Review of Image Splicing Forgeries

Misbah U.Mulla

M.Tech Student, Department of Computer Science and Engineering,B.L.D.E.A's Dr. P. G. Halakatti College of Engineering and Technology,Vijayapur, Karnataka, India

Prabhu R.Bevinamarad

Professor, Department of Computer Science and Engineering,B.L.D.E.A's Dr. P. G. Halakatti College of Engineering and Technology, Vijayapur, Karnataka, India

Abstract—In Today's world modification of images has become easy due to availability of various powerful software tools and applications which allows manipulation of the images and makes it to appear real. The image forgery is practiced in most of the fields such as manipulation of important government documents, wills, financial deeds and educational certificates etc. When the forged images are produced as a proof in a court room that might derive wrong decisions due to illegitimate. Hence checking the genuineness and authenticity of images is one of the most important and active research areas in digital image forensics. In this survey paper we attempt to provide an overview of different approaches for detecting image splicing forgeries.

Keywords - Forensics, Image Splicing.

I. INTRODUCTION

Digital images play a significant role in many fields and due to different tools ,advanced cameras and sophisticated softwares the manipulation of these images have become easier ,as they carry important information maintaining their integrity is very important for example they can be used as evidences in court rooms to solve different kind of cases ,in medical field ,in magazines, in newspapers ,movies and so on where the image can be changed and manipulated in such a way that it appears real ,the basic aim of image frogery detection techniques is to find out the forged image using different approaches.

In this paper, we are giving firstly the classification of the Image forgery detection. Secondly, we are giving different types of image forgery techniques and finally there is a extensive survey on different approaches for detecting image splicing forgeries.

A.Classification of Image forgery detection

Image forgery is the process of creating fake images with the help of various powerful editing tools and software which makes it hard to identify the tamperings from the original image.The image forgery detection is classified into

a . Active approach

b. Passive approach.

The Figure 1 depicts the classification and categorization of digital Image forgery.

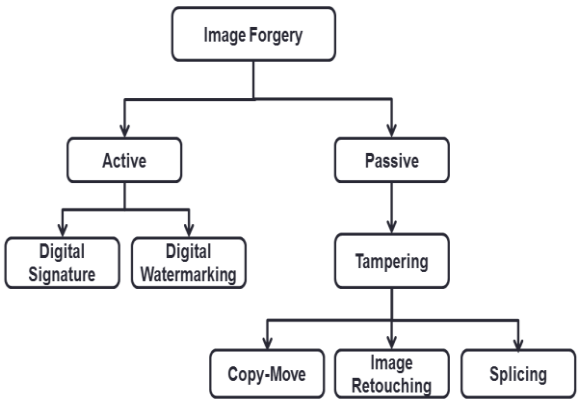

Figure1:Classification of Image Forgery detection.

some of the active approaches are digital watermarking, digital signature and these requires preprocessing such as embedding of watermark into the image or generating the signature during the image creation process and some of the passive approaches are copy move, image splicing, image retouching and in these there is no such preprocessing is done and it works on certain assumptions and algorithms and indicates the changes in underlying statistics of the image.

B.Types of image forgery techniques

1. Copy-move: It is the commonly used image forgery technique,it is the process of copying some part of image and pasting it into the other part of the same image here copy and paste is done in the same image so such tampering are difficult to detect by human eye[1]. The Figure 2 shows an example of Copy-Move forger attack. In the figure the original image (left side) contains only three missiles and its Copy-Moved version on the right has four missiles.

Figure 2: Copy-Move on Images

2. Image Splicing: Image splicing [16] is a mostly practiced process for generating forged images, defined as cutting some part of the image and pasting it into the another image without carrying out any pre-processing in others words we can say it is the process of concatinating two individual images to create a new image and the modifications are very hard to detect and just by seeing we cannot find whether the image is original or forged. The availability of image processing and editing tools and software such as photoshop helps the creation of a forged image by splicing it easily. The spliced image is difficult to identify by naked eyes but it is possible to detect the forgery with the assistance of advanced image splicing detection techniques.The Figure 3 shows an example of Image splicing attack.

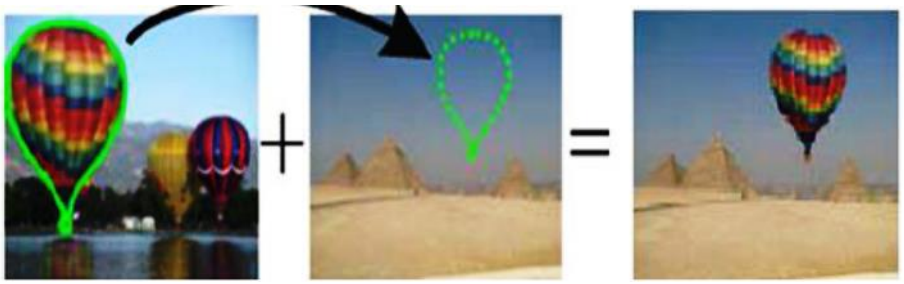

Figure 3: Image splicing forgery

3. Image Retouching: Retouching is done to make the images to appear real, it is possible to retouch any digital image to reduce the flaws in it to a far extent, Retouching involves basic photo restoration colour correction, photo Cartooning, skin retouching and so on[1],image retouching is detected by noticing the changes in the color ,illumination or any enhancements in the forged image,however it is not that difficult to find out this kind of forgery if the original image is available but detection in passive approach is difficult and challenging, the different ways of retouching images can be done using paint ,ink, air brushing or through software application available for changing the images.The Figure 4 shows an example of Image Retouching.

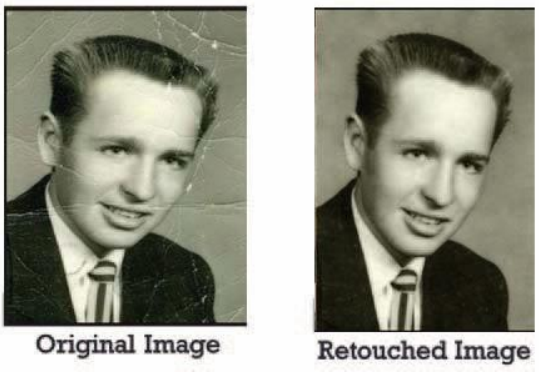

Figure 4:Image Retouching

II. LITERATURE SURVEY

The literature survey has been done to study in detail and to analyse the image splicing forgery detection techniques some of the important techniques applied for detecting image splicing forgeries has been discussed in this review paper.

In [2]authors have worked on detection of spliced images based on noise discrepancies between the original image and the spliced image ,in this first the image is divided into pixels of various scales for each and every scale the noise level function is calculated and analysed the region that is not under the noise level is termed as suspicious area and the group of pixels of suspicious area are finally identified as spliced region and the inconsistent noise level of the spliced segments indicated the presence of tamperings and the multiscale analysis generated the results,this technique is suitable to detect the splicing of multiple objects.

In[3]authors have worked on the detection of spliced image based on watermarking where two images are combined to create a spliced image and the watermark is recovered from the image which shows the presence of some noise which proves that tampering has been done to the watermarked image.

In[4] authors have implemented the forgery detection method by using HMM and SVM classifiers The digital image is represented by its feature vector where it has been transformed. LBP, Curvelet transform, DCT and Gabor filter are used for extracting features. First the system performance is tested by subjecting the image for testing on the HMM model and then with SVM as well, it was found that system performance improved when it had been trained with both the models and the results obtained by these were having some good accuracy.
In[5] a passive image forgery detection method has been used that uses entropy filter and local phase quantization texture operator. If the image is spliced than it disturbs the underlying statistics of the image which can be detected by this method, the boundary of the forged image is highlighted by the use of entropy filter in the spliced image.Hence it is because the entropy filter provides the randomness in pixel in its local neighbourhood.The another element which is used is the LPQ operator which is based on the phase information provides the in statistics of the image. In this first the image is transformed from RGB color space to YCbCr color space and the Cb and Cr components of the image are extracted, The entropy filter is applied on Cb and Cr components of image next the LPQ operator is applied on the filtered images and the feature vector is obtained by calculating the histogram of the image, and finally SVM classifier is used to classify the images into unforged or forged. Columbia, CASIA v1.0, v2.0 databases are used for image forgery evaluation that leads to classification of both forged and unforged images “This method works equally well for both type of forged images i.e. copy-move and spliced images”.

In[6] the authors have introduced a new blind detection method based on fuzzy run-length in which first the edge gradient matrix for a digital image is determined to find the gradient direction of each pixel and then quantified them to the main diagonal, minor diagonal, horizontal and vertical, directions. Then, according to the gradient direction of each pixel, such as the fuzzy run-length histogram, the fluctuation degree and count histogram are calculated than the three moments of the characteristic function of histograms are extracted and that is termed as histogram features which are used for detection of image splicing. Run length increases the features of fluctuation counting histogram to express a reasonable and huge difference in the pixel levels of the spliced images and unspliced images.

In[7] the authors have worked on“An effective passive splicing image forgery detection scheme based on Improved Local Binary Pattern (LBP) and Discrete Cosine Transform (DCT)”. The image’s chrominance

component is divided such that it results in non-overlapping blocks. Then, Improved LBP is calculated for all blocks and using 2D DCT it is transformed into frequency domain. Further the frequen
cy coefficients are evaluated to find the standard deviations for all blocks and used as features ,K-Nearest Neighbours (KNN) algorithm is used for classification.

In [8] the authors have worked on"An effective passive splicing image forgery detection scheme based on Discrete Cosine Transform (DCT) and Local Binary Pattern (LBP)". The image's chrominance component is divided such that it results in non-overlapping blocks. Then, LBP is calculated for all blocks and using 2D DCT it is transformed into frequency domain. Further the frequency coefficients are evaluated to find the standard deviations for all blocks and those acts as features. For classification support vector machine (SVM) is used.

In[9] the authors have worked on image forgery detection using weber local descriptors ,From the chrominance channels of a colorful image the multiscale WLD collects the features by extraction.The authors write about the in detail evaluation and analysis of multi scale Weber local descriptors (WLD) from image's chrominance components these features generally contains the tampering information, WLD contains the information such as gradient orientation of the pixel which is positioned at the centre, SVM is used as classifier. The experiments are carried out using Columbia, CASIA v1 and v2.0 databases. The results from experiments shown that this method hold 94.19%, 96.61% and 94.17% accuracy rate for CASIA v1.0,CASIA v2.0 and Columbia databases respectively.

In [10] the authors write about the forgery detection based On the Benford model statistical properties. For distributing the first digits of the DCT coefficients the model called statistical detection is built in discrete cosine transform (DCT) domain of the RGB channels, from every wavelet component the alternating current (AC) coefficients are extracted, and then probability distribution is determined for the most significant digit of AC coefficients in discreate cosine transform domain and the detection model of the proposed algorithm is constructed by using the Benford model.

In [11] the author presented the in detail information about image forgeries and their categories and different techniques to detect various kind of image forgeries. The common form of digital image manipulation is digital image splicing where two or more images are brought together to form an image.

In [12]authors have worked on passive image splicing detection method based on the image chroma's edge image .Experimentally it has been proved that the features of Cr and Cb component are stronger when compared with the Y component. After extraction of these features only few features are taken which are important in order to reduce the features dimension. In image splicing detection the detection of weak signal in the presence of strong signal in the background is difficult and almost impossible therefore the strong signal is removed i.e the image content by preserving safely the weak signals i.e. the image splicing edges due to which the tampered image can be detected easily, finally the optimal features are selected and SVM is applied for classification.
In [13]the authors have presented image splicing detection based on multi resolution histogram to detect the splicing between two images for this two factors are considered one is the feature that characterize image and other is the classifier which gives result of detection techniques in this the multi resolution histogram of the image act as feature which provides the spatial information of the image, and then subjected to SVM classifier to find out the image forgeries and to check whether the digital image is spliced or unspliced.

In[14]the authors have presented 12-D feature set based on the statistic moments characteristic function of run-length histograms which can be found easily and can be used for detection of tamperings in the image and due to splicing the image's corners and edges becomes more sharper when compared to regular image's corner and edges.Run is the string of pixels with same intensity of gray level,and the length of the run is the average number of repeating pixels along the run,three moments of the run length histogram of image are extracted as featutes in 12D ,these features are used for splicing detection ,SVM is used for classification purpose ,The local sharp image intensity variations are obtained using LoG detector and Sobel operator.

In[15]the authors have implemented the technique based on bicoherence features for detecting the blind image splicing forgeries,bicoherence is the normalised form of bispectrum and using bicoherence feature depending upon the image's pixel density the manipulations can be detected and finally SVM classifier is used for this purpose.

In[16] authors write about the data set, research committees dealing with data processing requires data sets with huge content and various splicing conditions to gain the progress in research studies the data set contains equal number of spliced image and authentic image blocks, which are further categorised,CASIA v1.0 dataset is used for detection of image splicing forgeries,it contains 800 authentic images and 921 spliced images in JPEG format,CASIA v2.0 dataset contains 7491 authentic images and 5123 spliced images it contains different format of images apart from JPEG,Columbia dataset is suitable for passive image authentication it contains four component image sets and the use of this dataset is restriced to only research purpose .

III.CONCLUSION

This paper presents the various existing techniques available to detect the image forgery but the main focus is on the detection of passive approach based image splicing forgeries where the images are brought together and concatinated to create a composite image and different techniques and methods are available to detect image splicing forgeries and few of them are in practice and used by image forsensic team to detect splicing tamperings,but there are many areas in passive approach to be worked on ,the methods which are existing and available for splicing detection are time consuming and also some are not cost effective,so there is a need for development of detection techniques which can be both fast and economically feasible.

REFERENCES

[1] Parameswaran Nampoothiri and V Dr. N Sugitha, “Digital Image Forgery - A threaten to Digital Forensics” in 2016 International Conference on Circuit, Power and Computing Technologies [ICCPCT].

[2] Chi-Man Pun, Bo Liu, Xiao-Chen Yuan , “Multi-scale noise estimation for image splicing forgery detection”in Journal of visual communication and image representation,pp.195-206,2016.

[3] D. Vaishnavi and T. Subashini, “Image Tamper Detection Based on Edge Image and Chaotic Arnold Map”, Indian Journal of Science and Technology, vol. 8, no. 6, pp. 548–555, 2015.

[4] M. F. Hashmi and A. G. Keskar, “Image Forgery Authentication and Classification using Hybridization of HMM and SVM Classifier.,” International Journal of Security & Its Applications, vol. 9, pp. 125-140,2015.

[5] S. Agarwal and S. Chand, “Image Forgery Detection using Multi ScaleEntropy Filter and Local Phase Quantization,” pp. 752-759,2015.

[6] Zenan Shi, Xuanjing Shen, Haipeng Chen, Xiang Li, “Blind Detection of Image Splicing Based on Fuzzy Run-Length”inInternational Conference on Computer and Information Technology;UbiquitousComputing and Communications Dependable,Autonomic and Secure Computing; Pervasive Intelligence and Computing,pp. 915-920,2015.

[7] FahimeHakimi, Mahdi Hariri,“Image-Splicing Forgery Detection Based On Improved LBP and K-Nearest Neighbors Algorithm” in Electronic information and planning ,vol.3,2015.

[8] A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, G. Bebis, and others, “Splicing image forgery detection based on DCT and Local Binary Pattern,” in Global Conference on Signal and Information Processing (GlobalSIP), 2013 IEEE, pp. 253–256,2013.

[9] S. Q. Saleh, M. Hussain, G. Muhammad, and G. Bebis, “Evaluation of image forgery detection using multi-scale weber local descriptors,” in Advances in Visual Computing, Springer, pp. 416–424,2013.

[10] Senfeng TONG, Zhen ZHANG,YongjieXIE,Xiaodi WU “Image Splicing Detection Based on Statistical Properties of Benford Model”,Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013),pp.792-795,2013.

[11] H. Farid, “Image forgery detection–A survey,” 2009.

[12] W. Wang, J. Dong, and T. Tan, “Effective image splicing detection based on image chroma,” in Image Processing (ICIP), 2009 16th IEEE International Conference on, pp. 1257–1260,2009.

[13] Jin Liu, Hefei Ling, Fuhao Zou, and Zhengding Lu, “Image Splicing Detection using Multi-resolution Histogram ”Springer, pp.858-866,2009.

[14] Jing Dong, Wei Wang, Tieniu Tan and Yun Q. Shi, “Run-Length and Edge Statistics Based Approach for Image Splicing Detection”,Springer, pp.76-87,2009.

[15] T.-T. Ng, S.-F. Chang, and Q. Sun, “Blind detection of photomontage using higher order statistics,” in Circuits and Systems, 2004. ISCAS’04. Proceedings of the 2004 International Symposium on,vol. 5, pp. V–688,2004.

[16] T.-T. Ng, S.-F. Chang, and Q. Sun, “A data set of authentic and spliced image blocks,” Columbia University, ADVENT Technical Report, pp. 203–2004, 2004.