FORGERY DETECTION IN DIGITAL IMAGE

Neeta R. Kadam and D. G. Bhalke
Rajarshi Shahu College of Engineering, Pune University, Pune, India

ABSTRACT

Due to availability of many image editing and processing tools, it is possible to easily change the information represented by a digital image without leaving any obvious traces of tampering. Tampering of digital images has become so easy that it is raises question about integrity/authenticity of digital image, so there is a need of a robust and reliable forgery detection method. A specific type of forgery in digital image is known as copy move forgery detection. This is done by copying a block of an image and pasting it on to some other block of the same image. This approach is based on the application of wavelet transform. To achieve this, first apply wavelet transform to the input image then reduced dimensions of image is divided into overlapping block of fixed size and duplicated blocks are identified using phase correlation.

KEYWORDS: *Copy Move Forgery, DWT, Phase Correlation*

I. INTRODUCTION

Images play a vital role in the forensic laboratory, as images are used to document any crime scene evidences. When these images are produced as evidences in courtrooms, integrity of images is very important. Image forgery has become a threat after the advent of the digital medium. Earlier, when analog images were used, tampering the images was very difficult to perform.

Image Forgery is the process of making an illegal modification or reproduction of an image information. Digital images can be modified or edited or forged in many possible ways. There are many algorithms or techniques for detecting tampered image. In general, these techniques can be divided into two major groups; Active Method and Passive Method. Active methods related to pre-processing concept. Examples of these methods are watermarking and digital signature. These methods work only when we have some prior information about the image. Hence such a method does not work when handling images from unknown or unreliable sources. There is a very low probability that images used in forensics like crime scene images, photographs of criminals, fingerprint images etc will be secured by digital watermarks or digital signatures. Hence, Passive techniques are the best approach to detect tampering in images.

Passive method does not require any prior information about the image. To detect the traces of tampering, passive methods use the image function and the fact that forgeries can bring into the image specific detectable changes. Most common approaches of tampering are listed below.[3]

1.1 Splicing: It is a method of tampering images by combining two sources to produce a new image which retains the majority of one image for detail.

1.2 Image Retouching: Image Retouching is done in most of the magazine covers to give images with a poor quality an enhanced appeal by changing the background, or by making changes in the hue of the picture to give a better feel to the picture.

1.3 Geometrical Transformation: Some images have a portion of the picture altered by some common geometric transformations such as translation, scaling and rotation. Forgers make a copy of the portion of the picture; make changes to it by geometrically modifying that portion of the image

1.4 Copy Move Attack: A copy move attack is commonly used to conceal parts of an image or to remove unwanted portions in an image. A portion from the picture is copied and pasted over any unwanted portion in the same image.

To make the computation quicker, J. Fridrich, David Soukal and Jan Lukas [2] suggested an effective blocking approach, in which the image blocks are represented by quantized DCT (Discrete Cosine Transform) coefficients, and a lexicographic sort is adopted to detect the Copy-Move blocks. Guohui Li,Qiong Wu, Dan Tu and Shaojie Sun[6] developed a sorted neighbourhood method based on DWT (Discrete Wavelet Transform) and SVD (Singular Value Decomposition). The DWT and SVD method suffers from the drawback that the computation of SVD takes lot of time and it is computationally complex. Irene Amerini, Ballan Caldelli, Bimbo, Serra [1] introduced a SIFT based forensic method for copy move attack detection and transformation recovery. SIFT (Scale Invariant Features Transform) used for image features extraction and matching. M. K. Bashar, N. Ohnishi and K. Mori [4] suggested a method for detecting forgery in the presence of flip and rotation. The method has been applied with PCA, KPCA and wavelet transformed images. Among these techniques i.e. PCA, KPCA and wavelet based against rotation, horizontal flips, and vertical flips, KPCA gives good result but time consuming and higher computational complexity.
This paper proposes 'wavelet based approach' to detect the copy move forgery. The organization of a paper as follows. Detection method explained in detail in section II. Results of the experiment are explained in section III. Finally, we concluded in section IV and section V briefs Future Work plan.

II. COPY MOVE FORGERY DETECTION IN DIGITAL IMAGE

Copy-move forgery is a specific type of image tampering where a part of the image is copied and pasted somewhere else in the image. Because the copied parts come from the same image, its color palette, dynamic range, and most other important properties will be compatible with the rest of the image and thus the forgery is widely used in digital image forgery.
Implementation of Copy Move forgery detection in digital image using wavelet transform is a context of this discussion. Now to find the any image is authenticate or not using proposed algorithm. So we start with an input image of size M×N having number of pixels.

2.1 ALGORITHM FOR DETECTION OF COPY MOVE FORGERY

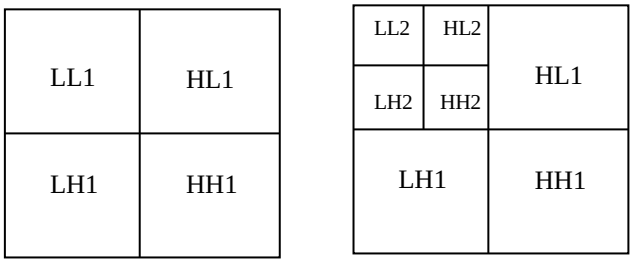
1. Read the image chosen by user.
2. If the input image is not gray scale then first convert it into gray scale image.
3. Apply wavelet transform depending upon size of image up to specified level 'L' to the gray image.
4. Initialize variables used in implementation:
   - M x N :- size of image.
   - b : - Number of pixels per block.
   - LLL:- DWT Levels
5. LLL part of DWT is used for further processing. Decide the block size b x b. Convert each overlapping b x b block in the LLL image into row matrix and store it into Matrix A. Now Matrix A contents b x b column and (M-b+1) x (N-b+1) rows.
6. Another Matrix named B is having size (b x b) +2 for columns and (M-b+1) x (N-b+1) for rows. It contents all values of Matrix A and its location values.
7. Now rows of Matrix B are sorted lexicographically.
8. For each row of matrix B computes the phase correlation for the below and above rows. If phase correlation calculation result is 'above and equal' to threshold value then these rows are indicated on particular LLL level with converted into b x b blocks.
9. End

2.2 DISCRETE WAVELET TRANSFORM

One of the most popular application of discrete wavelet transform is image compression. The basic idea of the discrete wavelet transform is to reduce the size of the image at each level. Images are two dimensional signals so there is one approach to the subband decomposition of two dimensional signals using separable transforms that can be implemented using one dimensional filters on the rows first and then on the columns(or vice versa). A image of size NxM , filter each row and down sample to obtain two NxM/2 images. Then filter each column and subsample the filter output to obtain four

N/2 x M/2 images. Of the four subimages, the one obtained by low pass filtering the rows and columns is referred as the LL image; the one obtained by low pass filtering the rows and high pass filtering the columns is referred to as the LH image; the one obtained by high pass filtering the rows and low pass filtering the columns is called the HL image; and the sub image obtained by high pass filtering the rows and columns is referred to as the HH image.
Fig.1 shows the decomposition at the first and second level. The sub-images are labelled LL, LH, HL and HH. LL corresponds to the coarse level coefficients or the approximation image. This image is used for further decomposition. LH, HL and HH correspond to the vertical, horizontal and diagonal components of the image respectively. If the number of levels used for decomposition is 'L', then the matching is performed on the LLL image. If any matches present in LLL level, resulted the forgery image.

.



(a) First Level (b) Second Level

Fig. 1 Image Decomposition

2.3 PHASE CORRELATION

The phase correlation method (PCM) is a popular Fourier domain method to register two images. It computes a phase difference map that (ideally) contains a single peak. The location of the peak is proportional to the relative translation between the two images. The PCM is resilient to noise and image defects and is readily automated. It is completely equivalent to correlation in the spatial domain, but the calculation is orders of magnitude faster in the Fourier domain. The mathematical details are as follows:
The ratio R between two images 'img1' and 'img2' is calculated as follows [8]:

$$R = \frac{F(img1) * conj(F(img2))}{|F(img1) * conj(F(img2))|} \quad (1)$$

where 'F' is the fourier transform, and 'conj' is the complex conjugate. The inverse Fourier transform of 'R' is the phase correlation ρ

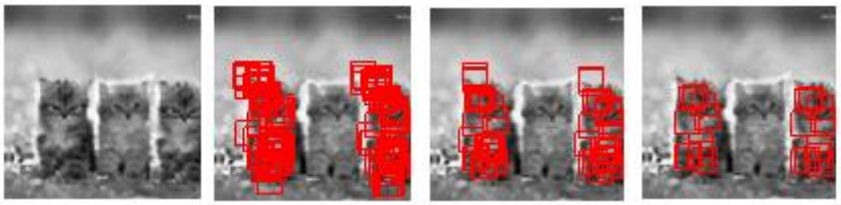
III. EXPERIMENTAL RESULT

In our experiments we have tampered several internet downloaded images by copying one part of image and paste it on same image only. Our data set consist of 50 images out of which, 25 images are forged by using copy move technique and other 25 images are authentic images. Sizes of images are 128 x 128, 256 x 256 and 512 x 512. This algorithm detects copy move forgery on these images correctly and efficiently. Shown figure are the output of our detection algorithm. In each representation, the duplicated regions are shown with coloured rectangles. DWT is applied for reducing the computational part of algorithm depending upon size of image. We applied the procedure for different images to get the output. The outputs of birds images are shown in Fig.2.

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

Figure 2. Copy Move Forgery Detection Result (a) Original image (b) Tampered image (c) Forgery detection result (d) Copied and forged area

Effect of the phase correlation results of different threshold values and detected results over tampered cat's image are shown in Fig 3.



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

Figure 3. Phase correlation result using different threshold value (a) tampered image (b) detection result when th=0.5 (c) detection result when th=0.7 (d) detection result when th=0.9

Effect of different wavelet filters used in DWT and number of matches found respective wavelet filters shown in Table 1.Here we used various wavelets.

Table 1: Different Wavelet with number of matches

Different Wavelet	Number of matches
Haar or db1	36
4th Order Daubechies	31
Biorthogonal 6.8	55
Jpeg 9.7	30
4th Order Symlets	33

IV. CONCLUSION

In this paper, we used an efficient method to detect copy move forgery of the digital image.
An experimental result proves that the proposed method detects the number of matches between two comparing blocks of the image for the different threshold values. Total number of matches is different for different wavelets means it changes according to wavelet.
Our method reduced computational complexity and the time needed for the detection process, but duplicated regions with rotation and scaled regions cannot be detected.

V. FUTURE WORK

In future, we would like to work find out some mechanism to reduce problems facing while detecting image forgeries using methods discussed in this paper. Further we will work on images where attacker has made detection more difficult by applying noise and JPEG quality level changes.

REFERENCES

[1]. Irene Amerini, Lamberto Ballan,Roberto Caldelli, Alberto Del Bimbo, Giuseppe "A SIFT-based Forensic Method for Copy-Move Attack Detection and Transformation Recovery", " IEEE Transcations on Information Forensics and Security, Vol. 6 No. 3 Sept.2011.
[2]. J. Fridrich, D. Soukal and J. Lukas, "Detection of copy–move forgery in digital images", Proceedings of Digital Forensic Research Workshop, IEEE Computer Society, Cleveland, OH, USA (August 2003), pp. 55–61.
[3]. Granty Regina Elwin J,Aditya T S, Madhu Shankar S "Survey on Passive Methods of Image Tampering Detection' Proceedings of the International Conference on Communication and Computational Intelligence – 2010, Kongu Engineering College, Perundurai, Erode, T.N.,India.27 – 29 December,2010.pp.431-436 .
[4]. M. K. Bashar, K. Noda, N. Ohnishi, K. Mori, "Exploring Duplicated Regions in Natural Images", IEEE Transactions on Image Processing 2010.
[5]. S. Bayram, H. Taha Sencar,N .Memon "An Efficient and robust method for detecting copy move forgery", IEEE International Conferences on Acoustics,Speech and Signal Processing 2009.

[6]. G.Li, Q.Wu, D.Tu, and Shaojie Sun, "A sorted neighbourhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," IEEE International Conference on Multimedia & Expo, 2007.
[7]. Zhang Ting, Wang Rang-ding "Copy-Move Forgery Detection based on SVD in Digital Image" pp 1-5,2nd International Congress on Image and Signal Processing(CISP'09) 2009, Tianjin.
[8]. Saiqa Khan, Arun Kulkarni "Robust Method for Detection of Copy-Move Forgery in Digital Images" 2010 IEEE International Conference on Signal and Image Processing.
[9]. Rafael Gonzalez, Richard Woods, Steven Eddins "Digital Image Processing Using MAT LAB" Second Edition.

AUTHORS

Neeta R. Kadam, secured B.E. degree in Electronics from Shivaji University, Kolhapur in 2002. She is a student of Rajarshi Shahu College of Engineering and pursuing her Master degree in Electronics stream.

Bhalke D.G. received B.E. degree from Aurangabad University and M.E. degrees from the Shivaji University Kolhapur in 1998 and 2005 respectively. He is currently pursuing towards the Ph.D. degree at the National Institute of Technology Warangal, India. He is also with the Rajarshi Shahu College of Engineering, Pune, India, where he is an Assistant Professor in the Department of Electronics and Telecommunication Engineering. His research interests include Speech processing and Music signal Processing. Mr. Bhalke is a life member of Indian Society for Technical Education (ISTE) and Institution of Electronics & Telecommunication Engineers (IETE) society.