RESEARCH ARTICLE OPEN ACCESS

Survey on Copy Move Image Forgery Detection Techniques

Jaseela S [1], Mrs. Nishadha S. G [2]
M.Tech Student [1], Asst. Professor [2]
Department of Computer Science and Engineering
Mohandas College of Engineering and Technology, Anad, Trivandrum
Kerala -India

ABSTRACT
The word 'image forgery' is very common in the world of powerful image editing tools. As the image is used for the verification processes, this is a severe issue. Detection of forged image from the original one is very hard. Naked eye cannot easily identify the tampered region from the forged Image. Since, it is crucial to develop a method which can detect the tampered image from the original one. Copy move image forgery is a common category of image forgery, in which the specific part of image is copied and pasted in the same image to conceal some important information. Copy-move forgery is done with the intention of either making an object "hidden" or creates additional copy of an object in a specified location. This survey paper is an attempt to study the different image forgery detection techniques which were proposed by many authors and their strengths and flaws.

Keywords:- Digital Forensics, tamper detection, copymove forgery, duplicated region detection

I. INTRODUCTION

Maliciously manipulating and tampering of digital images is very successful because of the use of powerful and easily available image editing tools such as Photoshop and Freehand. Because of this, there is a swift increase of the image forgery in news papers, TV and social media. An example for image forgery is shown in Fig.1.This trend leads to severe vulnerabilities and loss of credibility in the digital images. So detection of image forgery is essential, as the images are presented as evidence in a court. In this sense, image forgery detection is the central attraction of image forensics.

Nowadays, a large number of researchers have begun to focus on the problem of digital image forgery. Copy-move image forgery is a common category of image 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 forgery, image processing methods such as rotation, scaling, blurring, compression, and noise addition are applied to make convincing forgeries. An example for this type of forgery can be seen in Fig.2, where a group of people are copied and pasted to cover President George W. Bush. This process can be done without any modifications on the duplicated parts.

Because of the ease of use copy move image forgery is very common. Recently, many authors studied the problem of detecting these forgeries, considering the nature of region-duplication; there are at least two similar regions in a forged image.

According to the existing methods, there are two copy-move image forgery detection methods block-based algorithms and feature keypoint-based algorithms. In block-based methods, the image is divided into overlapping/non-overlapping blocks and feature vector is computed for each blocks. Similar feature are extracted and matched to find forged regions. In key-point based methods, keypoints are extracted and these keypoints are matched after calculating feature vector. The image is not divided into blocks, the feature vectors are matched to find forged regions.


INTERNET

Spies turn to high-tech info ops

PCs, Internet used for manipulating images, public opinion

ALTERED IMAGE

BY DANIEL VERTON

Federal intelligence agencies are studying ways to use computers and the Internet, rather than just leaflets and radio broadcasts, to shape and disseminate information designed to sway public opinion in the world's hot spots.

As part of its so-called "perception management" program, the intelligence community has for decades created misinformation to trigger political change without direct political or military involvement in countries where the United States has vested interests, such as Iraq and North Korea.

Acting on congressional recommendations to bolster research and development in information technology, intelligence agencies are turning to PCs to develop more sophisticated means of manipulating and delivering digital photos, video clips and recorded sound to portray fictitious events in hopes of provoking desirable outcomes.

1 2 3

Altered Egos

The top photo, of a fictitious meeting between President Clinton and Saddam Hussein, was generated by digitally altering and combining elements from three photos, shown below the altered image. Intelligence agencies plan to use similar techniques to create images and then disseminate them via the Internet in their efforts to influence events in foreign countries, such as Iraq.

Fig 1 Example of a digital forgery.

II. STEPS OF COPY MOVE IMAGE FORGERY

Since the copied part is from the same image, the color character, noise components and the other properties will be compatible with the rest of the image, some systematic approach needed to detect these forgeries. The general steps involved in copy-move image forgery are

Fig.2 Left is manipulated, right is the original image.

A. Pre-processing.

The scope of pre-processing is the improvement of image data and enhances features important for further detection. The image is converted into grey-scale when applicable. In both block-based and key-point based methods necessary pre-processing can be applied.

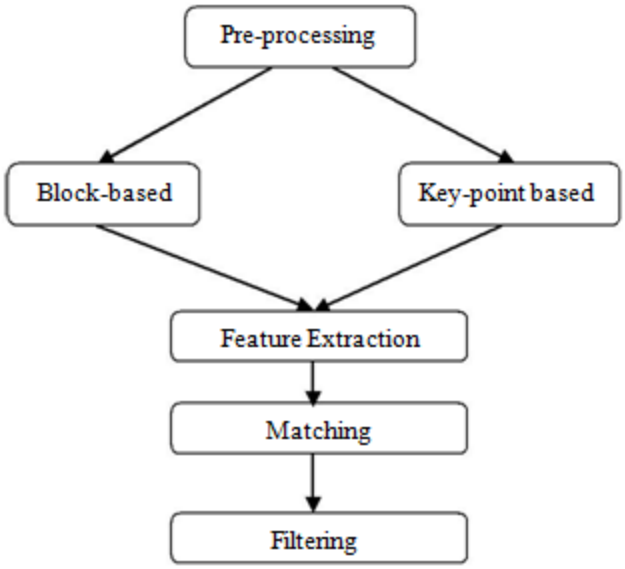

Fig3. Steps in Copy-Move forgery Detection

B. Feature Extraction

For block-based algorithms, feature vectors are extracted for each block. But in key-point based methods, feature vectors are computed only for key-points in the image such as regions with entropy etc.

C. Feature Matching

After feature extraction, the copy-move pairs are identified by searching blocks with similar features. High similarity between feature vectors can be interpreted as duplicated regions. In block-based method sort similar features and calculated approximate nearest neighbour in key-point based methods helps in the feature matching.

D. Filtering

We cannot predict presence and absence of forgery on the basis of a single similarity criterion. Filtering methods are used to reduce probability of false prediction. Finally post-processing can be adapted to preserve matches that exhibit a common behaviour.

III. LITERATURE SURVEY.

Jessica Fridrich, David Soukal, and Jan Lukas [1] proposed two techniques. One method is based on exact match for detection and other one is based on an approximate match. The first algorithm is for identifying those segments in the image that match exactly by ordering and matching of pixel representation of blocks. The technique behind the approximation (robust) match detection is similar to the exact match except it do not order and match the representation of the blocks. But robust depiction that consists of quantized Discrete Cosine Transforms coefficients. These methods successfully detect the forged part even when the forged area is modified to merge it with the background and when the forged image is saved in a distortion format, such as JPEG. But the time taking for matching is not relatively acceptable.

Alin C Popescu and Hany Farid [2] proposed an algorithm based on PCA (Principal Component Analysis) which is applied to analyse small fixed size image blocks to obtain a reduced dimensional representation. This representation is strong to predict minor variations in the image due to noise or lossy JPEG compression. Duplicated regions are then detected based on the alphabetical order of their component letters sorting all of the image blocks. This technique is more reliable in the case of additive noise and lossy JPEG compression.

Jian Li, Xiaolong Li, Bin Yang and Xingming Sun, [5] proposed a framework for copy move image forgery, in which the image is first segmented into non-overlapped patches. Then in first stage, try to find the suspicious matches by matching patches, and a transform matrix is estimated. Then in the second stage by refining the transform matrix confirm the existence of copy move image forgery. The key point-based methods are faster and more favourable than the block-based ones, but it poses faster detection compared with existing block based algorithms.

Saiqa Khan and Arun Kulkarni [3] proposed copy-move image forgery based on wavelet approach. In this technique, usage of wavelet transform for compression has been tested and phase correlation is used as similarity checking criterion for identifying duplicated of overlapping blocks formed. This is done through two phases. The first phase deals with the detection of reference and matching on the lowest level of wavelet transform compressed. For this, matrix is sorted and correlation is calculated with row ways relation. However this technique is good at detecting more difficult image cannot detected forgery with rotation and scaling.

Xunyu Pan and Siwei Lyu, [4] proposed keypoint based technique. In this method first the transform between matched SIFT (scale invariant feature transform) keypoints, which are insensitive to geometrical and distortions, and then finds all pixels within the duplicated regions after discounting the estimated transforms. Here they demonstrated its practical performance with several challenging forgery images created with most modern tools. The method is more reliable than other previous techniques. Since the SIFT algorithm, sometimes failed to find reliable keypoints in regions with little visual structures this method is not accurate.

Irene Amerini, Roberto Caldelli, Lamberto Ballan, Alberto Del Bimbo, and Giuseppe Serra, [6] proposed a method based on scale invariant features transform (SIFT) algorithm. This manages to detect copy–move forgery and, to recover the significant geometric transformation used to perform tampering. This algorithm extract robust features which can help to detect if a part of an image was copy-moved and whether it is undergo geometrical transformation. Since the pasted part has basically the same as of the original one, so that the extracted keypoints from tampered region same as the original ones. So, matching among SIFT features can be selected for the task of determining possible tampering. In the first step SIFT features are extracted and keypoints are matched, the second step consists of keypoint clustering and tampered region detection, and the third step involves estimation of the occurrence of geometric transformation, if forgery has been detected. This method also deals with multiple cloning. But it failed to detect forgery in the highly uniform texture image.

The details of the literature survey are summarized in Table.1

TABLE I

COMPARISON OF DIFFERENT COPY MOVE IMAGE FORGERY TECHNIQUES

Title	Method	Advantages	Disadvantages
Detection of Copy-Move Forgery in Digital Images[1]	Block based method. Image is divided to blocks and forged parts are detected with exact match and appropriate match	It can detect images with distortion format	Slow detection process
Exposing digital forgeries by detecting duplicated image regions[2]	Block based method. PCA applied to obtain reduced dimensional representation.	More reliable to detect noisy and lossy images	Sometimes it failed to detect difficult forgeries.
Robust Method for Detection of Copy-Move Forgery in Digital Images. [3]	Key-point based technique. Wavelet transform technique is used and computes phase correlation to detect similarity.	Lower computational complexity	Duplicated regions through angles and scaled regions cannot detect.
Segmentation-Based Image Copy-Move Forgery Detection Scheme [5]	Key-point based technique. Extracted key points from patches and matched for duplicated regions.	Segment image into semantically independent patches An accurate estimation of transform matrix is obtained by EM based algorithm [8]	Re-estimation of transform matrix is complex.
Region Duplication Detection Using Image Feature Matching [4]	Key point based method. By calculating SIFT key-points finds pixels within the duplicated regions.	Reliable than other key point techniques	Sometimes it gives vague results
A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery[6]	Key point based method. Key points are extracted and key point localization is done for detection.	Good at determine the Geometric transformation.	Not good at detection phase with respect to cloned image patch with high uniform texture

IV. CONCLUSION.

While going through the various papers, which describe techniques for copy move image forgery, it has been seen that most of the existing block based algorithms use a similar techniques, the only difference is that they apply different feature extraction methods. However these techniques are effective in copy move image forgery detection, they have three drawbacks:

1) The host image is divided into over-lapping and regular blocks, which is computationally expensive as the image size increases;

2) They cannot address complex geometrical transformations of the copied regions;

3) Recall rate is low as the blocks are in a regular shape

Although the existing key point based methods can avoid the first two drawbacks, but recall rate is poor. Chi-Man Pun, Xiao-Chen Yuan, and Xiu-Li Bi [7] proposed a copy move image forgery detection technique can solve these issues successfully. So I accepted this paper as my base paper for thesis work

REFERENCES

[1] Jessica Fridrich, David Soukal, and Jan Lukáš," Detection of Copy-Move Forgery in Digital Images", in *Proc. Digit. Forensic Res. Workshop*, Cleveland,OH, Aug. 2003.

[2] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions,"

Dept. Comput. Sci., Dartmouth College, Hanover, NH, USA, Tech. Rep. TR2004-515, 2004

[3] Saiqa Khan, Arun Kulkarni," Robust Method for Detection of Copy-Move Forgery in Digital Images" International Conference on Signal and Image Processing,2010.

[4] L. Fitzpatrick and M.Dent," Region Duplication Detection Using Image Feature Matching," Ieee Transactions On Information Forensics And Security, Vol. 5, No. 4,2010.

[5] Jian Li , Xiaolong Li ,Bin Yang and Xingming Sun," Segmentation-Based Image Copy-Move Forgery Detection Scheme," , IEEE Transactions on Information Forensics and Security ,Volume:10 , dec 2014.

[6] Irene Amerini, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, and 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

[7] Chi-Man Pun, Xiao-Chen Yuan, and Xiu-Li Bi," Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching," Ieee Transactions On Information Forensics And Security, Vol. 10, No. 8, August 2015.

[8] J. Bilmes, "A gentle tutorial of the EM algorithm and its application to parameter estimation for Gaussian mixture and hidden Markov models," Int. Comput. Sci. Inst., Berke ley, CA, USA, Tech. Rep. TR-97-021, 1997.