Copy Move Image Forgery Detection using Pseudo Zernike Moment for Better Detection Accuracy

Grishma Solanki[1] Mr. Karshan Kandoriya[2]
[1]P.G. Student [2]Assistant Professor
[1]Department of Information Technology [2]Department of Computer Science & Engineering
[1,2]Parul Institute of Engineering and Technology, Vadodara, Gujarat, India

Abstract— In modern era of information age, digitalization has revolutionized like never before. Powerful computers, advanced photo editing software packages and high resolution capturing devices have made manipulation of digital images incredibly easy. As per as image forensics concerns, one of the most actively researched area are detection of copy move forgeries. Higher computational complexity is one of the major component of existing techniques to detect such tampering. Moreover, copy move forgery is usually performed in three steps. First, copying of a region in an image then pasting the same one in the same respective image and finally doing some post-processing like rotation, scaling, shift, noise, etc. Consequently, pseudo Zernike moment is used as a features extraction method for matching image blocks and as a primary factors on which performance of detection algorithms depends.

Key words: Image, Image Forensics, Image Forgery, Copy-Move Image Forgery

I. INTRODUCTION

In our daily life digital media is playing a vital role because of popularity of low cost and high resolution cameras. As the image processing software 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, verification of authenticity is important for digital images. Among different forgery techniques using typical image processing tools, copy-move forgery is one of the most commonly used methods. The copy-move forgery copies a part of the image and pastes it into another part of the image to conceal an evidence or deceive people. 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].

In fig. 1(a), two major sections (encircled in black) appear to be replicated from other sections (encircled in white). Actually figure 1(a) was released on the front pages of those of newspapers and lately corrected to the original image as figure 1(b).

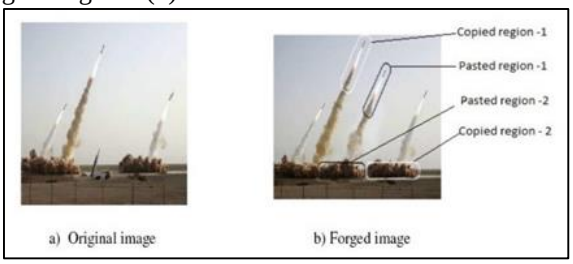

Fig. 1: An example of copy-move forgery [1]: (a) the forged image with four missiles and (b) the original image with three missiles

Image forgery can be broadly classified in three categories namely image forgery using splicing, copy move image forgery and image resampling [2]. This paper focuses on copy-move image forgery and its detection methods. The paper is organized as follows. In section-II, related work is discussed. In section-III, copy-move image forgery and its detection techniques are discussed. Section-IV proposed method. In section-V Implementation of proposed method and section-VI presents conclusion and future enhancement.

II. RELATED WORK

In digital images, there are many passive detection techniques have been proposed to detect image forgery. We can use block based or key point based matching methods for detection of forgery and the performance of the detection algorithms depends mainly on the features, which are used for matching the blocks [7].

Osamah M. Al-Qershi and Khoo Bee Ee discussed different methods of image forgery detection in digital image forensics. The problem of authentication of an images are addressed by digital image forensics [5].

Hoda Marouf and Karim Faez proposed new efficient facial-based identical twins recognition according to the geometric moment. Pseudo zernike moment is robust to rotation, scaling and shift. Also, the facial area inside an image is detected using Ada Boost approach [6].

In one paper Osamah M. Al-Qershi and Bee Ee Khoo proposed an enhanced matching method for copy move image forgery detection using Zernike moment. As Zernike moment is invariant to rotation and in some cases invariant to scaling also. It provide better detection accuracy compared to other passive techniques [7].

In one paper authors uses Zernike moment for detection of object which are copied moved or rotated. By using Zernike moment the ratio of false positive can be less [8].

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 [3]. 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 [4]. There is no subdivision

into blocks. The feature vectors are matched to find the copied blocks.

IV. PROPOSED METHOD

In this section pseudo Zernike moment is used as a feature extraction method for better detection accuracy and to overcome limitations of existing Zernike moment method.

Proposed method work well against objects that are rotated, scaled and shifted. In optical systems pseudo-zernike polynomials are widely used. It is also widely used in image analysis and shape descriptors. Pseudo Zernike moment uses global information in an image for extracting features.

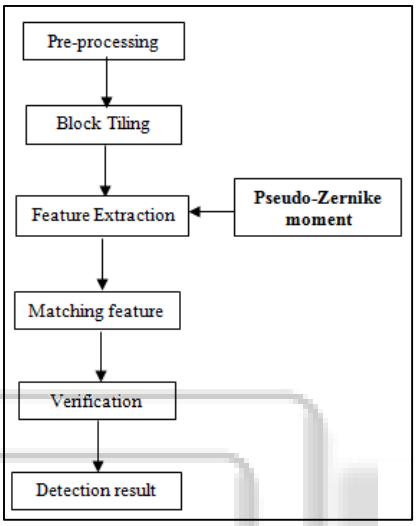

Fig. 2: Flowchart of proposed work

V. IMPLEMENTATION

For implementation MATLAB environment is used to run pseudo Zernike moment. Some of results from proposed method is mentioned here.

Below graph shows the comparison between Zernike and pseudo Zernike moment detection accuracy.

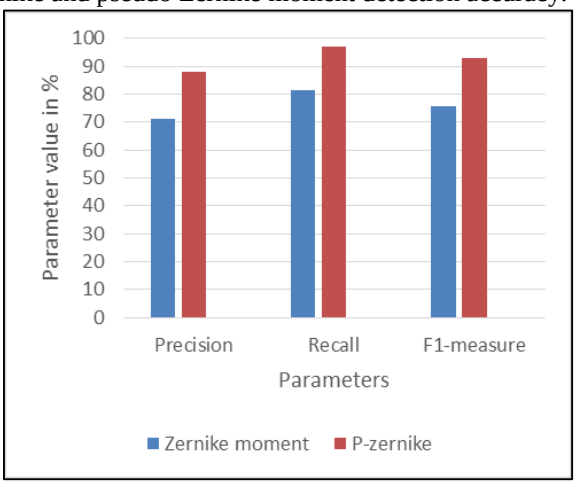

Fig. 3: Comparison graph of both methods

VI. CONCLUSION AND FUTURE ENHANCEMENT

From the recent surveyed methods on copy move forgery detection we can conclude that by using block based or matching methods with feature extraction we can reduce some intermediate and post processing operations like, noise, rotation, scaling. But Zernike moment does not invariant to shift and affine transformation. So we are using pseudo Zernike moment as a feature extraction method that is invariant to rotation, scaling, shift and affine transformation and it is also faster than Zernike moment. So it can improve accuracy and reduce computational overhead. So in future work we can use pseudo Zernike moment as a feature extraction method in video image forgery. So we can provide more security in video like in video surveillance system.

REFERENCES

[1] In an Iranian image, a missile too many, https://thelede.blogs.nytimes.com/2008/07/10/in-an-iranian-image-a-missile-too-many/
[2] Qureshi M. Ali and Deriche M., "A Review on Copy Move Image Forgery Detection Techniques", Feb. 2014.
[3] Kudke Swapnil H. and Gawande A. D., "Copy- Move Attack Forgery Detection by Using SIFT", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Apr 2013.
[4] Harpreet Kaur, Jyoti Saxena and Sukhjinder Singh, "Key-point based copy-move forgery detection and their hybrid methods: A Review", June 2015.
[5] Osamah M. Al-Qershi and Khoo Bee Ee, "Passive Detection of Copy-Move Forgery in Digital Images: State-of-the-art" 2013.
[6] Hoda Marouf and Karim Faez, "An efficient feature extraction method with pseudo Zernike moment for facial recognition of identical twins" 2014.
[7] 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.
[8] Seung-Jin Ryu, Min-Jeong Lee, and Heung-Kyu Lee, "Detection of Copy-Rotate-Move Forgery Using Zernike Moments" 2010.

