International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

Discussion and analysis on Copy-Move Image Forgery Methods

Miss. Neha Shelot[1], Mr. Sachin Jadhav[2]

[1]*Student, Dept. of information Technology, Pimpri Chinchwad College of Enginnering,Maharashtra,India*
[2]*Professor, Dept. of Information Technology, Pimpri Chinchwad College of Engineering, Maharashtra, India*

Abstract - *In the field of image processing image editing software, the term known as image forgery is generally used. It is major concern since the picture is used in the authentication processes. It is incredibly difficult to differentiate a forged image from the original. The tampered area in the forged image is difficult to spot with the naked eye. As a result, it's critical to devise a mechanism for distinguishing the tampered image from the original. Copy-and-paste image forgery is a most commonly used type of image forgery in which a region of an image is copied and pasted into another or same image to hide important information of the image. Image forgery detection has various applications in various fields of computer vision, digital image processing, biomedical technology, CID, image forensics, etc as there is increasing research in this field. It became more challenging due to use of advanced software tools that become difficult to confirm whether an image can be seen by naked eyes. Copy-move forgery detection approaches is given in this paper. The motivation to understand Image forgery detection techniques and their methods is also discussed.*

Key Words: Image Forgery, tampering detection technique, methods.

1. INTRODUCTION

Image plays important role in various fields such as forensic investigation, CID, surveillance systems, intelligence system, sports, social media, etc. Now-a-days many tools are available to alter the image with the help of correct computer skills. Digital forgery is defined as altering the original image.

For Eg: - fig 1 was circulated showing John Kerry (current US Secretary of State) and Fonda (Hollywood actress) chatting with a crowd at an anti-Vietnam peace rally. This photo was tempered by a hoaxer who was trying to raise a question about Kerry's patriotism.

Fig 1. Example of Image Forgery

Forgery detection techniques were classified into two categories;- active (non-blind,) Fig. 2 and passive (blind) [1]Fig 3. Active forgery detection techniques need some early information to detect the forgery in the image which may have been put in the image at the time of capturing the image. Digital watermarking [2-4] and digital signature [5,6] were the examples of active forgery detection techniques. Based on applications, digital watermarking further can be classified into fragile, semi-fragile, and robust watermarking [7].

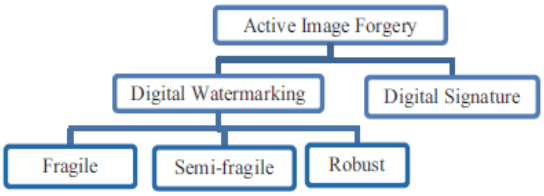

Fig 2. Active Image Forgery

Passive forgery detection techniques does not need any early information about the image like active forgery detection. Passive forgery is divided (Fig. 3) as dependent forgery and independent forgery. In dependent forgery alteration is done in the same image by cloning [8] some area within the image or by image splicing [9-12] to get agreeable composite. In independent forgery some properties of the same image are changed.

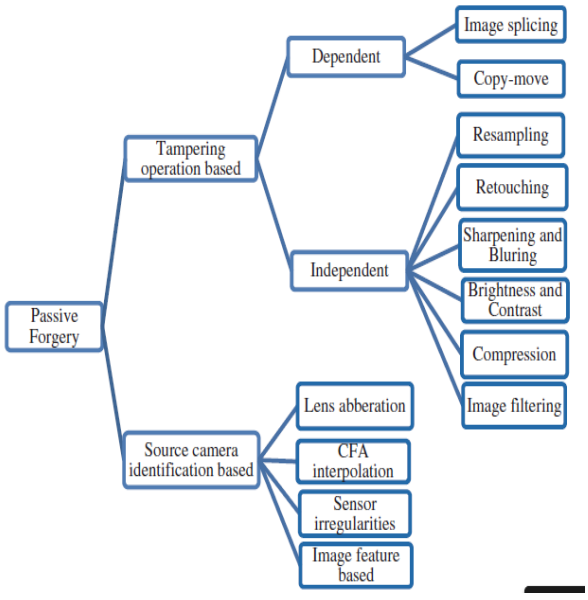

Fig 3. Passive Forgery

The remaining whole paper is organized as follows: Literature work 2. Copy-Move forgery methods is discussed in Section 3, Difference between algorithms 4, and Conclusion in Section 5.

2. Literature Survey

Last few years, many surveys have been carried out on image forgery detection. Lanh et al. [12] has discussed many techniques based on camera to detect image forgery. They gave a statement that camera-based techniques are better than other forgery detection techniques. Farid [`11], classified image forgery tools or techniques into five groups, like pixel-based techniques, format-based techniques, camera-based techniques, physically based techniques, and geometric based. Blind forgery detection techniques are given as tampering detection based and source camera identification based techniques. Tampering is defined as making change in the image to change meaning of the original image so that they can use it for unauthorized purpose. Four types of tampering detection techniques are given as follows:-

- Image splicing:-Image splicing is initial step to create a fake image from a set of images. To make fake image more realistic, scaling, cropping, retouching, rotating, overlapping, etc. operations are applied on each blocks, further, after performing splicing operation, we can again do postprocessing operation to hide any effects.

- Image resampling: - Resampling is mathematical technique used to change the size of the image, main purpose it is used for increasing size of image for printing banners and hoardings, digital advertisement, etc. or to decrease the size of image which can be used in email and website, etc.

- Image retouching detection: - In retouching polishing of the image is done. In short, retouching refers to improving the surface of the image. To eliminate visual clues from forged image contrast enhancement technique is mostly used.

- Copy-move forgery: - In copy-move forgery one region of image is copied and pasted in the other part or region of the same image. The aim of copy-move forgery is to hide some visual clues in image to mislead people. Its simplicity is the main reason to use copy-move forgery detection.

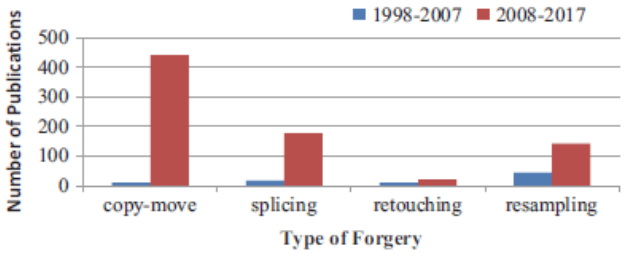

Fig 4.Types of Forgery

Figure 4 shows the bar chart of a number of publications against types of image forgery detection techniques of last two decades

2.2 Existing survey papers available on Google Scholar

Table 1.Existing survey paper

SR. NO.	Authors	Contribution	Observations
1	Lanh et al.	Reviewed various techniques in digital camera image forensics	Intrinsic features based of camera hardware methods are more reliable and better based on accuracy. Camera identification methods outstand as compared to its other forgery detection methods
2	Farid	Categorized the image forgery detection techniques into five groups (pixel-based, format-based, camera-based, physically based and geometric-based)	Some tools may not detect advanced forgeries but other forgery detection techniques are more reliable to challenge fake image. Due to the advance update in image modification tools, an race between the Forger and forensic analyst is unescapable
3	Mahdian and Saic	Reviewed various method based on blind image forgery	Existing methods produce higher false positive rates than which were reported in the existing papers As Existing methods are not fully automated, they need human interpretation
4	Christlein et al.	Reviewed state of the art approaches pertaining to	Keypoint-based methods are better than block-based methods in term of

		copy-move forgery	execution. However, block based methods give better detection accuracy than keypoint based methods.
5	Birajdar and Mankar]	Reviewed forgery detection techniques with more emphasis on passive tampering detection	Existing methods are not giving automated, outputs they need a human interpretation. Existing methods are not effective when small regions of the image are copy-moved Copy-move forgery detection, needs high time complexity and false positives There is need to extend forgery detection on audio and video

3. METHODS OF COPY-MOVE FORGERY

3.1 Introduction

In this section, three major types of methods are discussed of one of the most tampering detection technique i.e. copy-move forgery. So, the methods are as follows:-

A. ALGORITHMS USING TEXTURE AND INTENSITY DESCRIPTORS

• Davarzani et al. [15] proposed a way that depends on dividing the image into overlapping blocks so using Multi-resolution Local Binary Patterns (MLBP) to extract each block's feature vector. A lexographic map and the same step are applied by using the k-d tree for extended reduction and to decrease feature dimensions. They used a Random Sample Consensus (RANSAC) algorithm to use false match removal
Advantage and Disadvantage

- The most advantage is that the power to precisely detect copy-moved regions even with scaling, rotation, blurring, JPEG compression, and noise addition.
- It cannot detect duplicated regions with different rotation angles.

• Mushtaq et al. [16] developed an innovative algorithm that depends on if the local or statistical properties of an image are stable, slightly changeable or approximately frequent. So, the image has constant or homogenous texture. It uses Gray Level Run Length Matrix (GLRLM) supported reference pixels to research the image by intensity, length, and direction of the run. Features are extracted, and a linear Support Vector Machine (SVM) classifier is used to classify the extracted features.
Advantage and Disadvantage

- The algorithm is works nicely in copy-move forgery detection and image splicing.
- It suffers from an oversized percentage of true negative ratio.

B. DCT Based Algorithm

• Maind et al. [17] divide the image into fixed blocks and quantized these blocks by applying DCT on each. The transformed circular block is represented with four features for each block to chop back the dimension of it. A Lexographically representation is formed and it betting on a threshold value the duplicated blocks are detected.
Advantage and Disadvantage:-

- The algorithm shows robustness to repeated copy-move forgery and also robustness against blurring or nosing adding.
- Offers low computational complexity due to the lower dimensions of feature vectors
- The main disadvantage is that the high computational complexity just just in case of the massive size of feature vectors.

• Fadl et al. [18] trusted first dividing the image into fixed size overlapping blocks. Second, they applied DCT on each block to extract its features. They used fast K-means clustering technique over DCT to hurry up the search by classifying features into different classes. They used zigzag scanning to cut back the length of block features. Finally, a Lexographically representation was used with radix sorting to reduce complexity.
Advantage and disadvantage

- The advantage of this method appears in reducing execution time up to 50% compared with the previous work.
- The most disadvantage is that the low level of robustness against JPEG compression, blurring, rotating and scaling reprocessing, and so they should improve the response to geometric operations.

C. Algorithms Based Mutual Information

Chakraborty [20] proposed a latest technique supported the strategy of Soleimani et al. [19]. It detects copy-move forgery supported mutual information hunt for duplicated regions without extracting any features of the image. The steps of the algorithm are:

1) For the input image I with size M x N, divide the image into non-overlapping blocks of size m x n.

2) For each block Bi and embedded image region Rj, two matrices are represented.

3) Calculate the possibility distribution employing a histogram of the two regions represented by two matrices.

4) Calculate the mutual information between them. If the regions aren't duplicated, the mutual information value equals zero. On the alternative hand, if the regions are duplicated, the mutual information gives a matrix. The price of the mutual information exceeds a selected threshold, and this means a false rejection, and a lower threshold means false duplication detection probability.
Advantage and Disadvantage

- The most advantage of this method is its simplicity and its high speed. It doesn't extract any features from the image, it depends only on a mathematical way, and also it gives quite robustness against illumination changes.
- However, it needs more examinations about large illumination changes and other post-processing operations.

4. DIFFERENCE BETWEEN ALGORITHMS

1) Algorithm Based DCT

a. The strategy that each algorithm tries to chop back the scale of the feature vector and this has as way on the computational complexity.
b. The algorithm ready to detect different operations of image Processing utilized by attackers to hide tampering.

2) Algorithms Using Texture and Intensity Descriptors

a. Works with good robustness and experience interval
b. Algorithms uses the properties like exploited texture, structure of the image, and therefore the homogeneity to represent important features of the image.
c. Even properties like color, general texture and pixel coherence are accustomed detect image tampering.

3) Algorithms Based Mutual Information

a. It's quite robust against illumination changes.
b. It's simple and has high speed
c. Huge mathematical calculations are needed for giant illumination changes.
d. Even more examination is required for other post processing operations.

Based on the above discussion Algorithm Using texture and intensity descriptors is effective method to detect copy-move forgery detection as compared to others based on robustness and other image properties such as color pixel, noise.

5. Conclusion

Different image forgery identification methodologies have been surveyed and explored in this article. Many of the methods and methodologies discussed in this paper are capable of detecting fraud.

- Few algorithms are ineffective when it comes to detecting individual forged regions.
- Time complexity problem.

As a result, an effective (efficient) and accurate image forgery detection algorithm is required.
In future we will propose a method or system that can overcome above issues and detect the exact forged regions in the images.

REFERENCES

[1] Tyagi, V.: Understanding Digital Image Processing. CRC Press (2018). ISBN 9781315123905
[2] Wang, S., Zheng, D., Zhao, J., Tam, W.J., Speranza, F.: An image quality evaluation method based on digital watermarking. IEEE Trans. Circuits Syst. Video Technol. 17, 98–105 (2007)
[3] Singh, P., Chadha, R.S.: A survey of digital watermarking techniques, applications and attacks. IEEE Int. Conf. Ind. Inform. 2, 165–175 (2013)
[4] Arnold, M., Schmucker, M., Wolthusen, S.D.: Techniques and Applications of Digital Watermarking and Content Protection. A Cataloging in Publication Record, Artech House Inc, Norwood, MA, USA (2003)
[5] Lu, C., Liao, H.M., Member, S.: Structural digital signature for image authentication: an incidental distortion resistant scheme. IEEE Trans. Multimed. 5, 161–173 (2003)).
[6] Schneider, M., Chang, S.: A robust content based digital signature for image authentication. In: IEEE International Conference on Image Processing. pp. 227–230 (1996)
[7] Cox, I.J., Miller, M.L., Bloom, J.A., Kalker, T.: Digital Watermarking and Steganography Second Edition.
[8] N.Muhammad,M.Hussain,G.MuhammadandG.Bebis,"Copy-Move Forgery Detection Using Dyadic Wavelet Transform,"Eighth International Conference on

Computer Graphics, Imaging and Visualization(CGIV), Singapore,2011,pp.103-108.

[9] Christlein, V., Riess, C.C., Jordan, J., Riess, C.C., Angelopoulou, E.: An evaluation of popular copy-move forgery detection approaches. IEEE Trans. Inf. Forensics Secur. 7, 1841–1854 (2012)

[10] Hsu, Y., Chang, S.: Camera response functions for image forensics: an automatic algorithm for splicing detection. IEEE Trans. Inf. Forensics Secur. 5, 816–825 (2010)

[11] Carvalho, T.J.De, Member, S., Riess, C., Member, A., Angelopoulou, E., Pedrini, H., Rocha, A.D.R.: Exposing digital image forgeries by illumination color classification. IEEE Trans. Inf. Forensics Secur. 8, 1182–1194 (2013)

[12] .Farid, H.: Exposing digital forgeries by detecting traces of resampling. IEEE Trans. Inf. Forensics Secur. 53, 758–767 (2005)

[13] Lanh, T.V.L.T., Van Chong, K.-S., Chong, K.-S., Emmanuel, S., Kankanhalli, M.S.: A survey on digital camera image forensic methods. In: 2007 IEEE International Conference on Multimedia and Expo, pp. 16–19 (2007).

[14] Farid, H.: A survey of image forgery detection techniques. IEEE Signal Process. Mag. 26, 16–25 (2009)

[15] .Reza Davarzani, Khashayar Yaghmaie, Saeed Mozaffari, Meysam Tapak, " Copy-move forgery detection using multiresolution local binary patterns", Forensic Science International 231, 61-72, 2013.

[16] Saba Mushtaq, Ajaz Hussain Mir," Forgery Detection Using Statistical Features", International Conference on Innovative Applications of Intelligence on Power, Energy and Controls with their Impact on Humanity (CIPECH14) 28 & 29 November 2014

[17] Rohini.A.Maind, Alka Khade, D.K.Chitre, "Image Copy-moveForgery Detection using Block Representing Method", International Journal of Soft Computing and Engineering (IJSCE), 2231-2307, Volume-4, Issue-2, May 2014.

[18] Sondos M.Fadl, Noura A.Semary, "A Proposed Accelerated Image Copy-Move Forgery Detection", Visual Communications and Image Processing Conference, IEEE, 253 – 257, 7-10 Dec. 2014.

[19] Hussein Soleimani, Mohammadali Khosravifard, "Mutual Information-Based Image Template Matching with Small Template Size", 7th Iranian Machine Vision and Image Processing (MVIP), 1 - 5, Tehran, 16-17 Nov. 2011.

[20] Somnath Chakraborty, "Copy-moveImage Forgery Detection Using Mutual Information", Fourth International Conference on Computing Communications and Networking Technologies (ICCCNT), 1 - 4, Tiruchengode, 4-6 July 2013..