Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Copy-Move Image Forgery Detection Using Transform Domain

Rutuja Tendulkar, Associate Prof. Manoj Sabnis
Department of Information Technology,
V.E.S.I.T, Chembur, Mumbai University
Maharashtra, India

Abstract*— Digital image forgery is the process of modifying contents of an image after it leaves its capturing device. Now a day's digital image plays an important role in the world of technology used in the fields of medical, court of law, education, agricultural, etc. New technologies in the market introduce powerful image processing and editing software that are easily allowing people to edit digital images and present the edited copy as the true copy. These changes made in the image contents are undetectable by human eye. Due to this authentication of an image received from communication network is a challenging as well as a necessary task. Copy-move forgery is common type of digital image forgery where a region from the image is copied and pasted in the same image at different location. This paper proposes an algorithm to find copy-move forgery using transform domain. It applies Discrete Wavelet Transform (DWT) and Fast Fourier Transform (FFT) on a forged image to find matching blocks. With the help of border pixel variation technique, it finds the original and forged block from the detected matching blocks. This algorithm increases the accuracy of forged region detection and reduces computational complexity of detection process.

***Keywords*— Digital Image Forgery, Forgery Detection, Transform Domain, Phase Correlation, Noise Variation**

I. INTRODUCTION

Digital image forgery is the process of modifying contents of an image after it leaves its capturing device. Due to the availability of powerful image processing and editing software, it is easy to manipulate and edit digital images. A digital forgery takes place either to hide some contents of the image or to add some contents into the image. These changes made in the image contents are undetectable by human eye. Authenticity of an image received on communication network is important as digital images are accepted as evidence into court of law, in medical fields, in educational field, in agriculture field, etc.

Types of Image Forgery: - There are basically three types of digital image forgery. It includes image enhancing or retouching, image composition/splicing and image copy-move forgery [1] [6].

1. ***Image enhancing or retouching Forgery***: - It is less harmful kind of digital image forgery. It does not significantly change an image but enhances or reduces certain features of an image. One can enhance certain features of an image to make it more attractive but it is ethically wrong.

   Figure 1 shows an original image of lady's face whereas figure 2 shows the same face with enhanced effects applied to it


Fig 1: Original Image


Fig 2: Enhanced Image

2. ***Image composition or splicing Forgery***: - It is a technique that involves a composite of two or more images to create a fake image. Regions from various images are combined together in base image is known as image composition.

   Figure 3 shows a base image. Figure 4 shows shark inside sea. From figure 4 region occupied by shark is copied and it is pasted below the helicopter in the base image. This copy-paste operation from one image into another image forms a spliced image as shown in figure 5.


Fig 3: Base Image


Fig 4: Shark image


Fig 5: Base image with shark

3. ***Image copy-move forgery***: - It is a technique that copy background or other features from one part of the image and paste into the same image at another location to hide or alter regions from the image. In this type, instead of having an external image as the source, it uses portion of the original base image as its source. Part of the original image is copied and moved to desired location and pasted into it.
   Figure 6 shows original image of a garden view. In figure 7 a region occupied by a deer is copied and pasted on the grass at front side in the same view.


Fig 6: Original Image Fig 7: Forged Image

The copy-move forgery is one of the difficult forgeries to detect in image processing. It is common image tampering technique used now a day. In this some part of the image needs to be covered to add or remove information of an image [1] [4] [6].
There are two approaches for detecting digital image forgery. One is active approach and the other is passive approach [1] [4] [6].

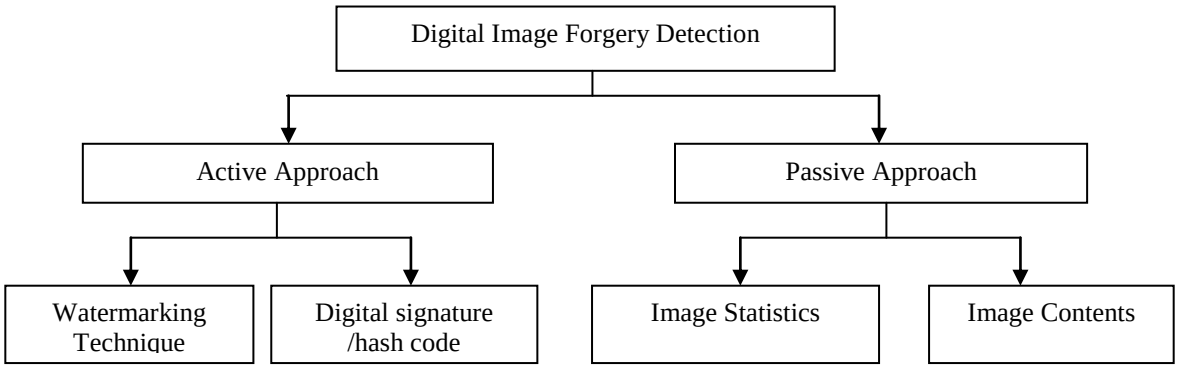


Figure 8: Digital Image Detection Approaches

Active approach requires prior information about the image such as watermark or signature embedded inside the original digital image at the time of recording of original image. **Passive approach** does not require explicit prior information about the image. This approach deals with image contents and its statistics.
In passive approach forgery can be detected using **spatial domain or transform domain [9]**. Spatial domain techniques directly deal with the image pixels. The value of the pixels of the image changes with respect to scene. Spatial domain techniques like the logarithmic transforms, power law transforms, histogram equalization, are based on the direct manipulation of the pixels in the image. In transform domain signal can be converted from time domain into frequency domain using mathematical operators. In this domain we analyse signal with respect to frequency. In frequency domain, we deal with the rate at which the pixel values are changing in spatial domain. Transform domain is better than spatial domain with respect to efficiency and computational speed as it reduces the size of the input image and rather than comparing the entire pixels of the blocks, only few features are compared [1].

II. RELATED WORK

There are several techniques proposed by various authors to detect image forgery in the literature of image forensics. In active approach, watermarking and signature must be inserted either at the time of recording the image , or later after further processing by a person authorized to do so. This embedding of data requires specially equipped cameras or subsequent processing of the original image [1-2, 5].Due to this, passive techniques can be used to detect digital image forgery when watermarking and signature is not embedded inside an image. A passive approach includes set of image forensic tool that are divided into five categories based on pixel, format, camera, physics and geometry [2] [6] [10]. Pixel based techniques that detect statistical anomalies introduced at the pixel level. Format based techniques that focus on the statistical correlation introduced by a specific lossy compression scheme. Camera based techniques that exploit artifacts introduced by camera lens, sensors and on chip post-processing. Physics based techniques that explicitly model and detects anomalies in three dimensional interactions between physical objects, light and the camera. Geometric based techniques that make measurements of objects in the world and their positions relative to the camera.
Authors of [3] proposed an algorithm to detect the forgery based on Scale Invariant Feature Transform (SIFT).SIFT detects local invariant features of image, then searches the matched feature points by SIFT feature matching. If the number of matched points is larger than the assumed threshold value, then it considers that the image has been forged.

Authors of [4] proposed an algorithm based on DCT. It accepts an input image and converts it to gray scale. Then it applies DCT on the image to find the intensity of that image and stores the intensity levels in a separate matrix. Then it divides an image into block size of 16×16.By applying SIFT feature extraction on each block, it extracts features from the input image. Then the algorithm stores extracted feature vector in the matrix and sorts it lexicographically. Then it applies quantization to assign some values to array and saves the coordinate values. Based on the similarity measures it identifies outlier and then compares with the set threshold value. At the end it performs matching and localization of forged regions.

Authors of [5] proposed an algorithm based on DWT-PCA (EVD-Eigen Value Decomposition) technique. This algorithm takes a gray scale input image and applies DWT on it. Proposed algorithm slides a b^2 window over the low frequency sub band and computes blocks. Then it performs PCA-EVD on each of the block to reduce vector length and generates a new matrix. Then algorithm sorts the matrix and each pair of adjacent rows of the new matrix is used to compute shift vector. Then by using morphological operations it computes final result.

Authors of [6] proposed an algorithm based on DWT and median filtering. First it applies DWT to the input image. Then median filtering is applied to DWT output. This will set each output pixel to an average of the pixel values in the neighbourhood of the corresponding input pixel. Then it divides the processed image of DWT and median filtering into overlapping blocks. Overlapping block pixels are used to form a new matrix. Then it sorts new matrix to arrange similar rows adjacent to each other. By applying pixel matching technique the algorithm finds copy move region.

Authors of [11] proposed two algorithms based on block level techniques. First algorithm applies DWT to the input image and works with LL sub band. It divides the image into sub images. Then the algorithm computes phase correlation to find spatial offset between the copy-move regions. With pixel matching technique it locates the forged region. Second algorithm works with block division and intensity values. By using average intensity function algorithm calculates average intensity. Then by using ratios of average intensities, differences of average intensities and shift vectors the algorithm detects copy move forgery.

Authors of [7] [13] proposed an algorithm based on DCT. It accepts input forged image and divides it into 8×8 fixed size blocks.DCT is applied to each block to generate the quantized coefficients. It represents each quantized block by a circle block and by dividing it into four parts it extracts features from each circle block. The algorithm arranges extracted feature vector in the matrix and sorts it lexicographically. Similar blocks are searched using Euclidean distance between adjacent pairs of sorted matrix. Then the algorithm applies morphological operations to display matching regions from the image.

Authors of [8] proposed an algorithm based on DWT. It accepts an input image and converts it into a gray scale image. Then apply DWT to the input image. The LL sub band image is used and it slides over B×B block while image scanning from upper left corner to the lower right corner. Then the algorithm calculates DWT and each block's DWT coefficients it stores into the new matrix as one row. It sorts the matrix lexicographically. Then it calculates shift vector for suspected pair of blocks and then the proposed algorithm performs block matching and detects the similar blocks from the image.

Most of the existing systems used to detect digital image forgery, search for similar regions in the forged image. The proposed algorithm works with Discrete Wavelet Transform along with Fast Fourier Transform to find similar regions from the image. It uses Block based method that works on frequency for detecting forgery [12]. Use of DWT and FFT will reduce the time complexity of the algorithm. After finding similar regions proposed algorithm will differentiate between the two regions using border pixel variation technique. It will show original and forged region from the image.

III. PROPOSED SYSTEM

The proposed system is based on Discrete Wavelet Transform (DWT). Discrete Wavelet Transform is used to reduce the size of .the image at each level. At each level, the image is decomposed into four sub images. The sub images are labelled as LL, LH, HL and HH.LL image is used for further decomposition. These sub images can be combined together to restore the original image.DWT performs iterative comparisons of matching blocks. The proposed system also uses Fourier Transform to calculate FFT coefficients and complex conjugate of an image to find phase correlation between two blocks. The phase correlation presents correlation matching between the two images in the frequency domain. The Phase Correlation method is proposed for the registration of translated images, which is based on the Fourier Shift property. It transforms shift as phase difference in the Fourier domain.FFT gives accurate correlation as compared to cross correlation [14]. By applying DWT and FFT similar blocks from the image are detected. To find forged block from the two matching blocks, border pixel variation is calculated. The difference between each pixel of the border and its eight neighbouring pixels is calculated. Then maximum difference from the eight differences is calculated and border variance is plotted on the image. The region having maximum variation in the border is considered as forged block.

A. Proposed Algorithm

Step 1: Read the input image. If the input image is not a gray scale image then convert it into a gray scale image.

Step 2: Find decomposition levels required for an input image based on image size and apply on the gray scale image.

Step 3: DWT is applied to the input image. Divide the LL sub band image into block of 8×8 size from the upper left corner to the lower right corner. The DWT coefficients of each block are stored in matrix X where it contains (M-B+1) × (N–B+1) rows and B×B columns (64), Where M and N represents number of rows and columns of input image respectively.

Step 4: Sort matrix X so that similar rows will be placed adjacent to each other.

Step 5: Apply Fourier Transform to each row and its adjacent row from sorted matrix X. Each row from matrix X represents 8×8 block size image. Calculate complex conjugate of adjacent row. Calculate Fourier Transform (FT) with following formula and find inverse Fourier transform of (FT) to get phase correlation (PC) between two rows:

$$FT = \frac{F(row1) \times conj(F(row2))}{|F(row1) \times conj(F(row2))|}$$

Step 6: Set threshold value to compare computed phase correlation between two rows in step 5.Compare value of phase correlation (PC) with the threshold value to find similar blocks and then plot the matching blocks in the input image.

Step 7: Compute connected components for matching blocks displayed on the image. Find upper left and lower right corners of each block and calculate the boundary coordinates for matching blocks.

Step 8: Perform dilation and erosion operations on the matching blocks to plot the borders of the matching regions from the input image.

Step 9: From the boundary region, read each pixel with its surrounding pixels. Calculate difference between a pixel and it's each surrounding pixel. Consider p is the pixel and its eight surrounding pixels are p1… p8.Then calculate difference between p and p1,p and p2 and so on up to p and p8.Find the maximum difference value from eight difference values to calculate border variation of each pixel with its neighbouring pixels.

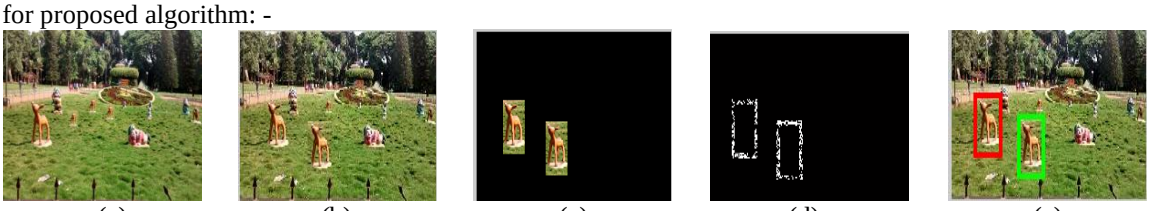
Step 10: From step 9, extract maximum difference from eight differences for each pixel of border and plot the pixel variation border of matching blocks. From both the blocks find a block with maximum border variation.

Step 11: Display final result showing original region and forged region in two different colours. Maximum variation in border indicates forged block with green colour and original with red colour.

IV. IMPLEMENTATION AND RESULT

Proposed algorithm accepts an input image of size 134×240 as shown in figure 9(b). If the image is colour, it is converted into gray scale form. Then DWT is applied to the input image and LL sub band image is used for further processing. But the accepted image is of less size so the image taken as it without applying DWT for further processing. The input image is divided into block size of 8× 8. The DWT coefficients of each block are stored in matrix X where it contains (M-B+1) × (N–B+1) i.e. 29591 rows and B×B i.e. 64 columns. Matrix X is then sorted to place similar rows adjacent to each other. Then Fourier Transform is applied to each row and its adjacent row from sorted matrix X. Then complex conjugate of adjacent row and FT is calculated. Inverse Fourier transform of FT gives phase correlation between two rows i.e. PC. Threshold value is set. Maximum value of phase correlation is compared with the threshold value to find matching blocks. Then matching blocks are plotted on the image as shown in figure 9(c) below. From the matching blocks their border is extracted. From the boundary region, each pixel value with its surrounding pixels value is extracted. Then difference between a pixel and it's each surrounding pixel is calculated. Consider p is the pixel and its eight surrounding pixels are p1… p8.Then we calculate difference between p and p1,p and p2 and so on up to p and p8. Then the algorithm computes the maximum difference value from eight values, to calculate border variation of each pixel with its neighbouring pixels. With the use of filter we have plotted the border variation of both the blocks on the image as shown in figure 9(d) below. Then the block with maximum variation is declared as forged and with minimum variation is declared as original region. The result of the algorithm shows original region with red colour border and forged region with green colour border as shown in figure 9(e) below.

Output for proposed algorithm: -



(a) (b) (c) (d) (e)

Figure 9: (a) original image. (b) Forged Image with one more Deer on the front side. (c) Image showing matching blocks i.e copy-move blocks. (d) Image showing border variation of two matching blocks. (e) Image showing original block in red color and forged block in green color.

V. CONCLUSIONS

The proposed system is based on Discrete Wavelet Transform (DWT), Fast Fourier Transform (FFT) and pixel variance technique. Due to use of DWT, image size is reduced and block matching is done with good speed. Proposed method gives exact location of copy-move forgery done in an image. It works well with .jpg as well as .png images. As compared to existing methods proposed system takes less time to locate exact forged area. It also detects small regions of copy move forgery in less time.

The future work includes detecting digital image forgery when the copied region is processed before pasting into the same image.

REFERENCES

[1] Tanzeela Qazi, Khizar Hayat, Samee U. Khan, Sajjad A. Madani, Imran A. Khan, Jonna Kolodziej, Hongxiang Li, Weiyao Lin, Kin Choong Yow, Cheng-Zhong Xu, *Survey on blind image forgery detection*, published in IET Image processing,Vol. 7,Iss. 7,2013

[2] Hany Farid, *Image Forgery Detection A survey*, IEEE Signal Processing Magazine, March 2009

[3] Li Jing and Chao Shao, *Image Copy-Move Forgery Detecting Based on Local Invariant Feature*, Journal of Multimedia,Vol 7,No 1,February 2012

[4] Ruchita Singh, Ashish Oberoi, Nishi Goel, *Copy Move Forgery Detection on Digital Images, International Journal of Computer Applications*, volume 98-No.9,July 2014.

[5] Michael Zimba,Sun Xingming, *DWT-PCA(EVD) Based Copy-Move Image Forgery Detection*, International Journal of Digital Content Technology and its Applications, Volume 5,Number 1,January 2011

[6] Ms. P.G. Gomase,Ms. N.R.Wankhade, *Advanced Digital Image Forgery Detection :A Review*, IOSR Journal of Computer Science(IOSR-JCE) e-ISSN:2278-0661,p-ISSN:2278-8727

[7] Yanjun Cao,Tiegang Gao,Li Fan,Qunting Yang, *A robust detection algorithm for copy-move forgery in digital images*, Forensic Science International 214 ,August 2011

[8] Preeti Yadav ,Yogesh Rathore , *Detection of Copy-Move Forgery of Images Using Discrete Wavelet Transform*, International Journal on Computer Science and Engineering (IJCSE)

[9] Snehal O. Mundhada,V.K.Shandilya ,*Spatial and Transformation Domain Techniques for Image Enhancement*, International Journal of Engineering Science and Innovative Technology(IJESIT) ,vol 1,issue 2,November 2012

[10] Mohd Dilshad Ansari,S.P.Ghrera,Vipin Tyagi, *Pixel Based Image Forgery Detection: A Review*, IETE Journal of Education,vol 55,no 1,Jan-Jun 2014

[11] Pradyumna Deshpande,Prashasti Kanikar, *Pixel Based Digital Forgery Detection Techniques*, International Journal of Engineering Research and Application (IJERA),Vol 2,Issue 3,2012

[12] Vincent Christlein,Christian Riess,Johannes Jordan,Corinna Riess,Elli Angelopoulou ,*An Evaluation of Popular Copy-Move Forgery Detection Approaches*, IEEE transactions on Information Forensics and security,vol 7,no 6,2012

[13] Rohini A. Maind,Alka Khade,D.K.Chitre ,*Image Copy Move Forgery Detection using Block Representing Method*, International Journal of Soft Computing and Engineering (IJSCE),Vol 4,issue-2,May 2014,ISSN:2231-2307

[14] Ping Lu, *Rotation Invariant Registration of 2D Aerial Images Using Local Phase Correlation*, IT 13 030 Examensarbete 30 hp Maj 2013, PDF Article

