Splicing Image Forgery Detection Based on DCT and Local Binary Pattern

Amani A. Alahmadi[1], Muhammad Hussain[1], Hatim Aboalsamh[1], Ghulam Muhammad[1], George Bebis[2]
[1]College of Computer and Information Sciences, King Saud University
Riyadh 11543, Saudi Arabia
[2]Department of Computer Science and Engineering, University of Nevada at Reno
mhussain@ksu.edu.sa

***Abstract*—The authenticity of a digital image suffers from severe threats due to the rise of powerful digital image editing tools that easily alter the image contents without leaving any visible traces of such changes. In this paper, a novel passive splicing image forgery detection scheme based on Local Binary Pattern (LBP) and Discrete Cosine Transform (DCT) is proposed. First, the chrominance component of the input image is divided into overlapping blocks. Then, for each block, LBP is calculated and transformed into frequency domain using 2D DCT. Finally, standard deviations are calculated of respective frequency coefficients of all blocks and they are used as features. For classification, a support vector machine (SVM) is used. Experimental results on benchmark splicing image forgery databases show that the detection accuracy of the proposed method is up to 97%, which is the best accuracy so far.**

***Keyword*: Image splicing, Image forensics, LBP, Forgery detection**

I. INTRODUCTION

Images have acquired the reputation of being inarguable evidence. However, with the development of imaging technology and the accessibility of powerful affordable image editing tools like Photoshop, the evidence of tampering on digital images is extremely difficult to uncover. As a result, today digital images are losing authenticity and taking their authenticity for granted is becoming increasingly difficult in legal cases, in electronic media, in medical profession, and in financial institutions etc. There are many proposals in the relevant literature to detect image forgeries [1], but their performances are not satisfactory. Based on these reasons, there is an urgent need to develop more reliable forgery detection techniques.

Image splicing is the most common technique used for creating digital image forgeries. In image splicing, forgery is done by copying a part from one image and pasting to another one or elsewhere in the same image to either add or hide objects. Usually, some processing is done on the copied part either before (e.g. scaling and rotation) or after (e.g. blurring and adding noise) pasting to make the editing less obvious and to eliminate irregularities that could show the image as tampered.

The existing image forgery detection techniques can be classified into two main categories: active (intrusive) and passive (non-intrusive) [2]. Active techniques, detect the forgery by validating the integrity of a pre-embedded (i.e. by a camera) signature or watermark. Since many available cameras are not having the ability to embed such kind of signature [1], this approach has a limited scope. On the other hand, passive techniques do not need to embed any information. They depend on the original characteristics of the image [3], which let them to be widely used.

Many passive approaches for image splicing forgery detection have been proposed so far. The method proposed by Shi *et al.* [7] employs statistical features based on 1D and 2D moments, and transition probability features based on Markov chain in DCT domain. He *et al.* [19] improved this method by combining transition probability features in DCT and DWT domains. In [6], Hussain *et al*. employ multi-scale Weber local descriptor (WLD) extracted from chromatic channel. Muneer *et al.* [11] proposed a method based on steerable pyramid transform and local binary pattern (SPT-LBP).

In this paper, we propose a novel passive image forgery detection technique based on Local Binary Pattern (LBP) and Discrete Cosine Transform (DCT) to detect image splicing forgeries. In this technique, the features are extracted from the chromatic channel, which has been shown to capture the tampering artifacts better than other color channels. In the first step, the chromatic component is divided into overlapping blocks and then LBP followed by 2D DCT are applied to each block. In the last step, standard deviations are calculated from the corresponding DCT coefficients of all blocks and are used as input features to SVM classifier. In the literature, there exist some image forgery detection techniques that either use DCT or LBP. So far as we know, this technique is the first one to combine LBP with DCT, which demonstrated its effectiveness in detecting the forgeries over three splicing image forgery detection datasets.

The rest of the paper is organized as follows. Section II introduces the detail of the proposed method. Experimental results and discussion are presented in Section III, while Section IV provides conclusion.

II. PROPOSED IMAGE FORGERE DETECTION METHOD

A diagram of the proposed technique is shown in Fig. 1. First, the input RGB color image is transformed to YCbCr color system. Then, the chrominance component (Cb or Cr) is divided into 16x16 overlapping blocks. Next, LBP and then DCT are applied to each block. For each DCT coefficient, in all blocks, standard deviation is computed and the resulted set of

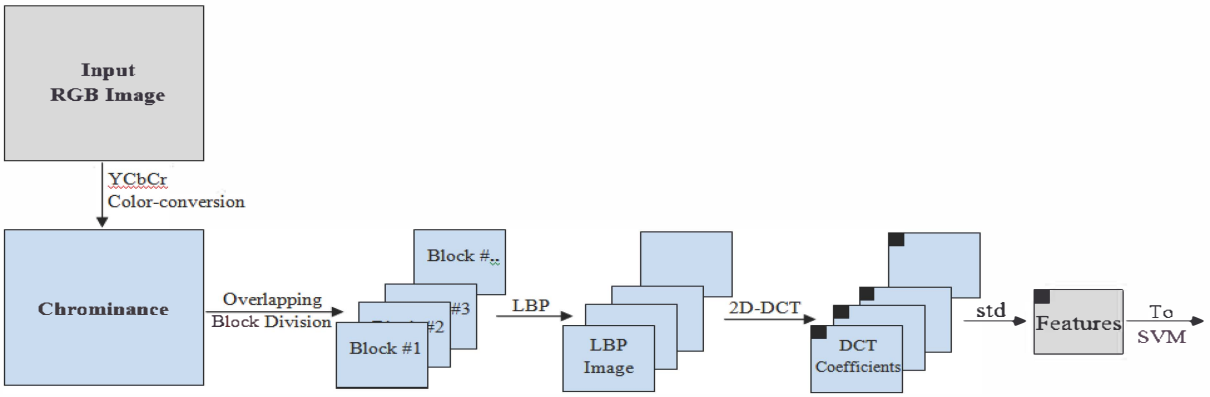

Figure 1. Flowchart of the proposed system.

standard deviations is used as feature vector. Finally, these features are sent to SVM classifier in order to make the decision about the input image whether it is an authentic or a tampered one.

A. YCbCr Chrominance Channel

The visibility of tampering traces varies in different color model. Image forgery detection techniques usually work in grayscale and RGB color systems. However, recent researches [9], [10] and [11] found that using chromatic channel rather than luminance or RGB enhanced the detection performance.

YCbCr color model represents colors in the form of luminance (Y) and chrominance (Cb and Cr) components. Equation (1) defines the formula used for computing Y, Cb and Cr channels from R, G and B channels.

$$\begin{pmatrix} Y \\ Cb \\ Cr \end{pmatrix} = \begin{pmatrix} 0.299 & 0.587 & 0.177 \\ -0.299 & -0.587 & 0.886 \\ 0.701 & -0.587 & -0.114 \end{pmatrix} \begin{pmatrix} R \\ G \\ B \end{pmatrix} + \begin{pmatrix} 16 \\ 128 \\ 128 \end{pmatrix}. \quad (1)$$

Human vision perceives the luminance component in a better way than the chrominance component. Therefore, most of the tampering traces, which could not detected by naked eyes, are hidden in the chromatic channel. Figure 2 shows Y, Cb and Cr components of an color image.

B. Local Binary Pattern (LBP)

LBP is a local operator which discriminates different types of textures. The original LBP operator [12] defines a label (LBP code) of each pixel of an image. To compute the LBP code, a 3x3 neighborhood of the pixel is threshold by its intensity value. If the neighbor's pixel value is less than the center, it will hold binary digit '0', otherwise it will hold '1'. The neighbors' binary digits are concatenating to build a binary code. The LBP code is the decimal value of that binary code. Figure 3 shows the LBP code computation process. Later, the neighborhood size of LBP operator was extended [13].

The LBP operator is denoted by $LBP_{P,R}$ and is defined as follows:

$$LBP_{P,R} = \sum_{i=1}^{p-1} S(p_i - p_c)2^i . \quad (2)$$

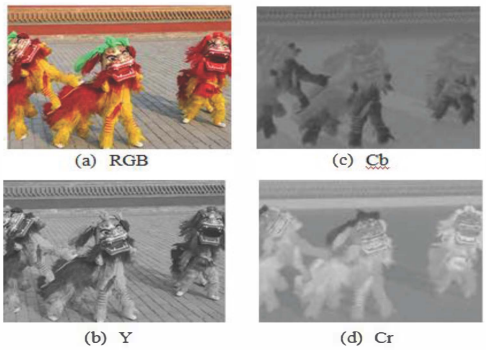

Figure 2. An RGB image and its YCbCr components.

where P is the number of pixels in the neighborhood and R is its radius, p_c is the center pixel value and the thresholding formula is defined as follows,

$$S(p_i - p_c) = \begin{cases} 1 & p_i - p_c \geq 0 \\ 0 & p_i - p_c < 0 \end{cases}. \quad (3)$$

When tampering is done, the original texture of the image is distorted. Due to the ability of LBP to capture the texture differences, it is an efficient tool for detection of the forgeries.

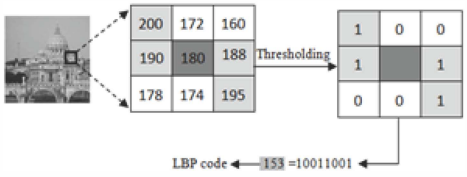

Figure 3. LBP code computation process.

III. Experiments and Discussion

In this section, we first introduce the evaluation policy and the datasets used to perform the experiments on the proposed method. Later, a set of experiments as well as discussions on their results are presented.

A. Database and Evaluation Policy

The proposed method is evaluated using three benchmark databases: CASIA Tampered Image Detection Evaluation Database Version 1.0 (CASIA TIDE v1.0) [14], CASIA TIDE

v2.0 [15] and Columbia Uncompressed Image Splicing Detection Evaluation Dataset [16]. Table I provides a description of these datasets. First, we perform experiments on CASIA v1.0 to find the optimal parameter sets, and then we test the consistency of the proposed method using the other datasets.

TABLE I. DESCRIPTION OF THE EVAUATED DATSES.

Dataset	No. of Images			Image Type	Image Size
	Authentic	*Tampered*	*Total*		
CASIA 1	800	921	1,721	jpg	384x256 256x384
CASIA 2	7,491	5,123	12,614	jpg tif bmp	240×160 To 900×600
Columbia	183	180	363	tif bmp	757x568 To 1152x768

For classification, SVM classifier with Radial Basis Function (RBF) kernel is used. To evaluate the performance of SVM, we use 10-fold cross validation.

The performance of the proposed technique is given in terms of accuracy and area under the curve (AUC) of a receiver operating characteristic (ROC). Accuracy measures the percentage of the images that are correctly classified by the classifier and it is computed as

$$\text{Accuracy} = 100 \times (TP+TN)/(TP+TN+FN+FP). \quad (4)$$

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.

B. Results and Discussion

First, we examine the effect of LBP with different parameters (P, R) to find their optimal values; here P is the number of pixels in the neighborhood, and R is its radius. It can be observed from Figure 4(a, b) that the best performance is achieved by using P = 8 and R = 1. Consequently, the next experiments are performed using these optimal values.

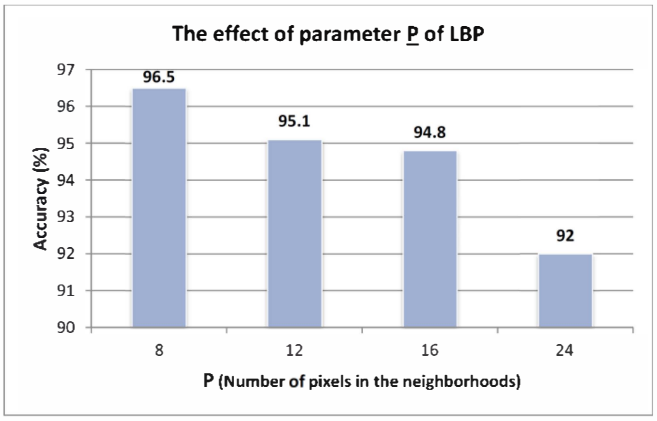

Figure 4(a). The effect of LBP parameter P on the performance.

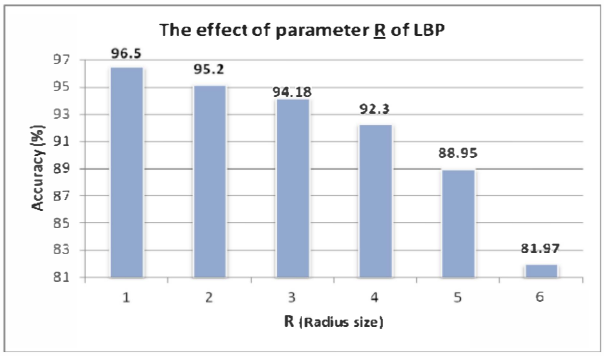

Figure 4(b).The effect of LBP parameter R on the performance.

Fig. 5 shows the detection accuracy of different components of color systems. It can be observed that Cb and Cr achieved the best detection performance (i.e. 96.5% and 95.8%, respectively) compared with the other channels. These results show that using chromatic component enhances the detection rate of image forgeries. The performance of Cb is almost similar to that of Cr. Fusion of the features from both Cb and Cr further improves the accuracy and it reaches 97%. The question arises why the proposed technique gives much better result. As high frequency information, such as edges, becomes pronounced in Cr and Cb components of the tampered image [17] and LBP operator further emphasizes the texture microstructures, so the standard deviation among DCT coefficients in different blocks become higher and causes to discriminate the tempering.

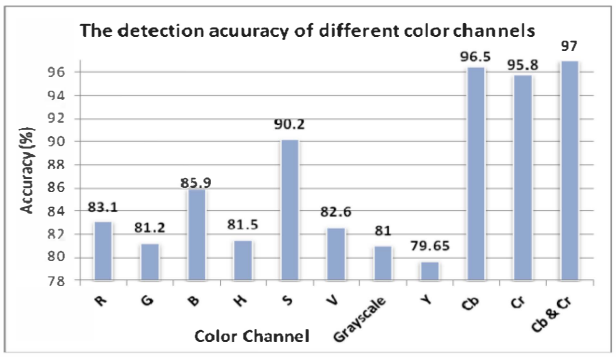

Figure 5. The detection accuracy using different color channels.

The ROC curves of the proposed technique using Cr, Cb and both (Cr and Cb) is shown in Figure 6.

Table II gives a comparison of the performance of the proposed method using CASIA v1.0, CASIA v2.0 and Columbia datasets. The results are comparable to each other which demonstrate the consistency of the proposed method.

To evaluate our proposed method comprehensively, we compare it with other recent methods [6, 11, 18, 19] which use experimental conditions similar to our method. The method described in [18] was evaluated using CASIA TIDE v2.0; while the method in [19] used Columbia. Table III shows the comparison of these methods. It can be observed from Table III, that the proposed method performs much better than the stat-of-the-art methods.

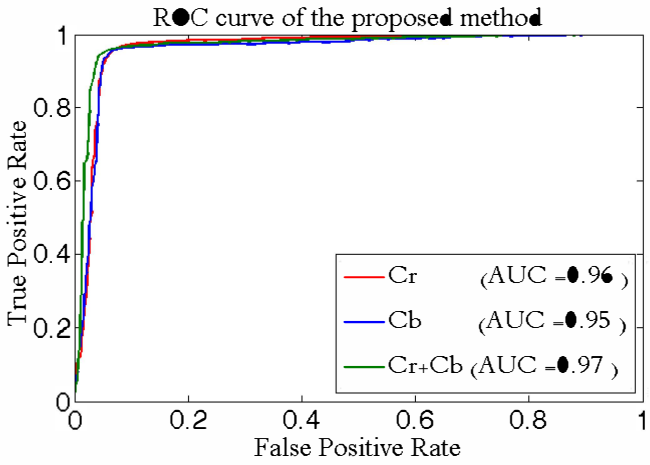

Figure 6. ROC curves of the proposed technique using Cr, Cb and both (Cr and Cb) channels.

TABLE II. THE PERFORMANCE ON DIFFERENT DATASETS.

Dataset	Accuracy (%)*	AUC*
CASIA 1	97	0.97
CASIA 2	97.5	0.976
Columbia	96.6	0.968

* Using both Cr and Cb channel.

TABLE III. RESULTS OF THE COMPARISON BETWEEN THE PROPOSED AND OTHER METHODS.

Dataset	Accuracy (%)				
	Proposed method	*Method in [19]*	*Method in [18]*	*Method in [6]*	*Method in [11]*
CASIA 1	**97**	-		93.33	95.2
CASIA 2	**97.5**	-	95.5	-	-
Columbia	**96.6**	93.55	-	-	-

IV. CONCLUSION

In this paper, a novel splicing image forgery detection method based on LBP and DCT is proposed. The image chromatic component is divided into overlapping blocks and then LBP code of each block is transformed into DCT domain. Later, standard deviations of DCT coefficients of all blocks are computed and areused as features. SVM classifier is used for classification. The experimental results show that the proposed features of the chromatic channel are outperforming that of other color channels. The proposed method show its consistency over CASIA TIDE v1.0, CASIA TIDE v2.0 and Columbia datasets with accuracies 97, 97.5 and 96.6, respectively. These results are significantly higher than that of other recent methods.

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] H. Farid. "A Survey of image forgery detection." *IEEE Signal Processing Magazine*, vol. 26, pp. 16-25, 2009

[2] B. Mahdian and S. Saic. "A bibliography on blind methods for identifying image forgery," *Signal Processing: Image Communication*, vol. 25, no. 6, pp. 389 - 399, July 2010.

[3] B. L. Shivakumar and Lt. Dr. Santhosh. "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.

[4] Y. Huang, W. Lu, W. Sun, D. Long, "Improved DCT-based detection of copy-move forgery in images", Forensic Science International, Vol. 206, Issues 1-3, pp. 178-184, March 2011.

[5] J. Fridrich, D. Soukal, and J. Lukas, "Detection of Copy-Move Forgery in Digital Images", in Proceedings of Digital Forensic Research Workshop, August 2003.

[6] M. Hussain, G. Muhammad, S. Q. Saleh, A. M. Mirza, and G. Bebis, " Image Forgery Detection Using Multi-Resolution Weber Local Descriptors," in Proc. *EUROCON 2013, Image Processing and Analysis*, (to appear).

[7] Y. Q. Shi, C. Chen, and W. Chen, "A natural image model approach to splicing detection," presented at the Proceedings of the 9th workshop on Multimedia & security, Dallas, Texas, USA, 2007.

[8] Z. Qianru, S. Wei, and L. Wei, "Digital spliced image forensics based on edge blur measurement," in *Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on*, 2010, pp. 399-402.

[9] M. K. Johnson and H. Farid, "Exposing Digital Forgeries Through Chromatic Aberration", in *ACM Multimedia and Security Workshop*, Geneva, Switzerland, 2006.

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

[11] G. Muhammad, M.H. Al-Hammadi, M. Hussain, A. M. Mirza, and G. Bebis, " Copy Move Image Forgery Detection Method Using Steerable Pyramid Transform and Texture Descriptor," in Proc. *EUROCON 2013. Image Processing and Analysis* (to appear).

[12] G. Zhang, et al, "Boosting local binary pattern (LBP)-based face recognition", Advances In Biometric Person Authentication, Vol. 3338, pp.179-186, 2004.

[13] T. Jabid, M.H. Kabir, O. Chae, "Gender Classification using Local Directional Pattern (LDP)", in Proc. ICPR, pp.2162-2165, 2010.

[14] "CASIA Tampered Image Detection Evaluation Database (CASIA TIDE v1.0) " Internet: http://forensics.idealtest.org:8080/index_v1.html, [Sep. 22, 2012].

[15] "CASIA Tampered Image Detection Evaluation Database (CASIA TIDE v2.0) " Internet: http://forensics.idealtest.org:8080/index_v2.html, [Feb. 10, 2013].

[16] Yu-Feng Hsu and Shih-Fu Chang. "Detecting Image Splicing Using Geometry Invariants And Camera Characteristics Consistency," *International Conference on Multimedia and Expo (ICME)*, Toronto, Canada, July 2006.

[17] W. Wang, J. Dong, and T. Tan, "Effective image splicing detection based on image chroma," presented at the Proceedings of the 16th IEEE international conference on Image processing, Cairo, Egypt, 2009.

[18] 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.

[19] Z. He, et al., Digital image splicing detection based on Markov features in DCT and DWT domain, Pattern Recognition (2012), http://dx.doi.org/10.1016/j.patcog.2012.05.014.