International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

Digital Image Forgery and Techniques of Forgery Detection

***[1]Ishrath Nousheen, [2]Anugu Lahari Reddy, [3]Poniganti Nikitha**

[1]Assistant Professor, Department of Information Technology, Bhoj Reddy Engineering College for Women, Hyderabad, India

[2,] Students, Department of Information Technology, Bhoj Reddy Engineering College for Women, Hyderabad, India

ARTICLEINFO

Article History:

Accepted: 10 April 2023
Published: 30 April 2023

Publication Issue
Volume 9, Issue 2
March-April-2023

Page Number
650-654

ABSTRACT

Image forgery means manipulation of digital image to conceal meaningful information of the image. The detection of forged image is driven by the need of authenticity and to maintain integrity of the image. A copy–move forgery detection theme victimization adaptive over segmentation and have purpose feature matching is proposed. The proposed scheme integrates both block-based and key point-based forgery detection methods. The proposed adaptive over-segmentation algorithm segments the host image into non-overlapping and irregular blocks adaptively. Then, the feature points are extracted from each block as block features, and the block features are matched with one another to locate the labeled feature points; this procedure can approximately indicate the suspected forgery regions. To detect the forgery regions more accurately, we propose the forgery region extraction algorithm which replaces the features point with small super pixels as feature blocks and them merges the neighboring blocks that have similar local color features into the feature block to generate the merged regions. Finally, it applies the morphological operation to merged regions to generate the detected forgery regions. In cut-paste image forgery detection, proposed digital image forensic techniques capable of detecting global and local contrast enhancement, identifying the use of histogram equalization.

Keywords : Copy-move forgery detection; Adaptive over-segmentation; Feature point matching and extraction; Cut-paste forgery detection.

I. INTRODUCTION

In this era, Digital Image Forgery has been increasingly easy to perform, so the reliability of the image is thus becoming an important issue to be focus on. It does not differ very much in nature to conventional image forgery. Instead of using photograph digital image forgery deals with the digital image. By using the tool such as Adobe Photoshop, GIMP, Coral Paint fake images can be created as some of the tools are open source. Image forgery may lead to hazards. In banking system image forgery is a big threat, this result into big

frauds. Nowadays detecting these types of forgeries has become very useful to reduce these problems at present. To determine whether a digital image is original is a big challenge. To find the marks of tampering in a digital image is a challenging task. Tampering is normally done to cover objects in an image in order to either produce false proof or to make the image more pleasant for appearance. There are many cases in digital image forgery, all this cases are classified into three categories based on the process of creating fake images the group are image retouching, and image splicing, copy-move attack. Image forgery is basically a modification of image to conceal some meaningful or useful information. The common manipulations of a digital image are copy-move and cut-paste forgery.

1.1 Copy-Move Forgery Detection

Copy-move forgery, which is to paste one or several copied region of an image into other part of the same image. During the copy and move operations, some image processing methods such as rotation, scaling, blurring, compression, and noise addition are occasionally applied to make convincing forgeries. Earlier blocked based forgery detection was used to detect forged image but this algorithm faced some drawbacks such as the host image is divided into over-lapping rectangular blocks, which would be computationally expensive as the size of the image increases and it was less efficient as it take more time to be process. To avoid such drawbacks along with the blocked based forgery, we proposed an image-blocking method called Adaptive OverSegmentation that divided the host image into non overlapping blocks adaptively with the help of two algorithm those are Simple Linear Iterative Clustering (SLIC) to segment the host image into irregular blocks and Discrete Wavelength Transform (DWT) which is employed to analyze the frequencies of the super pixel. Further the image block formed are pass to the Block Feature Extraction method where the block feature are extracted by using Scale Invariant Feature Transform (SIFT) as it possessed constant and better performance compared with the other extraction method. Further the process of Block Feature Matching is carried out which used Simple Linear Iterative Clustering (SLIC) for calculating super pixel and Discrete Wavelength Transform for finding super pixel from one block and checking other for other blocks. When the features are extracted and matched then we get to know which regions the host image has been forged.

1.2 Cut-And Paste Image Forgery Detection

Cut-and paste image forgery consists of creating a composite image by replacing a contiguous set of pixels in one image with a set of pixels corresponding to an object from a separate image. If the two images used to create the composite image were captured under different lighting environments, an image forger may need to perform contrast enhancement on so that lighting conditions match across the composite image. Failure to do this may result in a composite image which does not appear realistic. Image forgeries created in this manner can be identified by using localized contrast enhancement detection to locate, the cut-and-pasted region.

II. RELATED WORK

The existing block-based forgery detection methods divide the input images into overlapping and regular image blocks; then, the tampered region can be obtained by matching blocks of image pixels or transform coefficients. Fridrich [7], proposed a forgery detection method in which the input image was divided into over-lapping rectangular blocks, from which the quantized Discrete Cosine Transform (DCT) coefficients of the blocks were matched to find the tampered regions. In [8], proposed a method for detecting copy-move forgery over images tampered by copy-move. To detect such forgeries, the given image is divided into overlapping blocks of equal size, feature for each block is then extracted and represented as a vector, all the extracted feature vectors are then sorted using the radix sort.

DWT and SIFT [2] algorithms are proposed for copy-move detection. With DWT, the low frequency

information or image is obtained. With SIFT robustness is introduced, here it detect forgery of the image even it is copied, rotate scale and then pasted. In [3], survey done on various image forgery detection techniques and finally conclude the comparative study with some parameters. Also tools are mentioned to detect the forged images that travel over the network or by natural way for daily forensics, image processing, and security. Salam A.Thajeel [4], discussed digital image forensics and its types, challenges and research problems and detail analysis of the existing approaches for detect image tampering. Author also discussed block based method and key point-based method and popular techniques of two methods. Moreover, most of the methods may not address the problems. Therefore, there is a need to develop techniques that is efficient to deal with these challenges.

The Speeded Up Robust Features (SURF) [6] were applied to extract features instead of SIFT. However, although these methods can locate the matched key-points, most of them cannot locate the forgery regions very well; therefore, they cannot achieve satisfactory detection results and, at the same time, a sustained high recall rate [5].

A novel copy–move forgery detection scheme using adaptive over segmentation and feature point matching [1] is proposed, that integrates both block-based and key point-based forgery detection methods. Methods for detecting locally applied contrast enhancement as well as a method for identifying histogram equalization [9] are proposed. By observing that the intrinsic fingerprints of contrast enhancement operations add energy to the high frequency components of an image's pixel value histogram, we developed a global contrast enhancement detection technique. We extended this technique into a method for detecting locally applied contrast enhancement and demonstrated its usefulness for detecting cut and paste type forgeries.

A novel algorithm is proposed to identify the source-enhanced composite image created by enforcing contrast adjustment on either single or both source regions [10].The two source images used for creating cut-and-paste type of forged images may have different color temperature or luminance contrast. So, in order to make the forged image more real, contrast enhancement is performed on either one or both the regions.

III. PROPOSED SYSTEM

In this block based forgery method the image can be divided into blocks. Earlier in block based forgery detection schemes size of blocks divided into over-lapping regular blocks with predefined block size thus forgery region detected by matching the blocks in turn size of the host image is increased simultaneously by increasing computation of over-lapping blocks so we used adaptive over-segmentation method which can segment host image into non over-lapping region of irregular shape and image blocks as the host image into nonoverlapping region of irregular shape and in addition to this super pixels can be obtained by over-segmentation. For this purpose we employed SLIC algorithm to segment the host image into meaningful irregular super pixels for each block SLIC algorithm make use of k-means clustering approach to generate super pixels by using this we get rid of over-lapping block and hence decreased the computational expenses. DWT- Discrete Wavelength transform is employed to analyze the frequency distribution of host image here low frequency energy is discarded and high frequency energy of the host image is considered as smooth image.

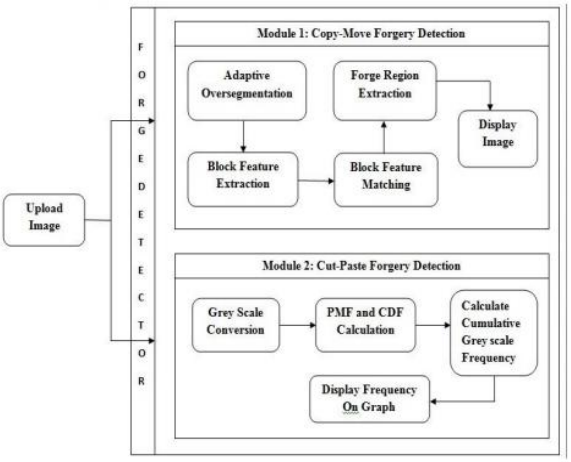

Fig 1: System Architecture

IV. RESULT ANALYSIS

The two characteristics precision and recall are used to evaluate the performance of the proposed forgery detection scheme. Precision is the probability that the detected regions are relevant, and it is defined as the ratio of the number of correctly detected forged pixels to the number of totally detected forged pixels. Recall is the probability that the relevant regions are detected, and it is defined as the ratio of the number of correctly detected forged pixels to the number of forged pixels in the ground-truth forged image.

Host Image		Fixed-size S=150	Fixed-size S=250	Adaptive-size S(11)=199 S(12)=159 S(13)=224
I1	*Precision (%)*	91.44	91.91	**93.85**
	Recall (%)	69.99	69.74	**99.12**
I2	*Precision (%)*	93.07	93.26	**96.60**
	Recall (%)	**90.75**	77.43	78.90
I3	*Precision (%)*	**96.90**	95.59	95.28
	Recall (%)	81.49	89.46	**95.19**

Table I Forgery Detection Results With/Without the Proposed Adaptive Over-Segmentation Algorithm

Table I shows the comparison results for the forgery detection with and without the proposed Adaptive Over-Segmentation algorithm. It can be easily observed that for host image I1, the proposed Adaptive Over-segmentation method can produce more accurate forgery detection results with a higher Precision=93.85% and, at the same time, gain a much better Recall=99.12%; for host image I2, the proposed Adaptive Over-segmentation method can produce more accurate forgery detection results with higher Precision=96.60%; and for host image I3, the proposed Adaptive Over-segmentation method can produce more accurate forgery detection results with higher Recall=95.19% and, at the same time, maintain good Precision=95.28%. The comparison results indicate that the proposed Adaptive Over-Segmentation algorithm can achieve much better forgery detection results than the other forgery detection methods with fixed-size blocks.

Histogram Equalization graph	Forgery Detection Result
If CDC is smooth	Image is Forged
If CDC is spiky	Image is not forged

Table 2 Cut-Paste Forgery Detection Result

V. CONCLUSION

Proposed system, Advanced Techniques for Image Forgery Detection uses the Adaptive Over-Segmentation algorithm to segment the host image into non-overlapping and irregularblocks adaptively according to the given host images; using this approach, for each image, we can determine an appropriate block initial size to enhance the accuracy of the copy-move forgery detection results and, at the same time, reduce the computational expenses. In Cut-paste image forgery detection, proposed digital image forensic techniques capable of detecting global and local contrast enhancement, identifying the use of histogram equalization. Characteristic features of histogram equalization's intrinsic fingerprint were identified and used to propose a scheme for cut and paste forgery detection.

In Future, I would like to implement the same concept on other types of forgery, such as splicing, multiple extension support or other types of media for example, gif images, videos.

VI. REFERENCES

[1]. Soumen Chakrabarti, Martin van den Berg 2, Byron Domc, "Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 8, August 2015.

[2]. Aditya R Hambarde, Avinash G Keskar,"Copy-move Forgery Detection Using DWT and SIFT Features", proceeding Department of Electronics Engineering Visvesvaraya National Institute of Technology, Nagpur, India 78699.

[3]. Mr.Arun Anup M,"Image forgery And Its Detection: A survey (2015)", Department of computer engg and science, MES college of Engineering.

[4]. Salam A.Thajeel, Ghazali Sulong,"A Survey Of CopyMove Forgery Detection Techniques", Journal of Theoretical and Applied Information Technology, 10th December 2014.

[5]. Vincent Christlein, " An Evaluation Of Popular CopyMove Forgery Detection Approaches", Student member IEEE,vol.07.no 6 December 2012.

[6]. X.bo.w.Junwen,"Image Copy-Move forgery detection based on SURF", in proc. Int. conf., multimedia inf.Netw.(MINES). Nov.2010.

[7]. Jessica Fridich, David Soukal,"Detection of Copy Move Forgery in Digital Image", Department of computer Science, NY 13902-6000.

[8]. Hwei-Jen Lin, Chun-Wei Wang, Yang-Ta Kao, "Fast Copy-Move Forgery Detection", WSEAS Transactions On Signal Processing, Issue 5, Volume 5, May 2009.

[9]. Matthew C. Stamm,, "Forensic Detection of Image Manipulation Using Statistical Intrinsic Fingerprints", IEEE Transactions On Information Forensics And Security, Vol. 5, No. 3, September 2010.

[10]. Rani Mariya Joseph, Chithra A.S.,"Literature Survey on Image Manipulation Detection" ,International Research Journal of Engineering and Technology (IRJET) ,Volume: 02 Issue: 04,July-2015.

Cite this article as :

Ishrath Nousheen, Anugu Lahari Reddy, Poniganti Nikitha, "Digital Image Forgery and Techniques of Forgery Detection", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 2, pp.650-654, March-April-2023.