Digital Image Forensics vs. Image Composition: An Indirect Arms Race

Victor Schetinger, Massimo Iuliani, Alessandro Piva, Senior Member, IEEE, and Manuel M. Oliveira

Abstract—The field of image composition is constantly trying to improve the ways in which an image can be altered and enhanced. While this is usually done in the name of aesthetics and practicality, it also provides tools that can be used to maliciously alter images. In this sense, the field of digital image forensics has to be prepared to deal with the influx of new technology, in a constant arms-race. In this paper, the current state of this arms-race is analyzed, surveying the state-of-the-art and providing means to compare both sides. A novel scale to classify image forensics assessments is proposed, and experiments are performed to test composition techniques in regards to different forensics traces. We show that even though research in forensics seems unaware of the advanced forms of image composition, it possesses the basic tools to detect it.

Index Terms—Digital Image Forensics, Image Composition

I. INTRODUCTION

The popularization of digital cameras and the Internet have made it easy for anyone to capture and share pictures. Current research suggests, however, that people are not very keen on discerning between real and edited pictures [1]. This poses a critical problem, as softwares such as Adobe Photoshop [2] and GIMP [3] allow anyone to easily create high-quality composites. In such a scenario, how can one be sure that an image is authentic and depicts a factual scene?

An arms race between forgers and forensic analysts is in progress [4]. While new and more sophisticated forges are being conceived, forensic techniques keep evolving to catch them. Most image manipulations, however, are neither malicious nor dangerous. There are plenty of legitimate reasons to edit images, such as for marketing and design. Unfortunately, sophisticated tools developed for these tasks can be used by forgers and the analysts have to struggle to catch up.

In this paper, we analyze the current state of this arms race between the field of image forensics and image composition techniques. Here, image composition is used as an umbrella term for all techniques from areas such as computer graphics, computational photography, image processing, and computer vision, that could be used to modify an image. More specifically, we discuss works that have the potential to either be used to perform or hide forges in digital images.

From a forensic point of view, image manipulation is usually classified as either splicing, copy-pasting (also called cloning), erasing, or retouching. A splicing operation consists of transferring an object from an image into another, but this could be done simply by cutting and pasting, or using an advanced technique that matches the gradient of the target image [5]. Copy-pasting is similar in essence, but the transferred object comes from the same image. Retouching has a vague definition that could fit a wide range of actions, such as blurring regions of the image, recoloring, and applying filters.

While many modern image-composition techniques could be used to make sophisticated forgeries, almost none of them have been scrutinized by forensic works. There is, however, a large body of forensic tools that could be used for this task. This paper surveys both the forensics arsenal and image-composition techniques to identify the best strategies to analyze these novel forgeries. We conclude that the field of digital image forensics is prepared to deal with image composition.

The main contributions of this paper include:

- A novel scale for the different levels of forensics image assessments (Section II);
- A new way to classify forensic techniques, combining the two most used classifications in the literature with the proposed scale (Section III);
- A new classification for image composition, extending the existing types worked in the forensics literature (Section IV);
- A theoretical and experimental analysis on image composition techniques from a forensics point of view (Sections V and VI).

II. THE FORGERY DETECTION SCALE

According to recent surveys [4][11][12], there are two main fronts to digital image forensics: source identification and forgery detection. Source identification tries to link an image to the device that took it. Acquisition traces are extracted from the investigated image and then compared with a dataset of possible fingerprints specific for each class/brand/model of devices. Matching fingerprints are exploited to identify the image source device. Forgery detection is concerned in determining if and how a target image has been altered. In the same sense, an image is provided for analysis, several different image features and traces can be observed, and there are different possible outcomes. This paper is focused on forgery detection, but our findings can provide useful insights for device identification.

Forgery detection mostly works twofold: either looking for patterns where there shouldn’t be, or looking for the lack of patterns where there should be. If someone, for example, splices an object from an image into another, and resizes it so it is in the same scale as the target picture; the resizing operation now creates a pattern of correlation between its pixels where there shouldn’t be one. On the other hand, the target image had several patterns, such as its CFA (Color Filter Array, explained on Section III-A), the illuminant color, etc. which were disrupted by the spliced object.
The most simplistic view would pose that there are only two outcomes for forgery detection: the image has been altered, or no evidence of alteration is found. However, this classification might not be sufficient. Simply compressing an image might be considered an alteration, even though it is a commonplace operation, making this classification useless. Different forensic techniques work on different assumptions of what traces could be present on the image and what they can infer from them, from the location to the nature of the forgery. There is no standard on the literature, however, for classifying and comparing techniques based on their outcomes.

Here, we propose a new general classification scale called the FD (short for Forgery Detection scale). This scale is based in the concept of an image being native or not: a native image is an image that was captured by a device and then outputted to the user “as-is”. Conceptually, this is easy to define, but technically there might be some complications: different devices process the image differently. These problems will be discussed in detail further in the paper.

The FD scale ranks forensic techniques based on the type of evidence they can provide about an image’s nativity. The first possible outcome is the negative case, when it is not possible to determine if an image has undergone any form of alteration. This could happen because the image is really native, or because the analyzed traces do not show forgery, but it makes no difference: it is not possible to say that an image is truly native, only that there is no evidence supporting it to be forged. This outcome falls outside our scale in practice, but can be called FD0 for simplicity. The following are the different levels of our Forensics Detection scale:

**FD0** No evidence can be found that the image is not native.
**FD1** The image has undergone some form of alteration from its native state, but the nature and location of it is unknown.
**FD2** The image has undergone some form of alteration from

Fig. 1: Different ways in which composition techniques can be used to alter images. a) Removing soft shadows [6]. The hand shadow from the top image has been removed on the bottom image. b) Inserting synthetic objects [7]. The marble angel in the picture is not real, it was rendered into the scene along with its complex light interactions. c) Performing edge-aware filtering [8]. The bottom image was filtered to perform a localized color editing on some of the stone statues. d-f) Morphing two different objects together to create a blend [9]. The cat in Figure 1e is a composite of the cat in Figure 1d and the lion in Figure 1f. g) Transferring an object from one image to another, adjusting its illumination according to the target scene [10]: the building was spliced on the field in the top image, and in the bottom it had its lighting adjusted to match the composition.
its native state and the location of the alteration can be determined, but its nature is not known.

**FD3** The image has undergone some form of alteration from its native state, the location of the alteration can be determined and the nature of it is known.

**FD4** All the conclusions of the previous item, and a particular tool or technique can be linked to the forgery.

These should be referred as FD (short for forgery detection) scale, with values FD0-4. It could be argued that the ultimate form forgery detection would go beyond identifying the used technique, by locating a forger or even estimating the historic of the image’s alterations [13]. It is a valid point, but they are not common in digital image forensics and fall out of this paper’s scope. The FD scale is backwards inclusive for FD $> 0$, meaning that if FD4 can be guaranteed so can FD3, FD2 and FD1. The following subsections provide in-depth explanation of the different levels of the FD scale and important considerations.

A. **FD1: Nativity**

The FD1 level differs from the negative case FD0 because it is possible to determine that the image is not native. This is not so simple to assess, as most modern cameras have a processing pipeline comprised of several operations (demosaicing, white balance, etc), changing the image before the user has access to it. Furthermore, demosaicing is such a fundamental operation in modern cameras that it makes little sense talking about images without it. For the sake of generality, we propose that any form of pre-processing on the image up until a single compression can be accepted without breaching the image nativity. In the cases where the capture device is known, a forensics specialist can limit the scope of his analysis and determine only some operations are valid. A forensic technique achieves FD1 when it is able to find evidence of alteration after capture. Techniques that analyze an image’s EXIF information are an example of FD1: they can detect an inconsistency in the metadata proving an image is not native, but nothing can be said about location or nature of the alteration.

B. **FD2: Location**

The FD2 level is obtained when the general location of the alteration in the image is known. It is possible that a region of an image has been erased by a series of copy-pasting operations, and then retouched with smoothing brushes. In this case the boundaries of the forgery might no be as clear. If a technique is able to obtain any form of specificity on the altered region, FD2 is achieved. This is the case when analyzing traces such as PRNU (Photo Response Non-Uniformity, Section III-A), CFA or ELA (Error Level Analysis, Section III-B), that are locally structured on the image. If evidence of any global alteration on the image is found, such as median or bilateral filtering, then the location of the forgery is the whole image. Similarly, operations that remove parts of the image such as seam carving and cropping can be detected but the actual altered area is not present in the analyzed image anymore. It is argued that the forgery location can be considered to be all image, reaching FD2.

C. **FD3: Nature**

The nature of the forgery can be subjective, because it is not possible to predict all ways in which an image can be altered. The most commonly studied forms of forgery such as splicing, copy-pasting and erasing, are just a subset of possibilities. As was discussed on the introduction, image composition techniques are able to alter the shape, texture and orientation of objects, and even merge them together. For simplicity, any meaningful information in addition to location of the processing that can be used to assist the forensics analyst can be considered FD3. If an object has been rotated and scaled, identifying any of these operations awards an FD3 level on the scale. Identifying a spliced object is worth an FD3 on the scale because the image is not native (FD1), its location on the target image is evident (FD2), and the nature of the alteration is known (FD3).

D. **FD4: Technique**

The highest level on our scale, FD4, is achieved when the analyst finds evidences that can link the forgery to a particular technique or tool. A splicing can be done by simply cutting a region from an image an pasting over another, but there are also sophisticated ways to blend them, such as Alpha Matting or Seamless Cloning. A forensic technique that is able to, after obtaining FD3, provide further insight into the technique or tool used to perform the forgery achieves FD4.

III. **THE FORENSICS ARSENAL**

The current state-of-the-art on digital image forensics provides an arsenal of tools and techniques for forensics analysts. In this section we investigate the most relevant approaches and their capabilities, both in terms of applicability (i.e. when we can use them) and assessment (i.e. the level that can be achieved in the FD scale). In a general way, it can be noted that there is a trade off between the generality and the FD level that a technique is able to reach. This is intuitive, because the higher the level on the scale, the more specific the assessments are. FD1 can be simplified as a boolean statement (the image is either native or not). From FD2 onwards, there is a large set of possible answers (all different combinations of pixels in the image). To identify the nature of the forgery in the image (FD3), a technique must be looking for more specific features or traces.

An image forensic tool is usually designed considering three steps:

1. Some traces in the image - possibly introduced by the forgery process - are identified; such traces can be scene-level information such as “the image lighting”, or signal-level, such as “the color filter array pattern”.
2. These traces are measured and quantified in some way, resulting in features, which are usually numeric in nature;
3. By analyzing through experimentation how the set of features behaves on native and forged images, a decision is taken about the image. This can be done using simple thresholds or sophisticated machine learning techniques.

In Table [1] we show a practical example of previous steps for the technique developed by Carvalho et. al. [14] to detect...
TABLE I: The steps of the tool by Carvalho et. al. [14].

| Layer  | Example                                |
|--------|----------------------------------------|
| Trace  | Illuminant or light source of the image. |
| Feature| Estimated illuminant colors and light intensity on object edges. |
| Decision| SVM classification. |

splicing. The used trace is the illuminant, or the light source. The key observation is that if an object is spliced and the original image had different light conditions, such as indoor or outdoor lighting, or even incandescent vs. fluorescent lights, this trace can be used to identify it. The features used are the estimated illuminant colors and the light intensity on the edges, for the different analyzed regions of the image. The decision process uses a Support Vector Machine (SVM) to classify the image as either spliced (FD3) or inconclusive (FD0) based on the features.

Forensic tools classification is based on the traces they analyze. Piva [12] distinguishes between traces left by three different steps of the image formation process: acquisition, coding and editing. Another intuitive classification has been proposed by Farid [4] where the forensic techniques are grouped into five main categories: pixel-based, format-based, camera-based, physically-based and geometric-based. Farid’s classification is more common in the literature and distinguishes better between traces, but Piva’s can be closely related to the FD scale. We propose a classification based on Piva’s approach (Fig. 2), but with greater specificity, similarly to Farid’s.

The most relevant traces and correspondent tools developed by the forensic community will be discussed in the following subsection. The FD scale will be used to describe which level of assessment can be expected when examining an image using a specific tool.

A. Acquisition Traces (AT)

Native images come to life with distinctive marks (artifacts, noise, inconsistencies) due to the acquisition process. Both hardware (e.g., lens, sensor) and software components (e.g., demosaicing algorithm, gamma correction) contribute to the image formation, introducing specific traces into the output (native) image. When a native image is processed some of these traces can be deteriorated or destroyed, exposing evidence of tampering. Forgery detection using acquisition traces generally falls in one of two categories:

1) Global: The analyzed trace is a global camera signature. Non-native images can be exposed when this signature does match with the supposed source device. For instance, in [15] non-native JPEG images are exposed by analyzing quantization tables, thumbnails and information embedded in EXIF metadata. In [16] the reference pattern noise of the source device is taken as a unique identification fingerprint. The absence of the supposed pattern is used as evidence that the image is non-native.

2) Local: The analyzed trace has a local structure in the image. Its inconsistencies in some portion of the image can be exploited to localize the tampering. For instance, Ferrara [17] uses demosaicking artifacts that form due to color interpolation. They can be analyzed at a local level to derive the tampering probability of each 2×2 image block. Fridrich [18] reveals forgeries by detecting the absence of the PRNU on specific regions of the investigates image.

Let us note that some traces can be considered both at a global or local level (e.g., demosaicing artefacts and PRNU), allowing to identify non-native images (FD1) or to localize forgeries (FD2). The analysis of acquisition traces is usually limited to matching a known pattern, and they can be easily disrupted. For this reason, FD2 is the highest we can expect to achieve on the FD scale using acquisition traces. The analysis of acquisition traces generally requires some additional information about the source device. In some cases this information depends on the source device model or manufacturer (e.g., color filter array pattern, quantization tables), and can be easily obtained to assess image nativity [19]. In other cases these traces are unique camera fingerprints (e.g. PRNU) and can be obtained by having the source device available, or be estimated by using different images captured by the same device.

B. Coding Traces

Lossy compression might happen in many occasions during the life of a digital image:

- Native images of non professional cameras and smartphones usually come to life in JPEG format;
- when uploading a photo on a social network lossy compression is usually applied to the image;
- when a JPEG image is altered and saved again in JPEG, double lossy compression occurs.
For this reason, most of the literature has focused on studying the traces left by single and multiple chains of JPEG-compression. This is a very prolific field of study in forensics, with a wide variety of techniques. Fan \cite{20} and Luo \cite{21} provide efficient methods to determine whether an image has been previously JPEG compressed, and, if so, are able to estimate some of the compression parameters. Further advances have been also provided by Li et al. \cite{22} to identify high-quality compressed images basing on the analysis of noises in multiple-cycle JPEG compression. On Bianchi’s technique \cite{23}, original and forged regions are discriminated in double compressed images, either aligned (A-DJPG) or non-aligned (NA-DJPG) even when no suspect region is detected. Yang et al. \cite{24} propose an error-based statistical feature extraction scheme to face the challenging case where both compressions are based on the same quantization matrix.

In most cases the analyst can exploit coding traces to disclose non-native images or to localize the tampering, reaching FD1 and FD2 in the forensic scale; FD3 has not been deeply investigated but, as shown in literature, coding traces can reveal something more than mere localization of the tamper. Farid \cite{25} shows that, when combining two images with different JPEG compression quality, it may be possible to recover information of the original compression quality of the tampered region. A stronger compression in later stages usually deteriorates the traces of previous compressions, compromising the effectiveness of these techniques. This technique has been proved effective only if the tamper was initially compressed at a lower quality than the rest of the image; on the contrary, when the compression is stronger in the latter stage, the traces of the first compression are probably damaged and the detection fail.

This behavior is common in most forensic techniques based on the analysis of multiple compression chains: stronger compression in later stages ruins the traces of previous compression stages, making the tools ineffective. The analyst, when using these tools, should take into account the reliability of the results based on the coding characteristics of the investigated image \cite{26}.

C. Editing Traces

Image editing modifies the visual information of the image and the scene depicted, introducing traces in several domains of the image such as pixel, geometric, and physical. Editing traces are the most numerous, and can be split into subcategories (Fig. 3) according to these domains.

Image illumination inconsistencies (light source direction, cast and attached shadows) are powerful traces considering that it is hard to achieve a perfect illumination match when composing two images. The are two main approaches for illumination techniques: geometric and illuminant. The first are based on the geometric constraints of light, trying use scene elements as cues to determine if the arrangement of lights \cite{27} \cite{28} \cite{29} \cite{30} \cite{31} or shadows \cite{32} \cite{33} are plausible. Illuminant techniques exploit the color, intensity and temperature aspects of the illumination, and are able to detect if a region or object in the image was lighted by a different type of light \cite{34} \cite{35}.

Similarly, geometric relations within an image (e.g., object proportions, reflections) are determined by the projection of the 3D real scene onto the image plane. This process is commonly modelled through the pin hole camera model \cite{36}. Any deviation from this model can be exploited as evidence of tampering. Yao \cite{37} uses a perspective constrained method to compare the height ratio between two objects in an image. Without the knowledge of any prior camera parameter, it is possible to estimate the relative height of objects and eventually identify objects that have been inserted on the scene. An extension has been proposed by Iuliani et al. \cite{38} to apply the technique on images captured under general perspective conditions. Conotter \cite{39} describes a technique for detecting if a text on a sign or billboard has been digitally inserted on the image. The method looks if the text shape satisfies the expected geometric distortion due to the perspective projection of a planar surface. The authors show that, when the text is manipulated, it is unlikely to precisely satisfy this geometric mapping.

When an editing trace exposes evidence of forgery, we can expect to infer something about its nature (FD3): if an object has as shadow inconsistent with the scene, he was probably inserted; if the illuminant color is inconsistent, the object could have been either spliced or retouched.

Obtaining other specific information about the techniques involved in the tampering process (FD4) is a very challenging task. There are two main reasons for this. The development of a technique for detecting the use of a specific tampering process/tool may require a strong effort compared to its applicability in a narrow range. Secondly, proprietary algorithms have undisclosed details about their implementation, making hard to develop analytical models for their traces. A first step toward this kind of assessment have been proposed by Zheng et al. \cite{40} to identify the feather operation used to smooth the boundary of pasted objects.

IV. IMAGE COMPOSITION

The term “Image Composition” is used to encompass different fields such as Computational Photography, Image Processing, Image Synthesis, Computer Graphics and even Computer Vision. Recent works on all of these fields were surveyed to determine which ones could be used to aid in forgery. For this purpose, techniques that a forger could use to perform any form of operation were considered, from splicing to highly creative operations.

The techniques were classified in five general classes based on the type of forgery they could perform:

- **Object Transferring**: transferring an object or region from one image to another image, or even to the same image. This is the most common type of forgery, and encompasses both splicing and copy-and-paste operations. It is divided into Alpha Matting, Cut-Out, Gradient Domain, Structurally Changing, Inpainting, and Composition;
- **Object Insertion and Manipulation**: inserting synthetic objects into an image or manipulating an existing object to change its properties. It is divided into Object Insertion, Object Manipulation, and Hair;
**Lighting**: altering image aspects related to lights and lighting. It is divided into Global Reillumination, Object Reillumination, Intrinsic Images, Reflections, Shadows, and Lens Flare;

**Erasing**: removing an object or region from the image and concealing it. It is divided into Image Retargeting, and Inpainting;

**Image Enhancement and Tweaking**: this is the most general class of forgery, and is related to what is considered retouching on the forensics literature. It is divided into Filtering, Image Morphing, Style Transfer, Recoloring, Perspective Manipulation, and Restoration/Retouching.

It must be noted that this classification considers forgery from the point of view of both Image Composition and Forensics. A composition technique that can be used to transfer an object from one image to the other can also transfer it to the same image. While those are distinct forgeries (and problems) from the forensics point of view, they can be performed by the same technique. Furthermore, some of the surveyed techniques could be used to perform more than one type of forgery in the classification. Erasing, for instance, is often performed by copy-pasting regions of the image to conceal an object. In this sense, a technique under the Object Transfering classification can be also considered on the Erasing class.

In this Section, we discuss each of the different forgery classes and their relation to the forensic traces and techniques. Most information about the effect of composition on forensic traces comes from performed tests (see Section V).

### A. Object Transferring

This class contains techniques that can be used with an end goal of transferring objects between images or in the same image. A fundamental task of transferring an object or region is defining its boundaries, and that can help on making good contours are classified as Cut-out [44][45]. These techniques do not change the content from the source or target images, they only aid in selecting a pixel area.

Most techniques to detect splicing or copy-and-paste are well-suited against Cut-out forgeries, because the pixel content is unaltered. From a forensics point of view, well-defined boundaries on the transferred region reduce the amount of information being carried from the original image. This might alter some traces and affect the performance of techniques based on those traces [46]. A bad cut can also be easy to note visually, without the use of additional tools.

One of the main limitation of transferring objects by cut-and-paste is that transparency is ignored. Hair, thin fabrics, glass, and edges may contain a mix of colors from the foreground and background of the source image. This can cause visual artifacts on the resulting composition, and the presence of foreign colors that can be used for traces. Alpha Matting techniques can estimate the transparency of a region in the image, which can be used to better extract it from the source image, and then composite on the target image (Fig. 3e-h). The visual aspect is the most critical on the use of alpha matting for object transferring, as it blends colors on borders and transparent regions, making convincing forgeries. In our tests, there was almost no difference between detecting Alpha Matting or regular cut-out.

The most sophisticated object transferring techniques are Gradient Domain ones. These techniques aim to combine the gradient of the transferred object with the target image, making a complex blend. The simplest technique is Poisson Image Editing [5], which matches the gradients by solving a Poisson equation from the boundaries of the transferred region. The resulting object has different colors and gradient, blending with the scene. Poisson Image Editing, also commonly referred to as Seamless Cloning, spawned several works that improved on its basic idea of solving differential equations for gradient matching on transferred regions [44][45][46][47][48].

Most of the Gradient Domain techniques use Laplacian Pyramids to manipulate the different image frequencies. Works such as Sunkavalli’s [49], however, focus on the Laplacian Pyramid as the main component for sophisticated blends between images, being able to maintain the noise and texture of the target image (Figures 3c through 3h) to some degree. This kind of approach was generalized [50] and improved [51] by other authors.

Gradient Domain techniques can be the most “dangerous” for object transferring, from a forensics point of view. They can blend the whole transferred area and merge the images on a profound level. There are big variations on the inner workings of each technique, and the results are very dependent on the images to be combined. This means that it is hard to evaluate them from a forensics point of view. A more specific and thorough study is required to determine the exact effect of compositing images on the Gradient Domain. In our tests they were easily identifiable using compression and noise traces, but these techniques have the potential to hide such traces if finely tuned. The safest way to detect forgeries of this kind would be focusing on high-level traces such as shadows and geometry. Light-based traces could help on cases where a full object is being transferred, because the resulting colors after the blending may create irregular lighting. When transferring parts of objects, such as changing faces on an existing head (Figure 3a), it is possible that the result can have plausible lighting and illuminant traces.

Object Transferring techniques are arguably the most relevant to the forensics community, because they can be used to perform both splicing and copy-pasting. Figure 3b shows an Alpha Matting (top row), and a Gradient Domain (bottom row) splicing. Both forgeries are visually unnoticeable. Notice how the alpha matte (Figure 3g) contains very precise information about the transparency of each hair, and the mixture of colors on the final composition (Figure 3h). The Gradient Domain composition exemplified does not use transparency information (Figure 3c), but is able to transfer some of the color and texture of the target image (Figure 3b) into the transferred region of the source region (Figure 3a). The final result (Figure 3d) is a very convincing composition.

### B. Object Insertion and Manipulation

Images are 2D projections of a 3D scene, with complex interactions of light and geometry. To insert a new object into
the image, or to manipulate existing objects, the properties of the 3D scene must be known. This is a very challenging task. Techniques under this category focus on estimating characteristics of the 3D scene or its objects, providing means to alter them on a visually convincing way.

Rendering a synthetic object into an image is a simple task if the scene lighting and camera parameters are known. Additional knowledge about scene geometry also helps to increase realism. For this reason, this is the focus of most object insertion techniques. The challenge is to obtain this information from a single image. The most advanced techniques for object insertion, developed by Karsch, are able to estimate perspective, scene geometry, light sources and even occlusion between objects. In [53] heavy user input was needed to aid the parameter estimation, whereas in a second work (Figure 1b) [7] most input tasks were replaced with computer vision techniques to infer scene parameters.

The manipulation of objects in an image suffers from similar problems than insertion. Scene lighting, camera parameters and geometry are required for a visually convincing composition, and the geometry of the object being modified must be also known. A slight advantage in relation to rendering synthetic objects is that the photographic texture of the modified object can be used, providing a more photo-realistic touch. It is possible to perform resizing operations on objects without directly dealing with its 3D geometry [54], but most techniques will focus on modeling it.

The easiest way to work with the geometry of objects in an image is to limit the scope to simple primitives. Zheng [55] focus on cube-like objects, modeling them through “cuboid proxies”, which allow for interactive transformations such as scale, rotation, and translation in real time. Chen’s work [56] uses user input to model an objects geometry through swipe operations. This technique works specially well on objects that have some kind of symmetry, such as a candelabrum or a vase, and allows changes in the geometry itself. Another solution for dealing with object geometry is to use a database of 3D models, and find one that fits with the object depicted in the image [57].

Manipulating human body parts in images is a specially hard task, because human bodies vary greatly in shape, and clothes affect the geometry. This type of manipulation, however, is of special interest due to its applications in marketing photography and modeling. Zhou [58] uses a parametric model of the human body, and fits a photography to a warped 3D model, achieving a correspondence between body parts in the image and 3D geometry. This allows the reshaping of body parts, making a person in a picture look thinner, stronger, taller, etc. Hair manipulation is also a hot topic in image composition, with a special focus on changing hair styles after the picture has been taken [59][60][61].

Even though state-of-the-art techniques in image insertion and manipulation can create visually convincing results, they should not pose a problem for modern forensic techniques.
Distinguishing between real and synthetic images is a very debated topic \[62\][63][64], and there are forensic techniques that focus on identifying them \[65\][66].

The weak point for this category of image composition is in the acquisition traces. The process of rendering a synthetic object is different from capturing it from a camera, so the acquisition traces should point to the manipulation, providing FD1 or FD2 results. Similarly, when performing transformations on an object (scaling, rotating, deforming, etc.), its pixels have to be resampled, changing the acquisition traces. Resampling detection also could be used to obtain an FD3 result in these cases, while compression-based techniques could identify this type of manipulation if the original image was compressed. Kee has demonstrated that object insertion might be able to fool geometry-based lighting techniques [33], which could also extend to object manipulation. The reason for this is that the same lighting parameters estimated to verify the integrity of the scene were used to generate the composition.

C. Erasing

An erasing manipulation is when an element of the image is intentionally removed or hidden, and not a consequence of other editing. This category is comprised mostly of Inpainting and Image Retargeting techniques.

Inpainting techniques are used to complete a region in an image, filling it with appropriate content \[67\]. By selecting a region that one wants erased as the region to be completed, inpainting can make objects disappear. Several works on inpainting are focused on stitching different parts of the image together \[68\][69], or filling large gaps \[70\]. There are implementations of inpainting techniques already available on commercial editing software, such as Photoshop’s Spot Healing Brush and Content Aware Fill tools. The main limitation of inpainting is filling regions with high amount of details, or using image features which are not local in the filling.

Huang’s \[71\] work is capable of identifying global planar structures in the image, and uses “mid-level structural cues” to help the composition process.

Image retargeting is a form of content-aware image resizing. It allows to rescale some elements in an image and not others, by carving seams in the image, i.e. removing non-aligned lines or columns of pixels \[72\]. The seams usually follow an energy minimization, removing regions of “low-energy” from the image. The objects and regions that have seams removed will shrink, while the rest of the image will be preserved. This can be used to remove regions of the image by forcing the seams to pass through certain places instead of strictly following the energy minimization. Most research on image retargeting focus on better identifying regions in the image to be preserved, and choosing the optimal seam paths \[73\][74].

Erasing manipulations should behave in a similar fashion to object insertion and manipulation, as the modified region will not come from a photograph, but from an estimation. This affects acquisition and compression traces, provided the original images were compressed. Image retargeting has already been analyzed from the point of view of image anonymization \[75\], and there is even a specific technique for its detection \[76\]. Detecting that a seam carving has been done in an image would constitute and FD4 in our scale.

D. Lighting

Lighting techniques are capable of changing the lighting of a scene \[77\] and objects \[78\][79], inserting light effects such as reflections \[80\][81], lens flare \[82\][83], and even manipulating shadows \[84\][85][86]. From a forensics point of view, lighting techniques are dangerous due to their potential of concealing other forgeries. After splicing an object in an image, for instance, a forger could add convincing shadows and change its lighting, making it harder for both human analysts and forensic techniques to detect it. Indeed, it is a concern in image composition when the source and target lighting conditions are different, and there are works focused on correcting this issue \[87\][88].

Due to the variety of lighting techniques, it is hard to make a general statement about them from a forensics point of view. As always, it seems plausible that at least an FD2 result can be achieved if compression is involved in the forgery. Techniques that add shadows or change the lighting in a visually convincing way, but do not account for all lighting parameters of the scene, could fail to deceive geometry and light-based forensics analysis. Specifically identifying light inconsistencies is an FD3 in our scale.

E. Image Enhancement/Tweaking

This is a broad classification for techniques that perform image modifications and are too specific to have their own category. Image morphing techniques \[9\][89] can fuse objects together, creating a composite that is a combination of them. Style transfer techniques are able to transform an image to match the style of another image \[90\], a high-level description of a style \[91\], or an image collection \[92][93]. In the same vein, recoloring techniques can add or change the color of image elements \[94\], and even simulate a different photographic process \[95\].

Filtering techniques can be very flexible, allowing for a wide variety of effects. They can be used to remove noise or detail from images (Figure 14) \[96][97][98][99], or even to add detail \[8\] while preserving edges. Different filters may be designed to obtain different effects. From a forensics point of view, filtering techniques can be used to remove low-level traces. A simple median or gaussian filter is able to remove compression and CFA traces, but it is easily detectable, as it softens edges. Edge-aware filtering, however, can be used to destroy such traces preserving edges. If used in a careful way, it can remove the aforementioned traces in a visually imperceptible way.

Perspective manipulation techniques allow an user to change the geometry \[98\], and perspective \[99\] of a scene, or to recapture an image from a different view point \[100\]. Its uses are mostly artistic and aesthetic, but these techniques could be used to forge photographic evidence. The final type of manipulation that will be discussed is Retouching. Retouching techniques aim to perform adjusts on image properties such as white balance \[101][102\], focus \[103\], or several at the same
time [103]. They can also aid in performing adjustments in several images at the same time [105].

V. TESTING AND RESULTS

To understand how Image Composition techniques affect forensics traces, we gathered images from several works and performed a forensics analysis (Table II). The images used were either obtained from the publication website or directly from the authors. Our main goal was to analyze the images directly before and after the techniques have been applied, to understand how the traces are affected by it.

The images obtained have varying amounts of preprocessing and compression. This influences the quality of the analysis, making it harder to evaluate all cases with the same standards. Obtaining all the implementation for the techniques and generating controlled test cases could solve this problem, but it is not feasible on an analysis of this scale.

As discussed in Section III, there are several techniques based on each trace. Each technique has a different level of success and scope. For this reason, our analysis is on a higher level. We discuss the plausibility of four different traces being used to detect a composition technique, rather than the performance of each particular forensic technique. In particular, a N/A result means there were no images for that technique that could be tested for that trace. An example of this would be compression traces when all available images were uncompressed. An Indecisive result means that the tests were inconclusive for that trace. This is probably due to some form of pre-existing processing or compression that made it impossible to evaluate the images for a particular trace. A Plausible result means that there are indications of editing or clear differences between the image before and after the composition technique was used, but it is not clearly identifiable. An Identifiable result means it is possible to identify that some form of editing has occurred using that trace. A Non-Identifiable result indicates that trace is not suitable for detecting that particular composition technique.

The CFA analysis was done using the technique from [17], which tries to measure the presence of demosaicing artifacts at a local level onto the image. It is a fragile trace, as almost any modification can destroy it. This means that it can be really useful to decide if an image is not native (FD1) or where it has been tampered (FD2) when the image is expected to be pristine. Since the modification history of our images was unknown, some test cases were inconclusive because the demosaicing pattern had already been disrupted.

Unfortunately no information about source device were available for any of the provided images. This limits the the type of analysis that can be done, for instance using PRNU-based analysis [18] to localize forgeries. Since the PRNU is a prominent trace used in the literature, we designed an experiment to test it. First, we captured a set of uncompressed images with a Canon 5D to be able to estimate the noise pattern. We were able to create compositions with the images using Alpha Matting [52] and Edge-Aware Filtering [8], both of which the implementation was easily available. In both cases, the PRNU analysis was able to identify the forgeries.

In Fig. 5c we report an example to show its effectiveness on localized recoloring. The blue region, representing a portion in which the pattern noise is uncorrelated with the one estimated by the camera, clearly localize the tampering.

Error Level Analysis (ELA) estimates the local compression error for each JPEG block. This is a very low-level trace that is common on forensics analysis tools, but requires a great deal of interpretation and can be misleading [111]. It is, however, an interesting analysis tool for our testing purposes. It allows us to compare differences in compression for images before and after the composition techniques were applied, rather than measuring a specific trace. In our tests (Table II), several techniques obtained a “plausible” result, which indicates that compression traces could be used to detect them. In Fig. 5a ELA is not able to identify any irregularity in the composed image while, in both 5b and 5c the forgery introduces distinct noise artefacts.

To evaluate double JPEG compression the technique from [112] was used. The results are more straight-forward to analyze than ELA, but its scope is more limited. It is specially useful if a foreign region is inserted in an image (object transfer/insertion). Reillumination (Fig. 5e) and seamless cloning (Fig. 5f) were easily identified in our tests, and our evidence indicates that the same could apply to Alpha Matting.

Noise analysis is very simple and subjective, but can be very powerful. A median filter is applied on the image, and the result is subtracted from the original one. The result is then scaled according to the local luminance, and the noise pattern is obtained. In essence, we are observing a combination of sensor noise, illumination noise, compression noise, and high frequencies. In natural images, the noise tends to behave similarly in almost all of the image. When a region has a distinct noise pattern (Figs. 5b and 4b), or strange artifacts appear (Fig. 5c), it can be a strong indicator of forgery.
The majority of tested composition types had at least one identifiable trace. This means that forgeries done using these techniques would probably be identified with a careful analysis. In some cases, there is also the possibility of developing a specific technique to detect them.

VI. CONCLUSION

In this work we surveyed both the fields of Image Composition and Digital Image Forensics, crossing them directly. A new classification scheme for techniques in both fields, along with a forgery detection scale were presented to help organize the discussion. This scale provides a more sophisticated way to compare the existing works on the literature, and assess the capabilities of forensic techniques. To understand the forensic aspect of composition techniques, their inner workings were studied and tests were performed for a wide variety of image effects. As a result, we uncovered that current state-of-the-art forensics has all the basic tools it needs to be able to detect most forgeries, provided that they are properly tuned for each specific case, and maybe even combined.

This work is an overview of both fields, and can be used either as an introductory reading, or as summary of the current challenges. In this sense, we provide groundwork for the development of novel forensic techniques against image composition. A natural extension for this work would be to increase the number of techniques surveyed and tested, considering other traces and forensic approaches. Since both fields are in an “eternal arms race” the list of available works to consider other traces and forensic approaches. Since both fields are in an “eternal arms race” the list of available works to consider other traces and forensic approaches.

ACKNOWLEDGMENT

The authors are partially supported by GNSAGA of INdAM, CAPES and CNPQ (grants 200960/2015-6/SWE and 306196/2014-0). We also thank all the authors that provided us with images and material to perform our tests.

REFERENCES

[1] V. Schettine, M. M. Oliveira, R. da Silva, and T. J. Carvalho, “Humans are easily fooled by digital images,” CoRR, vol. abs/1509.05301, 2015. [Online]. Available: http://arxiv.org/abs/1509.05301
[2] A. Systems, “Adobe photoshop.” [Online]. Available: http://adobe.com/photoshop
[3] P. M. Spencer Kimball, “Gnu image manipulation program.” [Online]. Available: www.gimp.org
[4] H. Farid, “A survey of image forgery detection,” IEEE Signal Processing Magazine, vol. 26(2), pp. 16–25, 2009.
[5] F. Perez, M. Gangnet, and A. Blake, “Poisson image editing,” ACM Trans. Graph., vol. 22, no. 3, pp. 313–318, Jul. 2003. [Online]. Available: http://doi.acm.org/10.1145/882262.882269
[6] M. Gryka, M. Terry, and G. T. Brostow, “Learning to remove soft shadows,” ACM Transactions on Graphics, 2015.
[7] K. Karsch, K. Sunkavalli, S. Hadap, N. Cair, H. Jin, R. Fonte, M. Sittig, and D. Forsyth, “Automatic scene inference for 3d object compositing,” ACM Trans. Graph., vol. 33, no. 3, June 2014.
[8] E. S. L. Gastal and M. M. Oliveira, “High-order recursive filtering of non-uniformly sampled signals for image and video processing,” Computer Graphics Forum, vol. 34, no. 2, pp. 81–93, May 2015, proceedings of Eurographics 2015.
[9] J. Liao, R. S. Lima, D. Nehab, H. Hoppe, P. V. Sander, and J. Yu, “Automating image morphing using structural similarity on a halfway domain,” ACM Trans. Graph., vol. 33, no. 5, pp. 168:1–168:12, Sep. 2014. [Online]. Available: http://doi.acm.org/10.1145/2629494.
[10] S. Xue, A. Agarwala, J. Dorsey, and H. Rushmeier, “Understanding and improving the realism of image composites,” ACM Transactions on Graphics, vol. 31, no. 84, pp. 84:1–84:10, 07/2010 2012. [Online]. Available: http://doi.acm.org/10.1145/1835520.2185580.
[11] A. Rocha, W. Scheirer, T. Boult, and S. Goldenstein, “Vision of the unseen: Current trends and challenges in digital image and video forensics,” ACM Comput. Surv., vol. 43, no. 4, pp. 26:1–26:42, Oct. 2011. [Online]. Available: http://doi.acm.org/10.1145/1978802.1978805.
[12] A. Piva, “An overview on image forensics,” ISRN Signal Processing, vol. 2013, pp. 1–22, 2013.
[13] Z. Dias, A. Rocha, and S. Goldenstein, “Image phylogeny by minimal spanning trees,” Information Forensics and Security, IEEE Transactions on, vol. 7, no. 2, pp. 774–788, 2012.
[14] T. Carvalho, C. Riess, E. Angelopoulou, H. Pedrini, and A. de Rezende Rocha, “Exposing digital image forgeries by illumination color classification,” IEEE Transactions on Information Forensics and Security, pp. 1182–1194, 2013.
[15] F. Kec, M. Johnson, and H. Farid, “Digital image authentication from jpeg headers,” Information Forensics and Security, IEEE Transactions on, vol. 6, no. 3, pp. 1066–1075, Sept 2011.
[16] J. Lukas, J. Fridrich, and M. Goljan, “Digital camera identification from sensor pattern noise,” Information Forensics and Security, IEEE Transactions on, vol. 1, no. 2, pp. 203–214, June 2006.
[17] F. Ferrara, T. Bianchi, A. De Rosa, and A. Piva, “Image forgery localization via fine-grained analysis of cfa artifacts,” Information Forensics and Security, IEEE Transactions on, vol. 7, no. 5, pp. 1566–1577, Oct 2012.
[18] M. Chen, J. Fridrich, M. Goljan, and J. Lukas, “Determining image origin and integrity using sensor noise,” Information Forensics and Security, IEEE Transactions on, vol. 3, no. 7, pp. 74–90, March 2008.
[19] C. Hass, “Jpegsnoop.” [Online]. Available: http://www.impulseadventure.com/photo/jpeg-snoop.html.
[20] Z. Fan and R. de Queiroz, “Identification of bitmap compression history: Jpeg detection and quantizer estimation,” Image Processing, IEEE Transactions on, vol. 12, no. 2, pp. 230–235, Feb 2003.
[21] W. Luo, J. Huang, and G. Qi, “Jpeg error analysis and its applications to digital image forensics,” Information Forensics and Security, IEEE Transactions on, vol. 5, no. 3, pp. 480–491, Sept 2010.
[22] B. Li, T.-T. Ng, X. Li, S. Tan, and J. Huang, “Revealing the trace of high-quality jpeg compression through quantization noise analysis,”

| Composition Technique | Images Tested | CFA | Double Jpeg | ELA | Noise |
|-----------------------|---------------|-----|-------------|-----|-------|
| Soft Shadow Removal [6] | 5             | N/A | Indecisive | Non-Identifiable | Identifiable |
| Dehazing [46]         | 9             | Plausible | N/A | Indecisive | Identifiable |
| Object Insertion [107] | 9             | Indecisive | Non-Identifiable | Identifiable | Identifiable |
| Reillumination [10]   | 11            | N/A | Identifiable | Plausible | Plausible |
| 3D Object Manipulation [108] | 3 | Plausible | Indecisive | Non-Identifiable | Non-Identifiable |
| Image Morphing [109]  | 12            | Plausible | Plausible | Plausible | Identifiable |
| Alpha Matting [52][110]| 9             | Identifiable | Plausible | Plausible | Non-Identifiable |
| Seamless Cloning [49][45][47] | 16 | Plausible | Identifiable | Plausible | Identifiable |
Fig. 5: Results of analyzing different traces for the images on Figure 1. a) ELA of Soft Shadow Removal. In this case, it is not possible to identify any irregularity in the composited image. b) Noise analysis of object insertion. The first identifiable irregularity is that the noise pattern for the shadow cast by the synthetic object greatly differs from other shadowed regions in the image (red arrows). The indirect illumination estimated after the scene’s light interactions with the object appear as salient planes in the noise map (orange arrows). c) PRNU analysis of localized recoloring. The more yellow, higher is the correlation between the region and the cameras sensor pattern noise. On the first image, there are some false positives thorough the image caused by high frequency areas. On the recolored image, the probability map shifts completely to the altered region. d-f) Noise analysis of image morphing. The morphing process creates distinct warping artifacts on the noise pattern. g) Double JPEG compression analysis of reillumination. The more yellow, higher the probability that the region has undergone double JPEG compression. While the top image shows a very noisy pattern, in the bottom image the uniform interpretation of a salient portion suggest that different compression traces (single and double) are present in the image.

[23] T. Bianchi and A. Piva, “Image forgery localization via block-grained analysis of jpeg artifacts,” Information Forensics and Security, IEEE Transactions on, vol. 7, no. 3, pp. 1003–1017, June 2012.
[24] J. Yang, J. Xie, G. Zhu, S. Kwong, and Y.-Q. Shi, “An effective method for detecting double jpeg compression with the same quantization matrix,” Information Forensics and Security, IEEE Transactions on, vol. 9, no. 11, pp. 1933–1942, Nov 2014.
[25] H. Farid, “Exposing digital forgeries from jpeg ghosts,” Information Forensics and Security, IEEE Transactions on, vol. 4, no. 1, pp. 154–160, March 2009.
[26] P. Ferrara, M. Fontani, T. Bianchi, A. De Rosa, A. Piva, and M. Barni, “Unsupervised fusion for forgery localization exploiting background information,” in Multimedia Expo Workshops (ICMEW), 2015 IEEE International Conference on, June 2015, pp. 1–6.
[27] E. Kee and H. Farid, “Exposing digital forgeries from 3-d lighting environments,” IEEE International Workshop on Information Forensics and Security, 2010.
[28] P. Saboia, T. Carvalho, and A. Rocha, “Eye specular highlights tell-tales for digital forensics: A machine learning approach,” in Image Processing (ICIP), 2011 18th IEEE International Conference on, sept. 2011, pp. 1937 –1940.
[29] E. Kee and H. Farid, “Detecting photographic composites of famous people,” Dartmouth College, Tech. Rep., 2009.
[30] M. Johnson and H. Farid, “Exposing digital forgeries in complex lighting environments,” Information Forensics and Security, IEEE Transactions on, vol. 2, no. 3, pp. 450 –461, sept. 2007.
[31] T. Carvalho, H. Farid, and E. Kee, “Exposing photo manipulation from user-guided 3d lighting analysis,” in IS&T/SPIE Electronic Imaging, vol. 9409, 2015, pp. 940902–940902–10.
[32] E. Kee, J. F. O’Brien, and H. Farid, “Exposing photo manipulation with inconsistent shadows,” ACM Trans. Graph., vol. 32, no. 3, pp. 28:1–28:12, Jul. 2013. [Online]. Available: http://doi.acm.org/10.1145/2487228.2488236
[33] E. Kee, J. F. O’Brien, and H. Farid, “Exposing photo manipulation
