IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 10, Issue 2 Ver. IV (Mar – Apr. 2015), PP 50-56
www.iosrjournals.org

Digital Image Forgery Detection using Wavelet Decomposition and Edge Detection

Lubhavni Sharma[1] and Mr. Parminder Singh[2]
[1, 2]*ECE Deptt., DIET, Kharar, Punjab, INDIA*

Abstract: *In the presented work, a copy-paste or cut-paste detection algorithm is discussed. The algorithm is based on wavelet decomposition of the input image and then extracting the edges so that the cut-paste or copy-paste region is detected by examining the edge pixels in wavelet domain. The scheme consists of: image acquisition, gray scale conversion, wavelet decomposition using haar wavelet, edge detection using sobel filter and then analysis of the region falling under the straight edge chain. The cut-paste or copy-paste region is normally in rectangular or square edge region. The edge pixels are analyse for their chain code so that the straight line could be extracted from the pixel tracing. This gives the possible region of image forgery. Further, the input image and forged images are compared with respect to different properties like entropy, power energy, standard deviation etc and re discussed in the algorithm.*

Keywords: *Haar Wavelet, Digital Image Forgery*

I. Introduction

The practice of forging photographs is probably as old as the art of photography itself. Digital photography and powerful image editing software made it very easy today to create believable forgeries of digital pictures even for a non-specialist. As digital photography continues to replace its analog counterpart, the need for reliable detection of digitally doctored images is quickly increasing. Verifying the content of digital images or identifying forged regions would be obviously useful for instance in the court of law, when digital pictures are presented as evidence.

The significant possible of visual media and the no difficulty in their acquisition, division and storage is such that they are more and more exploited to convey information. But digital images are easy to manipulate because of the availability of the powerful editing software and sophisticated digital cameras. Image processing experts can easily access and modify image content and therefore its meaning without leaving visually detectable traces. Moreover, with the spread of low-cost user friendly editing tools the art of tampering and counterfeiting visual content is no more restricted to experts. As a result, the modification (manipulation) of images for malicious purposes is now more common than ever. At the start, the manipulation is just improve the image's performance, but then many people started to change the image's content, even to gain their ends by these illegal and immorality methods. Based on the above reasons, it is important to develop a credible method to detect whether a digital image is tempered, so-called digital image forgery.

Copy-move is a simple and effective technique to create image forgeries in the digital image. In this technique a part of the image is copied and pasted to another part of the same image. Copy-move simply requires the pasting of image blocks in same image and hiding important information from the image. Thus, this changes the originality of the image and put at stake the authenticity of that image. 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. In passive approach, do not require any prior information about the image and depends on traces left on the image by different processing steps during image

II. Related Works

Xin Wang, Bo Xuan, Si-long Peng : A passive blind digital image forgery detection method was proposed in this paper. Basic defocus model shows that image patches with similar distances to the lens have similar blur kernel sizes. [1]

Jing Zhang, Zhanlei Feng□Yuting Su, Copy-Move attack is a special type of image forgery, inwhich a part of a digital image is copied and pasted to anotherpart in the same image in order to cover an important imagefeature. This paper describes a new and blind forensics approachfor detecting Copy-Move forgery. [2]

Wang Zhongmei1, Long Yonghong1: A passive blind digital image forgery detection method was proposed in this paper. Basic defocus model shows that image patches with similar distances to the lens have similar blur kernel sizes. [3]

Matthew C. Stamm, K. J. Ray Liu: Due to the ease with which convincing digital image forgeries can be created, a need has arisen for digital forensic techniques capable of detecting image manipulation. Once image alterations have been identified, the next logical forensic task is to recover as much information as possible about the unaltered version of image and the operation used to modify it. Previous work has dealt with the forensic detection of contrast enhancement in digital images. [4]

S.devi Mahalakshmi , K.vijayalakmi: In this modern age in which we are living, digital images play a vital role in many application areas. But at the same time the image retouching techniques has also increased which forms a serious threat to the security of digital images. [5]

Ruchita Singh, Ashish Oberoi and Nishi Goel:. In today's scenario forging of the Digital images has become a common phenomena. The availability of low cost manipulation software also boost to this practice. The foremost practice of manipulating the digital images employed by the most forgerer is the copy move forgery. [6]

Hieu Cuong Nguyen and Stefan Katzenbeisser: The use of digital photography has increased over the past few years, a 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. [6]

Tiago José de Carvalho,: For decades, photographs have been used to document space-time events and they have often served as evidence in courts. Although photographers are able to create composites of analog pictures, this process is very time consuming and requires expert knowledge. Today, however, powerful digital image editing software makes image modifications straightforward.[7]

Gang Cao, Yao Zhao, Senior Member: As a retouching manipulation, contrast enhancement is typically used to adjust the global brightness and contrastof digital images. Malicious users may also perform contrast enhancement locally for creating a realistic composite image. Assuch it is significant to detect contrast enhancement blindly for verifying the originality and authenticity of the digital images. In this paper, we propose two novel algorithms to detect the contrast enhancement involved manipulations in digital images. [8]

M. Ali Qureshi, M.Deriche,: Recent methods based on interest points and local fingerprints have been proposed to perform robust CBVCD (content-built visual copy discovery) of images and video. They include two steps: the search for similar local fingerprints in the database (DB) and a voting strategy that merges all the local results in order to perform a global decision. [9]

Seniha Ketenci I, Guzin: With the use of powerful image modifying software's, image authenticity is a big question for image forensics. One can no longer believe what they see. When a section of image is copied, geometrically transformed and pasted at different spot onto the same image with the intention of concealing or hiding some important information, it is copy move forgery. [10]

III. Image Acquisition

The images for detection of copy-pate or cut-paste or tampered detection are read in matlab environment in jpeg format using imread() function in matlab. This maps the input image into RxCx3 matrix form where RxCx1 is red component image, RxCx2 is green component image and RxCx3 is blue component image. The image pixel values are from 0 to 255 range i.e. 8-bit format and collectively the image is 24-bit color format in jpeg compressed form. The images are jpeg format and are converted to gray scale format using the following relation:

$$Gray(i,j) = 0.2989 * R(i,j) + 0.5870 * G(i,j) + 0.1140 * B(i,j)$$

Where Gray(i,j) is the gray scale intensity of the jpeg image. While, R(i,j), G(i,j) and B(i,j) are the R-, G- and B-color component of the input jpeg image. The R-, G- and B-color component can be extracted by converting the RGB or jpeg image into index image format.

RGB Image

Gray Image

IV. Image Decomposition using Haar Wavelet

In this approach, the images are decomposed using the haar wavelet in four sub-bands namely LL, LH, HL and HH sub-bands. The LL sub-band contains the maximum energy/entropy i.e. maximum information part, however, other sub-bands contains the information about the high frequency components like edges, sharp changes etc.

For the image decomposition and feature extraction the Haar transform has been applied as a basic tool used in the wavelet transform. The method described is used for description of the whole system enabling perfect image reconstruction. The proposed algorithm of the Haar wavelet image decomposition includes image feature based segmentation and comparison of results with the watershed transform. Individual methods have been verified for simulated images and then applied for processing of selected magnetic resonance biomedical images.

In 2-dimensions x and y become 2x2 matrices. We can transform at first the columns of x, by pre-multiplying by T, and then the rows of the result by post-multiplying by TT to find y = T x TT and in the next step x = TT y T

To show more clearly what is happening we can use a specific matrix x of the following form:

$$x = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Implying that

$$y = \frac{1}{\sqrt{2}} \begin{bmatrix} a+b+c+d & a-b+c-d \\ a+b-c-d & a-b-c+d \end{bmatrix}$$

These operations correspond to the following filtering processes:

Top left: 2-D low pass filter (Lo-Lo).
Top right: horizontal high pass and vertical low pass filter (Hi-Lo).
Lower left: horizontal low pass and vertical high pass filter (Lo-Hi).
Lower right: 2-D high pass filter (Hi-Hi).
To apply this transform to a complete image, we group the pixels into 2 × 2 blocks and apply Eqn. (1) to each block.
The energies of all four sub-band images have following %values:

Lo − Lo	Hi − Lo
88.2%	4.0%
Lo − Hi	Hi − Hi
6.3%	1.5%

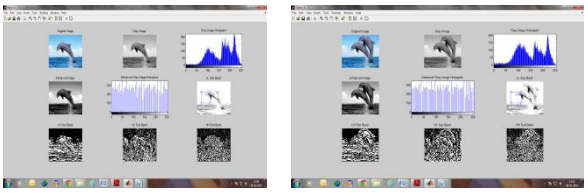
The wavelet coefficients are arranged as follows:

$$Coeff. = \begin{bmatrix} c_a & c_h \\ c_v & c_d \end{bmatrix}$$

After that a B×B block is slided over the resulting image and image is scanned from the upper left corner to the lower right corner. The DWT transform is calculated, For each block ,the DWT coefficients are stored as one row in the matrix A. The matrix will have (M-B+1)x(N–B+1) rows and B×B columns, where M and N represents number of rows and columns of input image respectively.

V. Lexicographically Sorting of Coefficients

In this step lexicographic sorting is performed on the rows of matrix A. Now, in place of comparison of the pixel representation DWT coefficients for each block are being compared, if two consecutive rows of the sorted matrix A are found, the algorithm stores the positions of the identical blocks in a separate list B and increments a shift-vector counter C. To identify the segments that might have been copied and moved, the matching blocks that contributed to that specific normalized shift vectors are colored with the same color. Thus the threshold value T is related to the size of the smallest segment that can be recognized by the algorithm.

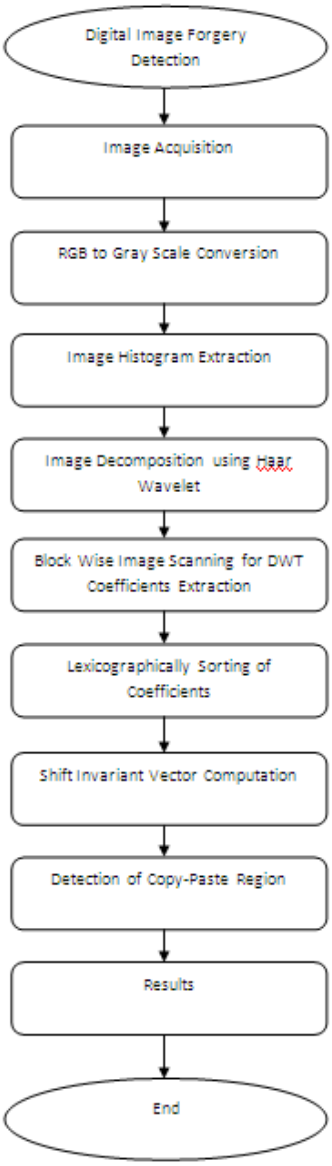


VI. Results

In the below test we took original photograph of two whale fishes together as a benchmark, now we have removed one of the fish that is considered to be forged image. To get the accurate results we will compare the parameters of the original image and forged image. If there is a change in the parameter values than we can say that there must be some amount of tempering on the image or either the image is forged.

Table 1 - Parameters for original and forged image

Sr. No.	Parameters	Image1	Image 2
1.	Contrast	1.27	0.93
2.	Correlation	0.86	0.89
3.	Energy	0.06	0.07
4.	Homogeneity	0.78	0.83
5.	Entropy	5.98	7.48
6.	Mean Intensity	0.50	0.50
7.	Threshold	0.50	0.50
8.	Mean – R	116.05	122.82
9.	Mean - G	158.78	172.53
10.	Mean - B	194.52	209.88
11.	Standard Deviation - R	11.22	10.63
12.	Standard Deviation - G	5.26	4.91
13.	Standard Deviation - B	11.78	10.56



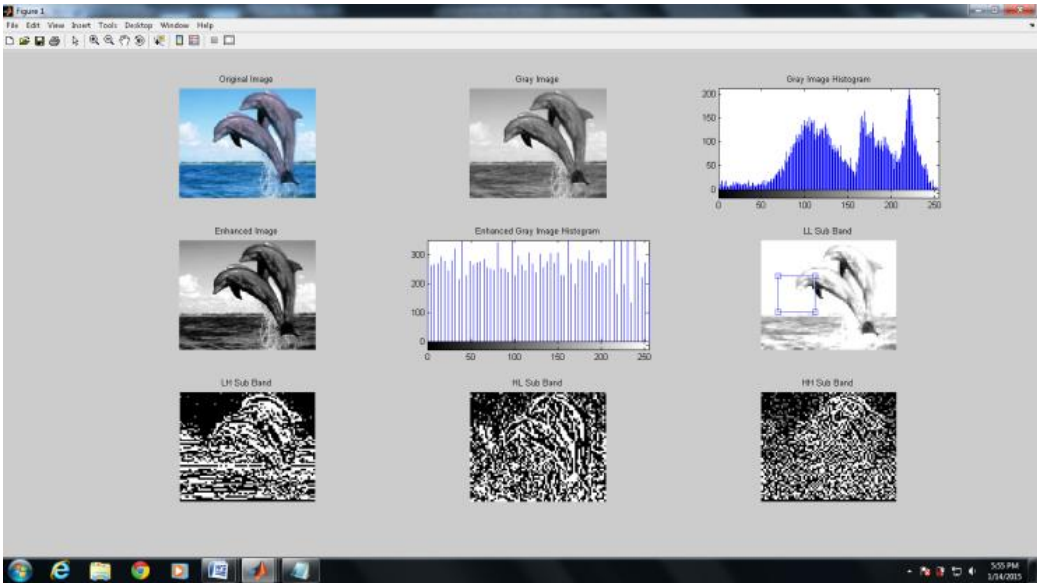


Figure 1
File Edit View Insert Tools Desktop Window Help
Original Image
Gray Image
Gray Image Histogram
Enhanced Image
Enhanced Gray Image Histogram
LL Sub Band
LH Sub Band
HL Sub Band
HH Sub Band

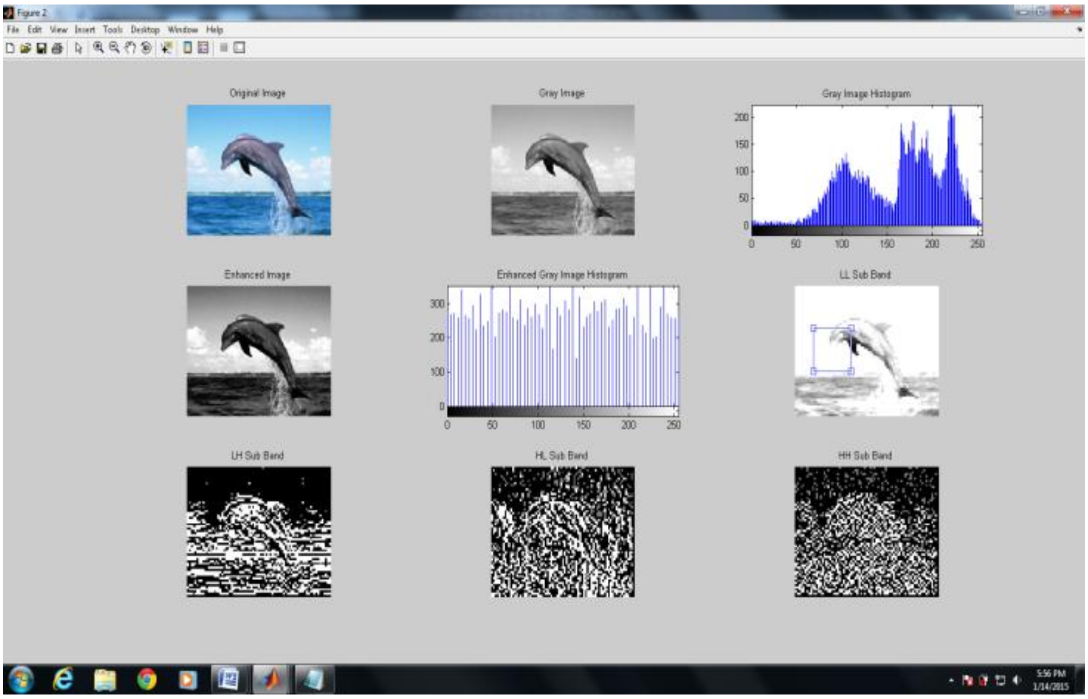


Figure 2
File Edit View Insert Tools Desktop Window Help
Original Image
Gray Image
Gray Image Histogram
Enhanced Image
Enhanced Gray Image Histogram
LL Sub Band
LH Sub Band
HL Sub Band
HH Sub Band

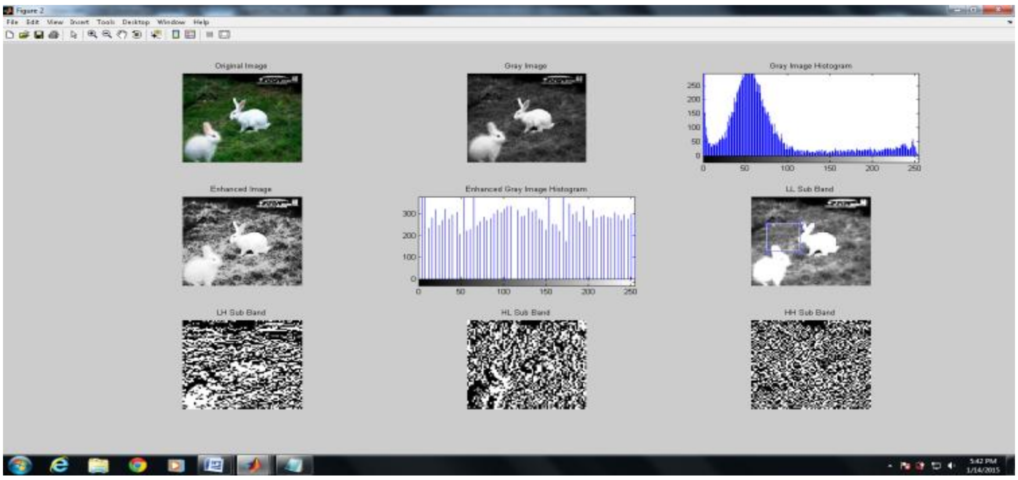


Figure 2
Original Image
Gray Image
Gray Image Histogram
Enhanced Image
Enhanced Gray Image Histogram
LL Sub Band
LH Sub Band
HL Sub Band
HH Sub Band

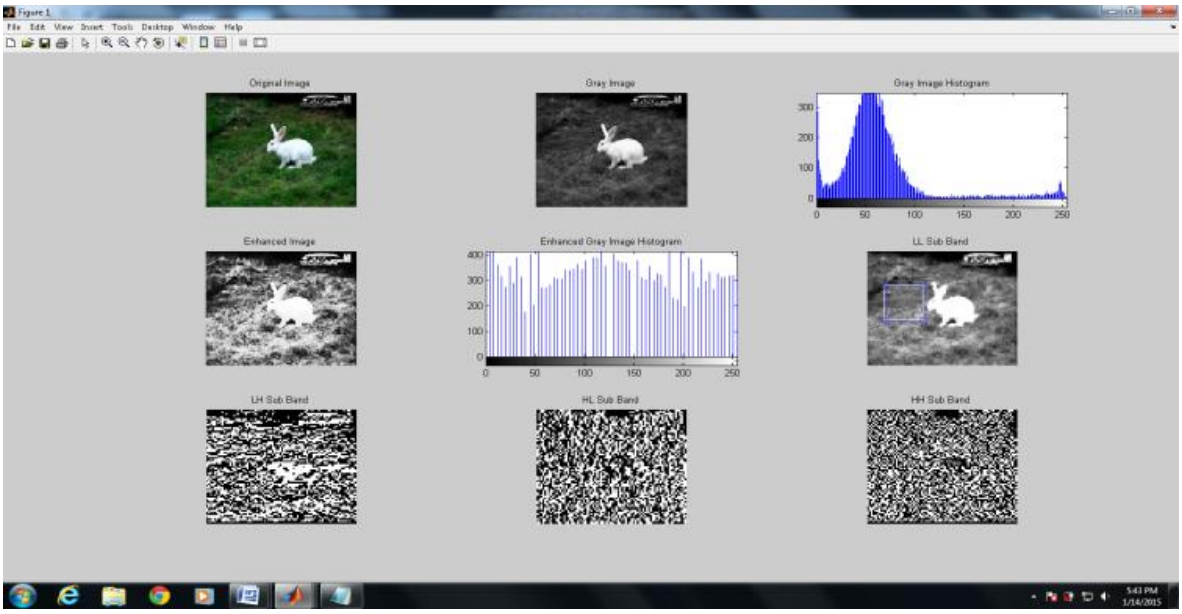


Table -2 Parameters for original and forged image

Sr. No.	Parameters	Image1	Image 2
1.	Contrast	2.90	2.38
2.	Correlation	0.67	0.73
3.	Energy	0.03	0.04
4.	Homogeneity	0.62	0.65
5.	Entropy	5.88	7.14
6.	Mean Intensity	0.50	0.50
7.	Threshold	0.49	0.50
8.	Mean – R	48.67	60.44
9.	Mean - G	75.30	84.49
10.	Mean - B	41.31	55.13
11.	Standard Deviation - R	22.54	22.26
12.	Standard Deviation - G	19.65	18.64
13.	Standard Deviation - B	28.07	26.97

VII. Conclusion

The proposed algorithm has been tested on different image section by just making copy – paste exercises. The algorithm is quite capable of e=identifying the copy paste area in the input image and extent of the forgery i.e. pasted part is computed by taking the ration of pasted area to that of the entire image area. This gives the penetration or degree of forgery or degree of tampering in the input image. In order to validate the results, the input image is verified by its original content so that when the algorithm is applied on unknown images, the results could be authentic

References

[1]. Xin Wang, Bo Xuan, Si-long Peng "Digital image forgery detection based on the consistency of defocus blur", 978-0-7695-3278-3/08 $25.00 © 2008 IEEE

[2]. Jing Zhang, Zhanlei Feng Yuting Su, "A New Approach for Detecting Copy-Move Forgery in Digital Images", 1-4244-2424-5/08/$20.00 ©2008 IEEE

[3]. Wang Zhongmei1, 2, Long Yonghong1, "Digital image forgeries detection based on blocking artifact", 978-1-4244-8886-5/10/$26.00 ©2010 IEEE

[4]. Hieu Cuong Nguyen and Stefan Katzenbeisser, "Detection of copy-move forgery in digital images using Radon transformation and phase correlation", 2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing

[5]. Tiago José de Carvalho, Student Member, IEEE, Christian Riess, Associate Member, IEEE, "Exposing Digital Image Forgeries by Illumination Color Classification", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 7, JULY 2013

[6]. Gang Cao, Yao Zhao, Senior Member, IEEE, Rongrong Ni, Member, IEEE, and Xuelong Li, Fellow, IEEE, "Contrast Enhancement-Based Forensics in Digital Images", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 3, MARCH 2014

[7]. Hrudya P, Lekha S. Nair, Adithya S.M, Reshma Unni,Vishnu Priya H, Prabaharan Poornachandran, "Digital Image Forgery Detection on Artificially Blurred Images", IEEE, 2012, pp 1-5

[8]. Archana V Mire, Dr. S. B. Dhok, Dr P. D. Porey and Dr N. J. Mistry, "Digital Forensic of JPEG Images", 2014 Fifth International Conference on Signals and Image Processing

[9]. M. Ali Qureshi, M.Deriche, "A Review on Copy Move Image Forgery Detection Techniques", 978-1-4799-3866-7/14/$31.00 ©2014 IEEE

[10]. Seniha Ketenci I, Guzin Ulutas 2, Mustafa Ulutas, "Detection of Duplicated Regions in Images Using ID-Fourier Transform", , lWSSIP 2014, 21st International Conference on Systems, Signals and Image Processing, 12-15 May 2014, Dubrovnik, Croatia

Author's Profile

[1]The author is pursuing her M.Tech. (ECE) thesis work in DIP from DIET, Kharar, Mohalai (Punjab). Her field of interest is in DIP based system integration.