Analysis and Detection of Image Forgery Methodologies

Vidhi P. Raval[1]
[1]Department of Computer Engineering
[1]Lok Jagruti Kendra Institute of Technology, India

Abstract—"Forgery" is a subjective word. An image can become a forgery based upon the context in which it is used. An image altered for fun or someone who has taken a bad photo, but has been altered to improve its appearance cannot be considered a forgery even though it has been altered from its original capture. The other side of forgery are those who perpetuate a forgery for gain and prestige. They create an image in which to dupe the recipient into believing the image is real and from this they are able to gain payment and fame. Detecting these types of forgeries has become serious problem at present. To determine whether a digital image is original or doctored is a big challenge. To find the marks of tampering in a digital image is a challenging task. Now these marks of tampering can be done by various operations such as rotation, scaling, JPEG compression, Gaussian noise etc. called as attacks. There are various methods proposed in this field in recent years to detect above mentioned attacks. This paper provides a detailed analysis of different approaches and methodologies used to detect image forgery. It is also analysed that block-based features methods are robust to Gaussian noise and JPEG compression and the key point-based feature methods are robust to rotation and scaling.

Key words: Image Forensic; Image Forgery; Copy-Move forgery;

I. INTRODUCTION

In today's digital world digital images are the major source of information. Images can be used as an evidence for any event in the court of law. The images broadcasted in any TV news are accepted as the certificate for the truthfulness of that news. Digital images are being used in many applications ranging from military to medical diagnosis and from art piece to user photography. Hence the digital image forensics emerges as fast growing need of the society. Thus the images are required to be authentic. Due to technology advancement and availability of low-cost hardware and software tools it is very easy to manipulate the digital images without leaving the visible traces of manipulation. It has become difficult to trace these operations. As consequences, the integrity and authenticity of digital images is lost. This modification of images can be used for some malicious purpose like to hide some important traces from an image. Thus using modified images to convey wrong information. In order to identify the integrity of the images we need to detect any modification on the image. Digital Image Forensic is that branch of science that deals at exposing the malicious image manipulation. Digital Image Forensic is a branch that deals with image authentication.

An image can be manipulated with a wide variety of manipulation techniques such as scaling, rotation, blurring, resampling, filtering, cropping, etc. We need image forgery detection technique in many fields for protecting copyright and preventing forgery. The verification of originality of images is required in variety of applications.

II. APPROACHES TO DETECT FORGERY

Now, to detect such forgery done in digital images, digital image detection techniques are classified into two principle approaches. They are: Active approach and Passive approach. In active approach, the digital image requires some pre-processing such as watermark embedding or signature generation at the time of creating the image, which would limit their application in practice. Moreover, there are millions of digital images in internet without digital signature or watermark. In such scenario active approach could not be used to find the authentication of the image.

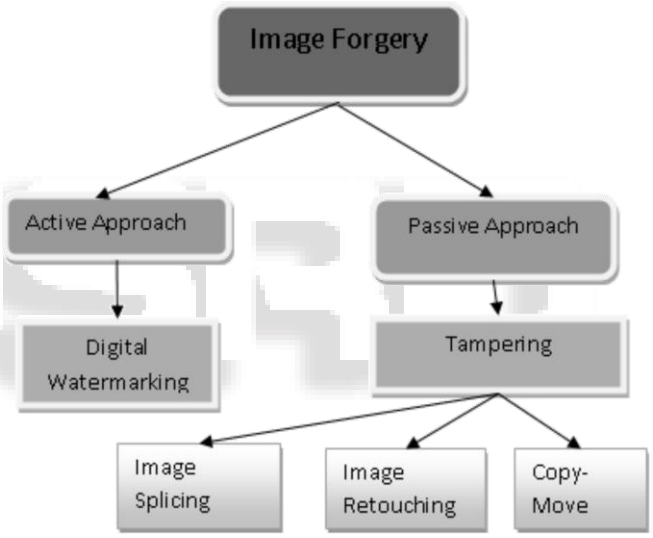

Fig. 1: Classification of Image Forgery.

Unlike the watermark-based and signature-based methods; the passive technology does not need any digital signature generated or watermark embedded in advance [1]. There are three techniques widely used to manipulate digital images [2]. 1) Tampering – tampering is manipulation of an image to achieve a specific result. 2) Splicing (Compositing) - A common form of photographic manipulation in which the digital splicing of two or more images into a single composite 3) Cloning (Copy-Move).

III. COPY-MOVE IMAGE FORGERY

Copy-Move image forgery is the widely used technique to edit the digital image. Copy-move simply requires the pasting of image blocks in same image and hiding important information or object from the image. Thus this changes the originality of the image and puts at stake the authenticity of that image. As the copied blocks are from same image they have same properties as the other blocks of image hence this makes it very difficult to detect forgery. The copied content of image which is used to perform forgery is called snippet.

A copy-move forgery introduces a correlation among the original image area and the pasted content. It is often necessary to perform post-processing of snippet of the image before pasting to create a convincing forgery. Good forgery detection method should be robust to post-processing operations, such as scaling, rotations, JPEG compression and Gaussian Noise addition. There are considerable numbers of algorithms available focusing on different post-processing on snippet.

IV. COPY-MOVE IMAGE FORGERY DETECTION WORK

First method for Copy-move forgery detection was suggested by Fridrich et al. [3]. In this method firstly the image was divided into overlapping segments and then feature extraction of these blocks was done by applying DCT. These blocks were then sorted lexicographically to find the similarity.

After then A. C. Popescu et. al. [2] applied a principle component analysis (PCA) on small fixed-size image to yield a reduced dimension discrete cosine transform (DCT) block representation. Each block was vectored and matrix was constructed. By finding the eigenvectors of the covariance matrix, a new linear basis was obtained. Then sorting the blocks lexicographically, duplicate regions are detected. This method was robust to compression up to JPEG quality level 50 and the time complexity of sorting was O(32x k log k) time.

Jing Zhang et al. [4] proposed an approach based on the idea of pixel-matching to locate copy-move regions. In this approach, DWT (Discrete Wavelet Transform) was applied to the input image to yield a reduced dimension representation. Then the phase correlation is computed to estimate the spatial offset between the copied and the pasted region. Pixel matching is done to locate copy-move region, which is shifting the input image according to

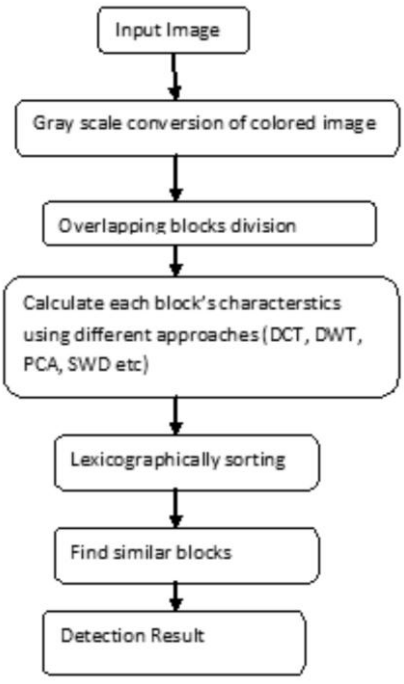

Fig. 2: Copy-Move image forgery detection system configuration

The spatial offset and calculating the difference between the image and its shifted version. At the end, Mathematical Morphological Operations are used to remove isolated points so as to improve the location. The proposed technique has lower computational complexity and it is reasonably robust to various types of Copy-Move post processing.

G. Li et. al. [5] proposed a method which reduced the time complexity for sorting to O(8k log k) time. The image was decomposed into four sub-bands by applying discrete wavelet transform (DWT). The singular value decomposition (SVD) was then applied on these blocks of low-frequency component in wavelet sub-band to yield a reduced dimension representation. Then matrix of SV vectors is sorted lexicographically to detect duplicate region.

W. Luo et al. [6] suggested a method based on the pixel block characteristics. The image was first divided into small overlapped blocks and measured block characteristics vector form each block. Then the possible duplicate region was detected by comparing the similarity of the block.

H. Huang et al. [7] presented a method to detect region duplication based on local image statistical features known as scale invariant features transform (SIFT). SIFT descriptors of an image are invariant to changes in illumination, rotation, scaling etc. First the SIFT descriptors of the image is extracted, and descriptors are then matched between each other to seek for any possible forgery in images. Even though this method enables to detect duplication, this scheme still have a limitation on detection performance since it is only possible to extract the key points from peculiar points of the image

B. L. Shivakumar et al. [8], In this method Harris Interest Point detector was used to detect the corners along with SIFT descriptors to detect copy - move forgery and then KD-Tree was used for matching the features. This method was not robust to rotation and noise.

G. Muhammad et al. [9], recently presented a method in which Dyadic wavelet transform is used. It is also shifting invariant therefore more suitable. For feature extraction DCT is used and then Euclidian distance is calculated for block matching so that copy-move region is located. This method is robust to rotation.

V. CONCLUSION

Our focus in this paper has been addressed to digital image forensics. Digital image forensics is a rapidly growing research field. Here, have introduced various existing copy move image forgery and blind methods for image tamper detection. One doesn't need the source image during detection i.e. detection is based on observation of only the tampered image. Credibility investigation is based on blind tamper detection in contrast to Digital-Watermarking technology. Tampering detection also assume no user interaction, but for current working of the algorithms some parameters are need to be provided before the running of the algorithm. These parameters can be optimised easily. Passive or blind techniques and methodologies for validating the integrity and authenticity of digital images is one of the rapidly growing areas of research. Passive methods require no extra prior knowledge of the image content or any embedded watermarks or signature. Different

image forgery detection techniques are classified and then generalized structure of image forgery detection is presented in this paper.

ACKNOWLEDGEMENT

I hereby thank to my guide Ms. Khushbu Shah, Assistant Professor in Department of Computer Engineering of Lok Jagruti Kendra Institute of Technology, India for suggesting me this line of research and helping me out in each and every manner.

REFERENCES

[1] Lou Weigi, Qu Zhenhua, Pan Feng, and Herang Jiwu, " Survey of Passive Technology for Digital Image Forensics", Frontiers of Computer Science in China, Vol. 1(2), pp. 166-179, May 2007
[2] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Technical Report TR2004-515, Dartmouth College, 2004.
[3] Fridrich, A. Jessica, B. David Soukal, and A. Jan Lukáš. "Detection of copy-move forgery in digital images." in Proceedings of Digital Forensic Research Workshop. 2003.
[4] Zhang, Jing, Zhanlei Feng, and Yuting Su. "A new approach for detecting copy-move forgery in digital images." Communication Systems, 2008. ICCS 2008. 11th IEEE Singapore International Conference on. IEEE, 2008.
[5] Li, Guohui, et al. "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD." Multimedia and Expo, 2007 IEEE International Conference on. IEEE, 2007.
[6] Luo, Weiqi, Jiwu Huang, and Guoping Qiu. "Robust detection of region-duplication forgery in digital image." Pattern Recognition, 2006. ICPR 2006. 18th International Conference on. Vol. 4. IEEE, 2006.
[7] Huang, Hailing, Weiqiang Guo, and Yu Zhang. "Detection of copy-move forgery in digital images using SIFT algorithm." Computational Intelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on. Vol. 2. IEEE, 2008.
[8] Shivakumar, B. L., and Lt Dr S. Santhosh Baboo. "Detecting copy-move forgery in digital images: a survey and analysis of current methods." Global Journal of Computer Science and Technology 10.7 (2010).
[9] Muhammad, Ghulam, Muhammad Hussain, and George Bebis. "Passive copy move image forgery detection using undecimated dyadic wavelet transform. "Digital Investigation 9.1 (2012): 49-57.

