A REVIEW ON THE DIGITAL IMAGE RESAMPLING FORGERY DETECTION TECHNIQUES

Er. Harish kundra[1].Er. Nancy Mahajan[2]
[1]Head of Department, [2]Research Scholer
[1,2]Department of Computer Science & Engineering, Rayat Insitute Of Engineering & Information Technology, Ropar, (Punjab) India
[1]hodcseit@rayatbahra.com, [2]nancymahajan000@gmail.com

***ABSTRACT*: With the development of image editing software a variety of exquisite images are presented, at the same time a great doubt on the authenticity of the image has appeared, so the authenticity identification of images make people helpless. Therefore, the technology of image forensic is raised. Digital image forensics seeks to authenticate image based on statistical patterns left on an image by tampering. The basic concept of image forgery is the digital manipulation of pictures with the aim of distorting some information in these images. Some images have a portion of the picture altered by some common geometric transformations such as translation, scaling and rotation is known by the term Resampling. Resampling causes certain pixels be a linear combination of its neighbors. These pixels are correlated with its neighbors and will appear periodically in the resampled image. Forgers make a copy of the portion of the picture; make changes to it by geometrically modifying that portion of the image. In this paper, we are presenting an overview on the existing digital image resampling/rotation forgery detection techniques. Also a study on digital image authentication concepts is described with explanation of active and passive methods of forgery detection.**

***KEYWORDS*: Image Resampling, Angular Rotation, Image Forensics,**

I. INTRODUCTION

Manipulation of digital media was almost impossible hardly 20 years ago, which is quite common now a day. The growing demand of digital photography has explored new work in the field of image forensic. Reasons to use the digital image are many; like digital camera that produce immediate images, along with the flexibility to the person for deciding to select the appropriate one without waiting for the development of the film. Also digital images can be stored easily. While considering the originality of the digital image, it is quite difficult for the researcher to decide the authenticity of the image. Due to easy manipulation on digital image along with challenges to detect the original one, a new field of image forensic has attracted many researchers [1]. Usually digital image forgeries are created by copy-pasting a portion of an image onto some other image. Forged area is often resized & rotated to make it proportional with respect to neighbouring unforged area. This is called as resampling operation which changes certain characteristics of the pasted portion. To create a high quality forged image, some selected regions have to undergo geometric transformations like rotation, scaling, stretching, skewing, flipping etc. The interpolation step plays a central role in the resampling process and introduces non-negligible statistical changes [2]. Resampling introduces specific periodic correlations into the image. These correlations can be used to detect forgery caused by resampling [3]. Thus resampling is the default fingerprint present in most of the forged image and resampling detection became a standard tool in digital image forensics. Generally resampling artifacts are not visible to human eye in interpolated images but periodic correlations get introduced in image pixels because of it. These periodic interpolation artifacts present in pixel intensities or other format of data representation such as DFT, wavelet are the features which detectors look for in order to decide if an image, or a segment of image, has undergone a geometrical transformation [4]. In this paper, we are presenting a review on the existing digital image resampling forgery detection techniques with complete description of active and passive image detection algorithms. Rest of the paper is presented in the following manner:Section II describes the different forgery detection methods including the authentication concept of active and passive methods, Section III briefs about the image resampling, Section IV discusses about the Different forgery detection methods and Section V concludes the paper with some future refrences.

II. DIGITAL IMAGE FORGERY DETECTION

Digital images are major sources of information for each field. It can be found in the form of newsletters, magazines, internet imagery etc. But the only question raises is about the trustworthiness of the digital images. Latest imagery tools can embed data on images in such a way that it becomes difficult to find the fraudness in images. Image forgery covers this concept of this fraudness of images. Forgery detection can be described in the form of authentication of the image and can be classified into broad categories of Active and Passive forgery detection techniques [5]. Figure 1 shows this classification of forgery detection concepts. This classification is based on the concept of availability of original image and prior data.

A. Active Methods

Active methods are those methods where the prior information and data is present to check the authentication & forgeries of image. For this a data hiding code is used to embed on the image during its generation. This code can be embedded either through camera or computer tools. These methods are further classified into digital signature and digital watermarking. We can find a lot of work on these two concepts [6][7][8]. The major drawback of this concept is that, to embed the

watermark & signature, there is the need of some prior information about the image.

B. Passive Methods:

Sometimes it is also known as image forensics and can be defined as the process of authentication of images with requirement of any proper information. With the help of software tools, it is difficult to detect the forgeries of images but the only trace can be found with the help of statics of the pixels of the image. Passive methods are further classified into forgery independent and forgery dependent methods [9][10]. Forgery dependent methods are like copy-move forgery and splicing forgery etc. Forgery independent methods are like image resampling (i.e. angular rotation of the imagery object) & lighting conditions (i.e. about the brightness and contrast of the image).

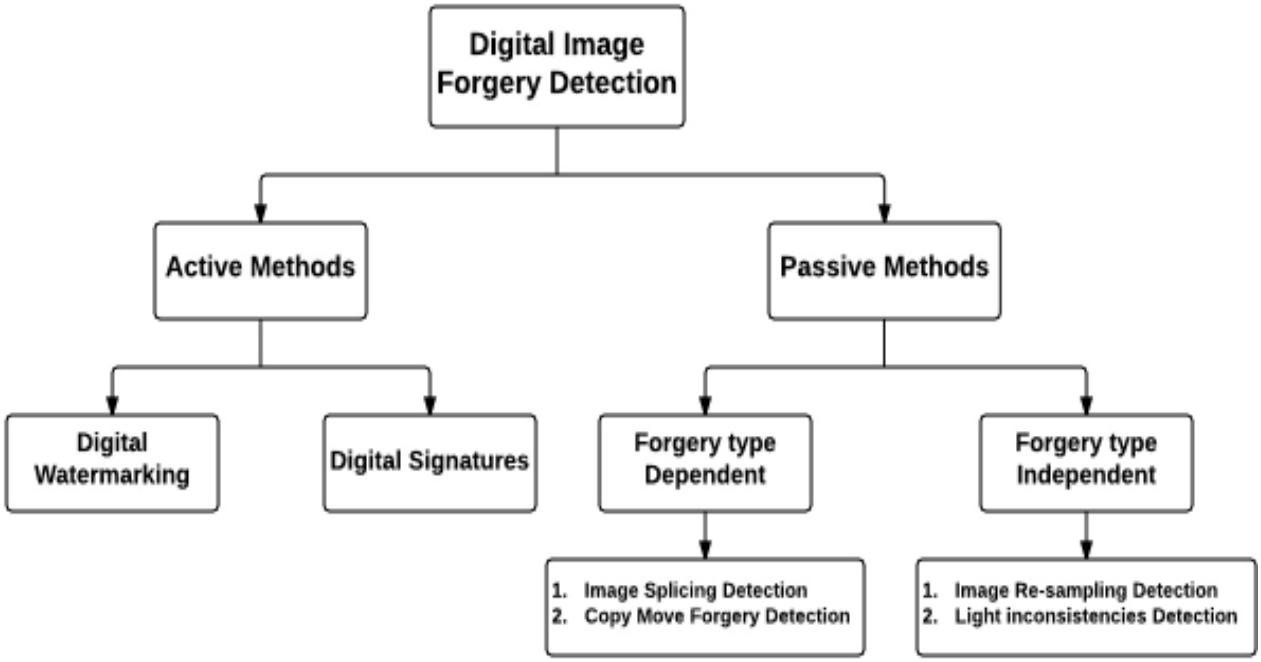

Figure 1: Classification f Digital image Forgery Detection Techniques

III. IMAGE RESAMPLING

Resampling operations roughly include rotation, scaling, stretching and so on. Sometimes it is required to perform some changes like resizing, rotating, stretching any portion of an image to produce a proper composite image. For example, if we are having an image of two persons with different heights, then to match the relative heights one person have to be resized [11]. In such process, there is a need to introduce specific periodic correlations between neighboring pixels. This is known as resampling. From the foregoing, the rank of image block which has undergone resampling will not greater than that of the original image block, resampling operations also affect the correlation between rows or columns, so the correlation dependence between the image block pixels will be influenced, whereas SVD (Singular Value Decomposition) can present the change of correlation very well so the singular value is used to detect resampling image. The correlation will be destroyed when original image is resampled and the stand or fall of image linear correlation decides the detection accuracy of the tamper image. As singular values can express linear dependence between rows or columns very well, so resampling feature can be extracted based on it. Figure 2 shows the concept of image resamling.

Figure 2: Resampled Image

IV. LITERATURE REVIEW

Weiqi Luo et al. [12] have used a vector with seven elements to describe the feature of each small blocks, a 9- dimensional vector is also introduced in [13] to solve the problem with a fixed angle rotation on the copied regions. Elements of this vector are calculated based on the intensities from four equal-sized sub-blocks on each block. The first element is the average intensity, the next four elements are ratios of average intensities and the last four elements are differences of average intensities. A radix sort algorithm is applied to perform lexicographical sorting on these vectors and a forgery manipulation is also detected. The rotation with fixed angle can be detected but not with arbitrary angles by this methods.

Time complexity is *O(9k)* and small copied regions are not be detected. The finding some features invariant to rotation is one method to deal with this problem.Hieu Cuong Nguyen and Stefan Katzenbeisser [14] proposed Radon transformation to extract the features and use phase correlation to detect the pairs of matching vectors. The proposed method is well performed for the forged images which the rotation angle of the copied region is less than 4o, has Gaussian noise addition with a SNR greater than 35dB and smaller block size 8x8 pixels. Since 2013, a new method to extract the image features by describing the spatial structure of the gray image texture called Local Binary Pattern (LBP) was introduced by Leida Li [15]. In the case of color image, it should be first converted to gray image by using I=0.299R+0.587G+0.114B and apply low pass filter to obtain the low frequency features which is more stable than the high frequency ones. As the previous methods, the feature matching is defined based on the threshold. Moreover, the post-processing including a special designed filter and morphological operations is also considered in the process of detection. The method is robust to JPEG compression, noise contamination, blurring, rotation and flipping. However, it is difficult to detect the rotated regions with general angles. Investigation of invariant block features and appropriate selection of the dimension of features are suggested to improve the random rotation. The achievement of detecting a manipulated image in which the copied area is rotated with arbitrary angles was introduced by Hailing Huang [16] in 2008. This method extracts keypoints which are invariant to changes in location, rotation, scale from an input unknown image using Scale Invariant Feature Transform (SIFT) algorithm including four steps: Scale-space extrema detection, keypoint localization, orientation assignment and keypoint descriptor. Each keypoint is described by a descriptor vector which computed as a set of orientation histogram on 4x4 pixel neighborhoods. Descriptor vectors are compared to search matched keypoints based on Euclidian distance and a threshold called Distance ratio threshold. The higher threshold value is, the more false matching is obtained. A suitable threshold and searching strategy for keypoints matching are applied. This gives good performance on post processing consisting of JPEG compression, rotation, noise, scaling, compound image processing and will be improved to apply to low SNR and small size tampered region. Seung-Jin Ryu suggested Zernike moments [17] as a method to extract the features from the overlapped subblocks in the suspicious image. These feature vectors are then sorted lexicographically and the similarity of two adjacent blocks is calculated using Euclidian distance and a threshold to find the candidates for the forgery. The Precision (exactness), Recall (completeness), and F1-measure (both Precision and Recall) are then applied to the suspicious regions to confirm the forgery. In the case of blocks with the similar Zernike moments, to ensure the exactness of detection, calculating the distance between of the actual blocks of image will be considered. Fourier –Mellin Transform (FMT) was presented as an efficient and robust method for detecting forgery by Sevinc Bayram at an international conference on acoustics, speech, and signal processing [18]. This paper used FMT to extract the features which are robust to lossy JPEG compression, blurring, noise addition, and invariant to translation, scale and slight rotation from small overlapping blocks in the image. These features then applies lexicographical sorting to get the successive blocks with the same features or counting bloom filters to obtain the blocks having the same hash values. The forgery detection can be obtained by using a distance vector D for the suggested blocks after passing lexicographical sorting or counting bloom filters. The algorithm is applied to images manipulated by translation, scaling and slight rotation at small degrees with the complexity is *MNlog2(MN)* in lexicographical sorting and *Olength(MN)* for Counting bloom filters. M. K. Bashar [19] proposed Kernel Principle Component Analysis (KPCA) or wavelet transform to extract the features of the small blocks divided from a given image which are then lexicographically sort to suggest the similarity of corresponding blocks. In addition, an automatic technique is efficient to limit the number of similar pairs and removes the unnecessary offset frequency threshold. The paper proposes algorithms to detect forged areas with translation, flip and rotation based on the global. The results also consider to cases of addition noise, lossy JPEG compression. KPCA is the best in case of noisy and compress data, rotation of any degree compared with PCA and wavelet based. In other hand, wavelet-based feature is the best with artifact free environment. However, the other geometric operations such as scaling and shearing have not been considered yet. The newest method which combines block-based and keypoint-based methods to solve the forged image detection with rotation, scaling, JPEG compression, etc. was briefly introduced by Amanpreet Kaur [20] in 2013. Although the paper has not presented an algorithm yet, theoretical backgrounds which are analyzed is logical to develop an applicable algorithm. The effective implementation of this algorithm should be done as the future work. Mire et al. (2013) has explained different resampling detection techniques in uncompressed image as well as re-compressed JPEG images. It has been found that most of the images fail on JPEG images. Also, this concept of shifted peaks can be observed in color filter array (CFA) interpolation. Scaling can be detected only at the final re-sampling stage. Also, various experimental tests were performed on unaltered and interpolated images and comparisons with newly proposed methods were also made. They concluded that these approaches have good performance but they fail on real life forgeries and more study in this is required [21]. Qazi [22] has presented an overview of the existing blind image forgery detection techniques. In this paper, the major three techniques are discussed are copy move forgery, splicing forgery and retouching forgery. Here, the author has categorized the image splicing detection techniques in to four major categories of camera response function (CRF), model based, special domain and transform domain. The author has analysed that most of the forgery detection methods are accurate but they exhibit high level of computational complexity. Also, most of the methods are not responsible for the geometric transformations like scrolling, rotation etc. In 2015, Zhou et al. detected the tamper of images using the frequently used JPEG compression and resampling operations. These operations were introduced at the time of image resampling and were saved as JPEG files. Then the moment of DCT coefficient histogram and singular value levariance were extracted and trained by SVM. The proposed method by

experiments proved to be efficient in detecting rate for resampling compression images, especially for the rotation operation and the scale factor greater than 1 [23]. Hashem and Sulong [24] have given a review on the existing passive approaches for the detection of tempered images. The author has classified the image forgery approaches into two major parts active & passive forgery approaches. Active approaches are like watermarking and signature on images. Passive approaches covers all the image tempering approaches like splicing, retouching, copy-move, re-sampling, false captioning and image processing operations etc. There exists a lot of work on the active areas of forgery detection. So, authors choose to have a review on the passive approaches due to "no requirement of the any prior information about the image under experimentation". Passive approaches use only the statics and content of the image to check the originality/ forgeries' of the images.

V. Conclusion

In this paper, we have presented a review on the existing techniques of image resamling and forgery detection. Among available framework of forgery detection techniques 'Resampling Detection' has emerged as a very promising technique. In order to obtain convincing forgery, it is often necessary to apply a geometrical transformation to some portions of the manipulated images, requiring the application of a resampling step. Although, very efficient techniques are available to detect resampling, even then the number of tampering is also increasing. Undoubtedly, processing information can be finding out by using these techniques for a manipulated image, but the fact is that an expert can do undetectable manipulations in the image. All these demand for a new technique in the forensic as well as in the anti forensic field. So, there is the need of some technique that can give solutions like nature inspired techniques. So, for future reference, we can use some nature inspired techniques for the forgery detection.

References

[1]. Gonzalez, R. C. (2009). Digital image processing. Pearson Education India.

[2]. Farid, H. (2009). Image forgery detection. Signal Processing Magazine, IEEE,26(2), 16-25.

[3]. Popescu, A. C., & Farid, H. (2005). Exposing digital forgeries by detecting traces of resampling. Signal Processing, IEEE Transactions on, 53(2), 758-767.

[4]. Yaroslavsky, L. P. (2014). Fast Transforms in Image Processing: Compression, Restoration, and Resampling. Advances in Electrical Engineering, 2014.

[5]. Birajdar, G. K., & Mankar, V. H. (2013). Digital image forgery detection using passive techniques: A survey. Digital Investigation, 10(3), 226-245.

[6]. Katzenbeisser, S., & Petitcolas, F. (2000). Information hiding techniques for steganography and digital watermarking. Artech house.

[7]. Wang, X., Xue, J., Zheng, Z., Liu, Z., & Li, N. (2012). Image forensic signature for content authenticity analysis. Journal of Visual Communication and Image Representation, 23(5), 782-797.

[8]. Shieh, J. M., Lou, D. C., & Chang, M. C. (2006). A semi-blind digital watermarking scheme based on singular value decomposition. Computer Standards & Interfaces, 28(4), 428-440.

[9]. Ng, T. T., Chang, S. F., Lin, C. Y., & Sun, Q. (2006). Passive-blind image forensics. Multimedia Security Technologies for Digital Rights, 15, 383-412.

[10]. Luo, W., Qu, Z., Pan, F., & Huang, J. (2007). A survey of passive technology for digital image forensics. Frontiers of Computer Science in China, 1(2), 166-179.

[11]. Qian, R., Li, W., Yu, N., & Hao, Z. (2012, July). Image Forensics with Rotation-Tolerant Resampling Detection. In Multimedia and Expo Workshops (ICMEW), 2012 IEEE International Conference on (pp. 61-66). IEEE.

[12]. Luo, W., Huang, J., & Qiu, G. (2006, August). Robust detection of region-duplication forgery in digital image. In Pattern Recognition, 2006. ICPR 2006. 18th International Conference on (Vol. 4, pp. 746-749). IEEE.

[13]. Lin, H. J., Wang, C. W., & Kao, Y. T. (2009). Fast copy-move forgery detection.WSEAS Transactions on Signal Processing, 5(5), 188-197.

[14]. Nguyen, H. C., & Katzenbeisser, S. (2012, July). Detection of copy-move forgery in digital images using radon transformation and phase correlation. InIntelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2012 Eighth International Conference on (pp. 134-137). IEEE.

[15]. Li, L., Li, S., Zhu, H., Chu, S. C., Roddick, J. F., & Pan, J. S. (2013). An efficient scheme for detecting copy-move forged images by local binary patterns. Journal of Information Hiding and Multimedia Signal Processing, 4(1), 46-56.

[16]. Huang, H., Guo, W., & Zhang, Y. (2008, December). Detection of copy-move forgery in digital images using SIFT algorithm. In Computational Intelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on (Vol. 2, pp. 272-276). IEEE.

[17]. Ryu, S. J., Lee, M. J., & Lee, H. K. (2010, January). Detection of copy-rotate-move forgery using zernike moments. In Information Hiding (pp. 51-65). Springer Berlin Heidelberg.