Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Digital Image Forgery Detection Using Improved Illumination Detection Model

Ms. V. Shanmugapriya[1], Dr. S. Sathappan[2], Mr. R. Subramanian[3]

[1]Research Scholar,[2]M.Sc., PGDCA., M.Phil., Ph.D.,
[2]Associate Professor of Computer Science,
[2,3]Department of Computer Science, Erode Arts and Science College (Autonomous), Erode, TN, India.

Abstract- Image processing methods are widely used in 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.

Image composition or splicing methods are used to discover the image forgeries. 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

Photographs can no longer be trusted. Forged images have appeared in tabloid magazines, main-stream media outlets, political attacks, scientific journals, and the hoaxes that land in our email in-boxes. These doctored photographs are appearing with growing frequency and sophistication, and even experts often cannot rely on visual inspection to distinguish authentic images from forgeries.

On the political front, for example, a photograph of Senator John Kerry and Jane Fonda sharing a stage at an anti-war rally emerged during the 2004 presidential primaries as Senator Kerry was campaigning for the Democratic nomination. The photograph, however, was a fake. The picture of Senator Kerry was from a speech in June of 1971, and the unrelated picture of Jane Fonda was from August 1972. The two photographs were composited together to give the impression that Senator Kerry shared the controversial anti-war views of activist Jane Fonda. On the scientific front, in 2004 Professor Hwang Woo-Suk of Seoul National University and colleagues published what appeared to be ground-breaking advances in stem cell research. Evidence slowly emerged that these results were manipulated and/or fabricated. After months of controversy, Hwang retracted the paper and resigned his position at the University. An independent Korean panel investigating the accusations of fraud found that at least nine of the eleven customized stem cell colonies that Hwang had claimed to have

made were fakes. Much of the evidence for those nine colonies, the panel said, involved doctored photographs of two other, authentic, colonies. Finally, in the news media, The Economist was criticized when it published, in June 2010, a cover photo showing a solitary President Obama on the Louisiana beach inspecting the BP oil spill. The photo was accompanied with the headline "The damage beyond the spill", eluding to potential political problems facing President Obama as a result of the oil spill. This photograph, however, had been altered to remove two other people standing alongside the President.

In addition to the ethical, political, and legal implications raised by this lack of trust in photography, studies have shown that doctored photographs can alter our own memories of actual events. In one such study participants were shown original and doctored photographs of memorable public events at which they were present. The doctored photographs, showing either larger crowds or more violence, changed the way in which participants recalled the events. This surprising finding is due to a number of factors including our natural trust in photographs and our general inability to easily detect doctored photographs.

High quality digital cameras and affordable photo-editing software such as Photoshop have made it easier for nearly anyone to create compelling photo fakes. In addition, recent advances in Computer Vision and Computer Graphics point to a future of growing sophistication for photo manipulators. The need for forensic techniques for exposing photo fakery is, therefore, critical. Digital watermarking has been proposed as a means for image authentication. 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 cameras. In contrast, passive forensic techniques operate in the absence of watermarks or signatures.

These techniques work on the assumption that although photo manipulation may leave no obvious visual clues, it may alter some geometric or statistical property in the image. With this approach, a collection of complementary techniques are each designed to detect specific types of artifacts. The combination of many such techniques makes creating a fake photo more difficult because the forger has to carefully consider a host of different possible artifacts that may not be visually obvious, and yet may be detectable by one of many forensic techniques. Even if a forger successfully fools most avenues of detection, a single failed test can conclusively and objectively discredit an image.

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 [8]. 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. It estimates the illumination direction from the intensity distribution along manually annotated object boundaries of homogeneous color. Kee and Farid [3] extended this approach to exploiting known 3-D surface geometry. In the case of faces, a dense grid of 3-D normal 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.* [2] propose a method for estimating 3-D illumination using shape-from-shading. In contrast to [3], no 3-D model of the object is required. This flexibility comes at the expense of a reduced reliability of the algorithm.

Johnson and Farid [4] also proposed spliced image detection by exploiting specular highlights in the eyes. In a subsequent extension, Saboia *et al.* 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 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 [6]. 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. To avoid this problem, Wu and Fang assume purely diffuse reflectance, and train a mixture of Gaussians to select a proper illuminant color estimator. The angular distance between illuminant estimates from selected regions can then be used as an indicator for tampering. Unfortunately, the method requires the manual selection of a "reference block", where the color of the illuminant can be reliably estimated. This is a significant limitation of the method.

Riess and Angelopoulou [8] followed a different approach by using a physics-based color 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. 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.* [10] 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, this approach oversmooths the illuminant boundaries. Gijsenij *et al.* [1] proposed a pixelwise illuminant estimator. It allows segmenting 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 [8]. We use the relatively rich illumination information provided by both physics-based and statistics-based color constancy methods as in [8]. Decisions with respect to the illuminant color estimators are completely taken away from the user, which differentiates this paper from prior work.

III. DETECTION OF IMAGE MANIPULATION

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

3.1. 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.

3.2. 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.

3.3. 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, apply a point wise 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.

Consider an edge where the pixels below the edge are of a constant color C_1 and the pixels above the edge are of a different color C_2. If the camera response is linear, then the intermediate pixels along the edge should be a linear combination of the neighboring colors. The deviation of these intermediate pixel values from this expected linear response is used to estimate the camera response function. The inverse camera response function that brings the pixel colors back to a linear relationship is estimated using a maximum a posteriori (MAP) estimator. In order to stabilize the estimator, edges are selected such that areas on either side of the edge are similar, the variances on either side of the edge are small, the difference between C_1 and C_2 is large, and the pixels along the edge are between C_1 and C_2. Constraints are also imposed on the estimated camera response function: the function should be monotonically increasing with at most one inflexion point and should be similar for each of the color channels. Since the camera response function can be estimated locally, significant variations in this function across the image can be used to detect tampering.

IV. PROBLEM STATEMENT

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 following problems are identified from the existing system.

- High illuminant errors
- Face boundary estimation is not optimized
- Classification accuracy is low
- High computational overhead

V. ILLUMINATION CLASSIFICATION

Image composition is one of the most common image manipulation operations. In which the girl on the right is inserted [5]. 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.

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 [8] 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 [9]. 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 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 of a bounding box.

VI. DIGITAL IMAGE FORGERY DETECTION PROCESS

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.

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 [11]. 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 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.

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. 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). 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.

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. 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.

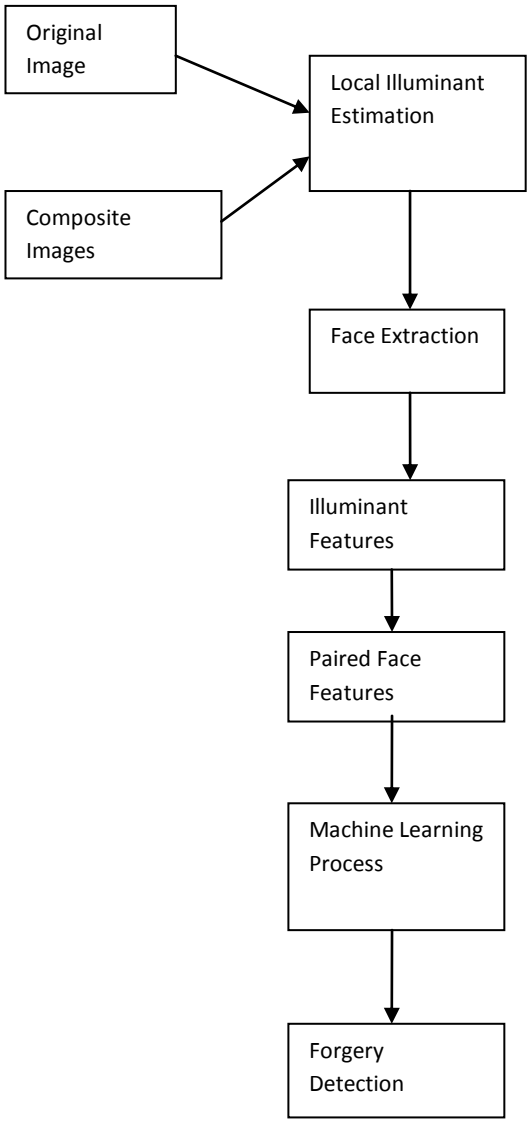

Figure 6.1. Digital Image Forgery Detection Process

VII. PERFORMANCE ANALYSIS

The image forgery detection system is tested with Illuminant Estimation Scheme (IES) and Enhanced Illuminant Estimation Scheme (EIES). Color feature extraction, texture feature extraction techniques are used in the system. Edge features are extracted using Canny edge detection algorithm. The illuminant estimator is used to detect the illuminant in images.

The classification scheme is enhanced with bayesian model in Enhanced Illuminant Estimation Scheme. False positive and false negative rates are used to measure the forgery detection quality. The false positive and false negative rate measures are used to estimate the detection error levels. The false positive rate analysis reflects the falsely assigned positive results.

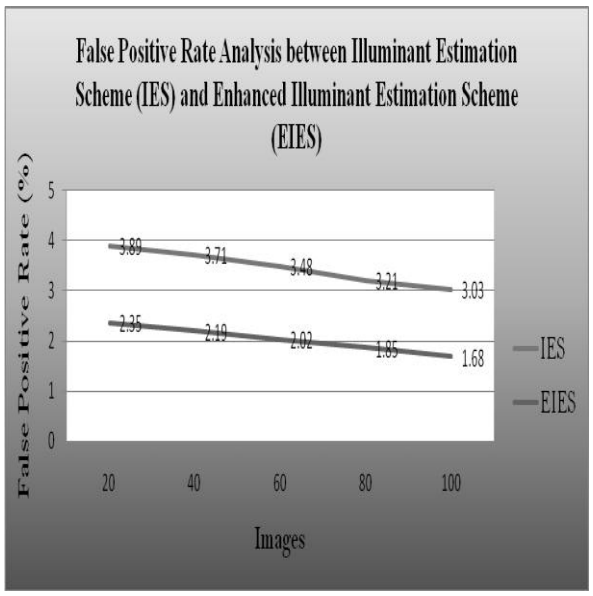

Figure 7.1. False Positive Rate Analysis between Illuminant Estimation Scheme (IES) and Enhanced Illuminant Estimation Scheme (EIES)

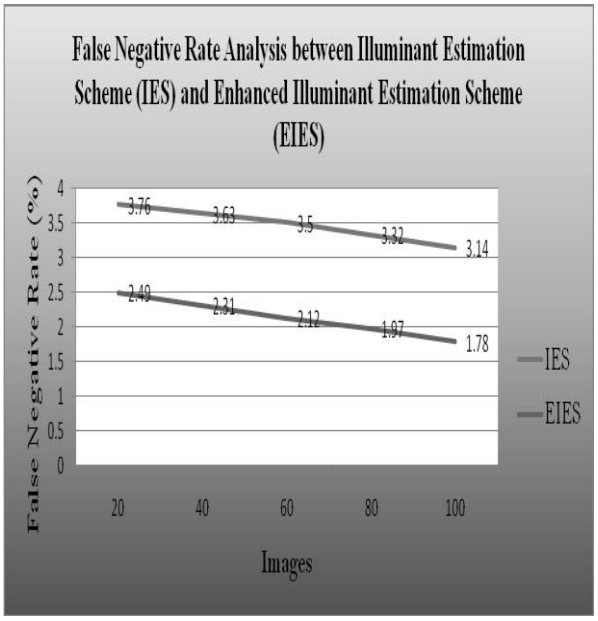

Figure 7.2. False Negative Rate Analysis between Illuminant Estimation Scheme (IES) and Enhanced Illuminant Estimation Scheme (EIES)

The false positive results are shown in figure 7.1. The results show that the EIES technique reduces the false positive rate 35% than the IES technique. Falsely assigned negative results ratio is analyzed using false negative rate model. The false negative ratio is analyzed in figure 7.2. The EIES reduces the false negative rate 30% than the IES technique.

VIII. CONCLUSION AND FUTURE ENHANCEMENT

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 is used to improve the image forgery detection process. The system can be enhanced with the following features.

- The system can be enhanced to detect forgeries from multi framed images
- The system can be improved to analyze video forgeries
- The system can be upgraded to detect any region that can be manipulated by the attackers
- The system can be enhanced to analyze Three Dimensional objects

REFERENCES

[1] A. Gijsenij, R. Lu, and T. Gevers, "Color constancy for multiple light sources," *IEEE Trans. Image Process.*, Feb. 2012.
[2] 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.
[3] 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.
[4] M. Johnson, "Exposing digital forgeries through specular highlights on the eye," in Proc. Int.Workshop on Inform. Hiding, 2007.
[5] 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.
[6] C. Riess and E. Angelopoulou, "Physics-based illuminant color estimation as an image semantics clue," in Proc. IEEE Int. Conf. Image Processing, Nov. 2009.
[7] M. Johnson and H. Farid, "Exposing digital forgeries in complex lighting environments," IEEE Trans. Inf. Forensics Security, Jun. 2007.
[8] C. Riess and E. Angelopoulou, "Scene illumination as an indicator of image manipulation," Inf. Hiding, 2010.
[9] H. Farid and M. J. Bravo, "Image forensic analyses that elude the human visual system," in Proc. Symp. Electron. Imaging (SPIE), 2010.
[10] M. Bleier and A. Kaup, "Color constancy and non-uniform illumination: Can existing algorithms work?," in Proc. IEEE Color and Photometry in Comput. Vision Workshop, 2011.
[11] Giovanni Chierchia, Giovanni Poggi, Carlo Sansone and Luisa Verdoliva, "A Bayesian-MRF Approach for PRNU-Based Image Forgery Detection", IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, April 2014

