International Journal of Research in Advent Technology, Vol.4, Issue 7, July 2016
E-ISSN: 2321-9637
Available online at www.ijrat.org

Forgery Detection by analyzing Individual Color Component of Digital Images

Firoj Sahu [1], Sampada Vishwas Messy [2]
CTA,CSE[1, 2]
Email: firoj.1102@gmail.com[1] *,sampada.satav@gmail.com*[2]

Abstract- Image forgery means modification of original images to wrap or delete from or to add some additional information to the original image. Now a days many advanced image processing softwares are available. By using these softwares image can be easily forged , which can not be recognized by open eyes. So for the detection of these forgeries in images some useful softwares are necessary to developed. In this paper a very efficient method is presented to detect the forgery in digital image by analyzing individual color components of digital images.

Index Terms- Image Forgery, Image processing, Color Filter Array Interpolation, Variance - Map

1. INTRODUCTION

An image forgery is an essentially concern with the alteration of the digital image to hide or to remove some useful portion of the image. Digital images can be altered 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 activities lead to serious consequences, and creating false beliefs 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. 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 is the original image and manipulation has been done in the original image where extra flower is added to upper left corner in the original image as shown in figure.

Figure 1 Example of image forger

2. LITERATURE REVIEW

In the past few years, many image tamper detection techniques have been proposed 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 Hwei-Jen Lin and Chun-Wei Wang, in this method Fast Copy- Move Forgery Detection Algorithm is used for tamper detection. In Which have the Input image is divided into four equal size sub blocks. Then the Average intensity function is calculated for each block .Ratios of average intensity of the block S1, S2, S3, & S4 to function (f1) are calculated. Differences of average intensity (f6 to f9) are calculated. Functions are normalized to integers

xi's (0 – 255).After that Radix sort algorithm is used to perform lexicographical sort. Shift vectors are defined as difference of two adjacent vectors. Accumulative no. of shift vectors is used to detect duplicate regions [13]. 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 system is based on the extraction of features of forged image which is directly related to pixels of that image. 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

$$h(x, y) = \frac{1}{16}\begin{pmatrix} -1 & -2 & -1 \\ -2 & -12 & -2 \\ -1 & -2 & -1 \end{pmatrix}$$

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. EXPERIENTAL RESULT

The proposed method can be implemented on forged image as shown in figure 2. Where left hand side image is original image and right hand side image is forged image where extra flower is added to upper left corner in the original image as shown in figure.

Figure 2 Example of image forger

Where this forged image was passed through various steps proposed in this paper and output can be obtained in two sections. First of all distinguishing whether the the input image is original or manipulated one.

If the input is manipulated then it will show the region which have been manipulated. As shown in figure 3-

Figure 3 Forged image (left) and output after experiment (right).

Here the left side image is the input forged image which was passed through various steps. And the right side image is the output after experiment in which the forge region is shown.

5. CONCLUSON

An image forgery detection method based on the features of the image has been proposed in this paper. 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.

REFERENCES

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

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

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

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

[5] G.R.Talmale., R.W.Jasutkar.2012." Analysis of Different Techniques of Image Forgery Detection". MPGINMC.13-18.
[6] Deshpande,Pradyumna., Kanikar, Prashasti.2012. "Detecting Forgery in Duplicated region Using key point matching".IJERA.2 (3):539-543.
[7] F. Battisti., M. Carli., A. Neri.2012. "Image forgery detection by using No-Reference quality metrics". Media Watermarking, Security, and Forensics. 8303.
[8] B.L.Shivakumar., Lt. Dr. S.Santhosh Baboo.2011. "Detection of Region Duplication Forgery in Digital Images Using SURF".IJCSI.8,(4):199-205.
[9] Frank Y., Shin., Yuan.2010. " A Comparison Study on Copy-Cover Image Forgery Detection" .OAIJ 4:49-54.
[10] V. Christlein., C. Riess.,E. Angelopoulou.2010. "A Study on Features for the Detection of Copy-Move orgeries". GISICHERHEIT.
[11] 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.
[12] 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.
[13] Ahmet Emir Dirik., Nasir Memon.2009. "Image Tamper Detection Based on Demosaicing Artifacts". IEEE Trans. on Signal Processing.1497-1500.
[14] Hwei-Jen Lin., Chun-Wei Wang., Yang-Ta Kao.2009. "Fast Copy-Move Forgery Detection". WSEAS Transaction on Signal Processing,. 5(5):188-197.