Volume 6, Issue 3, March 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Analysis of Popular Passive Techniques for Forgery Detection in Digital Images

[1]Manish Deoli[*], [2]Jyoti Joshi
[1] Department of Information Technology, HNBGU, Srinagar Garhwal, Uttarakhand, India
[2] Tadpole Store, Okhla Phase-I, New Delhi, India

Abstract*— In *the present world, digital images and videos are our main source of information and these images and videos can be tempered or manipulated to conceal some meaningful information by the use of largely available powerful and sophisticated image editing tools. So in this era of illusions, verifying the authenticity of images and locating the tempering regions without using any prior knowledge is an important area of research. In this paper, a comprehensive survey of some decent developments in passive forgery detection techniques, in the past few years has reviewed.

Keywords—passive forgery detection techniques; image forensic; copy move forgery detection;

I. INTRODUCTION

The authenticity of digital images has a fundamental need of many areas, including: forensic investigation, criminal investigation, insurance processing, surveillance systems, intelligence services, medical images and journalism. But, in today's digital world, it is very easy to create, alter and modify the information depicted by an image without leaving any visual evidence of tempering. This is mainly because of the existing powerful digital image technologies. Despite this, there is no such system exists which can detect forgery efficiently and correctly. A good example of image forgery is shown in the fig.1.

In the past few years passive digital image tempering detection field has been focused by the research community. This is proofed by fig.2. which depicts the number of review and research papers related digital image tempering detection that have been published in IEEE, Elsevier and springer conferences and journals over the last 10 years. Law enforcement has needed to stay aware of latest technological advances and use of these in crime investigation. The Scientific Working Group on Imaging Technology (SWGIT) has define guidelines to law enforcement agencies and others in the criminal justice system regarding the best practices for photography, videography and video and image analysis (https://www.swgit.org/documents,2012).Guidelines regarding the best use of various imaging technologies has provided by the release of documents such as the SWGIT best practice document.

A typical categorization of various image tampering detection techniques is presented in section 1.1 and then a workflow structure of image forgery detection is presented in section 1.2. This paper mainly focuses on the various blind or passive image tempering detection techniques.

A. Categorization of Image Forgery

Detection of image fakery is used to verify the integrity of digital images. The integrity of image can be verified by two methods.

(1) Active or intrusive (2) Passive or blind

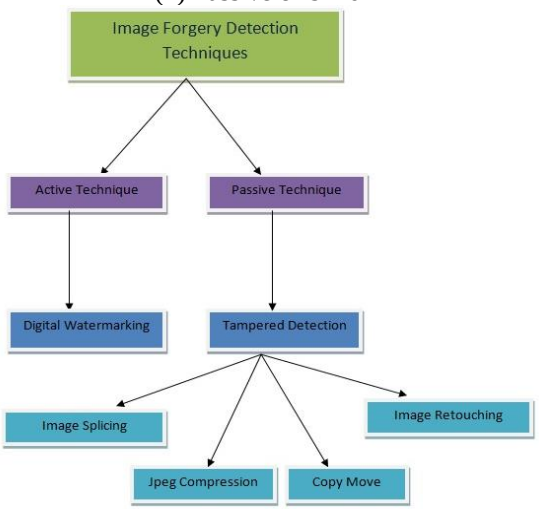

Fig.1 Classification of image forgery detection techniques

Active method requires some known digital information to be embedded in the original image. Authenticity of such images can be verified by comparing the code obtained from the image with the original embedded information. Watermarking and digital signature are some examples of active method. So before the distribution of the image this method requires dedicated hardware or software to embed the authentication code inside the original image.

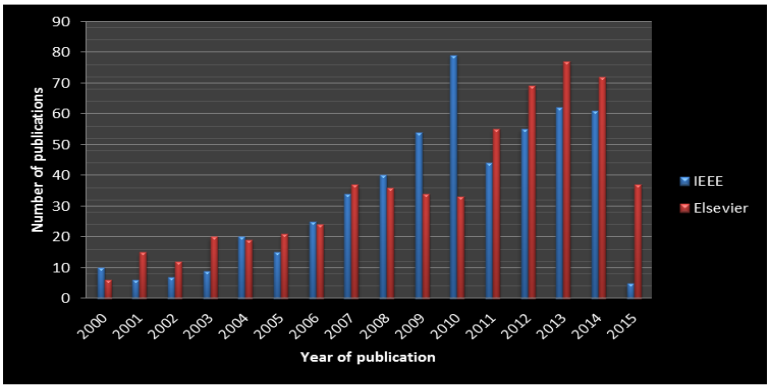

Fig.2. Number of publications over last 16 years.

On the other hand, passive method does not require any prior embedding of information in the original image. It is based on the fact that, some specific statistical properties of an image are highly disrupted when an attempt of tempering is made. This leads to introduction of various inconsistencies in the image. These inconsistencies are strongly used to detect the forgery. This is a very popular technique as it does not need any prior information about the image.

Many surveys have been published on digital image forgery detection in the past few years. Still most of the existing algorithms are untouched. This paper covers all the aspects of existing algorithms and the recent developments.

B. Workflow structure of image forgery detection techniques

Passive detection techniques take every image as a forged or tempered image. After performing a particular series of operations the image is classified into two categories: authentic images and forged images. We describe here a common workflow structure of passive image forgery detection techniques which comprises the following steps:

1) Image preprocessing: In this first step some preprocessing operations are performed on the image. As most of the method require gray scale images so the colored image is first converted into a gray-scale image. Then some other necessary operations like cropping and frequency domain transformations like DCT or DWT are also performed to enhance future processing. This step is common in both the block-based methods and key-point based methods.

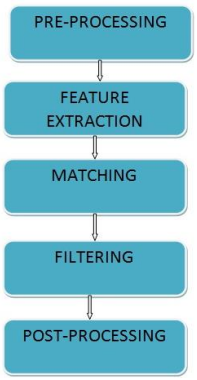

Fig.3 Workflow structure of forgery detection techniques.

2) Feature extraction: In this step a set of sensitive features (like color, texture, edge etc.) are extracted for each part of the image. These features are mainly used to distinguish each part from all others. Several methods are used for feature extraction: frequency domain, transform based, or spatial domain. After extraction these features are stored in a feature vector. One of the desirable characteristics of selected features and constructed feature vector should be with low dimension, which will reduce the computational complexity.

3) Matching: After feature extraction feature vectors are sorted so that the most similar feature vectors appear in consecutive rows. For block-based methods most researchers use lexicographic sorting. Whereas some other use k_d-tree method to find approximate nearest neighbors. k_d-tree method is mostly used in key-point based algorithms. It has been shown that k_d-tree approach is better than the lexicographic approach but the memory requirement for k_d-tree are significantly higher.

4) Filtering: Filtering methods are used to increase the probability of correct matches and also to reduce the probability of false matches. Euclidean distance is used by most of the algorithms between matched feature vectors. As neighbor pixels have similar features which may be leads to false matching. Bravo-Solorio and Nandi proposed an algorithm in which correlation coefficient is used as matching factor between two feature vectors. The purpose of this step is to categories images into two categories: original and forged images.

5) Post processing: This step mainly checks the accuracy of the technique against some common image post processing operations such as rotation, scaling and JPEG recompression and used to localize the exact forged region in the image.

II. COPY MOVE FORGERY

Now a day, many image tempering techniques are available which are frequently used to alter the information represented by an image. Copy-move forgery is one of the commonly used image tempering techniques, in which a selected part of image is copied and pasted over some other non-intersecting part of the same image, in order to hide an element, duplicate some features or highlight a particular object. Duplicate parts possess the identical properties since they come from the same image. An example of copy-move forgery is illustrated in Fig.4.

Fridrich et al. (2003) made first attempt to detect tampered areas of an image. In this paper a discrete cosine transform (DCT) based block matching approach is used to detect copy-move forgery. The author first divides the whole image into a fixed size overlapping blocks and then calculates DCT coefficient corresponding each block and thus formed a DCT feature matrix. Then use lexicographic sorting to identify identical rows of matrix. This method exactly detects the duplicated region in MNlog2 (MN) steps in an image of size M*N. But in some sophisticated manipulation like blurring or random noise addition it is hard to detect the duplicity [13].

Fig.4 Example of copy-move forgery

A method based on principle component analysis (PCA), proposed by **Popescu and Farid (2004).** In this method, due to the properties of PCA the number of features required to represent a block were reduced about by half as compared to the number of features used by Fridrich. The number of computations required are O(NtN log N), where Nt is the dimension of corresponding PCA representation and N the number of pixels. So this method has better time complexity and has better immunity to random noise and JPEG compression. But the method is not robust enough against small rotations of copy-moved regions [44].

Luo et al. (2006) proposed a more robust method against stronger attacks (like lossy compression, noise contamination, blurring and combination of these) and claims a better computational complexity. This is also a block matching algorithm. In this method seven characteristics features Cj (j=1,2,….,7) are computed for each overlapping block of an image of size M*N. In which C1, C2, C3 are average red, green and blue components respectively. Then each block is divided into two equal parts in four directions as shown in the fig.3 and corresponding features are computed in each direction as C4, C5, C6 and C7 respectively. After that the copied regions are identified based on some preset threshold values [32].

Langille and Gong (2006) proposed a method based on Zero mean Normalized Cross Correlation (ZNCC). In this method for each block Bi the cross correlation between Bi and B_j (for j=i+1,….,i+N_s) is computed then the computed result is compared against a ZNCC threshold value. For searching the blocks with similar intensity patterns a k-dimensional tree method was used. The proposed algorithm has a computational complexity of $O(N_bN_s)$, where N_b= number of blocks and N_s= neighborhood search size and $N_s<<N_b$. This method is quite robust in the presence of minor noise and intensity variations caused by lossy JPEG compression [23].

Another method to detect copy-move forgery using auto regressive coefficient for feature extraction and artificial neural network (ANN) for classification is proposed by **Gopi et al. (2006)**. 300 feature vectors collected from different digital images are used to train the ANN and the ANN is tested with another 300 feature vectors. This technique results 77.67% accuracy when manipulated images are used to train the ANN and 94.83% accuracy when a database of forged images is used [17].

Mahdian and Saic (2007) described a method based on detection of blur moment invariant, PCA and K_d-tree. This algorithm uses 24 blur moment invariants up to the seventh order to create the feature vector. Then k_d-tree method is used to sort the feature vector. Due to the large computational steps this algorithm has a large computational time (for a RGB image of size 640*480 average run time is 30 min with a block size of 24 and similarity threshold of 0.98) [36].

A method based on log-polar coordinate and wavelet transform (DWT) is proposed by **Myna et al. (2007)**. This method consists of two phases, in the first phase DWT of the original image is calculated up to the specified level then the image is divided into a fixed size overlapping blocks and these blocks are mapped on the log-polar coordinates to obtain a matrix corresponding to each block. To bring similar rows closer lexicographic sorting is used. Phase correlation is used as the similarity criterion. In the second phase, the saved block information is iteratively compared at each level of DWT. This algorithm works better even the pasted region has scaled and rotated [38].

Dybala et al. (2007) developed a method based on filtering operation and nearest neighbor search. In this method first the filters (like laplacian) are used to smoothen the pasted region. Then a K_d-tree method is used for clustering of the most similar blocks. Root mean square error is used as matching criterion. The method shows a reasonable robustness to high quality image compression [8].

Li et al. (2007) proposed a method based on Discrete Wavelet transform (DWT) and Singular Value Decomposition (SVD). In which SVD is used for feature collection and DWT is used to detect forged region. Sorting of duplicate regions is performed lexicographically. This method works even if the image is highly compressed or edge processed [25].

A JPEG based copy-move forgery detection method is proposed by **Li et al. (2008).** The method used Block Artifact Grid (BAG) mismatches for forgery detection. A DCT grid is the combination of horizontal lines and vertical lines that partition an image into blocks. A BAG is the grid embedded in an image where block artifact appears. In an undistorted image DCT grid and BAG match together. This fact is used to detect pasted region. When a BAG mismatch is detected the image is declared forged. This method works better even the image is truncated or multi compressed.

Huang et al. (2008) proposed a novel approach based on Scale Invariant Feature Transform (SIFT). In this method first the SIFT descriptors of an image are extracted. SIFT descriptors are invariant to changes in illumination, rotation, scaling etc. This key feature of SIFT descriptors is explore to detect the copy-move forgery. So SIFT features of copied and pasted region are matched to detect the tempering. This method performs very well up to JPEG compression 40 and SNR 20db. But problem of false positive is detected for very small block size [19].

A method based on Fourier-Mellin Transform (FMT) has proposed by **Bayram et al. (2009)**. In this method the features of overlapping blocks are extracted using FMT. FMT features are robust against rotation, scaling, blurring, noise addition and JPEG compression. Lexicographic sorting is used to collect similar blocks. Counter bloom filters are also used instead of lexicographic sorting to compare the similar blocks [2].

Another method based on radix sort is proposed by **Lin et al. (2009)** to increase the efficiency of copy-move forgery detection algorithm. The image is divided into the overlapping blocks of fixed size. The feature vector corresponding to each block is computed then radix sort is used to identify the similar blocks instead of lexicographic sorting. The author claims efficiency in the range of 94-98% when tested against various image manipulation techniques [27].

Bashar et al. (2010) suggested a method based on Discrete Wavelet Transform (DWT) and Kernel Principal Component Analysis (KPCA). KPCA is used for feature collection and lexicographic sorting is used to cluster the similar feature blocks. This method is robust against manipulations like translation-flip and translation-rotation of duplicate region [1].

A method for color image forgery detection is proposed by **Sutthiwan et al. (2010)**. Image features are extracted using rake transform from image luminance and using edge statistics from image Chroma. This algorithm collects Multi-size Block Discrete Cosine Transform-Markov Process (MBDCT-MP) features from Y-channel. A degree 2 polynomial kernel is employed with Support Vector Machine (SVM) for classification. The algorithm results 99% accuracy against various image manipulation techniques.

Liu et al. (2011) proposed a robust method to detect the cloning region with rotation by using the circle block and the Hu moments. To reduce the computation complexity first four Hu moments are used for feature extraction from the circle blocks in low frequency part of Gaussian pyramid decomposition.

Muhammad et al. (2011) suggested a passive copy-move forgery detection method using Dyadic Wavelet Transform (DyWT) in which both the LL and HH sub bands are used to find the similarity between the blocks of image. This algorithm results 95.9% accuracy [37].

Ngueyen and Katzenbeisser (2012) suggest a robust method using radon transformation and phase correlation. Radon transform is used for feature extraction and phase correlation is used to match copied blocks. This technique is robust against rotation with angles smaller than 4◦ and Gaussian noise addition with SNR values larger than 35 dB [43].

A novel technique based on transform invariant features to detect copy move forgery with post processing based on MPEG-7 image signature tool is proposed by **Kakar and Sudha (2012)**. The algorithm is quite complex but due to stringent multi-hypothesis matching process false positive rate is minimized [22].

III. IMAGE SPLICING OR IMAGE COMPOSITES

Image splicing is the process of making a composite image by cutting and joining two or more images. The spliced image may introduce a number of sharp transitions such as lines, edges and corners. It is also a very simple and frequently used image tempering techniques. Many algorithms are proposed to detect this type of forgery some of them are reviewed here.

Farid (1999) proposed a method based on bispectral analysis. This method is capable of detecting an un-natural higher-order correlation introduced into a signal by tempering process. It is successfully used to detect human speech splicing [9].

Ng and Chang (2004) introduce a method by the use of bicoherence magnitude and phase features with detection accuracy of 70%. Later the same authors developed a technique based on bicoherence to detect the abrupt spilicing discontinuity [40].

Fu et al. (2006) proposed a method to distinguish spliced images from the authentic images by using Hilbart-Huang (HHT) transform to generate features for classification and statistical natural image model [15].

Hsu and Chang (2006) presented a method which consists of two phases, in the first phase suspicious splicing areas are detected for an image and in second phase geometry invariants from pixels of each region are computed and the

Camera Response Function (CRF) is estimated based on these geometry invariants. The cross fitting errors are fed into an SVM classifier [18].

A method which extracts image features from moments of wavelet characteristics functions has proposed by **Chen et al. (2007)**. 2-D phase congruency, which is a sensitive measure of sharp transition, is used for image splicing detection [5].

Shi et al. (2007) constructed a model to detect image splicing based on statistical features extracted from the test images and 2-D arrays generated by applying the Multi-size Block Discrete Cosine Transform (MBDCT) [49].

Johnson and Farid (2007) introduced a method based on estimating cameras intrinsic parameters from the image of a person's eyes to detect compositing of two or more people into a single image. Inconsistencies in the estimated principal point were used as evidence of tempering [20].

Another method based on moment features extracted from the Multi-size Block Discrete Cosine Transform (MBDCT) and Image Quality Metrics (IQMs) extracted from the given test image has proposed by **Zhang et al. (2008)** to detect splicing. Extracted features are very sensitive to spliced image [59].

Ng and Tsui (2009) proposed a method based on the extraction of CRF signature using linear geometric invariants from the single image. An edge-profile-based method for extracting CRF signature from a single image has proposed by **Ng T.T. (2009)** to extract edge profiles reliably it requires straight edges and edges should be wide enough [41, 42].

QingZhong and Andrew (2009) proposed a two phase method to successfully detect image splicing. In first phase density features of DCT coefficient has exploited to extract neighboring joints. In the second phase SVM is applied to the features extracted in the first phase to detect image splicing [47].

Image splicing detection method based on Order Statistic Filters (OSF) has proposed by **Zhenhua et al. (2009).** In this method OSF is used to detect sharpness and visual saliency is used for feature extraction [61].

Yu-Feng and Shih-Fu (2010) proposed a method based on CRF for image splicing detection. First a test image is automatically segmented into distinct arbitrarily shaped parts. One CRF is calculated from each segmented part using geometric invariants from locally planar irradiance points (LPIPs) [56].

Zhang et al. (2010) suggest a method using planar homography constraint to locate the forged region. Graph cut based extraction method with online parameter selection has used to estimate the tempered region [58].

A method using chroma spaces has presented by **Zhao et al. (2010)**. In this method four gray level run-length run number (RLRN) vectors extracted with different directions from de-correlated channels. These RLRN vectors are used as distinguishing features for image splicing detection. SVM is used as a classifier [60].

Liu et al. (2011) suggested a technique using photometric consistency of illumination in shadows by formulating color characteristics of shadows measured by the shadow matte value [29].

IV. IMAGE TEMPERING DETECTION BY JPEG COMPRESSION FEATURES

JPEG is the most commonly used lossy compression standard for digital images. Digital cameras particularly produce images using this standard. To detect whether a bitmap image has been previously JPEG compressed or not is an important issue in image forensics and plays a very important role in image forgery detection.

Fridrich and Lukas (2003) proposed a method for estimating the primary quantization matrix from a double compressed JPEG image. The neural network classifier based approach is the most effective among all the three proposed approaches. In order to obtain accurate results sufficiently large images are required and due to the insufficient statistics it is hard to estimate quantization step for higher-frequency coefficients [11].

Popescu (2004) proposed a method to detect whether a JPEG image has double compressed or not by checking histogram of DCT coefficients. Double JPEG compression results double quantization of the DCT coefficients that introduces some special artifacts which are visible in the histogram of these coefficients. But this method is not reliably able to detect the forgery in which images are compressed first with high quality and then with a comparatively lower quality [46].

Neelamani et al. (2003) developed a technique based on DCT coefficient structure created by previous JPEG operation as JPEG compressed images shows a periodic behavior because of quantization. In this technique DCT is used to estimate JPEG compression history of image which includes color transformation, subsampling and the quantization table used during previous JPEG compression [39].

Jufeng et al. (2006) suggested a technique based on the double quantization effect of DCT coefficient. The effect of double quantization hidden among the DCT coefficients is used to identify the forged JPEG image and to locate the forged part. This method fails when the unforged part of the original image is not a JPEG image and when the image is heavily compressed after forgery [21].

Fu et al. (2007) proposed a modal based on Benford's law to obtain the probability distribution of the first digits of block-DCT and JPEG coefficients. The generalized Benford's law can be used to detect JPEG compression of images in bitmap format, to calculate JPEG compression factor Q for JPEG compressed bitmap image and for the identification of double compressed JPEG images [14].

Tjoa et al. (2007) proposed a method by detecting which transform was used in compression. In this method histograms of coefficients sub bands are used to determine the nature of the transform method. The three blocks transforms-DCT, Hadamard and Slant and three wavelet transforms-5/3, 9/3 and 17/11 were successfully determined using this method [51].

Tjoa et al. (2007) proposed a blind method to accurately estimate the block size in digital images. This method accurately classifies an image as block processed and results a probability of 95% and the probability of false detection is 7.4%, without making any assumption about the block size [52].

Luo et al. (2008) proposed a method based on maximum-likelihood estimation. Block-size is estimated using morphological operation. The author claims 40 % accuracy improvement in comparison with existing gradient-based method [30].

Fridrich and Penvy (2008) proposed a method based on support vector machine for classification and first order statistics of individual DCT modes of low-frequency DCT coefficients for feature collection, to detect double compressed JPEG images [12].

Qu et al. (2008) proposed a method based on the shifted double JPEG compression (SD-JPEG). Here author uses SD-JPEG for detecting whether a given JPEG image has ever been double compressed with inconsistent block segmentation. In this method total 13 characteristic features which represent the asymmetric characteristic of the independent value map, are then passed to a SVM classifier which results a detection accuracy of 90% at quality factor of 95 [48].

A machine learning technique based on markov process and transition probability matrix (TPM) has proposed by **Chunhua et al. (2008)** to detect whether an image has double JPEG compressed or not. Markov process and TPM is applied to the difference JPEG 2-D second order statistics arrays, which identify the artifacts left with double JPEG compression [7].

Li et al. (2008) proposed a method based on the mode based first digit features (MBFDF) to detect double JPEG compression in an image. The author utilizes probabilities of the first digits of quantized DCT coefficients from individual AC (alternate current) modes. Fisher linear discriminant (FLD) is used as a classifier to correctly identify the forgery [24].

Weihai et al. (2008) proposed a method to detect copy-move forgery in the JPEG images based on the BAG information mismatch. But this algorithm suffers from a high computation complexity [55].

A method based on double JPEG2000 compression has proposed by **Zhang et al. (2009)** to identify and locate the forged regions in a digital image. Double JPEG2000 compression results to double quantization of the sub band DWT coefficients, which introduces special artifacts in the image; this fact is exploited by the author in this technique. These artifacts are visible in the histogram of Fourier transform of DWT coefficients [57].

Fraid (2009) suggested an approach to detect image splicing created by different JPEG compression quality on low quality images and capable of detecting small regions that have been altered. This technique identify whether a part of the image has compressed at a lower quality compared to the rest of the image. This technique is advantageous only when the forged part of the image is of lower quality compared to the image into which it was inserted [10].

Mahdian and Saic (2009) suggest a technique based on histograms of DCT coefficients and SVM to identify double compressed JPEG image. This method uses the fact that change in a JPEG image brings some distortion such as periodic zeros and double peaks. This approach suffers from high false positive detection for natural images which has imperfect histograms [35].

Luo et al. (2010) presented a technique based on the analysis of the effect of quantization, rounding and truncation errors on the quantization table of a JPEG image, to estimate if a bitmap image has previously JPEG compressed or not. This method results 90% accuracy even if the image size has decreases to 8*8 with a quality factor of 95 [31].

Wang et al. (2010) proposed a technique to detect a forged region in a lossless compressed forged image when its unaltered part is output of JPEG decompressor. PCA is applied to classify spatial frequency quantization noise such as low, medium and high and use high frequency quantization noise to detect forged region. This method fails to detect forgery if the source image has again saved in JPEG format with higher quality than the quality of forged image [54].

Bianchi and Piva (2011) provide a technique by exploiting the integer periodicity feature of the DCT coefficients to locate the presence of non-aligned double JPEG compression (NA-JPEG). This method correctly calculates both the quantization step and the grid shift of the primary JPEG compression [3].

Chen and Hsu (2011) suggested an approach based on the periodic characteristics of JPEG images both in spatial and transform domains, to detect block-aligned or misaligned recompression. The method fails against some image post processing operations such as additive white Gaussian noise or blurring applied with a large distortion level before recompression [6].

Bianchi et al. (2011) proposed a statistical test to determine forged regions in JPEG images by computing probability models for DCT coefficients singly and doubly compressed parts [4].

V. IMAGE RESAMPLING DETECTION

Geometric transformations are generally applied to resize and/or rotate to a digital image. These transformations are applied in the pixel domain which affects the position of samples in the original image, so a new sampling lattice must be used to resample the original image. Specific correlation imposed by resampling in the image samples can be exploited to determine forgery.

Popescu and Farid (2005) suggested a technique based on Expectation-Maximization algorithm (EMA) to detect periodic correlation imposed in the image by common resampling kernels. EMA is used to calculate the interpolation kernel parameters and a probability map is estimated for each pixel which reflects its probability to be correlated with neighboring pixel. The periodicity of probability map is due to the presence of interpolated pixels is clearly visible in the frequency domain. This method has a high computational complexity [45].

Gallagher (2005) proposed a method based on periodicity of variance of second derivative of a digital image by analyzing its Fourier transform. This algorithm performs very well for a large range of interpolation factors, both integer

and non-integer factors. However, if rotation is applied to the source image after resampling this method fails to detect traces of resampling [16].

Mahdian and Saic (2008) proposed another approach based on the periodic characteristics of the covariance structure of interpolated signals and their derivatives. The author used radon transform on the derivative of the investigated signal and then search for periodicity. This approach is also very effective in estimation of geometric transformation factors. This method has some limitations against rotation angle and scaling factor estimation, due to the one-dimensional approach [34].

Mahdian and Saic (2009) proposed a method based on the hidden cyclostationarity features in the digital images, which gone through geometric transformations. In this method periodic patterns imposed in the digital images by interpolation are identified using cyclostationary analysis. Detection method is based on the fact that a cyclostationary signal has a specific correlation between its spectral components. This method is also capable of detecting the specific parameters of transformation [33].

Vazquez-padin et al. (2010) proposed a method by exploiting the almost cyclostationary fields in digital images to detect and estimate forgeries. This method is a two-dimensional extension of a statistical time-domain test and correctly estimates the resampling factor of a spatially transformed digital image, specifically the scaling factor and the rotation angle [53].

Qian et al. (2012) proposed a rotation-tolerant technique based on a measurement called rate-distance to detect resampling. This method takes advantage of the false peaks introduced by JPEG compression in the energy spectrum of second order differential images. These false peaks are detected by measuring rate-distance between two energy spectrum patterns. This method results accuracy of 97.2% to detect whether an image is forged or not with locating the fake region 93.6% accuracy [53].

VI. CONCLUSION

Copy-move forgery detection techniques are computationally very expensive with high false positive results. In case of image splicing, forgery detection accuracy of existing techniques decreases against some image post- processing operations such as adding noise, edge blurring and lossy compression. JPEG compression based digital image forgery techniques performs very well when the forged region had a comparatively lower JPEG quality with respect to the original image and the image content is consistent. In image resampling detection techniques deals with some popular image post-processing spatial transformations such as rotation, scaling. **Qian et al. (2012)** proposed rotation-tolerant technique with a meaningful accuracy to detect resampling.

Most of the techniques are reviewed in this paper are developed to detect image forgery and some of them are also able to locate forged areas. We hope this text provide enough information about passive forgery detection techniques in digital images and contribute to discover new promising techniques and ideas to researchers interested in the field of digital image forgery detection.

REFERENCES

[1] Bashar M, Noda K, Ohnishi N, Mori K., "*Exploring duplicated regions in natural images*" IEEE Trans Image Process 2010;99:1–40.

[2] Bayram S, Taha H, Memon N., "*An efficient and robust method for detecting copy-move forgery*" In: Proc. of the 2009 IEEE International confer-ence on acoustics, speech and signal processing 2009. p. 1053–6.

[3] Bianchi T, Piva A., "*Detection of non-aligned double JPEG compression with estimation of primary compression parameters*" In: Proc. International conference on image processing 2011. p. 1929–32.

[4] Bianchi T, Rosa A, Piva A, "Improved DCT coefficient analysis for forgery localization in JPEG images. In: Proc" International conference on acoustics, speech and signal processing 2011. p. 2444–7.

[5] Chen W, Shi Y, Su W., "Image splicing detection using 2-d phase congruency and statistical moments of characteristic function" In: Proc. of SPIE electronic imaging: security, steganography, and watermarking of multimedia contents 2007.

[6] Chen Y, Hsu C., "Detecting recompression of JPEG images via periodicity analysis of compression artifacts for tampering detection" IEEE Trans Inf Forensics Security 2011; 6(2):396–406.

[7] Chunhua C, Shi YQ, Wei S., "A machine learning based scheme for double JPEG compression detection" In: Proc. International conference on pattern recognition 2008. p. 1–4.

[8] Dybala B, Jennings B, Letscher D., "Detecting filtered cloning in digital images" In: Proc. of the 9th workshop on multimedia & security. ACM; 2007. p. 43–50.

[9] Farid H., "Detecting digital forgeries using bispectral analysis" Technical Report AIM-1657. AI Lab, Massachusetts Institute of Technology; 1999.

[10] Farid H., "Exposing digital forgeries from JPEG ghosts" IEEE Trans Inf Forensics Security 2009b; 1(4):154–60.

[11] Fridrich J, Lukas J., "Estimation of primary quantization matrix in double compressed JPEG images" In: Proc. of the digital forensic research workshop (DFRWS), vol. 2. 2003.

[12] Fridrich J, Pevny T., "Detection of double-compression for applications in steganography" IEEE Trans Inf Forensics Security 2008; 3(2):247-58.

[13] Fridrich J, Soukal D, Lukas J., "Detection of copy-move forgery in digital images" In: Proc. of digital forensic research workshop 2003. p. 55–61.

[14] Fu D, Shi Y, Su W., "A generalized Benford's law for JPEG coefficients and applications in image forensics" In: Proc. SPIE electronic imaging: security, steganography, and watermarking of multimedia contents, vol. 6505. 2007. p. 65051L.

[15] Fu D, Shi Y, Su W., "Detection of image splicing based on Hilbert-Huang transform and moments of characteristic functions with wavelet decomposition" In: Proc. of International workshop on digital water-marking 2006. p. 177–87.

[16] Gallagher AC., "Detection of linear and cubic interpolation in JPEG compressed images," in Proceedings of the Canadian Conference on Computer and Robot Vision, 2005 pp. 65–72.

[17] Gopi E, Lakshmanan N, Gokul T, Ganesh S, Shah P., "Digital image forgery detection using artificial neural network and auto regressive coefficients" In: Proc. Canadian conference on electrical and computer engineering 2006. p. 194–7

[18] Hsu Y, Chang S., "Detecting image splicing using geometry invariants and camera characteristics consistency" In: Proc. IEEE International con-ference on multimedia and Expo (ICME) 2006. p. 549–52.

[19] Huang H, Guo W, Zhang Y., "Detection of copy-move forgery in digital images using SIFT algorithm" In: Proc. of the 2008 IEEE Pacific-Asia workshop on computational intelligence and industrial application 2008. p. 272–6.

[20] Johnson M, Farid H., "Exposing digital forgeries through specular highlights on the eye" In: Proc. International workshop on information hiding 2007c. p. 311–25.

[21] Jufeng H, Zhouchen L, Lifeng W, Xiaoou T., "Detecting doctored JPEG images via DCT coefficient analysis" In: Proc. of the 9th European conference on computer vision, vol. Part III. 2006. p. 423–35

[22] Kakar P, Sudha N., "Exposing postprocessed copy-paste forgeries through transform-invariant features" IEEE Trans Inf Forensics Security 2012; 7(3):1018–28.

[23] Langille A, Gong M., "An efficient match-based duplication detection algorithm" In: Proc. of the 3rd Canadian conference on computer and robot vision 2006. p. 64

[24] Li B, Shi YQ, Huang J., "Detecting doubly compressed JPEG images by using mode based first digit features" In: Proc. IEEE workshop on multi-media signal processing 2008a. p. 730–5.

[25] Li G, Wu Q, Tu D, Sun S., "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD" In: Proc. International conference on multimedia & Expo 2007. p. 1750–3.

[26] Li W, Yuan Y, Yu N., "Detecting copy-paste forgery of JPEG image via block artifact grid extraction" In: Proc. International workshop on local and non-local approximation in image processing 2008b. p. 121–6.

[27] Lin H, Wang C, Kao Y., "Fast copy-move forgery detection" WSEAS Trans Signal Process 2009a;5(5):188–97.

[28] Liu G, Junwen W, Shiguo L, Zhiquan W., "A passive image authentication scheme for detecting region-duplication forgery with rotation" J Netw Comput Appl 2011a;34(5):1557–65.

[29] Liu Q, Cao X, Deng C, Guo X., "Identifying image composites through shadow matte consistency" IEEE Trans Inf Forensics Security 2011b; 6(3):1111–22.

[30] Luo W, Huang J, Qiu G., "A novel method for block size forensics based on morphological operations" In: Proc. of International workshop on digital watermarking (IWDW) 2008. p. 229–39.

[31] Luo W, Huang J, Qiu G., "JPEG error analysis and its applications to digital image forensics" IEEE Trans Inf Forensics Security 2010; 5(3):480–91.

[32] Luo W, Huang J, Qiu G., "Robust detection of region-duplication forgery in digital image" In: Proc. of the 18th International conference on pattern recognition 2006. p .746–9.

[33] Mahdian B, Saic S, "A cyclostationarity analysis applied to image forensics," in Proceedings of the Workshop on Applications of Computer Vision (WACV '09), 2009, pp. 1–6.

[34] Mahdian B, Saic S, "Blind authentication using periodic properties of interpolation," IEEE Transactions on Information Forensics and Security, 2008, vol. 3, no. 3, pp. 529–538.

[35] Mahdian B, Saic S., "Detecting double compressed JPEG images" In: Proc. of 3rd International conference on imaging for crime detection and prevention (ICDP-09) 2009a. P12.

[36] Mahdian B, Saic S., "Detection of near-duplicated image regions" In: Computer recognition systems 2Advances in soft computing, vol. 45. 2007. p. 187–95

[37] Muhammad G, Hussain M, Khawaji K, Bebis G., "Blind copy move image forgery detection using dyadic uncedimated wavelet transform" In: Proc. of 17th International conference on digital signal processing 2011. p. 1–6.

[38] Myna A, Venkateshmurthy M, Patil C., "Detection of region duplication forgery in digital images using wavelets and log-polar mapping" In: Proc. of the International conference on computational intelligence and multimedia applications (ICCIMA 2007) 2007. p. 371–7.

[39] Neelamani R, Queiroz R, Fan Z, Baraniuk R., "JPEG compression history estimation for color images" In: Proc. International conference on image processing, vol. 2. 2003. p. III–245–248

[40] Ng T, Chang S., "A model for image splicing" In: Proc. of IEEE International conference on image processing (ICIP) 2004. p. 1169–72.

[41] Ng T, Tsui M., "Camera response function signature for digital forensics - part I: theory and data selection" In: Proc. IEEE workshop on information forensics and security 2009p.156–160.

[42] Ng T-T., "Camera response function signature for digital forensics – part II: signature extraction" In: Proc. IEEE workshop on information forensics and security 2009. p. 161–5.

[43] Nguyen HC, Katzenbeisser S., "Detection of Copy-move Forgery in Digital Images Using Radon Transformation and Phase Correlation" Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2012 Eighth International Conference on, 18-20 July 2012, p.134-137.

[44] Popescu A, Farid H., "Exposing digital forgeries by detecting duplicated image regions" Technical Report TR2004-515. Department of Computer Science, Dartmouth College; 2004.

[45] Popescu AC, Farid H, "Exposing digital forgeries by detecting traces of resampling," IEEE Transactions on Signal Processing, 2005, vol. 53, no. 2, pp. 758–767.

[46] Popescu AC., "Statistical tools for digital image forensics (Ph.D. thesis)" Hanover: Department of Computer Science, Dartmouth College; 2004.

[47] Qingzhong L, Andrew H., "A new approach for JPEG resize and image splicing detection" In: Proc. ACM multimedia and security workshop 2009. p. 43–8.

[48] Qu Z, Luo W, Huang J., "A convolutive mixing model for shifted double JPEG compression with application to passive image authentication" In: Proc IEEE International conference on acoustics, speech and signal processing 2008. p. 1661–4.

[49] Shi Y, Chen C, Chen W., "A natural image model approach to splicing detection" In: Proc. of ACM workshop on multimedia and security (ACM MMSEC07) 2007a. p. 51–62.

[50] Sutthiwan P, Shi YQ, Wei S, Tian-Tsong N. "Rake transform and edge statistics for image forgery detection" In: Proc. IEEE International conference on multimedia and Expo (ICME) 2010. p. 1463–8

[51] Tjoa S, Lin W, Liu K., "Transform coder classification for digital image forensics" In: Proc. International conference on image processing (ICIP) 2007a. p. 105–8.

[52] Tjoa S, Lin W, Zhao H, Liu K., "*Block size forensic analysis in digital images*" In: Proc. IEEE International conference on acoustics, speech and signal processing 2007b. p. I-633–6.

[53] Vazquez-Padín D, Mosquera C, Pérez-González F, "*Twodimensional statistical test for the presence of almost cyclostationarity on images*," in Proceedings of the 17th IEEE International Conference on Image Processing (ICIP '10), 2010, pp. 1745–1748.

[54] Wang W, Dong J, Tan T., "*Tampered region localization of digital color images based on JPEG compression noise*" In: Proc. International workshop on digital watermarking 2010. p. 120–33.

[55] Weihai L, Nenghai Y, Yuan Y., "*Doctored JPEG image detection*" In: Proc. IEEE International conference on multimedia and Expo 2008. p. 253–6.

[56] Yu-Feng H, Shih-Fu C., "*Camera response functions for image forensics: an automatic algorithm for splicing detection*" IEEE Trans Inf Forensics Security 2010;5(4):816–25.

[57] Zhang J, Wang H, Su Y., "*Detection of double-compression in JPEG2000 images for application in image forensics*" J Multimed 2009a; 4(6):379–88.

[58] Zhang W, Cao X, Qu Y, Hou Y, Zhao H, Zhang C., "*Detecting and extracting the photo composites using planar homography and graph cut*" IEEE Trans Inf Forensics Security 2010;5(3):544–55

[59] Zhang Z, Kang J, Ren Y., "*An effective algorithm of image splicing detection*" In: Proc. International conference on computer science and software engineering 2008b. p. 1035–9

[60] Zhao X, Li J, Li S, Wang S., "*Detecting digital image splicing in chroma* spaces" In: Proc. International workshop on digital watermarking 2010. p. 12–22.

[61] Zhenhua Q, Guoping Q, Jiwu H., "*Detect digital image splicing with visual cues*" In: Proc. International workshop on information hiding 2009. p. 247–61.

