REVIEW PAPER ON DETECTING COPY MOVE FORGERY

Mandeep Kaur , Er.Mandeep Kaur

Abstract— **The different methods for processing and detecting forgery in digital images have received growing attention recently. This is due to the availability of up-to-date editing software and sophisticated digital cameras, which simplify the duplication of regions for the forgers where part of an image is pasted to another location to conceal undesirable objects. An example of these methods is copy-move (i.e., Cloning) forgery in digital images. Detection of copy-move forgery to search the copied regions and they're pasted ones, but detection may vary based on whether there has been any post-processing on the copied part before paste it to another party.**

Index Terms— **digital forensics, copy-move forgery, duplication forgery detection, forgery detection**

I. INTRODUCTION

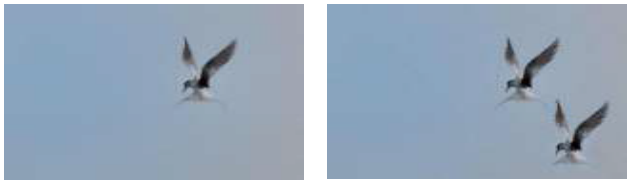
A digital image is a numeric representation of a two-dimensional image. Depending on whether the image resolution is fixed, it may be of vector or raster type. Without qualifications, the term "digital image" usually refers to raster images also called bitmap images. When we see a picture on our monitor 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. In Figure1, an example of copy-move forgery can be seen where the original image (Figure 1(a)) has one bird flying in the sky whereas in forged one (Figure (b)), Cloning tool of Photoshop has been used to show that there are two birds flying.



(a) (b)

Figure 1. Example of Copy-Move forgery (a) original image (b) tampered image

So, Digital image forensics aims at restoring some of the lost trustworthiness of digital images and revolves around the following two fundamental question:

- Where is the image coming from?
- (How) Has the image been processed after acquisition?

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

Manuscript received Oct 20, 2014

Mandeep Kaur, Assistant Professor, CSE department, Guru Kashi University, Talwandi Sabo, India

Er.Mandeep Kaur, Guru Kashi University , Talwandi Sabo, India

enforcement personnel, crime scene investigators (CSIs) or in rare circumstances, forensic scientists.
- 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. LITERATURE SURVEY

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

S.Bayram[2006] 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.

A.N.Myna[2010] As result of powerful image processing tools, digital image forgeries have already become a serious social problem. In this paper he describe an effective method to detect Copy-Move forgery in digital images. Our 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.

P.Kakar[2012] Image manipulation has become commonplace with growing easy access to powerful computing abilities. In this paper, the author propose 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. We obtain a feature matching accuracy in excess of 90% across post processing operations, and are able to detect the cloned regions with a high true positive rate and lower false positive rate than the state of the art.

III. TECHNIQUES USED

CFA (Color Filter Array) Forensic imaging device identification methods attempt to determine the type of device used to capture an image, ascertain the device manufacturer or model, and identify the particular imaging device used [10]. These method generally perform identification by estimating some device specific parameter such as CFA interpolation coefficients or sensor noise. Image forgery detection techniques have been proposed which operate by locating inconsistencies in these parameters [1], or by using these parameters to estimate a tampering filter.

DCT: DCT coefficients are quantized by dividing each coefficient by its corresponding entry in a quantization matrix, then rounding the result to the nearest integer. Finally, the quantized DCT coefficients are reordered into a single bit stream which is losslessly compressed. The image is decompressed by losslessly decoding the bit stream of quantized DCT coefficients, then reshaping it back into the series of blocks. The DCT coefficients are dequantized by multiplying each quantized DCT coefficient by its corresponding entry in the quantization matrix used during compression. Next, the inverse DCT (IDCT) of each block is computed, resulting in a set of pixel values in the YCbCr color space.

STATISTICALINTRINSIC INGERPRINTS OF PIXEL : A number of image processing operations, such as contrast enhancement, either include or can be specified entirely by a pixel value mapping. As is the case with most image processing operations, pixel value mappings leave behind distinct, forensically significant artifacts.

- **WAVELET TRANSFORM USING DAUBECHIES FILTER BANK**
- **INVERSE WAVELET**
- **WIENER FILTER**

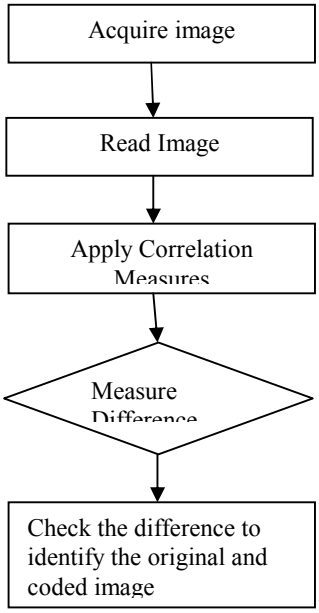
IV. METHODOLOGY

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:-



Flow chart to define the methodology

V. PARAMETERS CALCULATED

- MSE
- PSNR

CONCLUSION & FUTURE WORK

Copy-move forgery is one of the most frequently applied forgery technique. In this we use a robust method to detect the duplicated region in the digital image. We have conducted some test on the algorithm against sample images from the internet.We can improve the efficiency of forgery detection by applying wavelet transform. For future work, we plan to further optimize the data structures to gain additional query performance and further improve accuracy. The process can be further extended to different formats and works for binary scale, gray scale and color images also.

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.

[8]. M. Chen, J. Fridrich, M. Goljan, and J. Lukáˇs, "Determining image

[9]. origin and integrity using sensor noise," IEEE Trans. Inf. Forensics Security,vol. 3, no. 1, pp. 74–90, Mar. 2008.

[10]. T.-T. Ng, S.-F. Chang, J. Hsu, L. Xie, and M. P. Tsui, "Physics-motivatedfeatures for distinguishing photographic images and computergraphics," in Proc. ACM Multimdedia, Singapore, 2005, pp. 239–248.

[11]. M. K. Johnson and H. Farid, "Exposing digital forgeries in complexlighting environments," IEEE Trans. Inf. Forensics Security, vol. 2, no.3, pp. 450–461, Sep. 2007.

[12]. M. K. Johnson and H. Farid, "Exposing digital forgeries by detectinginconsistencies in lighting," in Proc. ACM Multimedia and SecurityWorkshop, New York, NY, 2005, pp. 1–10.

[13]. M. K. Johnson and H. Farid, "Exposing digital forgeries through chromaticaberration," in Proc. ACM Multimedia and Security Workshop,Geneva, Switzerland, 2006, pp. 48–55.

[14]. C. Popescu and H. Farid, "Exposing digital forgeries in color filterarray interpolated images," IEEE Trans. Signal Process., vol. 53, no.10, pp. 3948–3959, Oct. 2005.

[15]. T.-T. Ng, S.-F. Chang, and Q. Sun, "Blind detection of photomontageusing higher order statistics," in Proc. IEEE Int. Symp. Circuits Systems,Vancouver, BC, Canada, May 2004, vol. 5, pp. V-688–V-691.

[16]. S. Bayram, I.Avcibas, B. Sankur, and N. Memon, "Image manipulationdetection," J. Electron. Imag., vol. 15, no. 4, p. 041102, 2006.

[17]. Avcibas, S. Bayram, N. Memon, M. Ramkumar, and B. Sankur, "Aclassifier design for detecting image manipulations," in Proc. ICIP,Oct. 2004, vol. 4, pp. 2645–2648.

[18]. Swaminathan, M. Wu, and K. J. R. Liu, "Nonintrusive componentforensics of visual sensors using output image," IEEE Trans. Inf. ForensicsSecurity, vol. 2, no. 1, pp. 91–106, Mar. 2007.

[19]. J. Lukáˇs, J. Fridrich, and M. Goljan, "Detecting digital image forgeriesusing sensor pattern noise," in Proc. SPIE, Electronic Imaging, Security,Steganography, Watermarking of Multimedia Contents, San Jose,CA, Feb. 2006, vol. 6072, pp. 362–372.

[20]. Swaminathan, M.Wu, and K. J. R. Liu, "Digital image forensics viaintrinsic fingerprints," IEEE Trans. Inf. Forensics Security, vol. 3, no.1, pp. 101–117, Mar. 2008.

[21]. C. Popescu and H. Farid, "Exposing digital forgeries by detectingtraces of resampling," IEEE Trans. Signal Process., vol. 53, pp.758–767, Feb. 2005.