A Comprehensive Study on Image Tempering And There Detection

Vivek Nema[1], Prachi Parwar[2]
[1]Dept of Computer science and Engineering
[2]Asst. Prof., Dept of Computer science and Engineering
[1, 2] Takshshila Institute of Engineering And Technology

Abstract- *The paper focuses on the critical evaluation and comprehensive study of the image forgery techniques. The primary focus will be on the two most prominent types of techniques applied in the field of image forensic in the form of active protection and passive detection. Furthermore, the discussion involves comprehensive analysis of the primary image forgery techniques in the form of Image Splicing, Retouching and lighting condition manipulation as well as Copy-Move Forgery which are employed in order to create tempered photographs. The meticulous work that is now being put into forging of images is leading to difficulty in distinguishing of a forged photo from an original photo and therefore it is highly needed that effective tools are developed for the detection of the images.*

Keywords- Image Forgery ,Image Forgery Detection, Copy-Move Detection,, Image Splicing ,Image Splicing Detection Image forensics, CNN.

I. INTRODUCTION

The advent of digital era has led to a heavy use of digital images globally in all forms of communication as well as knowledge sharing along with entertainment. Such a heavy use of imagery and digital images has now led to forgery in the digital images. Forgery of the digital images is now a complex, sophisticated and highly technical process aided by advance technologies and software which directly compromises the integrity of the images and aid in forging of photographs. It has been highlighted that in the present era, powerful image editing software ensure easy modifications for images and this is directly leading to eroding of the trust of the consumers on the data that is fed to them in the form of information from the images. The increase in the use of forged images in all fields ranging from magazines, political campaigns, scientific journals, advertisements, courts and other fields is now the driving factor to ensure that adequate detection techniques and tools are available which can aid in effective digital multimedia governance and regulation. The variety of software availability for development of fake digital images and their free usage policies are both the driving factors towards image forgery. Image editing software in form of Photoshop, GIMP accompanied with Corel Paint Shop, are all freely available editing software that cater and facilitate powerful image processing. The concept of image forgery as discussed by numerous researchers emphasize that it is the manipulation of any type of digital image for hiding any type of significant data from it either via addition or subtraction of any vital information pertaining to that image. The study of the existent techniques available for forging an image range from copy-move detection to splicing and they are primarily based both on their robustness as well as their computational sophistication. The forging detection techniques are subdivided into primarily two main categories in the form of active and passive forgery. The concept of active method need preliminary data pertaining to the chosen image and images which do not contain any associated prerequisite data cannot be handled from such active method. Thus any images whose source is unknown remains non-suited for forging via the use of active methods. However there is no requirement of any supplementary or preliminary data pertaining to the image and the method is based on analysis of the binary information of the chosen image without the need for any supplemental information.

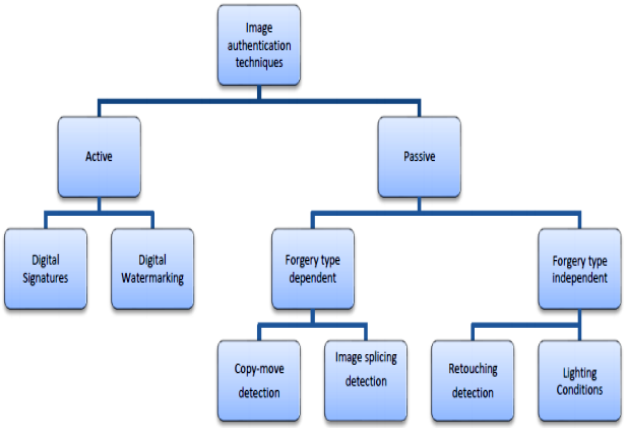
II. CLASSIFICATION OF IMAGE FORGERY

Active Image Forgery

Active Image forgery is related to Digital images we can defined it as digital signatures and digital watermarking. However, in practice this would limit their application to a major extent. Digital watermarking [4] and signature are two main active forging techniques, as something is embedded into images when they are developed . If an image cannot provide any specific information, then with the help of existing specialized tools, we can find out whether the available image has been tampered with or not. Watermarking is one such method of active tampering, since the security structure is embedded in the image, but most of the existing image tools today do not use any watermarking or signature module, it is similar to the application of active security. Using this structure means In order to check the integrity of the image, if any discrepancy is found then the image is tampered with and

the structure Inverted analysis of the image is detected by manipulating the regions of the image.

Passive image forgery is typically a major challenge in image processing techniques. There is not a single or specific method that can treat all cases, but we have several methods available that relate to a specific type of passive forgery. In passive tamper detection, the raw image is deeply analyzed based on various figures and semantics of the image content to localize the image manipulation. The security features are not inherent in passive forgery detection techniques as is the case with active forgery images, so this known as raw image analysis. Intersection localization is based entirely on image feature statistics. Therefore, the algorithm and methods of image detection and localization based on passive tampering vary depending on the type of protection used. Nevertheless, passive tamper detection is generally the objective of localization of tampering on the raw image.



III. IMAGE FORGERY DETECTION METHODS

A. Copy-Move Forgery.

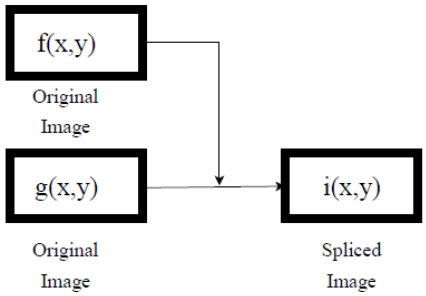
Copy-move image forgery is one of the most commonly used techniques today, it cannot be seen with people's eyes. using the copy-move technique, a new image is created by mixing any two images, It is like an image and it is not. Special software tools are used to identify this. “In Copy-Move image forgery, a part of the image is copied and pasted to another part of the same image. It simply requires the pasting of image blocks in same image and hiding important information or object from the image.” [1].

B. Image Retouching.

In image retouching it is most common used and less harmful image forgery then other types present. In this type of forgery Changing the image to the original image does not cause significant changes, but does increase or decrease some of the features of the original image. image retouching is most popular Among magazine photo editors they used this technique to enhance features of an image so that it is more attractive.

C. Image splicing

Image splicing forgery is more common then retouching forgery .it is basically simple technique can be done as cut and paste regions from the same or different sources. This feature refers to a paste- up also available with some digital image tools like Photoshop. In this technique there is piece of two or more images changing the original image radically to produce a tempered image. “Image splicing is a technology of image compositing by combining image fragments from the same or different images without further post-processing such as smoothing of boundaries among different fragments.” [2]



IV. RELEATED WORK

A. Signal processing based methods

Before technique of image forgery detection research is focused on signal processing. Therefore, many methods are proposed using interpolation marker [6]–[7]. In [8], Gallagher et al. exploit the second order derivative of image to expose the periodicity in the variance function generated by interpolation. A major downside of this method is that it cannot be applied to rotated or skewed images. Based on this, an improved approach is developed by Mahdian et al. [8]. SPT is used for discovering sub bands that make up the whole image. These sub bands usually have different intensity and angle. These sub bands are then exploited to extract LBP histograms. The intention is to use these histograms as features. An SVM classifier with linear kernel is used with these extracted features to train a binary classifier. Curvelet transform by replacing the SPT was found to be a better solution while keeping the LBP histogram phase intact. Their methods were evaluated in CASIA databases which is also the

target of our project. The authors in [10] also train an SVM classifier using features extracted maximum between-class separation of pixel pair histograms and Fourier Transform to achieve high classification rate. Gabor wavelets were the focus of the study by the authors in [11]. Only the magnitudes of these wavelets were considered. Extracted histogram Gabor magnitude after principal component analysis was fed into a statistical model. Fourier Mellin transforms results especially in copy-move image forgery detection. Compound statistical features were utilized by the authors in [11]. A wavelet-based de-noising filer was applied to extract sensor pattern noise image, which formed the basis of the compound features. The authors in [12] targeted to reduce false positives by exploiting multi-resolution LBP. An agreement protocol among random samples was maintained too for the said purpose.

B. Deep Learning based methods

In recent years, researchers begin to exploit deep learning based models, e.g. [13]–[14]. Deep learning based models are highly utilized for forged image segmentation and localization problems. Many of these models utilize the re-sampling features in image forgery detection. Therefore, the major weaknesses of these methods are similar to signal processing based methods. In an effort to be independent from re-sampling features, methods in, directly apply the neural network on the original images. Attempt to use a 10-layer CNN and use an auto encoder to perform forged image patch localization. However, their methods are prone to Over fitting on patch datasets. Employ a hybrid CNNLSTM-CNN model to capture discriminative features between the tampered and original regions. Their method focuses on the difference between edges, especially the difference of sharpness. While the sharpness of edges is a good indicator to classify tampered regions in high resolution images, it is not effective in low resolution images that are rather smooth. Gholap and Bora described dichromatic deflection method for forgery detection. It is obtained by reflection from the image. There are mainly two types of reflection from an image they are surface reflection and interface reflection. It estimates the intersection points in dichromatic deflection model. If it is greater than threshold it is identified as spliced image. Francis, Gholap and Bora identified splicing by detecting inconsistency in nose regions of the human present in the image, which is also based on dichromatic deflection model.

V. CONCLUSION

In this review papers we studied image forging, its types in details i.e.. We also studied further classification active and passive types i.e. digital watermark, digital signature, image retouching, image splicing, image. Deep learning process After that we studied active and passive image forging detection procedure in brief. Based on detection procedure, we can implement existing algorithms and by analyzing that in detail we can also invent some new algorithms in the field of image forgery detection.

REFERENCES

[1] X. Y. Jing, F. Wu, Z. Li, R. Hu and D. Zhang, "Multi-Label Dictionary Learning for Image Annotation," in IEEE Transactions on Image Processing, vol. 25, no. 6, pp. 2712- 2725, June 2016.

[2] Zhen Zhang, Ying Zhou, Jiquan Kang, and Yuan Ren, "Study of Image Splicing Detection," Advanced Intelligent Computing Theories and Applications. With Aspects of Theoretical and Methodological Issues, vol. 5226, pp. 1103-1110, 2008.

[3] Qureshi, Muhammad Ali, and Mohamed Deriche, A bibliography of pixel-based blind image forgery detection techniques, Signal Processing: Image Communication 39 (2015): 46-74.

[4] Xunyu Pan, SiweiLyu, "Region Duplication Detection Using Image Feature Matching", Information Forensics and Security IEEE Transactions on, vol. 5, pp. 857-867, 2010, ISSN 1556-6013.

[5] Mahmood, Toqeer& Nawaz Tabassam&Mehmood, Zahid&Khan, Zakir& Shah, Mohsin& Ashraf, Rehan. (2016). Forensic analysis of copy-move forgery in digital images using the stationary wavelets.578-58310.1109/INTECH.2016.7845040.

[6] Alin C Popescu and HanyFarid. Exposing digital forgeries in color filter array interpolated images. IEEE Transactions on Signal Processing, 53(10):3948–3959, 2005.

[7] Andrew C Gallagher. Detection of linear and cubic interpolation in jpeg compressed images. In Computer and Robot Vision, Proceedings.The 2nd Canadian Conference on, 2005.

[8] BabakMahdian and StanislavSaic, Blind authentication using periodic properties of interpolation. IEEE Transactions on Information Forensics and Security, 3(3):529–538, 2008.

[9] Shabanifard, Mahmood, Mahrokh G. Shayesteh, and Mohammad Ali Akhaee. ”Forensic detection of image manipulation using the Zernike moments and pixel-pair histogram.” IET Image Processing 7.9 (2013): 817-828.

[10] Isaac, Meera Mary, and M. Wilscy. ”Image forgery detection based on Gabor Wavelets and Local Phase Quantization”, Procedia Computer Science 58 (2015): 76-83.

[11] Li, Chang-Tsun. ”Source camera identification using enhanced sensor pattern noise.” IEEE Transactions on Information Forensics and Security 5.2 (2010): 280-287.
[12] Jawadul H Bappy, Amit K Roy-Chowdhury, Jason Bunk, LakshmananNataraj, and BS Manjunath. Exploiting spatial structure for localizing manipulated image regions. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2017.
[13] Belhassen Bayar and Matthew C Stamm.On the robustness of constrained convolutional neural networks to jpeg post compression for image resampling detection. In Acoustics, Speech and Signal Processing (ICASSP), 2017 IEEE International Conference on, 2017.
[14] Yuan Rao and Jiangqun Ni, A deep learning approach to detection of splicing and copy-move forgeries in images. In Information Forensics and Security (WIFS), IEEE International Workshop on, 2016.