International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT2063170

A Survey Paper on Image forgery detection Using Pseudo Zernike Moment

Brijesh Patel[1], Dr. Sheshang Degadwala[2]
[1]PG Scholar, Computer Engineering, Sigma Institute of Engineering, Vadodara, Gujarat, India
[2]Associate Professor, Department of Computer Engineering, Sigma Institute of Engineering, Vadodara, Gujarat, India

ABSTRACT
Photographs are taken as valid evidences in various scenarios of our day to day life. Because of the developments in the field of Image Processing, altering images according to ones need is not a difficult task. Techniques of Image Forensics play its crucial role at this juncture. One of the mostly found types of image tampering is Copy-Move forgery. A copy-move forgery is performed by copying a region in an image and pasting it on another region in the same image, mostly after some form of post-processing like rotation, scaling, blurring, noise addition, JPEG compression etc. Two types of copy-move forgery detection techniques exist in literature. They are the Block based methods and Key-point based methods. Both the methods have their own advantages and limitations. This paper presents a survey on the recent developments in block based methods. As forgeries have become popular, the importance of forgery detection is much increased. Copy-move forgery, one of the most commonly used methods, copies a part of the image and pastes it into another part of the image. In this paper, we propose a detection method of copy-move forgery that localizes duplicated regions using Zernike moments. Since the magnitude of Zernike moments is algebraically invariant against rotation, the proposed method can detect a forged region even though it is rotated. Our scheme is also resilient to the intentional distortions such as additive white Gaussian noise, JPEG compression, and blurring. Experimental results demonstrate that the proposed scheme is appropriate to identify the forged region by copy-rotate-move forgery.

Keyword: - Image Processing, Image Forensics, Image Tampering Detection Digital Forensics, Copy-Move Forgery, Copy-Rotate-Move Forgery, Zernike Moments.

I. INTRODUCTION

Digital Image forensics is a young and emerging branch of image processing, which is aimed at obtaining quantitative evidence on the origin and truthfulness of a digital image .One of the principal tasks of image forensics is image tampering detection. Tampering literally means to interfere with something in order to cause damage or make unauthorized alterations. Images are treated as proofs in various scenarios and thus image tampering is defined as intentional manipulation of images for malicious purposes. Image tampering dates its origin to the earliest twentieth century when it was used for political propaganda. Today, because of the advent of powerful image processing tools, image tampering is not a rare phenomenon and as a result the last decade marked tremendous developments in the field of image forensics techniques. Image forensics techniques can be classified under two different approaches, Active approaches and Passive/Blind approaches. Active approaches were used traditionally by employing data hiding (watermarking) or digital signatures. Requirement of

specialized hardware narrows its field of application. Passive approaches or blind forensic approaches use image statistics or content of the image to verify its genuineness. As the image processing software's have been developed, even people who are not experts in image processing can easily alter digital images. It brings about great benefits, but also side effects: a number of tampered images have recently been distributed or have even been published by major newspapers. Therefore, it is important to verify the authenticity of digital images. Among forgery techniques using typical image processing tools, copy-move forgery is one of the most commonly used methods. Figure 1 shows an example of the altered photograph released by Iran and published by western media including The New York Times, The Los Angeles Times, BBC News and etc. on July 9, 2008.[1]

Figure 1. An example of copy-move forgery [1]: (a) the forged image with four missiles and (b) the original image with three missiles

II. RELATED WORK

This section introduces the techniques and methods currently available in the area of digital image forgery detection. Currently, most acquisition and manipulation tools use the JPEG standard for image compression. As a result, one of the standard approaches is to use the blocking fingerprints introduced by JPEG compression, as reliable indicators of possible image tampering. Not only do these inconsistencies help to determine possible forgery, but they can also be used to light into what method of forgery was used. Many passive schemes have been developed based on these fingerprints to detect Resampling [4], Copy-paste [5,6], Luminance-level [7,], Double Compression JPEG [8,16], ANN [9], and Wavelet Transformation Coefficient [10].Above mentioned methodologies are derived from one another and they all contain constraints in implementations and limitations in performance. We concentrate on media photo images and propose and to develop an effective algorithm for detecting the forgery region in most popular image format JPEG and other digital camera supported image formats. Detection of digital image forgery having enormous number applications related Forensic science document questioning section although which is very helpful for media, publication, law, military, Medical image science application, satellite image, research and World Wide Web publications.

III. COPY-MOVE IMAGE FORGERY DETECTION

Copy-move is an image forgery technique in which parts of an original image, after some possible geometric and illumination adjustments, are copied, moved to a desired location in the same image and pasted (e.g. refer figure 1). The main aim of copy-move image forgery is to hide certain details or to duplicate some aspects of an image. Generally, Copy-Move forgery detection techniques can be classified into two: Block based approaches and Key-point

based approaches. In both the approaches some form of pre-processing will be there. In block based methods, the image will be divided into overlapping blocks of specified size and a feature vector will be computed for these blocks. Similar feature vectors are then matched to find the forged regions. In Key-point based methods, feature vectors are computed for regions with high entropy. There is no subdivision e. into blocks. The feature vectors are matched to find the copied blocks.

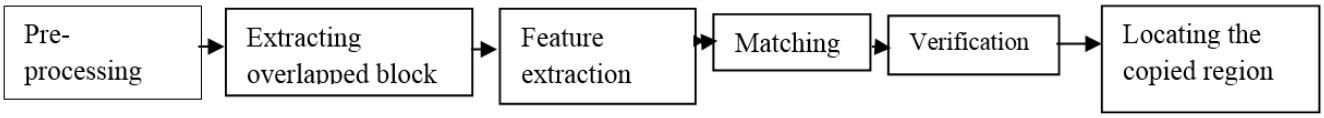

Figure-2 : Copy-move detection method pipeline

A very rich literature in the field of copy-move detection focuses mainly on the robustness of the detection method against different modifications, as well as the speed of the method. For this reason, methods are classified according to the selected feature used to check the duplication. However, most of them follow the same pipeline Figure 2.

This pipeline consist of the following steps:

1. **Preprocessing**: This step is used to improve the computational time by preparing the image for the next step. The most popular operations in this step are: Scale the image down before going on the remaining steps and converting color images into gray scale images. Converting image to gray scale makes its simple to enhance and interprets.

2. **Extracting Overlapped Blocks**: The image is divided into (squared or circular) overlapping blocks. Input image with resolution M×N is divided into (M–B+1)×(N–B+1) squared blocks, where each block is of B×B size.

3. **Feature Extraction**: Here, the representative features of each block are computed. Robustness of these features against different post-processing operations gives better chance in detecting the duplicated areas. Some examples are given in Table 1.

4. **Matching**: The aim of this step is to find the duplicated blocks based on their features descriptor that has been extracted in the previous step. These features are sorted and the high similarity between two features is interpreted as a hint for a duplicated region. Lexicographically sorting, and K-D tree [18], the most common sorting methods that were used [5].

5. **Verification:** This step is performed in order to reduce superior matches. This done by grouping matches that jointly follow a same transformation pattern. For example matches that belong to a copied region are expected to be spatially close to each other in both source and target blocks. Furthermore, matches that originate from the same copy-move action should exhibit similar amounts of translation, scaling and rotation.

6. **Locating the copied region***:* By coloring or highlighting them. Many methods were developed for copy-move forgery detection. Table 1 show some methods classified according to the selected feature that were used to represent the image.

Class	Feature used
1. Key-point based method.	SIFT [4] and SURF [24].
2. Block-based methods.	
a. Frequency domain-based.	DCT [6, 10, 13], FMT [5], DWT [14].
b. Dimensionality reduction-based.	SVD[27], and PCA[20].
c. Moment-based.	Hu [17] and Zernike[22, 23].

3. Segment-based approaches: the image is segmented using a multi-scale segmentation algorithm.	The image is segmented using a multi-scale segmentation algorithm [15, 19]

Table 1. Copy-move forgery detection method classification

IV. PSEUDO ZERNIKE MOMENTS

We first give a brief outline of PZMs, they will also serve as a reference to compare the performance of GPZMs. We then present the GPZPs and establish some useful properties of them in the second subsection. The definition of GPZMs is given in the last subsection.

1) A. Pseudo-Zernike moments

The 2D pseudo-Zernike moment (PZMs), Z_{pq}, of order p with repetition q is defined using polar coordinates (r, θ) inside the unit circle as·

$$Zpq=p+1\pi\int02\pi\int01Vpq*(r,\theta)f(r,\theta)rdrd\theta, \quad p=0, 1, 2, \ldots, \infty;0\leq|q|\leq p. \_\_\_\_\_(1)$$

where * denotes the complex conjugate, and $V_{pq}(r, \theta)$ is the pseudo-Zernike polynomial given by

$$V_{pq}(r, \theta) = R_{pq}(r)\exp(jq\theta)\_\_\_\_\_(2)$$

Here $R_{pq}(r)$ is the real-valued radial polynomial defined as

$$Rpq(r)=\sum s=0p-|q|(-1)k(2p+1-s)!s!(p-|q|-s)!(p+|q|+1-s)!rp-s\_\_\_\_(3)$$

The pseudo-Zernike polynomials satisfy the following orthogonality property

$$\int02\pi\int01Vpq(r,\theta)\cdot Vlk*(r,\theta)rdrd\theta=\pi(p+1)\delta pl\delta qk\_\_\_\_(4)$$

where δ_{nm} denotes the Kronecker symbol.

V. CONCLUSION AND FUTURE ENHANCEMENTS

In this study, copy-move forgery detection method based on PZM is explained. The copy-move forgery or cloning is extensively practiced to enhance the content of the image. Various methodologies, varying in terms of segmentation of image, feature extraction, sorting and detection schemes have been proposed by researchers. The problem is interesting in itself. A lot of effort has been done on identifying relevant features for detecting duplicity of object in an image. The proposed method uses an ACC which has not been used for copy-move forgery detection. The scheme is successful in accurately detecting the duplicated region. Also it is robust to transformations, such as scaling, translation and rotation. ACC is simple and a low complexity feature extraction scheme, along with the L1 norm, it is effective in detecting multiple copy-move forgeries in same image.

In future works, we will extend our research on improving the performance of image-forgery detection using the Pseudo Zernike Moment and also retrieval the other also.

VI. REFERENCES

[1]. Ashima Gupta, Nisheeth Saxena, S.K Vasistha, "Detecting copy move forgery using DCT" International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013.

[2]. A Survey of Partition-Based Techniques for Copy-Move Forgery Detection, the Scientific World Journal, 2014

[3]. Resmi Sekhar , Chithra A S, "Recent Block-based Methods of Copy-Move Forgery Detection in Digital Images" International Journal of Computer Applications (0975 – 8887) Volume 89 – No 8, March 2014.

[4]. A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Traces of Re-sampling," IEEE Trans. on Signal Processing, vol. 53,no.2, pp. 758–767, Feb. 2005

[5]. T. Ng, S.F. Chang, and Q. Sun, "Blind Detection of Photomontage using Higher Order Statistics", IEEE International Symposium on Circuits and Systems, Canada, May 2004

[6]. A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Traces of Re-sampling," IEEE Trans. on Signal Processing, vol. 53,no.2, pp. 758–767, Feb. 2005.

[7]. S. Murali, Anami Basavaraj S, and Chittapur Govindraj B. " Detection of Digital Imager forgery Using Luminance Level Techniques", IEEE Third National Conference of Computer Vision, Pattern Recognition, Image processing and Graphics, NCVPRIPG 2011 pp.215.

[8]. Fredric, J. and J. Lukas, "Estimation of Primary Quantization Matrix in Double Compressed JPEG Images." Proceedings of DFRWS 2003. Cleveland, OH, August 2003.

[9]. E.S.Gopi, N Lakshmanan, T.Gokul and S.Kumar Ganesh "Digital image forgery detection Using artificial Neural Network and Auto Regressive Coefficients" EEE/CCCGET, Ottawa, May 2006 1-4244-0038-4 2006.

[10]. Murali S.,Anami B. S, Chittapur G. B. "Digital Photo Image Forgery Techniques" International Journal Of Machine Intelligence ISSN: 0975-2927 & E-ISSN: 0975-9166, Volume 4, Issue 1, 2012, pp.-405.

[11]. Osamah M. Al-Qershi and Bee Ee Khoo, "Enhanced Matching Method for Copy-Move Forgery Detection by Means of Zernike Moments" Springer International Publishing Switzerland 2015.

[12]. Gajanan K. Birajdar, Vijay H. Mankar, "Digital image forgery detection using passive techniques: A survey" Elsevier 2013.

[13]. Seung-Jin Ryu, Min-Jeong Lee, and Heung-Kyu Lee, "Detection of Copy-Rotate-Move Forgery Using Zernike Moments". Springer-Verlag Berlin Heidelberg 2010

[14]. Hoda Marouf and Karim Faez, "An efficient feature extraction method with pseudo zernike moment for facial recognition of identical twins, International Journal of Computational Science and Information Technology, February 2014.

[15]. Leida Li, Shushang Li, Hancheng Zhu, Xiaoyue Wu, "Detecting copy-move forgery under affine transforms for image forensics" Elsevier 2013.

[16]. Gavin Lynch, Frank Y.Shih, Hong-Yuan Mark Liao, "An efficient expanding block algorithm for image copy-move forgery detection" Elsevier 2013.

[17]. Osamah M. Al-Qershi and Khoo Bee Ee, "Passive Detection of Copy-Move Forgery in Digital Images: State-of-the-art" Elsevier 2013.

[18]. Vincent Christlein, Christian Riess and Elli Angelopoulou, "On Rotation Invariance in Copy-Move Forgery Detection" IEEE 2010.

[19]. In an Iranian image, a missile too many, https://thelede.blogs.nytimes.com/2008/07/10/in-an-iranian-image-a-missile-too-many/

[20]. http://www.vcl.fer.hr/comofod/comofod.html

[21]. https://towardsdatascience.com/the-4-convolutional-neural-network-models-that-can-classify-your-fashion-images-9fe7f3e5399d

[22]. https://www.investopedia.com/terms/d/deep-learning.asp

[23]. https://machinelearningmastery.com/what-is-deep-learning

Cite this article as :

Brijesh Patel, Dr. Sheshang Degadwala, "A Survey Paper on Image forgery detection Using Pseudo Zernike Moment", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6, Issue 3, pp.879-883, May-June-2020. Available at doi : https://doi.org/10.32628/CSEIT2063170

Journal URL : http://ijsrcseit.com/CSEIT2063170