International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

A Survey on Copy Move Forgery Detection in Images

Rameeza M Ashraf[1], Veena K Viswam[2]

[1]Rameeza M Ashraf, MTech Student, KMEA, CSE Department, M.G University

[2]Veena K Viswam, Assistant Professor, KMEA, CSE Department, M.G University

Abstract: ***Nowadays, the use of digital images are increasing day to day. With the advancement in technology, newer and newer softwares like Adobe Photoshop, GIMP etc. are emerging. With these tools even a normal person can change the content from an original image. This leads to image tampering. Image tampering are of various types and one of the most common type is the copy-move forgery. Copy-move forgery is the process in which a portion of the image is copied and pasted into another portion in the same image. To make the detection difficult, a forger can apply some preprocessing operations also. By doing this, the forged region might not be visible at a glance. Since, the images are an important source of information, and is used in some legal investigations, medical fields etc. it is necessary to ensure the integrity and authenticity of an image. Therefore, an efficient detection method should be adopted to detect the forged areas.***

Keywords: Active method, Passive method, Copy Move Forgery, Copy Rotate Move, Scale Invariant Feature Transform

1. Introduction

Image forgery refers to the manipulation of the digital images. An image can be manipulated in different ways. One of the serious issues faced in the forensics field is the authentication of the digital images. There are mainly two classes of image forgery detection methods: active method and passive method. An Active method is a technique which requires some pre-embedded information like watermark and digital signatures. This method is not widely used in most of the cameras that are available nowadays do not have a feature to embed a watermark and digital signatures. Passive methods overcome this drawback as it does not require any pre embedded information. Passive image forgery detection techniques are classified into five types:

1.1 Pixel-based image forgery detection: The statistical anomalies present at the pixel level are detected by this technique. It is one of the most common technique and it is of four types.

a) **Copy move:** A copy-move is the process which involves copying and pasting content within the same image and further post processing it.

Figure 1: Copy Move Forgery

b) **Resampling:** It is a mathematical technique in which a new version of the image with different width and / or height in pixels is generated. There are two types of sampling techniques: Upsampling and Downsampling. Upsampling is the process of increasing the size of an image and Downsampling is the process of reducing the size of an image.

Figure 2: Image Resampling

c) **Splicing:** Image splicing is a common type of forgery of creating a forged image where a region from one image is copied and pasted into another image to create a composite image. This composite image is called the spliced image.

Figure 3: Image Splicing

1.2 Format-based image forgery detection: It is very difficult to detect forgery when an image is compressed. This method can detect forgery in the compressed image. It is of three types:

a) **Jpeg Quantization:** Most of the cameras encode the images in JPEG format. This lossy compression scheme provides some flexibility regarding how much compression is

achieved. The devices are configured differently by the manufacturers in order to balance the compression and quality of their needs.

b) **Double Quantization:** In this, the manipulated image is compressed twice due to the lossy nature of the JPEG image format. This double compression produces some specific artifacts that are not in singly compressed image. These artifacts can thus be used as an evidence of some manipulations.

c) **Jpeg Blocking:** The block DCT transform is the basis for the JPEG compression. Each of the 8 x 8 pixel image block is individually transformed and quantized and the artifacts are assumed to be appear at the border of neighboring blocks in the form of horizontal and vertical edges. These blocking artifacts may be disturbed when an image is manipulated.

1.3 Camera-based image forgery detection: The artifacts introduced by the camera lens, or sensors are exploited by this technique. These techniques are of four types:

a) Chromatic aberration: Lateral chromatic aberration manifests itself as a spatial shift in the regions where the light of varying wavelengths reaches the sensor.

b) Color filter array: CFAs consists of three color filters (red, green, blue) placed at the top of each sensor element. At each pixel location, only a single color sample is recorded. In order to obtain a three-channel color image, the other two color samples must be estimated from the neighboring samples.

c) Camera response: Most cameras, in order to enhance the final image, a point wise nonlinearity is applied. This is because, many digital camera sensors are linear and there should be linear relationship between the amount of light that is measured by each sensor element and the corresponding final pixel value.

d) **Sensor noise:** In this, the camera is modeled with an additive and multiplicative noise model. From the original camera, the parameters of the noise model are estimated. And for authenticating an image the correlation between the estimated camera noise and the extracted image is used.

1.4 Physical environment-based image forgery detection: The anomalies in the 3-D interaction between the physical objects, light and the camera can be modeled and detected by this method. This method works based on the lighting environment in which an image is captured, and the differences in background lighting can be taken as an evidence of detecting forgery. These techniques are of three types:

a) Light detection 2-D: In this, the estimation of light source direction is limited to 2-D as it is difficult to determine 3-D surface normals from a single image.

b) Light detection 3-D: In this, the estimation of 3-D direction to a light source can be determined and by leveraging a 3-D model, the required 3-D surface normals can be obtained.

c) Light Environment: In practice, different lighting environments can be created by placing any number of lights in any positions.

1.5 Geometry-based image forgery detection: The measurements of objects in the real world and their position relative to the camera are done by this method. This technique is of two types:

a) Principal Point: The principal point is near the center of the image for the authentic images. As when a person is moved the principal point also changes. Therefore, the differences in the estimated principal point across the image is then used as evidence of tampering.

b) Metric Measurement: This involves estimation of the world-to-image transformations, for the removal of planar distortions and also involves the ability to make real world measurements from a planar scale.

The main focus of this paper is on the different methods for the detection of copy-move forgery in digital images. Figure 4 shows an example of copy-move forgery.

(i) (ii)

Figure 4: An example of copy-move forgery.

This is one of the most common type of forgery most commonly used on these days. Copy-move forgery is the process of copying a portion of the image from the source image and duplicating the copied portion somewhere else in other portion of the same image.

In the Figure 4, the image in (i) shows an original photograph and an image in (ii) shows the forged photograph released by Iran. In the original image there were only 3 missiles but in the forged photograph there are 4 missiles instead of 3. This shows that the image has undergone copy-move forgery. The below section describes some methods that have been adopted to detect the copy-move forgery regions. Copy-move forgery detection is one of the important field in digital image forensics.

2. Literature Survey

Fridrich et al [1] proposed a method based on Discrete Cosine Transform (DCT) coefficients. Figure 5 shows the flowchart of the method proposed by Fridrich. In this method the image is first divided into overlapping blocks and to each of the blocks the DCT transform is performed. The DCT coefficients are then quantized. These quantized DCT coefficients are stored as a row in a matrix. The matrix will have (M-B+1) (N-B+1) rows and B x B columns. To detect

the tampered regions in an image a lexicographical sorting is introduced and the matched blocks are detected by comparing the quantized DCT coefficients. An advantage of this method is that it reduces the false matches, but when an image has large identical textures this method results in false positive.

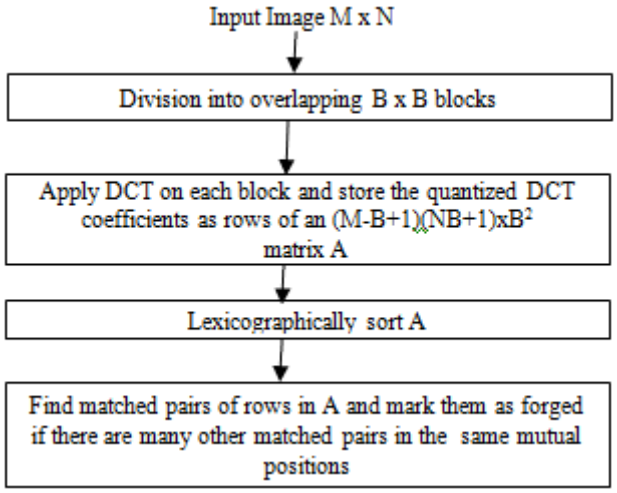

Figure 5: Flowchart of the method proposed by Fridrich et.al

S. Bayram et al. [2] developed a method based on Fourier-Mellin Transform (FMT). In this method the image is divided into many small sized blocks and the Fourier transform of every block is calculated. The features are extracted from the image blocks using FMT. These features are robust to JPEG compression, blurring, noise addition, and so on. Similar blocks are then found by sorting the blocks lexicographically. The efficiency of the detection step can thus be improved by the use of counting bloom filters, which essentially computes the hashes of features.

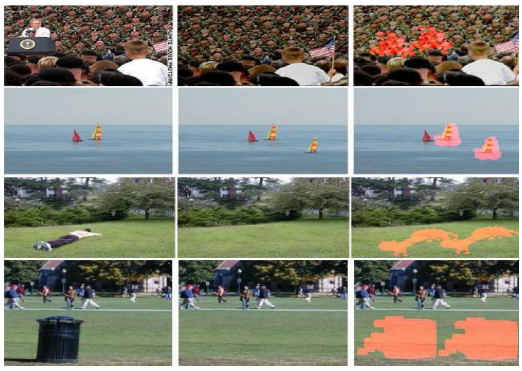

Figure 6: Each row indicates different images: first column is the original image; second column is the tampered image and the third column is the detection result of the algorithm.

Ryu et al [3] proposed copy rotate move (CRM) detection scheme using Zernike moments. In this method, the image is first divided into sub blocks. And the magnitude of Zernike moments are calculated to extract feature vectors of a given block. These vectors are then lexicographically sorted and the similarity of adjacent vectors are calculated. The measures such as Precision, Recall and F1 are used to find the suspected regions. Zernike moments are robust to compression, noise and blurring and is also rotation invariant. Figure 7 shows the CRM manipulation and the detection result.

(i) (ii) (iii)

Figure 7: CRM manipulation and its detection result. (i) Original image with two aircrafts (ii) forged image with three aircrafts by copy-move forgery (iii) forged image showing three aircrafts by copy-rotate-move (CRM) forgery.

One of the advantage of this method is that the forgeries in flat regions can be easily detected. A major drawback of this method is that complexity in calculating Zernike moment coefficients and also it is not good in detecting scaled copied blocks.

Kakar [4] proposed a method based on transform-invariant features. This is based on MPEG-7 image signature tools. These tools are developed or designed for the robust and fast content retrieval. The tools are modified to detect the copy-move forgeries. In this method a feature matching process is used to detect the cloned regions accurately. The method results in high true positives and low false positives.

H.Huang and W.Guo [5] proposed an effective method to detect copy-move forgery in digital images. The method first extracts SIFT descriptors from an image , an advantage of this algorithm is that the image do not undergo any changes to illumination, rotation, scaling and so on. Similarity between the copied and pasted region is used to detect the tampering. The SIFT algorithm extracts distinctive features of local image patches that are invariant to image scale and rotation. The algorithm has a good accuracy, and is features are robust to occlusion and is relatively efficient compared to other algorithms. It mainly consists of four steps: (1) Scale-space extrema detection; (2) Key point localization; (3) Orientation assignment; (4) Key point descriptor. The SIFT algorithm fails with lighting changes.

3. Comparison Study

S.No.	Author	Methods	Advantage	Disadvantage
1	Fridrich	DCT	Reduces False Matches	Results in False Positive in Large Images
2	S.Bayram	FMT	Efficient and robust	Fails in case of rotation above 10 degrees and scaling of 10%
3	S.Ryu	ZERNIKE	Forgeries in flat areas detected easily	Calculation of Zernike moment coefficie-nt is complex
4	Kakar	MPEG-7	Results in high True Positive and low False Positives	Difficult to detect forgery in regions that have undergone non affine transformations
5	H.Huang	SIFT	Efficient and robust method and has good accuracy.	The method fails when the SNR value is low.

4. Conclusion

Nowadays, digital images are used as information providers in many areas. This results in an increase chance of tampering the images also. Tampering of digital images can be done easily with the development in image editing tools available. Copy-move forgery is one of the main problem that is faced most probably in digital image forensics. There are several methods and techniques adopted to detect the copy-move forgery. Most of the methods is based either on block-based method or key point-based methods. These methods and techniques are having some advantages and disadvantages as well. Therefore, there is a need to find an effective technique which combines both the block based and the key point based methods that aims to improve the accuracy.

References

[1] A. J. Fridrich, B. D. Soukal, and A.J. Lukas, "Detection of copy-move forgery in digital images," in Proc, Digit. Forensic Res.Workshop, 2003.
[2] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), Washington, DC, USA, Apr. 2009, pp. 1053-1056.
[3] S. J, Ryu, M. Kirchner, M. J. Lee, and H. K. Lee, "Rotation invariant localization of duplicated image regions based on Zernike moments," IEEE Trans. Inf. Forensics Security, Aug. 2013, vol. 8, no. 8, pp. 1355-1370.
[4] P. Kakar and N. Sudha, "Exposing postprocessed copy-paste forgeries through transform – invariant features," IEEE Trans. Inf. Forensics Security, Jun. 2012, vol. 7, no. 3, pp. 1018-1028.
[5] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," in Proc. Pacific-Asia Workshop Comput. Intell., Ind. Appl. (PACIIA), vol. 2. Dec. 2008, pp. 272-276.

Author Profile

Rameeza M Ashraf received the Bachelor of Technology degree in Information Technology from KMEA Engineering College, Edathala in 2012 and currently doing Master of Technology in Computer Science and Engineering in KMEA Engineering College, Edathala.

Veena K Viswam received the Bachelor of Engineering degree in Computer Science and Engineering from Anna University, Chennai in 2006 and Master of Engineering in Computer Science and Engineering from Anna University in 2013. She has a total of 9.7 years of teaching experience and now currently working as an Assistant Professor in KMEA Engineering College, Edathala.