in 2012. She joined NIT Srinagar in September 2012, as a faculty member. Presently she is a research scholar at NIT Srinagar in Department Of Electronics and Communication.Her research interests are Image Processing and Biometrics. Saba can be reached at sab.mushtaq@gmail.com.

Ajaz Hussain Mir has done his B.E in Electrical Engineering with specialization in Electronics & Communication Engineering (ECE) .He did his M.Tech in Computer Technology and Ph.D both from IIT Delhi in the year 1989 and 1996 respectively. He is Chief Investigator of Ministry of Communication and Information Technology, Govt. of India project: Information Security Education and Awareness (ISEA). He has been guiding Ph.D and M.Tech thesis in Security and other related areas and has a number of International publications to his credit Presently he is working as Professor in the Department of Electronics & Communication Engineering at NIT Srinagar, India. His areas of interest are Biometrics, Image processing, Security, Wireless Communication and Networks.