Analysis of various copy move image forgery techniques for better detection accuracy

Ms. Grishma Solanki[1], Mr. Karshan Kandoriya [2]

[1]PG Scholar, Dept. of Information Technology, Parul Institute of Engineering and Technology, Gujarat, India

[2]Proffesor, Dept. of Computer Science Engineering, Parul Institute of Engineering and Technology, 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.***

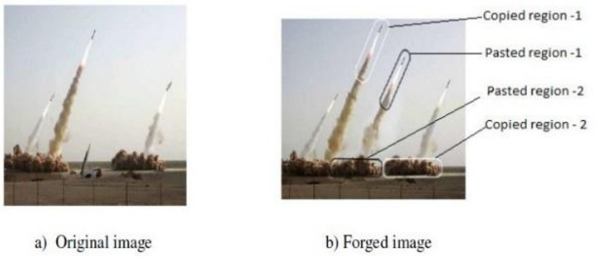
Key Words: *Copy-move image forgery, Digital image, Image processing, Image forgery*

1. INTRODUCTION

In our daily life digital media is playing a vital role because of popularity of low cost and high resolution cameras. However, due to sophisticated editing software like 3D max, Photoshop, etc. Digital images can be easily tampered without leaving any visible clues, so it creates serious social problem of trustworthiness for witness in a courtroom, criminal investigation, and scientific fraud.

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. Fig. 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 fig. 1(a) was released on the front pages of those of newspapers and lately corrected to the original image as fig. 1(b).



a) Original image

b) Forged image

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-2, copy-move image forgery and its detection techniques are discussed. Section-3 presents different algorithms for copy move image forgery detection. And section 4 presents conclusion.

2. 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 fig.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.

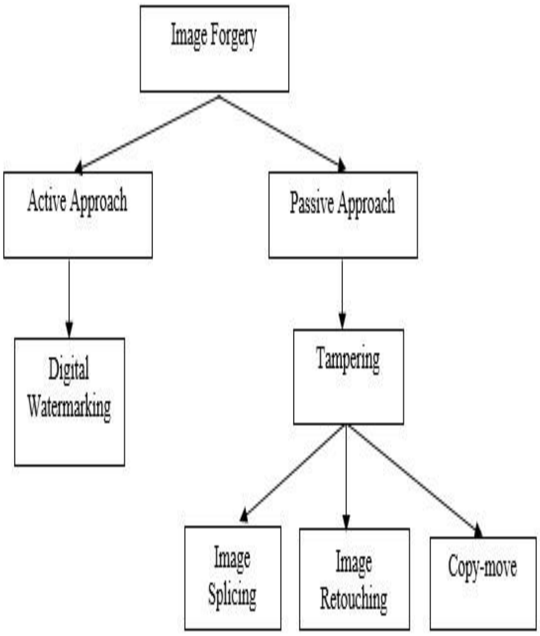


Fig. 2: Classification of Image Forgery [9]

Table -1: Comparison between various methods

Method	Characteristics (Rotation, Scaling, Shift, affine transformation)	Advantage	Limitation
DCT	-	Robust to noise, JPEG compression, blur	Not robust to rotation, scaling
Texture and intensity	Rotation	Robust to noise, JPEG compression	Scaling and affine transformation
Invariant moments	Rotation	Robust to rotation	Scaling and affine transformation
PCA	-	Robust to JPEG compression and noise	Not robust to scaling, blur, affine transformation
SVD	-	Robust to only noise	Not robust to rotation, scaling, JPEG compression, blur

The extracted features play a crucial role because the robustness of the detection algorithm comes from the characteristics of those features. For example, rotation invariant features make the detection algorithm able to detect duplicated regions, even if the copied region underwent some rotation operation before pasting it and vice versa.

Moments and invariant functions of moments have been extensively used for invariant feature extraction in a wide range of pattern recognition, digital watermark applications and etc.

3. COPY MOVE IMAGE FORGERY DETECTION ALGORITHMS

DCT-based algorithms

This category of algorithms exploits DCT coefficients as features that can be robust against JPEG compression and Gaussian additive noise. Fridrich proposed the first method for detecting copy-move forgery, and it was based on DCT. They suggested looking for matches among DCT coefficients of image blocks. To reduce the cost of the computation and to reduce the complexity of the comparisons, the DCT coefficients were sorted lexicographically. After the sorting, adjacent identical pairs of blocks are considered to be potentially tampered regions.

To refine the selection results, a histogram that counts the number of matching blocks separated by the same distance is calculated [5].

Texture and intensity-based algorithms

Texture and intensity are among the most often studied image features in image processing, computer vision, and computer graphics applications. Usually, texture can be considered to be a set of intensity variations that follow certain repetitive patterns. It is difficult to analyze texture by considering the value of a single pixel because it is affected by its neighboring pixels. As a result, texture is an important feature for image characterization and recognition. On the other hand, illumination-invariant intensity-based descriptors have been widely used for feature extraction at salient points. The main advantage of exploiting texture and intensity is to reduce the size of the feature vector [6].

SVD-based algorithms

Singular value decomposition (SVD) is a matrix factorization that is used to extract algebraic and geometric features from an image. SVD features have three properties, namely, stability, scaling, and rotation invariance. Because of these features, SVD has been used in many fields, such as digital signal processing, pattern recognition, and data compression. This algorithm do not show robustness against the different types of image processing operations [6].

Algorithms based on invariant image moments

Image moments are scalar quantities that are used to characterize a function and to capture its significant features. The main advantages of invariant moments are their insensitivity to specific deformations, such as geometric operations, and their discrimination power to distinguish objects that belong to different classes. Hu employed the results of the theory of algebraic invariants to introduce the moment invariants to the image processing community in 1962. Since then, researchers devoted hundreds of papers to study and analyse moment invariants and their uses in many applications areas. As a result, moment invariants have become one of the most important and most frequently used shape descriptors [7].

PCA-based algorithms

In this category, Principal Component Analysis (PCA) is not used as a feature or a descriptor and instead is used for reducing the size of the feature vector that is extracted from the image blocks. Performing PCA on the some extracted feature matrix involves computing the corresponding covariance matrix of the feature matrix, obtaining a new linear basis through eigenvectors of the covariance matrix, and obtaining a projection of each block onto those basis vectors that have higher eigenvalues, thereby reducing the dimensions of the feature vectors [8].

3. 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, shift and can improve accuracy and reduce computational overhead. Because copy move forgery detection is still at a very early stage, there is still much work such as object recognition, computer vision or image analysis can be done in future.

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

[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] 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.

[9] 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.