Comparison between WLD and LBP Descriptors for Non-intrusive Image Forgery Detection

[1]Muhammad Hussain, [2]Sahar Q. Saleh, [2]Hatim Aboalsamh, [3]Ghulam Muhammad, and [4]George Bebis

[1]Department of Software Engineering, [2]Department of Computer Science, [3]Department of Computer Engineering
College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[4]Department of Computer Science and Engineering, [2]University of Nevada at Reno, USA
Email: {mhussain, hatim, ghulam}@ksu.edu.sa, bebis@cse.unr.edu

Abstract— **Due to the availability of easy-to-use and powerful image editing tools, the authentication of digital images cannot be taken for granted and it gives rise to non-intrusive forgery detection problem because all imaging devices do not embed watermark. We investigated the detection of copy-move and splicing, the two harmful types of image forgery, using textural properties of images. Tampering distorts the texture micro-patterns in an image and texture descriptors can be employed to detect tampering. We did comparative study to examine the effect of two state-of-the-art best texture descriptors: Multiscale Local Binary Pattern (Multi-LBP) and Multiscale Weber Law Descriptor (Multi-WLD). Multiscale texture descriptors extracted from the chrominance components of an image are passed to Support Vector Machine (SVM) to identify it as authentic or forged. The performance comparison reveals that Multi-WLD performs better than Multi-LBP in detecting copy-move and splicing forgeries. Multi-WLD also outperforms state-of-the-art passive forgery detection techniques.**

Keywords - Image forgery detection; Copy-move forgery; Splicing forgery; Weber local descriptor; Local binary pattern; Multiscale methods

I. INTRODUCTION

Nowadays, we are living in a technically advanced world, where capturing pictorial information of any event in the form of digital images has become very simple. Currently, digital images play significant role in our everyday life, where they are being used as means for capturing pictorial information and are being employed in various domains such as medical diagnosis, daily newspapers, magazines, and as an evidence at court or for insurance claims [1]. Because of the widespread applications of digital images, very powerful and easy-to-use image editing tools like Photoshop are available. Using these tools even a novice can alter the digital contents of a digital image without leaving any visible traces, which can be noticed by human eyes. The digital contents are often altered with illicit designs in mind by hiding or adding important information to an image. Therefore, the authenticity of digital images cannot be taken for granted, it needs verification and is an object for research. Copy-move forgery (CMF) is the most common type of image forgery; in this case one region is copied from one place and pasted to another place of the same image in order to conceal important information. Sometimes, the copied region is modified by pre-processing operations like scaling, rotation, adding noise, etc. to make it matching with the surrounding region so that the tempering is not visible. In another similar kind of forgery, a part is copied from one image and is pasted to a different image. This type of forgery is called image splicing.

Authenticating digital images is a very serious issue and so far the researchers developed many methods, which can mainly be classified into (1) intrusive (active) and (2) non-intrusive (blind or passive) techniques [2]. Further, intrusive methods can be divided into two classes based on (1) embedding a watermark and (2) incorporating digital signature in an image. In each of these techniques, a piece of information is integrated into digital images as an aid for authenticating digital contents and security rights. Once the digital contents of an image are changed, the incorporated information is also modified. The authenticity of an image is validated by ensuring that the embedded information is unaltered. Though these methods are robust, their domain of application is restricted because all digital cameras are not equipped with the feature of embedding digital signature. In addition, these methods need pre-processing for creating labeled images. These limitations and constraints of active methods motivated the research to propose non-intrusive methods for authenticating digital images. This class of methods do not take into consideration any kind of embedded information (such as watermarks or signatures) to validate the authenticity of a digital image. Instead, these methods draw their conclusions about the originality of the digital content of images using its structural changes, which take place due to tempering.

One kind of structural changes that takes place in the digital content due to tampering is the distortion in textural microstructures. Texture descriptors can be employed to encode this change [3]. Multi-WLD and multi-LBP are two state-of-the-art texture descriptors that are being used for texture description in various applications. In this paper, we present the findings of our comparative study of multi-WLD and multi-LBP descriptors for non-intrusive image forgery detection. The forgery can be either copy-move or spliced. Multi-WLD and multi-LBP features are extracted from the chrominance components of a color image. Feature subset selection is applied to reduce the dimension of the feature space and to select the most discriminatory features. SVM is used to identify whether an image is authentic or forged. We performed experiments on CASIA TIDE V1.0 dataset, which is a public domain benchmark database for image forgery detection. The performance comparison shows that multi-

978-1-4799-3020-3/14/$31.00 ©2014 IEEE

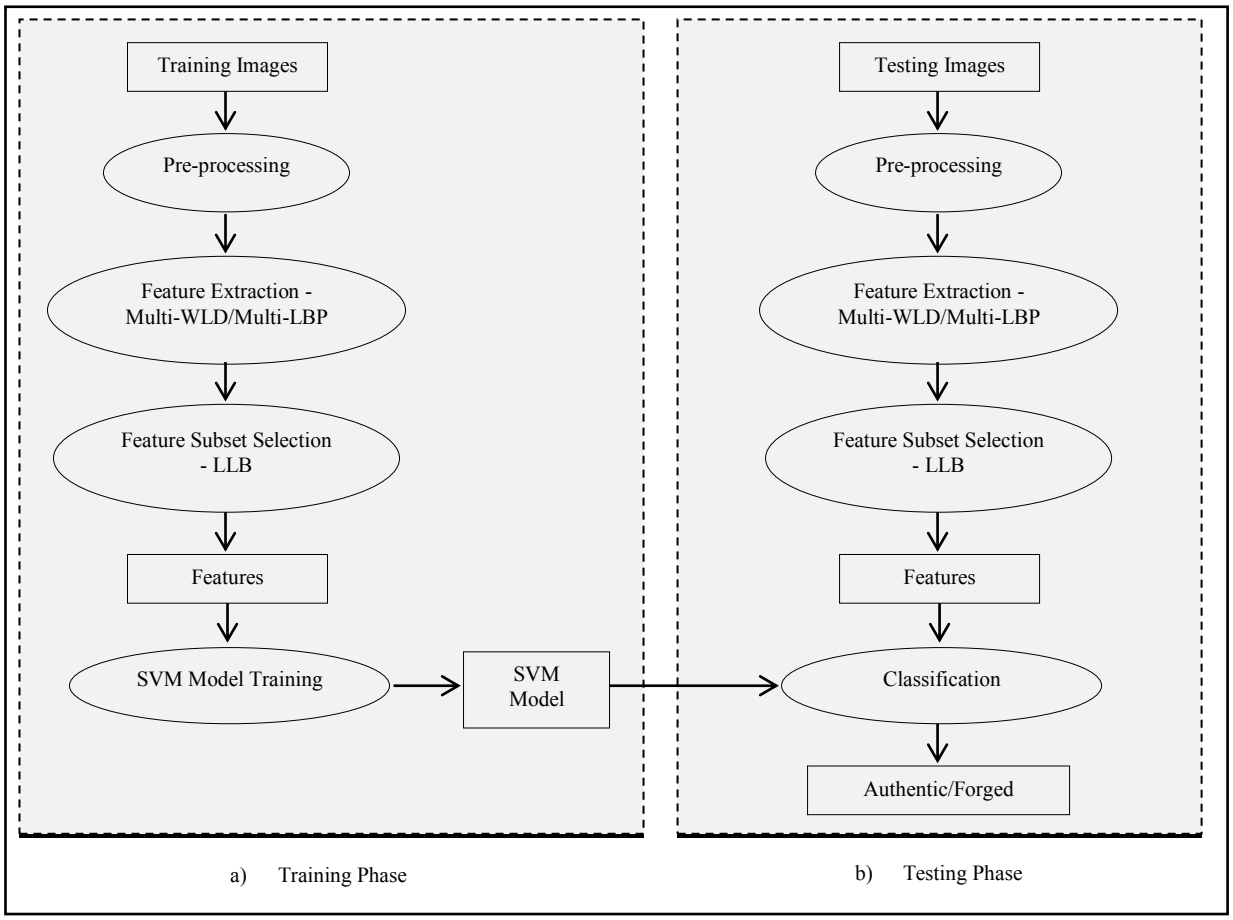


Fig. 1. A block diagram of the forgery detection System.

WLD achieves high detection rate for image forgery than multi-LBP.

The overall organization of the paper is as follows. Section II presents an overview of some related methods while Section III discusses the details of the image forgery detection technique. The experimental results with discussion have been given in Section IV and finally, Section V concludes the paper.

II. REALATED WORK

Non-intrusive image forgery detection research is focused on developing technologies to decide about the suspicious image if it is authentic or tampered. This research area emerged during the past few years and many techniques for digital image forgery detection have been introduced.

Huang et al. [4] proposed an image forgery detection technique for CMF using improved DCT. In this method, first an image is partitioned into square blocks, and then DCT is calculated. Later lexicographical order is used to sort the DCT coefficients and different blocks are compared using the sorted DCT coefficients. This technique is effective against additive Gaussian noise, JPEG compression and blurring distortion. Another method proposed by Cao et al. [5] is also based on improved DCT for locating the duplicated parts of a digital image. This method uses circular blocks for computing the DCT coefficients.

Muhammad et al. [6] introduced an image forgery detection method for CMF using noise pattern. In this method, first input image is denoised and then the denoised image is subtracted from the input image to estimate the noise pattern. The image is segmented and the noise histograms of different segments are used to detect the forged regions. The forgery detection method by Peng et al. [7] exploited sensor pattern noise. They used four statistical features (entropy, variance, average energy gradient and signal-to-noise ratio, and) of the noise for forgery detection.

He et al. [8] introduced a copy-move forgery detection method that relies on approximate run length (ARL). This method first computes edge-gradient array and then ARL along edge-gradient orientations. The forgery detection method proposed by Zhao et al. [9] uses chrominance components and RLRN (run-length run-number). In this method, first the transformation is applied to convert RGB image into YCbCr color system. RLRN is then employed for extracting features from chrominance components. SVM is used to identify whether the image is authentic or tampered. This method performs better on JPEG images than on TIFF images.

Muhammad et al. [10] used undecimated wavelet transform (UWT) for their image forgery detection method. Coefficients of low-frequency and high-frequency sub-bands

A) RGB color tampered image B) Luminance component (Y)

C) Chrominance component (Cb) D) Chrominance component (Cr)

Fig. 2. RGB color image with its chrominance components.

from UWT decompositions of overlapping blocks are used to compare blocks. This technique is robust against rotation and scaling (upto certain level) and JPEG compression.

Scale invariant feature transform (SIFT) was also employed for image forgery detection [11, 12, 13]. The methods based on SIFT are robust against scaling and rotation post-processing.

A splicing detection method was proposed by Shi et al. [14]. This method employs 1D and 2D statistical features and transition probability features determined from Markov chain computed in DCT domain. This method achieved an accuracy of 84.86% on CASIA v2.0 database [15]. Later, this method was improved by He et al. [16]; they combined transition probability features computed in DWT and DCT domains. Using SVM with recursive feature elimination (RFE), this method achieved an accuracy of 89.76% on CASIA v2.0 database. Two good surveys can be found in [2, 17].

Many non-intrusive forgery detection techniques have been introduced, but still the challenge is to develop more robust fully automatic methods to reduce false-positive rate.

III. FORGERY DETECTION SYSTEM

The forgery detection system is shown in the block diagram of Figure 1. There are two phases for the development of the system: training phase and testing phase. In the testing phase the system is modeled using training data and then it is tested using test data. The system involves 4 main components: preprocessing, feature extraction, feature subset selection and classification. In the following paragraphs, we give the detail of each of these components.

A. *Convertiom from RGB to YCbCr system*

Image tampering is done generally in RGB space and an attempt is made to hide the traces of forgery. For detecting copy-move or splicing forgery, the chrominance spaces (CSs) seem to be more effective. As such, first a digital image is transformed from RGB system to YCbCr system using the following transformation:

$$Y = 0.299\,R + 0.587\,G + 0.114\,B$$

$$Cr = 0.701\,R - 0.587\,G - 0.114\,B$$

$$Cb = -0.299\,R - 0.587\,G + 0.886\,B.$$

A digital image in RGB space and its corresponding YCbCr components are shown in Figure 2.

While tampering, the traces of forgery are made invisible. The human visual system is more sensitive to luminance component than chrominance components. It follows that the traces of forgery are left in chrominance components. As such, the chrominance components are suitable for extracting features that are sensitive to tampering traces [9].

B. *Feature Extraction*

To model the change that occurs in a digital image due to forgery is an essential step of a forgery detection system. Our assumption about this change is that it is distortion in texture micro-patterns and we use texture descriptors to model it. We employed two stat-of-art texture descriptors: multi-WLD and multi-LBP. In the following subsections, we give an overview of these descriptors.

1) *Multiscale WLD (Multi-WLD)*

WLD is one of the robust local texture features and is based on Weber's law [18]. It has many useful characteristics like edge detection and robustness to noise and illumination change.

WLD descriptor is determined using two important components: (1) differential excitation (*DE*) and (2) gradient orientation (*GO*). *DE* quantifies the relative intensity variation of each pixel using Weber's Law. The $DE(p_c)$ for a pixel p_c is calculated using the following equation:

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

where p_i is the i^{th} pixel in the neighbourhood of the pixel p_c and n is the number of its neighbouring pixels. Here, arctan function is used to control too quick changes which might be due to noise. For the whole image, *DE* is claculetd using the filters f_{00} and f_{01} shown in Figure 3.

GO component of WLD is representated by Φ. For pixel p_c, $\Phi(p_c)$ is calculated using the following equation:

$$\Phi(p_c) = \arctan\left(\frac{p_5 - p_1}{p_7 - p_3}\right) \quad (2)$$

where p_5 and p_1 are upper and lower neighbours of p_c and p_7 and p_3 are left and right neighbours of p_c. It can be calculted using the filters f_{11} and f_{10} shown in Figure 3. The range of Φ is $[-\pi/2, \pi/2]$ and it is mapped to Φ' so that its range is $[0, 2\pi]$. Then using quantization, it is mapped to T dominant orientations.

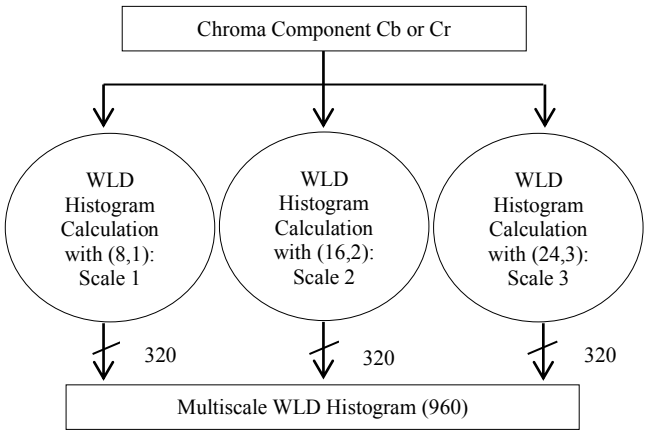


Fig. 4. Computing multi-WLD Histograms.

After computing *DE* and *GO* components, WLD histogram is claculated by binning the *DE* values according to dominant orientations. This histogram is refered to as WLD descriptor and it involves three parameters (T, M, S), where T, M, and S are, respectively, the numbers of dominant directions, differential excitation segments, and bins in sub-histogram segments, the detail can be found in [18].

f_{00}			f_{01}			f_{10}			f_{11}		
+1	+1	+1	0	0	0		-1				
+1	-8	+1	0	+1	0				+1		-1
+1	+1	+1	0	0	0		+1				

Fig. 3. Filters used in simple WLD calculation.

Simple WLD descriptor uses 3x3 square neighbourhood of the central pixel and cannot capture texture micro-structures existing with different scales. To encode the texure microstructures with different granularities, multiscale WLD descriptor is computed with symmetric square neighbourhoods (P, R) having P neighboring pixels and side (scale) of R pixels. For fogery detection, we employed three neighbourhoods with P = 8, 16, 24 and R = 1, 2, 3. The multi-WLD histogram is computed by fusing (using concatenation) the histograms calculated with these three neighborhoods, as shown in Figure 4.

2) *Multiscale LBP (Multi-LBP)*

LBP is a widely used local texture feature. It has very useful propetries like low computational cost and invarience to monotonic illumination changes and has been successfully applied for various applications. The LBP of a pixel p_c with circular neighbourhood (P, R), where P is the number of neighbour pixels on the circle of radius R around p_c, is represented by $LBP_{P,R}$ and claculated using the equation [19]:

$$LBP_{P,R} = \sum_{n=0}^{P-1} s(p_n - p_c)2^n \qquad (3)$$

where the thresholding operation $s(x)$ is defined as follows:

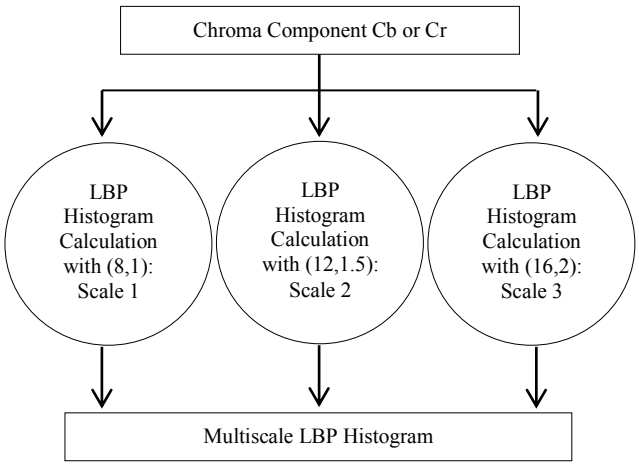


Fig. 5. Computing multi-LBP Histograms.

$$s(p_n - p_c) = \begin{cases} 1 & p_n - p_c \geq 0 \\ 0 & p_n - p_c < 0 \end{cases}$$

After computing LBP codes of all pixels, LBP histogram is calculated with 2^P bins. This histogram is referred to as LBP descriptor and used to represent an image.

Like multi-WLD, for capturing the texture micro-patterns of different granularities, multi-LBP descriptor is computed using three neighborhoods: (8, 1), (12, 1.5), (16, 2), for detail see Figure 5.

There are three variants of LBP operator: (1) rotation invariant LBP denoted by $LBP^{r_i}_{P,R}$, (2) uniform LBP denoted by $LBP^{u2}_{P,R}$, and (3) rotation invariant and uniform LBP denoted by $LBP^{r_iu2}_{P,R}$ [19].

The rotation invariant LBP $LBP^{r_i}_{P,R}$ is calculated using the following equation [19]:

$$LBP^{r_i}_{P,R} = \min\left\{RBS(LBP_{P,R}, i) \middle| i = 0,1,...,P-1\right\}$$

where $RBS(x, i)$ is a circular right bit shift operator that circularly right shifts i times bits of P bit number x. In case of P = 8, the number of distinct rotation invariant LBP codes is 36, and so $LBP^{r_i}_{P,R}$ descriptor is a histogram with 36 bins.

An LBP is termed as uniform LBP if there are at most two bitwise transitions from 0 to 1 or 1 to 0 in the binary code [19], e.g. 11111111, 11111000 and 00111100 are uniform LBP codes. In case of $LBP^{u2}_{P,R}$, histogram is calculated by putting distinct uniform LBP codes into corresponding bins and all non-uniform LBP codes in the same bin. When P = 8, the number of distinct uniform LBP codes is 58 and so $LBP^{u2}_{P,R}$ descriptor is a histogram with 59 bins.

In case of $LBP^{r_iu2}_{P,R}$, the histogram has only P+2 bins. For each variant of LBP, multi-LBP is computed to examine its effect on image forgery detection.

C. *Feature Subset Selection*

The presence of redundant features not only increases the computational overhead but also reduces the accuracy by misleading the classifier. For reducing the dimension of the

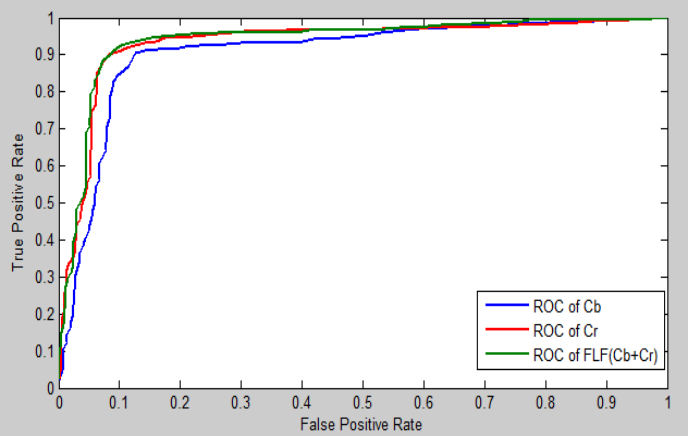


Fig. 6. ROC curves for splicing detection with multi-WLD.

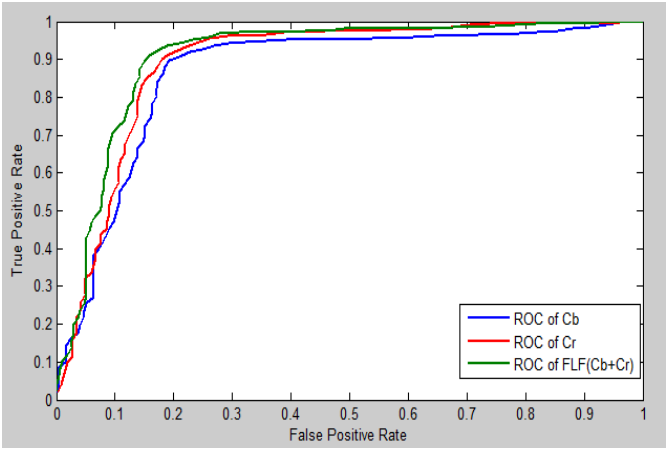


Fig. 7. ROC curves for copy-move forgery detection with multi-WLD.

feature space in each case, we employ Local Leaning Based (LLB) feature subset selection technique [20].

D. *Classification*

Image forgery detection is a two-class problem and in most of the applications, SVM, a two class classifier, has been shown to perform better than other classifiers [23]. As such, we employ SVM. Using the training data, SVM calculates the optimal hyper-plane that has maximum margin and ensures better generalization. Margin is defined as the sum of distances of the closest data points belonging the two classes to the optimal hyper-plane. SVM is basically a linear classifier but on the other hand most of the two-class problems are non-linear. To tackle this situation, kernel trick is used; employing a kernel function, the original space is mapped to a higher dimensional space where the problem becomes linear. Different kernel functions are in common use for different classification problems. For our experiments, we employed polynomial kernel.

IV. Results and Discussion

Here, first we give a brief description of the database that was used for performance evaluation and then the detail of evaluation policy. Finally results are presented and discussed.

A. *Dataset*

For evaluation, we used CASIA TIDE V1.0 dataset [15], which is a public domain benchmark database developed for research on image forgery detection, in particular copy-move and splicing forgery detection, and was released in January 2010. This database contains two datasets: (1) 800 authentic images and (2) 921 tampered images. Each image in the database is in JPEG format and its resolution is 384×256 pixels. There are eight categories of authentic images. For creating tampered images, authentic images from each category were arbitrarily selected and cut-and-paste process was employed for forgery. Also geometric transformations like scaling, rotation etc. were used to modify copied regions in some cases before pasting. Adobe Photoshop was employed for generating tampered images. Out of 921 forged images, 459 are forged with copy-move forgery and the rest are spliced.

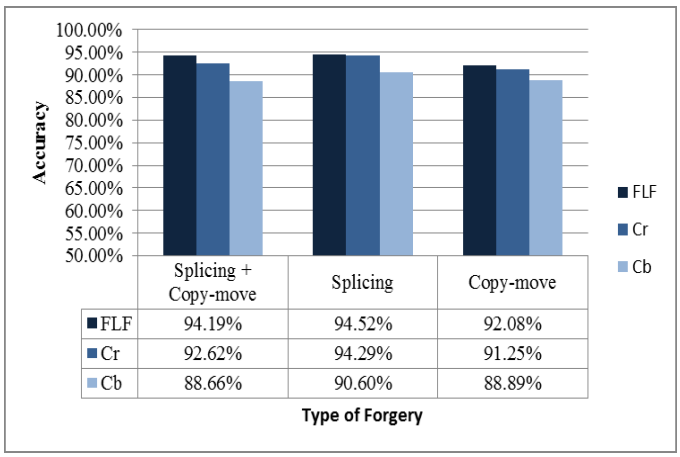
B. *Evaluation Policy*

For performance evaluation, we employed 10-fold cross validation. LIBSVM was utilized for SVM implementation [22]. SVM with polynomial kernel has four parameters: C, g, c_f and r, where last three parameters are due to polynomial kernel. Grid search was used to find the optimal parameter values, which are: $C = 2^{-3}$, $g = 2^{-3}$, $c_f = 10$ and $r = 2$.

We employed two widely used performance measures: accuracy and area under ROC curve (AUC). Accuracy (Acc) is the percent ratio of correctly classified images to the total number of images and is calculated using the following equation.

$$Acc = 100(TP + TN) / (TP + TN + FN + FP)$$

where TP, FN, FP and TN are, respectively, the numbers of true positive, false negatives, false poistives and true negatives.



	Splicing + Copy-move	Splicing	Copy-move
FLF	94.19%	94.52%	92.08%
Cr	92.62%	94.29%	91.25%
Cb	88.66%	90.60%	88.89%

Fig. 8. The performance results for fergry detection with multi-WLD and Cb, Cr & FLF.

The AUC is a better measurement and it takes value between 0 and 1. Standard deviation, which is represented by the symbol std, demonstrates how much variation exists from the average (mean, or expected value).

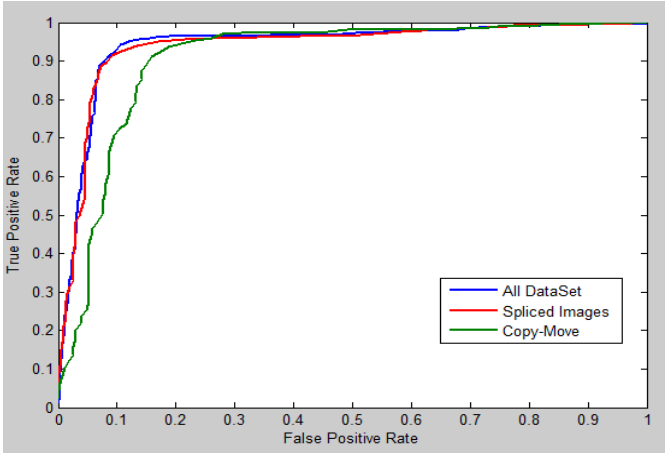


Fig. 9. ROC Curves for different forgery types with multi-WLD and FLF.

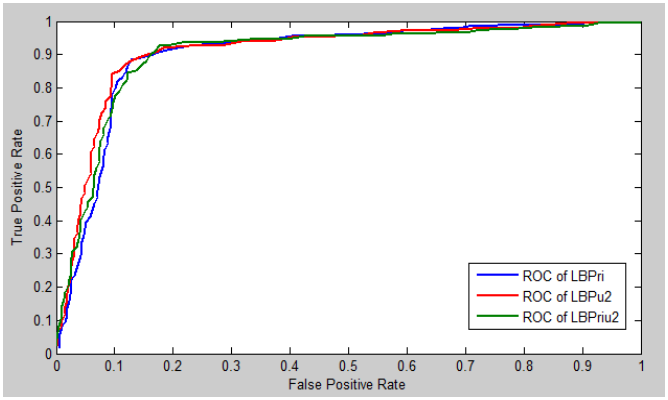


Fig. 10. ROC curves for splicing detection with multi-*LBP* and Cr component.

We tested the forgery detection system with and without LLB feature subset selection technique and compared the results. We found that LLB not only reduced the number of features but also improved the detection accuracy. We reported here only the results with LLB feature subset selection.

We considered three experiment cases: splicing detection, copy-move detection and full database i.e. forgery detection of splicing and copy-move together.

We tested the performance of features extracted from Cb and Cr components separately and also by fusing the features extracted from these components i.e. with feature level fusion (FLF).

C. *Detection Performance with Multi-WLD*

In this section, we present the forgery detection results for splicing, copy-move and combined splicing + copy-move forgeries using multi-WLD.

Multi-WLD has three parameters (T, M, S). Based on our experiments, we found that the parameter values (T = 4, M = 4, S = 20) gives the best result, so we used these values for all experiments whose results are reported in this section.

1) *Results on Splicing Detection*

The detection results with individual chrominance component and feature level fusion are shown in Tabel I. The chrominance component Cr and FLF gave better accuracy (94.29%) than Cb. Almost similar, results are obtained in terms of AUC; Cr resulted in AUC = 0.94 ± 0.02 which is slighly better than FLF but signifcantly better than Cb. Figure 6 shows ROC curves coresponding to chrominance components and FLF for splicing detection.

Table I. Detection performance for splicing detection with multi-WLD.

Channel	Acc (%) ± std	AUC ± std	# Features
Cr	94.29 ± 2.50	0.94 ± 0.02	473
Cb	90.60 ± 3.82	0.91 ± 0.04	467
FLF	**94.29** ± 1.84	0.938 ± 0.024	1330

Table II. Detection performance for copy-move forgery detection with multi-WLD.

Channel	Acc(%) ± std	AUC ± std	# Features
Cr	90.83 ± 2.09	0.89 ± 0.03	411
Cb	87.22 ± 3.19	0.85 ± 0.04	432
FLF	**90.97** ± 2.72	0.90 ± 0.05	455

2) *Results on Copy-move Forgery Detection*

The detection performance results for copy-move forgery with individual chrominance component and their fusion are shown in Table II. FLF gives the best accuracy of 90.97% and AUC of 0.90. Figure 7 shows ROC curves for copy-move forgery detection with two chriminance compnents and FLF.

3) *Results on Full Dataset* (i.e. *Splicing +Copy-move*)

For this experiment case, we combined the images forged with

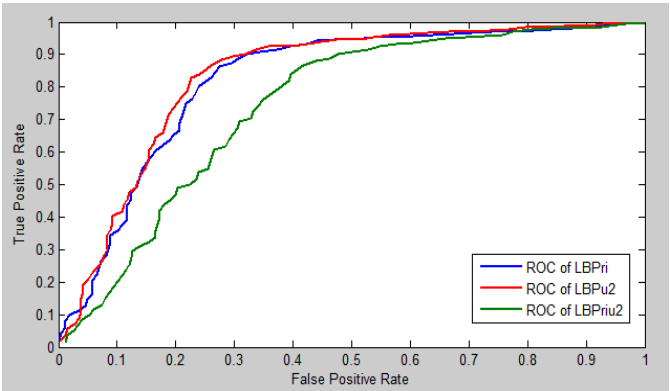


Fig. 11. ROC curves with multi-*LBP* and Cr compnent for copy-move forgery detection.

splicing and copy-move into one dataset to test the effect of the forgery detection system on splicign and copy-move together. Figure 8 gives the detection performance results for combined dataset in comparsion with individual forgery type. Figure 9 shows the correspong ROC curves. For combined dataset, the best accuracy (94.19%) is obtained with FLF. The performance with Cr has been decreased, which is probably

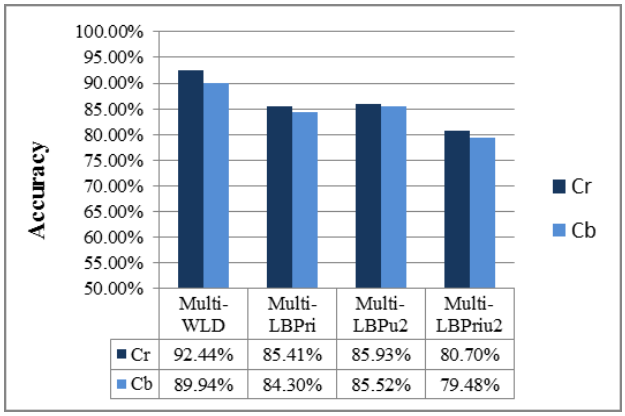


Fig. 12. Comparsion between the the dtection performance results with multi-WLD and multi-LBP on combined dataset.

due to the presence of copy-move forged images in the combined dataset.

D. *Detection Performance with Multi-LBP*

In this subsection, we present the detection results with multi-LBP. We tested the forgery detection system with three variants (LBP^{ri}, LBP^{u2} *and* LBP^{riu2}) of LBP to examine their effect on forgery detection performance. First we give the results on individual forgery type and then on combined dataset consisting of both splicing and copy-move forged images.

1) *Results on Splicing Detection*

The detection performance results for splicing detection using multi-LBP with three varients of LBP and Cr are shown in Table III while Table IV shows the results with chromonance componet Cb. The results indicate that almost similar and better detection performance is obtained with both LBP^{u2} and LBP^{riu2} and Cr crominance compnent, but LBP^{u2} shows more stable behavior because std in this case is smaller for accuracy as well as AUC. Fig.10. demonstrates corresponding ROC curves.

Table III. Detection results on splicing detection with multi-LBP and Cr chrominance component.

LBP variants	Acc(%) ± std	AUC ± std	#Features
LBP^{ri}	88.21 ± 3.70	0.89 ± 0.05	76
LBP^{u2}	90.36 ± 2.94	0.90 ± 0.04	256
LBP^{riu2}	**90.48** ± 4.20	0.90 ± 0.05	37

Table IV. Detection results on splicing detection with multi-LBP and Cb chrominance component.

LBP variants	Acc(%) ± std	AUC ± std	#Features
LBP^{ri}	86.55 ± 3.60	0.86 ± 0.04	117
LBP^{u2}	86.55 ± 2.81	0.86 ± 0.04	115
LBP^{riu2}	**86.67** ± 3.96	0.88 ± 0.05	39

2) *Results on Copy-move Forgery Detection*

The results for copy-move forgery detection with Cb and Cr are shown in Tables V and VI, respectively. We observe that in this case both Cr and Cb components give almost similar results. The results indicate that LBP^{ri} varaint performs better for copy-move forgery than LBP^{u2} and LBP^{riu2}. This fact is also depicted by ROC curves shown in Figure 11.

Table V. Detection performance results with multi-LBP and chrominance component Cr for copy-move forgery.

LBP variants	Acc(%) ± std	AUC ± std	# Features
LBP^{ri}	**85.56** ± 4.91	0.83 ± 0.06	1203
LBP^{u2}	85.28 ± 3.48	0.81 ±0.04	114
LBP^{riu2}	75.14 ± 4.65	0.71 ± 0.07	33

Table VI. Detection performance results with multi-LBP and chrominance component Cb for copy-move forgery.

LBP variants	Acc(%) ± std	AUC ± std	# Features
LBP^{ri}	**85.83** ± 5.31	0.83 ± 0.08	3842
LBP^{u2}	80.69 ± 3.49	0.78 ± 0.06	147
LBP^{riu2}	72.64 ± 3.59	0.66 ± 0.05	34

Table VII. Detection performance results with multi-LBP and chrominance components Cr and Cb for combined dataset.

LBP variants	Chrom. Comp.	Acc(%) ± std	AUC ± std	# Features
LBP^{ri}	Cr	85.41 ± 3.02	0.85 ± 0.03	4495
	Cb	84.30 ± 2.78	0.85 ± 0.04	4414
LBP^{u2}	Cr	**85.93** ± 4.95	0.86 ± 0.04	248
	Cb	85.52 ± 2.91	0.86 ± 0.04	274
LBP^{riu2}	Cr	80.70 ± 3.73	0.81 ± 0.04	38
	Cb	79.48 ± 2.26	0.79 0.03	34

3) *Results on full dataset* (*Splicing+Copy-move*)

Similarly to multi-WLD, we performed expariemnts for the combined dataset. The detection results with the three variants of LBP are shown in Table VII. The results show that for combined dataset, LBP^{u2} performs better than LBP^{ri} and LBP^{riu2} and it is with both Cr and Cb components.

E. *Disscusion*

The results shown in Figure 12 for combined dataset and the results presented in the previous sections indicate that multi-WLD performs better than multi-LBP in general. Out of three variants of LBP, LBP^{u2} results in better detection performance for both splicing and copy-move forgeries than other varients, LBP^{riu2} results in better accruacy for splicing detection but it is not better than LBP^{u2}, on the other hand LBP^{ri} gives better accruacy for copy-move forgery detection but it is not better than LBP^{u2}. In general both multi-WLD and multi-LBP give better perfromance for splicing detection than copy-move detection. It is due to the reason that in copy-move forgery the source and terget regions belong to the same image and so the texture microstructures are similar and the distortion in microstructures forgery is less pronoucned as compared to

splicing where the source and terget regions are from different images.

In general chrominance component Cr gives better performance than Cb with both multi-WLD and multi-LBP. In case of multi-WLD, Cr and FLF give alsmost similar results for both splicing and copy-move forgries, but for combined dataset FLF outforms Cr. In case of multi-LBP, we did not test FLF because the result without fusion is much less than that with multi-WLD and there is little chnance that the result will be better using fusion than that with multi-WLD.

F. *Comparison with other methods*

The forgery detection methods based on multi-WLD and multi-LBP have been compared with a similar method [21] that also uses chrominance channels. We implemented the method described in [21] and evaluated it on CASIA v1.0 dataset using Cr channel. Table VIII gives the comparison results in both copy-move and splicing forgeries detection. Not only Multi-WLD based method but also multi-LBP based method outperforms the method in [21] on CASIA TIDE v1.0

TABLE VIII. Comparison of Accuracies between the method based on Multi-WLD and the method in [21].

Type of forgery	Multi-WLD	Multi-LBP	Method in [21]
Spliced	**94.29%**	90.48%	79.90%
Copy-Move	**90.97%**	85.83%	76.30%

V. CONCLUSION

Assuming that image forgery distorts the texture micro-patterns in a digital image, the forgery detection problem has been addressed using texture descriptors. We thoroughly investigated two stat-of-the-art texture descriptors (multi-WLD and multi-LBP) for forgery detection. Multi-WLD results in better performance than multi-LBP. The best results achieved by multi-WLD based method are 94.29% for splicing detection, 90.97% for copy-move forgery detection and 94.19% for combined dataset. Both multi-WLD and multi-LBP perform better for splicing detection than copy-move forgery detection, which is due to the reason that in copy-move forgery the texture micro-pattern are similar in the copied and pasted regions and the distortion is less noticeable. This indicates that more powerful and sensitive texture descriptors are needed to improve the detection rate for copy-move forgery.

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

[3] M. Hussain, G. Muhammad, Sahar Q. S., G. Bebis, G., and Mirza, A. M., "Copy-move Image Forgery Detection using Multi-resolution Weber Descriptors," Proc. SITIS 2012, IEEE Computer Society Press, pp. 395-401, Nov. 25-29, 2012, Naples, Italy.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

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

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] Y. Q. Shi, C. Chen, and W. Chen, "A natural image model approach to splicing detection", ACM MM&Sec'07, pp. 51-62, 2007.

[15] CASIA image tampering detection evaluation database (CASIA TIDE) v1.0 and v2.0, available at http://forensics.idealtest.org.

[16] J Z. He, W. Lu, W. Sun, and J. Huang, "Digital image splicing detection based on Markov features in DCT and DWT domain", Pattern Recognition, http://dx.doi.org/10.1016/j.patcog.2012.05.014, 2012.

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

[18] 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.

[19] T. Ojala, M. Pietikainen, and T. Maenpaa, 'Multiresolution gray-scale and rotation invariant texture classification with local binary patterns", Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 24, no. 7, pp. 971–987, 2002.

[20] Y. Sun, S. Todorovic, and S. Goodison, "Local-learning-based feature selection for high-dimensional data analysis", Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 32, no. 9, pp. 1610–1626, 2010.

[21] 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.

[22] C. C. Chang and C. J. Lin, LIBSVM - a library for support vector machine, 2010, downloadable at http://www.csie.ntu.edu.tw/~cjlin/libsvm

[23] M. Hussain, Summrina K. W., A. Elzaart, M. A. Berbar, "Comparison of SVM Kernel Functions for Breast Cancer Detection," Proc. CGIV2011, IEEE Computer Society Press, pp. 145-150, August 17-19, 2011, Singapore.