Image Forgery Detection Using Multi-Resolution Weber Local Descriptors

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

[1] Department of Computer Science,[2] Department of Computer Engineering
College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[3]Department of Computer Science and Engineering, University of Nevada at Reno, USA
[*] ghulam@ksu.edu.sa

Abstract— **In this paper, a multi-resolution Weber law descriptors (WLD) based image forgery detection method is introduced. Due to the maturing of digital image processing techniques, there are many tools, which can edit an image easily without leaving obvious traces to the human eyes. So the authentication of digital images is an important issue in our life. The proposed multi-resolution WLD extracts the features from chrominance components, which can give more information that the human eyes cannot notice. A support vector machine is used for classification purpose. The experiments are conducted on a large image database designed for forgery detection. The experimental results show that the accuracy rate of the proposed method can reach up to 93.33 % with multi-resolution WLD descriptor on the chrominance space of the images.**

Keywords: image forgery detection, Weber local descriptor, splicing forgery, copy-move forgery, multi-resolution method

I. INTRODUCTION

Nowadays, we are living in an age, where digital imaging has grown and developed to become the widespread technology. It plays a significant role in human life, where the digital images are currently allowed as official documents that can be used in daily newspapers, magazines, military, and may be used as proof at court or in the medical diagnose field [1]. With the increasing applications of digital imaging, different types of software are introduced for image processing. Such software can do an alteration in digital image by changing blocks of an image with no showing the effect of the modification in the forged image. These modifications cannot be noticed by human eyes. The image forgeries can wipe off an important object from a proof image which can be a reason for miscarriage the court. Therefore, the security of digital images is a very important topic of research.

Many techniques have been developed for authenticity guarantee of the digital images. These techniques can be divided into intrusive (active) and non intrusive (blind or passive). The active techniques can be classified into two categories. The first one needs to embed a watermark in the image, while the second is a digital signature-based technique. In these methods, particular data is embedded in the digital images for supporting multimedia digital authentication and rights safety. If the image contents have been modified, the embedded data will be changed too. The image authenticity is done by checking whether the true signature corresponds to the signature that is retrieved from the suspicious test image. These techniques are restricted because of the inability of many digital cameras to embed the signature. Due to the restrictions of active techniques, which involve pre-processing in order to create the labeled images, the researchers tend to develop non intrusive techniques for validating the authenticity of digital images. These techniques examine images with no embedded data such as signatures or watermarks, and result whether these images are authentic or tampered.

The most commonly used forgery is copy-move forgery (CMF), where a region of an image is copied and moved to another region in the same image to make region-duplication in order to conceal an important object from the original image. The copied block may be changed by any kind of preprocessing procedures such as rotation, scaling, additive noise etc. to suit the copied area with the whole image. In another type of forgery, one part of an image is copied and pasted it in another image. This type of forgery is called splicing. In this paper, we propose a multi-resolution Weber law descriptor based method to detect image forgery. The forgery can be either copy-move or spliced. The proposed method is evaluated on different types of post-processing in forgery on a large image database.

The rest of the paper is organized as follows. Section 2 reviews some related previous work, Section 3 presents the proposed image forgery detection method, Section 4 gives experimental results with discussion, and finally, Section 5 draws some conclusion.

II. RELATED PREVIOUS WORK

An improved DCT (discrete cosine transform)-based technique was proposed in [2] to discover CMF in digital images without any previous information of the suspicious image. The image is subdivided into blocks and the DCT is computed. The DCT coefficients are lexicographically sorted, and compared with different blocks. The proposed technique is robust against JPEG compression, additive white Gaussian noise, or blurring distortion. Cao *et al* [3] proposed an improved DCT-based method to locate the duplicated regions in a given image. The method uses circle block for representing DCT coefficient's array.

Noise pattern based image forgery detection method was proposed in [4]. Noise pattern is obtained by subtracting the

978-1-4673-2232-4/13/$31.00 ©2013 IEEE

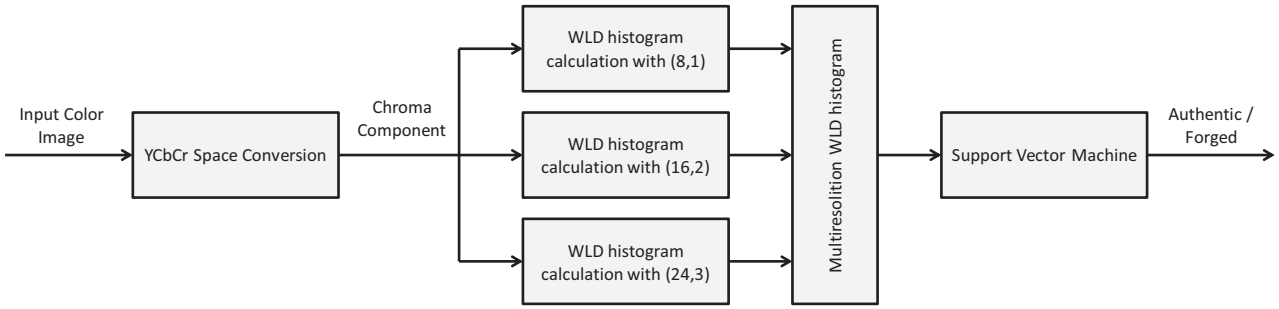


Fig. 1. Block diagram of the proposed image forgery detection method.

denoised image (after applying filter) from the input image. Then, histograms of noise from different segments of the image are compared to find the distortion caused by image forgery. Peng *et al* [5] also used sensor pattern noise to detect image forgery. Instead of using the histogram, they use four statistical measures, namely, variance, entropy, signal-to-noise ratio, and average energy gradient, from the noise pattern.

He *et al* in [6] proposed a method relied on approximate run length (ARL) to detect CMF. Firstly, the edge-gradient array of a given image is calculated, and then the ARL is computed along the edge-gradient orientation. After that, some features are extracted from the histogram of ARL. Support vector machine (SVM) is used to classify the spliced and authentic images by using the constructed features. Zhao *et al* used chrominance spaces with RLRN (run-length run-number) for CMF detection [7]. The input color image is transformed into the YCbCr color mode. Then RLRN is used to extract the features from the de-correlation of the chrominance channels. First 15 RLRN of each de-correlated image are extracted as a feature vector; so there are 60 dimensional features vector with four directions in each channel. SVM was used for classification purpose. This method gave better performance with JPEG image format than the TIFF image format. It did not provide any study about detection rate when the image went under post-processing operations.

Undecimated wavelet transforms (UWT) based image forgery detection was proposed in [8]. Approximation and detailed coefficients of the UWT from overlapping blocks of an image are used to find the similarity between the blocks. The method is robust against JPEG compression and a certain degree of rotation and scaling. Scale invariant feature transform (SIFT) based forgery detection methods are proposed in [9, 10, and 11]. They are quite robust against rotation and scaling post-processing.

Though different techniques for image forgery detection are proposed in the literature, none of them are fully capable of detecting the forgery under all types of post-processing. Two good surveys can be found in [12, 13].

III. PROPOSED METHOD FOR IMAGE FORGERY DETECTION

Fig. 1 shows a block diagram of the proposed copy-move image forgery detection system. In the first step, input color image is converted into the YCbCr color mode that stores the color in form of its brightness (luminance) and hue (chrominance), where human eyes are less sensible to chrominance component than luminance. In the second step, the chrominance component (either Cb or Cr) is used to extract image features. In the proposed method, Weber local descriptor (WLD) [14] based on Weber Law is used in the texture feature of an image. Multi-resolution WLD system is introduced where the histograms from different operators of variation (P, R) are concatenated and used to represent the image features; P is the count of the neighbors, and R is the spatial-resolution for the operator. The multi-resolution WLD can give better discrimination than the single resolution. In the last step, SVM based classifier is used to classify the input image as either authentic or forged.

A. Converting RGB image into chrominance components

Image forgers generally do image tampering in RGB color-space and attempt to wrap manipulated traces. For detecting the copy-move forgery in a digital image, the chrominance spaces (CSs), which are considered an efficient way for detecting forged images, are introduced in this paper. The input color image is transformed into CSs representations. The CSs are formed by subtracting luminance from red (Cr = R-Y) and by subtracting luminance from blue (Cb = B-Y).

YCbCr color space stores the color in terms of its luminance and chrominance, where the human eyes are less sensitive to chrominance than luminance. Even the tampered image looks natural, but some tampered traces are left in the chrominance channels. So the chrominance components are used to see if the feature extraction methods are more sensitive to forged images [7]. Fig. 2 shows an example of a color image and its luminance and chrominance components.

B. Feature extraction

The feature extraction is an important step in a pattern recognition system. It is used to analyze the image where the forged image features differ from the natural image features. In the proposed method, a multi-resolution WLD based features are used to detect image forgery.

WLD is a robust local descriptor, which is based on the fact that human sensitivity of a sample relies on the change of

the original stimulus intensity [14]. WLD which is texture descriptor used to extract features from an image. It has many advantages such as edge detection, and it is robust to illumination and noise change. WLD descriptor is described below for features extraction purpose. WLD based on Weber's law has two components: differential excitation (D) and orientation (Φ). An explanation for them is provided, and then WLD histogram is calculated for a given image.

Ernst Weber viewed that the ratio of the increase threshold to the intensity of the background is a constant. The Weber's law formula is:

$$\frac{\Delta x}{x} = C \qquad (1)$$

Where Δx is the increase threshold (noticeable distinction for discrimination), x indicates the initial stimulus-intensity, and C points to that the ratio on the left-side of the equation is constant in spite of variations in the x term.

A differential excitation (D) is used to change the intensity of each pixel in an image. The $D(p_c)$ for a pixel p_c is calculated as follows:

Step1: Compute the difference between the pixel p_c and its neighbours via the filter (f_{00}) in Fig. 3.

$$k_s^{00} = \sum_{i=0}^{N-1}(\Delta p_i) = \sum_{i=0}^{N-1}(p_i - p_c) \qquad (2)$$

where p_i is the ith neighbour of pixel p_c and N is the number of neighbours.

Step2: Calculate the proportion of the differences to the current pixel intensity by the outputs of the filter (f_{00}) and (f_{01}) in Fig. 3.

$$I = \frac{k_s^{00}}{k_s^{01}} = \sum_{i=0}^{N-1}\left(\frac{p_i - p_c}{p_c}\right) \quad (3).$$

Thus, the differential excitation $D(p_c)$ of the current pixel p_c is

$$D(p_c) = \arctan\left[\sum_{i=0}^{N-1}\left(\frac{p_i - p_c}{p_c}\right)\right] \quad (4).$$

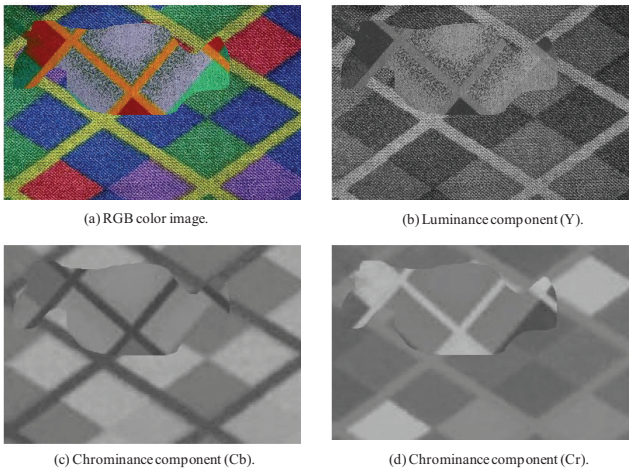
WLD orientation component is the gradient orientation and it is calculated as follows:

Compute the Φ (p_c)

$$\Phi(p_c) = \arctan\left(\frac{k_s^{11}}{k_s^{10}}\right) \qquad (5)$$

where, k_s^{11} and k_s^{10} are the outputs of the filters f_{11} and f_{10} filters.

Later, Φ is mapped to Φ' and is quantized into T dominant directions. After calculating differential excitation and gradient orientation, WLD histogram is formed. In WLD histogram, there are three parameters that affect on optimizing the results: the number of dominant orientations (T), the number of differential excitation segments (M), and the number of bins in sub histogram segments Hm,t (S).



(a) RGB color image. (b) Luminance component (Y). (c) Chrominance component (Cb). (d) Chrominance component (Cr).

Fig. 2. RGB color image and its luminance and chrominance components.

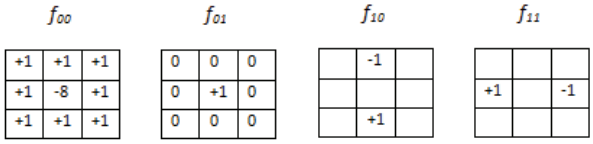


Figure 3. Filters used in WLD calculation.

In the proposed multi-resolution WLD, differential excitation and gradient orientation are calculated in three different neighborhoods, which are (8,1), (16,2), and (24,3), where the first component inside the parenthesis corresponds to the number of neighboring pixels and the second component is the radius of the neighbors from the center pixel. The histograms from these three neighborhoods are fused to produce the multi-resolution WLD histogram.

C. Classification

SVM is employed for tampered image detection, which is a two-class problem [15]. SVM is a machine learning technique that involves training and testing stage; so the features are fed in SVM for classification. SVM classifier can give good performance with radial basis function (RBF) kernel. With the two-class problem, training patterns (a_i, b_i) are given where i = 1, 2, …, M, $a_i \in R_d$, $b_i \in \{-1,+1\}$, a_i is a feature vector of the training set, and b_i is the label of a class, −1 and +1 point to the two classes C_1 and C_2. The aim is to build a classifier from the existing patterns that minimize the probability of misclassification of a novel pattern. SVM builds an optimal hyper-plane $g(a) = C^T x + C_0 = 0$ that locates the maximum margin for classification with better generalization performance. The margin is defined as the separated distance between the nearest data points of each class and the hyper-plane. Many kernel functions are used for different classifying problems. RBF kernel is employed in the experiments of the paper.

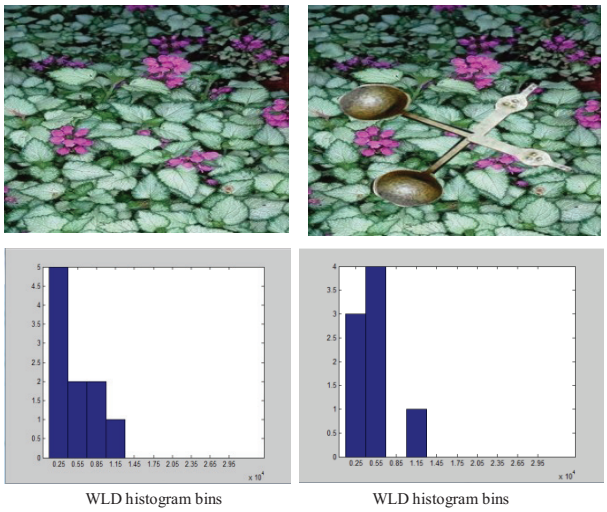


Fig. 3. The histograms of multi-resolution WLD using Cr chrominance component for (a) authentic and (b) spliced images.

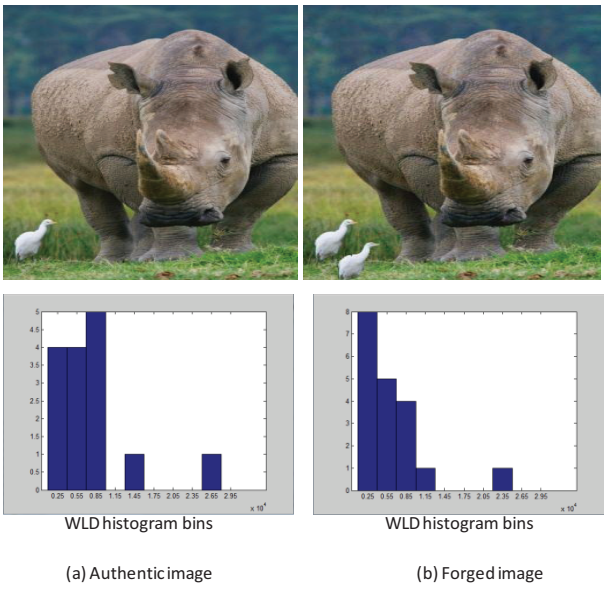


Fig. 4. The histograms of multi-resolution WLD using Cr chrominance component for (a) authentic and (b) copy-moved forged images without doing anything on the copied region.

Fig. 3 shows histograms of multi-resolution WLD (all three neighborhoods combined) of an authentic image and a spliced image using Cr channel. The multi-resolution WLD histograms using Cr chrominance component for authentic and corresponding copy-move forged images without doing anything on the copied region are illustrated in Fig. 4. Similarly, the histograms with rotation on the copied region are given in Fig. 5.

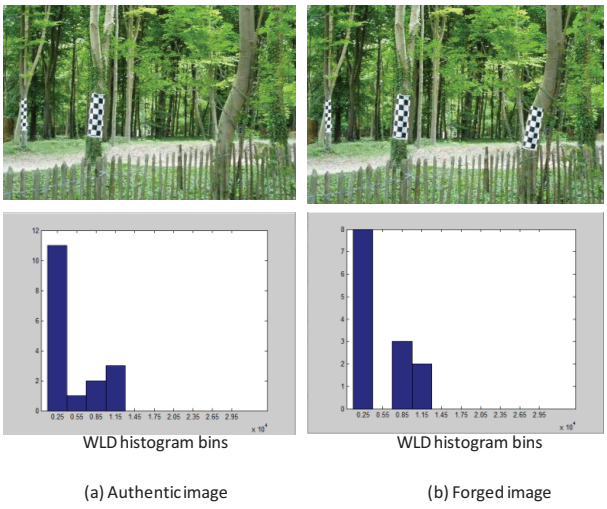


Fig. 5. The histograms of multi-resolution WLD using Cr chrominance component for (a) authentic and (b) copy-move forged images with doing rotation on the copied region.

IV. EXPERIMENTS

This study uses CASIA TIDE V1.0 Dataset [16] for evaluating the proposed copy-move image forgery detection method. All images have 384×256 size and they are in JPEG format. The original images are split into eight groups: animal, scene, character, plant, nature, architecture, texture and article. The authentic images from every group were arbitrarily chosen to create the tampered images. The tampering was done by cut-and-paste process; also several geometric transformations such as rotation, resizing, etc. were applied in some copied regions. The tool that was used to generate the tampered images was Adobe Photoshop. There are two types of forgery in the database, spliced and copy-moved. In the spliced set, there are 390 authentic and 459 tampered images. For copy-move forgery case, there are 261 authentic images and 462 tampered images.

The performance of the method is given in terms of specificity, sensitivity, and accuracy. Sensitivity is a measure of classification accuracy of true cases (i.e. an authentic image is classified as the authentic image and a tampered image is classified as the tampered image) and is calculated as

$$\text{Sensitivity (Sn)} = (100 * TP / (TP + FN)) \quad (6)$$

Specificity is a measure of classification accuracy of false cases and is calculated as

$$\text{Specificity (Sp)} = (100 * TN / (FP + TN)) \quad (7)$$

Accuracy is percent ratio between correctly classified images over total number of images, and is expressed as

$$\text{Accuracy} = 100 * (TP + TN) / (TP + TN + FN + FP) \quad (8)$$

where TP (true positive) is the number of tampered images which are classified as tampered images, FN (false negative) is the number of tampered images misclassified as authentic images, FP (false positive) is the number of authentic images misclassified as tampered images, and TN (true negative) is the number of authentic images, which are correctly classified as authentic images.

Firstly, the RGB images are converted to YCbCr color space. Then the WLD features are extracted from each chrominance component. Different scales with different number of points in the neighborhood and the radius of the neighborhood are used, where C1 means (8, 1), C2 corresponds (16, 2), C3 refers to (24, 3), C4 is a combination of (8, 1) and (16, 2), C5 is a combination of (8, 1) and (24,3), C6 is a combination of (16, 2) and (24, 3), and finally, C7 is the combination of all the scales (8, 1), (16, 2) and (24, 3).

Performance of SVM classification by employing RBF kernel function has been evaluated using 10-fold cross validation to validate the methods.

A) Effect of WLD Parameters

Fig. 6 shows the effects of T, M, S parameters of WLD on the detection accuracy in C7 using Cr channel. From (T, M, S) = (4, 4, 20) setup, two parameters are fixed and the other one is variable. In the first row of Fig. 6, we see that T = 4 gives the best result, and from the second row, we find that increasing M values decrease the accuracy; while in the third column, we observe that S = 20 provides the best result. In the subsequent experiments, we fix the parameters as (T, M, S) = (4, 4, 20).

B) Results on Splicing Detection

Fig. 7 demonstrates the splicing detection accuracy of Cr and Cb chrominance channels in different scales (resolutions) of WLD. Cr performs better than Cb in all the possible scales and their combinations. For individual scale (C1, C2, C3), C2 (16, 2) performs the best. In case of multi-scale, C7, which is the combination of all the three scales, has the highest detection accuracy. With Cr channel, C7 achieves 91.54% accuracy, and with Cb channel, it obtains 89.88% accuracy. Therefore, it is experimentally proved that multi-resolution WLD performs better than single scale WLD in case of image forgery detection. Each single scale WLD produces 320 features (bins in the histogram), so C7 has a total of (320×3=) 960 features.

In the next experiment, Cr and Cb histograms are combined to see the accuracy in C7 case. Table I gives the complete results of individual chrominance component, their concatenated version, and luminance component. The combined chrominance component gives the best accuracy of 93.33%, and the best area under curve (AUC) of 0.93.

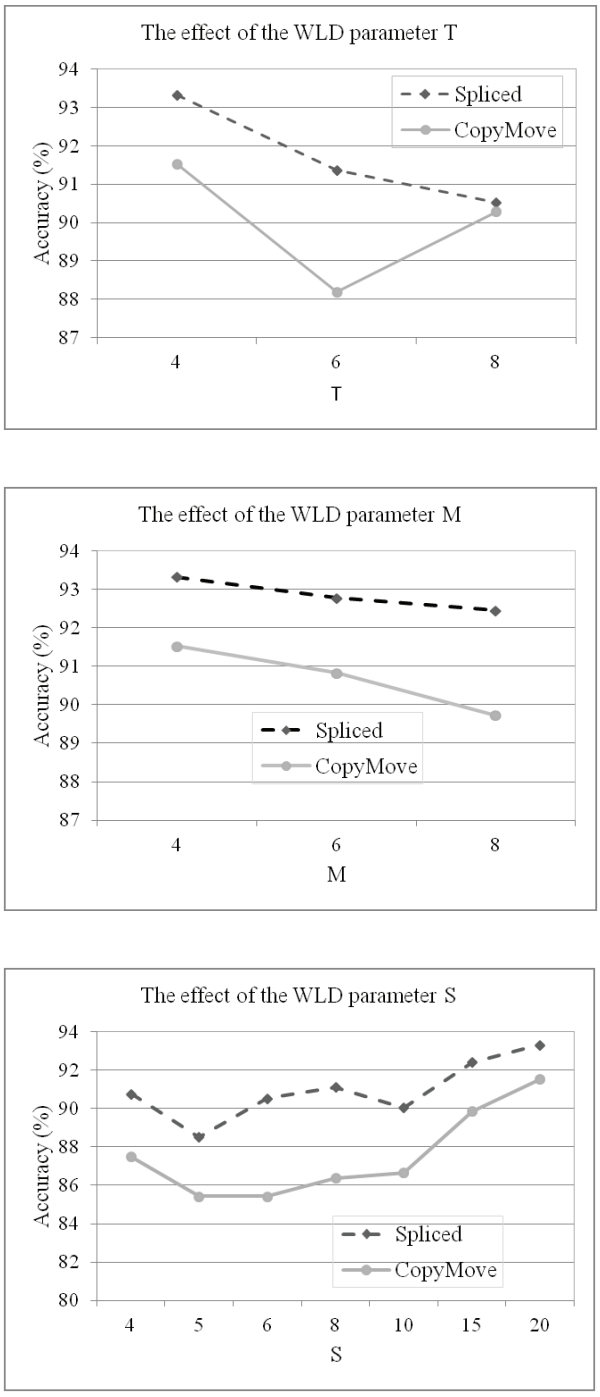


Fig. 6. Effects of T, M, S parameters (top, middle, and bottom row, respectively) of WLD on forgery detection using Cr chrominance component and multi-scale C7.

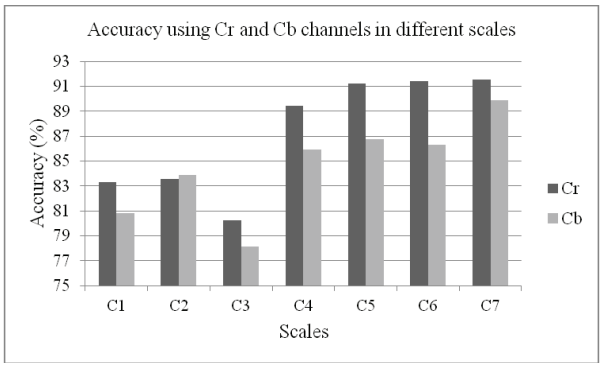


Fig. 7. Accuracy of splicing detection using chrominance channels in different scales of WLD.

TABLE I. PERFORMANCE OF DIFFERENT CHANNELS WITH COMBINED SCALES (C7) OF WLD IN SPLICING DETECTION.

Channel	%Acc	AUC	Sn	Sp	#features
Cr	91.54	0.90	92.66	90.35	960
Cb	89.88	0.89	90.89	88.69	960
Cr + Cb	**93.33**	0.93	92.95	93.70	1920
Y	53.57	0.48	93.56	6.92	960

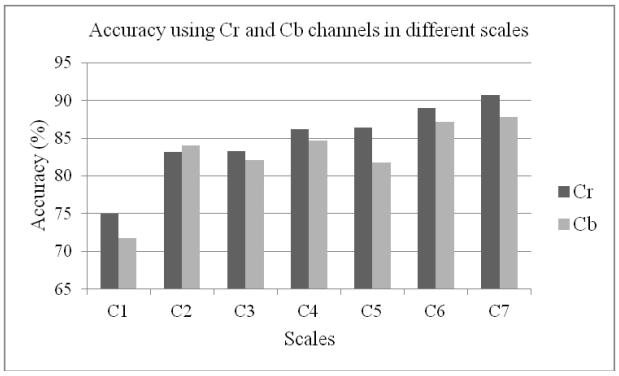


Fig. 8. Accuracy of copy-move detection using chrominance channels in different scales of WLD.

TABLE II. PERFORMANCE OF DIFFERENT CHANNELS WITH COMBINED SCALES (C7) OF WLD IN COPY-MOVE DETECTION.

Channel	%Acc	AUC	Sn	Sp	#features
Cr	90.69	0.88	95.89	81.01	960
Cb	87.77	0.84	94.09	76.74	960
Cr + Cb	**91.52**	0.88	96.81	82.23	1920
Y	68.33	0.59	93.43	24.35	960

C) Results on Copy-Move Forgery Detection

Fig. 8 shows the copy-move forgery detection accuracy of Cr and Cb chrominance channels in different scales of WLD. Cr performs better than Cb in most of the scales and their combinations. In case of multi-scale, C7 has the highest detection accuracy. With Cr channel, C7 achieves 90.69% accuracy, and with Cb channel, it gives 87.77% accuracy. If we compare Fig. 7 and Fig. 8, we find that copy-move forgery detection has lower accuracy than splice detection. This can be attributed to the fact that in copy-move forgery, the hidden noise pattern remains almost same, while in splicing there are two different background patterns as they come from two different images. So, it is comparatively easier to detect splicing than copy-move forgery.

Table II gives the complete results of individual chrominance component, their concatenated version, and luminance component in copy-move image forgery detection using C7. The combined chrominance component gives the best accuracy of 91.52%, and area under curve (AUC) in this case is 0.88.

D) Results on Forgery Detection Based on Transformation

Table III illustrates the results of multi-resolution WLD (C7) for splicing forgery based on transformation of the copied region with chrominance components. There are four types of transformations: (a) deform the copied region before pasting, (b) resize the copied region before pasting, (c) rotate the copied region before pasting, and (d) no transformation. Column 2 of Table III shows the number of authentic (Au) and forged (Fg) images that fall into the corresponding transformation category in the database. From the table, we find that rotation gives the least accuracy of 77.14%, while resize gives the best accuracy of 90.58%. However, this trend might be related to the number of images in the category.

Table IV gives the results of copy-move forgery detection based on transformation. The highest accuracy of 90.98% is achieved with no transformation.

TABLE III. PERFORMANCE FOR IMAGE SPLICING DETECTION BASED ON TRANSFORMATION USING C7.

Type	#images (Au / Fg)	Channel	%Acc	AUC
Deform	39 / 41	Cr	87.5	0.82
		Cb	81.25	0.79
		Cr + Cb	86.25	0.80
Resize	165 / 183	Cr	90	0.90
		Cb	84.70	0.85
		Cr + Cb	90.58	0.90
Rotate	18 / 18	Cr	62.58	0.51
		Cb	74.28	0.75
		Cr + Cb	77.14	0.76
Nothing	152 / 156	Cr	91	0.90
		Cb	84	0.83
		Cr + Cb	89	0.90

TABLE IV. PERFORMANCE FOR COPY-MOVE FORGERY DETECTION BASED ON TRANSFORMATION USING C7.

Type	#images (Au / Fg)	Channel	%Acc	AUC
Deform	12 / 12	Cr	75	0.61
		Cb	60	0.56
		Cr + Cb	55	0.51
Resize	23 / 23	Cr	66.66	0.63
		Cb	42.22	0.44
		Cr + Cb	62.22	0.64
Rotate	7 / 7	Cr	30	-
		Cb	30	-
		Cr + Cb	20	-
Nothing	204 / 406	Cr	90	0.87
		Cb	87.37	0.84
		Cr + Cb	90.98	0.87

TABLE V. PERFORMANCE FOR IMAGE SPLICING DETECTION USING C7 BASED ON THE SHAPE OF TAMPERED REGION.

Type	#images (Au / Fg)	Channel	%Acc	AUC
Arbitrary	372 / 425	Cr	92.40	0.92
		Cb	89.49	0.90
		Cr + Cb	92.65	0.93
Circular	12 / 12	Cr	80	0.81
		Cb	85	0.86
		Cr + Cb	95	0.9
Rectangular	21 / 21	Cr	75	0.84
		Cb	55	0.61
		Cr + Cb	75	0.71

TABLE VI . PERFORMANCE FOR COPY-MOVE FORGERY DETECTION USING C7 BASED ON THE SHAPE OF TAMPERED REGION.

Type	#images (Au / Fg)	Channel	%Acc	AUC
Arbitrary	111 / 110	Cr	87.27	0.88
		Cb	79.09	0.78
		Cr + Cb	82.27	0.81
Circular	102 / 102	Cr	79	0.77
		Cb	77.5	0.78
		Cr + Cb	80	0.80
Rectangular	148 / 148	Cr	82.41	0.80
		Cb	75.17	0.74
		Cr + Cb	80.43	0.80
Triangular	101 / 101	Cr	82.5	0.80
		Cb	77	0.73
		Cr + Cb	79.5	0.79

TABLE VII. COMPARISON OF ACCURACIES BETWEEN THE PROPOSED METHOD AND THE METHOD IN [17].

Type of forgery	Proposed method	Method in [17]
Splice	93.33%	79.90%
Copy-Move	91.52%	76.30%

E) Results on Forgery Detection Based on Shape of The Tampered Region

Table V and Table VI give accuracies of the proposed multi-resolution WLD method with C7 in different types of shapes of the copied regions in splicing and copy-move forgery detection, respectively. There are four shapes, (a) circular, (b) rectangular, (c) triangular (in case of copy-move only), and (d) arbitrary. In the case of splicing detection, 92.65% accuracy is obtained with arbitrary shape, while 95% and 75% accuracies are achieved with circular and rectangular shape, respectively. In the case of copy-move forgery detection, Cr performs better than the combined chrominance channels in most the shape cases.

F) Comparison with Method [17]

The proposed method is compared with another recent method [17] that also uses chrominance channels. Table VII gives the comparison results. In both splicing and copy-move forgery detection, the proposed method outperforms the method [17] on CASIA TIDE v1.0 database.

V. CONCLUSION

A multi-resolution WLD based image forgery detection method is proposed. WLD features are extracted from the chrominance channels of a color image. SVM is used for classification purpose. The proposed method achieved 93.33% and 91.52% accuracies in case of splicing and copy-move forgery detection, respectively when the chrominance channels are combined.

A future work will be to localize the forgery in a tampered image.

ACKNOWLEDGEMENT

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

REFERENCES

[1] B.L. Shivakumar and S. S. Baboo, “Detecting copy-move forgery in Digital images: A survey and analysis of current methods”, Global Journal of Computer Science and Technology, vol. 10, no. 7, 2010.

[2] Y. Huang, W. Lu, W. Sun, and D. Long, “Improved DCT-based detection of copy-move forgery in images”, Forensic science international, vol. 206, no. 1–3, pp. 178–184, 2011.

[3] Y. Cao, T. Gao, L. Fan, and Q. Yang, “A robust detection algorithm for copy-move forgery in digital images”, Forensic Science International, vol. 214, no. 1–3, pp. 33–43, Jan. 2012.

[4] N. Muhammad, M. Hussain, G. Muhammad, and G. Bebis, “A non-intrusive method for copy-move forgery detection”, Advances in Visual Computing, LNCS, Springer, pp. 516–525, 2011.

[5] F. Peng, Y. Nie, and M. Long, “A complete passive blind image copy-move forensics scheme based on compound statistics features”, Forensic Science International, 2011.

[6] Z. He, W. Sun, W. Lu, and H. Lu, “Digital image splicing detection based on approximate run length’”, Pattern Recognition Letters, pp. 1591–1597, 2011.

[7] X. Zhao, J. Li, S. Li, and S. Wang, “Detecting digital image splicing in chroma spaces”, Digital Watermarking, pp. 12–22, 2011.

[8] G. Muhammad, M. Hussain, and G. Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform," Digital Investigation, vol. 9, issue 1, pp. 49-57, 2012.

[9] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," IEEE Trans. Information Forensics and Security, vol. 6(3), pp. 1099-1110, 2011.

[10] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm", Proc. IEEE Pacific-Asia Workshop on Computational Intell. and Industrial Application, Volume: 2, pp. 272-276, Dec, 2008.

[11] H. Ling, H. Cheng, Q. Ma, F. Zou, and W. Yan, "Efficient image copy detection using multiscale fingerprints," IEEE Magazine of Multimedia, vol. 19(1), pp. 60-69, 2012.

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

[13] B. Mahdian and S. Saic, "A bibliography on blind methods for identifying image forgery," Signal Processing: Image Communication, vol. 25, pp. 389-399, 2010.

[14] J. Chen, S. Shan, C. He, G. Zhao, M. Pietikainen, X. Chen, and W. Gao, ‘WLD: A robust local image descriptor’, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 32, no. 9, pp. 1705–1720, 2010.

[15] N. Cristianini and J. Shawe-Taylor, *An Introduction to Support Vector Machines and Other Kernel-based Learning Methods*, Cambridge University Press, 2000.

[16] CASIA image tampering detection evaluation database (CASIA TIDE) V1.0, available at http://forensics.idealtest.org.

[17] W. Wang, J. Dong, and T. Tan, Image tampering detection based on stationary distribution of Markov chain', in 17th IEEE International Conference on Image Processing (ICIP), pp. 2101 – 2104, 2010.