Exposing Digital Image Forgeries by Illumination Color Classification using Sift Algorithm

Priyanka Manthale
Department of Electronics and Communication
PDA College of Engineering
Kalburgi, India

Geeta Patil, PhD
Professor, Department of Electronics and Communication
PDA College of Engineering
Kalburgi, India

ABSTRACT
A digital image is fundamentally composed of a series of pixels, a word derived from combining picture and element. Traditionally, a photograph implies the truth of what has happened. Our life is full of digital images and tampering these digital images can be done easily with the help of powerful image editing software's mainly to cover up the truthfulness of the photographs which often serve as evidence in court, in forensic investigation, criminal investigation, surveillance systems, intelligence services, medical imaging, and journalism. It is very easily to change the information represented by an image without leaving any obvious traces of tampering by using *photo editing software* like photo shop, photo grids which are easily available in the internet. In this work we presents a method to detect image retouching, image splicing and copy move attacks. Image splicing means specifically copying and pasting a person or any things from an image to another. Our approach is machine-learning based and requires minimal user interaction. The technique is applicable to images containing two or more people and requires no expert interaction for the tampering decision. To achieve this, we incorporate information from 'physics' and 'statistical-based' illuminant estimators on image regions of similar material. For implementation of this both IE we make use scale invariant feature transform(SIFT)algorithm in Matlab programming language. The proposed method detects the illuminate colour mismatch among different persons in a composite image. The illuminate colour obtained is quantified using chromaticity coordinates. It is then matched against that of different persons in the composite image to detect the forgery. We use SVM classification technique in our proposed work, since the classification performance using an SVM meta-fusion classifier is quite promising. We expect much better detection rate than those obtained in with the state of art methods.

Keywords
Digital image forgery, Color illuminant constancy, machine learning, SIFT algorithm, Matlab Programming language.

1. INTRODUCTION
In recent years the development of technology is been upholded. In today's digital world, digital images are the foremost source of information and they are the fastest means of information convey. As an evidence for any event in the court of law images can be useful. The images broadcasted in any TV news are accepted as the certificate for the truthfulness of that news. Unfortunately, it is not difficult to use computer graphics and image processing Techniques to manipulate images. Image composition (or splicing) is one of the most common image manipulation operations. One such example is shown in Fig. 1,

Fig1.Example of a spliced image involving people

The main goal of this paper is:

1. Briefly introduce what is image forgery.
2. Gives overview of different techniques that are used to detect forged area.

To present a comparative analysis of different techniques with their different parameters, merits and demerits. Image composition (or splicing) is one of the most common image manipulation operations. One such example is shown in Fig. 1, in which the girl on the right is inserted. Although this image shows a harmless manipulation case, several more controversial cases have been reported, e.g., the 2011 Benetton UnHate advertising campaign or the diplomatically delicate case in which an Egyptian state-run newspaper published a manipulated photograph of Egypt's former president, Hosni Mubarak, at the front, rather than the back, of a group of leaders meeting for peace talks. In this work, we make an important step towards minimizing user interaction for an illuminant-based tampering decision-making. We propose a new semiautomatic method that is also significantly more reliable than earlier approaches. Quantitative evaluation shows that the proposed method achieves a detection rate of 90%, while existing illumination-based work is slightly better than guessing. We exploit the fact that local illuminant estimates are most discriminative when comparing objects of the same (or similar) material. Thus, we focus on the automated comparison of human skin, and more specifically faces, to classify the illumination on a pair of faces as either consistent or inconsistent. User interaction is limited to marking bounding boxes around the faces in an image under investigation. In the simplest case, this reduces to specifying two corners (upper left and lower right) of a bounding box.

When creating a digital forgery from multiple images, it is often difficult to exactly match the lighting conditions. We have previously shown how to estimate the direction to a light source, and how inconsistencies in the illuminant direction can be used to detect tampering. Image splicing is a simple process that crops and pastes regions from the same or separate sources. A simple example is shown in below figure. It is a fundamental step used in digital photomontage which refers to a paste-up produced by sticking together images using digital tools such as Photoshop. Image splicing is an image editing method to copy a part of an image and paste it onto another image.

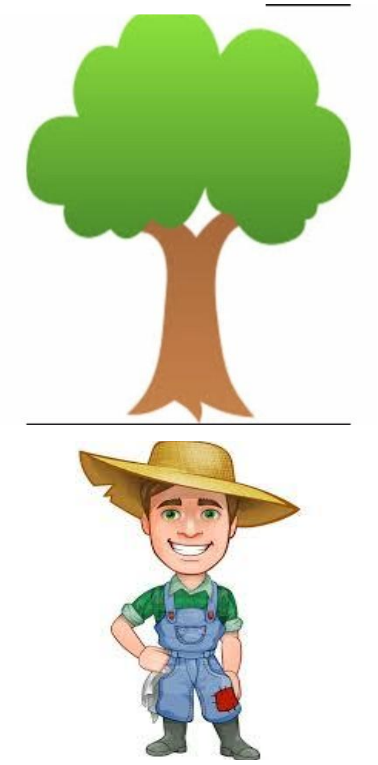


Fig 2. Original images

Fig 2a. Spliced image

2. RELATED WORK

A Comprehensive Study about Digital Image Tamper Detection Techniques. The increasing availability of low cost and sometimes free of cost image editing software such as Photoshop, GIMP etc., had made the tampering of digital images even more easier. Digital image tamper detection has emerged as an important research area to establish the authenticity of digital photographs by separating the tampered lots from the original ones.
Illumination-based methods for forgery detection are either geometry-based or color-based. Geometry-based methods focus at detecting inconsistencies in light source positions between specific objects in the scene , Two methods have been proposed that use the direction of the incident light for exposing digital forgeries. Johnson and Farid proposed a method which computes a low-dimensional descriptor of the lighting environment in the image plane (i.e., in 2-D). It estimates the illumination direction from the intensity distribution along manually an notated object boundaries of homogeneous color.

The goal of computational color constancy is to find a nontrivial illuminant invariant description of a scene from an image taken under unknown lighting conditions. This is often broken into two steps. The first step is to estimate illuminant parameters, and then a second step uses those parameters to compute illumination independent surface descriptors.

3. METHODOLOGY

Nowadays, many approaches have been proposed for detecting image forgery. Various operations that occur during forgery are, blurring, cropping, compression, retouching, resizing, scaling, etc. The input image is divided into various overlapping blocks of different shape and then the feature extraction from each block takes place. The sorting is done based on the features so that the region with same features can be easily located and remaining is considered as forged points. And lastly some morphological operation is applied so that it detects the forged region.

The techniques that help to detect forgery are:

- Discrete Wavelet Transform(DWT)
- Discrete Cosine Transform(DCT)
- Principle Component Analysis(PCA)
- Singular Value Decomposition(SVD)
- Scale Invariant Feature Transformation (SIFT)
- Locally Linear Embedding(LLE)

In this work we are using SIFT method, which is used to extract feature from the blocks and last a morphological operation is applied so the forged region is properly detected, with low computational expenses and high precision and recall rate. Down-sampling, scaling, rotation and JPEG compression operations are also detected. Spliced forgery can be detected with the help of this approach. with the help of this approach.

In this project we collect information using statistic based and physics based illuminant estimators from similar materials. We classify the illumination for each pair of faces in the image as either consistent or inconsistent. Throughout this, we abbreviate illuminant estimation as IE, and illuminant maps as IM. The proposed method consists of five main components:

1) *Dense Local Illuminant Estimation (IE):* 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 is the only step that may require 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. We then crop every bounding box out of each illuminant map, so that only the illuminant estimates of the face regions remain.

3) *Computation of Illuminant Features:* for all face regions, texture-based and gradient-based features are computed on the IM values. Each one of them encodes complementary information for classification.

4) *Paired Face Features:* Our goal is to assess whether a pair of faces in an image is consistently illuminated. For an image with faces nf, we construct (nf 2) joint feature vectors, consisting of all possible pairs of faces.

5) *Classification:* We use a machine learning approach to automatically classify the feature vectors. We consider an image as a forgery if at least one pair of faces in the image is classified as inconsistently illuminated.

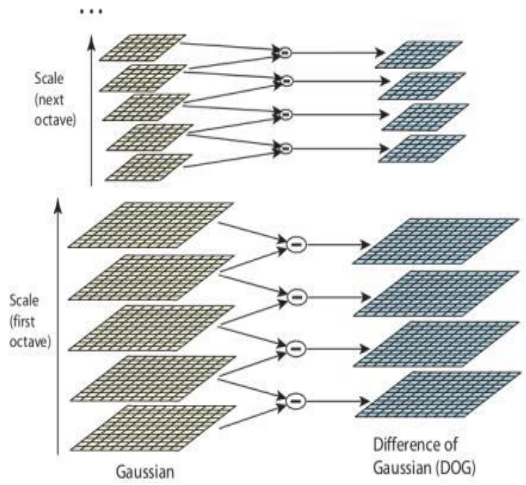
3.1 SIFT Algorithm

The scale invariant feature transform (SIFT) is an algorithm in computer vision to detect and describe local features in images. It consists of five main parts , they areas follows:

A. Scale-space extrema detection :

Search over multiple scales and image locations. Identify locations and scales that can be repeatably assigned under different views of the same scene or object. To detect larger corners we need larger windows. For this, scale-space filtering is used. In it, Laplacian of Gaussian is found for the image with various σ values. LoG acts as a blob detector which detects blobs in various sizes due to change in σ. In short, σ acts as a scaling parameter. For eg, in the above image, gaussian kernel with low σ gives high value for small corner while guassian kernel with high σ fits well for larger corner. So, we can find the local maxima across the scale and space which gives us a list of (x, y, σ) values which means there is a potential keypoint at (x,y) at σ scale. But this LoG is a little costly, so SIFT algorithm uses Difference of Gaussians which is an approximation of LoG. Difference of Gaussian is obtained as the difference of Gaussian blurring of an image with two different σ, let it be σ and $k\sigma$. This process is done for different octaves of the image in Gaussian Pyramid. It is represented in below image:

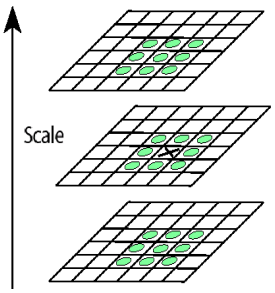
The best function is a Gaussian function for this assumption.The scale space of an image is a function $L(x,y,\sigma)$ that is produced from the convolution of a Gaussian kernel (at different scales) with the input image.



Once this DoG are found, images are searched for local extrema over scale and space. For eg, one pixel in an image is compared with its 8 neighbours as well as 9 pixels in next scale and 9 pixels in previous scales. If it is a local extrema, it is a potential keypoint. It basically means that keypoint is best represented in that scale. It is shown in above image.

B. Keypoint localization :

Fit a model to determine location and scale. Select keypoints based on a measure of stability. Detect maxima and minima of difference-of-Gaussian in scale space in fig below. Each point is compared to its 8 neighbors in the current image and 9 neighbors each in the scales above and below.



C. Orientation assignment :

Compute best orientation(s) for each keypoint region. Now we have set of good points. choose a region around each point(remove effects of scale and rotation). Create histogram of local gradient directions at selected scale. The highest peak in the histogram is taken and any peak above 80% of it is also considered to calculate the orientation. It creates keypoints with same location and scale, but different directions. It contribute to stability of matching.

D. Keypoint description :

Use local image gradients at selected scale and rotate onto describe each keypoint region. At this point,each keypoint has location, scale,orientation. Next is to compute a descriptor for the local image region about each keypoint that is highly distinctive, invariant as possible to variations such as changes in viewpoint and illumination. **:** Now keypoint descriptor is created. A 16x16 neighbourhood around the keypoint is taken. It is devided into 16 sub-blocks of 4x4 size. For each sub-block, 8 bin

orientation histogram is created. So a total of 128 bin values are available. It is represented as a vector to form keypoint descriptor. In addition to this, several measures are taken to achieve robustness against illumination changes, rotation etc. shown in below figure.

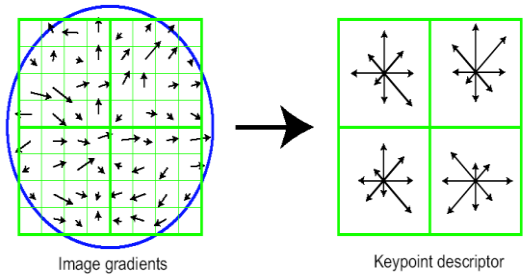


Fig 3. In experiments, 4x4 arrays of 8 bin histogram is used, a total of 128 features for one keypoint.

E. Keypoint Matching :
Keypoints between two images are matched by identifying their nearest neighbours. But in some cases, the second closest-match may be very near to the first. It may happen due to noise or some other reasons. In that case, ratio of closest-distance to second-closest distance is taken. For example, If it is greater than 0.8, they are rejected.

3.2 Classification

We classify the illumination for each pair of faces in an image as either consistent or inconsistent. Assuming all selected faces are illuminated by the same light source, we tag an image a manipulated if one pair is classified as inconsistent. Individual feature vectors, i.e., SIFT features on either gray world or IIC-based illuminant maps, are classified using a support vector machine (SVM) classifier with a radial basis function (RBF) kernel. The information provided by the SASI features is complementary to the information from the edge features. Thus, we use a machine learning-based fusion technique for improving the detection performance. Inspired by the work of Ludwig *et al*, we use a late fusion technique named SVM-Meta Fusion. We classify each combination of illuminant map and feature type independently using a two-class SVM classifier to obtain the distance between the image's feature vectors and the classifier decision boundary. SVM-Meta Fusion then merges the marginal distances provided by all individual classifiers to build a new feature vector. Another SVM classifier (i.e., on meta level) classifies the combined feature vector.

3.3 Software used

The best tool for image processing is MATLAB. It is a scientific programming language and provides strong mathematical and numerical support for the implementation of advanced algorithms. It is for that reason that matlab is widely used by the image processing and computer vision community. It allows one to ensure numerical precision is maintained all the way through the enhancement process.

It is user friendly as an application like Photoshop, however being a general purpose programming language it provides many important advantages for forensic image processing.

4. RESULTS

In this technique we determine a strong method for detection of the forged images, for assuring proper authentication of the image. Considering for forensic evidences this technique works good, we estimate the changes occurring in an images with respect to its color illumination by comparing all the subdivided portions on an individual image. Every image is divided into many regions and is then matched against that of different persons in the composite image to detect the forgery. The proposed method detects the illuminate colour mismatch among different persons in a composite image.The illuminate colour obtained is quantified using chromaticity coordinates, the differences on their illumination of color decides the robustness of an image. To test our algorithm under these conditions, we download some images of multiple objects in natural lighting environments from google and perform all the geometric and statistics based methods and then the classification performance using an SVM meta-fusion classifier is promising. The SIFT algorithm yields detection rates of 90% on a new benchmark data set consisting of 100 images.

5. CONCLUSION AND FUTURE WORK

In this work, we presented a new method for detecting forged images of people using the illuminant color. We estimate the illuminant color using a statistical gray edge method and a physics-based method which exploits the inverse intensity- chromaticity color space. We treat these illuminant maps as texture maps.We also extract information on the distribution of edges on these maps. In order to describe the edge information. We combine these complementary cues (texture- and edge-based) using machine learning late fusion using scale invariant feature transform (SIFT) algorithm. The segmented feature values are estimated using this algorithm. The proposed method requires only a minimum amount of human interaction and 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. Thus detection of any forged or tampered image can be identified accurately by this project work. For future work, can include combination of two techniques to develop more accurate technique for detection of forged images.

6. REFERENCES

[1] M. Johnson and H. Farid, "Exposing digital forgeries in complex lighting environments," IEEE Trans. Inf. Forensics Security, vol. 3, no. 2, pp. 450–461, Jun. 2007.

[2] S. Gholap and P. K. Bora, "Illuminant colour based image forensics," in Proc. IEEE Region 10 Conf., 2008E.

[3] Kee and H.Farid, "Exposing digital forgeries from 3-D lighting environments," in Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS), Dec. 2010.

[4] P.Saboia,T.Carvalho,andA.Rocha,"Eye specular highlights telltales for digital forensics: A machine learning approach,"inProc. IEEEInt. Conf.Image Processing (ICIP), 2011, pp. 1937–1940.

[5] K. Barnard, L. Martin, A. Coath, and B. Funt, "A comparison of computational colorconstancy algorithms–PartII:Experiments With ImageData,"IEEETrans.ImageProcess.,vol.11,no.9,pp.985–996, Sep. 2002.

[6] Charmil Nitin Bharti and Purvi Tandel, "A Survey of Image Forgery Detection Techniques," in Proc. IEEE WiSPNET 2016 conference.

[7] Mr.Arun Anoop M, "Image forgery and its detection:A survey",in Prof. IEEE (ICIIECS)2015.