International Journal of Research in Advent Technology, Vol.4, No.6, June 2016
E-ISSN: 2321-9637
Available online at www.ijrat.org

Study of Techniques Available for Image Forgery Detection on 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- Any digital image can be forged easily .The term forge can be defined as any manipulation performed in the digital image i.e. addition or removal of any important features. It is too hard to detect this forgery but not impossible .There are some techniques available for detection of forgery. In this paper some important techniques are discussed .

Index Terms- Copy-Move Forger; Color Filter Array; Image Forgery; Image Processing,;Keypoints and Tampering.

.

I. INTRODUCTION

Digital images can be manipulated very easily due to availability of many image processing and editing software. By using these softwares it is possible to add or remove important features from an image. Images can be manipulated in such a way that the tampering cannot be detected only by visualizing it. The authenticity of a digital image is a challenging task due to the various photo editing software packages available in the market. Digital images can be forged easily with today's widely available image processing software. The term tamper means any post-processing operations that perform on an image. In the past few years, many image tamper detection techniques have been proposed. Example of image forgery is shown in Figure 1 where one extra bottle in left side (which is original image) has been added . In this paper we discuss different techniques of image forgery detection.

Figure 1 Example of image forgery

II. COPY MOVE FORGERY

In a Copy-Move forgery, some part of the image itself is copied and pasted into another part of the same or different image. Copy move forgery is usually performed with the intention to make an object "disappear" from the image by covering it with a segment copied from another part of the image [1]. Textured areas, such as grass, foliage, leaves, fabrics with irregular patterns, are generally used for this purpose. One cannot easily detect this type of manipulation because the copied parts come from the same image. To make the forgery more powerful, one can use the retouch tool to further mask any traces of the manipulated segments.

Examples of the Copy-Move forgery are shown in Figure 2 which is original image and Figure 3 is forged image in which truck was covered with a leaves present in the left of the truck .

,

Figure 2 Original Image

Figure 3 Forged Image

III. Literature Review

1 Detection of 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

1.1 Exhaustive search

According to Jessica Fridrich 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.

1.2 Autocorrelation

The logic behind the detection based on autocorrelation is that the original and copiedsegments will introduce peaks in the autocorrelation for the shifts that correspond to the copied-moved segments [2]. Since original images contain most of their power in low-frequencies, if the autocorrelation is computed directly for the image itself, it would have very large peaks at the image corners and their neighborhoods. Thus, we compute the autocorrelation not from the image directly, but from its high-pass filtered version.

1.3 Exact Match

According to G.R.Talmale Exact Match algorithm is used for identifying those images that segment in the match exactly [4]. 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. Then the square is slid by one pixel along the image from the upper left corner right and down to the lower right corner for each position of the B×B block. The pixel values from the block are extracted by columns into a row of a two-dimensional array A with B2 columns and (M–B+1)(N–B+1) rows. The matching rows are easily searched by going through all MN rows of the ordered matrix A, and looking for two consecutive rows that are identical. The matching blocks found in the Figure 2 are shown in Figure 4, the blocks form an irregular pattern that closely matches the copied-and-moved portion.

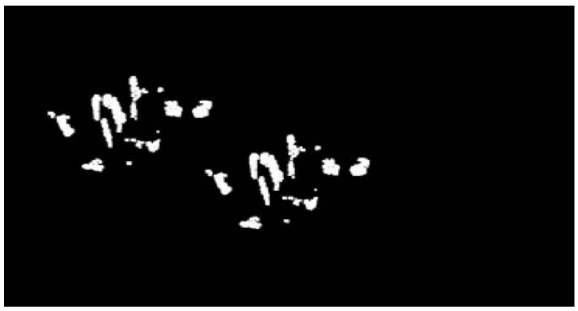

Figure 4 Result of Block Match Copy Detection Algorithm

1.4 Robust Match

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 [3]. The discrete quantization steps are calculated from a user-defined parameter Q. This parameter Q is equivalent to the quality factor in JPEG compression, i.e., the Q Factor determines the quantization steps for DCT transform coefficients. Higher values of the Q-factor lead to finer quantization, the blocks must match more closely segment. Lower values of the Q-factor produce more matching blocks.

2 Detection of Image Forgery by CFA Based Features

Almost all digital cameras contain an image sensor with a color filter array, for example, the Bayer filter array shown in Figure 5.

Figure 5 Different Bayer CFA patterns

A filter is positioned over each photo site, sensing either the red, green, or blue component of the incident light. The image from the image sensor contains only a single signal value at each pixel position. This pixel value further corresponds to only a single color component (red, green, or blue in the case of the Bayer filter array) [5]. The Color Filter Array can be use for image forgery detection. On the Basis of these CFA artifacts, there are two proposed methods. First based on CFA pattern number estimation and the secondly based on CFA based noise analysis.

2.1 CFA pattern number estimation

According to Ahmet Emir Dirik this 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. For a 2 × 2 cell CFA, there are 36 different filter arrangements, but basically digital cameras use one of the 4 Bayer CFA arrangements. Then for each of these patterns, the Mean Square Error (MSE) between the input image and re-interpolated image is computed.MSE values of the entire 4 Bayer pattern should be significantly smaller than the others[9]. If none of the 4 MSE values are significantly smaller than the others, the image may have manipulated.

2.2 CFA based noise analysis

The second way to measure CFA demosaicing artifacts is based on sensor noise power changes all across the image. If a given image is CFA interpolated, the sensor noise in the interpolated pixels is expected to be suppressed due to the low pass nature of interpolation [6]. As a result, the variance of the sensor noise in interpolated pixels becomes significantly lower than the sensor noise power in non-interpolated pixels after manipulation. CFA demosaicing artifacts can hence be measured by taking the ratio of noise variances of interpolated and un-interpolated pixels. If this ratio is close to 1, the Image is considered to be manipulated[8].

IV. PROBLEM IDENTIFICATION

After survey of various techniques of image forgery detection some Limitations of the CFA based tamper detection approach has been found that images taken with X3 Foveon sensors do not exhibit any CFA demosaicing artifacts [7]. Thus, the proposed techniques will not work for images acquired with X3 Foveon sensors[10]. Another limitation is the proposed scheme may also not work well if the tampered region area is too small.

Where as the Exact Match will work only for BMP images , if the forged image had been saved as JPEG, identical blocks would have disappeared because the match would become only approximate not exact[1,4].

V. CONCLUSION

This paper mainly focuses how to detect image forgeries. There are different methods for image forgery detection and limitations related to them. More convenience method can be developed to overcome these limitations.

REFERENCES

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

[2] N. Suganthi , N. Saranya, M. Agila. “Detecting forgery in Duplicated region using key point matching“. IJSRPA.vol.2.Issue 11.2012 .pp 1-5.ISSN 2250-3153.

[3] Murali S., Anami B. S, Chittapur G. B. “Digital Photo Image Forgery Techniques”. IJMI. Vol.4. Issue 1.2012.pp. 401-405.ISSN 0975-2927.

[4] G.R.Talmale, R.W.Jasutkar.” Analysis of Different Techniques of Image Forgery Detection”. MPGINMC.2012. pp.13-18. ISSN 0975 - 8887

[5] Pradyumna Deshpande, Prashasti Kanikar. “Detecting Forgery in Duplicated region Using key point matching“.IJERA.Vol.2.Issue3.2012.pp.539-543.ISSN 2248-9622.

[6] Frank Y. Shih and Yuan. ” A Comparison Study on Copy-Cover Image Forgery Detection” .OAIJ .vol 4.2010.pp. 49-54.

[7] B.L.Shivakumar, Dr. S.Santhosh Baboo,” Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Methods”.GJST.Vol.10.Issue7 .2010. pp. 61-65.

[8] Hwei-Jen Lin, Chun-Wei Wang and Yang- ta kao, “Fast Copy-Move Forgery Detection”.Wseas Transactions on Signal Processing.Vol. 5. Issue 5.2009.pp. 188-197.

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

[10] J. Lukáš. “Digital Image Authentication“. Workshop of Czech Technical University. 2001.