ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Image Fraud Identification Using Illuminant Analysis

P. Kaveen[1], Dr. G. Singaravel Ph.D., [2]

M.Tech (IT), Dept of IT, KSR College of Engineering, Tiruchengode, India[1]

Prof/Head, Dept of IT, KSR College of Engineering, Tiruchengode, India[2]

Abstract: Digital Images plays a vital role in every one's life in this modern world, where people easily fixes with the advertisement, magazines, blogs, website, television and more. When the digital images took their role, happening of crimes and escaping from the crimes happened becomes easier. To be with lawful, No one should be punished for not commencing a crime, to help them this application can be used. The identification using color edge method will give a exact detection of the crime and the forgeries that has been done in the digital image.

In Existing method, they have analyzed one of the most common forms of photographic manipulation, known as image composition or splicing. The approach is machine-learning- based and requires minimal user interaction and this technique is applicable to images containing two or more people and requires no expert interaction for the tampering decision. The obtained result by the classification performance using an SVM (Super Vector Machine) meta-fusion classifier and It yields detection rates of 86% on a new benchmark dataset consisting of 200 images, and 83% on 50 images that were collected from the Internet.

The further improvements can be achieved when more advanced illuminant color estimators become available. Bianco and Schettini has proposed a machine-learning based illuminant estimator particularly for faces which would help us in this for more accurate prediction. Effective skin detection methods have been developed in the computer vision literature and this method also helps us, in detecting pornography compositions which, according to forensic practitioners, have become increasingly common nowadays.

I. INTRODUCTION

We are undoubtedly living in an age where we are exposed to a remarkable array of visual imagery. While we may have historically had confidence in the integrity of this imagery, today's digital technology has begun to erode this trust. From the tabloid magazines to the fashion industry and in mainstream media outlets, scientific journals, political campaigns, courtrooms, and the photo hoaxes that land in our e-mail in-boxes, doctored photographs are appearing with a growing frequency and sophistication. Over the past five years, the field of digital forensics has emerged to help restore some trust to digital images. Here I review the state of the art in this new and exciting field. Digital watermarking has been proposed as a means by which an image can be authenticated. The drawback of this approach is that a watermark must be inserted at the time of recording, which would limit this approach to specially equipped digital cameras. In contrast to these approaches, passive techniques for image forensics operate in the absence of any watermark or signature. These techniques work on the assumption that although digital forgeries may leave no visual clues that indicate tampering, they may alter the underlying statistics of an image. The set of image forensic tools can be roughly grouped into five categories: 1) pixel-based techniques that detect statistical anomalies introduced at the pixel level; 2) format-based techniques that leverage the statistical correlations introduced by a specific lossy compression scheme; 3) camera-based techniques that exploit artifacts introduced by the camera lens, sensor, or on-chip postprocessing; 4) physically based techniques that explicitly model and detect anomalies in the three-dimensional interaction between physical objects, light, and the camera; and 5) geometric-based techniques that make measurements of objects in the world and their positions relative to the camera. I will

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

review several representative forensic tools within each of these categories. In so doing, I have undoubtedly omitted some worthy papers. My hope, however, is that this survey offers a representative sampling of the emerging field of image forgery detection.

1.1. Pixel-Based Detection

The legal system routinely relies on a range of forensic analysis ranging from forensic identification or fingerprint) to forensic odontology, forensic entomology and forensic geology. In the traditional forensic sciences, all manner of physical evidence is analyzed. In the digital domain, the emphasis is on the pixel—the underlying building block of a digital image. I describe four techniques for detecting various forms of tampering, each of which directly or indirectly analyzes pixel-level correlations that arise from a specific form of tampering.

1.2. Format Based Detection

The first rule in any forensic analysis must surely be "preserve the evidence." In this regard, lossy image compression schemes such as JPEG might be considered a forensic analyst's worst enemy. It is ironic, therefore, that the unique properties of lossy compression can be exploited for forensic analysis. I describe three forensic techniques that detect tampering in compressed images, each of which explicitly leverages details of the JPEG lossy compression scheme.

1.3. Camera Based Detection

Grooves made in gun barrels impart a spin to the projectile for increased accuracy and range. These grooves introduce somewhat distinct markings to the bullet fired, and can therefore be used to link a bullet with a specific handgun. In the same spirit, several image forensic techniques have been developed that specifically model artifacts introduced by various stages of the imaging process. I describe four techniques for modeling and estimating different camera artifacts. Inconsistencies in these artifacts can then be used as evidence of tampering. Because most digital camera sensors are very nearly linear, there should be a linear relationship between the amount of light measured by each sensor element and the corresponding final pixel value. Most cameras, however, apply a pointwise nonlinearity in order to enhance the final image. The authors describe how to estimate this mapping, termed a response function, from a single image. Differences in the response function across the image are then used to detect tampering.

II. RELATED WORK

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. Color-based methods search for inconsistencies in the interactions between object color and light color [2], [12]. Two methods have been proposed that use the direction of the incident light for exposing digital forgeries. Johnson and Farid [7] 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 annotated object boundaries of homogeneous color. Kee and Farid [9] extended this approach to exploiting known 3-D surface geometry. In the case of faces, a dense grid of 3-D normals improves the estimate of the illumination direction. To achieve this, a 3-D face model is registered with the 2-D image using manually annotated facial landmarks. Fan *et al.* [10] propose a method for estimating 3-D illumination using shape-from-shading. In contrast to [9], no 3-D model of the object is required. However, this flexibility comes at the expense of a reduced reliability of the algorithm.

Johnson and Farid [8] also proposed spliced image detection by exploiting specular highlights in the eyes. In a subsequent extension, Saboia *et al.* [13] automatically classified these images by extracting additional features, such as the viewer position. The applicability of both approaches, however, is somewhat limited by the fact that people's eyes must be visible and available in high resolution. Gholap and Bora [12] introduced physics-based illumination cues to image forensics. The authors examined inconsistencies in specularities based on the dichromatic reflectance model. Specularity segmentation on real-world images is challenging [5]. Therefore, the authors require manual annotation of specular highlights. Additionally, specularities have to be present on all regions of interest, which limits the method's applicability in real-world scenarios. Riess and Angelopoulou [2] followed a different approach by using a physics-based color

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

constancy algorithm that operates on partially specular pixels. In this approach, the automatic detection of highly specular regions is avoided. The authors propose 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*. Implausible illuminant color estimates point towards a manipulated region. Unfortunately, the authors do not provide a numerical decision criterion for tampering detection. Thus, an expert is left with the difficult task of visually examining an illuminant map for evidence of tampering. In the field of color constancy, descriptors for the illuminant color have been extensively studied. Most research in color constancy focuses on uniformly illuminated scenes containing a single dominant illuminant. However, in order to use the color of the incident illumination as a sign of image tampering, we require multiple, spatially-bound illuminant estimates. So far, limited research has been done in this direction. The work by Bleier *et al.* [4] indicates that many off-the-shelf single-illuminant algorithms do not scale well on smaller image regions. Thus, problem-specific illuminant estimators are required.

Ebner presented an early approach to multi-illuminant estimation. Assuming smoothly blending illuminants, the author proposes a diffusion process to recover the illumination distribution. Unfortunately, in practice, this approach oversmooths the illuminant boundaries. Gijsenij *et al.* [11] proposed a pixelwise illuminant estimator. It allows to segment an image into regions illuminated by distinct illuminants. Differently illuminated regions can have crisp transitions, for instance between sunlit and shadow areas. While this is an interesting approach, a single illuminant estimator can always fail. Thus, for forensic purposes, we prefer a scheme that combines the results of multiple illuminant estimators. In this paper, we build upon the ideas by [2] and [13]. We use the relatively rich illumination information provided by both physics-based and statistics-based color constancy methods as in [2]. Decisions with respect to the illuminant color estimators are completely taken away from the user, which differentiates this paper from prior work.

3. Illumination Color Classification

Every day, millions of digital documents are produced by a variety of devices and distributed by newspapers, magazines, websites and television. In all these information channels, images are a powerful tool for communication. Unfortunately, it is not difficult to use computer graphics and image processing techniques to manipulate images. Quoting Russell Frank, a Professor of Journalism Ethics at Penn State University, in 2003 after a Los Angeles Times incident involving a doctored photograph from the Iraqi front: "Whoever said the camera never lies was a liar". How we deal with photographic manipulation raises a host of legal and ethical questions that must be addressed [1]. However, before thinking of taking appropriate actions upon a questionable image, one must be able to detect that an image has been altered.

Image composition 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 Un-Hate 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Fig. 1. How can one assure the authenticity of a photograph? Example of a spliced image involving people.

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 adjustment of the illumination conditions is hard to achieve when creating a composite image [1]. In this spirit, Riess and Angelopoulou [2] proposed to analyze illuminant color estimates from local image regions. Unfortunately, the interpretation of their resulting so-called *illuminant maps* is left to human experts. 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 [3]. Thus, it is preferable to transfer the tampering decision to an objective algorithm.

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 86%, 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. In summary, the main contributions of this work are:

- Interpretation of the illumination distribution as object texture for feature computation.
- A novel edge-based characterization method for illuminant maps which explores edge attributes related to the illumination process.
- The creation of a benchmark dataset comprised of 100 skillfully created forgeries and 100 original photographs.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

IV. CONSTRUCTION OF ILLUMINANT MAPS

Fig. 2. Example illuminant map that directly shows an inconsistency.

To illustrate the challenges of directly exploiting illuminant estimates, we briefly examine the illuminant maps generated by the method of Riess and Angelopoulou [2]. In this approach, an image is subdivided into regions of similar color (superpixels). An illuminant color is locally estimated using the pixels within each superpixel. Recoloring each superpixel with its local illuminant color estimate yields a so-called *illuminant map*. A human expert can then investigate the input image and the illuminant map to detect inconsistencies. Fig. 2 shows an example image and its illuminant map, in which an inconsistency can be directly shown: the inserted mandarin orange in the top right exhibits multiple green spots in the illuminant map. All other fruits in the scene show a gradual transition from red to blue. The inserted mandarin orange is the only one that deviates from this pattern.

Fig. 3. Example illuminant maps for an original image (top) and a spliced image (bottom). The illuminant maps are created with the IIC-based illuminant estimator.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

In practice, however, such analysis is often challenging, as shown in Fig. 3. The top left image is original, while the bottom image is a composite with the right-most girl inserted. Several illuminant estimates are clear outliers, such as the hair of the girl on the left in the bottom image, which is estimated as strongly red illuminated [6]. Thus, from an expert's viewpoint, it is reasonable to discard such regions and to focus on more reliable regions, e.g., the faces. In Fig. 3, however, it is difficult to justify a tampering decision by comparing the color distributions in the facial regions. It is also challenging to argue, based on these illuminant maps, that the right-most girl in the bottom image has been inserted, while, e.g., the right-most boy in the top image is original.

Although other methods operate differently, the involved challenges are similar. For instance, the approach by Gholap and Bora [12] is severely affected by clipping and camera white-balancing, which is almost always applied on images from off-the-shelf cameras. Wu and Fang [13] implicitly create illuminant maps and require comparison to a reference region. However, different choices of reference regions lead to different results, and this makes this method error-prone.

Thus, while illuminant maps are an important intermediate representation, we emphasize that further, automated processing is required to avoid biased or debatable human decisions. Hence, we propose a pattern recognition scheme operating on illuminant maps. The features are designed to capture the shape of the superpixels in conjunction with the color distribution. In this spirit, our goal is to replace the expert-in-the-loop, by only requiring annotations of faces in the image.

Note that, the estimation of the illuminant color is error-prone and affected by the materials in the scene. However, (cf. also Fig. 2), estimates on objects of similar material exhibit a lower relative error. Thus, we limit our detector to skin, and in particular to faces. Pigmentation is the most obvious difference in skin characteristics between different ethnicities. This pigmentation difference depends on many factors as quantity of melanin, amount of UV exposure, genetics, melanosome content and type of pigments found in the skin. However, this intramaterial variation is typically smaller than that of other materials possibly occurring in a scene.

V. FORGERY DETECTION WITH ILLUMINANT IDENTIFICATION

We classify the illumination for each pair of faces in the image as either consistent or inconsistent. Throughout the paper, 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), 2) Face Extraction, 3) Computation of Illuminant Features, 4) Paired Face Features and 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.

VI. MACHINE LEARNING BASED ILLUMINANT DETECTION FOR FORGERY DETECTION

The image forgery detection system is designed with a set of techniques. The color and texture features are extracted to analyze the illuminant e status. The edge features are also used in the system. 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. Prior color-based work either assumes complex user interaction or imposes very limiting assumptions. The proposed method is custom-tailored to detect splicing on images containing faces. There is no principal hindrance in applying it to other, problem-specific materials in the scene. The classification process is improved with naïve Bayesian classification method. The pixels and their features are classified with the classification method. The classification process increases the forgery detection accuracy levels.

The image forgery detection system is designed to find out the image manipulation activities by the attackers. The feature selection and edge analysis mechanism is used for the detection process. The illuminant identification mechanism is used for the detection process. Statistical analysis is used for the detection process The system is divided into five major

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

modules. They are feature selection, illuminant identification, face extraction, color classification and forgery detection. Feature selection module is to fetch color, texture and shape features. The illuminant identification module is to identify illuminant features for the image. The face extraction module is to fetch face boundaries and its properties. The color classification module is to classify the color values in image. The forgery detection module is detect image modification process

6.1. Feature Selection

Low level and high level features are extracted from the images. The image pixel values are used in feature extraction process. Color and texture features identified from the pixel values. The shape features are extracted from the images.

6.2. Illuminant Identification

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).

6.3. Face Extraction

This is the only step that may require human interaction. An operator sets a bounding box around each face 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.

6.4. Color Classification

The color classification 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. Our goal is to assess whether a pair of faces in an image is consistently illuminated. For an image with faces, we construct joint feature vectors, consisting of all possible pairs of faces.

6.5. Forgery Detection

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.

VII. CONCLUSION

The proposed method is custom-tailored to detect splicing on images containing faces, there is no principal hindrance in applying it to other, problem-specific materials in the scene. 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. Prior color-based work either assumes complex user interaction or imposes very limiting assumptions. Machine-learning based illuminant estimator are used to improve the image forgery detection process.

REFERENCES

[1] A. Rocha, W. Scheirer, T. E. Boult, and S. Goldenstein, "Vision of the unseen: Current trends and challenges in digital image and video forensics," ACM Comput. Surveys, 2011.
[2] C. Riess and E. Angelopoulou, "Scene illumination as an indicator of image manipulation," Inf. Hiding, vol. 6387, pp. 66–80, 2010.
[3] H. Farid and M. J. Bravo, "Image forensic analyses that elude the human visual system," in Proc. Symp. Electron. Imaging (SPIE), 2010.
[4] M. Bleier, C. Riess, S. Beigpour, E. Eibenberger, E. Angelopoulou, T. Tröger, and A. Kaup, "Color constancy and non-uniform illumination: Can existing algorithms work?," in Proc. IEEE Color and Photometry in Comput. Vision Workshop, 2011, pp. 774–781.
[5] C. Riess and E. Angelopoulou, "Physics-based illuminant color estimation as an image semantics clue," in Proc. IEEE Int. Conf. Image Processing, Nov. 2009, pp. 689–692.
[6] 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, July 2013.
[7] 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

[8] M. Johnson and H. Farid, "Exposing digital forgeries through specular highlights on the eye," in Proc. Int.Workshop on Inform. Hiding, 2007, pp. 311–325.
[9] E. 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, pp. 1–6.
[10] 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.
[11] A. Gijsenij, R. Lu, and T. Gevers, "Color constancy for multiple light sources," IEEE Trans. Image Process., vol. 21, no. 2, pp. 697–707, Feb. 2012.
[12] S. Gholap and P. K. Bora, "Illuminant colour based image forensics," in Proc. IEEE Region 10 Conf., 2008.
[13] P. Saboia, T. Carvalho, and A. Rocha, "Eye specular highlights telltales for digital forensics: A machine learning approach," in Proc. IEEE Int. Conf. Image Processing (ICIP), 2011.