Digital Investigation 9 (2012) 49–57

Contents lists available at SciVerse ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Passive copy move image forgery detection using undecimated dyadic wavelet transform

Ghulam Muhammad [a,*], Muhammad Hussain [a], George Bebis [b]

[a] King Saud University, College of Computer and Information Sciences, PO Box: 51178, Riyadh 11543, Saudi Arabia
[b] Dept. of Computer Science and Engineering, University of Nevada, Reno, NV USA

ARTICLE INFO

Article history:
Received 5 September 2011
Received in revised form 29 February 2012
Accepted 9 April 2012

Keywords:
Dyadic wavelets transform
Copy move
Image forgery
Image forensics
Blind technique

ABSTRACT

In this paper, a blind copy move image forgery detection method using undecimated dyadic wavelet transform (DyWT) is proposed. DyWT is shift invariant and therefore more suitable than discrete wavelet transform (DWT) for data analysis. First, the input image is decomposed into approximation (LL1) and detail (HH1) subbands. Then the LL1 and HH1 subbands are divided into overlapping blocks and the similarity between blocks is calculated. The key idea is that the similarity between the copied and moved blocks from the LL1 subband should be high, while that from the HH1 subband should be low due to noise inconsistency in the moved block. Therefore, pairs of blocks are sorted based on high similarity using the LL1 subband and high dissimilarity using the HH1 subband. Using thresholding, matched pairs are obtained 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.

1. Introduction

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. This is because today digital images can be manipulated in such perfection that forgery cannot be detected visually. In fact, the security concern of digital content has arisen a long time ago and 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 (Yeung, 1998; Rey and Dugelay, 2002; Zhang et al., December 2008). This approach is limited due to the inability of many digital cameras and video recorders available in the market to embed extrinsic fingerprints (Farid, March 2009).

The limitations of intrusive techniques have motivated the need for non-intrusive (blind) techniques (Chen et al., 2008; Mahdian and Saic, September 2008; Farid, 2009; Mahdian and Saic, September 2009; Swaminathan et al., March 2008; Lin et al, Sept. 2009) to validate the authenticity of digital images. These techniques exploit different kinds of intrinsic fingerprints such as sensor noise of the capturing device or image specific detectable changes for detecting forgery. There are many challenges in blind techniques, for instance, reducing false positive rates (i.e., an authentic image being detected as a forged image), making the system fully automated, localizing the forgery, detecting forgery of any type of image format (compressed or uncompressed), increasing the robustness and reliability, etc.

Existing blind techniques have their limitations. For example, (a) need many prior images to estimate the intrinsic fingerprints, which is a serious bottleneck (i.e., in

* Corresponding author. Tel.: +966 1 4696281.
E-mail address: ghulam@ksu.edu.sa (G. Muhammad).

1742-2876/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2012.04.004

potential situations only one image is provided) (Chen et al., 2008) (Swaminathan et al., March 2008), and (b) use one image but the method used for noise estimation is not robust because it is based on the Discrete Wavelet Transform (DWT) (Mahdian and Saic, September 2009). This is mainly because DWT is decimated and is not translation invariant, resulting in many large wavelet coefficients across several scales, creating problems in noise estimation.

In this paper, we propose a blind method for copy move image forgery detection using undecimated 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. Some sophisticated image editing tools make this type of forgery undetectable in the naked eye by applying a 'soft' touch at the edges of the moved part. As the color and texture of the moved part is compatible with those of the copied part, it is very difficult to distinguish between these two parts. Also, two or more identical objects in the same original image contribute to the level of difficulty of forgery detection. Most of the existing copy move forgery detection methods either rely on similarity measurements or noise deviation measurements between the parts (blocks of an image). 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. Here, we use the dyadic wavelet transform, which is translation invariant. Moreover, we use the scaling coefficients (LL1) and wavelet coefficients (HH1) at scale one to obtain a smoothed version and noise estimation, respectively.

The rest of the paper is organized as follows. Section 2 reviews some of the previous methods in copy move forgery detection. Section 3 describes the proposed method. Experimental results and discussions are provided in Section 4, while Section 5 presents our conclusions.

2. Previous works on copy move forgery detection

Quite a few works have been reported on copy move image forgery detection. A bibliography on blind image forgery detection methods can be found in Mahdian and Saic (2010). Bayram et al. (Bayram et al., 2009) use a scale and rotation invariant Fourier-Mellin Transform (FMT) and the notion of bloom filters to detect copy move forgery. Their method is computationally efficient and can detect forgery in highly compressed images. Copy move forgery detection based on blur moment invariants has been proposed in Mahdian and Saic (2007). This method can detect duplicated regions degraded by blurring or corrupted with noise. Huang et al. (Huang et al., 2008) have proposed a copy move forgery detection method based on Scale Invariant Feature Transform (SIFT) descriptors. After extracting the descriptors of different regions, they match them with each other to find possible forgery in images. A sorted neighborhood approach based on DWT and Singular Value Decomposition (SVD) has been proposed in Li et al. (2007). In this method, first DWT is applied to the image and then SVD is used on low-frequency components to reduce their dimension. SV vectors are then lexicographically sorted, where duplicated blocks will be close in the sorted list. Solario and Nandi (Solario and Nandi, 2009) use log-polar coordinates to obtain a one dimensional descriptor invariant to reflection, rotation, and scaling for detecting duplicated regions. The Discrete Cosine Transform (DCT) was used in Fridrich et al. (August 2003). They use lexicographic sorting after extracting DCT coefficients of each block in an image. A computationally efficient method based on Principal Component Analysis (PCA) was presented in Popescu and Farid (2004). The DWT and phase correlation based method was proposed in Zhang et al. (2008). Their algorithm is based on pixel matching to locate copy move regions. Sutcu et al. (Sutcu et al., 2007) proposed tamper detection based on the regularity of wavelet coefficients. In their method, they used undecimated DWT. Regularity in sharpness or blurriness is measured in the decay of wavelet coefficients across scales.

Most of the above methods suffer from false positives. Therefore, human interpretation is necessary to obtain the correct result (Mahdian and Saic, 2010).

3. Proposed method

Wavelet transform is a multiresolution technique that has been preferred over Fourier transform in the field of image processing (Mallat, 2009). Unlike Fourier transform, wavelet transform not only can extract frequency (scale) information, but also can give location information. Wavelet transform decomposes an image into its average representation, which is called approximation, and different directional detail representations. We propose in this paper a robust blind copy move image forgery detection method using *undecimated dyadic wavelet transform* (DyWT). 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. A preliminary explanation of this method is given in our previous work (Muhammad et al., 2011).

3.1. Dyadic wavelet transform

Many previous methods on copy move forgery detection use DWT. For pattern recognition, signal representation (descriptors) must be shift-invariant, because when a pattern is shifted, the descriptors are also shifted not modified (Mallat, 2009). For example, in copy-move image forgery, the copied and the pasted parts may not be poisoned in the same place of two blocks (see Fig. 1). If the descriptors are not shift-invariant, they will produce two different representations for these two blocks and thereby miss the forgery detection. DWT is not shift-invariant because it involves downsampling. In DWT, during the convolutions in the decomposition stage (Eq. (1) and Eq. (2)) only every second wavelet coefficients is considered. It is obtained by downsampling by a factor of two (reduce the size by two in every direction) after the convolution. Due to this procedure, DWT is referred to as decimated.

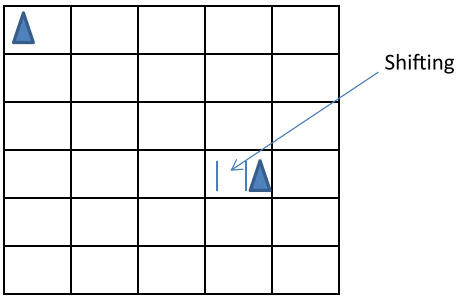

Fig. 1. Illustration of the need of shift-invariant descriptors. The triangle in the first block is copied and pasted in another position. A shift-invariant descriptor will give similar features if applied to these two blocks, while a shift-variant descriptor will result dissimilar features.

Because of the loss of shift-invariance, DWT exhibits pseudo-Gibbs phenomena (Coifman and Donoho, 1995) around singularities and does not give optimal results for signal analysis applications like edge detection, denoising, texture analysis. To overcome this drawback of DWT, Mallat and Zhong (Mallat and Zhong, July 1992) introduced the DyWT, which is shift invariant. In this case, the wavelet transform does not involve downsampling and the number of wavelet coefficients does not shrink between the scales like in DWT. Due to this characteristic, DyWT is undecimated. Starck et al. (Starck et al., 2007) proved that DyWT has better texture analysis and detection performance than DWT. A small shift in input image may result in big difference in DWT coefficients at different scales, which may produce different feature vectors for copied and pasted objects with little spatial shift.

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 *atrous* algorithm.

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

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

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

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 using filtering as follows:

- Start with **I**, which is assumed to be at scale zero, i.e., $\mathbf{I}^0 = \mathbf{I}$.

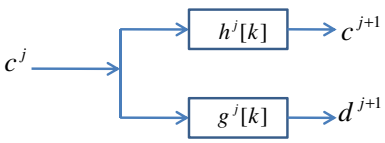

Fig. 2. One level decomposition of DyWT.

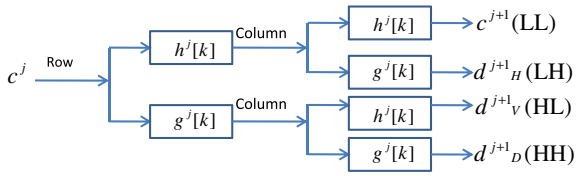

Fig. 3. One level decomposition of DyWT of a 2D image.

- To obtain the scaling and wavelet coefficients $\mathbf{I}^j$ and $\mathbf{D}^j$ at scales $j = 1, 2, \ldots, J$
  - ○ filter $\mathbf{I}^{j-1}$ with $h^{j-1}[k]$,
  - ○ filter $\mathbf{I}^{j-1}$ with $g^{j-1}[k]$.

The following diagram (Fig. 2) illustrates this algorithm one level decomposition.

As mentioned, there is no downsampling involved in DyWT. In the wavelet transform, $\mathbf{I}^j$ is called the low pass subband (L) and **Dj** are called the high pass subbands (H). In the case of two dimensional signals like images, we find four subbands LL, LH, HL, and HH at each scale of the decomposition. The size of each of these subbands is the same as the original image. We can decompose a 2D image using DyWT along rows and columns as illustrated in Fig. 3.

3.2. Steps of the proposed method

Fig. 4 shows the steps involved in the proposed copy move image forgery detection method. 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

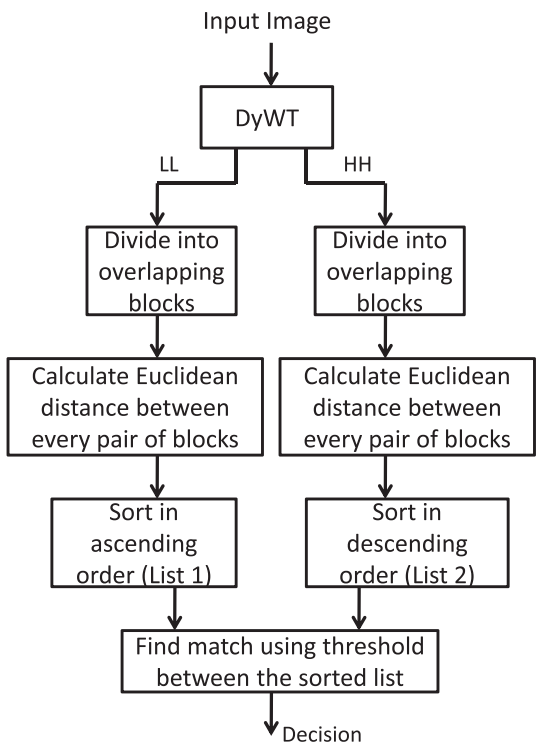

Fig. 4. Flowchart of the proposed copy move image forgery detection.

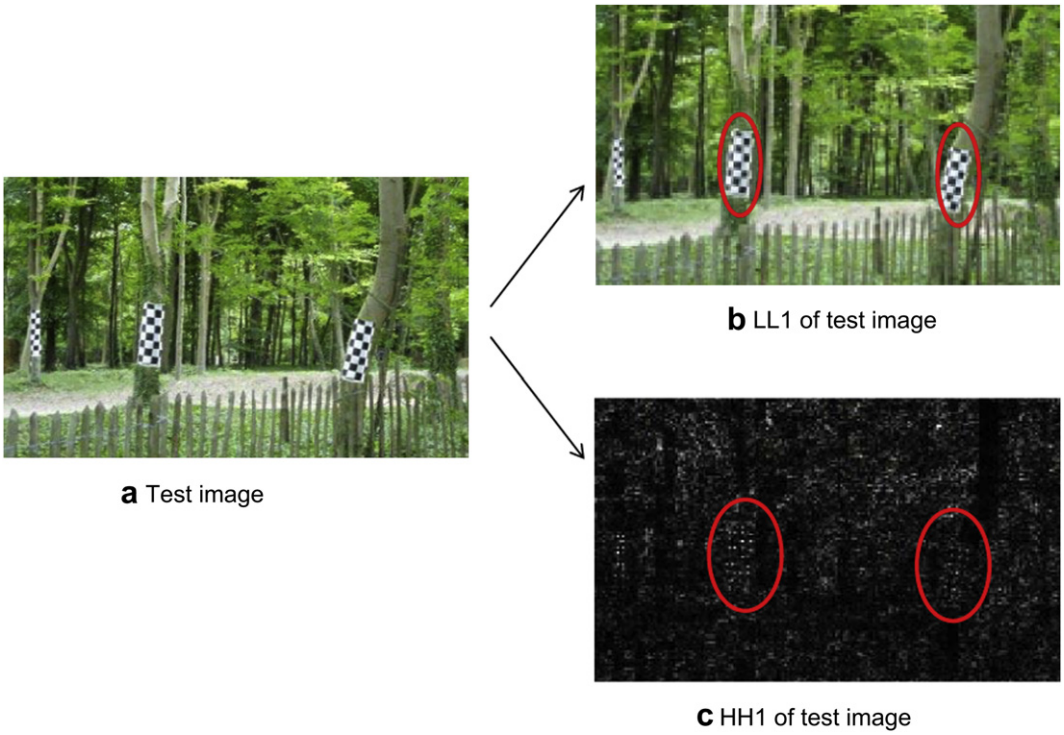

Fig. 5. (a) Example of a copy move forged image. The black-white square marks in the middle tree are copied and pasted with slight rotation on the right side tree. (b) LL1 and (c) HH1 subbands of (a) using DyWT. The circles in (b) and (c) represent copied and pasted parts.

image which is better for duplicate identification. LL1 is obtained by applying low pass filter both horizontally and vertically, and thereby represent low frequency component of the input image. 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. HH1 is obtained after applying high pass filter both horizontally and vertically. Fig. 5 shows an example case of copy move forged image and its LL1 and HH1 using DyWT. In the test image (Fig. 5(a)) the black-white square marks in the middle tree are copied and pasted with slight rotation on the right side tree. The circles in Fig. 5(b) and 5(c) represent copied and pasted parts in LL1 and HH1, respectively. From the figures, we can see that though encircled parts in LL1 look similar, they are distorted in HH1.

The LL1 and HH1 subbands are then divided into 16 × 16 pixel blocks with 8 pixel overlapping in both row and column. We assume that copy move forgery is performed in at least 16 × 16 pixel. Copied and moved blocks in LL1 should exhibit similarity between them. However, while performing the image forgery, the noise pattern, which is an intrinsic fingerprint of an image, is distorted. This is true for most copy move forgery, where traces of forgery are tried to hide by smoothing the resulted edges or adding some noise around. Therefore, copied and moved blocks should exhibit high dissimilarity between them in the HH1 subband. We calculate the similarity using the Euclidean distance:

$$d(p,q) = \sqrt{\frac{1}{N}\sum_{i=1}^{n}(p_i - q_i)^2} \tag{3}$$

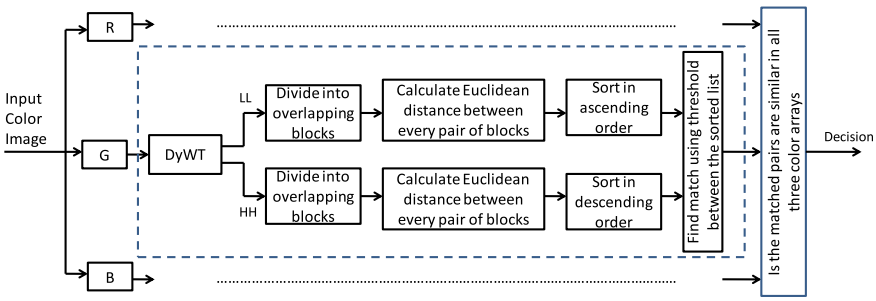

Fig. 6. Flowchart of the proposed copy move image forgery detection using three color arrays (R, G, and B) (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.).

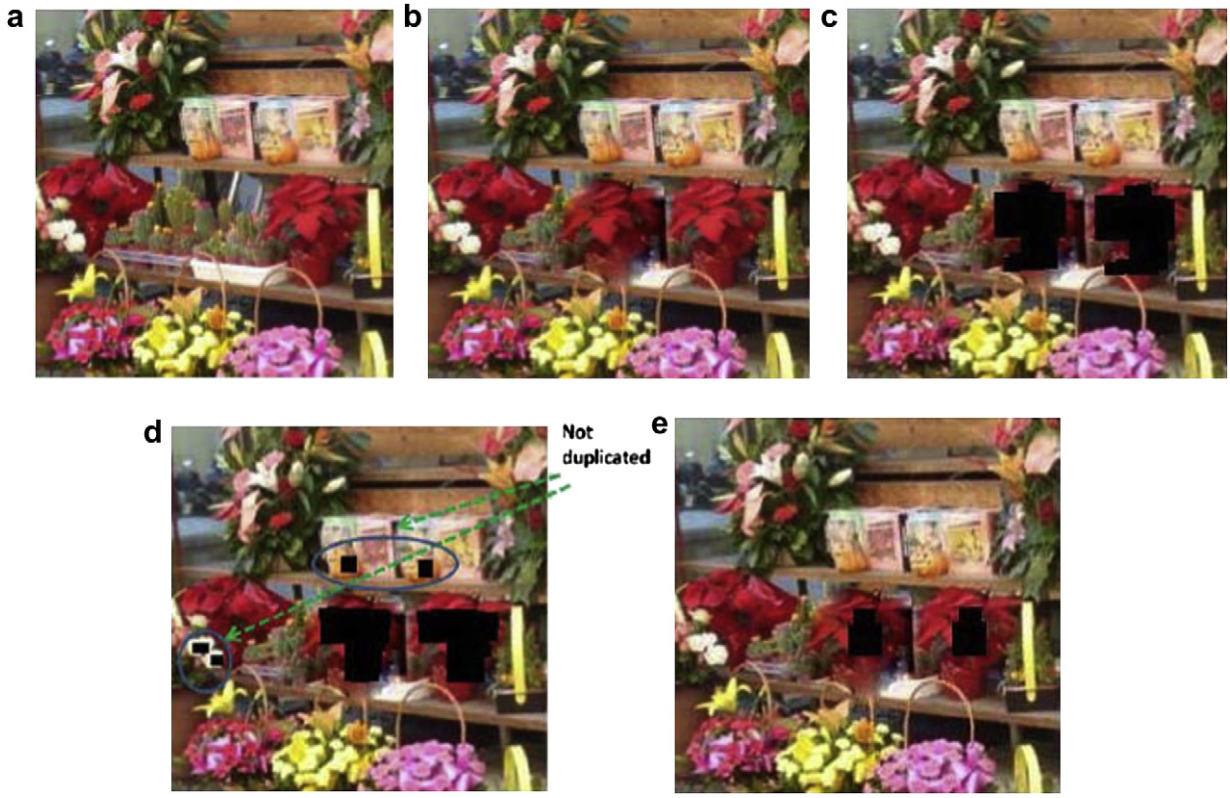

Fig. 7. (a) The original image. (b) The forged image where the middle red flower is a copy of the right red flower. (c) The result of the proposed method. (d) The result of the method in (Li et al., 2007); it shows false positives. (e) The result using modified (Mahdian and Saic, September 2009); it shows truncated area of forgery (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.).

where $d(p,q)$ gives the distance between blocks p and q, p_i and q_i are corresponding gray level 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 ($Th1$). 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 ($Th2$). 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. Particularly, if block pair (p, q) is located at nth location in List 1, and within $(n + i)$th and $(n - i)$th location in List 2, then the pair is detected as copy-move blocks. This band in List 2 is used to limit the false positive rate. The values of $Th1$ and $Th2$ were chosen as optimal after several trials. Also the value of i was varied between 1 and 15, and fixed to 7 that gave the optimal result.

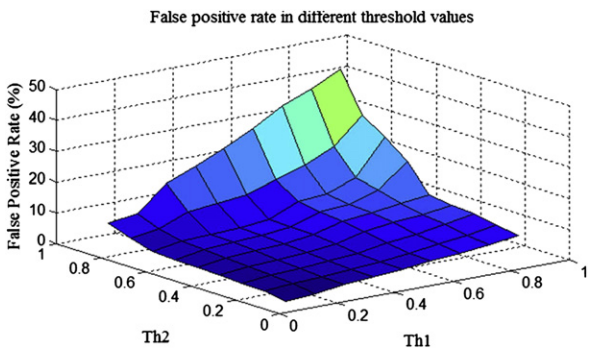

Fig. 8. False positive rates (%) for different threshold values of $Th1$ and $Th2$ with the proposed method.

Table 1
Number of blocks identified as copy move out of 1148 copy move blocks using different methods. All the results are obtained using gray scale conversion.

	Proposed method	Method of Li et al. (2007)	Modified method of Mahdian and Saic (September 2009)
Accuracy	1101 (95.90%)	1045 (91.03%)	932 (81.18%)
False positive (%)	4.54	9.65	10.03
False negative (%)	6.67	12.45	13.98

It should be mentioned that there may be similar objects in an original (not forged) image. In the case of LL1 subband only, similar objects will be identified as copy-moved objects resulting in false positives. On the other hand, in the HH1 subband, these objects will not be identified as copy-moved because of low dissimilarity in noise level. Therefore, we capitalize both on LL1 and HH1 to avoid false positives. In the case of color images, first we convert them to gray scale before applying DyWT.

The proposed method is also applied on color image without converting it into gray scale. In this approach, first the input color image is decomposed into three color components: red (R), green (G), and blue (B). Then DyWT and subsequent steps in Fig. 4 are applied on each of the three color arrays. If the matched pairs of blocks are similar in all the three arrays, forgery is detected. Fig. 6 shows the proposed method using the three color arrays.

4. Experimental results

The proposed method was evaluated on several test images that were forged using copy-move operation. We perform a series of tests using different types of forgery. The results are reported in three parameters, which are (a) false negative: the system detects forged image as genuine image, (b) false positive: the system detects genuine image as forged image, and (c) accuracy: the ratio between correctly detected images and the total number of images.

4.1. Copy-move forgery without rotation and with JPEG Q factor of 100

There were 10 different image sources and the forgeries on these sources were done 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 Q (quality) factor of 100.

Fig. 7 shows an example using the proposed method with a color copy move forged image. The image was forged by copying the right red flower and moving it to the middle position (i.e., middle red flower is a copy of right red flower). Fig. 7 (c) shows the output of the proposed method. The black area is identified as copy and move area. We compared our method with that in Li et al. (2007) that uses DWT and LL, and the one in Mahdian and Saic (September 2009) that uses DWT and HH1. We modified the method in Mahdian and Saic (September 2009) in the sense that instead of comparing the median of each block, we used Euclidean distances as described in Eq. (3). Fig. 7 (d, e) shows the results produced by the methods in Li et al. (2007) and modified (Mahdian and Saic, September

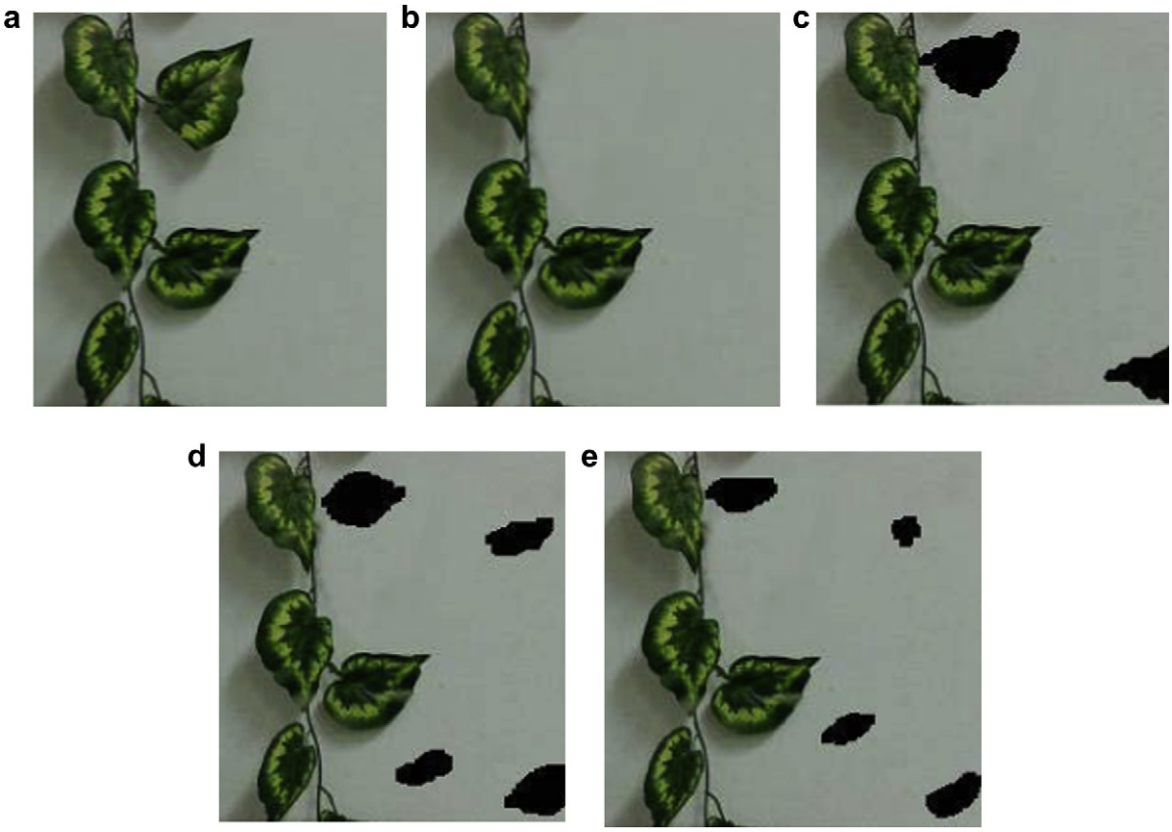

Fig. 9. (a) The original image. (b) The upper leaf on right side has been hidden by copying and pasting a portion of the image from lower corner of the image. (c) The result of the proposed method. (d) The result of the method in Li et al. (2007). (e) The result using modified (Mahdian and Saic, September 2009). All of the methods use gray scale conversion.

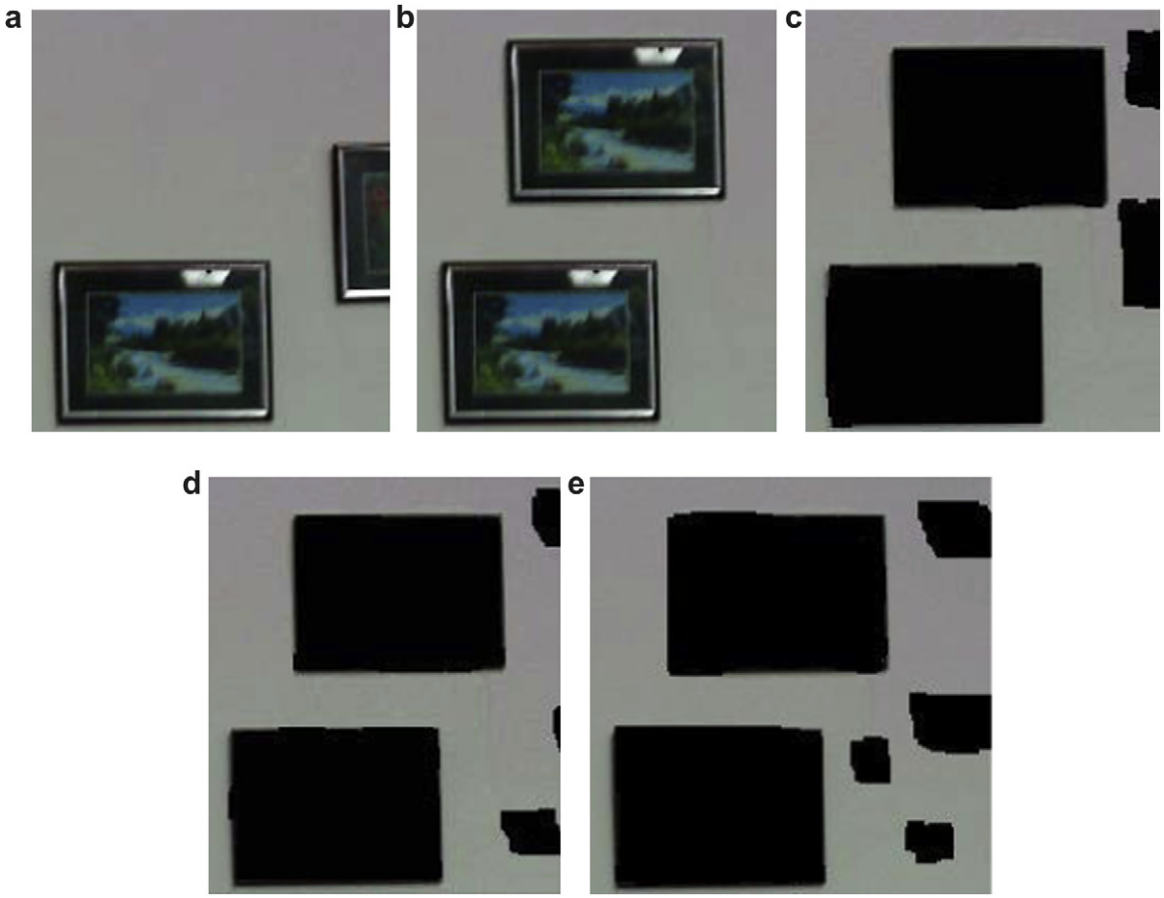

Fig. 10. (a) The original image. (b) The picture in the lower part has been copied and pasted in the upper part and the smaller picture has been hidden by copying a portion of the image from the upper part of the image. (c) The result of the proposed method. (d) The result of the method in Li et al. (2007). (e) The result using modified (Mahdian and Saic, September 2009). All of the methods use gray scale conversion.

2009), respectively. Fig. 7 (d) shows some false positives and Fig. 7 (e) shows some missing area of copy and move blocks.

We tested the proposed method on several test images with different copy move forgery. There were a total of 574 copied 16×16 blocks (i.e., a total of $574 + 574 = 1148$ blocks of copy-move). We considered a block as forged if more than 50% of that block area was copied/moved. The effect of thresholds $Th1$ and $Th2$ on false positive rate is shown in Fig. 8. The false positive rates in this figure are obtained when the input image is converted into gray scale. From the figure, we can see that when the values of $Th1$ and $Th2$ are increased, false positive rate is also increased. The false

Table 2
Number of blocks identified as copy move out of 1148 copy move blocks using different methods. All the methods are applied on the three color arrays.

	Proposed method	Method of Li et al. (2007)	Modified method of Mahdian and Saic (September 2009)
Accuracy	1129 (98.34%)	1067 (92.94%)	951 (82.84%)
False positive (%)	4.02	9.47	9.81
False negative (%)	6.35	12.01	13.25

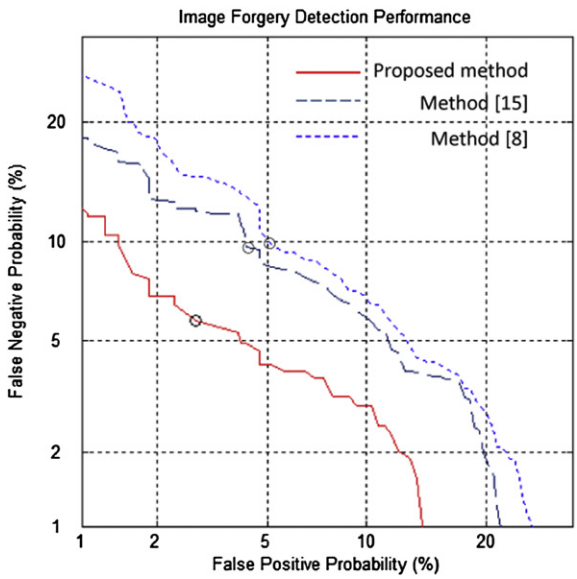

Fig. 11. DET curve for image forgery detection using the three methods with copy move forgery with/without rotation and with Q factor of 100.

Table 3
Comparison of performances between the three methods with copy move forgery with/without rotation and with Q factor of 100.

	Proposed method	Method of Li et al. (2007)	Modified method of Mahdian and Saic (September 2009)
False positive (%)	3.52	4.67	5.1
False negative (%)	6.92	9.91	9.98
EER (%)	4.81	7.62	8.03

positive rate is greater than 10% when the value of the pair <*Th1*, *Th2*> is higher than <0.5, 0.8> and <0.7, 0.7>. False positive rate has the similar behavior when the proposed method is applied on the three color arrays.

Table 1 gives a comparison between the proposed method with gray scale conversion and the methods of Li et al. (2007) and modified Mahdian and Saic (September 2009) in terms of detected forged blocks out of 1148. It should be mentioned that although (Li et al., 2007) shows comparable performance to the proposed method, it suffers from many false positives. The results shown with the proposed method use $Th1 = 0.7$ and $Th2 = 0.3$ that give the best accuracy, which is 95.9%. The proposed method also has the least false positive rate (4.54%) and false negative rate (6.67%).

Example results using gray scale conversion of two other test images are shown in Fig. 9 and Fig. 10.

Table 2 shows a comparison between the proposed method with the three color arrays and the methods of Li et al. (2007) and modified (Mahdian and Saic, September 2009). The thresholds are $Th1 = 0.7$ and $Th2 = 0.3$. For a fair comparison, methods (Li et al., 2007) and modified (Mahdian and Saic, September 2009) are also applied on the three color components. Comparing the results in Table 1 and Table 2, it can be found that applying the proposed method on the three color components significantly improves accuracy and decreases false positive rate and false negative rate. The accuracy of the proposed method reaches as high as 98.34%, which is far better than those of method (Li et al., 2007) (92.94%) and modified method (Mahdian and Saic, September 2009) (82.84%).

4.2. Copy-move forgery with/without rotation and with Q factor of 100

In this experiment, in addition to the images used in Section 4.1, 160 images (80 genuine and 80 copy move forged) from CASIA v1.0 Tampering Detection Evaluation Dataset (CASIA, 2009) were used. We chose 80 forged images in such a way that they correspond to copy move on the same image (not splicing), and without or with rotation less than 20°. The image sizes of CASIA v1.0 dataset are 374 × 256.

The results are given in Fig. 11 as Detection Error Tradeoff (DET) curve and in Table 3. The results are obtained using the three color arrays. 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 (Eq. (4)):

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

where, $C_{\text{False Negative}}$ and $C_{\text{False Positive}}$ are relative costs of detection errors P_{Forged} is *a* priori probability of the specified forged image. In the experiments, $C_{\text{False Negative}}$ and $C_{\text{False Positive}}$ are set to 1 and P_{Forged} to 0.5. Minimum cost is denoted as a small circle on the DET curve. In Table 3, EER (equal error rate) is defined as the point where false positive rate and false negative rate are equal.

From Fig. 11 and Table 3, we can see that the proposed method shows better performance than the methods in Li et al. (2007) and Mahdian and Saic (September 2009) even in case of large image size and forgery where rotation took place before pasting. At the point of minimum cost function, false positive rate and false negative rate of the proposed method are 3.52% and 6.92%, respectively. The proposed method has EER of 4.81%, which is much lesser than that obtained by method (Li et al., 2007) (EER = 7.62%) and method (Mahdian and Saic, September 2009) (EER = 8.03%).

4.3. Copy-move forgery with Q factor less than 100

In this experiment, the images in Section 4.1 were used except that the forged images were saved in JPEG format with Q factor of 90, 80, and 60 (i.e., three versions of each forged image). The results, which are obtained using the three color arrays, are shown in Table 4. The EER of the proposed method in the case of Q factor of 90, 80, and 60 is 3.56%, 4.02%, and 6.38%, respectively. These EERs are significantly lower than those using the methods (Li et al., 2007) and (Mahdian and Saic, September 2009). The results suggest that the proposed method works well even the Q factor is less.

Table 4
Comparison of performances between the three methods with copy move forgery with different Q factors in JPEG format.

	Proposed method			Method of Li et al. (2007)			Modified method of Mahdian and Saic (September 2009)		
Q factor	90	80	60	90	80	60	90	80	60
False positive (%)	4.26	4.93	7.74	9.61	10.03	12.89	9.98	10.53	13.54
False negative (%)	6.47	7.01	9.52	12.27	13.27	15.59	13.42	13.84	16.71
EER (%)	3.56	4.02	6.38	9.45	10.29	13.58	11.45	12.43	16.42

5. Conclusion

We proposed a blind copy move image forgery detection method based on DyWT. We utilized both the LL1 and HH1 subbands to find similarities and dissimilarities between the blocks of an image for robust detection of copy move. The method was evaluated in three test cases: (a) fixed size images and forgery without rotation, (b) different size images and forgery with or without rotation, and (c) different Q factors JPEG images. In the experiments, the proposed method performed significantly better than some of the previous methods in all the three cases.

In a future study, we wish to extract some statistical features from each block in LL1 and HH1, and compute the similarity. The features may include different order moments and transition probabilities between the coefficients of LL1 and HH1.

Acknowledgment

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

Bayram S, Sencar HT, Memon N. An efficient and robust method for detecting copy-move forgery. In: Proc. ICASSP09; 2009. p. 1053–6.

CASIA image tampering detection evaluation database (CASIA TIDE) V1.0. 2009. Available at: http://forensics.idealtest.org.

Chen M, Fridrich J, Goljan M, Lukas J. Determining image Origin and integrity using sensor noise. IEEE Transactions on Information Forensics and Security 2008;3(1):74–90.

Coifman R, Donoho D. Translation invariant de-noising. In: Wavelets and statistics; 1995. p. 125–50.

Farid H. Exposing digital forgeries from JPEG ghosts. IEEE Transactions on Information Forensics and Security 2009;4(1):154–60.

Farid H. Image forgery detection – a survey. IEEE Signal Processing Magazine March 2009;5:16–25.

Fridrich J, Soukal D, Lukas J. Detection of copy-move forgery in digital images. In: Proc. digital forensic research workshop. IEEE Computer Society; August 2003. p. 55–61.

Huang H, Guo W, Zhang Y. Detection of copy-move forgery in digital images using SIFT algorithm. In: Proc. IEEE Pacific-Asia workshop on computational Intell. Industrial app; 2008. p. 272–6.

Li G, Wu Q, Tu D, Sun S. A sorted neighborhood approach detecting duplicated forgeries based on DWT and SVD. In: Proc. ICME2007; 2007. p. 1750–3.

Lin WS, Tjoa SK, Zhoa HV, Liu JR. Digital image source coder forensics via intrinsic fingerprints. IEEE Transactions on Information Forensics and Security Sept 2009;4(3):460–75.

Mahdian B, Saic S. Detection of copy-move forgery using a method based on blur moment invariants. Forensic Science International 2007; 171(2–3):180–9.

Mahdian B, Saic S. A bibliography on blind methods for identifying image forgery. Signal Processing: Image Communication 2010;25:389–99.

Mahdian B, Saic S. Blind authentication using periodic properties of interpolation. IEEE Transactions on Information Forensics and Security September 2008;3(3):529–38.

Mahdian B, Saic S. Using noise inconsistencies for blind image forensics. Image and Vision Computing September 2009;27(10):1497–503.

Mallat S, Zhong S. Characterization of signals from multiscale edges. IEEE Transactions on Pattern Analysis and Machine Intelligence July 1992; 14:710–32.

Mallat S. A wavelet tour of signal processing: the sparse way. 3rd ed. Academic Press; 2009.

Muhammad G, Hussain M, Khawaji K, Bebis G. Blind copy move image forgery detection using dyadic undecimated wavelet transform. In: Proc. 17th digital signal processing (DSP) conference, Corfu, Greece; July, 2011.

Popescu AC, Farid H. Exposing digital forgeries by detecting duplicated image regions. Dept. of Computer Science, Dartmouth College; 2004. Technical report.

Rey C, Dugelay JL. A survey of watermarking algorithms for image authentication. EURASIP Journal on Applied Signal Processing; 2002: 613–21.

Solario SB, Nandi AK. Passive forensic method for detecting duplicated regions affected by reflection, rotation, and scaling. In: Proc. EUSIPCO09; 2009. p. 824–8.

Starck Jean-Luc, Fadili Jalal, Murtagh Fionn. The undecimated wavelet decomposition and its reconstruction. IEEE Transactions on Image Processing 2007;16(2):297–309.

Sutcu Y, Coskun B, Sencar HT, Memon N. Tamper detection based on regularity of wavelet transform coefficients. IEEE Transactions on Image Processing; 2007.

Swaminathan A, Wu M, Liu KJR. Digital image forensics via intrinsic fingerprints. IEEE Transactions on Information Forensics and Security March 2008;3(1):101–17.

Yeung MM. Digital watermarking. ACM Communications 1998;41(7):30–3.

Zhang J, Wang H, Su Y. A new approach of detecting copy-move forgery in digital images. In: Proc. IEEE Int. conf. on communication systems 2008; 2008. p. 362–6.

Zhang C, Cheng LL, Qiu Z, Cheng LM. Multipurpose watermarking based on multiscale curvelet transform. IEEE Transactions on Information Forensics and Security December 2008;3(4):611–9.