An Approach to Detect Image Forgery by Discrete Wavelet Decomposition

Dibakar Raj Pant

Department of Electronics and Computer Engineering, Pulchowk Campus
Institute of Engineering, Tribhuvan University, Nepal
Corresponding author: *drpant@ioe.edu.np*

Abstract: Image forgery or manipulation by using the multimedia technology is becoming a challenging issue. The most common type of image forgery is copy-move forgery where some part of one image is copied and spliced in the other image. In this article, first the images in RGB color space is converted into YCbCr color space and the four-level discrete wavelet transform (DWT) is implemented to detect image forgery. The output of the DWT is further processed by using the image gradient technique for the edge detection of spliced objects. Morphological operation and Wiener filtering are applied for locating the tempered region in the forged image. Sensitivity, specificity and accuracy calculated for spliced images of CASIA datasets are obtained 89%, 86% and 88% respectively.

Key Words: Image forgery, discrete wavelet transform, YCbCr color space

1. Introduction

Image manipulation by using multimedia technology and digital image processing software is growing day by day. Forged images that appeared in magazines, Newspaper, scientific journals and internet are becoming social and ethical issues [5]. It indicates serious vulnerabilities and decreases the credibility of digital images as shown in the Fig. 1. Therefore, Image forgery detection is a demanding and potential research area which aims to detect various image forgery possibilities.

**Fig. 1: Manipulated images appearing in the famous magazines from left to right
Newsweek from March 7, 2005 and New York from July 25, 2005**

The active digital image forgery techniques require preprocessing of image such as watermark embedding or signature generation, which limits their application in practice [6]. The blind techniques also known as the passive techniques do not need any watermark or prior information about images. They depend on the original characteristics of the image [8]. Basically, copy –move, image splicing and image retouching techniques are used for image manipulation [1]. The goal of all these above mentioned techniques is to construct a new concocted image, applying region duplication/swapping to hide/relocate certain objects in the image and applying image editing to remove/add new objects from/into the image. Mathematically this process can be written as given in equation (1).

$$I_s(x, y) = g_o(x, y) + h_{of}(x, y) \qquad\qquad (1)$$

where, $I_s(x, y)$ is spliced or manipulated image, $g_o(x, y)$ and $h_{of}(x, y)$ are the original image and the p art of the original image.

Fig. 2: Example of Image splicing forgery (Taken from CASIA Database) [2]

Source camera identification techniques in the forgery detection explore different processing stages of the digital camera for unique characteristics such as color filter array (CFA) interpolation [4], Chromatic aberration and sensor imperfections [3,7]. These techniques do not work well for compressed and cropped images. The most common type of image forgery is copy move type which is difficult to detect. Sheldon [9] has proposed a simple method of localizing a noise tampered region of a forged image but this method fails to find random noise that could be added across an entire image to conceal image tampering. Other researchers have proposed different methods, Wang et al. [11] introduced passive color image splicing detection, Zhang et al. [12,13] proposed the local binary pattern (LBP), and [11] used the 8x8 block Discrete Cosine Transform (DCT) transform and Shivakumar et al. [8] have applied LBP, wavelet and PCA for the image splicing forgery detection. However, these methods have some demerits such as over fitting and localizing the forged area. Recently, Ujjainiya et al. [10] have proposed the texture feature and clustering for digital forgery detection. However, this method requires both original and forged images.

In this article, the author has implemented four level decomposition of discrete wavelet transformation of the forged images. First, the images in RGB color space is converted into YCbCr color space where (Cb and Cr) components represent chroma and Y is the luminance. The four-level discrete wavelet transform on each color channels trace out the cut-paste

manipulation of objects. In other words, they are higher frequencies and are detected in detail sub-bands, i.e. LH, HL and HH sub-bands of decomposition. The output of the DWT is further processed by using the image gradient technique for the edge detection of spliced objects. Morphological operation and Wiener filtering are applied for locating the tempered region in the forged image.

2. Methods

The block diagram shown in the Fig. 3 illustrates the methods for detecting forged images.

2.1 Image Data Set

Image data are taken from CASIA Tampered Image Detection Evaluation Database Version 1.0 (CASIA TIDE v1.0) [2] and CASIA TIDE v2.0 [2]. It is image dataset designed to evaluate copy-move and image splicing detection methods. Table 4 provides a description of these datasets.

2.2 Color Space

YCbCr color model represents colors in the form of luminance (Y) and chrominance (Cb and Cr) components. In most cases, the tampering traces, are not be detected by the human visual system, because they are hidden in the chromatic channel. Here, RGB images are converted into YCbCr color model. The spliced regions will have sharp edges while the authentic objects in the image will have smooth edges. These spliced edges are more visible in chroma components.
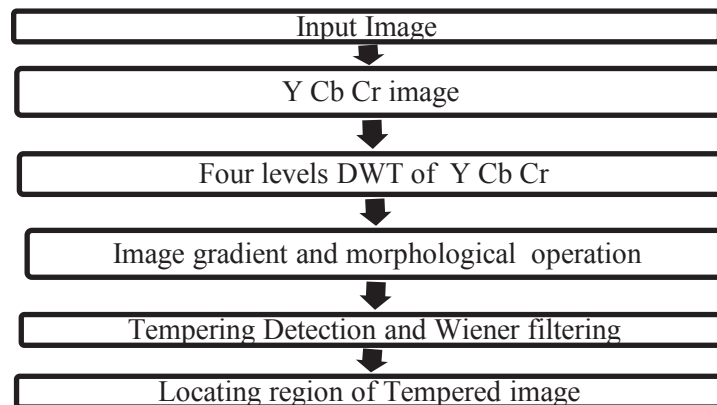
Input Image
↓
Y Cb Cr image
↓
Four levels DWT of Y Cb Cr
↓
Image gradient and morphological operation
↓
Tempering Detection and Wiener filtering
↓
Locating region of Tempered image

Fig. 3: Block diagram of methods for detecting forged images

### 2.3 Four Level Decomposition using Wavelet Transform

A wavelet transform can be used to decompose a signal into component wavelets. Once this is done the coefficients of the wavelets can be decimated to remove some of the details. The discrete wavelet transform (DWT) is an implementation of the wavelet transform using a discrete set of the wavelet scales and translations obeying some defined rules. The DWT of an image $f(x, y)$ of width M pixels and height N pixels is given in the Equation (2).

Table 1: Description of the Evaluated image Data

Dataset	No. of Images			Image Type	Image Size
	Authentic	Tampered	Total		
CASIA v1.0	800	921	1, 721	jpg	384x256 To 256x384
CASIA v2.0	7,491	5,123	12,614	jpg tif bmp	240x160 To 1152x768

$$f(x,y) = \frac{1}{\sqrt{MN}}\sum_m \sum_n W_\varphi(j_o,m,n)\,\varphi_{j_o,m,n}(x,y) + \frac{1}{\sqrt{MN}}\sum_{i=H,V,B}\sum_{j=j_o}^{\infty}\sum_m \sum_n W_\gamma^i(j,m,n)\varphi_{j_o,m,n}^i(x,y) \qquad (2)$$

where j_o is an arbitrary scale, $W_\varphi(j_o,m,n)$ are approximation coefficients of image $f(x,y)$ at scale j_o, and $W_\gamma^i(j,m,n)$ are coefficients used to add the horizontal, vertical and diagonal details for scale $j \geq j_o$. The result of decompose is sub-band low- low (LL), flat sub-band low-high (LH), vertical sub-band high-low (HL) and diagonal sub-band high-high (HH) for each component. The LL image is considered a reduced version of the original as it retains most details. The LH image contains horizontal edge features, while the HL contains vertical edge features. The HH contains high frequency information only. In wavelet decomposition, only the LL can be decomposed once again in same manner, thereby producing even more sub-bands. This can be done up to any level, thereby resulting in a pyramidal decomposition as shown in Fig. 4. In this work, four-level discrete wavelet transform is applied on each color channel. The sharped edges which are the traces of cut-paste manipulation are higher frequencies and are detected in detail sub-bands, *i.e.* LH, HL and HH sub-bands of decomposition. Therefore, the three sub-bands are considered to detect the edges. Also, the low frequencies in LL sub-band of fourth level decomposition are ignored by setting them to zero. The inverse discrete wavelet transforms is done to reconstruct the original image.
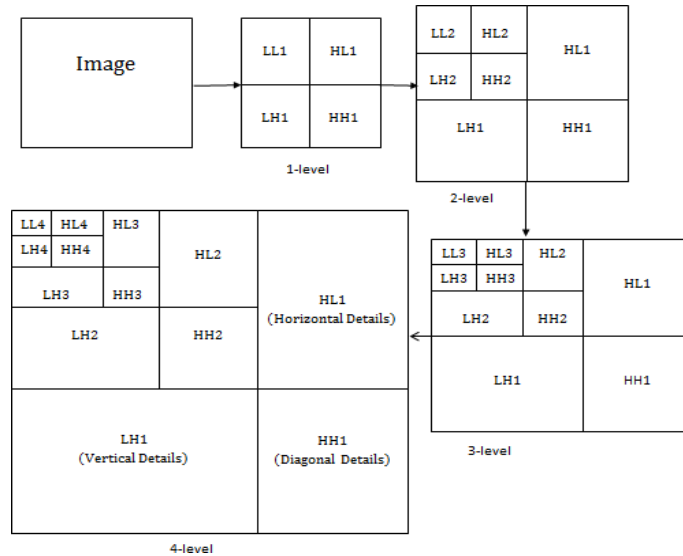
Fig. 4: Four level decomposition of an image by DWT

2.4 Image Gradient and Morphological Operation

Image gradient technique is used for identifying and locating sharp discontinuities in an image. Here, the sobel operator is used which approximately calculates the image gradient of each pixel by convolving the image with a 3×3 filter. The gradient of image in the horizontal (x) and vertical (y) directions is given in Equation (3).

$$\nabla f = \left[\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right] \tag{3}$$

There are two fundamental morphological operations: Dilation and erosion. Normally, at the tampered region, the borders will be smoothed using some software tools and as the consequence all the edges are not detected continuously. Dilation adds pixels to the boundaries of objects in an image which helps to locate forged region.

2.5 Wiener Filter

Every image is supposed to have a noise that comes from image acquisition system. But, such noise spreads fairly uniform throughout to an authentic image. So, the inconsistency in the noise can be used to detect whether the image is forged or not. The connected region obtained from the morphological operation is divided into two larger area sections of the image. The random noise generally exists during the tampering process. Therefore, for each section, a 3 x 3 Wiener filter is done and the filtered image is subtracted from the selected regions. This difference will result us the noise present in that section. The mean of the absolute value of this subtraction is calculated as expressed in Equation (4).

$$f = \frac{\sum_i^n |p_i - w_i|}{\text{total pixels}} \tag{4}$$

where p_i is a given pixel in the area and w_i is the corresponding pixel in the filtered region and n is the total number of pixels. If the noise value is below the threshold, it is original image else the image is tempered.

2.6 Locating region of Tempered Region

The maximum area of the forged image obtained is calculated and again edge is detected for that area. A contour line is drawn along the detected edge to locate the region of tempered image.

3. Results and Discussion

The output obtained at different steps of above mentioned method is shown in the Fig. 5. Fig. 5a and 5b are the original images. Fig. 5c is the forged image by the copy –move technique where Fig. 5a is taken as the base image and part of the image of figure 5b is copied and move. Fig. 5d, 5e and 5f are the Y, Cb and Cr components of Fig. 5c. Four level of discrete wavelet transformation of each channel is shown in the Fig 5g. Similarly, the result of image gradient, dilation and Wiener filtering are shown in Fig. 5h and 5i. The final out put locating forged part of image is shown in Fig. 5j.
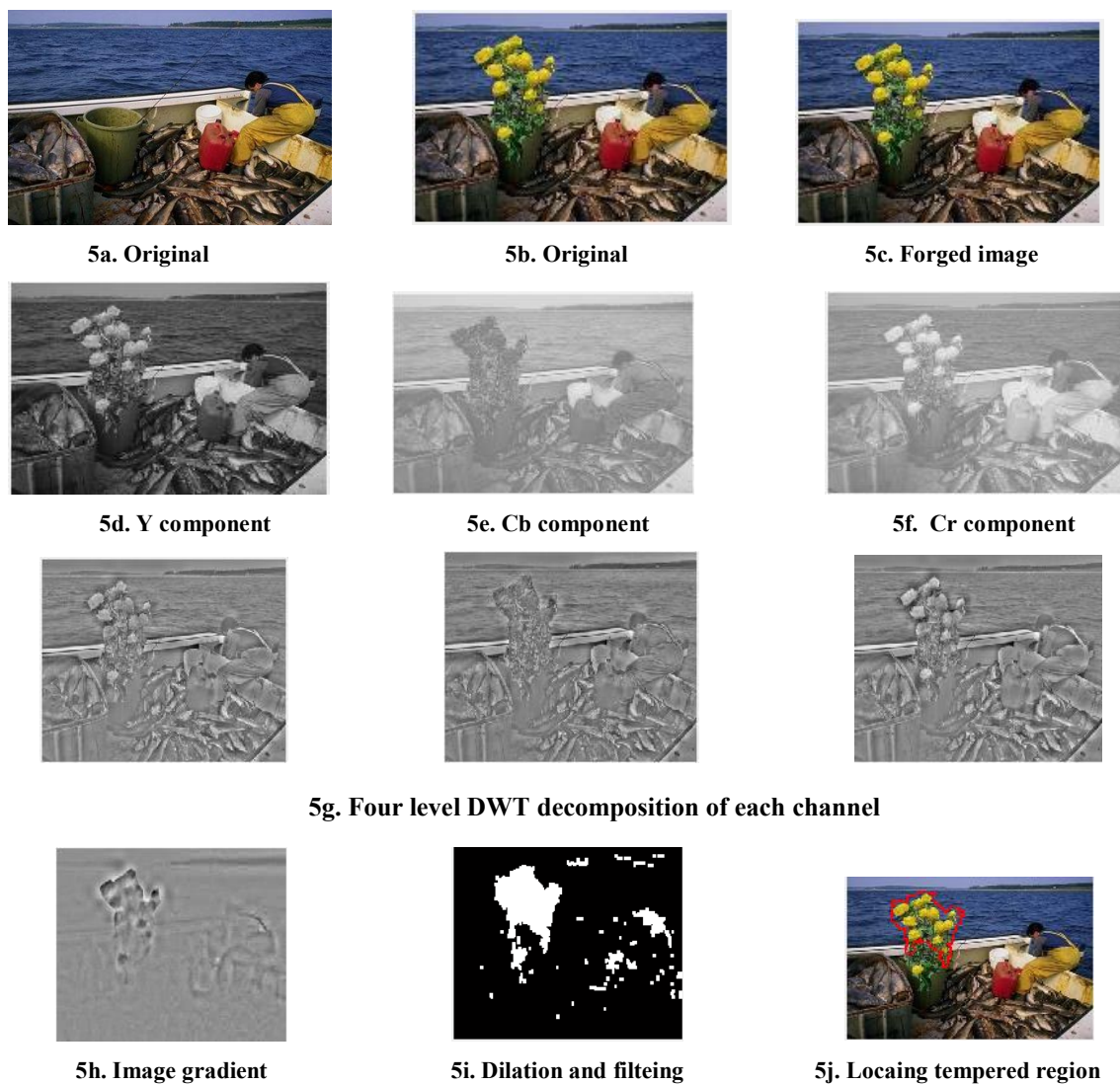
5a. Original   **5b. Original**   **5c. Forged image**

5d. Y component   **5e. Cb component**   **5f. Cr component**

5g. Four level DWT decomposition of each channel

5h. Image gradient   **5i. Dilation and filteing**   **5j. Locaing tempered region**

Fig. 5: The detailed process of detecting image splicing forgery

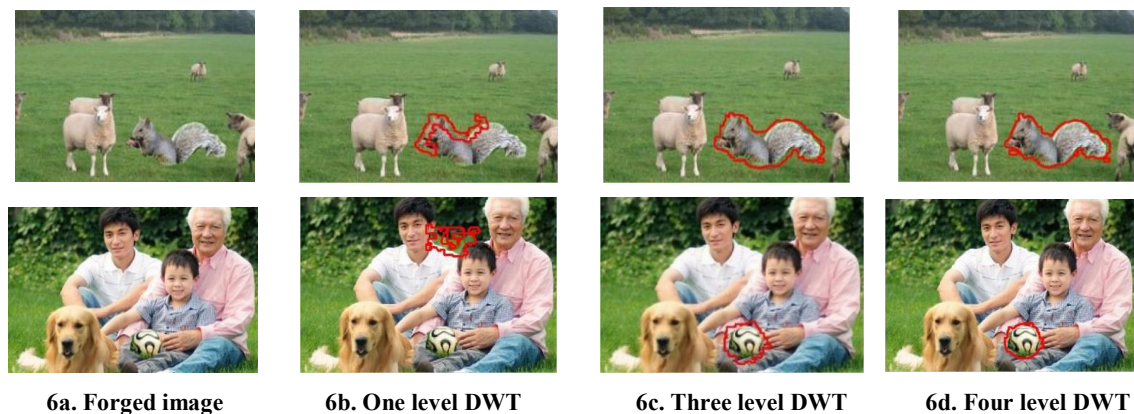**6a. Forged image**   **6b. One level DWT**   **6c. Three level DWT**   **6d. Four level DWT**

Fig. 6: Test images and forgery detection by different levels of DWT

Fig. 6 shows the effect of different levels of DWT operation on test images for detecting the forgery and locating region of the forged images. In compared to one level and three level DWT as shown in Fig. 6b and 6c, the four level DWT gives more accurate tampered region locations which can be seen in Fig. 6d.

Performance evaluation of different level of DWT operation on test image data set is performed by calculating sensitivity, specificity and accuracy as given in equations (5), (6) and (7).

$$Sensitivity = \frac{TP}{TP+FN} \tag{5}$$

$$Specificity = \frac{TN}{TN+FN} \tag{6}$$

$$Accuracy = \frac{TP+TN}{TP+FP+FN+TN} \tag{7}$$

where, TP, TN, FP and FN are true positive, true negative, false positive and false negative respectively.

Table 2: Forgery Detection on different level of wavelet transforms

Level	True Positive rate	False Positive rate	True negative Rate	False Negative rate	Sensitivity	Specificity	Accuracy
1	56	25	48	21	72.73%	65.75%	69.33%
2	66	19	48	17	79.52%	71.64%	76%
3	74	13	48	15	83.15%	78.69%	81.33%
4	84	8	48	10	89.36%	85.71%	88%

From the Table 2 sensitivity, specificity and accuracy is in four level DWT operation is high in compared to the first, second and third level DWT operation for detecting forged image.

4. Conclusion

The four levels DWT decomposition of Y Cb and Cr component of forged image is successfully implemented to detect image splicing. This technique identifies suspicious edge points of the spliced image. Applications of Image gradient, morphological operation and Wiener filtering further detect and smooth the forged area of image. Sensitivity, specificity and accuracy calculated for spliced images of CASIA datasets are obtained 89%, 86% and 88% respectively. The result shows that four levels DWT decomposition significantly solves the image splicing forgery.

References

[1] Bayram S, Sencar HT, Memon N (2007), Improvements on source camera-model identification based on CFA interpolation, *IEEE International Conference on Multimedia and Expo,* **10**: 24-27.

[2]   Dong J, Wang W and Tan T (2013), CASIA Image Tampering Detection Evaluation Database, *IEEE   China Summit and International Conference on Signal and Information Processing*, **4**: 422-426.

[3]   Granty RE, Aditya TS, and Madhu S (2010), Survey on passive methods of image tampering detection, *in IEEE International Conference on Communication and Computational Intelligence,* **4**: 31-61.

[4]   Hariri M, Hakimi F and GharehBaghi F (2015), Image splicing forgery detection using local binary pattern and discrete wavelet transform, *IEEE ,2nd International Conference on Knowledge-Based Engineering and Innovation,* **10** : 1074-1077.

[5]   Rocha A, Scheirer W, Boult TE and Goldenstein S (2011), Vision of the unseen: Current trends and challenges in digital image and video forensics, *ACM Comput. Surveys*, **43**: 1–42.

[6]   Redi A, Taktak W and Dugelay JL (2011), Digital image forensics: A booklet for beginners, *Multimedia Tool Appl.,* **51**: 133-162.

[7]   Rajapriya S, Nima S and Vinmathi J (2014), Detection of Digital Image Forgeries by Illuminant Color   Estimation and Classification*, International Journal of Innovative Research in Computer and   Communication Engineering,* **2**: 14-24.

[8]   Shivakumar BL and Baboo SS (2010), Detecting copy-move forgery in Digital images: A survey and analysis of current methods, *Global Journal of Computer Science and Technology*, **10** : 61-65.

[9]   Sheldon S (2010), Localizing Tampered Image Regions through Image noise features, *International conference in Digital water marking, Springer,* **1**:120-133.

[10]   Ujjainiya U and Chugh S (2016), Digital Image Forgery Detection Based on Texture Feature and Clustering Techniques*, International Journal of Computer Applications*, **147**: 11-17.

[11]   Wang W, Dong J and Tan Т (2010), Effective Image Splicing Detection Based on Image Chroma, *IEEE International Conference on Image Processing,* **1**:1257-1260.

[12]   Zhang Z, Zhao C, Yiming P, Shenghong L and Shilin W (2013), Image-Splicing Forgery Detection Based on Local Binary Patterns of DCT Coefficients, *Journal of Security And Communication Networks, Wiley*, **8**:2386-2395.

[13]   Zahra M, Hamid A, Jalab RM and Aghabozorgi S (2014), Improving RLRN image splicing detection with the Use of PCA and kernel PCA, *The Scientific World Journal, NCB, US,* **2014**: 60-70.