Detecting Copy –Paste Forgery in Images Using Statistical Fingerprints

Amandeep Kaur, Surbhi Gupta, and Parvinder S. Sandhu

***Abstract*—**Images have become the main information carriers in the digital era. Images contained tons of information also known as metadata. With the widespread availability of image editing software, digital images have been becoming easy to manipulate and edit even for non-professional users. Image manipulation has become commonplace with growing easy access to powerful computing abilities. One of the most common types of image forgeries is the copy-paste forgery, wherein a region from an image is replaced with another region from the same image (with possible transformations). Because the copied part come from the same image, its important properties, such as noise, color palette and texture, will be compatible with the rest of the image and thus will be more difficult to distinguish and detect these parts. Digital image forensics is a brand new research field which aims at validating the authenticity of images by recovering information about their history. The aim is to propose methodology to identify such unbelievable photo images and succeeded to identify forged region by given only the forged image.

***Keywords*—**About four key words or phrases in alphabetical order, separated by commas.

I. Introduction

A Digital image is a numeric representation of a two-dimensional image. Depending on whether the image resolution is fixed, it may be of vector or raster type. Without qualifications, the term "digital image" usually refers to raster images also called bitmap images. When we see a picture on our monitor or use our digital camera (or Scanner), the image we are viewing or dealing with, is not continuous like a pencil drawing – it is made up of many small elements next to each other. When we have enough elements, we get the illusion of a picture or image. Early digital images (before color) appeared in black and white. The tiny elements that comprised digital images were either black or white. These two 'colors' corresponded to 1 and 0 (called BITS or BI-nary digits). Digits 1 and 0 are used in the binary (base 2) system. Thus, a map (pattern) made up of these 1's and 0's was referred to as a bit-map. All digital images are a rectangle or square. Today, the elements are called pixels.

Forensics means the use of science and technology in the investigation and establishment of facts. So the photographs or other pictures can be transmitted to and reconverted into pictures by another computer.

Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices. Digital image forensics aims at validating the authenticity of images by recovering information about their history. Two main problems are addressed: the identification of the imaging device that captured the image, and the detection of traces of forgeries. Nowadays, thanks to the promising results attained by early studies and to the always growing number of applications, digital image forensics represents an appealing investigation domain for many researchers. With the widespread availability of image editing software, digital images have been becoming easy to manipulate and edit even for non-professional users. Image manipulation has become commonplace with growing easy access to powerful computing abilities. Some common image manipulation with the intension of deceiving a viewer includes:-

- Copy and paste
- Composition or Splicing
- Retouching,healing,cloning
- Content embedding or steganography

One of the most common types of image forgeries is the copy-paste forgery, wherein a region from an image is replaced with another region from the same image (with possible transformations). Because the copied part come from the same image, its important properties, such as noise, color palette and texture, will be compatible with the rest of the image and thus will be more difficult to distinguish and detect these parts. Digital image forensics is a brand new research field which aims at validating the authenticity of images by recovering information about their history.

Applications of Digital Image Forensics:-

The digital image forensics has been used in several applications. It includes:

Crime investigation – breach of rules or laws for which some governing authority (via mechanisms such as legal systems) can ultimately prescribe a conviction. Crime location where an illegal act took place, and comprises the area from which most of the physical evidence is retrieved by trained law enforcement personnel, crime scene investigators (CSIs) or in rare circumstances, forensic scientists.

Amandeep Kaur, Research Scholar, Punjab Technical University, Jalandhar and Assistant Professor, Department of Computer Science, RIEIT,Rupnagar, India.

Surbhi Gupta, Assistant Professor, Department of Computer Science, RBIEBT, Mohali, India.

Parvinder S. Sandhu, Professor, Department of Computer Science, RBIEBT, Mohali, India

- Mortuary investigations
- Laboratory examination
- Forensic document examination:- Forensic document examination or questioned document examination answers questions about a disputed document using a variety of scientific processes and methods. Many examinations involve a comparison of the questioned document, or components of the document, to a set of known standards. The most common type of examination involves handwriting wherein the examiner tries to address concerns about potential authorship.

II. Previous Work

Several reviews of the literature on image retrieval have been published, from a variety of different viewpoints.

Bayram (2006) has mentioned that most of the times a part of the image is copied and pasted on another part generally to conceal unwanted portions of the image. Hence, the goal in detection of copy-move forgeries is to detect image areas that are same or extremely similar. In this paper, the author review several methods proposed to achieve this goal. These methods in general use block-matching procedures, which first divide the image into overlapping blocks and extract features from each block, assuming similar blocks will yield similar features. Later, a matching step takes place where the aim is to find the duplicated blocks based on their feature vectors. A forgery detection decision is made only if similar features are detected within the same distance of features associated to connected blocks. The author examine several different block based features proposed for this purpose in relation to their time complexity and robustness to common processing scaling up/down, compression, and rotation.

As result of powerful image processing tools, digital image forgeries have already become a serious social problem. Myna, (2010) has described an effective method to detect Copy-Move forgery in digital images. The technique works by first applying DWT (Discrete Wavelet Transform) to the input image to yield a reduced dimensional representation. Then the compressed image is divided into overlapping blocks. These blocks are then sorted and duplicated blocks are identified using Phase Correlation as similarity criterion. 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.

Stammn (2010) has discussed that as the use of digital images has increased, so has the means and the incentive to create digital image forgeries. Accordingly, there is a great need for digital image forensic techniques capable of detecting image alterations and forged images. A number of image processing operations, such as histogram equalization or gamma correction, are equivalent to pixel value mappings. In this paper, the author showed that pixel value mappings leave behind statistical traces, which can be referred to as a mapping's intrinsic fingerprint, in an image's pixel value histogram. Then author proposed forensic methods for detecting general forms globally and locally applied contrast enhancement as well as a method for identifying the use of histogram equalization by searching for the identifying features of each operation's intrinsic fingerprint. Additionally, a method to detect the global addition of noise to a previously JPEG-compressed image is proposed by observing that the intrinsic fingerprint of a specific mapping will be altered if it is applied to an image's pixel values after the addition of noise.

One of the principal problems in image forensics is determining if a particular image is authentic or not. This can be a crucial task when images are used as basic evidence to influence judgment like, for example, in a court of law. Generally, to adapt the image patch to the new context a geometric transformation is needed. To detect such modifications, a novel methodology based on scale invariant features transform (SIFT) is proposed by Amerini (2011). Such a method explains if a copy–move attack has occurred and, furthermore, to recover the geometric transformation used to perform cloning. Extensive experimental results are presented to confirm that the technique is able to precisely individuate the altered area and, in addition, to estimate the geometric transformation parameters with high reliability. The method also deals with multiple cloning.

Kakar (2012) explained that image manipulation has become commonplace with growing easy access to powerful computing abilities. In this paper, the author proposed a novel technique based on transform-invariant features. These are obtained by using the features from the MPEG-7 image signature tools. Results are provided which show the efficacy of this technique in detecting copy-paste forgeries, with translation, scaling, rotation, flipping, lossy compression, noise addition and blurring. Author obtained a feature matching accuracy in excess of 90% across post processing operations, and was able to detect the cloned regions with a high true positive rate and lower false positive rate than the state of the art.

III. Proposed Work

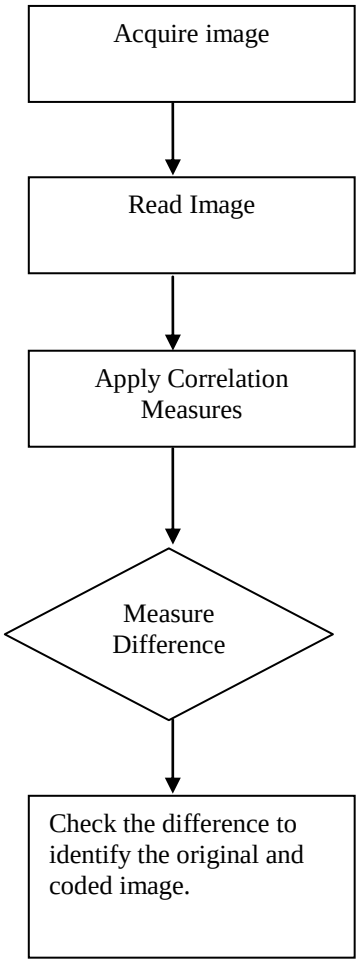
Image quality measures are figures of merit used for the evaluation of imaging systems or of coding/processing techniques. We consider several image quality metrics and study their statistical behavior when measuring various compression and/or sensor artifacts. A good objective quality measure should well reflect the distortion on the image due to, for example, blurring, noise, compression, sensor inadequacy. One expects that such measures could be instrumental in predicting the performance of vision-based algorithms such as feature extraction, image-based measurements, detection, tracking, segmentation etc. tasks. Our approach is different from companion studies in the literature focused on subjective image quality criteria, such as in . In the subjective assessment of measures characteristics of the human perception becomes paramount, and image quality is correlated with the preference of an observer or the performance of an operator on some specific task. A number of image quality measures have been proposed. One of the important quality measures is Correlation-based measures, that is, correlation of pixels, or of

the vector angular directions. Two correlation measures are:-

• Image Correlation Measures. The closeness between two digital images can also be quantified in terms of correlation function. These measures measure the similarity between two images, hence in this sense they are complementary to the difference-based measures.

• Moments of the Angles. A variant of correlation-based measures can be obtained by considering the statistics of the angles between the pixel vectors of the original and coded images. Similar "colors" will result in vectors pointing in the same direction, while significantly different colors will point in different directions.

This method will work as follows:-



IV. CONCLUSION

Several methods have been identified till yet to obtain the methods to detect copy paste forgeries in images. Image quality measures particularly are very useful in identifying image manipulation. The proposed technique aims at reduced set of quality measures to identify copy paste forgeries.

REFERENCES

[1] S.Khan and A.Kulkarni ,"Reduced Time Complexity for Detection of Copy-Move Forgery Using Discrete Wavelet Transform" International Journal of Computer Applications (0975 – 8887) Volume 6– No.7, September 2010.

[2] P.Kakar and N.Sudha "Exposing Post processed Copy-Paste Forgeries through Transform-Invariant Features", vol. 206, no. 1-3, pp. 178–184, 2011.

[3] S.Bayram,H.T.Sencar and N.Menon"A Survey of Copy-Move Forgery Detection Techniques", submitted to ICASSP 2009, 2009.

[4] A.C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," IEEE Transactions on Signal Processing, vol. 53(2), pp. 758–767, 2005.

[5] M.K. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," Proc. ACM Multimedia and Security Workshop, New York, pp. 1–9, 2005.

[6] M.Wu A. Swaminathan and K. J. Ray Liu, "Image tampering identification using blind deconvolution," Proc. IEEE ICIP, 2006.

[7] M.C.Stamnn,"Forensics Detection of Image Manipulation Using Statistical Intrinsic Fingerprints", IEEE Transactions on information Forensics And Security , vol. 5 No 3, 2010.