International Journal of Engineering & Technology, 7 (4.6) (2018) 217-219

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

LBP and GLCM Based Image Forgery Recognition

D. Vaishnavi[1] , T.S. Subashini[2], G.N. Balaji [3], D. Mahalakshmi[4]

[1]*Dept. of CSE,Vardhaman College of Engineering, Hyderabad, Telangana, India,*
[2]*Dept. of CSE, Annamalai University, Tamilnadu, India*
[3]*Dept. of IT, C.V.R College of Engineering, Telangana., India.*
[4]*Dept. of IT, A.V.C. College of Engineering, Tamilnadu, India*
**Corresponding author E-mail:vaishume11@gmail.com*

Abstract

The forgery of digital images became very easy and it's very difficult to ascertain the authenticity of such images by naked eye. Among the various kinds of image forgeries, image splicing is a frequent and widely used technique. Even though various methods are available to detect image splicing forgery, authors have attempted to provide a novel hybrid method which can yield greater accuracy, sensitivity and specificity. In this method, gray level co-occurrence matrix (GLCM) features are extracted using local binary pattern (LBP) operator on the image and the detection of the splicing forged images among the authentic images is done using the popular pattern recognition algorithms such as combined k-NN (Comb-KNN), back propagation neural network (BPNN) and support vector machine (SVM). The recorded results are also compared with the existing results of the previous studies to ascertain the quality of the results.

Keywords: *Image splicing forgery; local binary pattern; SVM; BPNN; combined k-NN.*

1. Introduction

Ensuring integrity of digital images has become vital due its content and the easy accessibility due to the advancements in digital communication systems. As an instance, telemedicine, centralized legitimate evidences, archival system's breach of integrity causes legal issues and grave damage to the human or the organization. Plenty of techniques and tools are available to tamper these images and that can even be done by the common man without expert skills in image processing. Advanced image edition tools allow doing such changes without leaving any marks to identify that it's tampered. One such technique is called "splicing" by which a section of an image is copied and pasted into another image. Even though, splicing leaves very minimal the traces of tampering, it is normally invisible to a naked eye. An in-depth statistical analysis needs to be carried out to identify such tampering. Image forgery detection using watermarking [1] and digital signatures [2] is used by experts to find tampers. Such detection techniques use some external information or clues for successful detection. Recent research studies indicate that the modern techniques are emerging to detect image forgery without the need of external information or clues [3–5].

Variety of methods is being proposed by researchers for identifying the tampering created using image splicing techniques. Alahmadi et al., proposed a method in which the chrominance of an image is extracted, analyzed using LBP method and then calculated the standard deviation of feature vectors of each block by applying 2D DCT [6]. Saleh et.al., used multi-scale weber law descriptor (WLB) method to extract histogram features to detect image splicing [7]. Hashmi & Keskar combined the DCT, LBP, curvelet and gobar features find spliced images [8]. Al- Hammadi proposed another method in which the curvelet transform is used to decompose the chrominance component into several scale and wedges and then constructed the feature vector using LBP histogram [9]. Mohammed et.al., applied the steerable pyramid transform (SPT) on the chrominance channel and extracted LBP features for classifying the images [10]. Agarwal & Chand proposed to use local phase quantization (LPQ) texture operator and an entropy filter for obtaining the internal statistics of the image according to the phase information [11]. He et al., obtained the Markov features from the transition probability matrices in DCT and DWT domain [12]. However, the authors have used LBP operator to extract GLCM features and applied classifiers such as support vector machine (SVM), back-propagation neural network (BPNN) and by proposing a combined k-nearest neighbor (Comb-KNN).

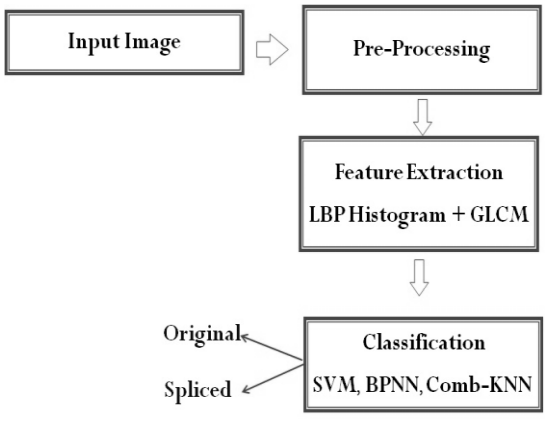


Fig. 1: Block diagram of proposed method

More about integration of CoT is cohesively described in the following sections.

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

2. Proposed method

The proposed process is illustrated in Fig.1. At first, the given image is converted into YCbCr colour space from RGB since YCbCr colour space provides better trace results when it's captured by using chrominance channel. Also it's noticed that some traces of tampering are undetectable in RGB [13]. The Cb and Cr channels of YCbCr color space are mainly used to obtain the image features. These activities are done in pre-processing step. As a next step, GLCM features are derived from the image at four directions after applying the LBP operator. Majority of the methods discussed in previous section have used the support vector machine (SVM) to distinguish the images. As a novel attempt, the authors attempted to use back propagation neural network (BPNN) and Comb-KNN classifiers besides SVM classifiers to ascertain best results. The rest of the process is explained in the following sections.

2.1. Feature extraction

The actual texture of the image is modified when the image is getting forged. Local binary pattern (LBP) is capable of capturing the pixel wise differences of the texture. This unique feature attracts the authors to use this technique for feature extraction. To explain the further, LBP operator divides the examined section of the image into cells such that each cell has 9 pixels. Then the central pixel is compared its adjacent pixel. If the central pixel's value is greater, it holds binary value "1" otherwise "0". By this, an eight digit binary code is formed which in turn is converted into decimal and called as LBP code [14].

Then, the GLCM features are derived from the image at four directions after applying the LBP operator in order to effectively categorize the spliced image. The four textural features such as correlation, contrast, energy and homogeneity are computed with distance of 1 pixel at different orientations. The contrast factor between the target pixel and its neighboring pixel correlated and it informs the relation between current pixel and its neighborhood pixels. Energy is a second angular moment. Homogeneity informs the distribution of GLCM elements towards its diagonal.

2.2. Classifiers used

The three classifiers used in this proposed method are explained below:

The popular machine learning technique SVM used as a classified in this method. This method utilizes the kernel function and separates the linearly inseparable data by mapping given data in higher order dimension [15]. Then a hyper-plane is sketched by keeping the margins between two classes as maximum. The data vectors lying near the hyper-plane are called support vectors which are further classified; this is a unique approach deployed by the proposed method in contrast to other methods which considers all data points.

The next technique used is BPNN. Because it is suitable for solving optimization problem and it's based on the gradient descent technique. Studies state that this method also has minimal network cumulative error [16]. In this study, BPNN is used to iteratively alter the weights in the gradient descent direction of the cumulative error. The iteration adjusts the weights by back propagating towards reaching acceptable level of mean square error.

The last method, k-NN algorithm is used to classify an object by majority vote of its neighbours. Initially, it calculates the similarity between inspected image and its adjacent images. Later it selects "k" closest neighbours among the training images for the inspected image and then finally, it assigns inspected image to a class based on the majority vote. Detailed explanation of this technique is beyond the scope of this article. To improve accuracy, the k-NN using three diverse distance measures namely Euclidean, Cosine and City-block are applied in this study and the majority value amongst the three distance output has been considered as the ultimate output. Owing to the mutual use of three distance measures, this k-NN algorithm is called as combined k-NN (Comb-KNN).

3. Experimental results and discussion

Authors had applied the proposed method using "Columbia uncompressed Image Splicing detection dataset". This dataset is an open source and it is available for research purpose without copyright restrictions. The dataset consists of one hundred and eighty (180) spliced images and one hundred and eighty three (183) original images. The resolution of images ranges from 757 × 568 pixels to 1152×768 pixels which are fair enough for the study. The statistical GLCM parameters are extracted after employing the LBP operator on the channel of the image to distinguish the spliced images. Out of three hundred and sixty three (363) images, eighty (80) images were applied for testing whereas the remaining images were used for training the classifiers. SVM is achieved a best results with kernel function of radial basis function. The BPNN classifier has been tested with sixteen (16) input neurons under different network structure. The performance of the proposed scheme is measured by the metrics: sensitivity, specificity and accuracy. These metrics were chosen because of that it represents the probability of spliced images that are found by the testing procedure, probability of authentic images that are found by the testing procedure, and probability of images that are correctly identified by the testing procedure. The study used Matlab© software for operational zing the proposed method. The generated results are presented in Table 1.

Table 1: Performance of the proposed method on Columbia dataset

Channel	Classifier	Accuracy	Sensitivity	Specificity
Cr	SVM	91.25	88.37	94.59
	BPNN	86.25	85.37	87.18
	Comb-KNN	85.00	85.00	85.00
Cb	SVM	92.50	92.50	92.50
	BPNN	87.50	87.80	89.47
	Comb-KNN	87.50	89.74	89.74

The proposed system has been tested on the both Cb & Cr channels of images with different classifiers and its performance results are furnished in Table 1. It's observed that SVM classifier has provided high accuracy with a value of 92.50% and 91.25 % in Cb and Cr channels respectively. The same classifier had generated highest results for sensitivity and specificity metrics compared to the results generated by other classifiers. The results of Cb are superior when comparing the average results of Cr channel. Hence, to ascertain the quality of the proposed method the results of Cb channel are taken into account and their results are comparatively analyzed with the existing methods and the outputs are illustrated in Table 2. There is a clear indication stating the SVM classifier used in proposed method recorded a best results compared to other related methods used in studies referred in [11].

Table 2: Comparative study of the proposed method with existing methods on Columbia image splicing dataset

Existing Methods	Classifier used	Accuracy
Proposed method	**SVM**	**92.50**
Entropy filter+ LPQ [1]	SVM	91.14
Morkov features[2]	SVM	87.52
Proposed method	BPNN	87.50
Proposed method	Comb-KNN	87.50

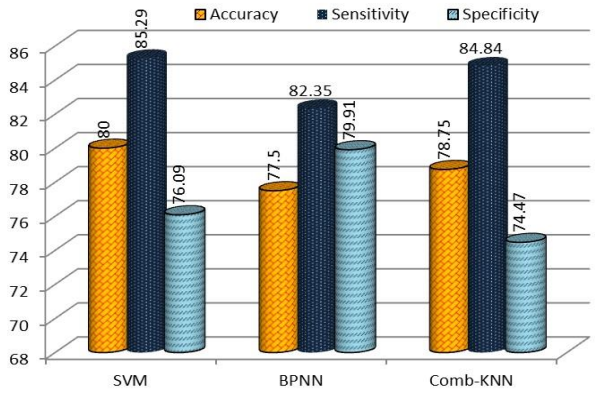


Fig. 2: Performance on 80 images

The proposed system is also experienced with one more set of eighty (80) images, which are downloaded from internet. From those images, forty (40) were spliced by the authors using the Adobe Photoshop CS5. The features were extracted on the Cb channel of these images and are provided as input to the BPNN, SVM and comb-KNN classifiers. The performances of all the three classifiers are shown as a graph in Fig. 2. The recorded results indicate that the proposed system has indicated an accuracy of 80% with SVM classifier, 77.50% for BPNN and 78.75% for comb-KNN respectively. The sensitivity and specificity of the SVM classifier were also obtained better compared with the BPNN and Comb-KNN.

4. Conclusion

A proposed hybrid method to recognize the image splicing forgery is implemented in this paper by extracting the GLCM features from LBP code of an image. The proposed method is deployed on the three different classifiers namely SVM, BPNN and Comb-KNN to find the optimal results. The performances are computed by accuracy, sensitivity and specificity on Columbia dataset, and their results are compared with the existing methods and also it is proved that the proposed method using SVM classifier has produced better results than the other methods and classifiers employed in this study. Finally, one more set of data are introduced to validate the system and their results are also shown that the proposed system is obtained the good results with SVM classifier than the others.

Acknowledgement

The authors express their gratitude and Credits for the use of the Columbia Image Splicing Detection Evaluation Dataset are given to the DVMM Laboratory of Columbia University, CalPhotos Digital Library and the photographers listed in http://www.ee.columbia.edu/ln/dvmm/downloads/AuthSplicedDataSet/photographers.htm.

References

[1] Vaishnavi, D., and Subashini, T. (2015) Fragile Watermarking Scheme Based on Wavelet Edge Features, *Journal of Electrical Engineering & Technology*, KOREAN INST ELECTR ENG 901 KSTC, 635-4 YEOKSAM-DONG, GANGNAM-GU, SEOUL, 135-703, SOUTH KOREA *10*, 2149–2154.

[2] Wang, X., Xue, J., Zheng, Z., Liu, Z., and Li, N. (2012) Image forensic signature for content authenticity analysis, *Journal of Visual Communication and Image Representation*, Elsevier 23, 782–797.

[3] Farid, H. (2009) Image forgery detection–A survey, Citeseer.

[4] Vaishnavi, D., and Subashini, T. (2016) Recognizing image splicing forgeries using histogram features. In *2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*, pp 1–4, IEEE.

[5] Vaishnavi, D., and Subashini, T. (2015) A passive technique for image forgery detection using contrast context histogram features, *International Journal of Electronic Security and Digital Forensics*, Inderscience Publishers (IEL) *7*, 278–289.

[6] Alahmadi, A., Hussain, M., Aboalsamh, H., Muhammad, G., Bebis, G., and others. (2013) Splicing image forgery detection based on DCT and Local Binary Pattern. In *Global Conference on Signal and Information Processing (GlobalSIP), 2013 IEEE*, pp 253–256, IEEE.

[7] Saleh, S. Q., Hussain, M., Muhammad, G., and Bebis, G. (2013) Evaluation of image forgery detection using multi-scale weber local descriptors. In *Advances in Visual Computing*, pp 416–424, Springer.

[8] Hashmi, M. F., and Keskar, A. G. (2015) Image Forgery Authentication and Classification using Hybridization of HMM and SVM Classifier., *International Journal of Security & Its Applications 9*.

[9] Al-Hammadi, M. H., Muhammad, G., Hussain, M., and Bebis, G. (2013) Curvelet transform and local texture based image forgery detection. In *Advances in Visual Computing*, pp 503–512, Springer.

[10] Muhammad, G., Al-Hammadi, M. H., Hussain, M., and Bebis, G. (2014) Image forgery detection using steerable pyramid transform and local binary pattern, *Machine Vision and Applications*, Springer *25*, 985–995.

[11] Agarwal, S., and Chand, S. (2015) Image Forgery Detection using Multi Scale Entropy Filter and Local Phase Quantization.

[12] He, Z., Lu, W., Sun, W., and Huang, J. (2012) Digital image splicing detection based on Markov features in DCT and DWT domain, *Pattern Recognition*, Elsevier *45*, 4292–4299.

[13] Zhao, X., Li, J., Li, S., and Wang, S. (2011) Detecting digital image splicing in chroma spaces. In *Digital Watermarking*, pp 12–22, Springer.

[14] Pietikäinen, M., Hadid, A., Zhao, G., and Ahonen, T. (2011) Local binary patterns for still images. In *Computer Vision Using Local Binary Patterns*, pp 13–47, Springer.

[15] Vapnik, V. N., and Vapnik, V. (1998) Statistical learning theory, Wiley New York.

[16] Yegnanarayana, B. (2009) Artificial neural networks, PHI Learning Pvt. Ltd.