IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 80-83
www.iosrjournals.org

ADVANCED DIGITAL IMAGE FORGERY DETECTION: A REVIEW

Ms. P. G.Gomase[1], Ms. N. R. Wankhade[2]
[1](IT Department, YeshwantraoChavanCollege of Engineering, India)
[2](IT Department, YeshwantraoChavanCollege of Engineering, India)

ABSTRACT : *The use of digital photography has increased over the past few years, the trend which opens the door for new and creative ways to forge images. Now a day's several software's are available that are used to manipulate image so that the image is look like as original. Images are used as authenticated proof for any crime and if these image does not remain genuine than it will create a problem. Detecting these types of forgeries has become serious problem at present. To determine whether a digital image is original or doctored is a big challenge. To find the marks of tampering in a digital image is a challenging task. A copy-move image forgery is done either for hiding some image entity, or adding more minutiae resulting in forgery. In both the case, image reliability is lost. Although this technology brings many advantages but it can be used as a confusing tool for hiding facts and evidences. In the paper, first, classification of Image forgery detection techniques is discussed and the two important techniques for pixel based forgery detection are discussed. A technique for copy-move forgery detections discussed. But this approach takes into account only shifting of copied regions. So another technique is discussed for fast-copy-move detection. Basic design and algorithm of proposed system is on the basis of above mentioned techniques. First technique i.e. copy move forgery has lower computational complexity but the final result is not precise, on the other hand second approach is complex but precise. Main disadvantage of second technique is that it is not be able to detect very small copied regions. Proposed system will cover disadvantages of both the system and can be robust to various types of copy move processing. All the methods which have been suggested draw strengths from different transforms to make them robust against post processing and to reduce the number of logical blocks to compare. However, as yet no method achieved 100% robustness against post processing operations.*

Keywords :*copy-move forgery, forensic, forgery detection techniques, image forgery, tampering.*

I. INTRODUCTION

In today's world it is easy to manipulate the image by adding or removing some elements from the image which results in a high number of image forgeries. With the increasing applications of digital imaging, different types of software are introduced for image processing. Such software can do an alteration in digital image by changing blocks of an image with no showing the effect of the modification in the forged image. These modifications cannot be noticed by human eyes. Therefore verification of originality of images has become a challenging task. An image can be manipulated with a wide variety of manipulation techniques such as scaling, rotation, blurring, resampling, filtering, cropping, etc. We need image forgery detection technique in many fields for protecting copyright and preventing forgery. The verification of originality of images is required in variety of applications such as military, forensic, media, scientific, glamour, etc. Image tampering is a digital art which needs understanding of image properties and good visual creativity. Detection of image tampering deals with investigation on tampered images for possible correlations embedded due to tampering operations. Detecting forgery in digital images is a rising research field with important implications for ensuring the credibility of digital images.

Digital image forgery detection techniques are classified into active 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, which would limit their application in practice. Moreover, there are millions of digital images in internet without digital signature or watermark. In such scenario active approach could not be used to find the authentication of the image. Unlike the watermark-based and signature-based methods; the passive technology does not need any digital signature generated or watermark embedded in advance.

Passive techniques for image forensics operate in the absence of any watermark or signature. These techniques work on the assumption that although digital forgeries may leave no visual clues

that indicate tampering, they may alter the underlying statistics of an image. The set of image forensic tools can be roughly grouped into five categories:

1. Pixel-based techniques that detect statistical anomalies introduced at the pixel level.
2. Format-based techniques that leverage the statistical correlations introduced by a specific lossy compression scheme.
3. Camera-based techniques that exploit artifacts introduced by the camera lens, sensor, or on-chip post-processing.
4. Physically based techniques that explicitly model and detect anomalies in the three-dimensional interaction between physical objects, light, and the camera;
5. Geometric-based techniques that make measurements of objects in the world and their positions relative to the camera [1].

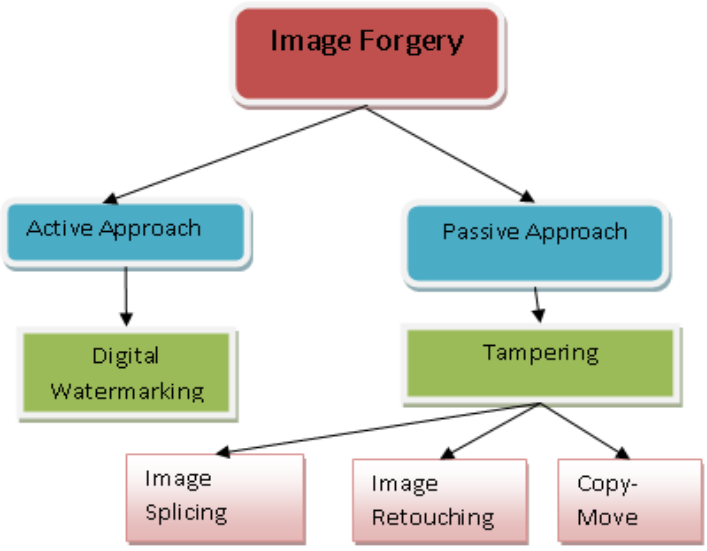

Fig.: classification of forgery detection techniques.

The copy move forgery is one of the difficult forgeries. This is the most common kind of image tampering technique used, where one needs to cover a part of the image in order to add or remove information. Copy-Move is a special type of image manipulation technique in which a part of the image itself is copied and pasted into another part of the same image. Image-splicing is defined as a paste-up produced by sticking together photographic images. In a copy-move attack, parts of the original image is copied, moved to a desired location, and pasted. Detecting copy-move in an image indulges broad search of local pattern or region matches [2].

II. Related Work

There were several techniques proposed to detect image forgery in the literature of digital image forensics. Copy move forgery is one of the popular methods to create the image forgery in which the part is copied and moved to the other place in the same image.

There are so many techniques to detect such type of forgeries. One approach to detect copy-move forgery detection, Classification of Image forgery detection techniques is discussed and the two important techniques for pixel based forgery detection are discussed. A technique for copy-move forgery detection is discussed. But this approach takes into account only shifting of copied regions. So, another technique is discussed for fast-copy-move detection and made the comparative study regarding both algorithms. While doing comparative study author introduces difference between two algorithms Copy move algorithm has lower computational complexity but the final result is not precise. Fast copy move approach is complex but precise. Main disadvantage of second technique is that it is not be able to detect very small copied regions[3].

The other approach presents the active and passive or blind techniques for detecting image tampering. Set of image forensics tools can be grouped into five categories: Pixel-based techniques, Format-based techniques, Camera-based techniques, Physics based techniques, Geometric-based techniques. Paper introduces Forgery detection using DCT followed by High Pass Filtering. In this method image is divided into 8x8 image sub blocks and DCT is applied. This paper mainly focuses on how we can achieve image forgery detection using passive techniques[4].

Another approach is to categorize the image tampering based on different points of view generally, most often performed operations in image tampering are:Deleting or hiding a region in the image.Adding a new object into the image and misrepresenting the information of image.Firstly, the given image is divided into overlapping rectangular blocks except in where overlapping circular block are created.Secondly, to reduce the search area and to make the search unit as robust as possible to post processing like compression, Gaussian noise, scaling and rotation, some transformation technique is used like DCT, PCA, DWT, SVD, LLE etc.Thirdly feature vectors, after transformation are sorted lexicographically or using k-d tree. The neighboring vectors are compared against the similarity parameters to hint the duplication of region[5].

The new techniques and methods currently available in the area of digital image forgery detection on JPEG images. Currently, most acquisition and manipulation tools use the JPEG standard for image compression.

As a result of one of the standard,the proposed approach has been evaluated using datasets containing different types of tampered images. Paper proposes two techniques:JPEG Block Technique and Result of Direction Filter. If image tampering occurs in a compressed then JPEG Block methodologies is to support and predict forgery region along with different image format at the same time uncompressed image and then that image is converted to the JPEG image format, the JPEG Block technique will fail to capture evidence of tampering. This conversion process destroys all proof of tampering since the original tampering does not affect any JPEG blocks. Additionally, any image tampering performed on an image prior to an image size reduction will eliminate detectable anomalies for the direction filter technique[6].

III. Performance Issues Of Existing System

Copy-Move is a specific type of image manipulation, where a part of an image itself is copied and pasted into another part of the same image. Copy- Move forgery is performed with the intention to make an object “disappear” from the image by covering it with a small block copied from another part of the same image.While comparing both algorithms each one has its own disadvantages:

1. Copy move algorithm has lower computational complexity but the final result is not precise.
2. Fast copy move approach is complex but precise. Main disadvantage of second technique is that it is not be able to detect very small copied regions.
3. But both algorithms fail to give accurate result when image having natural duplication.The applicability of any copy-move forgery algorithm depends highly upon the requirement that it should detect forged duplicated regions in an image but it should not detect regions which have natural or original duplication in them.
4. Both algorithms give poor result for the images where the attacker has made detection more difficult by applying noise and JPEG quality level changes

IV. Research Methodology

To cover the disadvantages of copy-move and fast copy-move technique we will develop an algorithm which combines operations of both techniques which gives the system having lower computational complexity with precise result. Proposed system first applies DWT which will describe local changes in brightness in that image.Due to DWT usage, detection is first carried out on lowest level image representation. This approach drastically reduces the time needed for the detection process and increases accuracy of detection process. Filtering is applied to remove the noise from image. Median filtering is similar to using an averaging filter, in that each output pixel is set to an average of the pixel values in the neighborhood of the corresponding input pixel. However, with median filtering, the value of an output pixel is determined by the *median* of the neighborhood pixels,

rather than the mean. The median is much less sensitive than the mean to extreme values (called *outliers*). Median filtering is therefore better able to remove these outliers without reducing the sharpness of the image. Then divide the overlapping block pixels into matrix and then sort the matrix, finally locate the copy move regions by pixel matching.

1. DWT:

Proposed system first applies DWT which will describe local changes in brightness in that image.Due to DWT usage, detection is first carried out on lowest level image representation. This approach drastically reduces the time needed for the detection process and increases accuracy of detection process.
Median Filter:
Filtering is applied to remove the noise from image. Median filtering is similar to using an averaging filter, in that each output pixel is set to an average of the pixel values in the neighborhood of the corresponding input pixel. However, with median filtering, the value of an output pixel is determined by the *median* of the neighborhood pixels, rather than the mean. The median is much less sensitive than the mean to extreme values (called *outliers*). Median filtering is therefore better able to remove these outliers without reducing the sharpness of the image.
We are using median filtering to avoid system from giving poor result for the images where the attacker has made detection more difficult by applying noise and JPEG quality level changes.

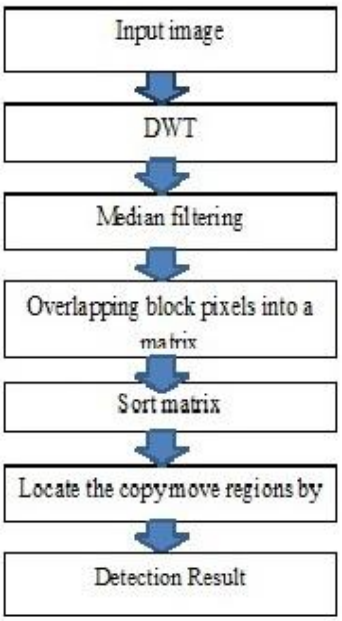

Fig 2: steps for detecting image forgery

2. Forgery detector: This is a main module of our project. It takes the processed image of DWT and median filtering as an input. Main work of this module is:
   2.1 Divide image into blocks
   2.2 Overlapping block pixels into a matrix
   2.3 Locate the copy move regions by pixel matching.

V. Conclusion

In this paper, classification of Image forgery detection techniques is discussed and the two important techniques for pixel based forgery detection are discussed. A technique for copy-move forgery detections discussed. But this approach takes into account only shifting of copied regions. So another technique is discussed for fast-copy-move detection. Basic design and algorithm of proposed system is on the basis of above mentioned techniques. First technique i.e. copy move forgery has lower computational complexity but the final result is not precise, on the other hand second approach is complex but precise. Main disadvantage of second technique is that it is not be able to detect very small copied regions. Proposed system will cover disadvantages of both the system and can be robust to various types of copy move processing.

References

[1] HanyFarid, "Image Forgery Detection", IEEE SIGNAL PROCESSING MAGAZINE, MARCH 2009, pp. 16-25.
[2] Ashima Gupta, NisheethSaxena, S.K Vasistha, "Detecting copy move forgery using DCT",International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013 1 ISSN 2250-3153
[3] PradyumnaDeshpande,PrashastiKanikar,"Pixel Based Digital Image Forgery DetectionTechniques", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp. 539-543.
[4] Nair S. Rajlaxmi and Vijaya C, "Detection of Forgeries in Digital Color Image", World Journal of Science and Technology 2011, 1(8): 32-36 ISSN: 2231 – 2587 www.worldjournalofscience.com.
[5] Sunil Kumar, P. K. Das, Shally, S. Mukherjee, "Copy-Move Forgery Detection in Digital Images: Progress and Challenges", International Journal on Computer Science and Engineering (IJCSE) ISSN : 0975-3397 Vol. 3 No. 2 Feb 2011.
[6] S.Murali,Govindraj B. Chittapur ,Prabhakara H. S and Basavaraj S. Anami, "Comparison And Analysis Of Photo Image Forgery Detection Techniques", International Journal on Computational Sciences & Applications (IJCSA) Vo2, No.6, December 2012..