IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 9, Issue 2 Ver. I (Mar – Apr. 2014), PP 47-52
www.iosrjournals.org

Automatic Image Forgery Exposure using Illuminant Measure of Face Region and Random Object Detection Method

[1]C. Prabhu, [2]Geethu Priya. P
[1]*Assistant Professor, Dhanalakshmi Srinivasan College Of Engineering, Coimbatore*
[2]*Dhanalakshmi Srinivasan College of Engineering, Coimbatore.*

Abstract: *For decades, photographs have often served as evidence in courts. One of the most common forms of photographic manipulation, known as image composition or splicing is analysed in this paper. The goal of blind image forensics is to distinguish original and manipulated images. We propose illumination color as a new indicator for the assessment of image authenticity. Many images exhibit a combination of multiple illuminants (ash photography, mixture of indoor and outdoor lighting, etc.). In the proposed method, the user selects illuminated areas for further investigation. The illuminant colors are locally estimated, effectively decomposing the scene in a map of differently illuminated regions. Inconsistencies in such a map suggest possible image tampering.The information from the physics and statistical-based illuminant estimators on image regions are incorporated to achieve this. From these illuminant estimates, texture and edge-based features are extracted and then provided to a machine-learning approach for decision-making. The classification performance is done by using a Random forest classifier. Automatic face detection is used in order to improve the accuracy of the result.*
Keywords: *Physics and statistical based illuminant estimator, texture, edge based features, Random forest, and automatic face detection.*

I. Introduction

The digital images can be easily tampered by using different methods. And today the society is facing a major problem of digital image forgery. A lot of fake images can be found in facebook, twitter, different magazines etc. This will leads to sever problems even in making the victims to commit suicide. Whoever said the photographs never lie was a liar [7]. Understanding the authenticity and validity of a digital image is always a problem and challenge for organizations especially who are working on e-forms and e-documents.

Now a days, there are several powerful tools for editing digital images, therefore it is possible to someone use these tools to change contents of digital images [2]. When assessing the authenticity of an image, forensic investigators use all available sources of tampering evidence. Among other telltale signs, illumination inconsistencies are potentially effective for splicing detection. From the viewpoint of a manipulator, proper adjustments of the illumination conditions are hard to achieve when creating a composite image [4]. The assessments of these illuminant inconsistencies are manually very difficult and sometimes it will result in misleading, so it will be better to use an objective algorithm.

The illumination color is a new indicator for the assessment of image authenticity. Many images exhibit a combination of multiple illuminants (mixture of indoor and outdoor lighting, etc.). In this method, the user selects illuminated areas for further investigation [1]. The illuminant features are difficult to match while making the manipulated images. The images taken at the same time by using the same camera will have almost same illuminant features.

The contemporary digital revolution has changed the way we access, manipulate and share information, but these advancements have also introduced critical security issues that shake people's confidence in the integrity of digital media [6]. Sophisticated digital technology and photo-editing software, such as Adobe Photoshop, are ubiquitous and have made the process of manipulating images to create forgeries a fairly accessible practice [3]. As a result, trust in digital imagery has been eroded. This situation is propelled by the excessive number of images floating virtually around us on the World Wide Web. The authenticity of the photos becomes particularly critical when their impact spans political and social arenas. Digital forgery is indeed a nightmare to individuals (example: faked images of celebrities and public figures), societies (example: provocative fake images targeting certain ethnicity, religion or race), journalism, and even scientific publication [5]. But image manipulation is not a particularly new phenomenon and can be traced as far back as the invention of photography itself.

II. Block Diagram Of Random Object Detection Method

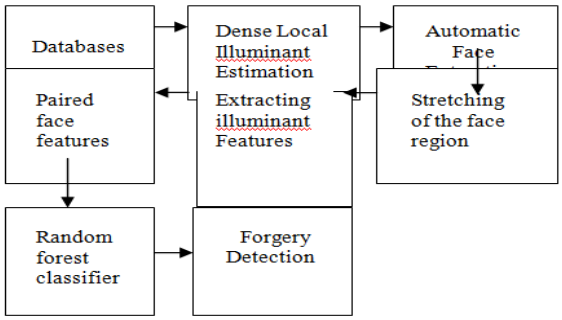

Fig 1: Block diagram of proposed system

III. Forgery Detection Description

The databases are the collected photographs. Then these images are segmented into super pixels. A user selects such super pixels whose incident illuminant wants to further investigate. Estimation of the illuminant color is performed twice. Automatic face detection can be used to extract the faces. Then both texture based features and edge based features are extracted. All the features extracted are then paired for comparison purposes. An illuminant estimator is used to extract the illuminant features from the photographs. Then pairing of the features will be done and the image will be classified as consistent or inconsistent. By using these forgery is detected.

IV. Related Works

A. Dense Local Illuminant Estimation

To compute a dense set of localized illuminant color estimates the input image is segmented into super pixels, that is, regions of approximately constant chromaticity. Per super pixel, the color of the illuminant is estimated. Two separate illuminant color estimators: the statistical generalized gray world estimates and the physics-based inverse-intensity chromaticity space are used. Thus obtain two illuminant maps by re-coloring each super pixel with the estimated illuminant chromaticities of each one of the estimators. Both illuminant maps are independently analysed in the subsequent steps.

i) Generalized Gray World Estimate

The classical gray world assumption states that the average color of a scene is gray. Thus, a deviation of the average image intensities from the expected gray color is due to the illuminant. The original gray world hypothesis is extended through the incorporation of following parameters,

i) Derivative order: The assumption that the average of the illuminants is achromatic can be extended to the absolute value of the sum of the derivatives of the image.

ii) Gaussian smoothing: To reduce image noise, one can smooth the image prior to processing with a Gaussian kernel of standard deviation.

Gray world is among the simplest estimation methods. The main premise behind it is that in a normal well color balanced photo, the average of all the colors is a neutral gray. Therefore, estimation of the illuminant color cast is done by looking at the average color and comparing it to gray.

ii) Inverse Intensity – Chromaticity Estimates

The second illuminant estimator is called inverse intensity-chromaticity (IIC). In contrast to the previous approach, the observed image intensities are assumed to exhibit a mixture of diffuse and specular reflectance. Pure specularities are assumed to consist of only the color of the illuminant.

B. Automatic Face Detection

The process requires bounding boxes around all faces in an image that should be part of the investigation. For obtaining the bounding boxes, use an automated algorithm. However, prefer an automatic operation for this task for main reasons like, this minimizes false detections or missed faces, Scene context are important when judging the lighting situation.

C. Inconsistencies in Illumination

The same process that used in computing the illuminant color estimates at the user-specified regions is now extended to the entire image. The voting, however, is now performed for every super pixel. Thus, every super pixel contains an individual illuminant estimate and store these illuminant estimates in a new image, where each super pixel is colored according to its estimated illuminant color. This new image is

called illumination map. This map gives already quite meaningful results for the analysis. Forensic analysis aims at quantifying the relationship between the illuminant estimates. In a scene with truly one dominant illuminant, this can be done by comparing the angular errors of the individual illuminant estimates. However, most real-world scenes contain a mixture of illuminants. Their influence on the scene is closely connected to the positions of the objects relative to the positions of the light sources. Since the geometric composition of the scene is typically unknown a tool for supporting the visual assessment of the scene, which is called distance map is developed.

The distance map captures how well the illuminant estimation at each super pixel fits to the estimated dominant illuminants. For improved clarity, assume two dominant illuminants I1 and I2 that were obtained from two user-selected regions. The methodology can however easily generalize to more illumination sources. The aim is to create a grayscale image that depicts the relative influence of both light sources. The distance map is created by assigning the value 0 (black) to the user-defined region corresponding to illuminant I1. Similarly, the second user-defined region, which gave rise to dominant illuminant I2, is assigned the value 1 (white).

D. Face pairing

To compare two faces of images, combine the same descriptors for each of the two faces. For instance, concatenate the SASI-descriptors that were computed on gray world. The idea is that feature concatenations from two skin-faces are different when one of the skin-faces is an original and one is spliced. The SASI and HOG edge descriptors capture two different properties of the skin-face regions. From a signal processing point of view, both descriptors are signatures with different behaviour. For a less cluttered plot, only visualize the feature dimensions with the largest difference in the mean values for this fold.

SASI and HOG edge, in combination with the IIC-based and gray world illuminant maps create features that discriminate well between original and tampered images, in at least some dimensions. The dimensions, where these features have distinct value, vary between the four combinations of the feature vectors. This exploits the property during classification by fusing the output of the classification on both feature sets.

E. Classification using Random forest classifier

The illumination for each pair of faces in an image is classified as either consistent or inconsistent. Assuming all selected faces are illuminated by the same light source, tag an image as manipulated if one pair is classified as inconsistent. Individual feature vectors, SASI or HOG edge features on either gray world or IIC-based illuminant maps, are classified using a random forest classifier with a radial basis function (RBF) kernel .The information provided by the SASI features is complementary to the information from the HOG edge features. Thus uses a machine learning based fusion technique for improving the detection performance.

V. Performance Analysis

To evaluate the performance and to compare it to related work, we considered two datasets. One consists of images that we captured ourselves, while the second one contains images collected from the internet. Additionally, we validated the quality of the forgeries using a human study on the first dataset. Human performance can be seen as a baseline for our experiments.

1) DSO-1: This is our first dataset and it was created by us. It is composed of 200 indoor and outdoor images with an image resolution of 2048*1536 pixels. Out of this set of images, 100 are original, have no adjustments whatsoever, and 100 are forged. The forgeries were created by adding one or more individuals in a source image that already contained one or more persons. When necessary, we complemented an image splicing operation with post-processing operations (such as color and brightness adjustments) in order to increase photorealism.

2) DSI-1: This is our second dataset and it is composed of 50 images (25 original and 25 doctored) downloaded from different websites in the Internet with different resolutions.

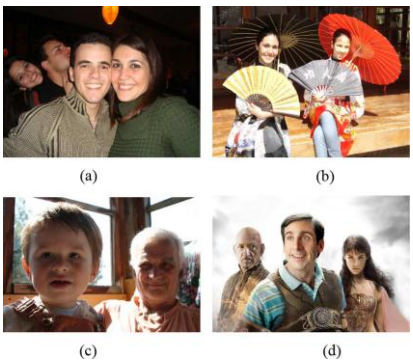

Fig 2: Original (left) and spliced images (right) from both databases. (a) DSO-1 Original image. (b) DSO-1 Spliced image. (c) DSI-1 Original image. (d) DSI-1 Spliced image.

VI. Results

For experimental comparison, we implemented the methods used earlier. Note that neither of these works includes a quantitative performance analysis. Thus, to our knowledge, this is the first direct comparison of illuminant color-based forensic algorithms. For the earlier algorithm three partially specular regions per image were manually annotated. For manipulated images, it is guaranteed that at least one of the regions belongs to the tampered part of the image, and one region to the original part. Fully saturated pixels were excluded from the computation, as they have presumably been clipped by the camera. Camera gamma was approximately inverted by assuming a value of 2.2.

The maximum distance of the dichromatic lines per image was computed. The threshold for discriminating original and tampered images was set via five-fold cross-validation, yielding a detection rate of 55.5% on DSO-1.

In the implementation of the method, the Weibull distribution is computed in order to perform image classification prior to illuminant estimation. The training of the image classifier was performed on the ground truth dataset. As the resolution of this dataset is relatively low, we performed the training on a central part of the images containing 180 *240 pixels (excluding the ground-truth area).

To provide images of the same resolution for illuminant classification, manually annotated the face regions in DSO-1 with bounding boxes of fixed size ratio. Setting this ratio to 3:4, each face was then rescaled to a size of 180*240 pixels. As the selection of suitable reference regions is not well-defined (and also highly image-dependent), directly compare the illuminant estimates of the faces in the scene. Here, the best result was obtained with three-fold cross-validation, yielding a detection rate of 57%. Here also performed five-fold cross-validation.

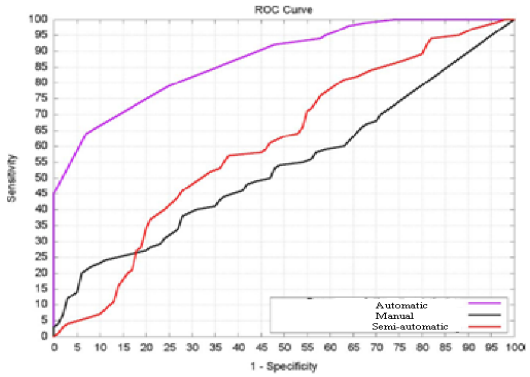

Fig 3: Comparative results between automatic, semi automatic and manual selections.

The results drop to 53% detection rate, which suggests that this algorithm is not very stable with respect to the selection of the data. To reduce any bias that could be introduced from training on the dataset, repeated the image classifier training on the reprocessed ground truth dataset. During training, care was taken to exclude the ground truth information from the data. Repeating the remaining classification yielded a best result of 54.5% on two-fold cross-validation, or 53.5% for five-fold cross-validation.

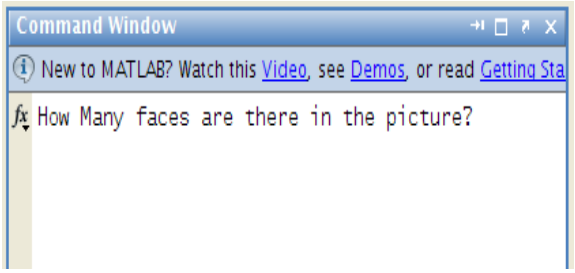

Fig 4: Confirming number of faces

An operator sets automatic bounding box around each face in the image that should be investigated. It can also be performed semi-automatically, by selecting a Euclidian distance from eye portion in the face. But the probability for occurrence of error in this selection will be higher. In semi-automatic selection by clicking at a corner or at the location of eye, a particular distance from the eye or corner will be bounded.

For all face regions texture based and gradient based features are computed. The main goal is to assess whether a pair of faces in an image is consistently illuminated. A machine learning approach is used to classify the images as consistent or inconsistent.

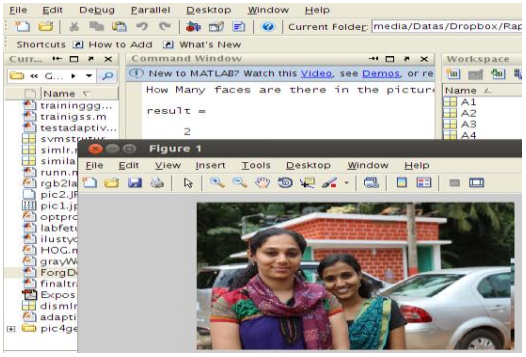

Fig 5: Bounding the faces

This is the input image which is given. After giving the number of faces, if it is correct then the input image will be appeared in the screen. Then the faces in this image should be bounded. After the selection of the faces the illuminant features of the faces will be verified as in figure 5. The selection of the faces should be proper otherwise the detection will be gone wrong. So only the portions of the faces are needed to be bounded properly.

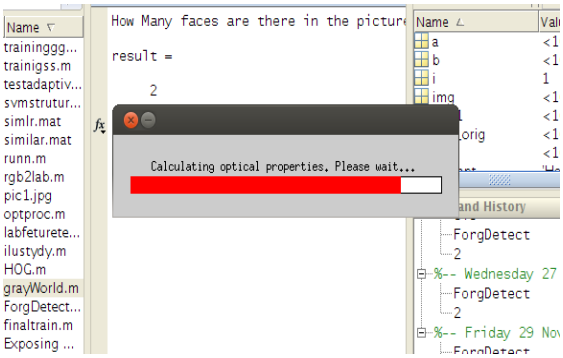

Fig 6: Verifying the illuminant features

Based on the illumination features in the faces present in an image the forgery is identified. The images taken using the same camera at a single time will have same illuminant features. Otherwise the light constancy will be different for each image.

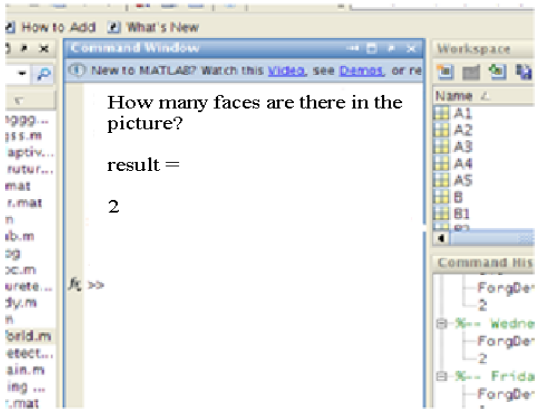

Fig 7: Forgery detection

Before verifying the result one should know the number of faces in the image. If the number of faces given goes wrong then the output will not be displayed. If the illuminant features of each faces in the given input image are same then the output will be displayed as "not detect any forgery" otherwise it will be shown as "this is a forger image" like in the figure 7. An image is considered as forged if at least one of the faces in the image is classified as inconsistently illuminated.

VII. Conclusion

In this work, a new method for detecting forged images of people using the illuminant color is presented. The illuminant color using a statistical gray edge method and a physics-based method which exploits the inverse intensity- chromaticity color space is estimated. These illuminant maps are treated as texture maps. Information on the distribution of edges on these maps is also extracted. In order to describe the edge information, a new algorithm based on edge-points and the HOG descriptor, called HOG edge are developed. These complementary cues (texture- and edge-based) using machine learning late fusions are combined. Good results are also achieved over internet images.

The method provides a crisp statement on the authenticity of the image. Additionally, it is a significant advancement in the exploitation of illuminant color as a forensic cue. Prior color-based work either assumes complex user interaction or imposes very limiting assumptions.

Acknowledgment

I, GEETHU PRIYA.P, student of M.E COMMUNICATION SYSTEMS, Dept. of ECE, Dhanalakshmi Srinivasan College of Engineering, Coimbatore would like to thank Asst. Prof. Mr.C.Prabhu for his encouragement and constant co-operation throughout the completion of the paper. I deeply express my gratitude to all the ECE department staffs for their valuable advice and co-operation.

References

[1] Barnard.K, Cardei.C, and Funt.B, 'A comparison of computational color constancy algorithms–Part I: Methodology and Experiments With Synthesized Data,' IEEE Trans. Image Process., vol. 11, no. 9,pp. 972–983,Sep. 2002.

[2] Bianco.S and Schettini.R, 'Color constancy using faces,'in Proc.IEEE Comput. Vision and Pattern Recognition,Providence,' RI, USA, Jun. 2012.

[3] Bishop.C.M, 'Pattern Recognition and Machine Learning (Information Science and Statistics),' Secaucus, NJ,USA: Springer-Verlag New York,2006.

[4] Gijsenij.A, Gevers.T, and van deWeijer.J, 'Computational color constancy:Survey and experiments,' IEEE Trans. Image Process., vol. 20, no. 9, pp. 2475–2489, Sep. 2011.

[5] Gijsenij.A, Lu.R, and Gevers.T, 'Color constancy for multiple light sources,' IEEE Trans. Image Process., vol. 21,no. 2, pp. 697–707, Feb. 2012.

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

[7] Lukas.J, Fridrich.J, and Goljan.M, 'Digital camera identification from sensor pattern noise,' IEEE Trans. Inf Forensics Security, vol. 1, no. 2, pp. 205–214, Jun. 2006.

[8] Popescu.A.C and Farid.H, 'Statistical tools for digital forensics,' in Proc. Inf. Hiding Conf., Jun. 2005, pp. 395–407.