COPY PASTE DETECTION FROM THE COLOR IMAGES USING DWT

*Jasdeep Kaur
GZS-PTU Campus, Bathinda

**Er. Jyoti Gill
GZS-PTU Campus, Bathinda

ABSTRACT
As the use of digital multimedia content such as images and video has increased, so the incentive to create digital forgeries. Presently, powerful editing software allows forgers to create perceptually convincing digital forgeries. Accordingly, there is a great need for techniques capable of authenticating digital multimedia content. In response to this, researchers have begun developing digital forensic techniques capable of identifying digital forgeries. We use DWT and different filters for forensic tasks such as identifying cut-and-paste forgeries from JPEG compressed images. Additionally, we consider the problem of multimedia security from the forger's point of view. We demonstrate the technique that is used to detect the copy paste part from the colour image. In this tempered image is their that is used to detect the temper image and calculate the frames and their PSNR values.

Keywords: *Copy –paste , forensics , jpeg, DWT etc.*

I. INTRODUCTION

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.

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. 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.

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

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

II. Forgery Detection

Forgery detection methods become much more complicated to deal with the latest forgery techniques. This back to the availability of digital editing tools, alteration, and manipulation become very easy and as a result forgery detection becomes a complex and threatening problem [13]. Image forgery detection can be manipulated in various ways with many simple operations like affine transforms such as translation, scaling, etc., compensation operations such as brightness, colors, contrast adjustments, etc., suppression operation such as noise extraction, filtering, compression, etc.

The Proposed method of copy-move forgery detection has following main parts.

1. Discrete Wavelet Transform
2. Lexicographic Sorting
3. Shift Vector Calculation
4. Neighbor block matching

Discrete Wavelet Transform

Wavelet decomposition of the images is used due to its inherent multiresolution characteristics. The basic idea of using Discrete Wavelet Transform is to reduce the size of the image at each level, e.g., a square image of size 2j ×2j pixels at level L reduces to size 2j/2 × 2j/2 pixels at level L+1. At each level, the image is decomposed into four sub images. The sub images are labeled LL,LH, HL and HH, The notation LH, HL and HH correspond to the vertical, horizontal and diagonal components of the image respectively. LL corresponds to the coarse level coefficients or the approximation image. This image(LL) is used for further decomposition.. These sub images can be combined together to restore the previous image which was decomposed. Below figure shows the image pyramid[7].Level-0 image is used for matching of blocks and then these matched blocks are carried to the next higher level. Final match is performed on the original image itself.

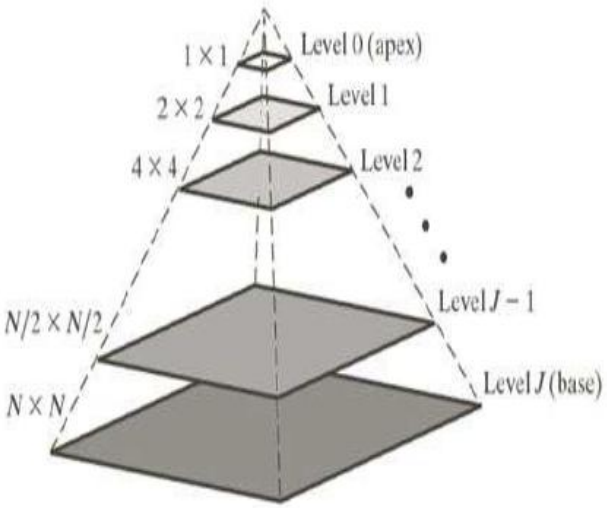

Figure 2:. Image pyramid

III. PROBLEM FORMULATION & OBJECTIVE

Digital image forensics aims at validating the authenticity of images by recovering information about their history. 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. The problem of detecting if an image has been forged is investigated; in particular, attention has been paid to the case in which an area of an image is copied and then pasted onto another zone to create duplication or to cancel something that was awkward. The photomontage detection problem, one of the fundamental tasks is the detection of image splicing. Image splicing assumes cut and paste of image regions from one image onto the another image.. Therefore, the originality and authenticity of images or data in many cases become challenging problem. Researchers have related the natural issues to the advance in computer graphics, animation, multimedia in the association of high computing machines,

algorithms, increases the complexity of the issue.

IV. OBJECTIVES

The main proposed aim of my thesis work is Detecting Copy –Paste Forgery in images Using Statistical Fingerprints.

The objectives can be written as follows:

Detecting copy paste forgery in images.

Exploiting the intrinsic statistical details to find the manipulation in images.

Comparison of this algorithm with an existing algorithm.

V. 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 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.

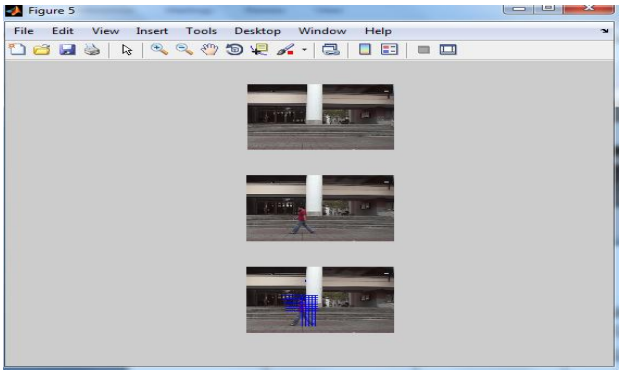

Figure 3:. Frame 14 Copy and paste detected images

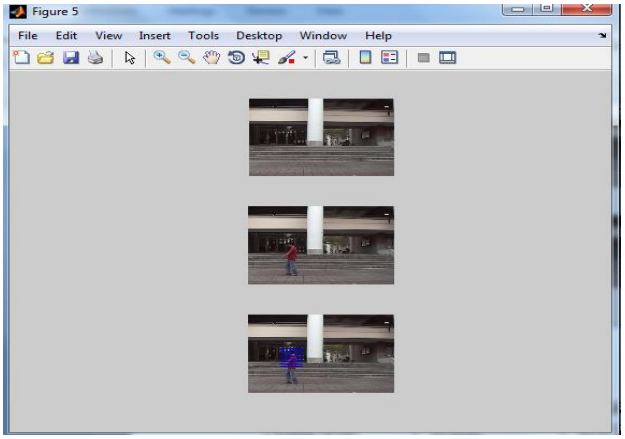

Figure 4. Frame 18 Copy and paste detected images

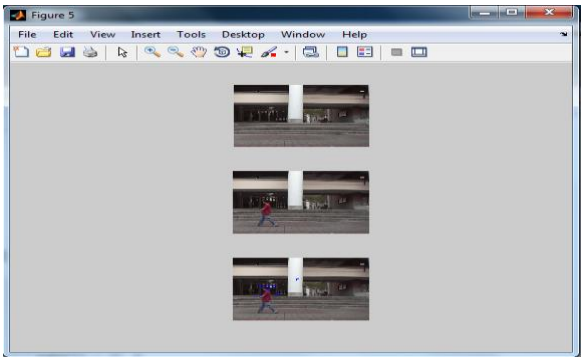

Figure 5:Frame 21 Copy and paste detected images

The above images shows the different copy paste parts of the images according to the true and false detected frame rates. In this all the above images have blue part that is the copy and paste part that is detected from the original images.

Table : 5.2 PSNR values according to frames

Frames	PSNR(:,:, 1)	PSNR(:,:, 2)	PSNR(:,:, 3)
Frame - 9/185	43.6393	43.4716	61.5756
Frame - 10/185	50.9982	51.2820	45.6538
Frame - 11/185	34.1377	35.1507	27.8444
Frame - 12/185	30.1017	30.9443	24.3336
Frame - 189/185	27.0845	27.5286	24.3597
Frame - 190/185	27.3697	27.9038	24.3729

CONCLUSION

Digital image forensics aims at validating the authenticity of images by recovering information about their history. 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 fundamental problems which research found in the literature can be categorized into the natural, forgery detection, flow mapping, and source identification. Therefore, the originality and authenticity of images or data in many cases become challenging problem. Researchers have related the natural issues to the advance in computer graphics, animation, multimedia in the association of high computing machines, algorithms, increases the complexity of the issue.In response to this, researchers have begun developing digital forensic techniques capable of identifying digital forgeries. These forensic techniques operate by detecting imperceptible traces left by editing operations in digital multimedia content. In this dissertation, we propose several new digital forensic techniques to detect evidence of editing in digital multimedia content. We use DWT and different filters for forensic tasks such as identifying cut-and-paste forgeries from JPEG compressed images. Additionally, we consider the problem of multimedia security from the forger's point of view.

REFERENCES

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.

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

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

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.

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

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

M. Chen, J. Fridrich, M. Goljan, and J. Lukáˇs, "Determining image origin and integrity using sensor noise," IEEE Trans. Inf. Forensics Security, vol. 3, no. 1, pp. 74–90, Mar. 2008.