Visual Computing and Machine Learning Techniques for Digital Forensics

Tiago Carvalho[1]
Hélio Pedrini[1]
Anderson Rocha[1]

Data submissão: 22.07.2014
Data aceitação: 20.03.2015

Seção melhores tutoriais XXVII SIBGRAPI, Rio de Janeiro, Brasil, 2014.

Abstract: A rapidez com que diversos campos da ciência vêm avançando dia após dia é notável. Em especial, os avanços tecnológicos têm impressionado muitas pessoas, uma vez que introduzem em suas vidas fatos que vão além da imaginação. Inspirados em métodos anteriormente apresentados por programas de ficção científica, a comunidade ligada à área de Computação criou um novo campo de pesquisa denominado *Análise Forense de Documentos Digitais*, o qual foca em desenvolver e implantar métodos capazes de auxiliar na luta contra crimes digitais, tais como a falsificação de imagens digitais. Este artigo apresenta alguns dos principais conceitos relacionados à Análise Forense de Documentos Digitais e, de forma complementar, apresenta algumas das mais recentes e poderosas técnicas baseadas em conceitos provenientes das áreas de Computação Gráfica, Processamento de Imagens, Visão Computacional e Aprendizado de Máquina para detectar falsificações em fotografias digitais. Alguns tópicos que são abordados neste trabalho incluem: atribuição de fonte, detecção de ataques, detecção de pornografia, filogenia multimídia e detecção de falsificações. Por fim, este trabalho destaca os desafios e problemas em aberto no campo da Análise Forense de Imagens Digitais para que os leitores se familiarizem com as oportunidades de pesquisa disponíveis.

[1] Institute of Computing, University of Campinas, Campinas, SP, 13083-852
`{tjose,helio,anderson.rocha@ic.unicamp.br}`

Abstract: It is impressive how fast science has improved day by day in so many different fields. In special, technology advances are shocking so many people bringing to their reality facts that previously were beyond their imagination. Inspired by methods earlier presented in scientific fiction shows, the computer science community has created a new research area named *Digital Forensics*, which aims at developing and deploying methods for fighting against digital crimes such as digital image forgery. This work presents some of the main concepts associated with Digital Forensics and, complementarily, presents some recent and powerful techniques relying on Computer Graphics, Image Processing, Computer Vision and Machine Learning concepts for detecting forgeries in photographs. Some topics addressed in this work include: source attribution, spoofing detection, pornography detection, multimedia phylogeny, and forgery detection. Finally, this work highlights the challenges and open problems in Digital Image Forensics to provide the readers with the myriad opportunities available for research.

1 Introduction

In November 2012, Brazil's former president Luiz Inácio Lula da Silva had some photographs tampered with depicting him side by side with Rosemary de Noronha, a woman investigated by Brazilian Federal Police in the "Safe Harbor operation". In March 2013, businessman Dimitri de Angelis was considered guilty in a court for deceiving investors using manipulated images. Such images depicted de Angelis side by side with influent people such as US former president Bill Clinton and were used to leverage investors confidence.

The aforementioned cases are just two of many examples that happen daily all around the world. Technology improvements are a *two-edged sword*: in one edge is all the benefits as the ease for producing special effects in big movies, easy communication tools, and even simpler ones, such as the possibility of taking thousands of pictures through a digital camera. However, the other edge brings many side-effects such as photo-manipulation, hacking attacks and many others.

Digital document forgery is a typical example of a very usual side-effect. Among all kinds of faked digital documents, images are one of the most common cases. By using advanced manipulation tools available in the Internet, an ordinary user can turn himself/herself in a reasonable counterfeiter in a few hours. These fake images, most of the times, aim at deceiving people to influence their opinion and leverage some personal gain.

To fight back against this falsification wave, researchers have created a brand new research field named Digital Forensics, which focuses on proposing methods for guaranteeing evidence preservation and document authenticity.

Among all kinds of problems that are investigated by Digital Forensics, such as copy-paste forgery detection or spoofing detection, *image splicing detection* is one that has received special attention. Image splicing is the process of using parts of two or more images to compose a fake one, depicting a moment/situation that never happened. This process includes all the necessary adjustments to turn the new image as realistic as possible. Figure 1 depicts an example of the main operations involved in image splicing.

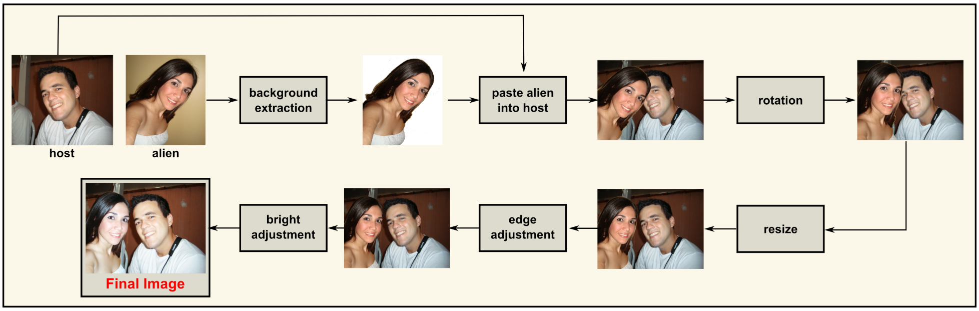


Figure 1. A simplified pipeline for the image splicing creation process.
Source: Carvalho et al. [6, 7].

Methods able to detect forgeries, as the one presented in Figure 1, explore inconsistencies left by the forgery construction process. In special, inconsistencies in the illumination process are very powerful and useful to detect image splicing.

This tutorial presents eight visual computing and machine learning techniques employed on the image forgery detection process. The remaining of this tutorial is organized as follows: Section 2 presents research of how forgeries affect our memories and fact perception. Section 3 presents some examples of cases involving forgeries throughout history. Section 4 presents a few problems addressed by Digital Forensics. Section 5 is the core of this tutorial, presenting concepts and methods related to image splicing detection. Finally, Section 6 presents some conclusions and points out further research directions in the Digital Forensic field.

2 The Image Power

Many researches have presented results suggesting that images are capable of influencing and, even changing, people's memory about some real events. In one of the studies published by Sacchi et al. [39], the authors performed an experiment whereby Italian participants have been presented to doctored pictures of two events: the 1989 Tiananmen Square protest in Beijing and the 2003 protest in Rome against the war in Iraq. After analyzing these pictures, they answered some questions about the events and the result of such answers was surprising. Most people had changed the form they remembered the events. The study concluded that doctored images of past public events can influence behavioral intentions, memory and attitudes.

In a most recent study, Frenda et al. [21] performed a memory study, whereby 5,269 participants have been asked about four political events. Among these four events, one of them was fabricated and, to support this fake event, one fake image related to it was also included. As a result of the study, half of the participants falsely remembered that the false event happened, with 27% "remembering" seeing the events in the news.

In a different study, this time not including fake images but highlighting the power of images to influence humans, Garry et al. [22] proposed an experiment to measure how images affect people's memory for the news. As described by the authors, participants have been presented to a hurricane news which describes its effects on a village located at a coastal region. The story made no mention of personal injury or death. Some of the participants saw a picture of a village before the hurricane hit, while other ones saw a different picture of the village after the hurricane hit. As a result of the study, the researchers found that 23% more of the participants who saw the *After* photograph falsely remembered reading about serious personal injuries caused by the hurricane, depicting the influence of images in people's minds.

The presented studies support the statement that images are a very powerful tool able to affect people's memory of past events. This fact makes even more important to design and deploy methods for helping forensic experts in their fight against forgeries and counterfeiters.

3 Forgeries Throughout the History

Since the invention of photograph, forgeries are present in our lives. It is not hard to imagine that image forgeries have been invented after Photoshop age, however, this is a common mistake. Figure 2 is an example of old image forgery. It has been composed by Oscar G. Reijland in 1857 using about 30 image pieces just a few years after the invention of photography [36].

History also shows that image forgeries are deeply involved in political subjects [2]. In 1930's, for example, it was very usual for dictator Joseph Stalin to erase his enemies from photographs. Figure 3 (left image) depicts a photograph whereby one of Stalin's commissar was removed from the original photograph (right image) after falling out of favor with Stalin.

Adolph Hitler was also a user of the *magic* that image doctoring can leverage. In 1937, as depicted in Figure 4, he used image manipulation to erase Joseph Goebbels (second from

[2] These and many other cases related herein are shown in `http://www.fourandsix.com/photo-tampering-history/`

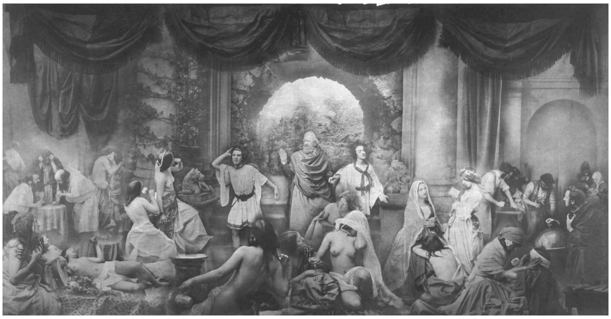


Figure 2. The image *The Two Ways of Life* is a creation by Oscar G. Rejland in 1857. Credits to Oscar G. Rejland.

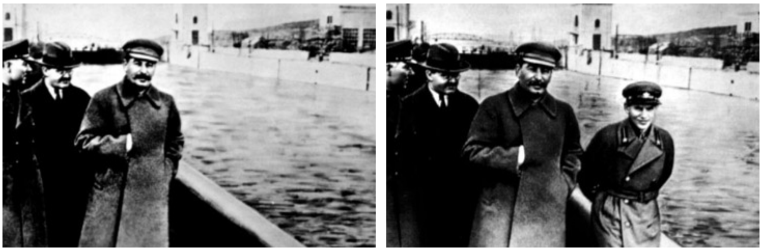


Figure 3. Stalin was a user of image manipulation. The image on the right depicts an original image while the one on the left depicts the same image but with Stalin's commissar wiped out. Source: Fourandsix Technologies[3].

the right) from an original photographic record. It is still unclear the reasons that promoted Goebbels fell out of favor with Hitler.

Even leaders of small countries, such as Cuba, have used tampered images in self-benefit. In 1968, after the Soviet intervention in Czechoslovakia, Cuba's dictator Fidel Castro lost the support of his trust man Carlos Franqui, who was exiled in Italy and had cut relationships with the Cuban regime. As a consequence, and to erase any trace of previous relationship, Fidel ordered Carlos Franqui removal from all photographs whereby he appeared with Fidel as depicted in Figure 5.

In 1989, the famous talk-show host Oprah Winfrey was surprised when seeing her picture in the cover of a TV Guide. The picture has been created without Winfrey's permission and depicted Winfrey's head onto the body of actress Ann-Margret Smith, which has been

[3] `http://www.fourandsix.com/photo-tampering-history/`

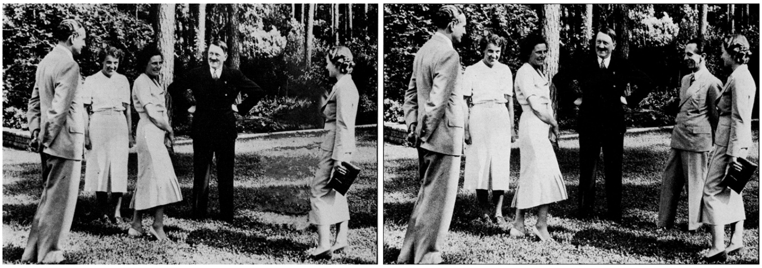


Figure 4. Adolph Hitler has also used image manipulation in his favor. The right image depicts an original image whereby the Reich minister of propaganda in Nazi Germany, Joseph Goebbels, stands side by side with Hitler. By unclear reasons, Goebbels has been erased from Hitler's photographs, as depicted in the image on the left. Source: Fourandsix Technologies[3].

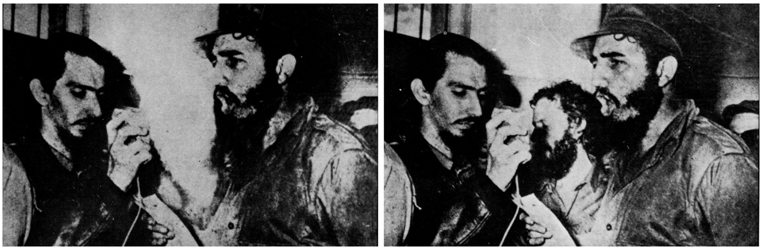


Figure 5. After some disagreements, Fidel Castro commanded the removal of Carlos Franqui from archival photographs whereby they appeared together. Source: Fourandsix Technologies[3].

extracted from a 1979 picture. Figure 5 depicts the cover of the TV Guide and the original picture of Ann-Margret Smith taken in 1979.

In 2003, one of the most famous U.S. newspapers, Los Angeles Times, stamped a doctored image in its front page, shortly after US led the invasion of Iraq. Such digital composite, which depicted a British soldier gesturing to Iraqi civilians urging them to seek protection, was created through two other pictures as depicted in Figure 7.

In 2009, current Brazilian president, Dilma Rousseff, by the time a minister of state, faced an embarrassing situation when an alleged criminal record of her, as depicted in Figure 8, was published in the front page of newspaper Folha de São Paulo, one of the most prestigious newspaper in Brazil. Rousseff hired experts who proved the record was a fake. The newspaper had to publish a public disclaimer about the fact.

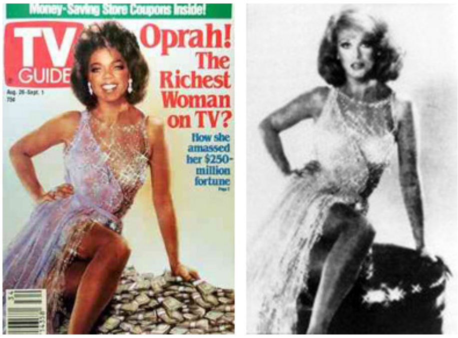

Money-Saving Store Coupons Inside!
TV GUIDE
Oprah! The Richest Woman on TV?
How she amassed her $250-million fortune

Figure 6. Oprah Winfrey has been surprised when visualized herself onto the body of actress Ann-Margret (right image). Source: Fourandsix Technologies[3].

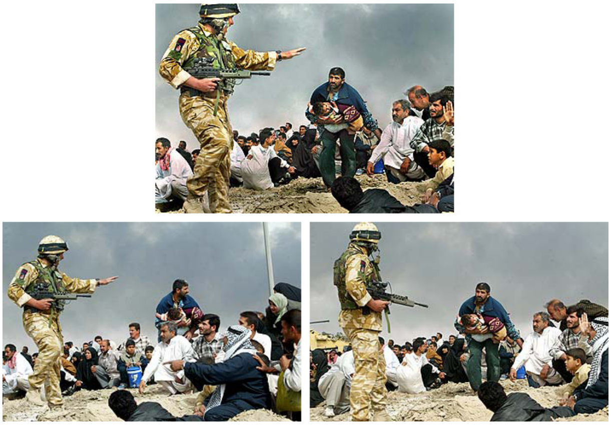
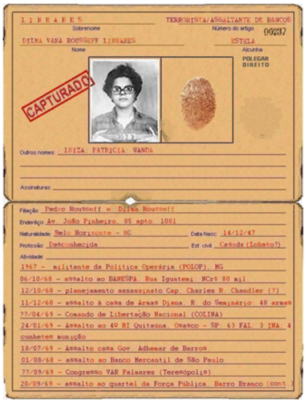


Figure 7. Front page of Los Angeles Times (top image) depicting a composition of two other images (bottom images). Source: Fourandsix Technologies[3].

Brazil's former president, Luiz Inácio Lula da Silva, was also a target of manipulated images. In 2012, an image depicting Lula standing side by side with Rosemary Novoa de Noronha, a woman accused of being one of the leaders of a gang for fraudulent technical advices, rapidly gained traction in the Internet. Shortly after, the original image was published as depicted in Figure 9 showing the composite.

The cases illustrated herein are just some of the examples involving digital document forgeries. We now turn our attention to a brief introduction to some topics related to Digital Forensics in Section 4.



LINHARES — TERRORISTA/ASSALTANTE DE BANCOS

Sobrenome — Número do artigo 00237

Nome: DILMA VANA ROUSSEFF LINHARES

Alcunha: ESTELA

POLEGAR DIREITO

CAPTURADO

Outros nomes: LUIZA; PATRICIA; WANDA

Assinaturas:

Filiação: Pedro Rousseff e Dilma Rousseff

Endereço: Av. João Pinheiro, 85 apto. 1001

Naturalidade: Belo Horizonte - MG — Data Nasc: 14/12/47

Profissão: Desconhecida — Est. civil: Casada (Lobato?)

Atividade:

1967 - militante da Política Operária (POLOP), MG

06/10/68 - assalto ao BANESPA, Rua Iguatemi: NCr$ 80 mil.

12/10/68 - planejamento assassinato Cap. Charles R. Chandler (?)

11/12/68 - assalto à casa de Armas Diana, R. do Seminário: 48 armas

??/04/69 - Comando de Libertação Nacional (COLINA)

24/01/69 - Assalto ao 4º RI Quitaúna, Osasco - SP: 63 FAL; 3 INA; 4 cunhetes munição

18/07/69 - Assalto casa Gov. Adhemar de Barros.

01/08/68 - assalto ao Banco Mercantil de São Paulo

??/09/69 - Congresso VAR Palmares (Teresópolis)

20/09/69 - assalto ao quartel da Força Pública, Barro Branco (cont.)

Figure 8. Fake criminal record published by newspaper Folha de São Paulo involving president Dilma Rousseff. After the forgery has been proved by forensics experts, the newspaper had to publish a public disclaimer about the fact. Source: Folha de São Paulo[4].

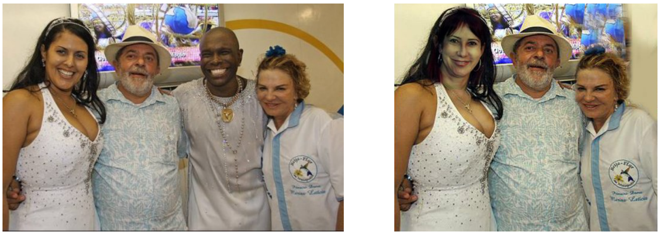


Figure 9. Questioned images involving Brazil's former president Luis Inácio Lula da Silva. The original one is on the left while its fake version appears on the right. Credits to Ricardo Stucker (original image).

4 Some Problems Addressed By Digital Forensics

As mentioned in Section 1, technology is both a boon and a bane and in spite of allowing amazing accomplishments for our society improving our quality of life it also can produce some undesired results sometimes. Despite the focus of this tutorial on image splicing detection, an overview of problems addressed by Digital Forensics is very useful, since efforts to solve these problems are still necessary. Based on this purpose, this section presents some problems addressed by Digital Forensics as a whole and their importance to the field.

[4] http://www1.folha.uol.com.br/fsp/brasil/fc0504200906.htm

4.1 Source Attribution

One of the first and, consequently, oldest problems addressed by Digital Forensics is the source attribution problem. This problem consists of associating a source device with a specific digital document, as an image or a printed document. Methods for performing such task are useful when is necessary to associate evidences with their source device to link proofs and suspects. A counterfeiter who has been arrested with fake money and with the printer used to produce such currency can have a different treatment when in trial.

To associate the document with its source device, existing methods explore some *intrinsic fingerprints*, such as pattern noise [12, 29], left on the document during its generation process.

4.2 Spoofing Detection

Biometric systems are a very common and useful technology present in many different places. Their objective is to replace current access keys (usually a login associated with a password) by more sophisticated systems, which can be based on different individual and unique features, such as, fingerprint, face, iris, among others.

A spoofing attack is an attempt of deceiving a biometric system using fake data, usually, to obtain private information. Since each kind of biometric system is based on a particular feature, each one of them can have different forms of spoofing attacks. As an example, in face recognition systems, one can display an image or a recorded video as an example of possible attack [40, 30].

4.3 Pornography Detection

Nowadays, it is extremely easy to capture thousands of pictures in a few minutes. However, it is not just the number of regular images that increase daily. Pornographic content produced in the digital era is also astonishing. Many times, it is paramount to identify this type of material. Internet filters to block porn images and search for pornography files in large amount of data are just a few examples of situations whereby pornography detection is necessary.

This problem has especial interest to the forensic community, which has been developing different approaches to automatically detecting pornography [3] and child pornography [43]. Even the Brazilian Federal Police has developed its own pornography detection software named *NuDetective* [34].

4.4 Copy Move Detection

One of the simplest and most useful operations to deceive viewers is copy-move operations. It consists of copying a specific image part and pasting it in a different portion of the same image. Although it is simple, such operation usually attempts to change perception of viewers duplicating objects or even, hiding specific parts of image content [4, 5, 11, 1].

More advanced image manipulation tools, such as *Adobe Photoshop*, make copy move easier with functions such as *Content Aware Fill*, which perform a good quality copy-move operation hiding selected parts of an image using parts of the whole image modelling the copy move operation as an optimization problem.

4.5 Multimedia Phylogeny

Multimedia Phylogeny is one of the newest problems addressed by Digital Forensics. It consists of tackling the relationship between object duplicates of one digital object (e.g., image near duplicates). In other words, given a set of similar, but not identical, copies of an image, Image Phylogeny algorithms [18, 16] are able to construct a hierarchical relationship among them showing their relationship over time.

These algorithms are very useful when it is necessary to track and find the source image from some viral image, trace child pornography distribution, etc. If the initial image is detected, it is possible to garner additional side information (e.g., IP addresses) and associate a narrow down the search for suspects.

Similarly to source image track problem, it is often necessary to track and find the source audio or video. Audio and video piracy is, nowadays, one of the most common crimes in Internet. Multimedia Phylogeny methods for audio [32] and video [17] are useful to help finding the responsible for sharing original piracy data and can help authorities collecting proper investigation evidence.

5 Image Splicing: Methods for Fighting It Back

In the last section, we have presented different problems addressed by Digital Forensics. However, the main focus of this tutorial is on how to detect image splicing, one of the most common problems in Digital Forensics.

We now turn our attention to forgery detection [2, 19, 44], more specifically, to image splicing detection. As we described in Section 1, image splicing is the process of using parts of two or more images to compose a fake one, depicting a moment/situation that never actually happened.

We present herein eight methods for detecting image splicing which search for inconsistencies in image illumination. These methods explore concepts of different areas, such as Image Processing, Computer Vision, Computer Graphics, Machine Learning, among others.

Methods that explore inconsistencies in illumination are specially attractive for different reasons. Saboia et al. [38] argue that these methods *are of particular interest since a perfect illumination adjustment in a digital composite is very difficulty to obtain.* Ostrovsky et al. [33] performed experiments which suggest that humans have great difficult to perceive image illumination inconsistencies. Such factors are, at the same time, a boon and a bane. In one hand, failing in perceiving illumination inconsistencies makes almost impossible to rely only upon expert skills to detect image composition. On the other hand, the fact that humans have troubles to perceive image illumination inconsistencies guarantees that most of the times counterfeiters will leave traces (in illumination) of their action, which might allow forensic techniques to detect forgeries.

It is worth mentioning that there are some data sets available for the evaluation of forgery detection methods, such as CASIA Tampered Image Detection Evaluation Database [9], Image Manipulation Dataset [25], and the Dresden Image Database [24].

5.1 Forgery Detection by 2-D Light Source Position

One of the first methods that explore illumination inconsistencies has been proposed by Johnson and Farid [26]. To detect image splicing, the authors estimate 2-D light source direction of different objects comparing the differences among these directions.

For modelling the problem, Johnson and Farid adopt some assumptions:

1. all the analyzed objects have Lambertian surface;
2. the surface reflectance is constant;
3. the object surface is illuminated by an infinitely distant light source.

These assumptions led to a representation of intensity I at position (x, y) as

$$I\left(x,y\right) = R\left(\vec{N}\left(x,y\right)\cdot\vec{L}\right) + A, \tag{1}$$

where R is the constant reflectance value, $\vec{L}$ is a 3-vector pointing in the direction of the light source, $\vec{N}\left(x,y\right)$ is a 3-vector representing the surface normal at the point (x, y), and A is a constant ambient light term [20].

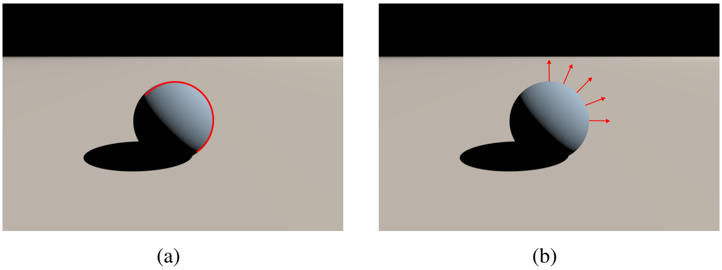
The constant reflectance value R has unit length since we are interested just in the light source direction. Equation 1 provides a single constraint in four unknowns, the three components of $\vec{L}$ and the ambient term A. Given four, or more, points with the same reflectance, R, and different surface normals, $\vec{N}$, it is possible to estimate $\vec{L}$ and A using standard least-squares estimation

$$\begin{pmatrix} \vec{N}_x(x_1,y_1) & \vec{N}_y(x_1,y_1) & \vec{N}_z(x_1,y_1) & 1 \\ \vec{N}_x(x_2,y_2) & \vec{N}_y(x_2,y_2) & \vec{N}_z(x_2,y_2) & 1 \\ & \vdots & & \\ \vec{N}_x(x_p,y_p) & \vec{N}_y(x_p,y_p) & \vec{N}_z(x_p,y_p) & 1 \end{pmatrix} \begin{pmatrix} \vec{L}_x \\ \vec{L}_y \\ \vec{L}_z \\ A \end{pmatrix} = \begin{pmatrix} I(x_1,y_1) \\ I(x_2,y_2) \\ \vdots \\ I(x_p,y_p) \end{pmatrix}, \qquad (2)$$

where p is the number of points along occluding contours.

Unfortunately, even using the previously described assumptions, light source direction estimation for an arbitrary object in an image needs 3-D normals, which is a very hard task using just one image and objects of arbitrary geometry, a common situation in a forensic scenario.

To deal with such drawback, Johnson and Farid used a solution proposed by Nillius and Eklundh [31], who suggested to use surface normals along occluding boundaries. At these surface normals, the z-component is zero and the calculation of x and y components is straightforward. Figure 10 depicts an example of an occluding-contour region (red contour in the left image) and its 2-D surface normals direction (right image). To estimate 2-D light source position, just points along occluding contours of bright region are valid.


(a)

(b)

Figure 10. Examples of occluding contour region (a) and 2-D surface normals (b).

After relaxing the problem as described above, it is possible to estimate x and y components of light source direction using at least three different points with the same reflectance R and different surface normals, $\vec{N}$ using

$$\begin{pmatrix} \vec{N}_x(x_1,y_1) & \vec{N}_y(x_1,y_1) & 1 \\ \vec{N}_x(x_2,y_2) & \vec{N}_y(x_2,y_2) & 1 \\ & \vdots & \\ \vec{N}_x(x_p,y_p) & \vec{N}_y(x_p,y_p) & 1 \end{pmatrix} \begin{pmatrix} \vec{L}_x \\ \vec{L}_y \\ A \end{pmatrix} = \begin{pmatrix} I(x_1,y_1) \\ I(x_2,y_2) \\ \vdots \\ I(x_p,y_p) \end{pmatrix}. \qquad (3)$$

Figure 11 depicts an example of Johnson and Farid's method [26] application over an original image (left image) and a fake image (right image). Observe that the light direction in the pristine image has a better match than in the fake image.

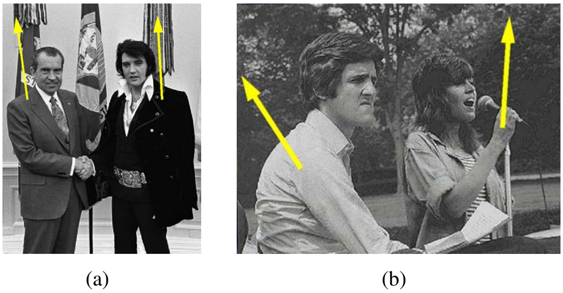


Figure 11. Images depicting the result of Johnson and Farid method's application. In the pristine image (a), the light direction of both objects point to the same direction, while being inconsistent in the fake image (b). Source: Johnson and Farid [26].

5.2 Forgery Detection by Specular Highlights on the Eye

The method previously presented was a significant step toward image splicing detection. However, when a researcher develops forensic methods for detecting forgeries, he/she tries to explore complementary telltales as much as possible.

Saboia et al. [38] extended a method proposed by Johnson and Farid [27], which explores a characteristic specially difficult to tamper with: specular highlight of the eye. Their extension explores additional discriminative features not considered in the first solution while also incorporating machine learning fusion techniques to the decision-making process. The proposed method is composed of three main stages, as depicted in Figure 12.

The method starts with a pre-processing of the images whereby, for each eye present in the image, the region named *limbus* is manually selected. Given this selection, for each eye in the image, Stage 1 performs estimation of three 3-D vectors: light direction ($\vec{L}$), surface normal ($\vec{N}$) and viewer direction ($\vec{V}$). By performing this estimation, the authors assume the eye is a perfect reflector and rely upon the physic reflection law

$$\vec{L} = 2(\vec{V}^T\vec{N})\vec{N} - \vec{V}. \tag{4}$$

To estimate these 3-D vectors from a single 2-D image, the authors relax the problem through some assumptions:

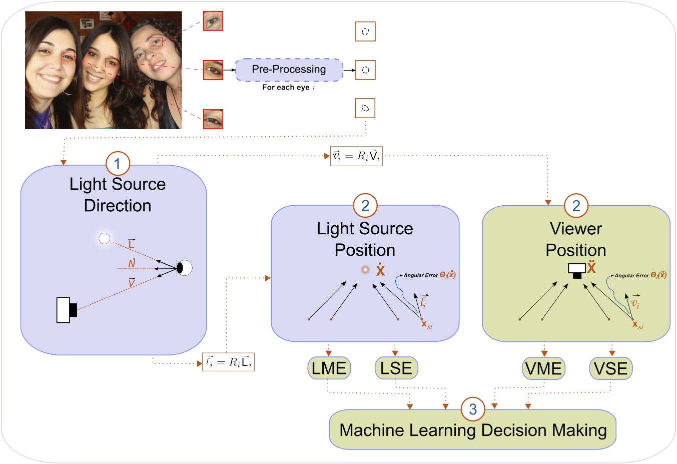

Pre-Processing
For each eye i
1
Light Source Direction
L
N
V
$\vec{v}_i = R_i\vec{V}_i$
$\vec{l}_i = R_i\vec{L}_i$
2
Light Source Position
Angular Error $\Theta_i(\hat{X})$
2
Viewer Position
Angular Error $\Theta_i(\ddot{X})$
LME
LSE
VME
VSE
3
Machine Learning Decision Making

Figure 12. Saboia et al. [38] method's overview. Blue boxes represent stages proposed by Johnson and Farid [27]. Green boxes represent new and important stages proposed by Saboia et al. [38]. Source: Saboia et al. [38].

1. the limbus (the boundary between the sclera and iris) is modelled as a circle in the 3-D world system and as an ellipse in the 2-D image system;
2. the distortion of the ellipse with respect to the circle is related to the pose and position of the eye relative to the camera;
3. and points on a limbus are coplanar.

The aforementioned assumptions allow the estimation of a planar projective transform matrix H able to map world points $\mathbf{X}$ onto image-coordinate points $\mathbf{x}$ and vice-versa. H is estimated by means of an iterative and non-linear least squares minimization function, such as Levenberg–Marquardt [37] using the error function

$$E(\boldsymbol{P};\, H\,) = \sum_{i=1}^{m} \min_{\hat{\mathbf{X}}} \|\mathbf{x}_i - \, H\,\hat{\mathbf{X}}_i\|^2, \tag{5}$$

where $\hat{\mathbf{X}}$ is on the circle parameterized by $\mathbf{P} = (C_1, C_2, r)^T$, and m is the total number of data points in the image system. Starting from H and performing some additional calculations[3], it is possible to estimate $\vec{L}$, $\vec{N}$ and $\vec{V}$ in world and image coordinates.

[3] Details of $\vec{L}$, $\vec{N}$ and $\vec{V}$ estimation can be found in [6].

Based on the previously estimated direction vectors, the second stage of the method assumes that estimated light directions [4] $\vec{l}_i$ converge toward the position of the scene light source, which can be estimated by minimizing the error function

$$E(\dot{\mathbf{x}}) = \sum_{i=1}^{n} \Theta_i(\dot{\mathbf{x}}), \tag{6}$$

where $\Theta_i(\dot{\mathbf{x}})$ represents the angle between the position of scene light source ($\dot{\mathbf{x}}$) and the estimated light source direction $\vec{l}_i$, at the i^{th} specular highlight ($\mathbf{x}_{si}$). Additionally, $\Theta_i(\dot{\mathbf{x}})$ is given by

$$\Theta_i(\dot{\mathbf{x}}) = \arccos\left(\vec{l}_i^{T} \frac{\dot{\mathbf{x}} - \mathbf{x}_{si}}{||\dot{\mathbf{x}} - \mathbf{x}_{si}||}\right). \tag{7}$$

Following the same idea, the scene viewer is also estimated in the second stage assuming that estimated viewer directions $\vec{v}_i$ converge toward the position of the scene viewer, which can be estimated by minimizing the error function

$$E(\ddot{\mathbf{x}}) = \sum_{i=1}^{n} \Theta_i(\ddot{\mathbf{x}}), \tag{8}$$

where $\Theta_i(\ddot{\mathbf{x}})$ represents the angle between the position of scene viewer($\ddot{\mathbf{x}}$) and the estimated viewer direction $\vec{v}_i$, at the i^{th} specular highlight ($\mathbf{x}_{si}$). Additionally, $\Theta_i(\ddot{\mathbf{x}})$ is given by

$$\Theta_i(\ddot{\mathbf{x}}) = \arccos\left(\vec{v}_i^{T} \frac{\ddot{\mathbf{x}} - \mathbf{x}_{si}}{||\ddot{\mathbf{x}} - \mathbf{x}_{si}||}\right). \tag{9}$$

For an image comprising p eyes, the average of all available angular errors is calculated, for light source and viewer, as well as the corresponding standard deviation. Then, Saboia et al. [38] proposed to use four characteristics, described below, in a decision-making stage (Stage 3):

1. **LME:** mean of the angular errors $\Theta_i(\dot{\mathbf{x}})$, related to the light source $\vec{l}$;
2. **LSE:** standard deviation of the angular errors $\Theta_i(\dot{\mathbf{x}})$, related to the light source $\vec{l}$;
3. **VME:** mean of the angular errors $\Theta_i(\ddot{\mathbf{x}})$, related to the viewer $\vec{v}$;
4. **VSE:** standard deviation of the angular errors $\Theta_i(\dot{\mathbf{x}})$, related to the viewer $\vec{v}$.

[4] Lower caption indicates 2-D vectors on image coordinates.

Finally, in the third and last stage, these features are used in association with different combinations of the Support Vector Machine (SVM) classifier (with and without fusion) to detect whether or not the image is a fake. Since light and viewer directions are non-deterministic approximation problems, we estimate such features several times and, for each estimation, we classify it using a trained SVM classifier. In the end, we combine results using simple rules such as: one pristine (if any classifier points out that image as pristine, the final class is pristine), one fake (if any classifier points out that image as fake, the final class is fake), etc.

5.3 Forgery Detection by Manual Illuminant Analysis

The methods presented in Sections 5.1 and 5.2 search for illumination inconsistencies in scene lighting. This section and the next ones, in turn, present methods which are able to detect inconsistencies in light color.

Inconsistency in light color is a different way of analyzing light properties because it is no longer based on physics interaction between the light and the object, but in similarity (or difference) present in image *illuminants*. According to Carvalho et al. [6], *an illuminant (also called illuminant light or light-source color) can also be understood as the color of a light that appears to be emitted from a light source.*

5.3.1 Forgery detection by dichromatic plane analysis Illuminant consistency was firstly investigated by Gholap and Bora [23], who used dichromatic reflection to model image illuminants. According to this model, the reflected light in a specific point of some object composed by non-homogeneous materials consists of diffuse reflection $L_B(\lambda)$ and surface reflection $L_S(\lambda)$. The resulting reflected light $L(\Theta, \lambda)$ can be written as the additive mixture of these two components as [42]

$$L(\Theta, \lambda) = m_S(\Theta) L_S(\lambda) + m_B(\Theta) L_B(\lambda), \tag{10}$$

where $m_S(\Theta)$ and $m_B(\Theta)$ are geometrical scaling factors and together $L_B(\lambda)$ and $L_S(\lambda)$ constitute the *dichromatic plane*.

Based on this dichromatic plane formulation, Tominaga and Wandell [42] propose to estimate dichromatic planes from specular regions on the object using a singular value decomposition (SVD) on the pixels of region, which allows to determine the two more significant eigenvalues and their associated eigenvectors. These eigenvectors constitute the dichromatic plane which can be mapped onto a straight line in the normalized r-g chromaticity space.

To detect image forgeries, Gholap and Bora [23], proposed to analyze the straight lines provided by different objects. The assumption here is that, if it is a pristine image, all the lines should auto intersect in a unique point. Otherwise, there are signs of forgery.

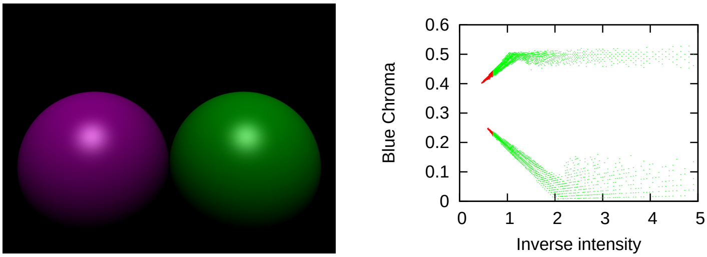
5.3.2 Forgery detection by illuminant map analysis Riess and Angelopoulou [35] proposed to use illuminant colors in a slightly different way. Despite using dichromatic reflection model, Riess and Angelopoulou estimate image illuminants locally through a modified version of a physics-based approach, originally proposed by Tan et al. [41], named *Inverse Intensity-Chromaticity (IIC) space* .

According to this modified version, a local illuminant can be estimated for a small patch such as

$$\chi_c(\mathbf{x}) = m(\mathbf{x})\frac{1}{\sum_{i\in\{R,G,B\}} f_i(\mathbf{x})} + \gamma_c, \tag{11}$$

where $f_i(\mathbf{x})$ is the intensity and $\chi_c(\mathbf{x})$ is the chromaticity (i.e., normalized RGB-value) of a color channel $c \in \{R, G, B\}$ at position $\mathbf{x}$, respectively. γ_c is the chromaticity of the illuminant in channel c and $m(\mathbf{x})$ is an approximated parameter which comprises information that captures geometric influences, i.e., light position, surface orientation and camera position.

For estimating an illuminant color from a specific patch, per color channel c, pixels belonging to the patch are projected onto the IIC space which is a per-channel 2-D space, where the $x-$axis is obtained by the inverse of the sum of the chromaticities per pixel, $1/\sum_i f_i(\mathbf{x})$, and the $y-$axis is the pixel chromaticity for that particular channel. Figure 13 depicts an example of pixels mapping onto IIC.



(a) (b)

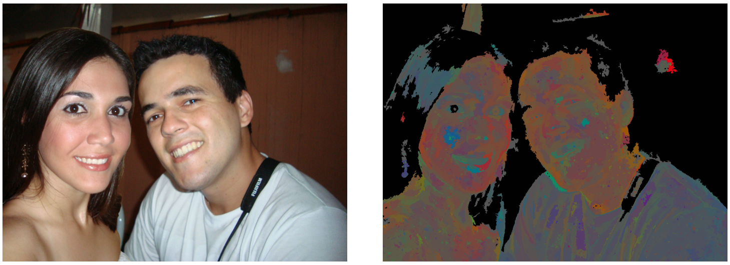
Figure 13. Example of IIC (blue channel). Mapping pixels from violet and green balls (a) onto IIC space (b). Both sets of pixels converge toward the blue illuminant color (in $y-$axis). Source: Carvalho et al. [8].

In summary, the method proposed by Riess and Angelopoulou is described through four main steps:

1. segmentation of the image regions with approximately same color, which is named *superpixels*;
2. manual selection of interest superpixels, the ones that will be deeply investigated;

3. for each super pixel, an illuminant color is estimated by using IIC space. Superpixels selected in Step 2 have their illuminant estimated a second time. This process results in an image comprising illuminant colors of all of the superpixels, as depicted in Figure 14, and it is named *illuminant map*;

4. the last step of the algorithm calculates a grayscale image, with values between 0 and 1, named *distance map*. This map captures the influence of each interest superpixel over the remaining super pixels present in the image.



(a) (b)

Figure 14. Illuminant map (a) produced when applying Riess and Angelopoulou [35] method on an image (b).

5.3.3 Forgery detection by block similarity analysis Wu and Fang [45] have also used illuminants estimation to detect image splicing. The authors use three statistical illuminant color estimation algorithms, Grey-Shadow, first-order Grey-Edge and second-order Grey-Edge, which can be estimated using the framework below, proposed by Weijer et al. [15]

$$k\mathbf{e}^{n,p,\sigma} = \left(\int \left| \frac{\partial^n \mathbf{f}^\sigma(\mathbf{x})}{\partial \mathbf{x}^n} \right|^p d\mathbf{x} \right)^{1/p}, \qquad (12)$$

where $\mathbf{x}$ denotes a pixel coordinate, k is a scale factor, $|\cdot|$ is the absolute value, ∂ the differential operator, $\mathbf{f}^\sigma(\mathbf{x})$ is the observed intensities at position $\mathbf{x}$ smoothed with a Gaussian with standard deviation σ, p is the Minkowski norm, and n is the derivative order.

Their algorithm divides the image into overlapping blocks, calculating illuminant color for each block using one of the three previously described algorithms. For selecting the best illuminant algorithm, the authors use a maximum likelihood classifier based on mixture of Gaussians (GMM). Once the illuminant color for every block in the image has been estimated, it is necessary to manually select a reference block to be used as ground truth. The next step is to calculate, for all the blocks in the image, the difference between the estimated and the reference illuminant color, tagging blocks as fake the ones which present differences larger than a threshold.

5.4 Forgery Detection by Automatic Illuminant Map Analysis

The methods presented in Section 5.3 represent a significant step toward a deep analysis of images using illumination characteristics. However, all of them heavily depend on the user which, many times, lead to inaccurate and incomplete analyses. Furthermore, users are usually not able to detect intrinsic patterns, which can be detected by more sophisticated algorithms, such as machine learning techniques. In this section, we present a method which explores illuminant inconsistencies based on image processing and machine learning techniques.

Carvalho et al. [8] proposed to extract features from illuminant maps and analyze these patterns using machine learning algorithms to detect whether an image involving people is genuine. To compare the illuminants of two different objects at the same scene, it is necessary that both objects have the same material since illuminant color is the result between interaction of scene illuminant and the light incident on the material. Among all possible different materials in a scene, skin is one of particular interest since it is relatively homogeneous. Also, image splicing involving people is one of the most common kinds of manipulations. Due to these reasons, Carvalho et al. [8] analyzed patterns on pairs of people's face to detect forgeries.

Given an illuminant map, such as the ones provided by Riess and Angelopoulou [35], the authors analyzed texture and edge features looking for inconsistencies. It is important to highlight here that the authors use two kinds of illuminant maps: one based on a physical model and another one based on a statistical model. This is necessary since each model captures different information.

According to Carvalho et al. [8], the texture of pristine faces presents a different pattern from faces produced by fake images, as depicted in Figure 15. The authors have used the SASI [10] algorithm to capture texture features.

Edge features used as illuminant maps usually have certain discontinuities in edge regions. When analyzing a pristine image, these discontinuities need to appear in both faces. When a similar region of two different faces present different discontinuities, this can be a sign of manipulation. Figure 16 depicts an example of this situation.

For capturing edges information, the authors proposed a new algorithm named HOGedge, which calculates Histograms of Oriented Gradients (HOG) [14] in a region around edge points and use the concept of bag of words [13] to project descriptions of different lengths onto a fixed size space.

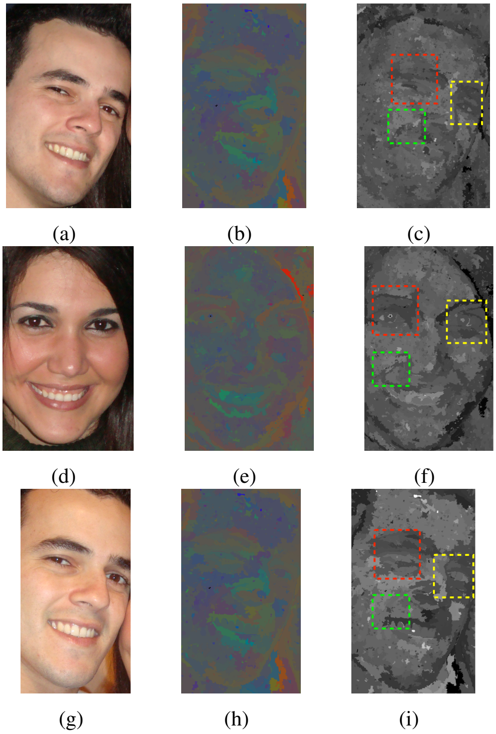
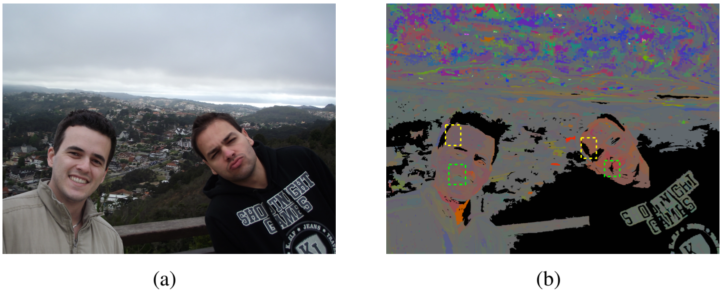


Figure 15. Difference in texture between pristine and fake images. First and second rows depict people (and their illuminant maps) from the same image. The third row presents the same person in the first row but extracted from a different image. The similarity of regions highlighted by colored boxes (red, yellow, and green) is larger in pristine than in fake images. Source: Carvalho et al. [6].

After coding such important information into feature vectors, a combination of machine learning techniques, using Support Vector Machines (SVM), is applied to detect whether an image is a fake. Figure 17 shows an overview of Carvalho et al. [8] method.

5.5 Forgery Detection by Shadow Constraints

Analyzing light inconsistencies in a different way, Kee and Farid [28] propose to use inconsistencies in cast and attached shadows to detect image splicing. Kee and Farid [28] use the intersection of many wedge-shaped constraints, each one of them constructed connecting a straight line from the point in shadow to points on the object that may have cast the shadow,



(a) (b)

Figure 16. Different illuminants can generate different discontinuities as depicted in the highlighted regions of (b). The person on the left does not show discontinuities in the highlighted regions (green and yellow). On the other hand, the spliced part (person on the right) presents discontinuities in the same regions highlighted in the person on the left. Source: Carvalho et al. [6].

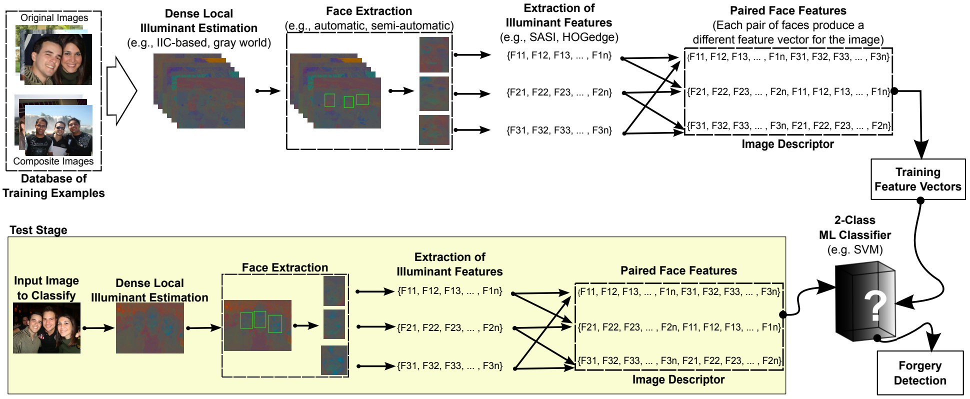

Original Images
Composite Images
Database of Training Examples
Dense Local Illuminant Estimation (e.g., IIC-based, gray world)
Face Extraction (e.g., automatic, semi-automatic)
Extraction of Illuminant Features (e.g., SASI, HOGedge)
{F11, F12, F13, ... , F1n}
{F21, F22, F23, ... , F2n}
{F31, F32, F33, ... , F3n}
Paired Face Features (Each pair of faces produce a different feature vector for the image)
{F11, F12, F13, ... , F1n, F31, F32, F33, ... , F3n}
{F21, F22, F23, ... , F2n, F11, F12, F13, ... , F1n}
{F31, F32, F33, ... , F3n, F21, F22, F23, ... , F2n}
Image Descriptor
Training Feature Vectors
2-Class ML Classifier (e.g. SVM)
?
Test Stage
Input Image to Classify
Dense Local Illuminant Estimation
Face Extraction
Extraction of Illuminant Features
{F11, F12, F13, ... , F1n}
{F21, F22, F23, ... , F2n}
{F31, F32, F33, ... , F3n}
Paired Face Features
{F11, F12, F13, ... , F1n, F31, F32, F33, ... , F3n}
{F21, F22, F23, ... , F2n, F11, F12, F13, ... , F1n}
{F31, F32, F33, ... , F3n, F21, F22, F23, ... , F2n}
Image Descriptor
Forgery Detection

Figure 17. Overview of the method proposed by Carvalho et al. [8]. Source: Carvalho et al. [8].

to restrict the projected location of the light source. However, due to perspective geometry, the projected light source location can present signs of ambiguity, flipping the resulting wedge constraint region by 180 degrees.

Another useful information used by Kee and Farid [28] is attached shadow. This kind of shadows happens when parts of an object occlude light from itself creating a shadow part. The edge between shadow and bright parts in the object is named *terminator* and it is a surface contour where normals make an angle of exactly 90 degrees with a vector point toward light source. Attached shadows are provided by any locally convex surface in the object and their constraints are specified by half-planes. Figure 18 depicts examples of cast and attached shadow constraints.

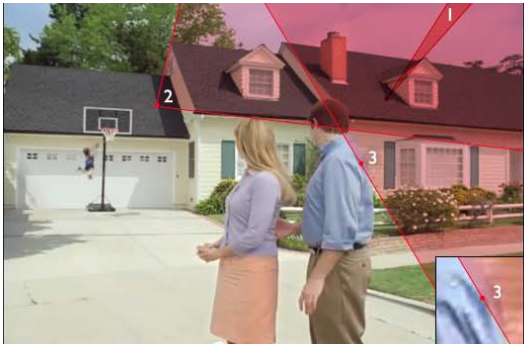


Figure 18. Examples of cast and attached shadows. Cast shadow constraints (1 and 2) delimit wedge-shape areas while the attached shadow constraint (3) delimits half-planes. Source: Kee and Farid [28].

Together, the intersection of cast and attached shadow constraints is able to satisfactorily restrict the projected light source location since, for an authentic image, there must be a location in the infinite plane that satisfies all cast and attached shadow constraints [28].

Computationally, cast and attached shadow constraints can be represented as linear inequalities in the plane. The wedge-shaped constraint is defined by two linear inequalities in the unknown $\mathbf{x}$

$$\mathbf{n}_i^1 \cdot \mathbf{x} - \mathbf{n}_i^1 \cdot \mathbf{p}_i \geq 0 \quad \text{and} \quad \mathbf{n}_i^2 \cdot \mathbf{x} - \mathbf{n}_i^2 \cdot \mathbf{p}_i \geq 0, \tag{13}$$

where $\mathbf{n}_i$ is normal to the line and $\mathbf{p}_i$ is a point on the line selected by the user for casting shadow. Similarly to wedge-shaped constraints, a half-plane constraint is defined by a linear inequality in the unknown $\mathbf{x}$

$$\mathbf{n}_i \cdot \mathbf{x} - \mathbf{n}_i \cdot \mathbf{p}_i \geq 0. \tag{14}$$

All of the constraints can be grouped into a system of m inequalities as

$$\begin{pmatrix} \mathbf{n}_1 \\ \mathbf{n}_2 \\ \vdots \\ \mathbf{n}_m \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} - \begin{pmatrix} \mathbf{n}_1 \cdot \mathbf{p}_1 \\ \mathbf{n}_2 \cdot \mathbf{p}_2 \\ \vdots \\ \mathbf{n}_m \cdot \mathbf{p}_m \end{pmatrix} \geq 0. \tag{15}$$

If the system belongs to a consistent scene, it has a solution. Otherwise, the image presents inconsistencies.

6 Conclusion and Research Directions

This tutorial has briefly presented some concepts related to Digital Forensics. After presenting evidences that users are strongly influenced by images, we presented some important historical records involving image tampering. Also, we discussed some relevant research topics in Digital Forensics. Finally, we described some visual computing and machine learning techniques applied to detect image splicing in the literature.

Digital Forensics is a new and very interesting field in Computer Science. In the last years, methods have been improved constantly, however, we are still far from a final “silver bullet”. Methods that properly work in a specific scenario can fail drastically in a different one. Considering illuminant-based detection approaches, for example, it is necessary to develop more robust techniques for estimating illuminant maps.

Problems related with Multimedia Phylogeny are also very interesting. Since it is a brand new research field in Digital Forensics, many problems need a more robust and efficient solution along with a proper theoretical formulation. Continuous improvement and extensions might allow audio and video phylogeny techniques, for example, to strongly help protecting copyright content.

Child pornography and spoofing detection are also active research areas in Digital Forensics. The first one is becoming more and more important for authorities all over the world once laws against this kind of crimes have become stronger in the last years. The second one is receiving attention because companies invest heavily in research for their security, which in many times it is performed using biometrical systems.

As one future research direction, extensions to Carvalho et al. [8] method for analyzing any skin region (instead of only faces) would be very useful. Furthermore, it is necessary to develop and deploy methods that make the forgery creation task harder. For instance, methods that analyze 3-D light direction, instead of 2-D, would be more challenging for counterfeiters to deceive when seeking to create realistic forgeries.

In a more extensive view for research directions, methods able to combine solutions for different problems into a single solution probably are a big challenge and research opportunity in Digital Forensics. A method able to detect splicing and copy-paste through the automatic combination of different evidence would avoid experts to waste time testing different and isolated techniques for detecting forgeries.

7 Acknowledgments

The authors thank the financial support of Unicamp, Brazilian National Research Counsel – CNPq (Grants #140916/2012-1, #477662/2013-7, #307113/2012-4, and #304352/2012-8), São Paulo Research Foundation – FAPESP, (Grant #2010/05647-4 and #2011/22749-8), Coordination for the Improvement of Higher Education Personnel – CAPES (Grants #0214-13-2), CAPES DeepEyes Project, IF Sudeste MG, and Microsoft Research.

References

[1] O. M. Al-Qershi and B. E. Khoo. Passive Detection of Copy-Move Forgery in Digital Images: State-of-the-Art. *Forensic Science International*, 231(1-3):284–295, 2013.

[2] M. D. Ansari, S. P. Ghrera, and V. Tyagi. Pixel-Based Image Forgery Detection: A Review. *IETE Journal of Education*, 55(1):40–46, 2014.

[3] S. Avila, N. Thome, M. Cord, E. Valle, and A. A. Araújo. Pooling in Image Representation: The Visual Codeword Point of View. *Computer Vision and Image Understanding*, 117(5):453 – 465, 2013.

[4] C. Barnes, E. Shechtman, A. Finkelstein, and D. B. Goldman. PatchMatch: A Randomized Correspondence Algorithm for Structural Image Editing. *ACM Transactions on Graphics (ToG)*, pages 24:1–24:11, July 2009.

[5] C. Barnes, E. Shechtman, A. Finkelstein, and D. B. Goldman. The Generalized PatchMatch Correspondence Algorithm. In *European Conference on Computer Vision (ECCV)*, pages 29–43, 2010.

[6] T. Carvalho. *Illumination Inconsistency Sleuthing for Exposing Fauxtography and Uncovering Composition Telltales in Digital Images*. PhD thesis, Institute of Computing, University of Campinas, 2014.

[7] T. Carvalho, H. Pedrini, and A. Rocha. Illumination Inconsistency Sleuthing for Exposing Fauxtography and Uncovering Composition Telltales in Digital Images. In *Workshop of Theses and Dissertations - XXVII SIBGRAPI Conference on Graphics, Patterns and Images*, Rio de Janeiro, RJ, Brazil, 2014.

[8] T. Carvalho, C. Riess, E. Angelopoulou, H. Pedrini, and A. Rocha. Exposing Digital Image Forgeries by Illumination Color Classification. *IEEE Transactions on Information Forensics and Security (T.IFS)*, 8(7):1182–1194, 2013.

[9] CASIA. Tampered Image Detection Evaluation Database, Last Access: March 2015. `http://forensics.idealtest.org:8080/index_v2.html`.

[10] A. Çarkacıoğlu and F. T. Yarman-Vural. SASI: A Generic Texture Descriptor for Image Retrieval. *Pattern Recognition*, 36(11):2615–2633, 2003.

[11] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou. An Evaluation of Popular Copy-Move Forgery Detection Approaches. *IEEE Transaction on Information Forensics and Security (T.IFS)*, 7(6):1841–1854, 2012.

[12] F. O. Costa, M. Eckmann, W. J. Scheirer, and A. Rocha. Open Set Source Camera Attribution. In *SIBGRAPI*, pages 71–78, 2012.

[13] G. Csurka, C. R. Dance, L. Fan, J. Willamowski, and C. Bray. Visual Categorization With Bags of Keypoints. In *Workshop on Statistical Learning in Computer Vision*, pages 1–8, 2004.

[14] N. Dalal and B. Triggs. Histograms of Oriented Gradients for Human Detection. In *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 886–893, 2005.

[15] J. V. de Weijer, T. Gevers, and A. Gijsenij. Edge-based Color Constancy. *IEEE Transactions on Image Processing*, 16(9):2207–2221, 2007.

[16] Z. Dias, S. Goldenstein, and A. Rocha. Large-Scale Image Phylogeny: Tracing Image Ancestral Relationships. *IEEE MultiMedia*, 20(3):58–70, July 2013.

[17] Z. Dias, A. Rocha, and S. Goldenstein. Video Phylogeny: Recovering Near-duplicate Video Relationships. In *IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 1–6, 2011.

[18] Z. Dias, A. Rocha, and S. Goldenstein. Image Phylogeny by Minimal Spanning Trees. *IEEE Transactions on Information Forensics and Security*, 7(2):774–788, April 2012.

[19] H. Farid. A Survey of Image Forgery Detection. *IEEE Signal Processing Magazine*, 26(2):16–25, 2009.

[20] J. D. Foley, A. van Dam, S. K. Feiner, and J. F. Hughes. *Computer Graphics: Principles and Practice*. Addison-Wesley Publishing Company, 2 edition, 1993.

[21] S. J. Frenda, E. D. Knowles, W. Saletan, and E. F. Loftus. False Memories of Fabricated Political Events. *Journal of Experimental Social Psychology*, 49(2):280 – 286, 2013.

[22] M. Garry, D. Strange, D. M. Bernstein, and T. Kinzett. Photographs Can Distort Memory for the News. *Applied Cognitive Psychology*, 21(8):995–1004, 2007.

[23] S. Gholap and P. K. Bora. Illuminant Colour Based Image Forensics. In *IEEE Region 10 Conference*, pages 1–5, 2008.

[24] T. Gloe and R. Böhme. The 'Dresden Image Database' for Benchmarking Digital Image Forensics. In *25th Symposium On Applied Computing*, volume 2, pages 1585–1591, Mar. 2010.

[25] IMD. Image Manipulation Dataset, Last Access: March 2015. `http://www5.cs.fau.de/research/data/image-manipulation/`.

[26] M. K. Johnson and H. Farid. Exposing Digital Forgeries by Detecting Inconsistencies in Lighting. In *ACM Workshop on Multimedia and Security*, pages 1–10, New York, NY, USA, 2005. ACM.

[27] M. K. Johnson and H. Farid. Exposing Digital Forgeries Through Specular Highlights on the Eye. In T. Furon, F. Cayre, G. J. Doërr, and P. Bas, editors, *ACM Information Hiding Workshop (IHW)*, volume 4567 of *Lecture Notes in Computer Science*, pages 311–325, 2008.

[28] E. Kee, J. O'brien, and H. Farid. Exposing Photo Manipulation with Inconsistent Shadows. *ACM Transactions on Graphics (ToG)*, 32(3):28:1–28:12, July 2013.

[29] J. Lukas, J. Fridrich, and M. Goljan. Digital Camera Identification from Sensor Pattern Noise. *IEEE Transaction on Information Forensics and Security (T.IFS)*, 2:205–214, 2006.

[30] J. Määttä, A. Hadid, and M. Pietikainen. Face Spoofing Detection from Single Images using Micro-texture Analysis. In *International Joint Conference on Biometrics (IJCB)*, pages 1–7, Oct. 2011.

[31] P. Nillius and J. Eklundh. Automatic Estimation of the Projected Light Source Direction. In *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 1076–1083, 2001.

[32] M. Nucci, M. Tagliasacchi, and S. Tubaro. A Phylogenetic Analysis of Near-Duplicate Audio Tracks. In *IEEE International Workshop on Multimedia Signal Processing*, pages 099–104, 2013.

[33] Y. Ostrovsky, P. Cavanagh, and P. Sinha. Perceiving Illumination Inconsistencies in Scenes. *Perception*, 34(11):1301–1314, 2005.

[34] M. C. Polastro and P. M. S. Eleuterio. NuDetective: A Forensic Tool to Help Combat Child Pornography through Automatic Nudity Detection. In *2010 Workshop on Database and Expert Systems Applications (DEXA)*, pages 349–353, Aug 2010.

[35] C. Riess and E. Angelopoulou. Scene Illumination as an Indicator of Image Manipulation. In *ACM Information Hiding Workshop (IHW)*, volume 6387, pages 66–80, 2010.

[36] 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 Computing Surveys*, 43(4):1–42, 2011.

[37] A. Ruszczyǹski. *Nonlinear Optimization*. Princeton University Press, 2006.

[38] P. Saboia, T. Carvalho, and A. Rocha. Eye Specular Highlights Telltales for Digital Forensics: A Machine Learning Approach. In *IEEE International Conference on Image Processing (ICIP)*, pages 1937–1940, 2011.

[39] D. L. M. Sacchi, F. Agnoli, and E. F. Loftus. Changing History: Doctored Photographs Affect Memory for Past Public Events. *Applied Cognitive Psychology*, 21(8):1005–1022, 2007.

[40] W. R. Schwartz, A. Rocha, and H. Pedrini. Face Spoofing Detection through Partial Least Squares and Low-Level Descriptors. In *International Joint Conference on Biometrics (IJCB)*, pages 1–8, Oct. 2011.

[41] R. Tan, K. Nishino, and K. Ikeuchi. Color Constancy through Inverse-Intensity Chromaticity Space. *Journal of the Optical Society of America A*, 21(3):321–334, 2004.

[42] S. Tominaga and B. Wandell. Standard Surface-Reflection Model and Illumination Estimation. *Journal of the Optical Society of America A*, 6(4):576–584, 1989.

[43] A. Ulges and A. Stahl. Automatic Detection of Child Pornography using Color Visual Words. In *IEEE International Conference on Multimedia and Expo (ICME)*, pages 1–6, 2011.

[44] W. Wang, J. Dong, and T. Tan. A Survey of Passive Image Tampering Detection. In A. Ho, Y. Shi, H. Kim, and M. Barni, editors, *Digital Watermarking*, volume 5703 of *Lecture Notes in Computer Science*, pages 308–322. Springer Berlin Heidelberg, 2009.

[45] X. Wu and Z. Fang. Image Splicing Detection Using Illuminant Color Inconsistency. In *IEEE International Conference on Multimedia Information Networking and Security (MINES)*, pages 600–603, 2011.