International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-05, Issue-02, May 2019

Copy-Move and Splicing Image Forgery detection using DCT and Local Binary Pattern

S. Alagu[1], K.BhoopathyBagan[2]

Dept. of Electronic Engineering, Madras Institute of Technology Campus, Anna University, Chennai, Tamil Nadu, India. alagupugal@gmail.com

Abstract— Digital images are very important in our daily lives and it can also be used as forensic evidence. Digital images play vital role in the field of medical and Journalism. Due to technical advancement, it is very difficult to detect Image Forgery. Image forgery detection is of great importance in digital forensics. In this paper, a new approach for image forgery detection is proposed based on local binary pattern (LBP) and discrete cosine transform (DCT) to detect copy–move and splicing forgeries. Initially the input image is preprocessed and texture features are extracted by applying DCT in LBP space. Support vector machine classifier is employed to distinguish tampered images from authentic images. The experiment results show that the proposed method gives better accuracy than others.

Keywords— Discrete cosine transform (DCT), Local binary pattern (LBP), Support vector machine (SVM), copy–move and splicing.

I. INTRODUCTION

In digital image processing, image forgery is the technique by which the visual content of image being altered. The digital contents cannot be considered as a strong proof due to several types of digital image forgeries. It is essential to develop some analytical method to check genuineness of the digital contents.

Image forgery also known as image tampering involves various techniques. Copy–move and splicing are the two common forgery techniques. In copy–move forgery, some of content of the image is copied and pasted into other areas of the same image. Splicing forgery is characterized by copying the content of one image and pasting it into another. The main difference between the two types of forgery is whether the sources of the forged content are from the same images.

Digital image authentication methods can also be categorized into two types: active and passive. In active methods, additional information must be embedded into the image. If a watermark is embedded in an image, the forgery can be detected when the watermark is found to be modified. The active method is limited because in most cases, information regarding the original watermark is unavailable for comparison with the extracted watermark. Researchers now focus on the development of passive methods, which are also called blind techniques. In these methods, forgery can be detected directly from the forged image without any preprocessing.

In the proposed work, an image authentication procedure that is based on recently proposed methods. In this procedure, first transform the image into the YCbCr color space. Second, the image block division method is applied to the chrominance components, which is the Cb channels. Third, a local binary pattern (LBP) operator and discrete cosine transform (DCT) are employed for each image block. Subsequently, mean deviation is applied to calculate the degree of dispersion of the DCT coefficients. Finally, the calculated results are used as features to classify the original image as authentic or tampered

The organization of the paper is given as follows. Section1 gives a brief introduction of the proposed work. Section II discusses a review of the literature on image forgery detection and section III gives a view on the methodology to detect the forged images. Section IV presents about the results and discussions of the proposed technique. Finally, the conclusion and future scope of the work are given in section V.

II. RELATED WORKS

In this section, a brief review of literature on copy move and splicing image forgery detection are discussed

Jian Li, Xiaolong et al., (2014) [1] designed a forgery detection method with two stages. First stage was designed to find the closeness of the pixels in the edges using transform matrix. In the second stage, copy move forgery was identified by means of refining the transform matrix.

In Fahime Hakimi et. al., (2015) [2] splicing detection is based on three methods such as SVM (Support Vector Machine) classifier, LBP and PCA (Principal Component Analysis). Two research datasets such as CASIA and Columbia were utilized.

Khosro Bahrami et al., (2015) [3] introduced a method to reduce the problem of blur type inconsistencies. Anselmo

DOI : 10.35291/2454-9150.2019.0156
© 2019, IJREAM All Rights Reserved.

Ferreira et al., (2016) [4] introduced a technique for copy-move forgery detection. The issue of individual pixel classification, present in most copy-move detection approaches solved by incorporating the post-processing step to the detection BKS-based technique. The practical analysis was carried out on CPH dataset.

Mohsen Zandi et al., (2016) [5] proposed new filtering scheme in order to preserve the correct matches .An iterative improvement strategy performed depend on the new interest point detector which greatly enhances the pixel-based accuracy. The practical evaluation was conducted using two public research datasets such as SBU-CM161 and IMD (Image Manipulation Dataset).

III. METHODOLOGY

Image tampering is performed by copying some image components and pasting the new image on the original image. 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 .Capturing these structural changes is a key step to successful detection of tampering. The system design of the proposed technique is shown in Figure 1.The main components of the system are: preprocessing, feature extraction and classification.

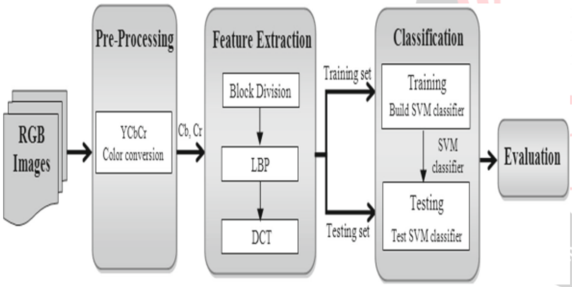

Fig. 1 The system design of the proposed method

PREPROCESSING

Although a tampered image appears natural, some tampered traces may remain in the chrominance component. Humans might not be able to identify a tampered image. YC_bC_r color space is more suitable than the RBG, HSV, and Grayscale colour spaces for tampered image detection. Furthermore, the chrominance component in the YCbCr colour space has a high performance level in detecting tampered images. Cb component is used for image authentication.

An image in RGB color space is converted in to the YC_bCr color space through the following equation.

$$Y = 0.299R + 0.578G + 0.114B$$

$$C_b = 0.564(B - Y)$$

$$Cr = 0.713(R - Y) \qquad (1)$$

Where Y is the luminance component, C_b and C_r are the chrominance components, and R, G, and B are the component of the RGB color space.

FEATURE EXTRACTION

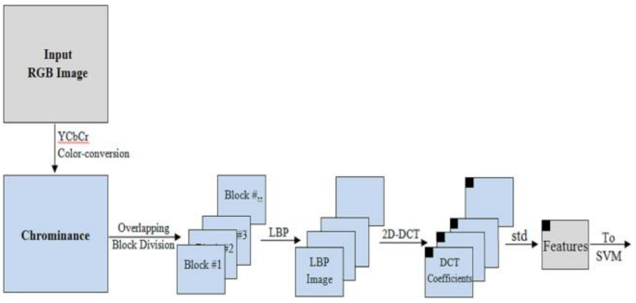

Fig. 2 Feature extraction

The tampering traces were modelled using LBP and 2D DCT. A systematic diagram of proposed approach is shown in Fig. 2. The chrominance component C_b is selected and divided into image blocks. The main purpose of this is to capture tampered image blocks.

Local Binary Pattern (LBP)

LBP operator is adopted in the proposed work. When an image is forged, the original texture is distorted.

The formula of the LBP operator is expressed as follows.

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

Where

$$S(x) = \begin{cases} 1, & x \geq 0 \\ 0, & x < 0 \end{cases} \qquad (3)$$

P is the number of neighbouring pixels, R is the radius of the neighbourhood, p_n is the neighbouring pixel value, and p_c is the central pixel value.

Discrete Cosine Transform (DCT)

When an image is tampered, the local frequency distribution changes. Hence, to calculate the local frequency distribution, LBP blocks are transformed from the spatial domain into the frequency domain by using the following formula

$$D(i,j)=C(i)$$

$$C(j) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \cos \frac{(2x+1)i\pi}{2M} \cos \frac{(2y+1)j\pi}{2N} \qquad (4)$$

$$\text{for } 0 \leq i \leq M-1 , 0 \leq j \leq N-1$$

where

$$C(i) = \begin{cases} \frac{1}{\sqrt{M}}, i = 0 \\ \sqrt{\frac{2}{M}}, \ 1 \leq i \leq M-1 \end{cases} \qquad (5)$$

$$C\ (j) = \begin{cases} \frac{1}{\sqrt{N}}, \ j = 0 \\ \sqrt{\frac{2}{N}}, \ 1 \leq j \leq N-1 \end{cases} \qquad (6)$$

DOI : 10.35291/2454-9150.2019.0156
© 2019, IJREAM All Rights Reserved.

D (i, j) is the DCT coefficient, M and N are the row and column sizes, respectively, of f (x, y), which is the LBP block. The formula (4) is called the two-dimensional DCT (2D-DCT).

The tampered regions can be discovered on the basis of the frequency distribution. Using feature extraction, a feature vector is obtained .The dispersive degree is calculated from the corresponding DCT coefficients in all DCT blocks. Mean deviation (MD) is used to calculate the local frequency fluctuation. The mean deviation replaces the standard deviation because we found that it provides superior performance. A large local frequency fluctuation indicates that the corresponding DCT coefficients include tampered traces, because tampered traces change the local frequency distribution. The mean deviation is calculated as follows:

$$\text{MD}=\frac{1}{N}\sum_{i=1}^{N}|x_i-\bar{x}| \qquad (7)$$

Where MD is the mean deviation, N is the total number of DCT blocks, xi is the DCT coefficient, and $\bar{x}$ is the arithmetic mean of all DCT coefficients (xi). After the calculation of the mean deviations, the values from local binary pattern and mean deviation are used as feature vectors to train a classifier to determine the authenticity of images.

CLASSIFICATION

Image forgery detection is a two-class problem (i.e., authentic vs. tampered). Support vector machine (SVM) is used it to classify the original and forged images in the proposed work.

EVALUATION

The performance is evaluated using tenfold cross validation and commonly adopted performance measures are accuracy, true positive rate and true negative rate.

Accuracy= (TP+TN)/ (TP+TN+FN+FP)

True positive rate (TPR) = TP/ (TP+FN)

True negative rate (TNR) =TN/ (TN+FP)

IV. RESULTS AND DISCUSSION

In this section, a brief view on the step by step results of the image forgery detection methods are discussed.

PREPROCESSING OF IMAGES

Original and forged images of copy-move and spliced are taken. The size of the images are adjusted as 384x256 pixels and given as input to the matlab.

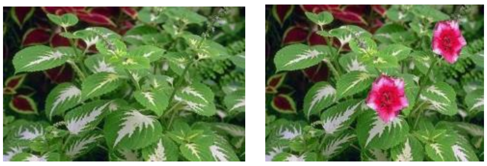

Fig. 3 Original and forged images of copy-move forgery

The human visual system is quite sensitive to luminance but not to chrominance, so humans might not be able to identify a tampered image. Thus, first the images are transformed from RGB model to YCbCr image, where Cb and Cr are chroma channels. The chroma channels encode tampering traces better than any other channel, so the chrominance and luminance component are separated from YCbCr model. From this, the Cr component can be used for further processes.

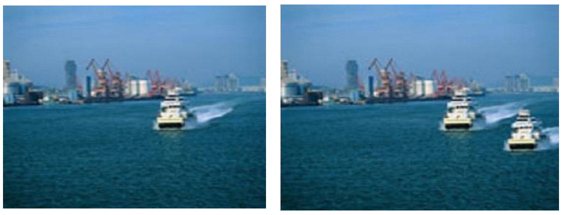

Fig. 4 Original and forged images of splicing forgery

The below figures shows the model conversion and separation of the components from the images.

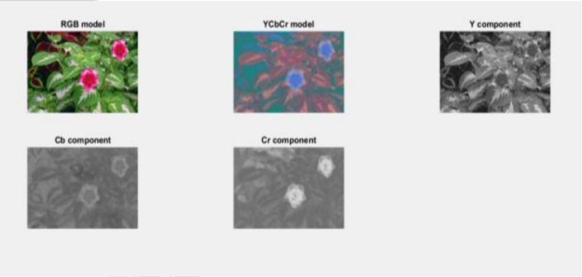

Fig. 5 Model conversion and component separation of copy-move image

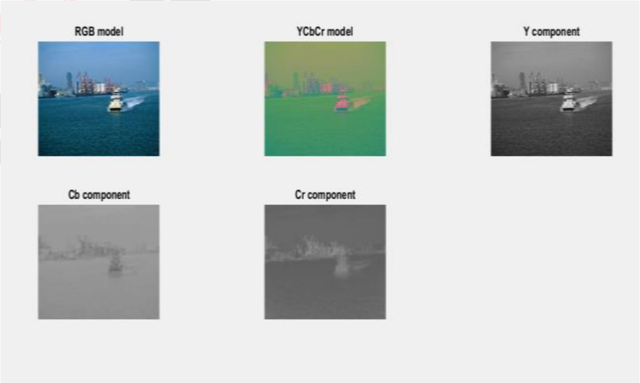

Fig. 6 Model conversion and component separation of spliced image

BLOCK DIVISION OF THE PREPROCESSED IMAGE

The separated C_b component is divided into 8x8 blocks for localization. Instead of taking the entire image and applying local binary pattern, image blocks provide better results. The below figures shows the block division of copy-move and spliced images.

DOI : 10.35291/2454-9150.2019.0156
© 2019, IJREAM All Rights Reserved.

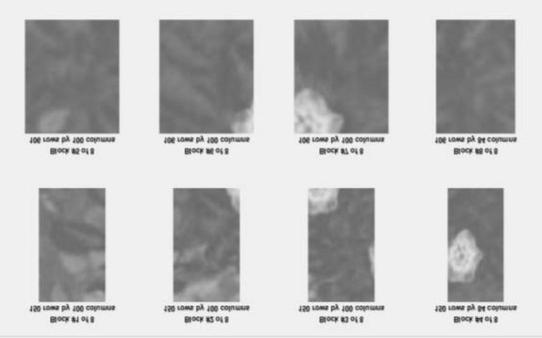

Fig. 7 8x8 block division of copy-move image

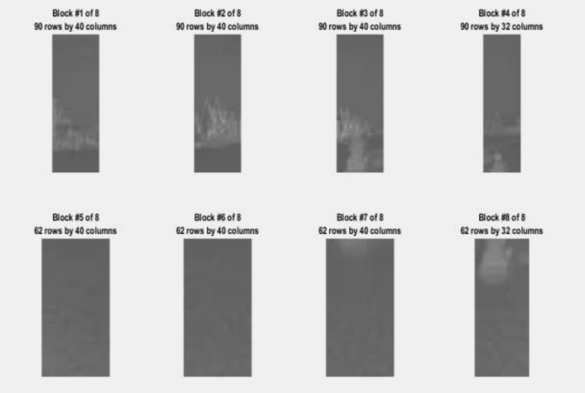

Fig.8 8x8 block division of spliced image

LOCAL BINARY PATTERN ON EACH BLOCK

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 correlation between image pixels in the region.

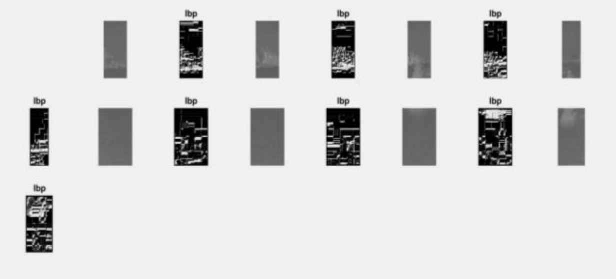

Fig. 9 Local Binary pattern (LBP) applied on each block

The above figure shows the difference in the micro-texture pattern in the boundary of the pasted region. LBP operator applied on each block highlights the introduced tampering artefacts and made them more pronounced in the host image.

SUPPORT VECTOR MACHINE CLASSIFIER

Various original and forged images are collected from several datasets and own dataset are also done to process and calculate the feature vectors. Nearly 200 original and 200 forged images are taken and processed to get feature vectors. The feature vectors can be used train the support vector machine classifier. The feature vectors must be labelled as their original or forged images to train the support vector machine.

EVALUATION METRICS

The performance of the classifier is measured using various parameters like the accuracy, sensitivity, specificity and precision.

Metric	Values (%)
Accuracy	93.75
Precision	94.02
Specificity	93.75
sensitivity	93.75
F Score	93.87

Table. 1 Performance Evaluation metrics

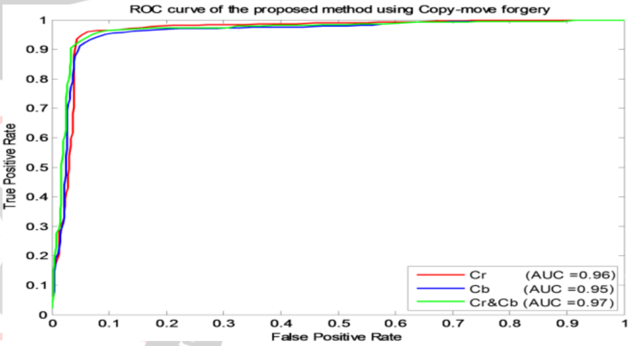

Fig. 10 ROC curves for Copy–move forgery detection using Cr, Cb and both (Cr+Cb)

Figures 10 and 11 show the ROC curves for copy–move and splicing, respectively. It can be observed 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.

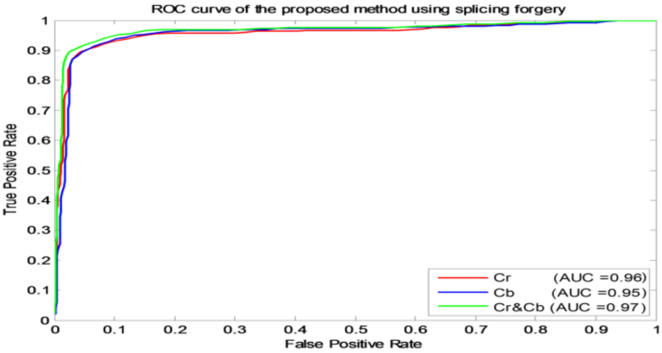

Fig. 11 ROC curves for splicing forgery detection using Cr, Cb and both (Cr+Cb)

Effectiveness of combining LBP with DCT

It can be observed that the integration of LBP and DCT achieves higher results.

DOI : 10.35291/2454-9150.2019.0156
© 2019, IJREAM All Rights Reserved.

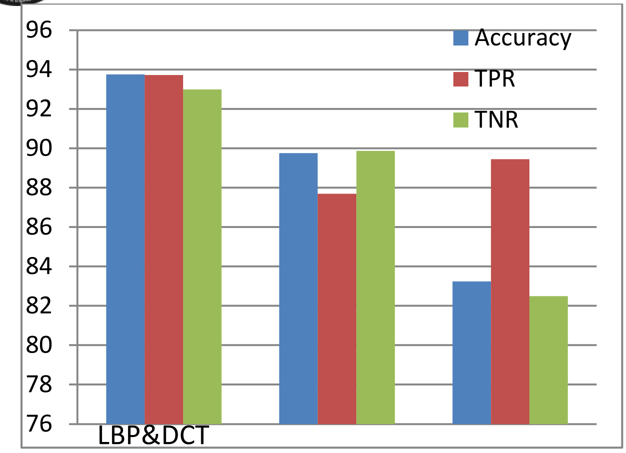

Fig. 12 The effectiveness of combining LBP and DCT in the proposed method

V. CONCLUSION

In the proposed work, a novel copy–move and splicing forgery detection method based on LBP and DCT was done. SVM classifier is used for classification and gives an accuracy of 93.75% which is higher than those of other recent methods. It also indicates that the proposed method is robust and consistent for an image forgery detection.

REFERENCES

[1] Hussain, M., Saleh, S.Q., Aboalsamh, H., Muhammad, G., Bebis, "Comparison between WLD and LBP descriptors for nonintrusive image forgery detection". In: Proceedings of the IEEE International Symposium on Innovations in Intelligent Systems and Applications (INISTA 2014) (2014)

[2] Alahmadi, A.A., Hussain, M., Aboalsamh, M., Muhammad, G.,Bebis, "Splicing image forgery detection based on DCT and local binary pattern". In: IEEE Global Conference on Signal and Information Processing (Global SIP 2013) (2013)

[3] Ng, T.-T., Chang, S.-F.: A Data Set of Authentic and Spliced Image Blocks. ADVENT Technical Report, #203-2004-3, Columbia University(2004)

[4] Zhen, Z., Jiquan, "An effective algorithm of image splicing detection". In: Proceedings of the International Conference on Computer Science and Software Engineering, Wuhan, Hubei, pp. 1035–1039 (2008)

[5] Wei, W., Jing, " Image tampering detection based on stationary distribution of Markov chain". In: 17th IEEE International Conference Image Processing (ICIP 2010), Hong Kong, pp. 2101–2104 (2010)

[6] CASIA, Image Tampering Detection Evaluation Database, http://forensics.idealtest.org

[7] Yu-Feng, H., Shih-Fu, "Detecting image splicing using geometry invariants and camera characteristics consistency". In: IEEE International Conference on Multimedia and Expo, Toronto, ON (2013).

[8] Muhammad, G., Al-Hammadi, M., Hussain, M., Bebis," Image forgery detection using steerable pyramid transform and local binary pattern". Mach. Vis. Appl. **25**(4), 985–995 (2014)

[9] Zhang, G., Huang, X.: "Boosting local binary pattern (LBP)-based face recognition". Adv. Biometr. Person Authent. 3338, 179–186(2005)

[10] Hussain, M., Wajid, S.K., Elzaart, A., Berbar, "A comparison of SVM kernel functions for breast cancer detection". In: Proceedings of the 2011 Eighth International Conference on Computer Graphics, Imaging and Visualization (CGIV 2011), Singapore, pp.145–150 (2011)

[11] Hsu, C.-W., Chang, C.-C., Lin, C.-J.: A practical guide to support vector classification. http://www.csie.ntu.edu.tw/~cjlin (2010)

[12] Sokolova,M and Japkowicz, " Beyond accuracy, F-score and ROC: a family of discriminant measures for performance evaluation". Adv.Artif. Intell. 4304, 1015–1021 (2006).

DOI : 10.35291/2454-9150.2019.0156
© 2019, IJREAM All Rights Reserved.