Advanced Research in Electrical and Electronic Engineering
Print ISSN: 2349-5804; Online ISSN: 2349-5812 Volume 1, Number 3 (2014) pp. 58-60

http://www.krishisanskriti.org/areee.html

Image Authentication using Forgery Detection by Extracting Features and Estimating Positional Variance

Geetanjali Sahu[1], Usha Kiran[2]

[1]*M-Tech in CSE, Chhatrapati Shivaji Institute of Technology, Durg, Chhattisgarh*
[2]*Dept of CSE, Chhatrapati Shivaji Institute of Technology, Durg, Chhatisgarh*

Abstract: **Image authentication is very essential due to availability of various photo editing softwares with the help of which one can manipulate the image in such a way that, it is difficult to recognize whether image is original or manipulated. Different Image forgery detection methods have been developed according to technique used for making forgery. An approach for providing image authentication is presented in this paper. This image forgery detection method is based on the pixels present in the original image and forged image, where features of forged image is extracted and followed by various steps to detect any post processing operation on original image.**

1. INTRODUCTION

Basically image forgery means any post processing operation on digital image to hide or remove some useful information for making fraud or illegal purpose. Digital images can be manipulated very easily with the help of many image processing softwares. By using these softwares, it is possible to add or remove important features from an image. These kinds of alteration on images lead to serious consequences, and may create fraud in many real-world applications such as in criminal justice, journalism etc. Image authenticity is important in many Social areas. For instance, the trustworthiness of photographs has an essential role in courtrooms, where they are used as evidence.

Figure 1 Example of image forgery

Every day newspapers and magazines depend on digital images [11]. In the medical field, physicians make critical decisions based on digital images. Images can be manipulated in such a way that the tampering cannot be detected only by visualizing it. The originality of a digital image is a challenging task due to the various image processing softwares available in the market and digital images can be forged easily with these image processing software. Example of image forgery is shown in figure 1 where face of the girl in left side (which is original image) has change with another face in right side.

2. LITERATURE REVIEW

In the recent past few years, many image tamper detection techniques have been developed according to the technique used for making image forgeries. One of the basic approaches used for making image forgery is Copy-Move forgery.

Copy move forgery can be detected by different techniques which is surveys in this paper. There are various forgery detection methods.

- Exhaustive search
- Autocorrelation
- Exact match
- Robust match

According to Jessica Fridrichs, in exhaustive Search method, the image and its circularly shifted version are looks for closely matched image segments. The image is first broke and then dilates with the neighborhood size corresponding to the minimal size of the copy-moved area.[5]

According to G.R.Talmale, R.W.Jasutkar , the logic behind the detection based on autocorrelation is that the original and copied segments will introduce peaks in the autocorrelation for the shifts that correspond to the copied-moved segments [2].Exact Match algorithm is used for identifying those images

that segment in the match exactly. First of all we have to specify the minimal size of the segment that should be considered for match. The input image is of size M×N is divided into square with B×B pixel [5].

The idea for the robust match detection is similar to the exact match except we do not order and match the pixel representation of the blocks but their robust representation that consists of quantized DCT coefficients [2].According to Ahmet Emir Dirik and Nasir Memon, in the CFA pattern number estimation method based on the estimation of the CFA interpolation pattern of the image. For identifying the CFA pattern of an image, the image is re-interpolated with several factors of CFA patterns. Forgery detection can be done on the basis of Mean Square Error (MSE) value of the pixel [15].

3. PROPOSED METHODOLOGY

The proposed methodology is categorized in two parts:

- Methodology for Distinguishing PIM from PRCG
- Methodology for Detecting forged image regions

PIM refers to photographic image and PRCG refers photo realistic computer generated image. Distinguishing of PIM from PRCG can be done by Estimating positional variance & Peak Analysis of each pixel values of image. Digital cameras contain an image sensor with a color filter array (CFA) having Red, Green, Blue (RGB) components. Positional variance is obtained by interpolation of color pixels of CFA. After estimating positional variance DFT is applied to get normalized frequency, to check whether peak is strong or weak is called peak analysis. The original image contains strong peak while forged image have low peak value. forged region contains low value of peak signals. The regions having low peak signal will be forged region.

All digital cameras contains image sensor which capture the raw image that contains only a single signal value (red, green, or blue) at each pixel position. Other two color component is calculated by using interpolation, after that a complete RGB image is formed [6]. Hence in the first step it is necessary to separate each color component from RGB image for further processing, and select any one color component (red, green or blue) at a time and followed by various steps. Some time real image is appears noisy or duplicate due to image acquisition in a wrong way. So in the second step high pass operator h(x,y) is applied in the extracted green component to remove low frequency information. Where distinguishing of real image from the manipulated one can be done by estimating positional variance of each pixel in the forged image, since only green component is selected for further processing which contains only green pixel value. Hence in the next step cubic interpolation is applied on the filtered image for calculating missing pixel values. After interpolation, variances of an image are calculated by taking a square window of a set size around a center pixel, and calculate the variance of the values of the pixels. Mean gives the average over each pixel value, where central pixel is compared with threshold value which is typically 140, if this value is less than threshold value then it returns array of zero values.

At the same time Discrete Fourier Transformation is applied on interpolated image for getting normalized frequency, to check whether peak is strong or weak is called peak analysis. On the basis of this transformation we can find out whether any given image is real or forged. If the image contains strong peak while forged image have low peak value.

4. EXPERIMENTAL RESULT

The proposed method has been implemented on forged image as shown in figure 2. Where image present in the top is original image and the image present in the bottom is forged image in which extra flower is added.

(a) Original image

(b) Forged image

Figure 2 Forged image "jeep" (Bottom) and its original version (Top).

First of all we take forged image as an input, and then extract each color component for further processing. After this extraction we select green component of the same image, then this component is followed by high pass filter. Cubic interpolation is applied in the filtered image for calculating missing pixel values in green component. After calculating variance of interpolated image we get variance-map image where the region which has variance value less than threshold value is mapped as black and remaining portion is mapped as white. On the basis of this variance-map image we can conclude that the image is forged image and the region which

contain black portion is the manipulated region as shown in figure 3.

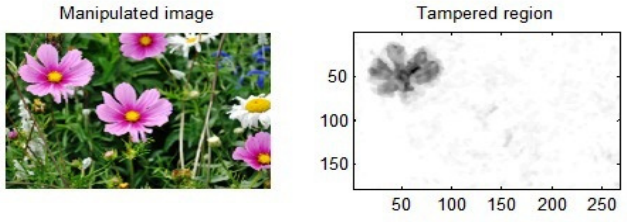

Figure 3 Forged image and its manipulated region

5. CONCLUSON

An image forgery detection method based on the pixels present in the image has been proposed. This is followed by various steps and detect whether the image is original or forged. If the given image is forged then detect the regions which have been forged. Experimental result shows that the proposed method can detect the image forgery but more accuracy is to be needed for future work.

REFERENCES

[1] Sahu, Geetanjali.'Usha Kiran.2013."Survey of Different Techniques for Image Tamper Detection on Digital Images", IJARCET.2 (1):3215-3218.

[2] Fridrich, Jessica, Soukal,David., Lukáš.,AJan.2013 "Detection of Copy-Move Forgery in Digital Images".

[3] N. Suganthi.,N. Saranya.,M. Agila. 2012."Detecting forgery in Duplicated region using key point matching". IJSRPA.2 (11):1-5.

[4] Jessie. Yu-Feng Hsu.2012. " Image Tampering Detection for Forensics Applications", ISA seminar.

[5] Murali S., Anami B., Chittapur G. B. 2012. "Digital Photo Image Forgery Techniques".IJMI.4 (1)401-405.

[6] G.R.Talmale., R.W.Jasutkar.2012." Analysis of Different Techniques of Image Forgery Detection". MPGINMC.13-18.

[7] Deshpande,Pradyumna., Kanikar, Prashasti.2012. "Detecting Forgery in Duplicated region Using key point matching".IJERA.2 (3):539-543.

[8] F. Battisti., M. Carli., A. Neri.2012. "Image forgery detection by using No-Reference quality metrics". Media Watermarking, Security, and Forensics. 8303.

[9] B.L.Shivakumar., Lt. Dr. S.Santhosh Baboo.2011. "Detection of Region Duplication Forgery in Digital Images Using SURF".IJCSI.8,(4):199-205.

[10] Frank Y., Shin., Yuan.2010. " A Comparison Study on Copy-Cover Image Forgery Detection" .OAIJ 4:49-54.

[11] V. Christlein., C. Riess.,E. Angelopoulou.2010. "A Study on Features for the Detection of Copy-Move orgeries". GISICHERHEIT.

[12] B.L.Shivakumar., Dr. S.Santhosh Baboo.2010. " Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Methods".GJST.10 (7): 61-65.

[13] Hwei-Jen Lin., Chun-Wei Wang and Yang- ta kao.2010 "Fast Copy-Move Forgery Detection".Wseas Transactions on Signal Processing.5 (5):188-197.

[14] Ahmet Emir Dirik., Nasir Memon.2009. "Image Tamper Detection Based on Demosaicing Artifacts". IEEE Trans. on Signal Processing.1497-1500.

[15] Hwei-Jen Lin., Chun-Wei Wang., Yang-Ta Kao.2009. "Fast Copy-Move Forgery Detection". WSEAS Transaction on Signal Processing,. 5(5):188-197.