International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 05, May-2015

Digital Image Forensics in Multimedia Security: A Review

Vivek Singh
Computer Science & Engineering Department
Jaypee University of engineering and technology,
Raghogarh, guna, india

Neelesh Kumar Jain
Computer Science & Engineering Department
Jaypee University of engineering and technology,
Raghogarh, guna, india

***Abstract*— Determining the authenticity of an image is now an important area of research. This report attempts to classify whether a digital image is a genuine image or is a manipulated version of some authentic image. Survey describes that the reliability of digital visual information has been scrupled, due to the ease in counterfeiting both its origin and content. Digital image forensics is validating the authenticity of images by the identification of the imaging device that captured the image, and the detection of trails of forgeries. An overview of passive image authentication and the existing blind forgery detection techniques are reviewed and techniques discussed to detect the fake regions in the picture. A thought given to distinguish copied locales notwithstanding when the duplicated segment have experience post handling operations. This paper portrays passive digital picture forensic methodologies for identifying copy move falsification.**

Keywords*— *Copy move forgery; image forensics; image tampering; geometric distortion; passive techniques

I.INTRODUCTION

Images and videos have become the main information carriers in the digital world. The expressive ability of visual media and the ease in their delivery and storage is such that they are widely used to carry information, even sensible. Today images and videos are common source of evidence, both in every-day life dispute and in court of laws. Together with obvious advantages, the accessibility of digital media has a major drawback. Experts can easily access and alter image content, and therefore its meanings and consequences, without leaving discoverable trails as in fig 1. Acquiring and tampering both leave some trails and forensic experts expose these trails by image processing techniques [1]. Digital image forensics acquires its techniques from digital watermarking and steganography techniques. Image security includes active (digital watermarking) and passive techniques (no previous integrity protection set). Mainly digital image forensics focuses on "Digital image source identification" and "tampering detection techniques" [1].

Image source identification done through the traces produced in acquiring process, as specific lens produces geometrics distortions. Also identification of source device is done through sensor imperfection qualities, and properties of the imaging devices like color related management. Tampering means the intentional alteration of images for malicious purpose [2]. Image alteration includes removing or adding information in the images and mainly there are two types of tampering methods single image tampering and composite image tampering. In single image tampering there is usage of single image whether in composite image tampering two or more images used for alteration [1].

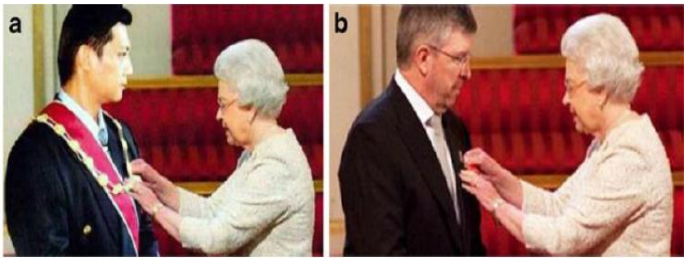

Fig. 1 The doctored image depicting Jeffrey Wong Su En while receiving the award from Queen Elizabeth II, published in Malaysian dailies, and the original picture of Ross Brawn receiving the Order of the British Empire from the Queen (b) [1]

Active and passive two main techniques used for image forgery detection in which active needs some pre-processing like including digital watermarking and digital signature in images, whether in passive there is no need of previous integrity protection mechanism [1]. Due to high impact we reviewed here passive techniques mainly.

II.FORGERY INVOLVING SINGLE IMAGE AND MULTIPLE IMAGES FOR SOURCE OF TAMPERING

In forgery with single image, forgers copy a portion of same image and replace it with left place from deletion known as copy-move technique. To make forgery more hide able forgers performs some post geometric transforms such as rotation, scaling and reflection on the copied regions, also matting and blending [3,4]. Seam carving was a powerful tool for object removal in images. Basically seam is connected path of pixels increase monotonically including a pixel per row. For specific region it is a very useful and accurate tool for object removal [5].

Forgery using multiple images used the insertion of material for one image carries from different image or images. For non-detectable composition it requires some geometric transformations like scaling, rotation, translation etc. but

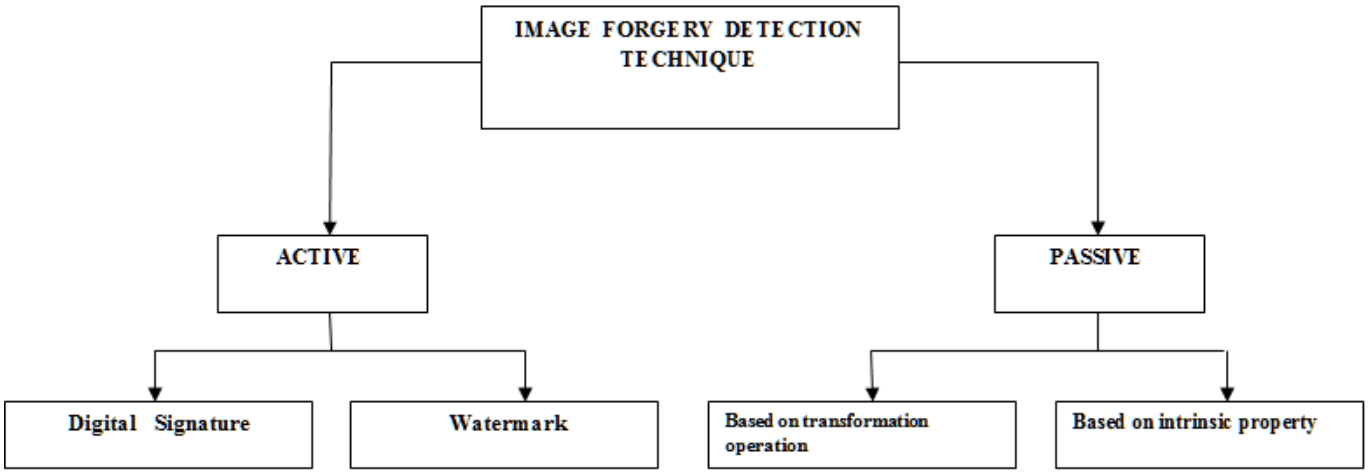

Fig. 2 Basic image forgery detection techniques

transformation produces some artifacts in the resultant image

histograms which are sometimes detectable so the forgery also. Sometimes some 3-D model used for composite in the original image to fulfill the forger aims, mainly to modify facial expression in video rewriting techniques [6].

III.METHODS FOR FORGERY DETECTION

In copy move attack the altered area have some intrinsic properties which are differ from rest of images. Fridrich J. et al. proposed a DCT representation of image segment based on above traces to find forgery in [7]. DCT coefficients are indexed and adjacent similar pairs are considered as tampered regions. Based on these coefficients histogram is built for no. of matching segment separated by same distance and higher probability of that the segments belongs from copy-move region.

Another approach based on principal component analysis for image segments was proposed by Popescu and Farid. It has higher calculation power with less cost. It shows less no. of false positive matches and less image degradation. Limitations of this approach were the post processing operations like scaling and rotations performed on tampered image hides the forgery [8]. Zhang et. al. Proposed detection of forged region based on analyzing the shadow geometric photometrical properties. It is done by relating an object which is illuminated by a point light source and its shadow on a plane. For this purpose use shadow malte value along with its boundary points and make a histogram. This method has limitations if the image is infinitely far away to light source and also there is manual selection of shadow boundaries take place [9]. Again the popsecu and Farid uses the expectation algorithm for estimated calculation of the probability from which each pixel to be correlated with its neighboring pixels. They show that for forged image these probabilities are arranged in a periodic pattern whose detection proves the forgery in image [10]. This method was weaker in the case of highly compressed images.

A generalized framework for blind image forgery detection consists following steps [11].

Image preprocessing- operations performs on images such as cropping, transforming RGB into grayscale image, DCT or DWT transformation etc.

Feature extraction- A set of features are extracted from image for each class which helps for distinguish with another classes.

Classifier- selection and feature preprocessing based on the extracted features select the classifiers and then train the classifiers using the set of images and the basis of which find some parameters for the classification.

Classification - to discriminate the given image and classified it into whether the image was forged or original one.

Post processing- in some of the forgeries, to hide the artifacts of the forgery like in copy-move some post processing involves localization of forged image.

In copy move or region duplication forgery parts of original image is copied and moved to a desired location and pasted. Since these areas are similar color and noise variation properties so difficult to human eye to find inconsistencies in image statistical properties. Langille and gong proposed k-dimension tree to search the blocks with similar intensity values using matching techniques. Zero normalized cross correlation was used as a similarity measure and accurate outcome occur. Luo et.al. Introduced copy-move forgery detection and localization method [11]. They divide the image into overlapping blocks and finally identify the possible duplicated regions using intensity features. It has also a lower computational complexity. Myna et. al. Use log polar coordinates and wavelets transform to detect copy-move

forgery which is later used as log polar fast fourier transform. This process is based on rotation and scale in variation and it has also a lower computational complexity. Dybala et. al. Gives cloning detection method based on filtering operation and nearest neighbor search approach. It uses singular value

river, mountains) produces a significant number of false matches.

DCT(discrete cosine transform) has been widely used to represent the image in frequency domain. It has ability to

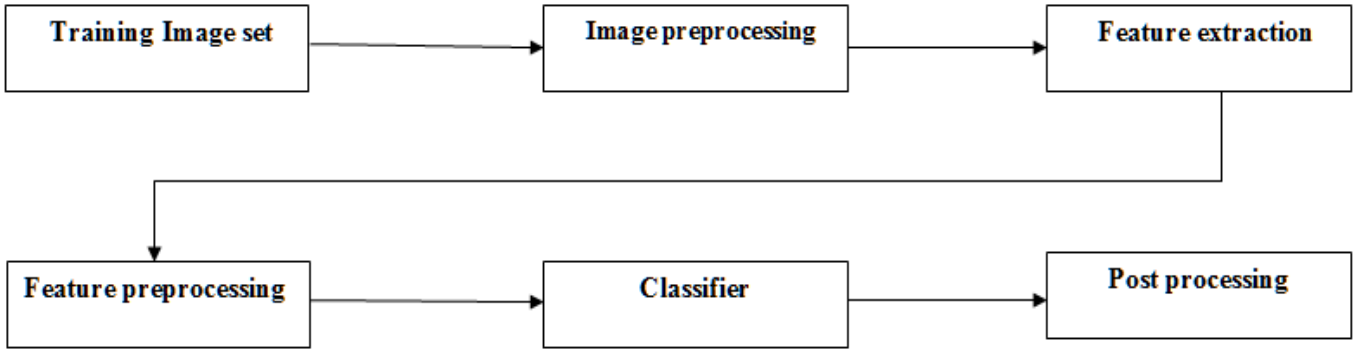

Fig. 3 A generalized framework for blind image forgery detection

decomposition for feature vector dimensionality reduction and wavelet transformation for duplicated or copied region detection. Another approach named as scale invariant feature transform (SIFT) is used which is stable with respect to changes in illumination of source light, rotation and scaling related to cloned region [11].

Existing digital image technology provides various Processing tools that can be used for tampering which cannot be easily identified, even by skilled professionals. This has created serious problems about the use of digital images in areas that deals with sensible information, such as medical and military applications. Additional post-processing operations, which could abrade the localization performance, should be considered. For example, the detection of forged areas modified by JPEG compression. This concern was first discussed by Myna et al. Here, overlapping blocks of discrete wavelet coefficients with lower resolution are mapped to log-polar coordinates. The resulting blocks are sorted and examine to identify similar pairs. The formed pairs are filtered by removing those blocks that do not fulfill the similarity criteria in the particular wavelet resolution levels [11]. Forensic techniques aimed to image interpolation, could be identify regions altered by rotation and scaling. However, cloned areas affected by geometric distortions that do not require interpolation (e.g. reflection) would go unmarked by these methods. A new forensic method reviewed to detect and localize copied regions that have undergone reflection, rotation and/or scaling and JPEG compression. To perform an efficient search, in terms of storage, overlapping blocks of pixels are mapped to 1-D descriptors derived from log-polar maps. Then, feature vectors, extracted from each block, are used to decrease the computational cost of the search stage. Finally, a filtering or refinement stage has been given to deal with duplicated regions that have undergone geometric changes [12]. A problem generally faced by this method is to detect duplicates is posed or detect by areas of uniform luminance (e.g. sky,

represent most of the intensity distribution with fewer values. So the next forgery detection algorithm is based on DCT. The DCT based method uses the DCT coefficients to show the overlapping blocks. The DCT coefficients are arranged in zigzag order to keep the low frequency coefficients together and before the high frequency coefficients in the row order. The algorithm steps are as follows [13]

- The input image is a gray scale image it can be converted to a gray scale image using the standard formula.
- Slide a fixed-sized square window by one pixel from the upper left corner to the bottom right of the image to divide it into overlapping blocks.
- Apply DCT to every block and reshape quantized coefficient matrix to a row vector by ordering DCT coefficients in zigzag order.
- All vectors are sorted and form a matrix.
- For each row in matrix test its neighboring rows which satisfy the condition that the some initial quantized DCT coefficients are same. As these DCT coefficients are sufficient to represent the major intensity distribution over the block.
- If distance between similar blocks is greater than some threshold value which can decide by some training sets, and greater than a significant amount then the traces of copy are seemed to be there.

The given method removes complexity limitations of popular block matching algorithms by modifying the matching algorithm. The matching step performed after sorting the coefficient array, not all row vectors within a fix range are considered to be similar but a more strict criteria is used to show the similarity. The high frequency coefficients are supple to noise, so the row vectors are repudiated. First few coefficients represent the major intensity distribution of the

block. Hence the low frequency coefficients must be either similar or so close for the copy- moved regions [13].

The DWT(discrete wavelet transform) has been found to be an efficient signal and image-processing tool, which can be used in time and frequency localization, multi rate filtering, scale-space analysis, and multi-resolution analysis. In this study, we extract the various features from the wavelet coefficients through a multilevel 2-D DWT [14]. Method is based on the assumption that copied regions must have several statistical compatibilities, which other regions do not have. Therefore, we can extract the peculiar features from regions for copy detection. The method can be divided into seven steps as converting color image to gray-scale image, dividing image into overlapped blocks, feature extraction, feature vector sorting, block matching, filtering and output. If the original images are color images, they will be converted to gray-scale images first by calculating a weighted average of the Red (*R*), Green (*G*) and Blue (*B*) components. The conversion is done as shown following,

$$f(R,G,B) = 0.2989R + 0.5870G + 0.1140B \quad ..(1)$$

A square block with $B \times B$ pixels is used to slide over the image from the upper left corner to the lower right corner. The slide step is only one pixel and no padding will be applied. Therefore, the original image with size of $M \times N$ will generate $(M-B+1) \times (N-B+1)$ overlapping blocks in total. The 2-D DWT is applied to each block for two times. For each iteration, we extract features from the coefficients of low frequency detail, horizontal and vertical detail of sub images in high frequency. The diagonal high frequency sub images, which mainly contains noise, is not used. For each sub image, some energy signatures like mean, standard deviation, and average residual are computed. After feature extraction, there are $(M-B+1)*(N-B+1)$ feature vectors generated. We compare all of these vectors, two at a time, to find the similarities. Because of the computation complexity for doing this is very high, a better solution is to sort the vectors first and then only compare a vector with its adjacent neighbors. Considering that cloned regions would have similar features, the probability that their corresponding feature vectors are located adjacently in the sorted vector array is high. Two vectors will be compared in the matching step to find the similarity of the corresponding blocks based on some limitations applying on the similarity measure of two coefficients that are assumes to be close. For this purpose The threshold values for each feature are computed from a training set [14]. If the original image has large smooth regions, similar blocks can be found in these regions we need to remove these false positives. Also, if the resultant duplicated areas are too small, they are not meaningful and have to be ignored as false positives. The above solution is capable of finding the copied regions without any prior information about the image. Compared to the DCT based method, the above method has better performance, especially when the forged images are heavily noised [14].

Another method uses 2D-Fourier Transformation to extract features from the overlapping blocks. fixed number of FT coefficients is used to show feature vector. This method is higher efficient even if the image is blurred or compressed by JPEG. The method also can detect multiple copy move forgery [15]. Techniques used in the literature divide image into blocks and after segmentation extract some features using these blocks. Similarity between the different feature vectors indicates the possibility of the forgery. In this section, we give brief explanation of the method. The algorithm can be given in the form of steps as below [15]

- Input image is smoothed by mean filter with a suitable window size.
- Forged image is divided into square sub blocks.
- 2D-FT is applied on each block to extract features.
- The vector created in the previous step is quantized with by a factor which is determined by the user during the detection algorithm.
- The dimension of the feature vector is reduced with some constant . The value of constant falls in some specific range to normalize the dimensions.
- Each feature vector is inserted into a matrix, matrix is sorted to make the similar vectors more close and to reduce the false matches, based on training set some threshold method applied.

Most works in this method use block based approaches to trace the forgery. Method of feature extraction in the algorithms affects the accuracy ratio of the method. The size of the feature vectors also affects the complexity of the approach in aspects of time. This work detects multiple copy move forgery and robust to JPEG compression attacks even if the quality factor is low. On the other hand, this work uses no. of elements feature vectors less than Huang et al.'s method elements feature vectors [15]. So reducing the dimension of feature vectors is another quality in this area.

Next method is named as expanding block algorithm which uses direct segmented block comparison rather than indirect comparisons of block features [16]. This method first divides an image into small blocks just like in the sliding block method. But approach to comparing the blocks is different here. Several blocks are far different and do not need to be compared to each other. A dominant feature is computed for each block of image. We use the mean of gray value computed from the pixels of a block as a dominant feature. If there is a huge difference between block dominant feature values, there is no need for compare those blocks. Blocks are gathered according to their dominant features. The blocks are sorted by these features and placed into groups, each of which contains the blocks with a compatible dominant feature [16]. The expanding block algorithm is as below.

- Divide an image into small overlapping square blocks.
- For each block, compute the mean gray value as the dominant feature.
- Sort the blocks according to dominant feature.
- From the sorted blocks ,place the blocks into groups.
- Create buckets. Place the blocks from previous and next groups into current bucket.
- Now apply matching between buckets based on dominant feature and applying threshold for detecting the cloned regions.

- Threshold values are depend upon the training set performs to ignore the false positives.

IV.PERFORMANCE COMPARISON BETWEEN SOME COPY-MOVE DETECTION METHODS

In this part survey of several copy move forgery detection methods has been given based on [16]. Now the question occurs of their effectiveness under different circumstances because every method has some limitation.

Methods/Thresholds	1	0.95	0.9	0.85
DCT	46.7	21.5	10	5
Statistical	61.7	33	13.8	6.1
PCA	31.6	14.7	7.8	4.9
EB	94.2	47.6	14.4	8.6

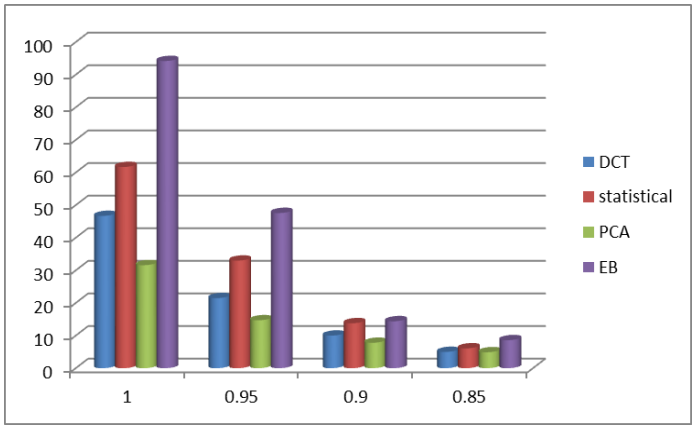

Fig. 4.1 Table & chart for percent of true positives in different methods under jpeg compression

Methods/Thresholds	1	0.95	0.9	0.85
DCT	1	1	1	1
Statistical	3	2	3	3
PCA	0	0	0	0
EB	3	3	4	5

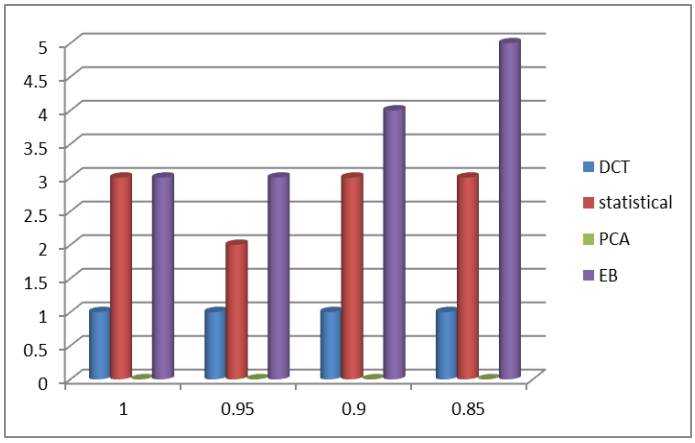

Fig. 4.2 Table & chart for number of false positives in different methods under jpeg compression

Methods/Thresholds	1	0.95	0.9	0.85
DCT	41.0	18.1	8.1	2.8
Statistical	54.5	28.8	11.5	4.7
PCA	27	12	6	3
EB	88.6	28.2	5.4	2.4

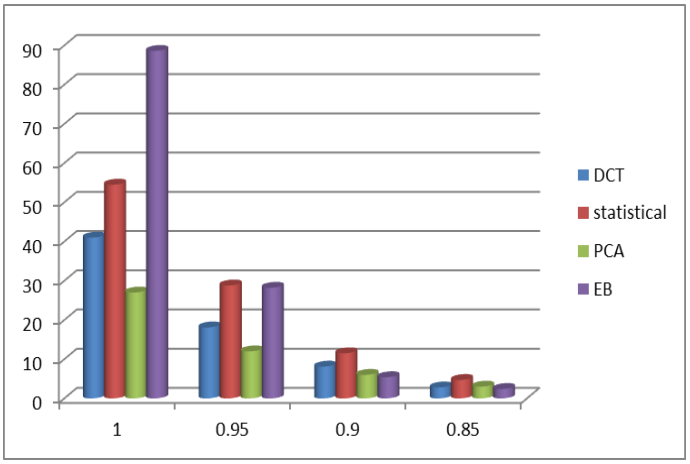

Fig. 4.3 Table and chart for percent of correctly defined regions in different methods under jpeg compression

Methods/Thresholds	1	0.95	0.9	0.85
DCT	554	438	414	319
Statistical	718	478	440	456
PCA	89	45	25	29
EB	76	78	86	159

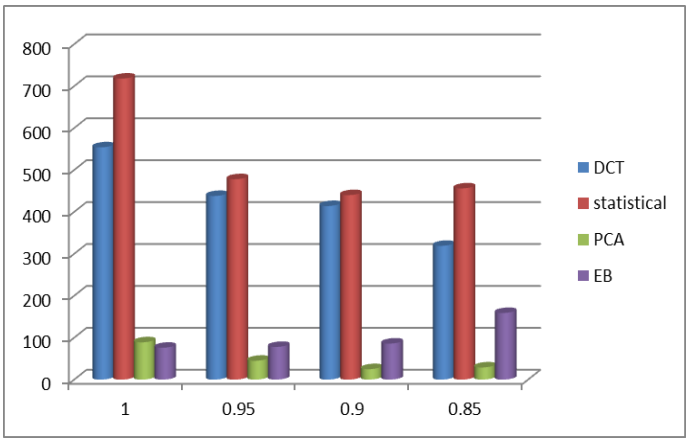

Fig. 4.4 Table and chart for pixels incorrectly identified in different methods under jpeg compression

Different post processing operations like rotation, scaling, and several other transformations like JPEG compression affects the performance of discussed algorithms. In fig.4 we discuss the performance comparison between some of these methods under jpeg compression given in [16]. In all figures the X-axis of chart contains the threshold values takes as experimental value by different methods.

V.CONCLUSION

The methods that we reviewed in this survey are able to discuss the important aspects for multimedia security. Reviewed methods also consider those problems which are previously unexplored. A large set of image processing tools is now available to inquire on image sources and to validate acquisition devices. Tools that analyze pattern noise were known to be auspicious for finding even different replicas of the same device model. Larger numbers of techniques have been developed to detect image forgery; some of them are also able to localize the forged areas. Regardless these achievements, several challenges are still there for Digital Image Forensics as first robustness of the existing tools, the discovery of different counter-forensic tools etc. Another aspect for Digital image Forensics is the usage for other media as video. Videos are most powerful medium than images for communication. More techniques are still needed to overcome all these limitations and to make digital media more secure and authenticated. Still these methods are unable to give accurate result in the case of uniform luminance region and if there is exactly two same objects exists then most of above methods show the false positives. So there is a need of huge work to solve these entire problems which is the motive of our future work.

REFERENCES

[1] A Judith. Redi, W Taktak, J L Dugelay, "Digital image forensics: a booklet for beginners", Multimed Tools Appl 51:133–162 , 2011.

[2] H Cao, AC Kot, " Accurate detection of demoisaicing regularity for digital image forensics" IEEE 2009.

[3] P Pérez, M Gangnet, A Blake , "Poisson image editing". ACM Trans Graph (SIGGRAPH'03) 22 (3):313–318 2003.

[4] J Wang, "M-F Cohen Image and video matting: a survey". Found Trends Comput Graph Vis 3(2):97–175 2007.

[5] M Rubinstein, A Shamir, S Avidan " Improved seam carving for video retargeting". SIGGRAPH 2008.

[6] C Bregler, M Covell, M Stanley Video rewrite: driving visual speech with audio. In: Computer Graphics Proceedings, Annual Conference Series. ACM SIGGRAPH 1997.

[7] J Fridrich, D Soukal, J LukasDetection of copy-move forgery in digital images. In: Proceedings of Digital Forensic Research Workshop 2003.

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

[9] W Zhang, X Cao, J Zhang, J Zhu, P Wang, "Detecting photographic composites using shadows". IEEE International Conference on Multimedia and Expo, pp 1042–1045 2009.

[10] A Popescu, H Farid, " Exposing digital forgeries by detecting traces of re-sampling". IEEE Trans Signal Process 53(2):758–767 2005.

[11] K Gajanan. Birajdar, H Vijay Mankar, "Digital image forgery detection using passive techniques: A survey". Digital Investigation 10: 226–245 2013.

[12] Sergio Bravo-Solorio, AsokeK.Nandi, "Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics". Signal Processing 91:1759–1770 2011.

[13] S Kumar, J Desai,S Mukherjee, "A Fast DCT Based Method for Copy Move Forgery Detection" IEEE 2013.

[14] Y Wang, K Gurule, J Wise, J Zheng, "Wavelet Based Region Duplication Forgery Detection" IEEE 2012.

[15] S Ketenci, G Ulutas, "Copy-Move Forgery Detection in Images via 2D-Fourier Transform", IEEE 2013.

[16] G Lynch , F .Shih, H Y Mark Liao, "An efficient expanding block algorithm for image copy-move forgery detection", Information Sciences 239:253–265 2013.