ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Exposing Digital Image Forgeries by Illumination Color Classification

Sathvik H.N. [1], Premananda B.S. [2]

P.G. Student, Department of Telecommunication Engineering, R.V. Engineering College, Bengaluru, Karnataka, India[1]

Assistant Professor, Department of Telecommunication Engineering, R.V. Engineering College, Bengaluru, Karnataka, India[2]

ABSTRACT: Digital images have been commonly used in our day to day applications. It plays a vital role in communication media. Since Digital image forgery is becoming common nowadays, it is being done without much difficulty with the help of image editing tools mainly in order to cover up the truthfulness of the image. In this paper, one of the most common image manipulations called splicing is studied. The technique requires a minimal user interaction. The splicing forgery detection technique is carried out in two stages. The first stage involves the extraction of illuminant estimates from the illuminant map. From this illuminant estimates the Grey level co-occurrence matrix (GLCM) features are computed. The second stage involves the extraction of the Local binary pattern (LBP) features from the gray converted image. Both the GLCM and the LBP features are then paired and provided to the classifier for automatic decision making. Kernel nearest neighbour classifier (KNN) classifier is utilized to detect an image as authentic or tampered.

KEYWORDS: Edge detection, Illuminant map, GLCM features, LBP features, Image splicing detection, KNN classifier.

I. INTRODUCTION

Digital images are being widely used in day to day life for various communication purposes. Due to the existing availability of high speed internet, users can download and upload huge amount of images for their communication purposes. Images serve as essential tool for the communication purposes. Because of the availability of powerful image editing tools it is becoming difficult to prevent the misuse of images. There are different techniques available for the forgery detection of the images namely splicing, copy-move forgery, resampling etc. Image splicing is one of the most common image manipulation operations. It refers to copying the parts from the image and pasting it to the other image. Hence, it is also termed as copy-paste forgery.

Among other telltales signs, illumination inconsistencies are potentially effective for splicing detection: from the viewpoint of a manipulator, proper adjustment of the illumination conditions is hard to achieve when creating a composite image. Thus illuminant color estimates from local image regions are analysed and illumination map is obtained as a result. As it turns out, this decision is, in practice, often challenging. Moreover, relying on visual assessment can be misleading, as the human visual system is quite inept at judging illumination environments in pictures. Thus, it is preferable to transfer the tampering decision to an objective algorithm.

The K-nearest neighbour (KNN) algorithm is a method for classifying objects based on closest training examples in the feature space. K-Nearest Neighbours classification divides data into a test set and a training set. For each row of the test set, the K nearest (in Euclidean distance) training set objects are found, and the classification is determined by majority vote with ties broken at random. If there are ties for the K^{th} nearest vector, all candidates are included in the vote. The effective technique for splicing forgery detection is by finding out the illumination features by the GLCM approach and the texture features by LBP approach. Illuminant estimates are more distinguishable when

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

relating objects of identical material, so it is better to detect the human skin especially the faces. Also it becomes complex for a manipulator to achieve proper illuminant conditions when creating a composite image.

Paper is organized as follows. Section II discuss the related work, Section III describes overview of the proposed methodology, algorithmic details are given in Section IV and Section V presents experimental results showing results of images tested. Finally, conclusions are discussed in Section VI.

II. RELATED WORK

Recently, many techniques have been developed to reveal image tampering. Tiago C. et al. [1] presented a work on splicing forgery detection applicable to images containing more than one individual i.e., it is applicable only to people. It exploits lighting inconsistencies in the images due to the illumination color. Riess et al. [2] followed a different approach by using a physics-based color constancy algorithm that operates on partially specular pixels. In this approach, the automatic detection of highly specular regions is avoided. They proposed to segment the image to estimate the illuminant color locally per segment. Recoloring each image region according to its local illuminant estimate yields a so-called illuminant map.

Johnson et al. [3] developed a method to determine whether an image has been tampered with the assumption that both the original part and tampered part were taken under the same or approximately similar lighting conditions. Illuminant estimation is done using the statistical generalized gray world estimates. Each image region is recolored using the estimated illuminant to yield a so-called illuminant map. A work is carried in [4] using the DCT and the local binary pattern for image forgery detection and the chrominance component is divided into overlapping blocks. Color constancy in [5] measures the color of the objects which is independent to the color of the light source and the work is carried on color constancy based on the edges.

Texture features play an important role in determining the spatial features associated with an image. An effective facial descriptor called the LBP operator is suggested for describing the facial regions in an image [6]. Liya et al. [7] combined both the GLCM features and edge based features which are extracted from the illuminant map of an image and then provided to a machine learning approach for obtaining the result. A. Gebejes et al. [10] presented a work where the texture features are extracted by making use of the Grey-Level co-occurrence matrix.

III. OVERVIEW OF THE PROPOSED METHODOLOGY

.

The proposed system aims at splicing image forgery detection using semi-automated approach. The Figure 1 shows the block diagram of the proposed framework.

The steps involved in classifying the image as authentic or tampered is divided into two stages:

The first stage consists of the following steps:

1. **Dense Local Illuminant Estimation:** The input image is segmented into homogeneous regions. Per illuminant estimator, a new image is created where each region is colored with the extracted illuminant color. This resulting intermediate representation is called illuminant map (IM).
2. **Face Extraction:** This step requires human interaction. An operator sets a bounding box around each face (e.g., by clicking on two corners of the bounding box) in the image that should be investigated. Alternatively, an automated face detector can be employed. Then crop the bounding box out of each illuminant map, so that only the illuminant estimates of the face regions retained.
3. **Edge Detection:** Edge detection is a completely established field on its own within image processing. Since there is frequently a sharp regulation in intensity at the edge boundaries, area boundaries and edges are firmly related. The edges are detected from the extracted face regions from the obtained illuminant map by utilizing canny edge detector. From these illuminant edges the GLCM features are computed.
4. **Computation of Illuminant Texture Features:** For every face regions, statistical information of the image i.e., the GLCM texture features are calculated on the IM values. Some of the GLCM features computed include Energy, Entropy, Correlation and Homogeneity. Each of these features is given as input for classification.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

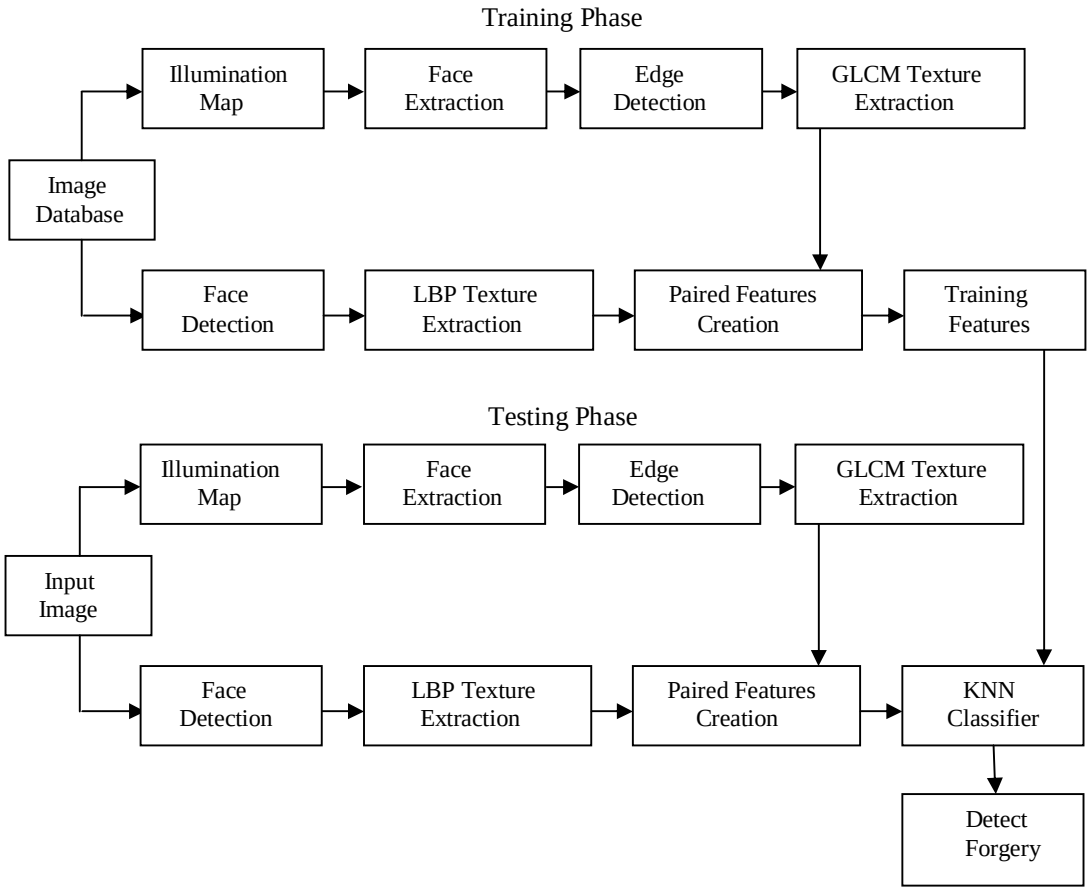

Figure 1: Overview of the proposed model

5. **Paired Face Features:** The GLCM features obtained for all face regions are then paired in matrix form which is then later utilized for classification.

The second stage consists of the following steps:

1. **Face Detection:** The input image is converted to gray scale image. Face regions in the image are detected using Viola Jones algorithm. Viola-Jones algorithm utilizes the cascade object detector to identify the face regions of the humans.
2. **Computation of LBP Texture Features:** The face region is segmented into small non-overlapping regions. The LBP operator is applied to small non-overlapping regions and thus the LBP histograms are computed for every sub regions. The LBP histograms calculated for all sub regions are then combined into a single and spatially enhanced histogram features.
3. **Paired Face Features:** The concatenated histogram features are then combined with extracted GLCM paired features and sent to the KNN classifier.
4. **Classification:** These features are then compared with the nearest neighbour features in the training phase and hence make decision by machine learning approach i.e., the KNN classifier which is incorporated to detect an image as authentic or tampered.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

IV. ALGORITHMIC DETAILS

The algorithms for: Illuminant map, Face extraction, Edge detection, GLCM, Face detection, LBP and the KNN classifier are discussed as follows:

1. **Illuminant Map:** The illuminant map is obtained from the input image.
   The steps involved in obtaining the illuminant are:
   - Read the image (color image).
   - Resize the image and store the RGB values into each rows and columns.
   - First consider a red pixel value and assign it to x and y variables. Normalized value for red pixel is calculated and then the values are restored in existing x and y values of the red pixel, where n indicates Derivative order, p indicates Minkowski norm and σ indicates Gaussian smoothing.

$$ke^{n,p,\sigma} = \left(\left(\int \left| \frac{\partial^n f^\sigma(x)}{\partial x^n} \right) \right| dx \right)^{\frac{1}{p}} \quad (1)$$

     Here, the integral is computed over all pixels in the image where x denotes a position (pixel coordinate). Furthermore, k denotes a scaling factor, |.| the absolute value, ∂ the differential operator, and f^σ the observed intensities at position x, smoothed with a Gaussian kernel σ.

   - Loop continues for green and blue pixels similarly.
   - All the calculated values are stored in their respective rows and columns.
   - Array multiplication is performed between the RGB pixels to get proper illumination.

2. **Face Extraction:** The illuminant map obtained is subjected for extraction of faces.
   The steps involved in face extraction are:
   - First define the function cascadeobjectdetector by assigning it to a variable.
   - Next call the step method with the input image, I, the cascade object detector, which is assigned to a variable.
     This method performs multi-scale object detection on the input image, I. Each row of the output matrix, BB, contains a four-element vector, [x y width height], that specifies in pixels, the upper-left corner and size of a bounding box.
   - Display the image and construct a loop for defining the size of the bounding box by specifying the curvature of the rectangle sides.
   - Cropped image is created by double clicking on the crop box which was created around the face by making use of the crop tool. This displays the face extracted region.

3. **Edge Detection:** The edges are detected for the face extracted region.
   The steps involved in detection of edges are:
   - The extracted face region is then assigned a variable.
   - The binary input image is then applied with the canny edge detector to detect the edges. The canny is an in-built function used in MATLAB.

4. **GLCM:** The GLCM texture illuminant features are extracted from the edges obtained from the illuminant map**.**
   The steps involved in detection of GLCM texture features are:
   - Assign the edge detection output to a variable k.
   - Apply the gray level co-occurrence matrix function to the assigned variable k to obtain the GLCM features.
   - The GLCM features computed for all the face regions are then combined in matrix form which is then later used for classification.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

5. **Face Detection:** The faces in the input image are detected by using Viola-Jones algorithm.
   - The cascadeobjectdetector in-built function is used to detect the face regions in an image.

6. **LBP:** The steps involved in extraction of LBP texture features are :
   - First the input image is converted to a gray scale image (color image).
   - Initiate a window and place around each pixel.
   - Next, check if the pixel in window greater than center pixel.
   - Generate binary pattern with values 1, 0.
   - Convert binary to decimal and replace in center pixel.
   - Normalize the Image.
   - Divide the normalized image into sub-regions and calculate LBP histograms for every sub-region. The feature histogram is obtained as given by equation (2).

$$H_{i,j=\sum_{x,y} I(f_l(x,y)=i)} \quad (2)$$

   where $I((x,y) \in R$, i = 0,....n-1 in where n is the number of different labels produced by the LBP operator, j=0,...m-1 where m is the number of blocks obtained by segmenting the image into regions, f_l (x ,y) is the labelled image obtained from the LBP operator given as $LBP_{P,R}^{u2}$. The subscript represents using the operator in a (P, R) neighborhood. I (A) is 1 if A is true and it is 0 if A is false.

7. **Pairing of GLCM and LBP Texture Features:** The GLCM texture features obtained in the first stage is combined with the LBP texture features which is obtained from the second stage. These combined features are sent to the KNN classifier which compares the features with the training features and classifies the image as original or forged.

8. **KNN:** The algorithm for KNN can be summarised as:
   - A positive integer k is specified with a new sample.
   - From the database K passages are chosen which is closest to the new sample.
   - The most basic characterization of these entries is found.
   - This is the classification that is given to the new sample.

V. EXPERIMENTAL RESULTS

The proposed system is evaluated using two datasets: The dataset 1 consists of 40 images (20 original and 20 forged). The dataset 2 consists of 40 images downloaded from the internet. The original images in dataset 1 are shot with a high definition camera to obtain the images of high quality for good illumination. The dimension of the images that are taken varies from 250*201 pixels to 541*250 pixels. The forged images in dataset 1 are created using the Adode Photoshop cs6 (64 bit) software on windows 8 operating system. These images can be used for the detection of splicing image forgery detection. The dataset 2 is composed of 40 images which are downloaded from the internet. The images collected from the internet consist of 20 original images and 20 forged images. The dimension of the images that are taken varies from 250*201 to 260*194 pixels. MATLAB codes are developed for verifying the approach.

All the images used in the testing phase are tested and the results obtained for one of the image used for testing are shown in the following Figures 2, 3, 4, 5 and 6 respectively. The input image in Figure 2 is verified for forgery detection. The illuminant map is obtained from the input image using the statistical generalized gray world estimator as shown in Figure 3. From the obtained illuminant map the face regions in the image is extracted by marking bounding boxes around each face in the image. The extracted face region is subjected to edge detection by utilizing canny edge detector. The Figure 4 shows the edge detection for the first face in Figure 2. Similarly, the second face in the image is extracted and subjected to edge detection.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Figure 2: Input Image

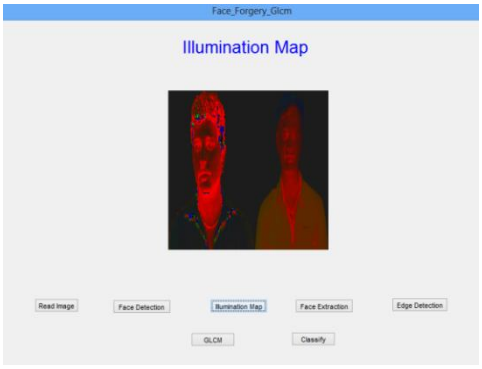

Figure 3: Illuminant Map

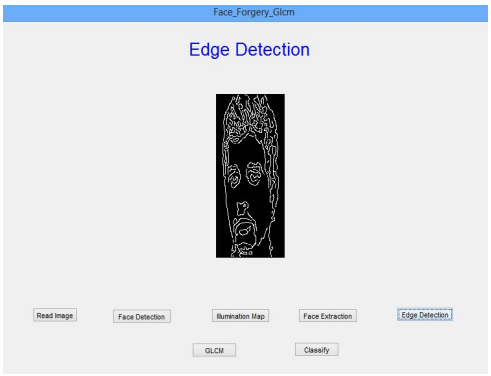

Figure 4: Edge Detection

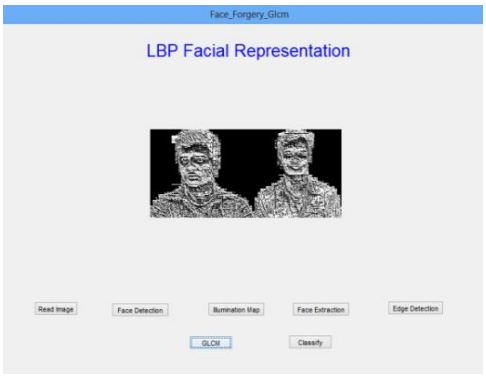

Figure 5: LBP based Facial Representation

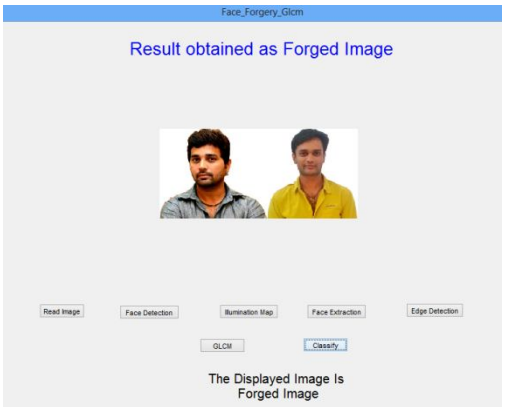

Figure 6: Result Classified as Forged Image

The GLCM and the LBP features are computed for both the faces in the image and thus the features are combined and paired in matrix form. The LBP based facial representation for both the faces in the image is shown in Figure 5. The paired features are sent to the KNN classifier where it compares with the training features to check whether the image is forged or not. The final result obtained is shown in Figure 6. Thus the image considered is classified correctly as forged image by the KNN classifier. Similarly the results are evaluated for images in dataset 2.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

VI. CONCLUSIONS

The need for image forgery detection is very much essential since the huge advancement in digital image editing tools has made the manipulators little easy to create a forged image. In this paper, a new method for splicing forgery detection based on the GLCM and the LBP texture features is presented. Estimation of the illuminant color is done using the Statistical generalized gray world estimator. The edges for the extracted faces from the illuminant map were detected using a canny edge detector. The GLCM features obtained from the first stage is combined with the LBP features computed from the second stage and are sent to the KNN classifier for classification. The algorithm requires a minimal user interaction to detect the image as original or forged. All the images in both the datasets are tested and classified by the KNN classifier.

It is difficult to decide whether the image is spliced or not from IM in some of the images. Thus, further improvements can be achieved by improving the learning. The fusion algorithm is a classifier that receives the likelihoods from the others single-classifiers and decides the class [16]. Two or more different classifiers can be combined for spliced detection.

REFERENCES

[1] Tiago José de Carvalho, Christian Riess, Elli Angelopoulou, Hélio Pedrini, and Anderson de Rezende Rocha, "Exposing Digital Image Forgeries by Illumination Color Classification", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 7, pp. 1182 - 1194 2013.

[2] C. Riess and E. Angelopoulou, "Scene Illumination as an Indicator of Image Manipulation," Conference on Information Hiding, Calgary, Canada, pp. 66-80, 2010.

[3] Johnson MK, Farid H, "Exposing Digital Forgeries by Detecting Inconsistencies in Lighting", Proceedings of the Seventh Workshop on Multimedia and Security, New York, pp. 1–10, 2005.

[4] Alahmadi, A.A. Hussain, M. Aboalsamh, H. Muhammad, and G. Bebis, "Splicing Image Forgery Detection Based on DCT and Local Binary Pattern", IEEE Global Conference on Signal and Information Processing (Global SIP), pp. 253 - 256, 2013.

[5] J.van de Weijer, T. Gevers, and A. Gijsenij, "Edge-based Color Constancy", IEEE Transactions on Image Processing, Vol. 16, No. 9, pp. 2207–2214, 2007.

[6] Timo Ahonen, Abdenour Hadid, and Matti Pietikainen, "Face Description with Local Binary Patterns: Application to Face Recognition", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 28, No. 12, pp. 2037-2041, 2006.

[7] Liya Baby and Ann Jose, "Detection of Splicing in Digital Images Based on Illuminant Features", International Journal of Innovation and Scientific Research, Vol. 11, No. 1, pp. 126-129, 2014.

[8] M.H. Yang, "Kernel eigenfaces vs. fisherfaces: Face Recognition using Kernel Methods", Proceedings of Fifth International Conference on Automatic Face and Gesture Recognition, pp. 215-220, 2002.

[9] Xuemin Wu and Zhen Fang Image, "Image Splicing Detection Using Illuminant Color Inconsistency", Third International Conference on Multimedia Information Networking and Security (MINES), pp. 600 - 603, 2011.

[10] A. Gebejes, R. Huertas Gebejes, A. Huertas, R. Tomic, and I. Stepanic, "Grey-Level Co-occurrence Matrix", Color and Visual Computing Symposium (CVCS), pp. 1-5, 2013.

[11] Mohammad Farukh Hashmi and Avinash G. Keskar, "Image Forgery Authentication and Classification using Hybridization of HMM and SVM Classifier", International Journal of Security and its Applications, Vol. 9, No. 4 , pp. 125-140, 2015.

[12] P. Mohanaiah, P. Sathyanarayana, and L. GuruKumar, "Image Texture Feature Extraction Using GLCM Approach", International Journal of Scientific and Research Publications, Vol. 3, No. 5, 2013.

[13] K. Barnard, L.Martin, A.Coath, and B.Funt, "A Comparison of Computational Color Constancy Algorithms – Part II: Experiments with Image Data," IEEE Transactions on Image Processing, Vol. 11, No. 9, pp. 985–996, 2002.

[14] J. Canny, A Computational Approach to Edge Detection, IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol. 8, No. 6, pp. 679-698, 1986.

[15] M. Benco M and R. Hudec, "Novel Method for Color Texture Features Extraction based on GLCM", Conference on Radioengineering, Vol. 16, No. 4, pp. 64-67, 2007.

[16] O. Ludwig, D. Delgado, V. Goncalves and U. Nunes, "Trainable Classifier-Fusion Schemes: An Application to Pedestrian Detection", Proceedings of Twelfth IEEE International Conference on Intelligent Transportation Systems, pp. 1–6, 2009.