IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 23, Issue 6, Ser. I (Nov. –Dec. 2021), PP 35-39
www.iosrjournals.org

A Literature Review on Image Tampering Detection Techniques

Chithra Shaji Thomas
Assistant Professor
Department of Computer Science and Engineering
Mount Zion Institute of Science and Technology
Alappuzha, India

Abstract: *Digital images become popular for transferring visual information. There are many advantages for using these images instead of traditional camera film. Digital cameras produce instant images. These images can be viewed without the delay of waiting for film processing. There is no need of external development or processing. They can be stored easily because digital images do not take additional physical space. It can also be widely distributed electronically without time delay. But it is important to check the authenticity of digital images while using them. Because comparing to conventional images, the alteration in digital images are much easier. Many techniques are available in the field of image forensics to detect manipulations done in an image. In this paper, we discuss the various image tampering detection techniques used to find manipulations done in an image.*

Keywords: *Digital images**,**image forensics, authenticity, tampering, manipulations*

Date of Submission: 12-11-2021 Date of Acceptance: 28-11-2021

I. INTRODUCTION

"A digital image is a representation of a two-dimensional image as a finite set of digital values called pixels"[16]. Resolution of an image is related to number of pixels in a spatial measurement of a physical image[16]. Resolution of a digital camera can be finded out by multiplying the width and height of the pixel dimensions[16].A digital image is stored in bits. So it can also be characterized in terms of bit depth. The greater the bit depth of an image is, the greater the number of colors that can be represented. Image tampering is a digital art which needs understanding of image properties and should have image manipulation abilities.The various commonly used image tampering techniques are:

A. Copy-move:

A copy-move forgery is created by copying and pasting content within the same image and post-processing it[18]. This is the tampering method in which a region of an image is copied from one part and is moved to another part in the same image[19]. Further processing such as rotation, scaling, etc. is done in the copied region. The tampered image is manipulated using techniques that make it difficult for the human eyes to discover the forgery[20]. There is also another class called copy-create forgery. It is done by taking one or more images, and copying and pasting from various areas within each image to form a forged image. This is the image forgery done using several sources.

B. Image-splicing:

Image splicing[17] is a process of cropping and pasting regions from same or separate sources. Image splicing is an image editing method to copy a part of an image and paste it onto another image. It is a simple process.

C. Resize:

Resize operation is used to enlarge or reduce the size of an image or part of an image. Image reduction,zooming and scaling are the various operations that can be done during resizing.

II. IMAGE TAMPERING DETECTION TECHNIQUES

Sintayehu Dehnie, Taha Sencar and Nasir Memon proposed a method for differentiating computer generated and digital camera images[1]. The image acquisition in a digital camera is fundamentally different from the generative algorithms deployed by computer generated imagery. This difference is captured in terms of the properties of the residual image extracted by a wavelet based denoising filter. This difference is used for differentiating computer generated and digital camera images. For a given digital camera, the pattern noise remains approximately unchanged in each image. It can be modeled as an additive noise. Also, the pattern noise

is relatively stable over the camera life span and a reasonable range of conditions such as temperature. So the assumption is made that traces of pattern noise is a reliable indicator that can be used to distinguish digital camera images from computer generated images. For testing, a reference noise pattern for a class of computer generated images is generated using a given algorithm. The pattern noise, e is obtained by applying a wavelet based denoising filter to extract the noise from each image. The reference noise pattern, e_{ref} is obtained by averaging over many instances of e .To classify a given image X as digital camera or computer generated image the normalized correlation between the residual image, $e(1)$,and the reference error pattern of a generative algorithm is computed. Finally the results show that the test camera images exhibit stronger correlation with the reference error pattern. On the other hand,computer generated images have weaker but non-zero correlation to the reference error pattern. Also,the test images from the same camera showed stronger correlation with the reference error pattern. Computer generated images exhibit weaker but non-zero correlation.
Liu Zhulong, Li Xianghua, Zhao Yuqian proposed a method for passive detection of copy-paste tampering[2]. Copy-paste processing is a frequently used method to tamper an image. Two copy-paste tampering scenarios are introduced in this paper. One is conducted between JPEG images and saved in a lossless format. The other is also conducted between JPEG images, but is saved in the JPEG format. Then analysis and detection method is simulated for the two tampering scenarios. The tampered region is detected by computing the Sum of Absolute Difference(SAD) images between the tampered image and a resaved JPEG compression image at different quality factors. There are many advantages for this method. It can be used to detect the tampered region of the copy-paste tampered image that is conducted between JPEG compressed images. It can be used to detect small tampered region. It can be used to detect the tampered region even if the inserted image or the original image is rotated. Also the method is computationally simple and effective. The disadvantage is that it is not effective in tampering scenario-1 if the JPEG Q-factors of two regions are equal or very close.

Zhipeng Chen, Yao Zhao, and Rongrong Ni proposed a method for forensics of blurred images based on no-reference image quality assessment[3]. No-reference image quality assessment can evaluate image quality without any prior information from the original image. The features are extracted from Mean Subtracted Contrast Normalized(MSCN) coefficients and fed to SVM, which can distinguish the tampered regions from the original ones and can quantify the tampered regions. In image forgery, one essential element is blurring, which can conceal the anomalies of tampered region. The blurring is usually applied only on the edge of the tampered region. Therefore edge-based approaches aim to detect the blurred edge to identify the forgery images. A no-reference image quality assessment is adopted in this proposed method that considers blind/reference less image quality evaluator(BRISQUE). In this method a figure is copied, pasted, resized and blurred in some inconsistent texture and edge. Then forgery image is created. Finally detection of tampering is done by calculating the blur score using blur scores estimation scheme. The suspicious tampered regions have been identified and quantified with blur scores. The disadvantage of this method is that, if the whole tampered image is poor resolution, then the false-alarm of detection result might be higher. Also works are essential to improve the robustness of the algorithm.

Xiaobo Zhai, Rongrong Ni, and Yao Zhao proposed a system for recaptured image detection, based on texture features[4]. A set of features based on image texture are used in this work to identiy the recaptured images. The recapture process will accompany with some image quality losses. Also the process will change the texture features of an image. Therefore the effectiveness of Local Binary Patterns Variance(LBPV) and the proposed relative contrast are studied. These two kinds of features are combined to make a distinction between real-scene images and the corresponding recaptured ones. As the recaptured images become blurred, the corresponding variance will have smaller values. Based on this analysis, the feature values of recaptured images are generally smaller than those of real-scene ones. Thus the LBPV histogram of real-scene and recaptured image will have huge difference. Thus LBPV is a suitable characteristic for detecting the recaptured image from the real one. Also,the value of relative contrast for real-scene images and recaptured images is having difference. So the relative contrast value can also be used for distinguishing real-scene and recaptured images.

Huang Yan-li, Ziu Shao-zhang, Zou Jian-cheng, and Zhou Lin-na proposed an image tampering detection method based on the consistency of illuminant chromaticity[5]. This forensics scheme is proposed with the consistency of illuminant chromaticity in the three color channels, RGB, as the identification indicator of an image. The experimental results show that the detection way, which use the chromaticity consistency of different objects in the image as the feature of image tampering forensics, works well for the modifications of copy-paste and scaling on the pasted region in the same image. Based on the theories of dichromatic reflectance model, inverse chromaticity space, and Hough space, the highlight regions of objects firstly are determined in the image and then the chromaticity values can be estimated about three color channels. Then the difference model of the chromaticity between different objects is build, and finally the difference value is compared with threshold value. If the difference of the illuminant chromaticity exceeds the threshold, the consistency of illuminant chromaticity should be broken. Hence, the image can be authenticated as doctored in this way.

Shruti Agarwal and Hany Farid proposed a forensics method using JPEG dimples[6]. The described method is a JPEG artifact that can arise depending on the choice of the mathematical operator used to convert DCT coefficients from floating point to integer values. It is shown that the commonly used floor and ceiling operators introduce a periodic artifact in the form of a single darker or brighter pixel, which is termed as a dimple, in 8x8 pixel blocks. It is shown that these JPEG dimples can be used to reliably detect a wide range of manipulations from content-aware fill to re-sampling, airbrushing and compositing. The nature of JPEG dimples, its prevalence in commercial cameras, and how this artifact can be quantified and used to detect a wide range of digital manipulations, are all described in the paper. A technique is provided to locally and globally detect JPEG dimples.

Rahul Dixit, Ruchira Naskar and Aditi Sahoo proposed a copy-move forgery detection method by exploiting statistical image features[7]. In this paper, a technique is introduced to find duplicate regions in an image, which exploits statistical features of an image. Mean and variance for this purpose here, by splitting the image into pixel blocks. Mean is used to find the contribution of each individual block with respect to pixel intensity of the entire image. Variance is used to find how each pixel varies from its neighbors in a block. The proposed method operates by splitting an image into fixed size overlapping blocks, in its frequency domain, and considering statistical features, mean and variance, of each individual block. The proposed methodology performance is evaluated by using matrices DA and FPR. Improvements which can be done includes the association of copy-scale-move and copy-rotate-move duplicated image areas.

Sondos M.Fadl and Noura A.Semary proposed an accelerated copy-move forgery detection scheme[8]. The proposed method accelerates block matching strategy. Firstly, the image is divided into fixed-size overlapping blocks. Then discrete cosine transform is applied to each block to represent its features. Fast k-means clustering technique is used to cluster the blocks into different classes. Zigzag scanning is performed to reduce the length of each block feature vector. The feature vectors of each cluster blocks are lexicographically sorted by radix sort. Correlation between each nearby blocks indicates their similarity. In this method, a fast and efficient method for CM forgery detection, by using FKM and DCT features, is proposed. It works in the absence of digital watermarking and does not need any prior information about the tested image. The method can be improved for detecting duplicated region under the influence of geometric transformations.

Yong Yew Yeap, U.U.Sheikh, and Ab Al-Hadi Ab Rahman also proposed an image copy move forgery detection scheme[9]. The method focuses on passive forgery detection on images tampered using copy move technique, better known as Copy Move Forgery Detection (CMFD). A CMFD technique consisting of oriented Features from Accelerated Segment Test and rotated Binary Robust Independent Elementary Features (Oriented FAST and rotated BRIEF) as the feature extraction method and 2 Nearest Neighbour (2NN) with Hierarchical Agglomerative Clustering (HAC) as the feature matching method is proposed. Evaluation of the proposed CMFD technique was performed on images that underwent various geometrical attacks. The disadvantage of the proposed system was that the performance degraded for images with reduced copied object size and asymmetrical scaling.

Hailing Huang, Weiqiang Guo, and Yu Zhang proposed a copy-move forgery detection method using SIFT(Scale Invariant Feature Transform) algorithm[11]. This method works by first extracting SIFT descriptors of an image, which are invariant to changes in illumination, rotation, scaling etc. Owing to the similarity between pasted region and copied region, descriptors are then matched between each other to seek for any possible forgery in images. Due to the strong stability of SIFT feature descriptors, this method has a good performance on different kind of post image processing (JPEG compression, rotation, noise, scaling etc), and is also robust to compound image processing. However, suggestions are given that further works can be done to improve the robustness against low SNR and small size tampered region.

Jing Zhang, Zhanlei Feng, and Yuting Su proposed a method for detecting copy-move forgery in digital images[14]. This technique works by first applying DWT(Discrete Wavelet Transform) to the input image to yield a reduced dimension representation. Then the phase correlation is computed to estimate the spatial offset between the copied region and the pasted region. The Copy-Move regions can be easily located by the idea of pixel-matching, which is shifting the input image according to the spatial offset and calculating the difference between the image and its shifted version.

Owen Mayer and Matthew C. Stamm proposed an image forgery detection technique using Lateral Chromatic Aberration[12]. In this method, a new methodology to detect forged image regions that is based on detecting localized LCA inconsistencies is proposed. To do this, a statistical model is formed that captures the inconsistency between global and local estimates of LCA. This model is then used to pose forgery detection as a hypothesis testing problem and derive a detection statistic, which is show is optimal when certain conditions are met. To test its detection efficiency, a series of experiments that demonstrate the proposed methodology is conducted and it significantly outperforms prior art and addresses deficiencies of previous research. Additionally, a new and efficient LCA estimation algorithm is proposed. To accomplish this, a block matching algorithm, called diamond search, is adapted. It efficiently measures the LCA in a localized region.

M. F. Fahmy and O. M. Fahmy proposed a natural preserving transform based image forgery detection scheme[13]. The proposed technique uses the fact that, the copied or tampered parts of the image, will not contain the correct camera fingerprint, of the regions it copied to. The technique is based on locating dissimilar blocks between the forged image fingerprint and its corresponding mother camera fingerprint. Dissimilarity is measured through searching for blocks in the forged fingerprint image, having the *M* largest Euclidian distance from their mother cameras fingerprint counterparts. A binary image is then constructed to mark these *M* probable tampered locations. Morphological labeling and dilation techniques, in conjunction with Natural Preserving Transform NPT of the forged image are used to get rid of isolated and superficial blocks. This is done by constructing a global binary image identifying tampered locations. This global binary image is constructed as the intersection of binary images resulting from decomposing the NPT, of the forged fingerprint, using blocks of different sizes. Cases of weakly correlated fingerprint images are also considered. Several illustrative examples are given in the paper to verify the ability of the proposed scheme to check whether the image under investigation is forged or not, and detect forgery even for weakly correlated fingerprints.

Na Huang, Jingsha He, and Nafei Zhu proposed a novel method for detecting image forgery based on convolutional neural network[10]. This method proposes to build a convolutional neural network. The proposed network involves five convolutional layers, two full-connected layers and a Softmax classifier. Resmi M.R and Vishnukumar S. proposed a novel segmentation based copy-move forgery detection method for digital images[15]. The method is used to detect copy-move forgery in digital images. This segmentation based method detects the forged area in an image by using two steps. In the first stage, the input image is segmented into independent patches and the features of these patches are compared with other patches to find the matching areas. Using the suspicious pair of patches from the first stage, a second stage of matching is done to confirm the existence of forgery using oversegmentation.

III. COMPARISON

Table 1 : Comparison of different tampering detection techniques

SL. NO.	TITLE	TAMPER DETECTION TECHNIQUE	DRAWBACK
(1)	Digital image forensics for identifying computer generated and digital camera images	Pattern noise generated using denoising filter	Less efficient
(2)	Passive detection of copy-paste tampering for digital image forensics	Computing sum of absolute difference(SAD) images	Not efficient when the JPEG Q-factors of two regions are equal
(3)	Forensics of blurred images based on no-reference image quality assessment	Using MSCN coefficients and SVM	If the tampered image is of poor resolution , the false alarm of detection result is higher
(4)	Recaptured image detection based on texture features	LBPV and Relative Contrast	Complex algorithm
(5)	Forensics of image tampering based on consistency of illuminant chromaticity	Consistency of illuminant chromaticity	Computational complexity
(6)	Photo forensics from JPEG dimples	JPEG dimple analysis	Adobe Photoshop does not introduce JPEG dimples
(7)	Copy-move forgery detection exploiting statistical image features	Exploits statistical features: mean, variance	No association of copy-scale-move and copy-rotate-move
(8)	A proposed accelerated image copy move forgery detection	FKM and DCT	Cannot detect forgery under influence of geometric transformations
(9)	Image forensic for digital image copy-move forgery detection	Oriented FAST and rotated BRIEF	Low performance for images with reduced copied object size.
(10)	A novel method for detecting image forgery based on convolutional neural network	Using convolutional neural network	Complex
(11)	Detection of copy-move forgery in digital images using SIFT algorithm	SIFT feature	Should improve robustness against low SNR and small size tampered region
(12)	Accurate and efficient image forgery detection using lateral chromatic aberration	LCA (Lateral Chromatic Aberration)	Complexity is more
(13)	A natural preserving transform based forgery detection scheme	NPT(Natural Preserving Transform)	Less efficient for weakly correlated finger prints
(14)	A new approach for detecting copy-move forgery in digital images	DWT(Discrete Wavelet Transform)	Difficult when copy-move regions lie in several sub-images
(15)	A novel segmentation based copy-move forgery detection in digital images	Segmentation	Negligible drawbacks , comparatively good

IV. CONCLUSION

Many methods are existing for image forgery detection. A study on most of these methods is done and a review is given. Many methods are existing, but the anti-forensic technique such as adding a specially designed noise called tailored noise into the image will prevent detection of forgery, even when forensic methods are applied. Future researches can be done on this area.

References

[1]. Sintayehu Dehnie, Taha Sencar, and Nasir Memon, "Digital image forensics for identifying computer generated and digital camera images," IEEE Conference Publications, Pages:2313-2316, Year: 2006.

[2]. Liu Zhulong, Li Xianghua, and Zhao Yuqian, "Passive detection of copy-paste tampering for digital image forensics," IEEE 4th International Conference on Intelligent Computation Technology Publications, Pages:649-652, Year: 2011.

[3]. Zhipeng Chen, Yao Zhao, and Rongrong Ni, "Forensics of blurred images based on no-reference image quality assessment,"IEEE Conference Publications, Pages:437-441, Year: 2013.

[4]. Xiaobo Zhai, Rongrong Ni, and Yao Zhao,"Recapture image detection based on texture features," IEEE 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Pages:234-237, Year: 2013.

[5]. Huang Yan-li, Niu Shao-zhang, Zou Jian-cheng, and Zhou Lin-na, "Forensics of image tampering based on the consistency of illuminant chromaticity,"IEEE Conference Publications, Year: 2014.

[6]. Shruti Agarwal, and Hany Farid, "Photo forensics from JPEG dimples",IEEE Conference Publications, Year: 2017.

[7]. Rahul Dixit, Ruchira Naskar, and Aditi Sahoo, "Copy-move forgery detection exploiting statistical image features,"IEEE WiSPNET Conference Publication, Year:2017.

[8]. Sondos M.Fadl, and Noura A.Semary, "A proposed accelerated image copy-move forgery detection,"IEEE Conference Publications, Year: 2014.

[9]. Yong Yew Yeap, U. U. Sheikh, and Ab Al-Hadi Ab Rahman, "Image forensic for digital image copy move forgery detection,"IEEE 14th International Colloqium on Signal Processing and its Applications(CSPA 2018), 9-10 March 2018, Penang, Malaysia.

[10]. Na Huang, Jingsha He, and Nafei Zhu, "A novel method for detecting image forgery based on convolutional neural network,"IEEE 17th International Conference on Trust,Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering, Year:2018.

[11]. Hailing Huang, Weiqiqng Guo, and Yu Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm,"IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Year:2008.

[12]. Owen Mayer, and Matthew C. Stamm, "Accurate and efficient image forgery detection using lateral chromatic aberration,"IEEE Conference Publications, Year:2018.

[13]. M. F. Fahmy, and O. M. Fahmy, "A natural preserving transform based forgery detection scheme,"IEEE International Symposium on Signal Processing and Information Technology(ISSPIT),Pages:215-217 Year:2015.

[14]. Jing Zhang, Zhanlei Feng, and Yuting Su, "A new approach for detecting copy-move forgery in digital images,"IEEE Conference Publications, Pages:362-366, Year:2008.

[15]. Resmi M. R, Vishnukumar S, "A novel segmentation based copy-move forgery detection in digital images,"IEEE International Conference on Networks and Advances in Computational Technologies(NetACT), 20-22 July 2017 Trivandrum, Pages:346-350, Year:2017.

[16]. Voruganti Arun Kumar Raj, Hochschule,"Digital image tamper detection tools,"Karlsruhe Technik and Wirtschaft,UNIVERSITY OF APPLIED SCIENCES, September 2005.

[17]. Splicing.Available:http://www.ee.columbia.edu/ln/dvmm/trustfoto/projs/splicing/homepage-splicing.png

[18]. Copy move.Available: https://www5.cs.fau.de/research/areas/computer-vision/image-forensics/evaluation-of-copy-move-forgery-detection/

[19]. Sahar Qasim Saleh, King Saud University College of Computer and Information Sciences Department of Computer Science, , "Image Splicing and Copy-Move Forgery Detection,"December 2012.

[20]. Swapnil H.Kudke, A. D. Gawande, Electronics and Telecommunication Department, Sipna College of Engineering and Technology, Amravati, , "Copy-Move Attack Forgery Detection by Using SIFT", IJITEE,Volume-2, Issue-5, April 2013.

Chithra Shaji Thomas. "A Literature Review on Image Tampering Detection Techniques." *IOSR Journal of Computer Engineering (IOSR-JCE),* 23(6), 2021, pp. 35-39.