International Journal of Electronics Signals and Systems

Volume 3 | Issue 2 Article 7

October 2013

IMAGE FORGERY DETECTION USING DYADIC WAVELET TRANSFORM

O.M. PRATHIBHA
Department of Electronics and Communication, SDM College of Engineering and Technology,
prathibhaom90@gmail.com

N. S. SWATHIKUMARI
Department of Electronics and Communication, SDM College of Engineering and Technology,
swathins.30@gmail.com

P. SUSHMA
Department of Electronics and Communication, SDM College of Engineering and Technology,
sushma_chowdary20@yahoo.com

IMAGE FORGERY DETECTION USING DYADIC WAVELET TRANSFORM

PRATHIBHA.O.M[1], SWATHIKUMARI. N. S[2] & SUSHMA P[3]

[1,2&3]Department of Electronics and Communication, SDM College of Engineering and Technology
E-mail : prathibhaom90@gmail.com, swathins.30@gmail.com, sushma_chowdary20@yahoo.com

Abstract - In this paper, we propose a blind copy move image forgery detection method using dyadic wavelet transform (DyWT). DyWT is shift invariant and therefore more suitable than discrete wavelet transform (DWT) for data analysis. First we decompose the input image into approximation (LL1) and detail (HH1) subbands. Then we divide LL1 and HH1 subbands into overlapping blocks and measure the similarity between blocks. The key idea is that the similarity between the copied and moved blocks from the LL1 subband should be high, while the one from the HH1 subband should be low due to noise inconsistency in the moved block. We sort pairs of blocks based on high similarity using the LL1 subband and high dissimilarity using the HH1 subband. Using thresholding, we obtain matched pairs from the sorted list as copied and moved blocks. Experimental results show the effectiveness of the proposed method over competitive methods using DWT and the LL1 or HH1 subbands only.

Keywords *- DyWT : Dyadic Wavelet Transform, LL1 SUBBAND: Subband obtained on performing 2 level decomposition of an image by passing it through a low pass filter, HH1 SUBBAND: Subband obtained on performing 2 level decomposition of an image by passing it through a high pass filter, DWT: Discrete Wavelet Transform.*

I. INTRODUCTION

We are undoubtedly living in an age where we are exposed to a remarkable array of visual imagery. While we may have historically had confidence in the integrity of this imagery, today's digital technology has begun to erode this trust. Digital imaging has matured to become the dominant technology for creating, processing, and storing pictorial memory and evidence. Though this technology brings many advantages, it can be used as a misleading tool for hiding facts and evidences .From the tabloid magazines to the fashion industry and in mainstream media outlets, scientific journals, political campaigns, courtrooms, and the photo hoaxes that land in our e-mail in-boxes, doctored photographs are appearing with a growing frequency and sophistication. Over the past five years, the field of digital forensics has emerged to help restore some trust to digital images. Different techniques for validating the integrity of digital images have been developed. These techniques can be divided into two major groups: intrusive and non intrusive. In intrusive (active) techniques, some sort of signature (watermark, extrinsic fingerprint) is embedded into a digital image, and authenticity is established by verifying if the true signature matches the retrieved signature from the test image. The drawback of this approach is that a watermark must be inserted at the time of recording, which would limit this approach to specially equipped digital cameras. Non-intrusive techniques exploit different kinds of intrinsic fingerprints such as sensor noise of the capturing device or image specific detectable changes for detecting forgery. The method explained in this paper i.e. copy-move forgery detection using DyWT is an example for non-intrusive (blind) technique. In this paper, we propose a blind method for copy move image forgery detection using dyadic wavelets. Copy move is one of the most common techniques used for image forgery. In this type of forgery, one or more objects in an image are hidden by copying a part and moving it to another place of the same image.

II. TYPES OF FORGERY

1. Image Retouching

Image Retouching can be considered to be the less harmful kind of digital image forgery. Image retouching does not significantly change an image, but instead, enhances or reduces certain feature of an image to make it more attractive. This technique is popular among magazine photo editors.

2. Image Splicing

This technique is more aggressive than image retouching. Image Splicing is a technique that involves a composite of two or more images which are combined to create a fake image.

3. Copy-move forgery

Copy-move attack is more or less similar to Image Splicing in view of the fact that both techniques modify certain image region (of a base image), with another image. However, instead of having an external image as the source, copy-move attack uses portion of the original base image as its source. In other words, the source and the destination of the modified image originated from the same image. In a copy-move attack, parts of the original image is copied, moved to a desired location, and pasted. This is usually done in order to conceal certain details or to duplicate certain aspects of an image. Blurring is usually applied along the border of the modified

region to reduce the effect of irregularities between the original and pasted region.

4. Copy-paste forgery

In copy-paste forgery an external image is used as the source to modify or manipulate a base image. Here parts of an external image are copied and pasted to the desired location in base image.

III. ADVANTAGES OF THE PROPOSED METHOD

1. Previous method employed DWT which had the following disadvantage that DWT is decimated and is not translation invariant, resulting in many large wavelet coefficients across several scales, creating problems in noise estimation.
2. Unlike the DWT, the UWT has the translation-invariant, or shift-invariant, property. If two signals are shifted versions of each other, the UWT results for the two signals also are shifted versions of each other. The translation-invariant property is important in feature-extraction applications.
3. Unlike the discrete wavelet transform (DWT), which downsamples the approximation coefficients and detail coefficients at each decomposition level, the undecimated wavelet transform (UWT) does not incorporate the downsampling operations. Thus, the approximation coefficients and detail coefficients at each level are the same length as the original signal. The UWT upsamples the coefficients of the lowpass and highpass filters at each level. The upsampling operation is equivalent to dilating wavelets. The resolution of the UWT coefficients decreases with increasing levels of decomposition.

IV. PROPOSED METHOD

The proposed forgery detection method utilizes two types of information for detecting copy move forgery: (a) similarity between copied and moved parts in the smoothed version of the image and (b) noise inconsistency between these parts caused by the forgery. Initially an input image to be tested for forgery is taken and one level Decomposition Using DyWT is applied to obtain subbands LL1 and HH1. After extracting low frequency component (approximate) LL1 and high frequency component (detail) HH1 at scale one, a similarity measure is applied between the blocks in LL1 and HH1 separately. A decision is made based on the similarity between blocks in LL1 and dissimilarity between the blocks in HH1.

ONE LEVEL DECOMPOSITION

We go for one level decomposition of the input image using DyWT. We use atrous algorithm.

Steps followed:

Let **I** be the image to be decomposed, and $h[k]$ and $g[k]$ be the scaling (low pass) and wavelet (high pass) filters. The DyWT of an image can be computed using the following *a'trous* algorithm.

Start at scale $j = 0$, and take, and compute the scaling and wavelet coefficients at scales $j = 1, 2\ldots J$ using Eqs. (1) and (2):

$$c^{j+1}[n] = \sum_k h[k]c^j[n + 2^j k] \quad (1)$$

$$d^{j+1}[n] = \sum_k g[k]c^j[n + 2^j k] \quad (2)$$

Here j is taken as zero as we are performing decomposition at scale zero. Hence equation one and two reduces as follows

$$C[n] = \sum_k h[k]c[n]$$

$$d[n] = \sum_k g[k]d[n]$$

Input image is chosen along with the transfer function of a low pass and high pass filter . As the first step the rows of the input mage is passed through a low pass filter and a high pass filter. Then the columns of the image obtained as the output of the low pass filter is passed through a low pass filter again to obtain LL1 subband. Next the columns of the image obtained as the output of the high pass filter is passed through a high pass filter again to obtain LL1 subband. There is no downsampling involved in DyWT. The size of each of these subbands is the same as the original image.

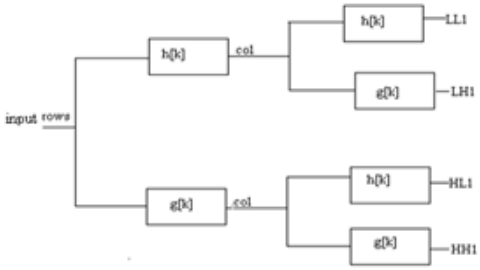

Fig. One Level Decomposition

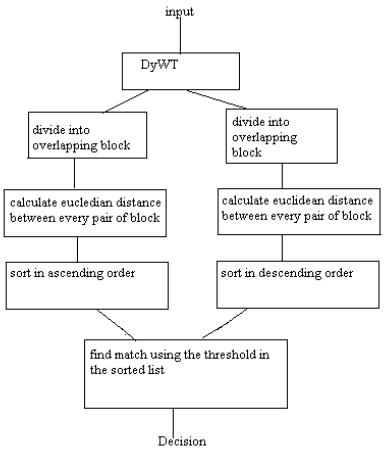

Fig. Flowchart of the proposed method

RESULT.

(a) HH1 subband

(b) LL1 subband

ALGORITHM

In the proposed method, first, the image in question is decomposed using DyWT up to scale one. We use only LL1 and HH1 for further processing. The LL1 subband is an approximation of the image which is better for duplicate identification. The HH1 subband encodes noise present in the image, which is distorted while performing the forgery.HH1 actually contains high frequency information, which consists of mostly due to noise and sharp edges. In the case of color images, first we convert them to gray-scale before applying DyWT.

The LL1 and HH1 subbands are then divided into 16×16 pixel blocks with 8 pixel overlapping in both row and column. However, while performing the image forgery, the noise pattern, which is an intrinsic fingerprint of an image, is distorted. Therefore, copied and moved blocks should exhibit high dissimilarity between them in the HH1 subband. We calculate the similarity using the Euclidean distance:

$$d(p,q) = \sqrt{\frac{1}{N}\sum_{i=1}^{n}(p_i - q_i)^2}$$

Where $d(p,q)$ gives the distance between blocks p and q, pi and qi are corresponding LL1 or HH1 transform coefficient values and N is the total number of pixels in a block. In our case, N = 256. The distances are normalized by the maximum distance to scale the values between 0 and 1. Before calculating the distance, we arrange the pixels of a block in one dimensional vector.

The distances found using LL1 are then sorted in ascending order (List 1), putting highly similar pairs of blocks at the top of the list. We discard all the pairs of blocks that have distances > 0.7. We refer to this value as threshold 1 (*Th*1). On the contrary, the distances calculated using HH1 are sorted in descending order (List 2); this places pairs of blocks with highly inconsistent noise at the top. Again we discard all the pairs of blocks that have distances lower than 0.3. We refer to this value as threshold 2 (*Th*2). Now, if a pair of blocks according to its distance appears at the similar location in both of the lists (List 1 and List 2), then the pair is detected as copied and moved block. For example, if block pair (*p, q*) is located at *n*th location in List 1, and *n*th or (*n*+1)th or (*n*-1)th location in List 2, then the pair is detected as copy-move blocks. The values of *Th1* and *Th2* were chosen as optimal after several trials

V. RESULT

(a) (b)

Fig. (a) The original image. (b) The forged image.

REFERENCES

[1] M. M. Yeung, "Digital watermarking," ACM Commun, vol. 41, no. 7, pp. 30–33, 1998.

[2] C. Rey and J. L. Dugelay, "A survey of watermarking algorithms for image authentication," EURASIP Journal on applied Signal Processing Vol. 2002 N6, pp. 613–621, 2002.

[3] C. Zhang, et al., "Multipurpose Watermarking Based on Multiscale Curvelet Transform," IEEE Trans. Inf. Forensics Security, vol. 3, no. 4, pp. 611–619, December 2008.

[4] H. Farid, "Image forgery detection - a survey," IEEE Signal Processing Magazine, vol. 5, pp. 16–25, March 2009.

◈◈◈