AN APPROACH FOR COPY-MOVE ATTACK DETECTION AND TRANSFORMATION RECOVERY

Snehal P. Chavhan[1] , Prof. D. W. Wajgi[2]

[1]Student, Department of Computer Engineering, St. Vincent Palloti College of Engineering & Technology, Nagpur, India , Maharashtra, India

[2]Assistant Professor, Department of Computer Engineering, St. Vincent Palloti College of Engineering & Technology, Nagpur, India

, Maharashtra, India

Abstract **- Digital images play an important role in the carrier of information and are widely used in all areas of day-to-day life. However, with the development of modern science and technology, more and more image processing software's are developed. This leads to the forgery of digital images. So, the authenticity of the image information faces great challenge in Digital Image Forensics. The main area of concern is the Copy-Move forgery in Digital Images. Copy-move forgery is one of the forensic technique in which particular area is get copied and then pasted onto the other portion of the image. Therefore, the main aim is to identify the forged region in an given image. The SIFT (Scale Invariant Feature Transform) algorithm is used for extracting the features from an image. This algorithm is divided into four stages. Each stage plays an important role in extracting features from an image. The forgery is detected when similar features are detected within the pre-defined areas. After detecting the features, next task is to detect geometric transformations made in an image. The RANSAC (Random Sample Consensus) algorithm is used to detect the geometric transformations made in an image.**

Keywords **: C**opy-Move Forgery, Feature Extraction, Geometric Transformations.

1. INTRODUCTION

Copy-move forgery in Digital Image is a simple and effective technique. In this type of forgery, a part of the image is copied and pasted to another part of the same image. Copy-move simply requires the pasting of image blocks in same image and hiding important information from the image. Thus, this changes the originality and degrades the authenticity of the image. Digital image forgery detection techniques are divided into active approaches and passive approaches. In active approach, the digital image requires some pre-processing such as watermark embedding or signature generation at the time of creating the image. In passive approach, don't require any prior information about the image and depends on traces left on the image by different processing steps during image manipulation. A number of techniques proposed to detect copy-move forgery which can be classified into two main categories such as Block-based methods and Key-point based methods [1]. Good forgery detection method should be robust to manipulations made on the copied content. These attacks are not detected by the single method. There are several methods by which these attacks can be detected.

In copy-move forgery, some transformations such as, rotation, scaling can be made. To detect those transformations some methods are available. To maintain the originality of the image transformations made in an image should be detected and if possible the image should be recovered. The detection algorithm should be robust enough to detect the manipulations done in an image. Nowadays, due to rapid advances and availabilities of powerful image processing software, modifying the content of digital images becomes much easier with the help of sophisticated software such as Adobe Photoshop. Pictures are the most common and effective way of giving or conveying information. Digital imaging has matured to become the dominant technology for creating, processing, and storing pictorial memory and evidence. Though this technology brings many advantages, it can be used as a misleading tool for hiding facts and evidences. This is because today digital images can be manipulated in such perfection that forgery cannot be detected visually. In fact, the security concern of digital content has arisen a long time ago and different techniques for validating the integrity of digital images have been developed. There are many ways to categorize the image tampering, and generally, we can tell that some usually performed operations in image tampering are:

1. Deleting or hiding a region in the image.
2. Adding a new object into the image.

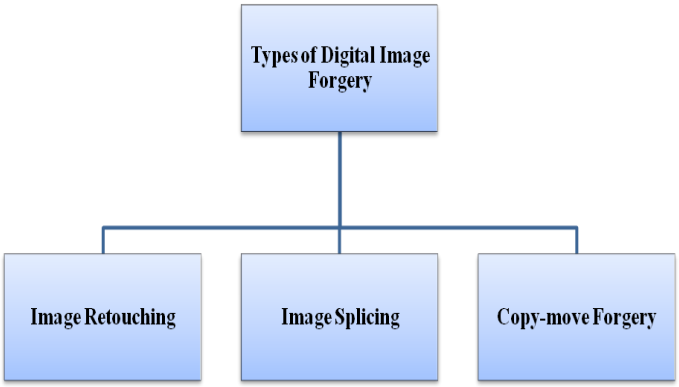
3. Misrepresenting the image information.

To insert and splicing image part of the original image is the one of the most typical method. Watermarking is the popular way to counterfeit the forgery image. Unlike conventional film photographs, however, digital images can be easily edited and modified with the aid of today's computer technology. Modification and synthesis of digital images can be easily performed by a novice with available sophisticated image processing software's like Adobe Photoshop [2]. While this has the significant advantage of enjoying the creation of digital works, it has the shortcoming of being maliciously abused in cases where "proof" is required such as in images of medical reports or crime scenes. Since digital images are subjected to illicit distribution, owners of such data are cautious about making their work available without some method of identifying ownership and copyright.

In the fields such as forensics, medical imaging, e-commerce, and industrial photography, authenticity and integrity of digital images is important. In medical field physicians and researchers make diagnoses based on imaging which is crucial as one is dealing with human life. E-commerce has drastically increased in recent years due to advancement of information technology and the internet. As per the world internet statistics, from 2000-2005 a growth of 160% has been reported [4]. This is currently a market of approximately 50 million internet users who have made an online retail purchase. This cohort will grow to nearly 100 million internet users by 2008 and will be responsible for nearly 90% of all online retail sales by that time.

Online marketing is mainly based on multimedia technology with images and video as basic elements of product description. With the increase of sophisticated and advanced image processing and manipulation software's coming in to markets, even a novice has gained with power to tamper images and counterfeit revising the age old saying "A picture is worth a thousand words" to "A picture unworthy a thousand true words". "The introduction and rapid spread of digital manipulation to still and moving images raises ethical issues of truth, deception, and digital image integrity", [5]. "With professionals challenging the ethical boundaries of truth, it creates a potential loss of public trust in digital media", [5].

There are many cases of digital image forgery. All of these cases can be categorized into three major groups, based on the process involved in creating the fake image. The groups are image retouching, image splicing, and image copy-move forgery.



2. LITERATURE SURVEY

In Paper [1], the CLBA (Classification Based Attack) algorithm is used for tampering detection. The main aim behind this paper is the identification of image whose SIFT (Scale Invariant Features Transform) keypoints have been removed artificially from the image and then the keypoints are re-inserted in an image, which are fake keypoints. This algorithm point out only to the first octave keypoints i.e those extracted from the image at its original resolution.

In paper [2], the Dempster–Shafer Theory of Evidence is used. This paper aims at decision fusion strategy for image forensics. The proposed system operates by combining at the measurement level thus it permits to retain the relevant information. The proposed framework includes:
i) The use of soft reasoning approach based on Dempster – Shafer theory of evidence.
ii)The ease with which new information can be included as soon as it becomes available.
iii)The framework which provides hierarchical structure, allows to trade-off between granularity about information provided by the fusion.

In paper [3], author has proposed a new approach of J-linkage along with copy-move detection algorithm where the SIFT features are considered. J-linkage is a method which starts with Random Sampling and is robust for multiple model fitting. It uses agglomerative clustering procedure that link elements with Jaccard distance smaller than one.

In paper [4], a forensic algorithm which differentiates between original and copied regions in JPEG images have been proposed. They have used hypothesis that the tampered image presents a double JPEG compression. There are two compression i.e aligned (A-DJPG) or nonaligned (NA-DJPG) and one of the scheme is used. Unlike previous approaches, the algorithm in this paper does not need to manually identify the suspected region in order to test the presence or the absence of double compression artifacts. Based on an improved and unified statistical model characterizing the arti- facts that appear in the presence of both A-DJPG or NA-DJPG, the proposed algorithm automatically computes a likelihood map indicating the probability for each 8×8 discrete cosine transform block of being doubly compressed.

In paper [5], author has proposed new methodology based on Transform Invariant Features. The main aim is based on MPEG-7 image signature tools that forms a part of the MPEG-7 standard. These tools are used for fast image and video retrieval. Basically such tools are designed to detect the duplicated region in an image or in video, but in separate image. Author aims to find the duplicated region in a same image.

The proposed method in [6], is based on a new feature measuring the presence of demosacking artifacts at local level. Demosacking is the digital process used to re-construct a full color image from incomplete image samples output from an image sensor overlid with a color filter array. Green channel extraction is used for extracting the features and then Map generation and Filtering is used by which the forgery map is created.

The author in paper [7], has proposed a spliced image detection technique based on Markov feature in DCT & DWT domain. The proposed system consists of two kinds of Markov features which are generated from the transition probability matrices e.g the expanded Markov in DCT & DWT domain. In this paper they made use of the DCT domain to capture the correlation between DCT coefficients and DWT domain is used to characterize the dependency among wavelet coefficients across positions, scales and orientations.

3. PROPOSED METHODOLOGY

The Proposed methodology uses both SIFT algorithm and RANSAC algorithm stated in previous chapter. The proposed approach is based on SIFT algorithm which extracts strong features. By which we can discover if a part of an image is was copy-moved and to detect which geometrical transformations was applied. The copied part has the same appearance that of the original one. Therefore the keypoints which are extracted in the forged region will be similar to some extend to the original ones. So, matching among SIFT features can be adopted for determining possible tampering.

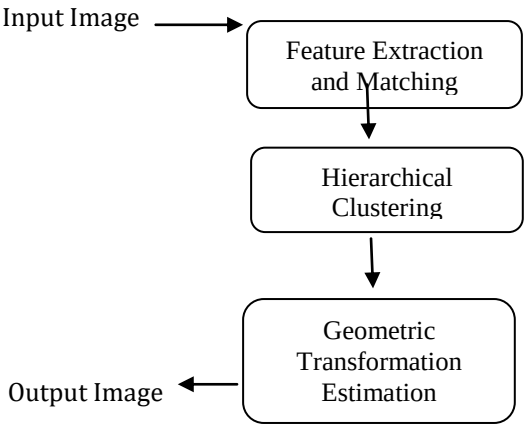


Figure 1: Overview of Proposed System

The first step consist of SIFT feature extraction and keypoint matching, the second step is keypoint clustering and detection, while the third step estimates the geometric transformation made, if transformation has been made.

4. CONCLUSION

The copy-move forgery detection is one of the emerging problems in the field of digital image forensics. Many techniques have been proposed to deal with this problem. One of the biggest issue in these techniques is to detect the duplicated image regions without getting affected by the common image processing operations, e.g. compression, noise addition, rotation. In this paper, several methods have been studied and compared, where the main idea in common was to detect cloned region, instead of detecting the whole duplicated regions. A novel methodology to support image forensics investigation based on SIFT features has been proposed.

REFERENCES

[1] Ghulam Muhammad, Muhammad Hussain, George Bebis "Passive copy move image forgery detection using undecimated dyadic wavelet transform", in Elsevier, 2012.

[2] Andrea Costanzo, Irene Amerini, Roberto Caldelli, and Mauro Barni, "Forensic Analysis of SIFT Keypoint Removal and Injection", IEEE Transactions on

Information Forensics and Security, Vol. 9, no. 9, September 2014.

[3] Marco Fontani, Tiziano Bianchi, Alessia De Rosa, Alessandro Piva, and Mauro Barni,"A Framework for Decision Fusion in Image Forensics Based on Dempster–Shafer Theory of Evidence", IEEE Transactions on Information Forensics and Security, Vol. 8, no. 4, April 2013.

[4] Irene Amerini, Lamberto Ballan, Roberto Caldelli, Alberto DelBimbo, Luca Del Tongo, Giuseppe Serra, "Copy Move Forgery Detection And Localization By Means Of Robust Clustering with JLinkage" ,L.Amerinietal./SignalProcessing:ImageCommunicatio n28(2013)659–669.

[5] Tiziano Bianchi and Alessandro Piva, "Image Forgery Localization via Block-Grained Analysis of JPEG Artifacts" IEEE Transactions on Information Forensics And Security, Vol. 7, No. 3, June 2012.

[6] Pravin Kakar, S and N. Sudha, "Exposing Post processed Copy–Paste Forgeries Through Transform-Invariant Features", IEEE Transactions On Information Forensics And Security, Vol. 7, No. 3, June 2012 .

[7] Pasquale Ferrara, Tiziano Bianchi, Alessia De Rosa, and Alessandro Piva, "Image Forgery Localization via Fine-Grained Analysis of CFA Artifacts" IEEE Transactions On Information Forensics And Security, Vol. 7, No. 5, October 2012.

[8] Zhongwei He, WeiLu, WeiSun, JiwuHuang, 'Digital Image Splicing Detection Based on Markov Features in DCT and DWT', Elsevier 2012, 4292-4299.

[9] Sebastiano Battiato, Giovanni Maria Farinella, Enrico Messina, and Giovanni Puglisi, "Robust Image Alignment for Tampering Detection", IEEE Transactions On Information Forensics And Security, Vol. 7, No. 4, August 2012.

[10] Irene Amerini, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimboand Giuseppe Serra,"A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery", IEEE Transactions On Information Forensics And Security, Vol. 6, No. 3, September 2011.

[11] Y. Huang, W. Lu, W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images". Forensic Sci. Int. Vol. 206, pp. 178_84, 2011.

[12] Pravin Kakar, N. Sudha, and Wee Ser, "Exposing Digital Image Forgeries by Detecting Discrepancies in Motion Blur" IEEE Transactions On Multimedia, Vol. 13, No. 3, June 2011.

[13] Ahmet Emir Dirik, Nasir Memon, "Image Tamper Detection based on Demosaicing artifacts", IEEE Transactions 2010.