DYADIC WAVELETS AND DCT BASED BLIND COPY-MOVE IMAGE FORGERY DETECTION

Ghulam Muhammad[1], **Muhammad Hussain**[2], **Anwar M. Mirza**[1], and **George Bebis**[3]*

[1]Department of Computer Engineering, [2]Department of Computer Science
College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia
[3]Department of Computer Science and Engineering, University of Nevada at Reno, USA
**Email: ghulam@ksu.edu.sa*

Keywords: Dyadic wavelet transform, discrete cosine transform, copy-move forgery, image forgery detection.

Abstract

This paper proposes a blind method of copy move image forgery detection using dyadic wavelet transform (DyWT) and discrete cosine transform (DCT). An input image is decomposed using DyWT to approximation (LL) subbands and detail (HH) subbands. DCT is then applied to overlapping blocks in LL and HH subbands, and Euclidean distances between the blocks are calculated using DCT coefficients. Decision is made based on similarity of the blocks in LL subband and dissimilarity of the blocks in HH subband. The proposed method is evaluated with images of different sizes, different compression qualities, and with or without rotation before pasting. Experimental results show that the method performs better in all cases than two other multiresolution based methods.

1 Introduction

One image can carry a lot of information that cannot be expressed in many lines. Human visual system is more sensitive to images than the texts. It can extract information very fast from an image. Therefore, photography became an important element in human society. In early ages, pictures could be taken only analog. However, the progress in digital photography in the recent decades increased the use of images and made the photography easier.

Nowadays, digital images play a very important role in our community in a wide variety of applications. Digital imaging can be employed in military applications, insurance processing, surveillance systems, medical imaging, the internet websites, advertisement media, cover of magazines and newspapers, forensic investigation, etc. [20]. Unfortunately, this high popularity of digital images and the development in image editing and manipulating computer software that are low-cost, user-friendly and powerful such as Adobe Photoshop, GIMP and Freehand, make it easy to edit digital images and led to a rapid increase in digitally forged images in mainstream media and on the Internet which decreases the credibility of digital images, and their content integrity can no longer be fully trusted [20]. Therefore, there is a high demand of verifying an image about its authenticity.

In the recent past, there have been a lot of researches in the field of image forgery detection. The authenticity of an image can be checked by verifying its origin, by tracing the forgery steps, or by analyzing the inconsistency in the image. Image forgery detection can be classified into two major groups: active method and blind method. In active methods, it is assumed that the image has watermark embedded, and the authenticity is verified by checking the extracted watermark against the original watermark [18, 23 and 5]. However, these methods are limited to only those images that have watermark embedded. Blind methods, on the other hand, do not use watermark information. Blind methods can be classified into task dependent and task independent. Every camera model has some specific sensor noise pattern, and this can be treated as intrinsic fingerprint of an image. While doing forgery, this specific pattern is lost. In task independent blind methods, the inconsistency of this specific noise pattern is checked; if the inconsistency is found, the image is classified as forged [20, 4, 12, and 10]. On the other hand, task dependent blind methods check for specific type of forgery technique [13, 6, and 11]. Each forgery technique has a unique impact on the image, and these blind methods try to detect this specific impact.

Most of the current blind methods suffer from limitations, for example, (a) need enough training images to train the system for specific camera noise method or the particular forgery method, (b) need human secondary observation, etc.. Therefore, we propose in this paper a blind task independent method that does not need either prior training or human secondary observation, for copy move forgery detection. In the proposed method, we use dyadic wavelet transform (DyWT), which is shift invariant, and discrete cosine transform (DCT) in the feature extraction module. DCT is applied on blocks of approximation subband (LL) and diagonal detailed subband (HH). Euclidean distances between the pair of blocks are calculated using lower DCT coefficients of the blocks to find the similarity. Based on the similarity of the blocks, a decision is made. In this way, the proposed method verifies the claim of authenticity of a test image without any prior knowledge. To prove the efficiency of the method, several experiments are conducted using various

JPEG images with or without rotation before pasting, and different quality factor (Q) of JPEG compressed images. We focus only copy-move forgery in this paper.

The rest of the paper is organized as follows. Section 2 reviews some previous related works; Section 3 describes the proposed method; Section 4 gives the experimental setup, results, and discussion; Section 5 draws some conclusions with future work.

2 Related previous works

Many types of methods have been proposed to detect copy move image forgery. In copy move forgery, a part of an image is copied and pasted in another part of the same image. Before pasting, the copied part may be scaled, rotated, or reflected. The studied methods can be classified into different approaches. Some approaches are moment based approach [14, 21]; frequency domain based approach [7, 8, and 16], and dimensionality reduction based approach [17, 1].

Fridrich et al. [7] divide an image into small overlapping blocks and use DCT coefficients to represent the features of these blocks. The coefficients are lexicographically sorted, and the pair of blocks are assigned to some shift vector. The method looks for any shift vector with occurrence counter greater than a predefined threshold. The blocks contributed to that shift vector are considered to be duplicated blocks. A method based on discrete wavelet transform (DWT), and singular value decomposition (SVD) is proposed in [9]. DWT is calculated from the test image, and the low frequency component (LL) is divided into overlapping blocks. Then SVD is used to represent each block by a reduced feature vector, and these vectors are lexicographically sorted. The matching blocks having more than a certain distance between themselves are considered to be duplicated blocks. It is stated that this method works well with BMP images, and with JPEG compressed or edge processed to a certain extent.

Bayram et al. [2] use Fourier-Mellin Transform (FMT), which is translation, scaling and rotation invariant to detect copy move forgery. FMT is applied to blocks of the input image and counting bloom filters are used instead of lexicographic sorting. According to the authors, the method is robust against scaling, rotation up to 10°and JPEG compression up to a quality factor of 70. Huang et al. [8] proposed a DCT-based detection method for copy move forgery. DCT coefficients are calculated for each overlapping block of the input image and reshaped into a raw vector in the zigzag order to represent the features of each block. Feature vectors are then lexicographically sorted in a matrix. In the matching step, each pair of consecutive vectors are checked for similarity. If the blocks of a pair satisfy similarity condition and are apart not less than by a certain threshold, they are considered as copy-moved blocks. Authors found that the ability of this method in copy move detection is quite robust to JPEG compression, blurring or noise distortion.

In [16], authors proposed a blind copy move forgery detection method that utilizes two types of information, the similarity between copied and moved regions in the smooth version of a tampered image, and the noise inconsistency caused by the forgery in detailed regions. Translation invariant dyadic wavelet transform is used in the first step to decompose the questioned image up to scale one. Only the approximation sub band (LL1) and the detail sub band (HH1) are used for further processing. The two sub bands are divided into overlapping blocks of 16×16 pixels. The similarity between the blocks in LL1 sub band and the dissimilarity between blocks in HH1 are calculated using Euclidean distance between every pair of blocks within the corresponding sub band. In another method, noise inconsistency is measured in each block of HH1 subband to detect the moved block [12]. This method use DWT as a pre-processing technique.

Despite the attractiveness of this field of research and the huge number of studies that were done during the last few years, more effort is still needed, since there is no perfect copy move forgery detection scheme with high robustness against all kinds of post processing operations.

3 The proposed method

Figure 1 shows a block diagram of the proposed copy move forgery detection method. First, the input image is transformed into red, green, and blue components, if the image is a color image. DyWT is applied to each of the color components in one level, and only LL and HH subbands are processed further. The subbands are divided into 16 × 16 overlapping blocks where half of the block size is overlapped to both horizontal and vertical directions. DCT is applied to each block, and Euclidean distance is calculated between the blocks using DCT coefficients. A decision is made based on the distances in LL and HH subbands, and along all three-color components.

3.1 Dyadic wavelet transform

Multiresolution technique is useful to analyze an image in different levels and orientations (directions). Some multiresolution techniques based image forgery detection have been proposed before, however, most of them use DWT, which is shift variant. DWT is not shift-invariant because it involves down-sampling. Because of the loss of shift-invariance, DWT exhibit pseudo-Gibbs phenomena [3] around singularities and does not give optimal results for signal analysis applications like edge detection, denoising, texture analysis. DyWT does not suffer from these drawbacks; it is shift-invariant because it does not involve down-sampling operation [15]. Starck et al [19] proved that DyWT has better texture analysis and detection performance than DWT. A small shift in the input image may result in big difference in DWT coefficients at various scales, which may produce different feature vectors for copied and pasted objects with a little spatial shift.

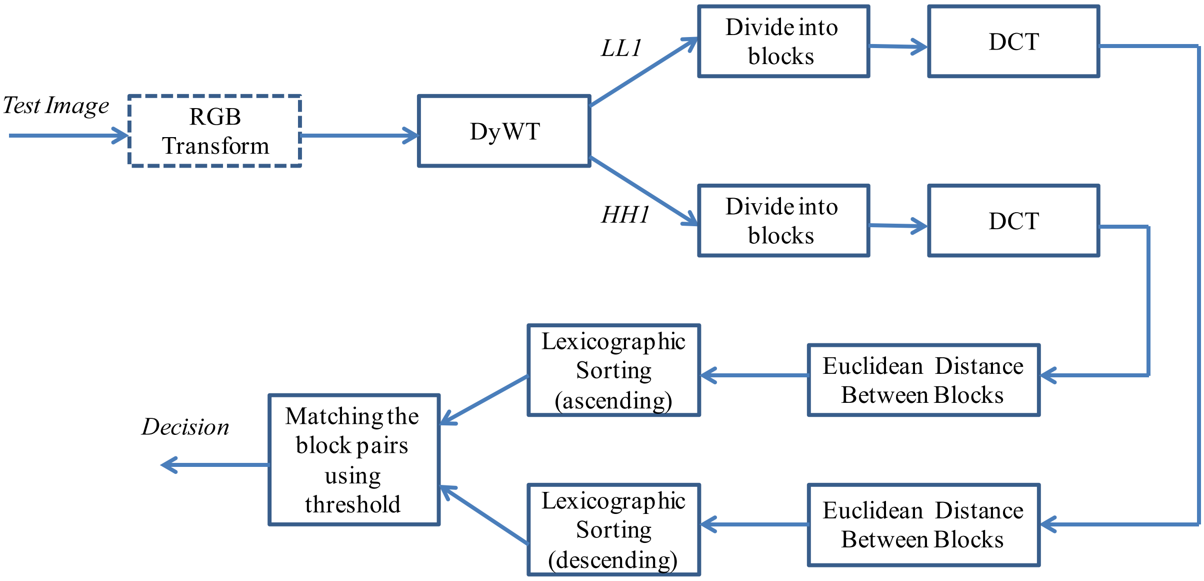

Test Image
RGB Transform
DyWT
LL1
HH1
Divide into blocks
DCT
Divide into blocks
DCT
Euclidean Distance Between Blocks
Lexicographic Sorting (ascending)
Euclidean Distance Between Blocks
Lexicographic Sorting (descending)
Matching the block pairs using threshold
Decision

Figure 1: Block diagram of the proposed method.

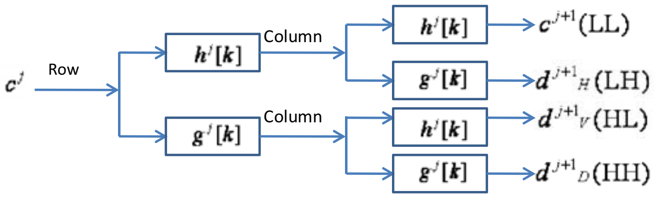


Figure 2: One level decomposition of DyWT of a 2D image.

Let **M** 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 algorithm [16].

(i) Begin at scale *j* = 0, and take $\mathbf{M}^0 = \mathbf{M}$.
(ii) Compute the scaling and wavelet coefficients at scales *j* = 1, 2, …, *J* using Equations (1) and (2):

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

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

Until these steps, it is similar like DWT. Now let $h^j[k]$ and $g^j[k]$ be the filters obtained by inserting $2^j - 1$ zeros between the terms of *h*[*k*] and *g*[*k*]. Then we can perform DyWT as follows:

(iii) Start with **M.**
(iv) Obtain the scaling and wavelet coefficients $\mathbf{M}^j$ and $\mathbf{D}^j$ at scales *j* = 1, 2, …, *J*

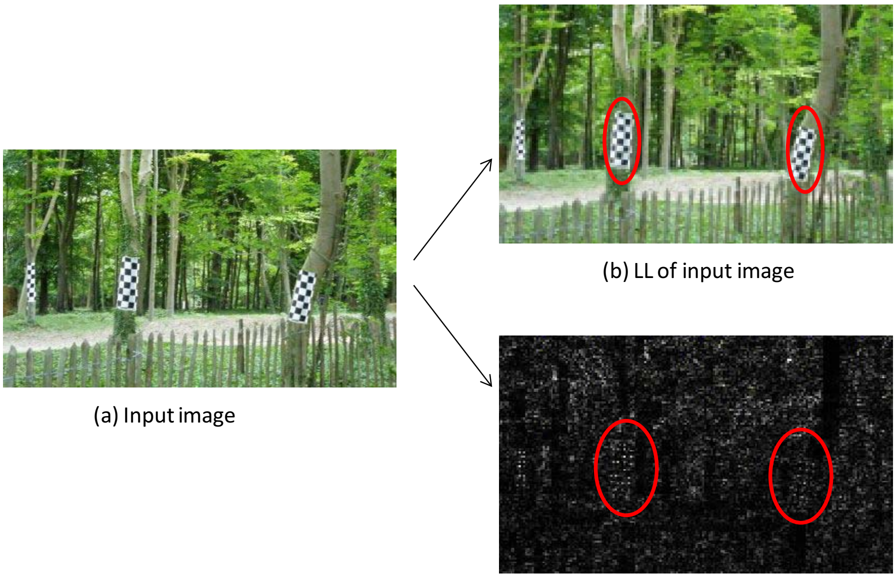
- Filter $\mathbf{M}^{j-1}$ with $h^{j-1}[k]$,
- Filter $\mathbf{M}^{j-1}$ with $g^{j-1}[k]$.

Figure 2 shows one-level decomposition of a two-dimensional image. LL is the low-frequency component and called approximation, while HH is the high-frequency component and called detailed. In the proposed method, only LL and HH are taken into account.

3.2 Feature extraction and matching

In most of the cases, when copy move forgery is done, post processing is applied to hide the traces of forgery. Post processing may include smoothing (blurring), adding a small amount of noise, etc. to the pasted region. In this type of copy move forgery, original noise pattern is distorted, whereas the overall (approximation) similarity is maintained between the copied part and the pasted part. Based on this assumption, the proposed method finds a similarity in LL subband and dissimilarity in HH subband. The copy-move blocks' pair must have high similarity between themselves in LL and dissimilarity in HH. In many natural genuine images, there may be similar two or more objects. If we cannot measure dissimilarity in HH subband, these natural authentic images may be classified as forged image (false positive) due to high similarity in LL subband. Figure 3 gives an example of an input image, its LL subband and HH subband. In the image of this figure, black-and-white zigzag in the middle tree is copied, rotated slightly, and pasted on the right-side tree. From the figure, we can see that while the zigzag pattern is preserved in LL, it is distorted in HH.

In the proposed method, each of LL and HH subbands are divided into 16 × 16 overlapping blocks where overlapping is



(a) Input image

(b) LL of input image

(c) HH of input image

Figure 3: (a) Example of a copy-move forged image. The black-white zigzag marks in the middle tree are copied and pasted with slight rotation on the right side tree. (b) LL and (c) HH subbands of (a) using DyWT. The circles in (b) and (c) represent copied and pasted parts.

by 8 pixels. DCT is applied to each block to decorrelate the wavelet coefficients and compact the energy in lower coefficients. Most of the high coefficients have zero values and have almost no contribution. Therefore, we retain only first 30 DCT coefficients for each block and for each subband.

The similarity between the blocks is calculated using Euclidean distance with 30 coefficients from the subbands. The Euclidean distance is defined as follows:

$$d(x,y)=\sqrt{\frac{1}{N}\sum_{i=1}^{n}\left(x_i-y_i\right)^2} \qquad (3)$$

where $d(x,y)$ is the distance between blocks x and y, x_i and y_i are corresponding DCT coefficients from the subband and N is the total number of coefficients in a block (in this case, $N = 30$). The distances are normalized so that they fall between 0 and 1.

After calculating the distances, they are lexicographically sorted in ascending order in case of LL subband and in descending order in case of HH subband. In this way, the highly similar blocks will appear at the top of the list from LL (List 1) and most dissimilar blocks will be at the top of the list from HH (List 2). The entries of these two lists are reduced by using two thresholds *Th1* and *Th2*. All the entries greater than *Th1* are removed from List 1 and all the entries smaller than *Th2* are removed from List 2. If a pair of blocks (x,y) exits in both the reduced lists, it is considered as a copy-moved pair. Based on the experiments, we set the values of *Th1* as 0.7 and *Th2* as 0.3.

4 Experimental results and discussion

In the experiments, authentic and forged images were taken from CASIA v1.0 Tampering Detection Evaluation Dataset [22]. CASIA provides tampered images under the directory of splicing. We chose 80 forged images in such a way that they correspond to copy-move on the same image, and without or with rotation less than 20°. The corresponding 80 authentic images were also used in the experiments. The image sizes of CASIA v1.0 dataset are 374×256. We also used our own small image datasets that contain 10 different image sources and their forged version using Adobe Photoshop tool. The test images, both original and forged, can be found at http://faculty.ksu.edu.sa/ghulam/Pages/ImageForensics.aspx. All the image sizes are 200×200. The forged images are in JPEG format with the highest Q.

To report the results, several error measures are used. False positive corresponds to identify a genuine image as a forged image, while false negative corresponds to detect a forged image as an authentic image. Equal error rate is defined as a point where false positive rate and false negative rate are same. Results are also reported in detection error tradeoff (DET) curve. DET curve shows false positive rates vs. false negative rates at different thresholds. The detection cost function is defined as a weighted sum of false negative and false positive probabilities as follows:

$$C_{Det} = \left(C_{FalseNegative} \times P_{FalseNegative|Forged} \times P_{Forged}\right) + \left(C_{FalsePositive} \times P_{FalsePositive|Genuine} \times (1 - P_{Forged})\right) \quad (4)$$

where, $C_{FalseNegative}$ and $C_{FalsePositive}$ are relative costs of detection errors P_{Forged} is *a* priori probability of the specified forged image. In the experiments, $C_{FalseNegative}$ and $C_{FalsePositive}$ are set to 1 and P_{Forged} to 0.5. Minimum cost is denoted as a small circle on the DET curve.

Figure 4 and 5 show the effect of threshold Th1 and Th2 on false positive rates and false negative rates, respectively. From the figures, we find that increasing Th1 and Th2 increases the false positive rate, while the best false negative rate is achieved near Th2 = 0.5 and Th1 = 0.1.

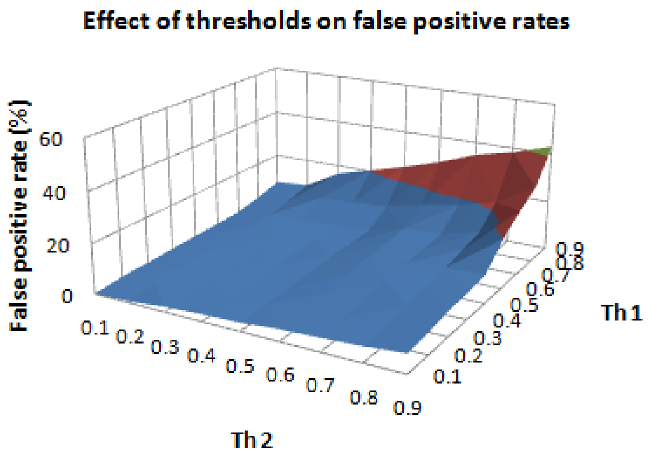


Figure 4: Effect of thresholds on false positive rate.

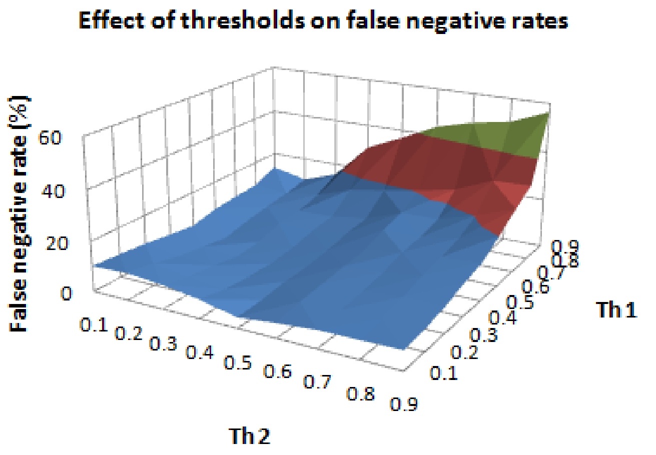


Figure 5: Effect of thresholds on false negative rate.

Figure 6 gives the DET curve of the proposed method and the methods in [9] and [12]. We make the comparison with [9] and [12] because these two methods also use multiresolution techniques. The method [9] uses DWT and LL (so it checks only similarity) and [12] uses DWT and HH (so it checks only dissimilarity). The method in [12] is modified in our experiments slightly because we use Euclidean distance with Equation (3) instead of comparing the median of each block. From the figure, we can find that EER of the proposed method is 4.2%, which is much lower than 7.3% obtained by [9] and 8.1% obtained by [12]. The minimum cost is achieved with the method at a false positive rate of 3.97% and false negative rate of 5.8%.

In a separate set of experiments, we used our own small dataset as described before, except that the forged images were saved in JPEG format at different Q factors (Q = 90, 80, 60). The results are given in Table 1. The EER of the proposed method does not degrade too much at Q factor of 90 and 80; however a significant degradation can be observed at Q factor of 60. Methods [9] and [12] have higher EER than the proposed method in all Q factors. These results suggest that the proposed method is more robust to compression quality than the other investigated methods.

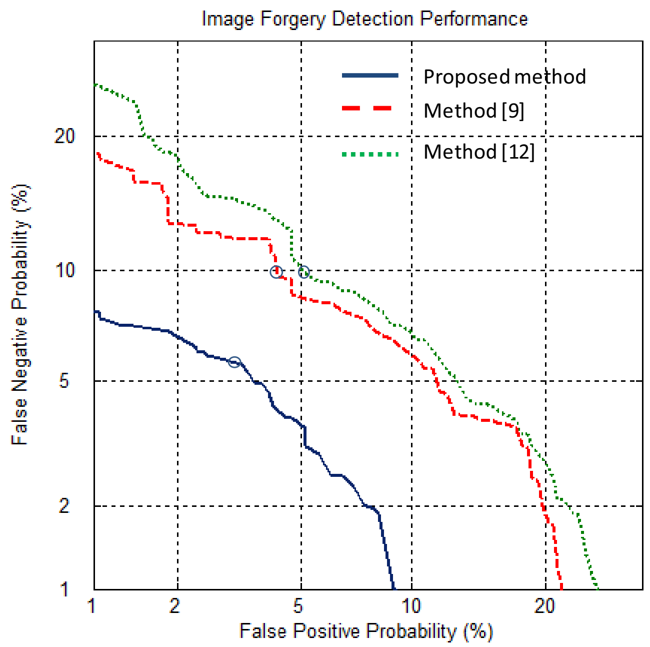


Figure 6: DET curve for the methods.

Q →	90	80	60
Proposed method	4.33	4.76	9.67
Method [9]	9.45	10.29	13.58
Method [12]	11.45	12.43	16.42

Table 1: EER (%) of the methods at different Q factor JPEG images.

5 Conclusion

DyWT and DCT based copy move image forgery detection method was proposed. The proposed method utilized both the similarity information in copy-moved parts and the dissimilarity information due to post processing in those parts. The experimental results showed that the proposed method performed well in different sizes of images, in cases with or without rotation, and in various compression qualities in JPEG format.

In a future study, we wish to investigate other multiresolution techniques in image forgery detection.

Acknowledgements

This work is supported by the grant 10-INF1140-02 under the National Plan for Science and Technology (NPST), King Saud University, Riyadh, Saudi Arabia.

References

[1] I. Amerini, et al.,