Noname manuscript No.
(will be inserted by the editor)

Passive Detection of Image Forgery using DCT and Local Binary Pattern

Amani Alahmadi[1], Muhammad Hussain[1,a], Hatim Aboalsamh[1], Ghulam Muhammad[1], George Bebis[2], Hassan Mathkour[1]

Received: date / Accepted: date

Abstract With the development of easy-to-use and sophisticated image editing software, the alteration of the contents of digital images has become very easy to do and hard to detect. A digital image is a very rich source of information and can capture any event perfectly, but because of this reason, its authenticity is questionable. In this paper, a novel passive image forgery detection method is proposed based on Local Binary Pattern (LBP) and Discrete Cosine Transform (DCT) to detect copy-move and splicing forgeries. First, from the chrominance component of the input image, discriminative localized features are extracted by applying 2D DCT in LBP space. Then, support vector machine (SVM) is used for detection. Experiments carried out on three image forgery benchmark datasets demonstrate the superiority of the method over recent methods in terms of detection accuracy.

Keywords Copy-move forgery, Image splicing, Forgery detection, Image forensics, LBP, DCT, SVM

1 Introduction

In today's visual world, digital images have become an integral part of our everyday life due to their ability to convey a wide range of information in a compact way and the availability of digital image acquisition tools. On the other hand, one needs not to be skillful to alter the contents of a digital image without leaving obvious traces of changes because of the development of user-friendly image editing tools. It has become easy to use digital images for nefarious designs and negative propaganda on social and electronic media, and hiding the facts, which can be crucial for criminal investigation, medical imaging, scientific discoveries, etc. As such, the authenticity of digital images cannot be taken for granted.

Image splicing and copy-move are two very harmful and commonly used types of forgery. Some techniques have already been proposed to detect such forgeries [1]. These techniques are either intrusive (active) or non-intrusive (passive, blind) [2]. An active technique detects tampering by verifying the integrity of a signature (embedded by a digital camera) such as watermark; it has a restricted scope due to the limitations of most of the cameras to embed such signatures [1]. On the other hand, a non-intrusive technique has a widespread scope since it depends only on analyzing the characteristics of a digital image[3].

Passive techniques can be broadly classified into learning based [4] and block-matching based methods [5][6]. The latter category of methods detects forgery by localizing the regions, which have been tampered by copy-paste. It is useful for sensitive applications like evidence in court rooms, insurance claims, etc., but it is time-consuming and unsuitable for applications like social media, where a bulk of images is being shared every day, and it is enough to verify whether an image is forged or not. In this paper, we propose a learning based passive technique that detects copy-move and image splicing forgeries. The challenge in a learning based method is how to model the change incurred by tampering. The key idea of the proposed method was inspired from analyzing the tampering procedure. When tampering is done, it disturbs the local distribution of micro-edge patterns by introducing new micro-patterns in the interior of the pasted region and sharp edges along its

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

boundary, and thus it changes its regularity and local frequency distributions [7][8]. Keeping in view this fact, we propose a novel way of modeling these changes using LBP (which encodes the micro-edge patterns) and DCT (which encodes the frequency content). We focus on the chromatic channel, which is insensitive to human vision and captures the tampering artifacts better than other color channels [9][10]. Discriminative localized features are extracted by applying 2D DCT in LBP space. Support Vector Machine (SVM) is used for classification. This idea was initially presented in [11], where the focus was only on splicing detection, this paper includes copy-move detection as well. In addition, results of intensive experiments are reported, which were performed to analyze the robustness of the method against post-processing operations, tampered region shape and forgery type. Moreover, the effectiveness of our way of integrating LBP and DCT is validated. To demonstrate the effectiveness of the method, extensive results are reported for three benchmark datasets and comparison is made with existing methods.

The rest of the paper is organized as follows. Section 2 reviews related works, Section 3 introduces the proposed method. The experimental and evaluation details are discussed in Section 4 and the results are presented and discussed in Section 5. Comparison with state-of-the-art works is given in Section 6. Finally, Section 7 provides conclusion and future work.

2 Related Works

Recently, many passive methods for the detection of copy-move and image splicing forgeries have been proposed. In the following paragraphs, we give an overview of the representative methods. We focus only on state-of-the-art learning based methods. The main differentiating factor among these techniques is the way the structural changes introduced by tampering are modeled.

Some researchers used DCT to model tampering changes. The splicing detection method by Shi et al. [7] models tampering changes using statistical features extracted from 2-D arrays generated by applying multi-size block discrete cosine transform (MBDCT). It gives an accuracy of 91.40 ± 1.87 on Columbia Image Splicing Detection Evaluation Dataset (Columbia) [12] with SVM. The method by Zhen et al. [13] represents the tampering changes using moment features extracted from 2D-arrays generated by applying MBDCT and image quality metrics (IQMs) and uses SVM for classification. It achieves an accuracy of 87.10% on Columbia. Zhang et al. [8] use LBP to extract features from 2-D arrays generated by MBDCT, PCA for dimensionality reduction and SVM for classification. This method results in an accuracy of 89.93 ± 1.50 on Columbia.

Wei et al. [14] model the tampering changes using stationary distribution of the edge image extracted from the chroma component using a finite-state Markov chain and use SVM as a classifier. This method achieves an accuracy of 95.6% on CASIA TIDE v2.0 [15]. He et al. [16] extended this method by including Markov features generated from the transition probability matrices in DCT and DWT domains. Using SVM-RFE classifier with recursive feature elimination, this method gives an accuracy of 89.76 on CASIA TIDE v2.0.

Dong et al. [17] model the discontinuity of image pixel correlation and coherency caused by splicing using statistical features extracted from run-length representation and edge statistics of the image and use SVM as a classifier. The accuracy of this method is 84.36% on Columbia. Zhao et al. [10] explored the effect of different color spaces on splicing forgery detection using four gray level run-length run-number (RLRN) vectors. This research revealed that chroma channels are more effective in forgery detection. Their technique gives the best accuracies of 94.7% and 85.0%, respectively, on CASIA TIDE v1.0 [15] and Columbia Color Image Splicing Detection Evaluation Dataset (Columbia-color)[18].

Texture descriptors like LBP and Webre's local descriptor (WLD) have also been used for modeling tampering traces. Hussain et al. [19] employ multiscale WLD to represent the tampering traces and SVM for classification, and compare it with LBP. WLD achieves an accuracy of 94.29% whereas LBP results in 90.48% accuracy on CASIA TIDE v1.0. Muhammad et al. [20] model tampering changes using steerable pyramids and LBP (SPT-LBP) and use SVM as classifier. This method achieves an accuracy of 94.89% on CASIA TIDE v1.0.

All the methods discussed above differ only in the way they model the structural changes caused by forgery. The success of a method depends on how accurately it represents these changes. We propose a method that exploits LBP and DCT in a novel way to model tampering changes.

3 Image Forgery Detection Method

Image tampering (copy-move or splicing) is done simply by copying and pasting. The pasting operation introduces structural changes in the host image. The micro texture patterns inside and along the boundary of the pasted region become different and discontinuity is introduced along its edges. In this way, local frequency distribution is changed and there is no more correla-

tion between image pixels is the region [7][8]. Capturing these structural changes is a key step to successful detection of tampering. Since the core idea behind LBP is to capture the occurrences of different micro patterns such as edges [21], LBP operator is suitable for highlighting the tampering artifacts and making them more pronounced in the host image. The next step is to trace the changes in the local frequency distribution of the LBP image. This is done by first transforming LBP image into frequency domain using block-based DCT and then computing the statistical measures of individual DCT coefficients across all blocks.

The system design of the proposed technique is shown in Figure 1. The main components of the system are: preprocessing, feature extraction (modeling the tampering traces) and classification. The detail of each component is given below.

3.1 Preprocessing

Chroma channels encode tampering traces batter than any other channel [11]. As such, first, RGB image is transformed to YCbCr image, where Cb and Cr are chroma channels. Human vision perceives the luminance component much better than the chroma components [22]. Therefore, most of the tampering traces, which cannot be detected by naked eyes, are hidden in the chroma channels.

3.2 Modeling the Tampering Traces

According to our idea, we model the tampering traces using LBP and 2D DCT. A systematic diagram of our approach is shown in Figure 2. First, for localization, a chroma component is divided into overlapping blocks with 50% overlap. Next, due to the ability of LBP to capture the occurrences of different micro patterns [21], LBP operator is applied on each block to highlight the introduced tampering artifacts (i.e. micro-edges inside the pasted region and the sharp edges along its boundary) and to make them more pronounced in the host image. Finally to capture the changes in the local frequency distribution, each block of LBP codes is transformed into frequency domain using 2D DCT, the standard deviations of the corresponding DCT coefficients are computed and arranged as a feature vector.

LBP is a local binary operator that discriminates different texture micro-patterns. The LBP operator is denoted by $LBP_{P,R}$ and is defined as follows [23]:

$$LBP_{P,R} = \sum_{i=1}^{P-1} S(P_i - P_c)2^i \quad (1)$$

where P is the number of points P_i on the circular neighborhood (of radius R) of the current pixel P_c, and the threshold function $S(x)$ is defined as:

$$S(P_i - P_c) = \begin{cases} 1 \; P_i - P_c \geq 0 \\ 0 \; P_i - P_c < 0 \end{cases} \quad (2)$$

3.3 Classification

Image forgery detection is a two-class problem (i.e. authentic vs. tampered). As Support Vector Machine (SVM) has given excellent performance in many two-class problems, so in the proposed technique, SVM with Radial Basis Function (RBF) is employed for classification. SVM classifier defines an optimal hyper-plane that separates the data into two different classes. The optimal hyper-plane that enhance the generalization of the classifier is the one with maximum margin (i.e. maximum distance between the hyper-plane and the closest samples known as support vectors) [24]. SVM uses kernel functions to map the samples to a higher dimension space where the classes become linearly separable [25].

4 Experimental Setup

In this section, we provide an overview of the datasets and the evaluation policy.

4.1 Description of Datasets

The proposed system is evaluated using three benchmark datasets: CASIA Tampered Image Detection Evaluation Database Version 1.0 (CASIA TIDE v1.0) and Version 2.0 (CASIA TIDE v2.0) or (CASIA 2010) and Columbia Image Splicing Detection Evaluation Dataset (Columbia) [12]. Table 1 provides a description of these datasets.

4.2 Evaluation Policy

For classification, we employed SVM with radial basis funtion (RBF) as kernel, because it has shown promising performance results in many applications. SVM with RBF kernel involves two parameters: C and γ; to find their best values, we used a loose and fine grid-search method [26], the best values of C and γ were found to be 2^5 and 2^{-5}.The performance was evaluated using 10-fold cross validation and commonly adopted performance measures: accuracy, true positive rate (TPR), true negative rate (TNR) and area under ROC curve

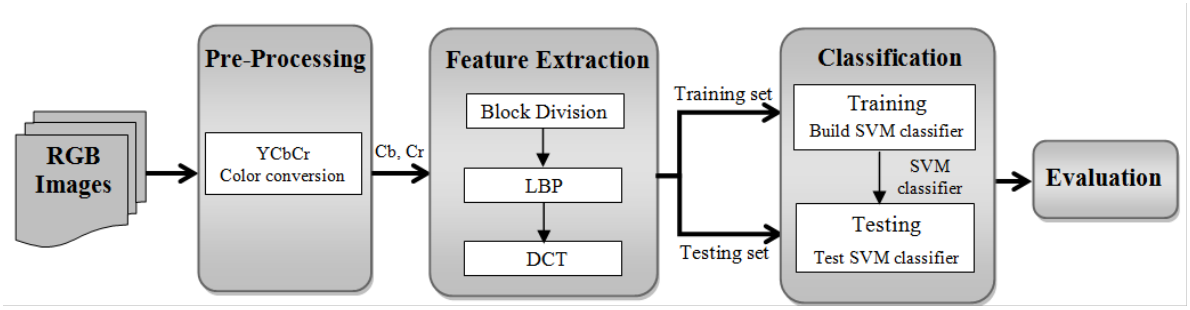

Fig. 1: The system design of the proposed method.

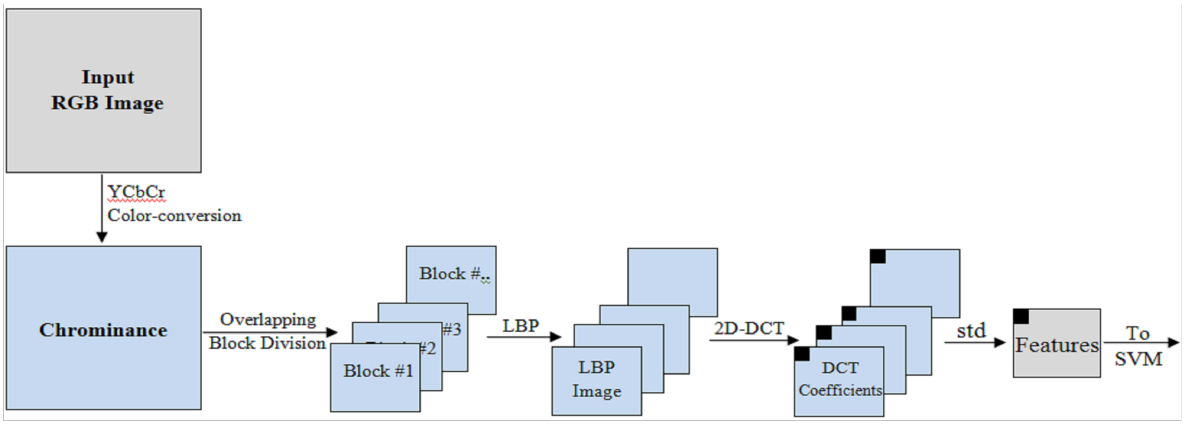

Fig. 2: The detail of the process of modeling the tampering traces.

Table 1: Description of the Datasets.

Dataset	No. of Images			Image Type	Image Size
	Authentic	Tampered	Total		
CASIA 1	800	921	1,721	Jpg	384×256, 256×384
CASIA 2	7,491	5,123	12,614	Jpg, tif, bmp	240×160 to 900×600
Columbia	183	180	363	tif, bmp	757×568 to 1152×768

(AUC), which are defined as follows: Accuracy = (TP + TN) / (TP + TN + FN + FP), TPR = TP / (TP + FN), TNR = TN / (TN + FP), where TP (True Positive) is the number of tampered images, which are classified as tampered; FN (False Negative) is the number of tampered images, which are classified as authentic; TN (True Negative) is the number of authentic images, which are classified as authentic, and FP (False Positive) is the number of authentic images, which are classified as tampered ones.

ROC curve is used to visualize the performance of a binary classifier. It plots TPR vs. FPR for different thresholds of the classifier outcomes. AUC is a way to quantify an expected performance of ROC which equals the probability that a classifier can classify a random positive instance higher than a negative one. A perfect performance is represented by AUC=1 [27]. Moreover, to assess whether the performance difference of two methods is statistically significant, the paired t-test with 95% confidence level is performed. Finally, after the statistical test if we do not find significant difference between two methods, then we choose the one that has less running time.

The proposed system involves different parameters such as: color channel, block division type and size, and LBP parameters. We performed extensive experiments on CASIA v1.0 considering different combinations of these parameters to figure out the set that results in the best perform. We found that chrominance channels, non-overlapping blocks of size 16×16, LBP parameters R = 8, R = 1 give the best performance, see detail in [12] and Figure 3. For the reported results, we used these parameters.

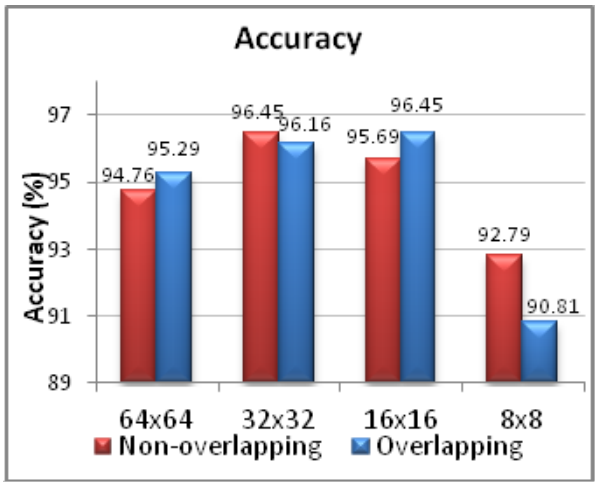

Fig. 3: The effect of different block types and sizes on CASIA v1.0 dataset.

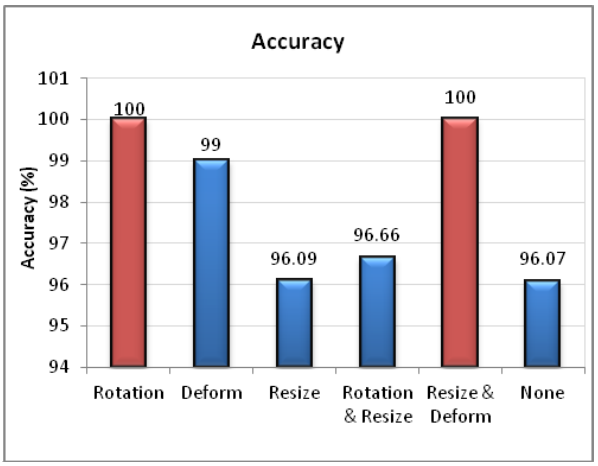

Fig. 4: Effects of post-processing operations on the detection accuracy (%) using CASIA v1.0.

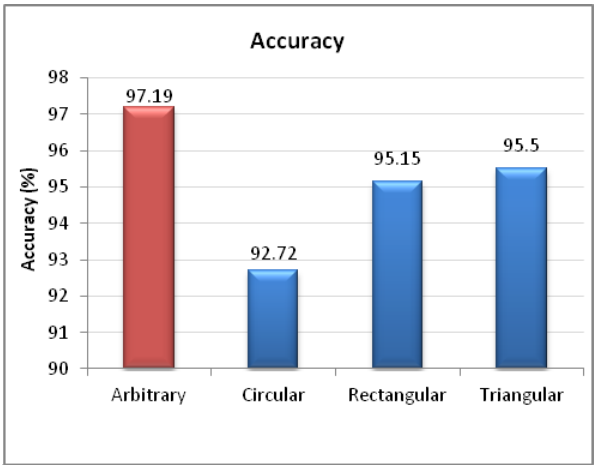

Fig. 5: Effects of the shapes of regions on the detection accuracy (%) using CASIA v1.0.

5 Results and Discussions

In this section, first we report and discuss the results of extensive experiments, which we performed to examine the robustness of the method against post-processing operations, shape of copied and pasted region, and forgery types using CASIA v1.0, and then we present the results on CASIA v2.0 and Columbia.

5.1 Effects of Post-processing Operations

In CASIA v1.0, three post-processing operations were applied on the copied region(s) before pasting: resize, deform and rotate. In some cases, either a combination of two operations or none of these operations were applied. Figure 4 shows the results for each category. The detection accuracy is the highest in case of rotation, deform and resize+deform. One simple justification of such results is that in these cases, there is a significant change inside and along the boundary of the tampered regions. In general, the method is robust against different post-processing operations.

5.2 Effect of the Shape of Tampered Region

CASIA v1.0 used copied regions of four shapes: circular, rectangular, triangular and arbitrary. Figure 5 shows that the best result is achieved against arbitrary shape, whereas it is poor in case of circular shape. The reason is related to the type of micro-edge patterns that are introduced by each region shape. Circular shape introduces similar micro-edge patterns whereas the arbitrary shape incorporates different micro-edge patterns making the tempering traces more detectable.

5.3 Effect of Forgery Type

Copy-move and splicing are similar from the tampering procedure point of view but they are different because they introduce different artifacts in the tampered image; in case of copy-move, source and target image is the same but in case of splicing, source and target are different. CASIA v1.0 contains 461 copy-move forged images and 460 spliced images. For the copy-move experiment, all the spliced images were removed from the dataset; the same thing was done for splicing experiment. Figures 6 and 7 show the ROC curves for copy-move and splicing, respectively. It can be observed from Table 2 that the proposed method performs well in detecting both types of forgery. However, the detection performance of splicing forgery is slightly better than that for copy-move. The reason is that splicing introduces

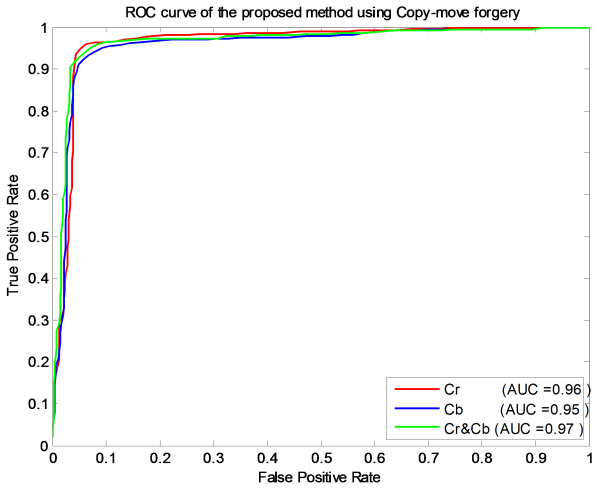

Fig. 6: ROC curves for Copy-move forgery detection using Cr, Cb and both (Cr+Cb) and CASIA v1.0.

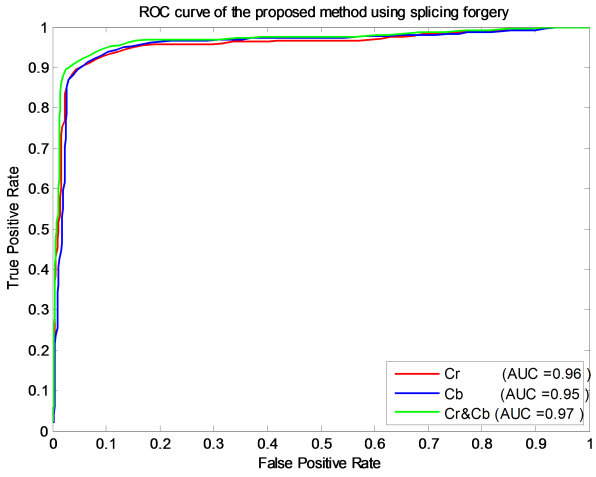

Fig. 7: ROC curves for splicing forgery detection using Cr, Cb and both (Cr+Cb) and CASIA v1.0.

more artifacts than copy-move since the source and the target are different images.

5.4 Experiments with CASIA v2.0 and Columbia Datasets

To test the robustness and consistency of the method, we performed experiments with CASIA v2.0 and Columbia datasets. Table 3 lists the detection results using the Cr, Cb channels and their fusion (Cr + Cb) on CASIA v2.0 and Columbia. A comparison of the detection accuracies on CASIA v1.0, CASIA v2.0 and Columbia datasets is illustrated in Figure 8. The detection rate on these datasets is comparable, which indicates that method is robust and consistent. It can be observed

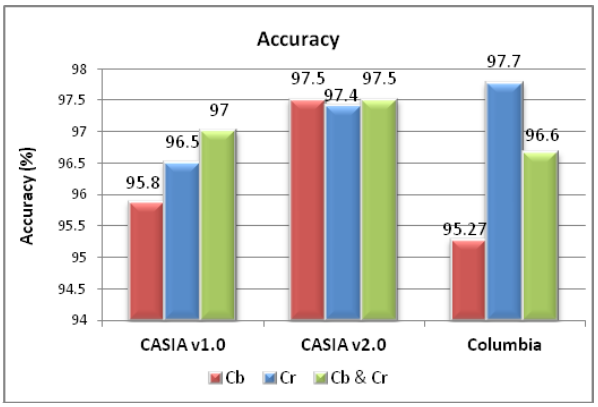

Fig. 8: Comparison of the detection accuracies on CASIA v1.0, CASIA v2.0 and Columbia datasets using Cr, Cb and Cr + Cb

that Columbia with Cr channel achieves the best performance. In general, Cr performs better on all datasets.

5.5 Effectiveness of Combining LBP with DCT

As we discussed, LBP operator highlights tampering artifacts and then block based DCT transfers the LBP image into the frequency domain to capture the local frequency fluctuations, caused by these artifacts, using statistical measures. In this section, we investigate the effectiveness of integrating LBP and DCT. To achieve this goal, we implemented the method by extracting the features using only one of them at a time. The results of using LBP alone, just DCT and their integration are shown in Figure 9. It can be observed that the integration of LBP and DCT achieves higher results. Moreover, we notice that DCT has a stronger effect on the detection performance than LBP. This observation supports what we mentioned above, that the role of LBP is to highlight the tampering artifacts, and the key factor in forgery detection is to trace the effect of these artifacts in the local frequency distribution which is done by using DCT.

6 Comparison with Existing Methods

In the literature, there exist some image forgery detection techniques that either use DCT or LBP. To our best knowledge, there is only one technique that combines LBP with DCT [8]. Zhang et al. [8] employed LBP and DCT for feature extraction in a different way. Their method was evaluated on Columbia dataset using SVM with RBF kernel. For the validation of our approach, it is important that we thoroughly compare our method

Table 2: Performance (mean±std) for copy-move and splicing forgery detection on CASIA v1.0 dataset.

Fogery Type	Channel	Accuracy(%)	TPR(%)	TNR(%)	AUC
Copy-move	Cr	96.63 ± 1.73	97.38 ± 1.71	95.97 ± 2.28	0.96 ± 0.01
Splicing	Cr	96.41 ± 1.45	95.48 ± 2.62	97.28 ± 2.26	0.96 ± 0.01
Copy-move	Cb	95.86 ± 1.9	96.27 ± 2.83	95.51 ± 3.45	0.95 ± 0.02
Splicing	Cb	96.52 ± 1.83	95.94 ± 3.45	97.09 ± 2.98	0.95 ± 0.02
Copy-move	Cr+Cb	96.30 ± 1.93	97.03 ± 2.82	95.71 ± 2.67	0.96 ± 0.02
Splicing	Cr+Cb	97.5 ± 1.36	96.75 ± 3.02	98.24 ± 2.53	0.97 ± 0.01

Table 3: Detection performance (mean±std) on CASIA v2.0 and Columbia datasets.

Fogery Type	Channel	Accuracy(%)	TPR(%)	TNR(%)	AUC
CASIA-2	Cr	97.41 ± 0.33	98.01 ± 0.59	96.93 ± 0.63	0.97 ± 0.004
Columbia	Cr	97.77 ± 2.19	98.30 ± 3.78	97.07 ± 4.15	0.97 ± 0.03
CASIA-2	Cb	97.5 ± 0.41	98.31 ± 0.44	96.88 ±0.56	0.97 ± 0.005
Columbia	Cb	95.27 ± 3.47	95.12 ± 3.98	95.52 ± 5.93	0.95 ± 0.04
CASIA-2	Cr+Cb	97.5 ± 0.31	98.45 ± 0.41	96.84 ± 0.56	0.97 ± 0.04
Columbia	Cr+Cb	96.66 ± 2.86	96.33 ± 4.31	79.09 ± 4.09	0.96 ± 0.03

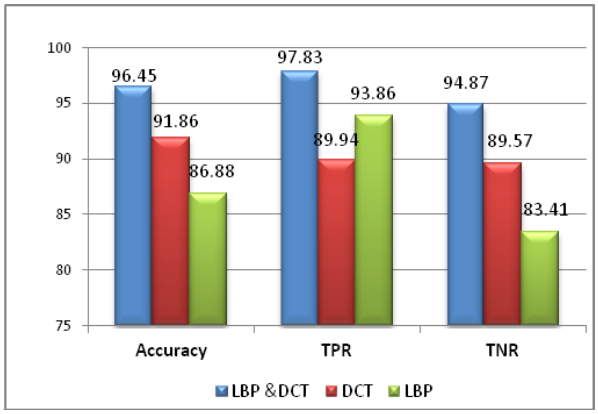

Fig. 9: The effectiveness of combining LBP and DCT in the proposed method.

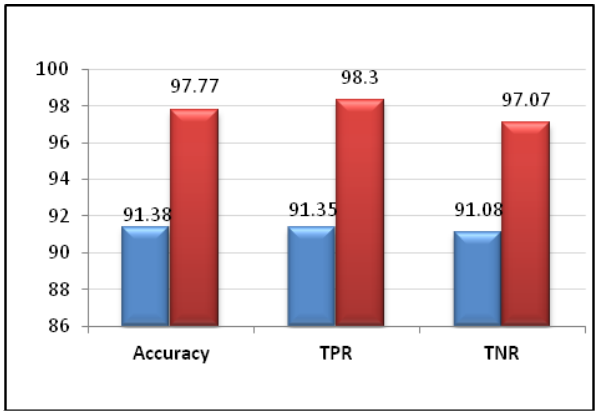

Fig. 10: A comparison between the results of the proposed method (red) and the method in [8] using Cr (blue).

with Zhang's method; we implemented this method using both grayscale and Cr channel. Our implementation achieved similar results compared with that of the original paper when grayscale images were used (89.93%). When we tested this method using Cr channel, we found that the detection performance is better than that of the grayscale (91.38%). A comparison between the results of our method and Zhang's method using Cr channel is depicted in Figure 10. It can be observed that our method achieved a higher detection performance. To check whether this achievement is statistically significant, the t-test with 95% confidence level was applied and significant difference was found. Table 4 presents a comparison between the proposed method and state-of-the-art forgery detection methods, which use SVM with RBF kernel and the same datasets. It can be observed that the proposed method outperforms the existing techniques.

7 Conclusion

In this paper, a novel copy-move and splicing forgery detection method based on LBP and DCT has been proposed. The chroma channel of an input image is divided into overlapping blocks and then LBP code of each block is transformed into DCT domain. Later, standard deviation of each DCT coefficient of all blocks is computed and used as features. SVM classifier is used for classification. The method was extensively evaluated. The experimental results showed that the chroma channels, when used in the proposed method, outperform the other color channels; it further validates the fact that the chroma channels are more suitable for forgery detection. The proposed method was evaluated using three benchmark datasets (CASIA TIDE v1.0, CASIA TIDE v2.0 and Columbia datasets); it gives almost similar results i.e. accuracies of 97%, 97.5% and

Table 4: Comparison between the detection accuracies (%) of the proposed methods and state-of-the-art methods. .

Method	Accuracy (%)		
	CASIA-1	CASIA-2	Columbia
Proposed method	**97.00**	**97.50**	**97.77**
Muhammad et al.[20]	94.89	97.33	96.39
Hussain et al. [4]	94.29	-	-
Zhang et al. [8]	-	-	91.38
He et al. [16]	-	89.76	93.55

97.77%, respectively, on the three datasets, which are higher than those of other recent methods. It also indicates that the proposed method is robust and consistent. Our future plane is to localize the tampering regions. Also, apply feature selection techniques and tuning the parameters using meta-heuristics methods.

Acknowledgements This project was supported by NSTIP strategic technologies programs, grant number 10-INF1140-02 in the Kingdom of Saudi Arabia.

References

1. Farid, H., A Survey of image forgery detection, IEEE Signal Processing Magazine 2(26), 16-25 (2009).
2. Mahdian, B. and S. Saic, A bibliography on blind methods for identifying image forgery, Signal Processing: Image Communication 25(6), 389-399 (2010).
3. Shivakumar, B. L. 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, 10(7), 61-65 (2011).
4. Hussain, M., S. Q. Saleh, Aboalsamh, H., Muhammad, G., Bebis, G., Comparison between WLD and LBP descriptors for non-intrusive image forgery detection, Proc. IEEE International Symposium on Innovations in Intelligent Systems and Applications (INISTA 2014), (2014).
5. Muhammad, G., Hussain, M., Bebis, G., Passive copy move image forgery detection using undecimated dyadic wavelet trans- form, Digital Investigation, 9(1), 49-57 (2012).
6. Jaberi, M., Bebis, G., Hussain, M., Muhammad, G., Accurate and robust localization of duplicated region in copy-move image forgery, Machine Vision and Applications, 25(2), 451-475 (2014).
7. Shi, Y. Q., C. Chen, A natural image model approach to splicing detection, Proc. 9th workshop on Multimedia and Security, Dallas, Texas, USA, 51-62 (2007).
8. Zhang, Y., C. Zhao, Revealing Image Splicing Forgery Using Local Binary Patterns of DCT Coefficients, Communications, Signal Processing, and Systems, 202, 181-189 (2012).
9. Johnson, M. K. and H. Farid, Exposing digital forgeries through chromatic aberration, Proc. 8th workshop on Multimedia and Security, Geneva, Switzerland, 48-55, (2006).
10. Zhao, X., J. Li, Detecting Digital Image Splicing in Chroma Spaces, Digital Watermarking, 6526: 12-22 (2011).
11. Alahmadi, A. A., Hussain, M., Aboalsamh, M., Muhammad, G., Bebis, G., Splicing image forgery detection based on DCT and Local Binary Pattern, IEEE Global Conference on Signal and Information Processing (GlobalSIP 2013) (2013).
12. Ng, T.-T. and S.-F. Chang, A Data Set of Authentic and Spliced Image Blocks, ADVENT Technical Report, #203-2004-3, Columbia University (2004).
13. Zhen, Z., K. Jiquan, An Effective Algorithm of Image Splicing Detection, Proc. International Conference on Computer Science and Software Engineering, Wuhan, Hubei, 1035 - 1039 (2008).
14. Wei, W., D. Jing, Image tampering detection based on stationary distribution of Markov chain, 17th IEEE International Conference Image Processing (ICIP 2010), Hong Kong, 2101 - 2104 (2010).
15. CASIA, Image Tampering Detection Evaluation Database, *http : //forensics.idealtest.org*.
16. He, Z., W. Lu, Digital image splicing detection based on Markov features in DCT and DWT domain, Pattern Recognition 45(12), 4292-4299 (2012).
17. Dong, J., W. Wang, Run-Length and Edge Statistics Based Approach for Image Splicing Detection, Digital Watermarking, 5450, 76-87, (2009).
18. Yu-Feng, H. and C. Shih-Fu, Detecting Image Splicing using Geometry Invariants and Camera Characteristics Consistency, IEEE International Conference on Multimedia and Expo, Toronto, Ontario, Canada (2006)..
19. Hussain, M., Muhammad, G., Saleh, S., Q., Mirza, A., M., Bebis, G., Image forgery detection using multi-resolution Weber local descriptors, Proc. IEEE EUROCON, Zagreb, 1570 - 1577 (2013).
20. Muhammad, G., M. Al-Hammadi, Hussain, M., Bebis, G., Image forgery detection using steerable pyramid transform and local binary pattern, Machine Vision and Applications, 25(4), 985-995 (2014).
21. Zhang, G., X. Huang, Boosting Local Binary Pattern (LBP)-Based Face Recognition, Advances in Biometric Person Authentication, 3338, 179-186 (2005).
22. B. B. Lee, J. Pokorny, Luminance and chromatic modulation sensitivity of macaque ganglion cells and human observers, JOSA A,7, 2223-2236(1990).
23. Di, H., S. Caifeng, Local Binary Patterns and Its Application to Facial Image Analysis: A Survey, IEEE Transactions on Systems, Man, and Cybernetics, 41(6), 765-781 (2011).
24. Cortes, C. and V. Vapnik, Support-Vector Networks, Machine Learning, 20(3), 273-297 (1995).
25. Hussain, M., Wajid, S., K., Elzaart, A., Berbar, M., A Comparison of SVM Kernel Functions for Breast Cancer Detection, Proc. 2011 Eighth International Conference on Computer Graphics, Imaging and Visualization (CGIV 2011), Singapore, 145-150 (2011).
26. Chih-wei Hsu , Chih-chung Chang , Chih-jen Lin, A practical guide to support vector classification, (2010).
27. Sokolova, M., N. Japkowicz, Beyond Accuracy, F-Score and ROC: A Family of Discriminant Measures for Performance Evaluation, Advances in Artificial Intelligence, 4304, 1015-1021 (2006).