Exposing Digital Image Forgeries by Illumination Color Classification

Ms. Shraddha R. Asati *1 , Mr. Sudarshan Awale*2
Assistant Professor, CSE Department, SSPACE, Wardha, India1
asati.shraddha810@gmail.com
Assistant Professor, CSE Department, PIGCOE, Nagpur, India2
sudarshanawale@gmail.com

Abstract:

In this digital era, lots of information is expressed through images. A variety of social networking websites and mobile applications such as Facebook, Twitter, MySpace, Whatsapp, hike, etc. provides a platform for the users to post any type of images or photo. However, with the development in image editing technologies, large number of users has become victims of digital forgery as their uploaded images were forged for malicious activities. Photo Manipulation is the process of editing a photograph in such an extreme way that it takes on an entirely different look.The motivation for the recognition of forged images is the need of authenticity and to keep the reliability of the image. In this paper we are presenting a semiautomatic machine learning method for detecting the forgery is considered due to image composition or splicing. This method is only applicable to the images containing the faces of two or more human being. We make valuation in the areas of faces only. First of all convert the RGB digital image into a gray image and YCbCr format. At this point LBP features and edge based features are extracted from gray image and then extract the GLCM feature from the illuminant map of an image .To evaluate two faces, we combine the same descriptors for each of the two faces. The idea behind that a feature concatenation from two faces is different when one of the faces is an original and one is forged. Here we are using SVM classifier for categorizing the digital image as whether it is original or spliced.

Keywords: Support Vector Machine (SVM), Local Binary pattern, machine learning, GLCM feature, illumination.

1. INTRODUCTION:

These days' digital images are all over from our mobiles to the online sites. Photography is essential because it put emphasis on the information through the visual capture of the things as they actually are. This means a huge amount of visualinformation is offered to the users every time. People have emotional reaction towards the images. People belief in whatever they see rather than what they read or hear. The Data protection Act (DPA) is boarded upon all the images containing private data however there is some dishonest ambiguity in this. This is well-known as forgery in the images. Forgery of an image means inserting a fake thing, object or image into the original image which is not simple to recognize. With the easy availability of low price digital cameras in the market, high speed internet services as well as powerful image editing software it is not complicated to tamper the images without having anexcellent knowledge in that field. It will acutelytouch the authenticity of the image. Thus,Today Digital Image Forensics is a developing research area that goals at authenticating the images and to identify various image forgery possibilities. People have used image according to their need and these forgeries have been put to many uses. For example Journalists who want to write their own stories, dramatic scenes produced by photo journalist repetition of images in scientific paper by politicians or scientists who give their public view by wrongly creating political pictures or events. Therefore to maintain the integrity and authenticity of the image we propose a detection method. The more importance is on that kind of images on which the detection process will be used. The images must strictly have minimum two or more faces of human being. We propose the method based on the illumination of the color of each face in the image. There are basically two types in this either inconsistent or consistent .When the illuminant estimates are found, then the texture and edge based features are provided to machine-leaning approach for the tampering of the decision. We suggest a new semiautomatic approach for detection of forgery in the photography. The SVM classifier is used for the tamperingdecision. Firstly find out the illuminant map and gray image of the original image. Then find the faces from that image for that we are using the violo john technique. After face recognition extract the LBP feature from the gray image& also detect the GLCM (Gray Level Co-Occurrence Matrix). For animage having minimum two or more faces, we tend to construct joint feature vectors consisting of all potential pairs of faces to compare two faces. Then it will pass to the SVM classifier for the training purpose. The trained classifier will concludethat whether it is an original image or forensic image.

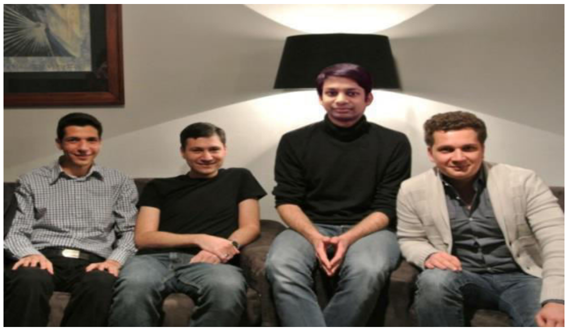

Fig.1. Example of a composite image involving people.

Image composition (or splicing) is very well-known image manipulation process. One such example is shown in Fig. 1,is a composite image in which there are group of boys .The boysare sitting 2nd and 3rd from left are inserted. But this type of image shows aninnocent manipulation case, there are several more controversial cases have been reported.

2.FORGERED IMAGE

These days' digital images play very essential role in areas like forensic investigation, insurance processing, intelligence services, surveillance systems, medical imaging and journalism. With the improvement of knowledge, technology and availability of fast computing resources, it is not very difficult to manipulate or forge the digital images. Before discussion of forgery detection methods; it is necessary to know about the different types of manipulation done with various digital images. There are several ways to classify the image tampering based on different points of view. Generally; we can say that the most commonly performed operations in image tampering are:

- Hiding or removing a region from the original the image.
- Adding a different object into the original image.

• Misrepresenting the important information in the image.

Copy move image tampering is one of the mostfrequently used techniques to hide or manipulate the information of the image. Some part of the original image or some new image is paste on another part of image. To identify the region of some other image statistical methods may work but if the region pasted belongs to the similar image then it is very difficult to detect this forgery. Many methods have been suggested to detect this type of forgery.

3. METHOD DETAILS

3.1 DENSE LOCAL ILLUMINANT ESTIMATION

Dense local illuminant estimation is carry out by subdividing the input image into super pixels.The illuminant color of each superpixel of input image is estimated. Here we convert the input image into YCbCr format and gray image.YCbCr is a family of color spaces which is used as a part of the color image pipeline in video and digital photography system. Y is the luma component where CB and CR are the blue-difference and red-difference chroma components.

3.2 FACE EXTRACTION

The illuminant color estimation is error prone and is affected by various materials in the scene. Here we consider the illuminant of each of the faces in the image because local illuminant estimates are most discriminative when comparing objects of similar material. This can be performed either in automatic or semiautomatic method. Then we find the face from the image and for that here we are using the violo john technique. Object Detection using Haar feature-based cascade classifiers is an efficient object detection technique proposed by Paul Viola and Michael Jones. This is a machine learning based approach where a cascade function is trained from lots of positive and negative images. It is used as to detect objects in other images. Now we will only work with face detection. Firstly, the algorithm requires a lot of positive images (images of faces) and negative images (images without faces) to train the classifier. Then we want to extract features from it. For this, haar features shown in below image are used. this is a fully automated technique but we also used semiautomatic face detection to avoid false detection of faces. It is the only step where a human operator is required to draw bounding boxes around the faces in the image which is not recognized by the automatic technique. Than crop the bounding boxes out of the illuminant map to obtain the illuminant estimates of the face region only.

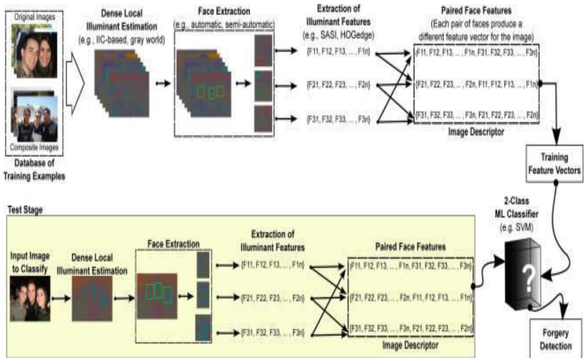
Original Images
Composite Images
Database of Training Examples
Dense Local Illuminant Estimation (e.g., IIC-based, gray world)
Face Extraction (e.g., automatic, semi-automatic)
Extraction of Illuminant Features (e.g., SASI, HOGedge)
{F11, F12, F13, ..., F1n}
{F21, F22, F23, ..., F2n}
{F31, F32, F33, ..., F3n}
Paired Face Features (Each pair of faces produce a different feature vector for the image)
{F11, F12, F13, ..., F1n, F31, F32, F33, ..., F3n}
{F21, F22, F23, ..., F2n, F11, F12, F13, ..., F1n}
{F31, F32, F33, ..., F3n, F21, F22, F23, ..., F2n}
Image Descriptor
Training Feature Vectors
2-Class ML Classifier (e.g. SVM)
Test Stage
Input Image to Classify
Dense Local Illuminant Estimation
Face Extraction
Extraction of Illuminant Features
Paired Face Features
Image Descriptor
Forgery Detection

Fig.2. Overview of proposed system.

3.3 EXTRACTION OF ILLUMINANT FEATURES

Feature extraction is a reduction method in which the input data is transformed into a reduced representation. The transformation of input data into a set of features is called feature extraction. Texture based feature is extracted by using LBP feature extraction and GLCM feature extraction from each of the faces in the image.

LBP Feature Extraction:

LBP is a very effective method to explain the texture and shape of a digital image. Therefore this methodis suitable for feature extraction in face recognition systems. A face image is initially divided into small regions from which LBP histograms are extracted and then it is concatenated into a single feature vector. These features areconsisting of binary patterns that describe the surroundings of pixels in those regions. The obtained features from those regions are concatenated into a single feature histogram, which forms a representation of the image. Then images can be compared by evaluating the similarity (distance) between their histograms. The method seems to be quite robust against face images with different facial expressions, different lightening conditions, image rotation and aging of persons because of the way the texture and shape of images is described.

The operator works with the eight neighbors of a pixel, using center pixel as a threshold value. If any neighbor pixel has a higher gray value than the center pixel (or the same gray value) than one is assigned to that pixel, else assigned zero to that pixel. The LBP code for the center pixel is then calculated by concatenating the eight values(ones or zeros) to a binary code as shown in figure 3.

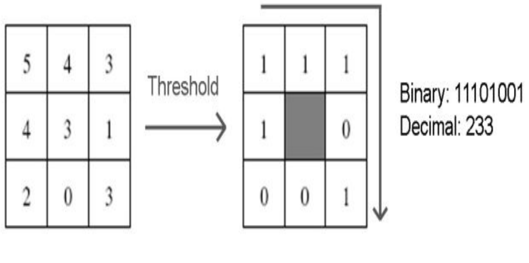

Fig.3.The original LBP operator

Once the LBP for every pixel is calculated then feature vector of the face image can be constructed. For an efficient representation of the face, initially the image is divided into k2 regions.For every region (obtain by dividing the image) a histogram with all possible labels is constructed. This means that each and every bin in a histogram represents a pattern and it contains the number of its appearance in the region. The feature vector is then constructed by concatenating all regional histograms to one big histogram.

The mostsignificant property of the LBP operator in real-world application is its tolerance against illumination changes. It is possible to analyze images in challenging real time settings due to its computational simplicity. Assigning weights to the different regions of the image improves the recognition performance drastically. This is especially true for faces from which the photographs are taken under different lighting conditions. Eyes and the mouth are the important regions for feature extraction.

GLCM Feature Extraction:

In statistical texture analysis, texture features are measured from the statistical distribution of observed combinations of intensities at specified positions relative to each other in the image. According to the number of intensity points (pixels) in each combination, statistics are divided into first-order, second-order and higher-order statistics. The Gray Level Coocurrence Matrix (GLCM) process is a method of extracting second order statistical texture features.

A GLCM is a matrix where the number of rows andnumber of columns is equal to the number of gray levels, G, in the image. The matrix element P (i, j | Δx, Δy) is the relative frequency with which two pixels are separated by a pixel distance (Δx, Δy) and occur within a given neighborhood, one with intensity „i" and the another one with intensity „j". The matrix element P (i, j | d, ɵ) have the second order statistical probability values for changes between gray levels „i" and „j" at a particular displacement distance (d) and at a particular angle (ɵ). With a large number of intensity levels G implies storing a lot of temporary data, i.e. a G × G matrix for each combination of (Δx, Δy) or (d, ɵ). The GLCM are very sensitive to the size of the texture samples on which they are estimated due to their large dimensionality. As a result, the number of gray levels is often reduced. GLCM matrix calculation can be explained with the example illustrated in fig 4 for four different gray levels. Here we are using one pixel offset (a reference pixel and its immediate neighbour). The top left cell will be filled with the how many number of times the combination 0,0 occurs, i.e. how many time within the image area a pixel with grey level 0 (neighbour pixel) falls to the right of another pixel with grey level 0(reference pixel).

neighbour pixel value ---> ref pixel value:	0	1	2	3
0	0,0	0,1	0,2	0,3
1	1,0	1,1	1,2	1,3
2	2,0	2,1	2,2	2,3
3	3,0	3,1	3,2	3,3

Fig 4. GLCM calculation

3.4 PAIRED FEATURE CREATION

In this step all the face pairs in the image are detected and feature vector of each of the face in the image is concatenated with other face in the pair. To compare two faces,

here we combine the same descriptors for each of the two faces.The idea behind that feature concatenation of two faces is different when one face is original and the other is forged. For an image having nf faces(nf>=2) , the number of face pairs is (nf(nf-1))/2. The LBP and GLCM descriptors contain two different properties of the face regions. From a signal processing point of view, both descriptors i.e LBP and GLCM descriptors are signatures with different behavior. We exploit this property through classification by fusing the output of the classification on both feature sets, as explained in the nextsection.

3.5 CLASSIFICATION

We classify the illumination for each pair of faces in an image whether it is consistent or inconsistent. If we assumethat all selected faces are illuminated by the same light source then we tag an image as manipulated if one pair is classified as inconsistent. Individual feature vectors classification is done by using a support vector machine (SVM) classifier.

4 EXPERIMENTAL RESULTS

To quantitatively evaluate the proposed algorithm, here we considered a dataset composed of 60 images. The dataset is consist of number of images that we captured ourselves; forgeries were created by adding one or more individuals in a original image that already contained one or more persons and images collected from the web.

Performance of Forgery Detection UsingFully Automated and Semiautomatic Face Detection

• Automatic Detection:

We used the violaJones based face detector method to detect faces in the images. In our experiment, the automatic face detector successfully located all present faces in only 65% of our images. To training the classifier, we used the manually annotated bounding boxes around the face. In the test images, we used the bounding boxes found by the automated face detector.

Semiautomatic Detection (Corner Clicking):

In this method, we used the same marking procedure as giving the diagonal values of face and create the bounding box around it and remaining procedure is same as in automatic detection. We find user-selected faces are more reliable for a forensic setup then automatic face detection.Because automated face detection algorithms are not accurate in bounding box detection (location and size). In our experiments, the detector successfully located all present faces in only 86% of our images.

5 CONCLUSIONS

Here new technique for detecting forged images of people using the illuminant color has been discussed. The illuminant colors a physics-based method and a statistical gray edge method which exploits the inverse intensity chromaticity color space has been measured. This illuminant map is considered as texture maps. Then information on the distribution of edges on illuminant maps is extracted. Good results are also achieved over web images and under cross-database training/testing. The proposed system have need of only a least amount of human interaction and provides a crisp statement on the authenticity of the image. Additionally, it is a significant progress in the exploitation of illuminant color as a forensic cue.

6 REFERENCES

[1] Tiago Jose de Carvalho,Christian Riess,Elli Angelopoulou and Helio Pedrini "Exposing Digital Image Forgeries By Illumination Color Classification" IEEE Trans. Inf. Forensics Security ,Vol. 8, no. 7, pp. 1182 - 1194, July 2013.

[2] R. Kawakami, K. Ikeuchi, and R. T. Tan, "Consistent surface color for texturing large objects in outdoor scenes," in Proc. IEEE Int. Conf. Comput. Vision, 2005, pp. 1200–1207.

[3] S. Gholap and P. K. Bora, "Illuminant colour based image forensics," in Proc. IEEE Region 10 Conf., 2008, pp. 1–5.

[4] J. F. O‟Brien and H. Farid, "Exposing photo manipulation with inconsistent reflections," ACM Trans. Graphics, vol. 31, no. 1, pp. 1–11, Jan. 2012.

[5T. Ahonen, A. Hadid and M. Pietikäinen, "Face recognition with local binary patterns. Computer Vision", ECCV 2004 Proceedings, Lecture Notes in Computer Science 3021, Springer, pp. 469-481, 2004.

[6] M. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," in Proc. ACM Workshop on Multimedia and Security, New York, NY, USA, 2005, pp. 1–10.

[7] T. Ojala, M. Pietikainen, and D. Harwood, "A comparative study of texture measures with classification based on feature distributions," Pattern Recognition, vol. 29 , 1996, pp. 51-59.

[8] T. Ahonen, A. Hadid and M. Pietik¨ainen. Face recognition with Local Binary Patterns. Machine Vision Group, University of Oulu, Finland, 2004.

[9] W. Fan, K. Wang, F. Cayre, and Z. Xiong, "3D lighting-based image forgery detection using shape-from-shading," in Proc. Eur. Signal Processing Conf. (EUSIPCO), Aug. 2012, pp. 1777–1781.

[10]Mryka Hall-Beyar,GLCM Tutorial,February 2007 [Online] Available: http://www.fp.ucalgary.ca/mhallbey/tutorial.htm (February 21, 2007).

[11] R. Tan, K. Nishino, and K. Ikeuchi, "Color constancy through inverse- intensity chromaticity space," J. Opt. Soc. Amer. A, vol. 21, pp. 321–334, 2004.

[12] J. van de Weijer, T. Gevers, and A. Gijsenij, "Edge-based color constancy,"

IEEE Trans. Image Process., vol. 16, no. 9, pp. 2207–2214, Sep. 2007.

[13] H. R. Chennamma, Lalitha Rangarajan "Image Splicing Detection Using Inherent Lens Radial Distortion" IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 6, November 2010.pp 149-158.

[14] T. Ahonen, A. Hadid and M. Pietikäinen, "Face recognition with local binary patterns. Computer Vision", ECCV 2004 Proceedings, Lecture Notes in Computer Science 3021, Springer, pp. 469-481, 2004.