Image Forgery Detection and Localization: Review

Anju Jose
M.Tech Student, Computer Science and Engineering
NSS College of Engineering
Palakkad, Kerala, India
iamanjujosek@gmail.com

Maya Mohan
Assistant Professor, Computer Science and Engineering
NSS College of Engineering
Palakkad, Kerala, India
mayajeevan@gmail.com

***Abstract*—Image forensics, a specific domain in forensics, uses science and technology to perform image content analysis and image authenticity to establish the facts in front of the court of law. Any operation which alters the original content of an image is considered as a forgery. 2 types of forgeries such as Copy Move and Splicing forgeries are most common nowadays. Copy Move forgery copies a part of image and paste it in the some other part of image to add or hide some information. While in Splicing forgery a part of image is copied from an image and pasted in some other image. Contrast enhancement, Image retouching, JPEG compression etc. are also considered as image forgery. Since the forged images can be visually feasible it is difficult to detect the forgery. So it is inevitable to have an image forgery detection tool to prove the genuineness of the digital image. Keypoint based and Block based approaches are the fundamental approaches used in these tools to detect forgery. Application of these approaches in different color spaces such as RGB, YCbCr etc. and feature spaces paved way for the development of different forensic techniques and tools. Different feature matching and pattern matching algorithms are used to detect copy move forgery while machine learning approaches are more effective for detecting the splicing forgery. Most of the forensic tools are specific to one or two type of forgery and some can only detect forgery while some other techniques can detect and localize the exact region of forgery in tampered images. Inpainting based techniques which were developed to remove tampered region from forged images and filling those regions with visually feasible objects are misusing widely for generating the tampered images. This paper presents a survey on different types of image forgeries and different techniques for detecting and localizing image forgery.**

***Index Terms*—forensics, image forgery, Copy Move, Splicing, Contrast enhancement, Image retouching, JPEG compression, Keypoint based and Block based approaches, detection and localization, Inpainting**

I. Introduction

Technology evolves over time. The widespread adoption of digital content over traditional physical media has given rise to a number of new information security challenges. Rapid development in digital media editing techniques and tools make digital image manipulations rather convenient and easy. Even though these techniques and tools are benefits to the legal image processing, malicious users might use such innocent manipulations to tamper digital photographic images. Digital pictures (images and videos) can be enhanced, compressed, transmitted, translated across different standards, and displayed in a variety of devices. Thus digital content can be altered, falsified, and redistributed with relative ease by adversaries. In many important real world scenarios, digital information originates from an unknown or untrusted source. When this happens, a forger or information attacker can easily manipulate digital content such as images or video to create perceptually realistic forgeries. Encryption cannot ensure that the information being distributed is unaltered and authentic. Before multimedia information of this nature can be trusted, several questions must often first be answered such as: what is the true origin of this content? How has it been processed? Is this content authentic or has it been manipulated? Compared with the efforts made to ensure the secure and trusted delivery of information, research approaches that are aimed at answering these questions are still relatively new.

With the rapid development of digital media editing techniques, digital image manipulation becomes rather convenient and easy. In response to the increasing need to verify the trustworthiness of multimedia content, the field of information forensics was born. Information forensics is concerned with determining the authenticity, processing history, and origin of digital multimedia content with no or minimal reliance on side channels other than the digital content itself. It further aims at reconstructing who, when, how, and what has been done to the content. The goal of blind image forensics is to assess the authenticity and origin of digital images without an embedded security scheme.

II. Image Tampering Approaches

Tampered images are not a new phenomenon. The earliest recorded example occurred in the 1840s. The first photographic forger was Hippolyte Bayard and he created a false image of himself committing suicide. This hoax was a reaction to Louis Daguerre, the inventor of the Daguerreotype, receiving a patent for a photographic process before Bayard could, much to Bayards frustration [8]. The forging of digital imagery is similar to conventional photo forgery. Instead of manipulating analog film or negatives, digital forgery changes the digital data that comprises the image. Computer programs like Adobe Photoshop, GIMP, and Corel Paint Shop have made the alteration of digital photos incredibly easy, considering their power and versatility as well as their low price, some of them are completely free of charge.

Any operation on the image which alters the original content of an image can be considered as image tampering. Image tampering can be broadly classified into 2 categories: Active

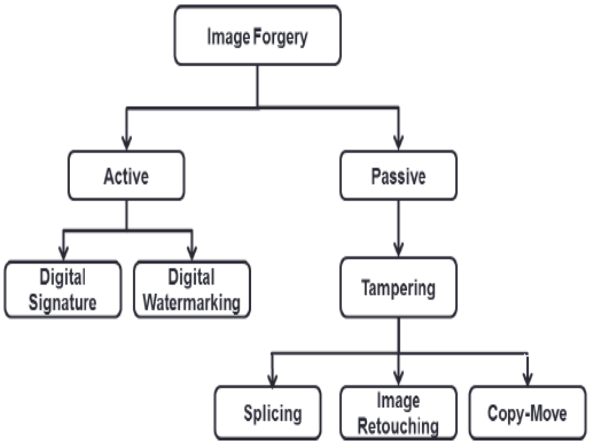

Fig. 1. Image forgery classification

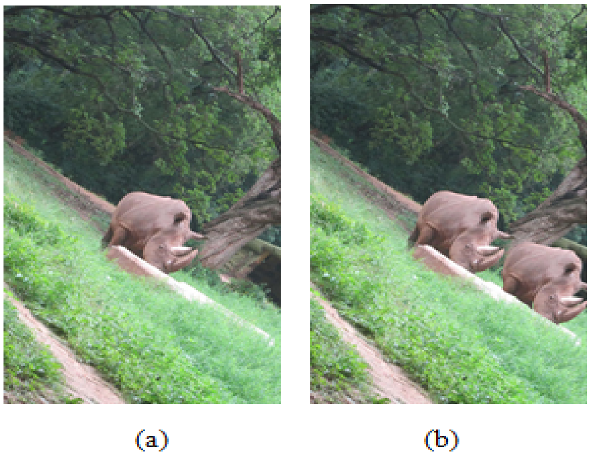

Fig. 2. Example of Copy Move forgery. (a) Pristine image. (b) Forged image

and passive blind approaches. In active forgery approach, the traces of tampering are directly visible in most cases. In this approach, some type of pre-processing such as watermarking, digital signature is done at the time of image creation. Digital watermarking and digital signature are the major protection techniques, as something is embedded into images when they are obtained from the authenticated sources. In passive blind approach, there will not be any evidence of tampering. In contrast to active approaches, passive methods do not require any prior information about the picture. Passive image forgery detection is a challenging task in image processing. There are many passive image forgery detection techniques which can detect specialized forgery in a different manner. Passive detection deals with the raw image analysis based on different statistics of image content to localize tampering of an image. The methods and algorithms of detection are highly dependent upon the type of security constraints used.

A. Copy Move Forgery

Copy-move is the popular and most common kind of image tampering technique. One part of the image is used to add or remove information. Copying from one part and pasting the same in some other part in the same image with an intention to hide certain content in the original image or duplicating some content that is not actually present in the image. Textured areas in an image like grass, foliage, or fabric with non-regular patterns, are ideal for this purpose due to the blend of the copied areas with the background and it is difficult for the human eyes to recognize the forgery. Duplicate image regions can be created using this technique. Since the copy-paste is within an image, properties of the tampered portion will be same as that of other regions and it is difficult detect. Figure 1 shows an example of copy-move operation.

B. Image Splicing

Splicing is a commonly used forgery technique in Image tampering . Replacing one or more portions of a picture with fragments other picture causes the splicing operation. There are many tools available for image tampering like morphing, enhancement, rebroadcast, computer generation etc. Splicing is a form of photographic manipulation in which there is digital splicing of two or more images into a single composite image may not have further post processing such as smoothening of boundaries among different fragments. Splicing can cause inconsistencies in many features like the abnormally sharp transient at the splicing edges and these inconsistencies are used to detect the forgery. Following Figures describes how two images are spliced to form the third one.

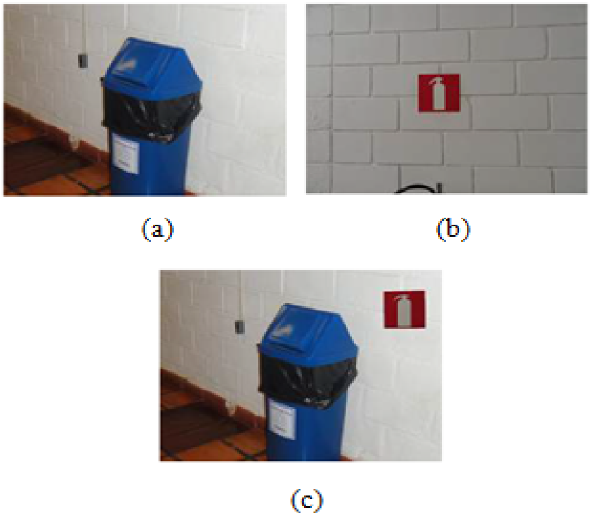

Fig. 3. Example of image splicing forgery. (a) - (b) Pristine images. (c) Forged image.

C. Image Retouching

Image Retouching is an incredibly common and potentially least-harmful kind of digital alteration. Instead of completely changing the subject of the photo, retouching is enhancement or reduction of certain features in the image. Modification of the image using any image editing tool to achieve some specific result such as to make fun of others comes under this

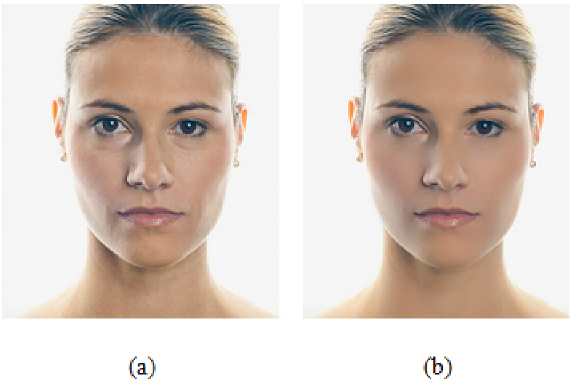

Fig. 4. Example of retouching. (a) Pristine images. (b) Forged image.

category. It is a balancing act and an art. Retouching makes the images look as real as possible. No matter which camera is used to take pictures, it is possible to retouch each photo to get rid of any flaws later on. Retouching involves a lot of treatments like basic colour correction, glamor retouching, skin retouching, photo restoration, photo cartooning etc. Image retouching detection is carried out by trying fine enhancement, colour changes and illumination changes in the forged image. The most common users of this technique are magazines or other photo-heavy publications. By altering the images used on their covers or in their articles, such publications can make the subjects of the photos seem more attractive and encourage buyers to purchase the publication, disregarding the ethical problems of such an action. One best example of retouching is shown in figure 4.

D. Image Inpainting

In the past few years, image inpainting has made great progress and is now playing an important role in content correction and image restoration. Image inpainting is a technique used for image restoration that can recover the lost information in old photographs and remove scratches in images. However, it could also be exploited to remove image semantic objects for malicious motives. In this case, image inpainting becomes a forgery manipulation. Inspired by real techniques for painting restoration, image inpainting methods fill the holes left by object removal by exploiting the information preserved in the surrounding regions. Object removal achieved by image inpainting can preserve texture and structure continuity.

Based on their application in image restoration, inpainting techniques can be mainly divided into two categories. One is pixel-based approaches which are mainly focused on structural repairing and used to repair small-scale defects (such as cracks, and scratches). However, it will generate obvious blur when the damaged region is large or the texture is rich. The other one is exemplar-based approaches, which combine structure recovery with texture repairing and can be used to restore the larger loss of information in the image. As a result, it leaves no obvious traces of tampering, which makes passive image forensics extremely challenging. Fig. 5 shows an example of image inpainting forgery.

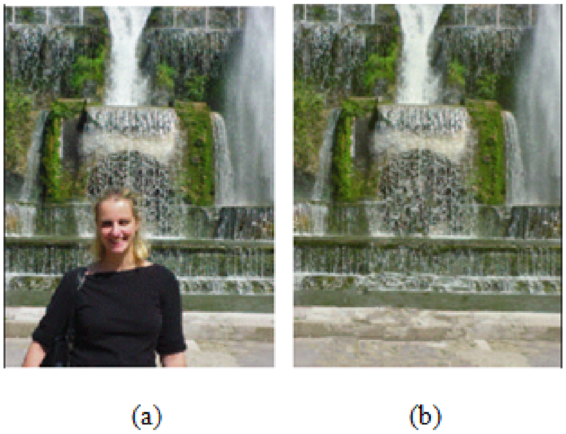

Fig. 5. Example of retouching. (a) Pristine images. (b) Forged image.

III. FORGERY DETECTION AND LOCALIZATION TECHNIQUES

There are two main problems in image forensics, one is forgery detection and the other one is forgery localization. Forgery detection aims to discriminate whether a given image is pristine or fake. Image localization aims to locate the exact location at which forgery is done. In image forensics, passive approach is followed to detect and localize forgery. The Basic idea behind the passive approach is that, although the tampering may not leave any visual clues, some of the underlying statistical features might have changed. These features can be used for detecting forgery. The set of image forensic tools can be roughly grouped into five categories [1]: 1) pixel-based techniques that detect statistical anomalies introduced at the pixel level; 2) format-based techniques that leverage the statistical correlations introduced by a specific lossy compression scheme; 3) camera-based techniques that exploit artifacts introduced by the camera lens, sensor, or on-chip post processing; 4) physically based techniques that explicitly model and detect anomalies in the three-dimensional interaction between physical objects, light, and the camera; and 5) geometric-based techniques that make measurements of objects in the world and their positions relative to the camera.

An Image Forgery Detection System (IFDS) [2], a kind of Pattern Recognition System (PRS) which intends to assign one of prespecified categories to an unknown input pattern (object), is the fundamental framework for detecting image tampering. In IFDS the pattern is an image and the categories are specified as authentic and tampered. A typical IFDS consists of five main components (steps) which are: preprocessing, features extraction, feature selection, classification, and evaluation. The output of each step is considered as an input to the next step. The input image is processed first and then the features are extracted from it and only the important features will be selected. Then, the selected features are used to train and build the classifier. Finally, the performance of the classifier is evaluated. In order to develop the system with high detection accuracy, each step should be designed carefully.

For a Copy - Move forgery detection system (CMFD) pattern matching can be used while classification can be used in the image splicing detection system.. So instead of using selected features for training the classifier, it will be used for pattern matching as shown in figure 6.

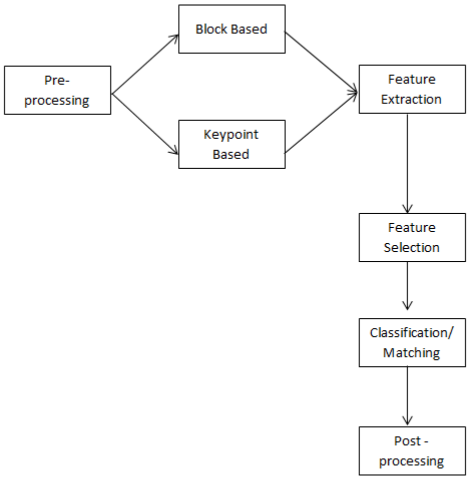

Fig. 6. General Copy move forgery detection

A. *Copy- Move Forgery Detection Techniques*

In this section, we discuss state-of-the-art image forgery detection techniques, which focus on detecting copy-move forgery only. Most of the techniques that have been used in copy-move forgery detection utilize the nature of this kind of forgery; where the copied and pasted parts are included in the same image. The existing of identical or similar parts is used as an indication of tampering. These techniques can be categorized into Block-based methods and Keypoint-based methods .

1) Block Based Methods: In this method, an image is broken up into blocks, and then a feature vector is extracted from each one. To figure out the similar area, most methods involve lexicographic sorting which recognizes similar vectors. In this kind of sorting, feature vectors are ordered into rows in form of a matrix. Then, this matrix is sorted in row-wise format, so similar vectors appear consecutively. The discriminating factor among these methods is the block shape and the type of features used to represent each block.

Weiqui Luo et al. [3] presents a technique for region duplication forgery detection. It follows the concept that, in an image, there will never have 2 very similar regions. The Input image is divided into several overlapped regions of blocks and compares the similarity among blocks and identifies the duplicated region. The basic concept behind this technique is that in an image, there will never have 2 very similar regions that are larger than .85% of actual image size. But this technique cannot distinguish between original and duplicated region. Fridrich et. al. [4] commenced the research on the copy move detection. They proposed to extract quantized DCT (Discrete Cosine Transform) coefficients of all overlapping blocks. Lexicographic sorting was also exploited in the matching stage in order to overcome the computational complexity.

An improved DCT-based technique has been proposed in [5]. It is robust for JPEG compression and blurring distortion. The method works as the following. First, DCT is computed for each block. Then, a quantization matrix is applied to DCT coefficients. After that, the quantified coefficients are rounded to the nearest integers and then they ordered in a zigzag order to form a feature vector. If the difference between two feature vectors is less than the threshold value then they have a similar content, which interprets as cues of tampering. It has been tested on few grayscale images selected from Columbia University dataset. The accuracy rate achieved to detect tampered regions is about 85%. Cao et al. [6] proposed another detection algorithm based on enhanced Discrete Cosine Transform (DCT). Instead of using rectangular blocks, it uses circular blocks. From each block, DCT coefficients are extracted and quantized to form a feature vector. It involves low dimension feature vectors and because of this, its computational complexity is low. It has been tested using nine images taken from three different datasets Columbia , uncompressed color PNG Kodak dataset and their own dataset. It can successfully detect 80% of the tempered regions with FPR less than 13%.

Cozzolino et al. [7] proposed a new algorithm for the accurate detection and localization of copy-move forgeries, based on rotation-invariant features computed densely on the image. Here, the PatchMatch algorithm was used to compute efficiently a high-quality approximate nearest neighbor field for the whole image. Some other techniques have been proposed to improve the efficiency. Christlein et. al. [8] proposed an algorithm for the filtering phase in which the underlying affine transformations between the duplicated regions are estimated. Random sample consensus (RANSAC) was also employed to estimate affine transformations in which mismatched points (outliers) are discarded using a random process. Moreover, in [9], a matching threshold is adapted for each block. The effect of utilizing the adaptive threshold is the higher performance in the matching step, and therefore in the rest of the detection phases. PatchMatch [10] (a matching algorithm based on random search) is also suggested and utilized to detect CMFD. The major drawback of this type of techniques is their limitation in detection the scaled and rotated tampered regions. In addition, they require high computational complexity due to the blocks matching.

2) Keypoint Based Methods: As an alternative to the block-based methods, keypoint-based forgery detection methods were proposed, where image keypoints are extracted and matched over the whole image to resist some image transformations while identifying duplicated regions. Some works have recently appeared on copy-move forgery detection based on Scale Invariant Features Transform (SIFT) or Speed up Robust Feature (SURF) features. Amerini et al. [11] proposed a novel methodology to support image forensics investigation based on SIFT features, which are used to robustly detect and describe clusters of points belonging to cloned areas. After detection, these points are exploited to reconstruct the parameters of the geometric transformation. Jaberi et al. [12] adopted keypoint-based features for copy-move image forgery detection, which employing a new set of keypoint-based features, called MIFT, for finding similar regions in an image. To estimate the affine transformation between similar regions more accurately, an iterative scheme was proposed which refines the affine transformation parameter by finding more keypoint matches incrementally. Chen et al. [13] proposed an effective method to detect region duplication based on the image interest points detected through the Harris corner detector. After the interest points are obtained, a rotation robust image region description method based on step sector statistics is proposed to give a unique representation for each small circle region around the interest points. Then the matching of the representations of the interest points will reveal the duplicate regions in the forged digital images. Although these methods can locate the matched keypoints, most of them cannot locate the forgery regions very well; therefore, they cannot achieve satisfactory detection results and, at the same time, a sustained high recall rate.

M. F. Hashmi [14] proposed a method to detect copy move forgery using DWT and SIFT. This paper proposed an algorithm of image-tamper detection based on the Discrete Wavelet Transform i.e. DWT. DWT is used for Dimension reduction, which in turn improves the accuracy of results. First DWT is applied on a given image to decompose it into four parts LL, LH, HL, and HH. Since LL part contains most of the information, SIFT is applied on LL part only to extract the key features and find descriptor vector of these key features and then find similarities between various descriptor vectors to conclude that the given image is forged. This method allows us to detect whether image forgery has occurred or not.

In paper [15] Chi Man Pun et.al proposed an adaptive over-segmentation and feature point matching algorithm to deal with copy move forgery. This scheme integrates both block-based and keypoint based forgery detection methods. This scheme can detect flat regions as well.

B. Splicing Forgery Detection Techniques

Image acquisition involves multiple steps where some fingerprints maybe left on the camera images that are related to the camera model and its single sensor. However, the issue is that these features are permanent. It is because when splicing of images taken with different cameras take place then the final composition of images will produce inconsistent patterns. The inconsistencies found in the sensor pattern noise obtained from the image are analyzed first by Lukas et al. [16]. For different areas of the image, the noise patterns are calculated and correlated to corresponding regions found in the reference pattern of the camera. Then, by comparing the region of interest correlation results with the results of the other regions a decision is made. Hence, the authors reached a conclusion that even after repeated JPEG compressions, obtaining verifiable forgery detection could be done. Bayram et al. [17] proposed a method that identifies the camera used to take an image using RGB color channels interpolation. The color surface interpolation occurs because of using a color filter array (CFA). In order to classify the image, SVM is applied. The accuracy rate of experiments carried out on 140 images is 89.3%.

In [18], Angelopoulou and Riess proposed a different approach that uses lighting based methods to detect tampering, by using a method that estimates the color of the illuminant from a single image. The image is first segmented into regions of similar color. The user selects suspect regions among these and a map is generated which shows how much each region is illuminated consistently with respect to the dominant illuminant colors. Amerini et.al [11] proposed a method to distinguish and then localize a single and a double JPEG compression in portions of an image through the use of the DCT coefficients first digit features and Support Vector Machine (SVM) classifier is employed.

C. Techniques dealing with Copy-move and Splicing Forgery

David et al. [19] proposed an image forgery localization technique which fuses the outputs of three complementary tools, based on sensor noise, machine-learning and block-matching, respectively. To apply the sensor noise tool, a preliminary camera identification phase was required, followed by estimation of the camera fingerprint, and then forgery detection and localization. The machine-learning is based on a suitable local descriptor, while block-matching relies on the PatchMatch algorithm. A decision fusion strategy is then implemented, based on suitable reliability indexes associated with the binary masks.

G. Muhammad et al. [20] implemented a method that works on Chroma Channel. First, it applies The Steerable Pyramid Transform (SPT) on Chroma component (i.e. Cb and Cr of YCbCr system) which results in multi-scale bands. Then it computes LBP histogram from each band. Finally, it combines the histograms of all bands and using them as features. For classification, a SVM is used. It gives 95.2% accuracy in Cr while Cb gives 93.8%. Y. Zhang et al. [21] are also employed LBP operator in their method. Instead of using chroma component, they used grayscale images. The method first applies Multi-size DCT on the grayscale image. Then it exploits LBP operator to estimate the magnitude of each BDCT coefficients. After that, all the LBP operators are combined to construct the features vector. Finally, Principle Component Analysis (PCA) is used to decrease the dimension of the features vector. The method was evaluated on Columbia dataset. SVM with RBF kernel is used for classification. The highest detection performance achieved was: accuracy= 89.93%, TPR=90.52% and TNR=89.32%.

Musaed Alhussein [22] proposed an image tampering detection method based on local texture descriptor and extreme learning machine. The image was divided into luminance and 2 Chrominance components where each of these channels were divided into non-overlapping blocks. Then local binary pattern was extracted from each of these blocks and histograms of the patterns of all the blocks were concatenated to form a feature vector. This feature vector is then fed to an ELM for classification. This method was evaluated on CASIA v2.0 and obtained 97.4% accuracy.

H. Li et al. [23] proposes a framework to improve the performance of forgery localization via integrating tampering possibility maps. In this framework results of statistical feature based detector and copy-move forgery detector are adjusted to obtain tampering possibility maps. In Statistical feature based detectors for detecting splicing forgery, the image is divided into overlapping blocks and SCRM features are computed for each of these blocks and later these feature vectors are trained using Ensemble classifier. A modified patch match algorithm is used to detect copy move forgery. Then these tampering possibility maps are fused to obtain the final localization results. This method achieves the F1-score of 0.4925, and outperforms the existing method by about 4%, implying a significant improvement in image forgery localization.

Inferences

In this paper, various approaches of image tampering and image forgery detection techniques have been reviewed and discussed. Image Splicing and Copy Move are the 2 main approaches in image tampering. A number of block based and keypoint based methods are developed so far to detect copy move forgery. Block based approach along with machine learning techniques makes splicing forgery detection more accurate. Pattern matching is the key concept behind Copy move forgery detection. All the methods and approaches discussed in this paper are able to detect forgery, but some are specific to the type of forgery. Some techniques are not effective in terms of forgery localization. Identification of the source and the pasted region is one of the main challenges to be addressed in Copy move forgery.

References

[1] H. Farid, Image forgery detection, *IEEE Signal Process. Mag.*, vol. 26, no. 2, pp. 1625, March 2009.

[2] Rachana, Ashok Kumar, H.L.Mandoria, Binay Pandey, "Study and Analysis of Copy-Move Forgery Detection in Digital Image: A Review", *International Research Journal of Engineering and Technology (IRJET)*, vol. 3, pp. 1246-1252, june 2016.

[3] W. Luo, J. Huang, and G. Qiu, Robust detection of region-duplication forgery in digital image, in *Proc.18th Int. Conf. Pattern Recognition,* vol. 4,pp. 746749, August 2006.

[4] J. Fridrich, D. Soukal, and J. Luk, "Detection of copy-move forgery in digital images " in *Proc. of Digital Forensic Research Workshop*, 2003

[5] Y. Cao, T. Gao, L. Fan, and Q. Yang. "A robust detection algorithm for copy-move forgery in digital images," *Forensic Science International*, vol. 214, pp. 33-43, January 2012.

[6] T. G. b. Yanjun Cao , Li Fan , Qunting Yang, "A robust detection algorithm for copy-move forgery in digital images", *Forensic Sci. Int.*,pp. 33-43, January 2012.

[7] Cozzolino D, Poggi G, Verdoliva L, Copy-move forgery detection based on patchmatch, in *International Conference on Image Processing (ICIP), Paris,*, pp. pp 53125316, 2014.

[8] V. Christlein, C. Riess, and E. Angelopoulou, "On rotation invariance in copy-move forgery detection", *IEEE Int. Workshop on Information Forensics and Security*, pp. 1-6, 2010.

[9] C. Barnes, D. B. Goldman, E. Shechtman, and A. Finkelstein, "The PatchMatch randomized matching algorithm for image manipulation", *Commun. ACM,* vol. 54, pp. 103-110, November 2011.

[10] C. Barnes, D. B. Goldman, E. Shechtman, and A. Finkelstein, Patchmatch: A randomized correspondence algorithm for structural image editing,*ACM Trans. Graph.* , vol. 28, no. 3, pp. 24:124, August 2009.

[11] Amerini I, Ballan L, Caldelli R, "A SIFT-based forensic method for copy-move attack detection and transformation recovery", *IEEE Trans. Information and Forensics Security* 10991110, September 2011.

[12] Maryam Jaberi, George Bebis Muhammad Hussain, Ghulam Muhammad ,Improving the Detection and Localization of Duplicated Regions in Copy-Move Image Forgery, *IEEE Int. Workshop on Information Forensics and Security*, October 2014.

[13] Chen L, Lu W, Ni J, Sun W, "Region duplication detection based on Harris corner points and step sector statistics", *J Visual Communication Image Represent* , pp.244254, April 2013.

[14] M. F. Hashmi, A. R. Hambarde and A. G. Keskar, Copy move forgery detection using DWT and SIFT features, *13th International Conference on Intellient Systems Design and Applications, Bangi*, pp. 188-193, 2013.

[15] Chi-Man Pun, Xiao-Chen Yuan, Xiu-Li Bi1, Image Forgery Detection Using Adaptive Over-Segmentation and Feature Point Matching, *IEEE Transactions on Information Forensics and Security*, 10 (8), pp.1705-1716, April 2015.

[16] Lukas J, Fridrich J, Goljan M, "Detecting digital image forgeries using sensor pattern noise", in *Proc of Security, Steganography, and Watermarking of Multimedia Contents VIII, part of EI SPIE*, February 2006.

[17] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery", in *IEEE ICASSP*,pp. 1053-1056, April 2009.

[18] C. Riess and E. Angelopoulou, Scene illumination as an indicator of image manipulation, in *Proceedings of the International Conference on Information Hiding*, pp. 6680, 2010.

[19] D. Cozzolino, D. Gragnaniello, and L. Verdoliva, Image forgery localization through the fusion of camera-based, feature-based and pixelbased techniques, in *Proc. IEEE Int. Conf. Image Process.*, pp. 53025306, 2014.

[20] G. Muhammad, M. Al-Hammadi, M. Hussain, and G. Bebis, "Image forgery detection using steerable pyramid transform and local binary pattern," *Machine Vision and Applications*, pp. 1-11, September 2013.

[21] Y. Zhang, C. Zhao, Y. Pi, and S. Li, "Revealing Image Splicing Forgery Using Local Binary Patterns of DCT Coefficients," in *Communications, Signal Processing, and Systems*. vol. 202, November 2012.

[22] Musaed Alhussein, "Image Tampering Detection Based on Local Texture Descriptor and Extreme Learning Machine",in *UKSim-AMSS 18th International Conference on Computer Modelling and Simulation*, April 2016

[23] Haodong Li, Weiqi Luo, Xiaoqing Qiu, Jiwu Huang, Image Forgery Localization via Integrating Tampering Possibility Maps, *IEEE Trans. Information and Forensics Security*, pp. 15566013, May 2016.