Fake Image Detection by Illumination Color Classification

Nishit Gupta¹, Anant Kumar², Abhishek Mishra³, Mayank Kumar⁴

¹Department of Computer Science Savitribai Phule Pune University, India
²Department of Computer Science Savitribai Phule Pune University, India
³Department of Computer Science Savitribai Phule Pune University, India
⁴Department of Computer Science Savitribai Phule Pune University, India

nishitgupta76@gmail.com; anantraj2125@gmail.com; abhishekmishra1313@gmail.com; kshatriya.mks@gmail.com

Abstract — As images can fetch more information than words, most of the people are dependent on them for communication and use them as powerful evidence in courts and media companies. Nowadays, however, advanced image processing tools and graphical editing techniques makes it easier to edit and modify the digital image. This diminishes our trust in photographs and objects pictures as evidence for real world concept. To maintain the authenticity that the image is not a mixed or spliced image, this paper proposes a new method of detecting digital image forgeries using illumination color classification. Image splicing is a common type of image manipulation operation. To maintain the consistency of the image as well as identifying the areas of manipulation on images without the need of an external support or human process image contents is now days becoming the challenging research problem. In this paper, we are concentrating on authenticity of images that are based on concept of using illumination color estimation. To achieve this, illuminant color is calculated using the physics based method as well as statistical based edge method on similar image region. The estimate of illuminant color is extracted individually from the different face and non-face regions of the image. For the classification performance Support Vector Machine (SVM) approach is used. This technique yields maximum detection rates of 86%.


I. INTRODUCTION

Pictures and Images have become the main information carriers in today’s world and used to store real world events. Digital images are easy to manipulate because of the availability of the powerful editing software and advanced digital cameras. Image processing specialists can easily access, edit and modify image content and hence it’s meaning without leaving visually detectable traces. The modification (manipulation) of images for unkind purposes is now more common than ever. At the start, the manipulation is just to improve the image’s performance, but then many people started to change the image’s content, even to gain their ends by these unlawful and illicit methods. Therefore for the above reasons, it is necessary to develop a method to detect whether a digital image is damaged, so-called digital image forgery.
Image composition (or splicing) is one of the most common image manipulation operations. Image composition is to create a new image from two or more images, and it is broadly used for image forgery. Image splicing detection is a main difficulty in image forensics. Based on the fact that no two pictures taken for splicing have similar lighting conditions, the illuminant extract of the image can be used for splicing detection; i.e., the amount of light falling on the faces chosen from different images to create a composite image is not the same. Though manipulating the image content is easy, it is difficult to adjust the illuminant conditions proportional to other image taken for splicing. Most of the image editing tools does not notice the difference in illuminant of the image. Therefore the extracted illuminant of the image can be a strong tool in forensic analysis of splicing detection. In this work, we make an essential step towards minimizing user interaction for an illuminant-based tampering decision-making. We propose a method that is particularly more reliable than earlier approaches. Evaluation shows that the proposed method achieves a detection rate of 86%, while existing illumination-based work is slightly better than manual human interpretations.

The important contributions of this paper are summarized as follows:
1) Creating illuminant maps of images.
2) Introducing an integrated approach of feature extraction.
3) Minimizing human interaction in tampering decision making.
4) Semi – automated Forgery detection.

II. RELATED WORK
There are two methods for forgery detection which are either geometry-based or color-based. The detection of inconsistencies in light source positions between specific positions in the scene is done by geometry-based methods. The inconsistencies which are seen in interactions mostly between color of the object and the light color. Hence the color based methods is described to be more accurate and used [2]. A method which is available computes a low-dimensional descriptor in the image plane for the lighting environment (i.e in 2D). The estimation is done about the illumination direction from the intensity along manually object which are annotated boundaries of color that is homogenous. This approach was later extended to exploiting the (3D approach). Hence it would be misleading to rely on the visual assessment as human visual system is not that accurate to judge illuminations in the pictures. We propose a forgery detection method that exploits subtle inconsistencies in the color of the illumination of images. The automatic detection of highly specular regions is avoided. We make an important step towards minimizing user interaction for illuminant-based tampering decision-making. The algorithms used are most accurate and yield good results. The classification of illumination on color is done on all the faces in the images.

III. OVERVIEW AND DETAILS IN ALGORITHMS

![Fig. 1 Architectural workflow Design of the proposed system](image-url)
ALGORITHMS

1. The AdaBoost Algorithm

This is a fast face detection algorithm, which was proposed by Yoav Freund Robert and E.Schapire in 1995 and it is a milestone in the progress of the face detection field [3]. The basic idea is that it constructs a strong classifier as linear combination of simple weak classifiers. The AdaBoost algorithm is one kind of self-adaptation iterative algorithm. It selects the most important features from a big feature candidate set and makes a weak classifier for every selected one. Then the multi weak learners are combined to a strong one. In this algorithm, every training sample is assigned a weight representing the probability to be selected into the training set by some classifier. If it is not classified correctly, its weight will be raised[3].

(1) Given \((x_1, y_1), (x_2, y_2), ... , (x_n, y_n)\) \(X; E X \) is the training sample set and \(y; E Y \) classifies the category symbol. And \(y=\{0,1\} \), \(y=0 \) stands for negative examples(non-face) and \(y = 1 \) stands for positive examples (face). \(n \) is the total number of training samples. \(w_i; \) is assumed to be the error weights of the i th samples in the t th cycle.

(2) Weight initialization

When \(y;=0 \), then \(w_0 = 1/(2m) \) when \(y;=1 \), then \(W_0 = 1/(2l) \). Where \(m \) and \(l \) are the number of non-face example and face example respectively.

(3) For \(t = 1,oo.,T : \)

1) Normalized the weight: \(w_{i,0} = \frac{W_0}{(\sum w_{i,0})} \)

2) For each feature \(j\), trains its weak classifier \(h_{j,x(j,p,O)}\) to determine the threshold \(O_J\) and the offset \(P_j\), so it could obtain the minimum value of the \(c\) function

3) After the weak classifiers are determined in step 2) select the weak classifier \(h\), which has the minimum error rate

4) Set the update threshold of the weight for this training:

\[HW_t = \frac{W_t}{(1 - \epsilon_t)} \]

Where \(\epsilon_t = \epsilon_0 / (1 - \epsilon)\), \(z\) is factor to make \(\sum w_t = 1\).

(4) The final strong classifier is: \(C(x)\)

In order to get the ideal detection results, the number of training set should not be reduced, so we could only reduce the number of feature.

A. The Pearson Correlation

Correlation between sets of data is a measure of how well they are related. The most common measure of correlation in stats is the Pearson Correlation. The full name is the Pearson Product Moment Correlation or PPMC. It shows the linear relationship between two sets of data. Two letters are used to represent the Pearson correlation: Greek letter rho \((\rho)\) for a population and the letter “r” for a sample.

\[
\rho = \frac{n(\Sigma xy) - (\Sigma x)(\Sigma y)}{\sqrt{[n\Sigma x^2 - (\Sigma x)^2][n\Sigma y^2 - (\Sigma y)^2]}}
\]
The results will be between -1 and 1. You will very rarely see 0, -1 or 1. You’ll get a number somewhere in between those values. The closer the value of r gets to zero, the greater the variation the data points are around the line of best fit. **High correlation**: .5 to 1.0 or -0.5 to 1.0 **Medium correlation**: .3 to .5 or -0.3 to .5 **Low correlation**: .1 to .3 or -0.1 to -0.3

For Example:

![Graphs of different Pearson's results](image)

**Fig. 3** Graphs of different Pearson's results

### IV. CONCLUSION

The verification of integrity of the image as well as identifying the areas of tampering on images without need of any expert support or manual process or prior knowledge of the original image contents is now days becoming the challenging research problem. Thus to solve we have discussed different methods of detection for digital image forgery as well as illumination inconsistencies. There is no principal hindrance in applying it to other. This is problem-specific materials in the scene requires only a minimum amount of human interaction. This provides a crisp statement on the authenticity of the image. Also it gives significant advancement in the exploitation of illuminate color as a forensic cue new descriptor, classifier and combination method for taking advantage of illumination maps for forensic purposes.

Our results are encouraging, yielding an accuracy of over 86% correct classification. Good results are also achieved over internet images and under cross-database training/testing. Thus this machine-learning based illumination method will help to overcome the forgery of images in the future.

### ACKNOWLEDGEMENT

We would like to express the deepest appreciation to our guide Prof. Mrs. C.R Jadhav and our Head of Computer Engineering Department Prof. Pramod Patil. We thank our parents who have shown tremendous support and inspired us with their blessings. We would like to express our gratitude with a word of thanks to all of those who have directly or indirectly helped us by giving beneficial information and knowledge.
REFERENCES


[12] Engineering Exhibition[Online]”,2010,