Digital Signal Processing 71 (2017) 1–26

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

Digital image integrity – a survey of protection and verification techniques

Paweł Korus

Department of Telecommunications, AGH University of Science and Technology, al. Mickiewicza 30, 30-059 Kraków, Poland

ARTICLE INFO

Article history:
Available online 1 September 2017

Keywords:
Content authentication
Digital image forensics
Forgery detection
Tampering localization
Digital watermarking

ABSTRACT

We are currently on a verge of a revolution in digital photography. Developments in computational imaging and adoption of artificial intelligence have spawned new editing techniques that give impressive results in astonishingly short time-frames. The advent of multi-sensor and multi-lens cameras will further challenge many existing integrity verification techniques. As a result, it will be necessary to re-evaluate our notion of image authenticity and look for new techniques that could work efficiently in this new reality. The goal of this paper is to thoroughly review existing techniques for protection and verification of digital image integrity. In contrast to other recent surveys, the discussion covers the most important developments both in active protection and in passive forensic analysis techniques. Existing approaches are analyzed with respect to their capabilities, fundamental limitations, and prospective attack vectors. Whenever possible, the discussion is supplemented with real operation examples and a list of available implementations. Finally, the paper reviews resources available in the research community, including public data-sets and commercial or open-source software. The paper concludes by discussing relevant developments in computational imaging and highlighting future challenges and open research problems.

1. Introduction

Increasing ease of editing digital images has important implications for our trust in photography. Preparing convincing forgeries is within reach of mainstream consumers, and new image editing technologies harness state-of-the-art developments in artificial intelligence to further improve the quality and photorealism of photo manipulations. Some of the most noteworthy recent developments include fully (or nearly) automatic techniques for: (a) beautifying faces with *Adobe Sensei* [1]; (b) changing facial expression or age with *FaceApp* [2]; (c) replacing skies and matching scene lighting with *Adobe Sky Replace* [3]; (d) changing visual style of photographs by example (e.g., for weather or time-of-day hallucination) with *Deep Photo Style Transfer* [4]. Many of these techniques are not only available as easy-to-use 3rd party applications, but also as default mechanisms in our smart devices (e.g., see face beautification features in Huawei or Xiaomi smart-phones [5]). Given that humans are unreliable in identifying fake images [6], automatic & accurate forgery detection schemes are of critical importance in a number of applications.

Researchers in academia and industry have devised four general approaches to image authentication: (a) *digital signatures*; (b) *authentication watermarks*; (c) *forensic analysis*; (d) *phylogeny reconstruction*. Digital image signatures rely on standard cryptographic primitives and should to be computed upon image acquisition, ideally by a digital camera itself [7,8]. The signatures are typically attached to the image as meta-data and allow for verifying authenticity of a binary image representation. Such an approach lacks flexibility as the bit-stream is highly fragile and changes when the image is converted to a different format during subsequent transmission or storage. This problem is addressed by *robust hash functions*, which aim to be sensitive to important semantic changes in the content, while remaining robust to unintentional, global post-processing like brightness adjustments or lossy compression [9].

In contrast to the easily removable meta-data-located signatures, *authentication watermarks* are irreversibly embedded in the image by means of carefully designed, imperceptible changes in the image content. A dedicated decoder analyzes consistency of the watermark, and verifies the integrity of the investigated image or its individual regions. Authentication watermarks deliver advanced features like *precise localization* of a forgery [9] or even *approximate restoration* of the original appearance [10] – both based solely on the visual content of a potentially doctored image.

The main limitation of the above techniques, collectively known as *active protection* techniques, consists in the necessity to pro-

E-mail address: pkorus@agh.edu.pl.
URL: http://kt.agh.edu.pl/~korus/.

http://dx.doi.org/10.1016/j.dsp.2017.08.009
1051-2004/

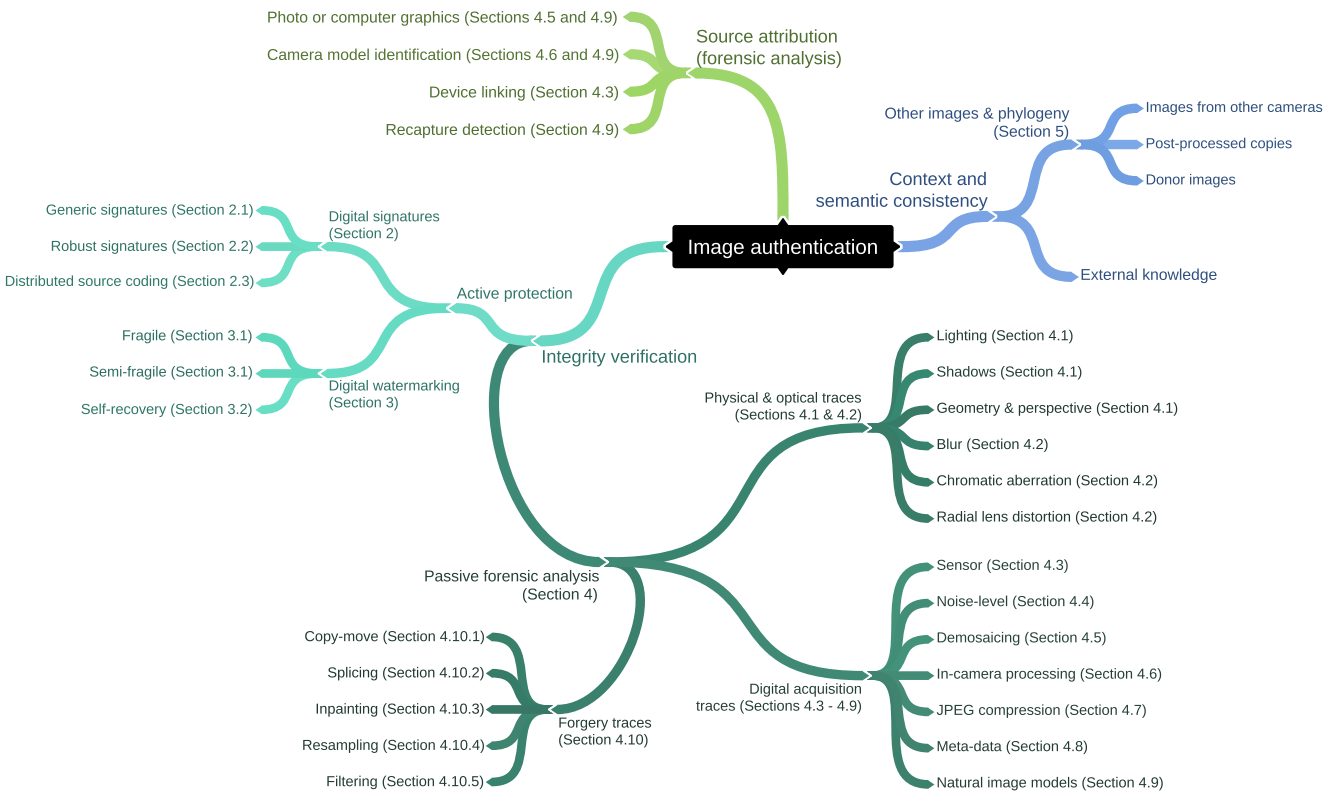

Fig. 1. General taxonomy of image authentication and integrity verification problems and the corresponding structure of this survey; the broader problem of image authentication encompasses not only integrity verification, but also source attribution and context verification, including external knowledge that is currently difficult to capture automatically, e.g., witness testimony, coherence with the laws of physics, consistency of weather conditions withe the alleged time of capture, etc.

tect the images upon their acquisition by a secure camera [11] or registration in a media repository. Such an approach is not feasible in many applications, and is best suited for strict document work-flows. In general, such side information is not available and image authentication can only be performed with *passive forensic analysis*. As a result, in the recent years we have witnessed a massive shift of interests towards passive techniques from both the research community and prospective end users.

Despite the of variety of existing techniques, the field of digital image forensics has yet to deliver fully automatic and reliable tampering detection and localization schemes. Even the most mature techniques work only in limited conditions, and remain vulnerable to relatively simple malicious attacks, referred to as *anti-forensics*. A recent evaluation of state-of-the-art methods on uncontrolled images harvested from the Internet has demonstrated their poor performance and unpredictable behavior when dealing with random images with unknown origin and processing history [12]. In such conditions, the trend seems to proceed towards *image phylogeny* which aims to identify various versions of a given image within a large photo collection (e.g., available online) and to reconstruct their mutual relationships and processing history.

DARPA has recently launched the *MediFor* program in order to advance the development of media forensics and image phylogeny techniques [13]. One of the program's goals is to prepare a large realistic test corpus and organize a series of image forensics challenges. Early results from the most recent 2017 edition [14] seem to corroborate the above findings that existing forensic detectors perform poorly outside of laboratory conditions [15].

1.1. Paper scope, goal & organization

The goal of this paper is to provide a thorough survey of the most important developments in the field of *digital image authentication* with emphasis on *image integrity* protection and verification techniques. The distinction between image authenticity and integrity is not always clear is scientific communication, and bears particular importance in legal proceedings, as exemplified by the recommendations of the Scientific Working Group Imaging Technology (SWGIT) [16] which used to be tasked with drafting recommendations for law enforcement agencies.

Image integrity involves ensuring that the content represented by the image is the same as at the time of its acquisition. *Image authenticity* is a more general term which refers to the truthfulness of the presented scene in a broader context. Hence, authenticity takes into account the possibility of using an unaltered image in an incorrect context (e.g., taken in a different moment in time) or staging the photographed scene. As a result, authentication will encompass not only content integrity verification, but also source attribution, and context verification. Source attribution addresses problems of confirming the origin of the investigated images, and includes aspects like: (a) confirmation that a given photograph was taken with a specific camera; (b) confirmation that the image is a photograph and not a photo-realistic computer graphic image; (c) detection whether the investigated photograph is re-captured from a print-out or a computer screen. Context verification may include analysis of similar images from social media or other photographers, as well as integration of external sources of knowledge, e.g., consistency of weather with the alleged time of capture. The discussed taxonomy is shown in Fig. 1. For the sake of consistency, in this paper I follow the usual convention in the research community and use the terms *image integrity* and *image authenticity* interchangeably. The intended meaning will be clear from the context.

In contrast to recent surveys of image forensics [17–20], I will address both active and passive approaches to image authentication. My aim is not to review all reported variations of possible analysis techniques. Instead, I analyze and compare state-of-the-art

approaches with respect to: (a) analysis capabilities; (b) fundamental limitations; (c) documented vulnerabilities; (d) maturity and availability of software tools. The paper draws on my experience in designing and implementing both active and passive image authentication schemes.

Compared to previous surveys, this paper is structured differently. Discussion of each authentication approach covers all relevant aspects starting from analysis capabilities up to documented attack vectors. For the sake of presentation clarity, longer descriptions are divided into separate sub-sections. Selected techniques are illustrated with operation examples. I generated all of the figures by myself using either my own or publicly available implementations. Tampering examples come from a recent dataset with realistic forgeries [21]. The dataset includes uncompressed and non-resized images from various cameras which allows to demonstrate the behavior of many acquisition traces.

Whenever possible, the discussion covers available software tools, be it commercial or academic. I believe such a survey gives a clear picture of the maturity, applicability and reliability of specific protection/verification schemes. I also believe that such a survey is of particular interest now, when we are on a verge of a revolution in imaging technology. The emerging multi-sensor and multi-lens cameras will render many existing traces useless, and will require another look at our approach to image authentication.

The remaining part of this paper is organized as follows (see Fig. 1 for a compact visualization of the problem taxonomy and the corresponding paper structure). First, I discuss active protection techniques based on digital signatures (Section 2) and authentication watermarking (Section 3). Then, I introduce a model of the image acquisition pipeline, and review various traces that can be used for blind forensic analysis (Section 4). Image phylogeny techniques are presented in Section 5. In Section 6, I briefly describe some recently proposed alternative approaches to image authentication that do not directly fall into any of the discussed classes. In Section 7, I review resources available in the research community, including publicly available datasets and software tools. I conclude and discuss open problems and future research perspectives in Section 8.

2. Signature-based verification techniques

This section discusses techniques based on generic cryptographic signatures (Section 2.1), robust image signatures (Section 2.2) and more advanced signatures based on distributed source coding (Section 2.3). In all of these techniques, the signature is separated from the image content. It is either stored as easily-removable meta-data, or delivered on demand during online content authentication.

2.1. Generic cryptographic signatures

2.1.1. General information & analysis capabilities

The most straightforward and the least flexible approach to digital image authentication involves standard digital signatures, i.e., signed cryptographic hashes of the image content [22]. Raw pixel values (and optionally image meta-data) are fed to a hashing function, such as the functions from the secure hash algorithms (SHA) family, and the hash is subsequently encrypted with a private key of an asymmetric cipher. The resulting signature is commonly stored as an additional field in the meta-data. Upon verification, this approach yields a binary decision regarding image authenticity.

2.1.2. Limitations

Due to the nature of generic hash functions, such an approach is sensitive to any changes of the pixels' values. In many practical work-flows this is undesirable since the binary image representation is likely to change as the image is stored or transmitted by different actors. When lossy compression formats are employed, even subsequent re-saving with the same compression settings will most likely alter the bit-stream and invalidate the signature. In addition, it may be desirable to allow for certain global post-processing, e.g., minor brightness or contrast adjustments, that does not affect the semantic content of the image. Finally, generic signatures deliver only a single binary decision. It is impossible to infer anything about the processing history of a processed image. A number of techniques addressing the above issues are discussed in Sections 2.2 and 2.3.

2.1.3. Available software

The above protection technique relies on standard cryptographic primitives which are implemented in a variety of libraries, including the open source *OpenSSL* [23]. Complete image authentication systems have been deployed as commercial products and integrated with their cameras by most important manufacturers like Nikon [7], or Canon [8]. Selected cameras can be supplemented with additional software which attaches signatures upon photo acquisition. Digital signatures are also used for image authentication in Tetra mobile terminals produced by Motorola for law enforcement agencies [24]. A recently developed smart-phone application *Photo Proof* [25] allows to protect digital photographs by including their signatures in the Bitcoin Blockchain. However, the details of the method are not publicly available.

2.1.4. Known vulnerabilities & attacks

Image authentication systems developed by Canon and Nikon have been cracked by Elcomsoft, an IT security company, in 2010 and 2011, respectively [26,27]. In both cases, the vulnerability involved extraction of authentication keys from the camera, which allowed the attackers to generate fake images that pass verification. To the best of my knowledge, the vulnerability has not been addressed and the image authentication products have been retracted.

2.2. Robust image signatures

2.2.1. General information & analysis capabilities

Adoption of robust image signatures often follows the same general approach as for the generic ones: a hash of image content is encrypted with a private key of an asymmetric crypto-system. In this case however, the hash function is robust to non-invasive post-processing that retains the same semantic content. Hence, such techniques are better suited to practical work-flows, where images may be re-compressed by service providers (e.g., social networks, or photo galleries) without notice.

Robust hash functions are typically computed from perceptually significant components in a certain content representation. Hence, important semantic changes, or an excessive intensity of an allowed operation will trigger an alarm. Allowed post-processing typically includes operations like lossy compression, resizing, and brightness or contrast adjustments. The hash may also be computed in a block-wise manner, which enables *tampering localization*. Validity of the signature is then checked for individual image regions, which allows to indicate areas affected by a forgery. In a recent work by Yan and Pun [28] the hash contains two separate parts for global and local editing. The global hash allows to recover from geometric transformations like rotation or scaling. The local hash allows to detect local image editing.

Robust signatures are often used in combination with semi-fragile watermarking, which involves carefully tailored modifications of the image content. These imperceptible changes enforce certain properties that are retained by allowed and destroyed by

forbidden post-processing. The reader is referred to Section 3.1 for more information.

2.2.2. Protection techniques

A variety of robust hash functions have been proposed including [29]: (a) simple statistical features (e.g., histogram or moments); (b) statistics of low-level image features (e.g., edges); (c) random projection and quantization of a coarse image representation (e.g., DCT, SVD); (d) robust relations between groups of coefficients; (e) matrix factorization [30]. The following description provides an overview of selected popular algorithms.

A popular technique by Lin and Chang [31] exploits invariance of inter-block relations between pairs of discrete cosine transform (DCT) coefficients. The hash is hence computed as a sequence of robust features for randomly chosen block pairs. After appending some auxiliary meta-data, the hash is encrypted with a standard asymmetric cipher. Another popular and thoroughly analyzed method has been proposed by Fridrich and Goljan [32]. It involves 1-bit quantization of multiple random projections of image block content. The resulting robust hash can be either used directly, or utilized to generate a spread-spectrum semi-fragile watermark. An improved approach involves exploitation of rotation invariance of the Fourier–Mellin transform and controlled randomization of the feature extraction process [33]. Information-theoretic analysis indicates that such an approach improves security, measured by means of differential entropy.

A robust content hash can also be obtained by means of matrix factorization, e.g., by means of singular value decomposition (SVD) or non-negative matrix factorization (NMF) [30]. The latter is preferable due to its non-negativity constraints which allow only for additive combinations of basis vectors leading to reduced misclassification rates. Moreover, geometric attacks manifest themselves as an approx. i.i.d. noise in the NMF domain which simplifies derivation of optimal decision rules. The algorithm proposed by Monga and Mihcak [30] operates by randomly selecting overlapping sub-images and constructing an auxiliary image from their NMF-based approximations. The hash is obtained from NFM factorization of the auxiliary image by mean of random projection. The authors performed a detailed theoretical analysis and experimental evaluation which confirm significant improvement of NMF over other factorization methods.

A novel hashing mechanism proposed by Yan and Pun [28] generates a two-part signature with both local and global hashes. The local hashes are computed by binarization of a coarse image representation obtained by low pass filtering of a quaternion image representation. The global hash is obtained from quaternion Fourier–Mellin moments, and hence allows to recover from geometric transformations like rotation and scaling. After alignment, local hashes are used for precise tampering localization. The method was designed to address an important trade-off between the hash length and localization resolution. The scheme performs multi-scale analysis of hash difference maps and fuses the results in order to improve localization performance. The fusion is performed by manifold ranking.

2.2.3. Limitations & known vulnerabilities

In practice, there is always a trade-off between the security and robustness of the hash. Our understanding of both of these aspects is still incomplete. While robust hash functions are typically designed to allow for mild post-processing, the notion of mildness often eludes specific definition. It remains challenging to deliver a scheme that could precisely distinguish between multiple allowed and disallowed types or strengths of processing. In many cases the hash is designed to tolerate only a small number of operations and the impact of others is not investigated at all. A good example is the one of lossy compression. If the hash follows a specific structure of one image format (e.g., the blocking structure of JPEG) it is unlikely to work well with another (e.g., wavelet-based JPEG2000, or prediction-based WebP). A possible approach to address this limitation involves a set-theoretic formulation [34].

Further work is also necessary to clarify security requirements – both for the hash function and for its practical deployments. Two popular approaches of measuring security involve differential entropy [33] and unicity distance [35]. The latter is essentially a measure of conditional entropy of the hashing key given the observable images and the corresponding hash values. Analysis of these parameters shows that it is possible to estimate the key with high accuracy if it is reused several dozen times. Hence, in practical deployments an appropriate key rotation policy should be established.

Note that some robust hash functions were intended not for authentication but for image search applications. Although they share some of the design principles, e.g., invariance to common post-processing, they are not designed with security in mind and may be a poor choice for image authentication systems. Their adoption should be subject to careful consideration. One common property that robust hash functions should possess in security applications is controlled randomness of the hash. Otherwise, an attacker could easily adapt the image content and cause a collision [29].

2.2.4. Available software

Robust image hashing is often combined with digital watermarking. While there are companies with relevant expertise, such products are often not advertised in the official product portfolio which currently focuses on more mainstream applications of copy control and piracy prevention. That said, I am not aware of reliable, publicly available implementations of robust image signatures. However, some robust hash functions have mature open source implementations in the pHash library [36]. Their use may be considered when implementing a custom image authentication solution, but care needs to be taken to ensure sufficient randomness and address potential security concerns.

2.3. Distributed source coding

An alternative approach to digital image authentication has recently been proposed by Lin et al. based on the distributed source coding theory [37]. The authors consider a work-flow where the signature is downloaded on demand from a trusted server. Each time a request is made, a new randomly initialized signature is generated that entails two components: a signature of quantized random projection coefficients, and a Slepian–Wolf bitstream based on low density parity check (LDPC) codes. The latter will be used by the receiver to correct errors in the projection that stem from using a distorted image in place of the original one. The rate of the code, and hence the length of the signature, grows together with the tolerable distortion. The distortion constraint is specified in a compression-oblivious manner, and hence the algorithm is not targeted at any specific compression standard.

The system also provides an adaptive signature generation mechanism which allows for advanced authentication features. An expectation–maximization algorithm can recover from contrast and brightness changes, and from mild affine warping (e.g., resizing, rotation) by estimating the most likely parameters of the involved post-processing operations. Incorporation of a space-varying channel model allows to deliver precise tampering localization capabilities.

3. Watermarking-based protection techniques

This section describes active protection methods based on authentication watermarking. The techniques discussed here bear resemblance to digital signatures (Section 2) but rely on a different

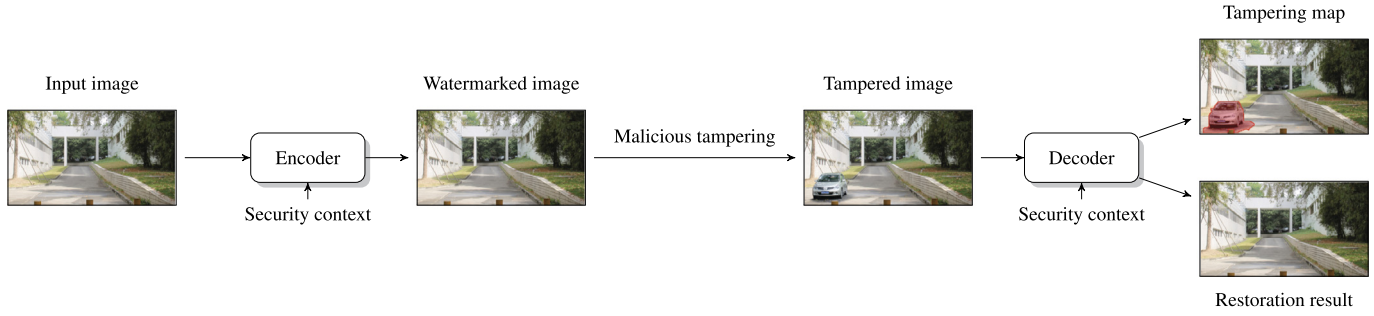

Fig. 2. Schematic work-flow of an active image protection system based on digital watermarking: a protected version of an image is generated by a watermark *encoder*; a corresponding *decoder* extracts the embedded watermark and analyzes it to locate the malicious forgery or restore the original appearance of the image, depending on the reference information available in the watermark.

carrier. Instead of easily removable meta-data, a digital watermark is used for embedding necessary side information directly into the image content.

A general work-flow for watermarking-based protection techniques is shown in Fig. 2. A typical system consists of two modules: (1) an *encoder* – responsible for embedding a watermark into the image; (2) a *decoder* – responsible for extracting the watermark and locating malicious tampering or restoring the original image content. Depending on system functionality, different terminology is used. Systems with exact authentication capabilities are referred to as *fragile* watermarking (Section 3.1.1). Systems capable of tolerating selected mild post-processing are referred to as *semi-fragile* watermarking (Section 3.1.2). Finally, systems that can recover the original content of a tampered image are referred to as *self-recovery* watermarking (Section 3.2).

3.1. Authentication watermarking

I use the term *authentication watermarking* to denote systems capable of tampering detection and localization. This is an umbrella term for both fragile and semi-fragile systems.

3.1.1. Fragile watermarking

The family of fragile watermarking includes techniques for precise image authentication with bit-level sensitivity.[1] As a result, the authentication mechanism is sensitive to the slightest changes in the image content, which inherently limits its applicability to lossless image formats, e.g., PNG, TIFF, or lossless variations of JPEG 2000, or WebP. Thanks to considerable embedding capacity of lossless image representation, fragile watermarking schemes can deliver not only very precise localization, but can also be equipped with self-recovery capabilities. The issue will be discussed in more detail in Section 3.2.

Fragile watermarking schemes typically operate by dividing the image into small non-overlapping blocks.[2] For each block, a short signature is generated and subsequently embedded as a digital watermark in either the current block itself, a randomly chosen different block, or spread over many blocks. For example, the technique proposed by Zhang and Wang [39] generates a 31-bit signature for every pixel and then pseudo-randomly combines bits from multiple such signatures before embedding. Statistical analysis of errors observed in extracted signatures allows to identify the most likely tampered pixels.

[1] Least significant bits are typically not authenticated since they are used for watermark embedding. In applications where complete bit-wise fidelity with the original is required, one may consider reversible authentication watermarks, e.g., [38].

[2] Note that pixel-wise operation can be considered as a boundary case with 1 px blocks.

3.1.2. Semi-fragile watermarking

Semi-fragile watermarking uses robust hash functions that are sensitive to important, semantic changes to the image content but remain robust to global, non-invasive post-processing. A brief overview of existing hash functions has already been presented in Section 2.2. Analogously to their fragile counterparts, semi-fragile schemes typically operate on non-overlapping image blocks. The main difference involves adoption of carefully designed signatures, watermark embedding methods, and decision criteria that warrant robustness to acceptable post-processing. Hence, such schemes will typically use larger image blocks (with popular choice of 64×64 px blocks), and introduce more severe embedding distortion.

In contrast to signature-based systems, the ground truth hashes in semi-fragile watermarking are embedded in the image itself which makes them susceptible to watermark extraction errors. As a result, asymmetric encryption is not used and hash verification is often modeled as a statistical detection problem. A good illustration of this principle can be found in the popular scheme by Fridrich and Goljan [32]. In addition to a binary hash generation algorithm, the authors also discuss a method of generating a robust spread-spectrum watermark. The final decision is made based on the watermark detection strength.

3.1.3. Fundamental limitations

Two principal limitations of watermarking-based protection methods consists in: (a) adoption of work-flows where images can be pro-actively protected; (b) degradation of image quality due to watermark embedding. The former can be facilitated by accessible implementations of protection techniques for popular acquisition devices, either digital cameras or smart-phones. Meerwald has demonstrated a proof-of-concept implementation of spread-spectrum watermarking in a custom camera firmware CHDK [40]. A recent study has shown that modern smart-phones can efficiently embed sophisticated authentication watermarks with self-recovery capabilities even for high-resolution photographs [41].

The second limitation can be addressed by proper scheme design, relaxation of authentication requirements, or adoption of reversible watermarking [38]. Depending on the maximal acceptable distortion, different authentication performance can be expected. While fragile watermarking can deliver negligible distortion and even pixel-wise tampering localization, semi-fragile techniques will typically use blocks of the order or 32×32 or 64×64 px and introduce slightly perceptible noise.

3.1.4. Known vulnerabilities & attacks

Over time, many vulnerabilities of early naive fragile watermarking techniques have been eliminated. Among others, problems with insecure block mappings, or inter-block dependencies have been successfully addressed by newer schemes [43,44]. Modern

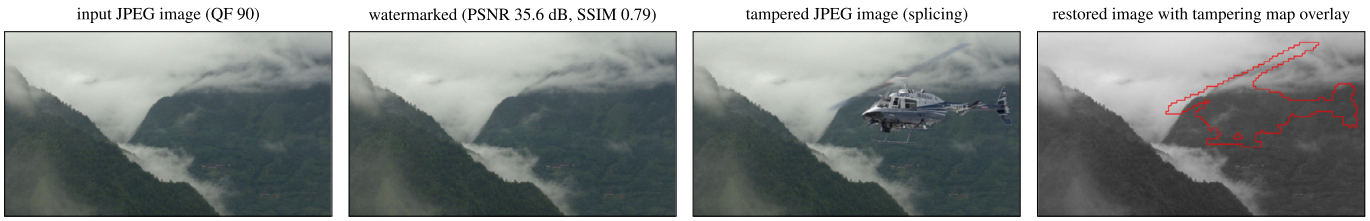

Fig. 3. An example result of image authentication based on self-recovery watermarking: a JPEG image was protected with the scheme described in [41]; a forged image was then obtained by splicing a helicopter into the protected image, and saving it as a JPEG with the same quality settings; the scheme precisely located the inserted object and restored a high-quality gray-scale version of the original content.

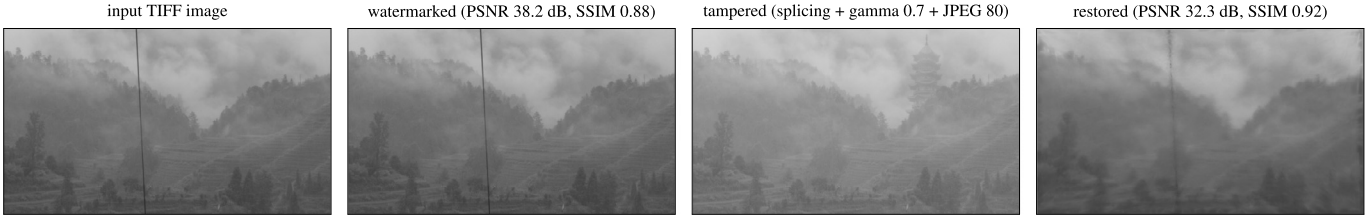

Fig. 4. An example result of image authentication with self-recovery in the presence of global post-processing: an input TIFF image was protected with the scheme described in [42]; the protected image was tampered by inserting an object, post-processed by gamma correction with $\gamma = 0.8$, and saved as JPEG with quality 90; the system successfully restored an approximate appearance of the full original image.

approaches can spread the embedded information over the entire image [39].

The primary goal of attacking fragile watermarking systems is to trigger false negative errors in tampered block detection. The most popular attacks, referred to as collage and vector quantization attacks, involve identification of equivalence classes, i.e., sets of image blocks that can be replaced without causing an alarm [45]. Provided that the cardinality of the equivalence class is large enough, it might be possible to generate a plausible approximation of a tampered image which would be accepted by the decoder. This typically requires a large data-set of images protected with the same key. Countermeasures involve adoption of a sufficiently frequent key rotation policy, and inclusion of context information within the generated signatures, e.g., spatial location of the block, or some features of its neighborhood [46].

Another attack vector involves minor adjustments of a tampered image until a perceptibly close acceptable variant is found. Examples include the constant-average attack [47] and the XOR-equivalence attack [48]. These vulnerabilities are mostly applicable to older techniques with trivial signatures, like the average value of a block. However, it is important to keep this attack vector in mind when designing new techniques.

3.2. Self-recovery watermarking

One of the most compelling features of watermarking-based protection involves its ability to recover the original appearance of tampered regions based solely on the protected, and potentially tampered, image. This capability is referred to as *self-recovery* or *self-embedding*. The idea has been originally proposed by Fridrich and Goljan [10] and subsequently refined in the following years by various scholars.

3.2.1. General information & analysis capabilities

Self-recovery is typically an extension of conventional authentication watermarking. In addition to local hashes, the watermark contains also a compressed and encoded representation of the image content [49–54]. The decoder extracts this reference information from authentic image regions, and uses it to restore the original appearance in the tampered ones. Hence, although often characterized by impressive tolerance for tampering, such schemes essentially rely on localized character of the forgery. Alternatively, self-recovery schemes may aim at approximate reconstruction of the whole image [42,55]. Such approaches are typically more robust and can possibly work in the presence of global post-processing (e.g., brightness adjustments, or lossy compression).

Due to significant requirements with respect to embedding capacity, most self-recovery schemes are limited to lossless image representations. They are, however, capable of impressive restoration performance – high quality recovery (with PSNR above 35 dB) is possible even in case of extensive tampering (even above 50% of the image area). While most of the schemes need to be designed with specific maximum tampering rate in mind, some deliver flexible reconstruction capabilities, i.e., high-quality restoration is achievable in case of small forgeries, and larger ones lead to gradually lower quality [51–53].

Very few self-recovery schemes can work with lossy-compressed images [41,42,55,56]. The most recent examples include two algorithms proposed by Korus et al. [41,42]. Example authentication results for both of these methods are shown in Figs. 3 and 4. Fig. 3 shows a splicing forgery of a 2 Mpx JPEG image. A helicopter was inserted into the protected photo, and the forgery was saved as JPEG with the same quality settings as the input image (quality factor 90, 4:2:2 chroma sub-sampling). The embedded watermark allowed for accurate localization of the forgery (10% of image area) and for high-quality reconstruction of a gray-scale version of the original image.

Fig. 4 shows an example of robust self-recovery with full-frame reconstruction. A gray-scale 2 Mpx TIFF image was protected with the method from [42] while retaining high fidelity of the watermarked image (PSNR of 38 dB). A forger inserted a pagoda into the background and removed an electric wire from the foreground by inpainting (in total 5% of image area was affected). Then, the forger adjusted image brightness with gamma correction ($\gamma = 0.7$) and finally saved the image as JPEG with quality factor 80. Despite both localized editing and composite global post-processing, the method was able to recover an approximate version of the original image with reasonable quality. Despite coarse reconstruction, the restored image clearly reveals not only the large spliced object, but also the small electric wire and the original brightness level.

3.2.2. Protection techniques

Self-recovery essentially involves communication of the original image content to the decoder through a potentially tampered dig-

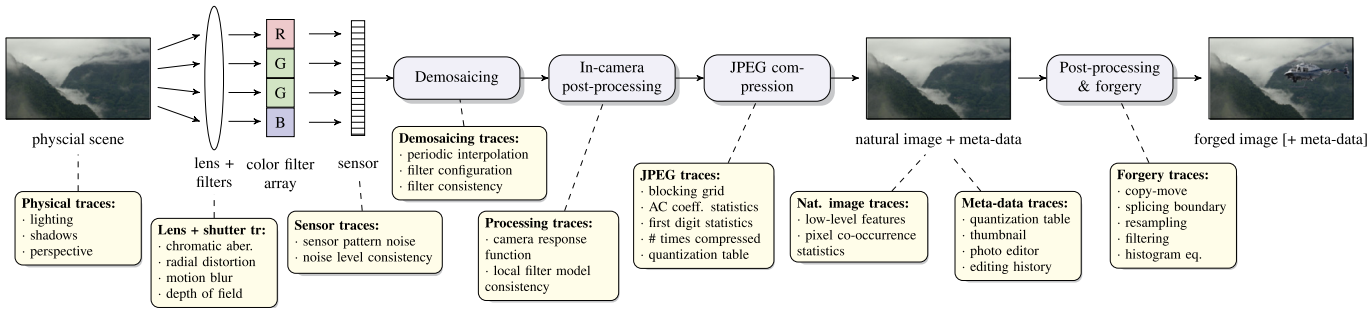

Fig. 5. Overview of a typical digital photo acquisition pipeline along with relevant operation traces that can be analyzed to assess image integrity.

ital image. A recent study has demonstrated that the problem can be modeled as an extension of the erasure channel [49], which leads to superior reconstruction performance. A reference implementation based on random fountain codes outperformed 5 different state-of-the-art methods on uncompressed gray-scale images. Adoption of more efficient image compression and error correction codes has recently shown further improvement in the reconstruction performance [54].

The erasure model is also effective when dealing with real-world imagery, i.e., high-resolution, color JPEG images [41]. The additional color channels can be used either for color reconstruction, or for strengthening protection of the luminance channel. Computational scalability issues were addressed by careful analysis of possible parallelization strategies. As a result, a reference implementation for smart-phones allowed for efficient image protection on mainstream devices (e.g., Samsung Galaxy S3, or Sony Xperia Z1). Protection in the low-quality color reconstruction mode required only about 4–5 seconds for 8 Mpx photographs.

Performing self-recovery in the presence of global post-processing requires a robust content representation that can tolerate errors. Zhu et al. proposed a model based on irregular sampling and restored the image with projections onto convex sets [56]. Cheddad et al. embedded a dithered binary representation of the image and performed reconstruction with inverse half-toning [55]. Korus et al. represented the image by means of random sections and filled the missing information by push-and-pull inpainting [42].

3.2.3. Challenges & limitations

While fragile self-recovery for lossless image representations is a fairly well-investigated topic, very few studies are available for the semi-fragile case. Due to limited embedding capacity in the presence of lossy compression, it remains a challenging problem to design a robust content representation and hence obtain high-fidelity self-recovery. Moreover, due to special handling of chrominance channels during lossy compression, naive replication of the protection mechanism for the additional channels is unfeasible. While a recent study discusses some possible strategies [41], further work in this direction is required.

3.3. Available software

I am not aware of publicly available mature implementations of authentication watermarking. Several commercial companies have the necessary expertise, but such products are not advertised to the mainstream audience.[3] Existing deployed solutions are custom-made and their details are not published in order to avoid targeted attacks [59].

An academic implementation of a recent self-recovery mechanism based on fountain codes is available as supplementary materials to the original publication [49,60]. This reference implementation supports uncompressed images only and is not readily applicable to real-world scenarios.

4. Forensic verification techniques

The necessity to actively protect digital images is in many cases an excessively restrictive and impractical requirement. In order to address this issue, scholars have studied passive authentication techniques which exploit intrinsic fingerprints introduced into the photographs during their acquisition or manipulation. These forensic traces allow to reason about the origin, processing history and authenticity of the captured images. A schematic view of the digital photo acquisition pipeline is shown in Fig. 5 along with a general classification of traces documented in the literature. I follow this classification in my discussion, and review the analysis capabilities, robustness and limitations of individual fingerprints. I begin with physical traces in Section 4.1 and work my way towards the traces of specific manipulations in Section 4.10.

This paper focuses on the problem of image integrity verification. Hence related forensic problems, e.g., source attribution, will not be described in detail although they often utilize the same traces, e.g., sensor noise signatures for device linking [61], pixel co-occurrence statistics for camera model identification [62], or natural image models for detecting computer graphics or photo recapture [63]. My main goal is to give a balanced summary of analysis capabilities and not to review the variety of reported analysis techniques. I do present a general overview of selected state-of-the-art algorithms, but a detailed discussion is out of scope of this work. For a detailed treatment of these topics, interested readers are referred to the original publications, other topic-specific surveys [17–20,64,65], or books [66,67].

Similarly to active protection techniques, passive forensics can also aim at either forgery detection or localization. The latter is typically obtained by straightforward application of a detection rule in a fixed-size sliding-window manner. The window size needs to be carefully chosen to balance contradicting requirements of good localization resolution (where small windows are preferred) and sufficiency of detection statistics (where large windows are often necessary). I review existing localization protocols and possible ways of addressing this trade-off in Section 4.11.

Due to their simplicity, individual forensic traces are often easy to reintroduce after a forgery, which may render forensic analysis either more difficult or even completely unreliable. Techniques designed for this purpose are referred to as *anti-forensics*, and they will be discussed along with relevant traces that they target. Due to limited robustness of forensic traces, and the risk of their falsification, reliable analysis needs to assess multiple traces and reach a joint decision that accounts for all of them. Decision fusion frameworks are discussed in Section 4.12. The necessity to cover up

[3] Watermarking-based protection is often offered as an integrated feature in closed-circuit television (CCTV) cameras or recorders [57,58] in order to meet local surveillance standards or regulations.

many independent traces of a prospectively undetectable forgery significantly increases its complexity and the required skill set.

The discussed traces are motivated by the photo acquisition pipeline shown in Fig. 5. However, in the emerging multi-sensor and multi-lens setups, photo acquisition is more complex and many of the discussed traces may work in a limited manner or become useless completely. I discuss the perspectives and challenges of forensic analysis in these emerging systems in Section 4.13.

4.1. Physical traces

4.1.1. General information & analysis capabilities

Physical traces for image authentication include consistency of lighting [65,68,69], shadows [70,71], as well as geometry and perspective [72,73]. Since they rely on the observance of the laws of physics within the photographed scene, they are not inherently tied to a particular image representation. Hence such techniques are suitable for highly compressed or down-sampled images where other, signal-level traces have long been destroyed.

Although they are unable to generate an accurate tampering localization map, physical traces are an effective tool to detect object insertion or removal. However, due to their complexity, their analysis is typically manual or semi-automatic. Even though such analysis is more demanding of the analyst, preparation of convincing forgeries also requires greater care and skills from a forger since no automatic techniques exist that would allow to mask these kinds of artifacts.

4.1.2. Analysis techniques

Validation of geometric and perspective constraints builds upon the pinhole model that assumes central projection of 3-D space points onto the image plane. The model allows to compute vanishing points of a perspective projection, whose inconsistencies can reveal malicious changes in the image content. Yao et al. presented a method for comparing height ratios of objects based on a vanishing line of a common plane [74]. The method does not require knowledge of camera parameters, but is limited to images taken with zero tilt and roll angles. A generalization of the above analysis method that addresses this limitation was recently presented by Iuliani et al. [75]. Analysis of perspective constraints can also be useful in revealing forgeries of signs and billboards [72]. The technique consists in verifying consistency of perspective between the sign and its text, which may be challenging to match accurately.

Lighting inconsistencies include artifacts like mismatch in the direction of light [65] or the color of the dominant illumination [69]. Detection techniques for the former involve estimating the light direction from Lambertian surfaces with constant reflectance. The analysis typically assumes a single distant point light source and can be carried out either in 2D or in 3D, depending on the availability of the surfaces' normals (which can be obtained, e.g., from 3D models of known objects like a human eye [65]). Statistical estimators allow to take into account the color of the light, which may be difficult to match exactly during a forgery. A semi-automatic approach proposed by Carvalho et al. extracts texture-based and edge-based features from illuminant maps to look for lighting mismatch between pairs of human faces [69]. A general low-dimensional model that characterizes the lighting environment has also been studied [68]. However, the method requires to compute the lighting descriptor from patches of homogeneous materials, which is challenging in realistic conditions. A possible approach to address this problem is to integrate reflectances from multiple materials [76]. The topic is currently a subject of ongoing research. In a recent paper, Peng et al. propose a generalized 3D lighting estimation algorithm [77] which relaxes the requirement for constant reflectance and convexity. The described method takes into account the geometry and texture information and achieves better lighting estimation performance.

Analysis of shadows can exploit both geometric constraints [70] and shadow color or matte inconsistencies [71]. The former approach bears some resemblance to perspective projection verification, but relies on tracing shadow projection from a light source. It also takes into account potential interactions of the objects within a scene. Unfortunately, such analysis cannot be performed automatically and may be infeasible in complex lighting environments. The latter approach that involves estimation of the shadows' matte can be performed automatically provided that certain assumptions are met. The method presented by Liu et al. [71] estimates the matte value for each detected shadow and cross-validates them for consistency. The method follows a popular assumption of a single distant point light source, and nearly Lambertian surfaces. Moreover, the shadow-casting objects need to be opaque.

4.1.3. Available software

Although specialized tools that facilitates forensic analysis of physical traces do exist, I am not aware of publicly available software for most of the discussed methods. The only exception are the illuminant color analysis method by Carvalho et al. [78] and the 3D lighting environment estimation method by Peng et al. [79] which have academic implementations provided by the authors.

4.2. Lens & shutter traces

4.2.1. General information & analysis capabilities

Malicious changes in image content can also be exposed by inconsistencies in lens and shutter-related parameters of a photograph including chromatic aberration [80], radial lens distortion [81], motion blur [82–84] and depth-of-field [84]. Since all of these techniques look for local deviations from a general expected model, they are capable of localizing the forgery. In contrast to physical traces, it is often possible to perform localization automatically.

4.2.2. Analysis techniques

Chromatic aberration is caused by refractive index variation for different wavelengths of light which manifests itself in radially increasing relative shift between color components. The resulting fringing artifacts can be estimated by locally maximizing mutual information between color channels [80]. Although the technique can reveal local editing, it operates on excessively large image blocks of 300×300 px, which makes it poorly suited for detecting small forgeries. However, well predictable radial character of this trace makes it possible not only to detect image cropping, but also to estimate the approximate location of the current rectangle within the original canvas [66].

Tampering localization based on blur inconsistencies involves local estimation of motion blur direction from gradient analysis [82] or general estimation of blur kernels [84]. The latter approach allows for distinguishing between the types of blur (motion vs. depth of field) but requires human interaction. The analysis can be performed with windows of intermediate size, e.g., 64×64 or 128×128 px which allow for reasonable resolution of tampering localization. While the method is robust to post-forgery processing, it does not work in complex situations when both motion and out-of-focus blur are present.

Estimation of radial lens distortion relies on straight lines of sufficient length [81]. First, an edge detector is used to find possible lines in the image. Then, potentially distorted straight lines are detected within an acceptable margin. Finally, a 1-dimensional polynomial distortion model is fitted to determine the radial distortion. Straight lines that violate the globally expected model are marked as belonging to a potentially spliced object. However, the

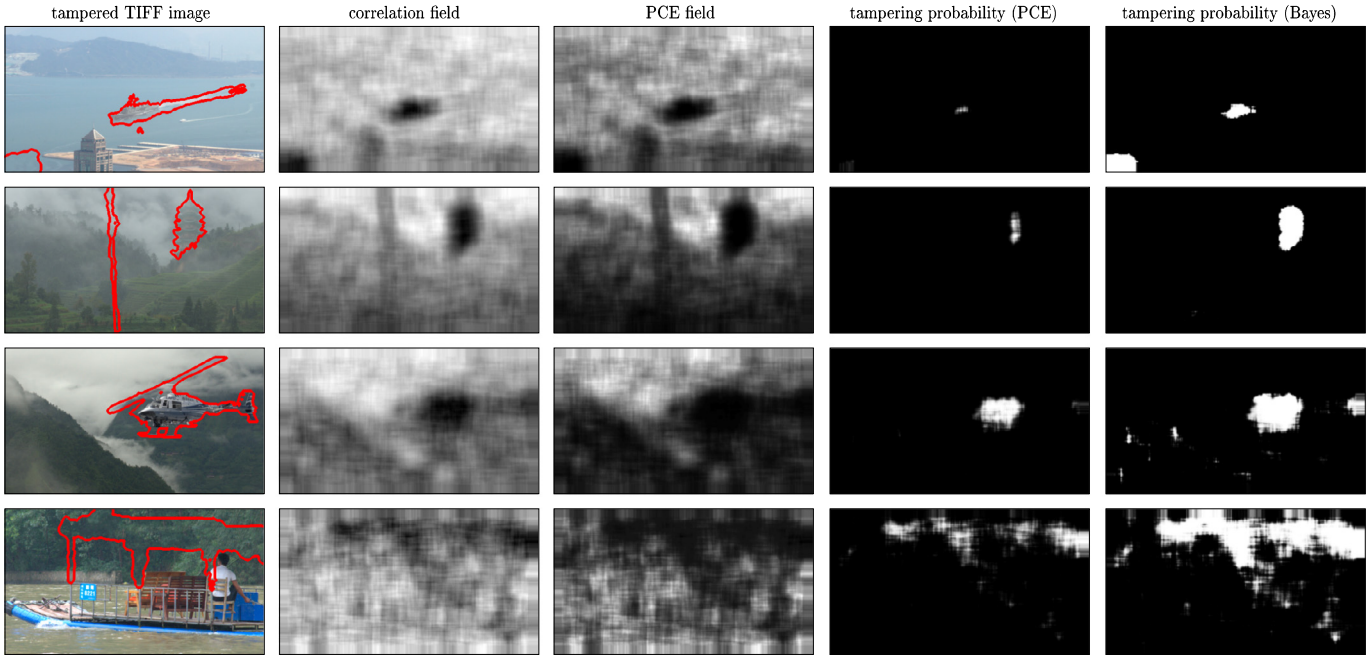

Fig. 6. Example results of tampering localization by local analysis of sensor pattern noise; successive columns represent different variants of analysis including: (2nd column) standard normalized correlation field; (3rd column) peak-to-correlation energy (PCE); (4th column) tampering probability estimated from the PCE; (5th column) tampering probability from a Bayesian formulation with a correlation predictor.

method is not capable of generating an accurate tampering localization map.

4.2.3. Fundamental limitations & anti-forensics

For the sake of better image quality, both chromatic aberration and radial lens distortion are commonly removed in post-processing – either in digital darkrooms (e.g., Adobe Lightroom) or directly in the camera. Hence, these traces are not necessarily widely applicable. The ease of removal of chromatic aberration artifacts makes it also easy to design relevant anti-forensic techniques [85].

Camouflaging blur inconsistencies can be performed manually in photo editing software. An automatic algorithm for this purpose has recently been discussed by Rao et al. who propose to blend the target object into the background with properly designed alpha matte that takes into account the local blur model [86]. The described attack was successfully used to mask splicing forgeries both in a synthetic and a realistic evaluation.

4.3. Sensor traces

4.3.1. General information & analysis capabilities

Due to manufacturing imperfections, pixels in imaging sensors exhibit minor variations in photo response sensitivity leading to consistent multiplicative noise in all acquired images. This photo response non-uniformity (PRNU) pattern is stable over time and can be used as a unique signature of each device [61]. Remarkable robustness of this signature against common image post-processing (e.g., resizing, compression) has lead to its wide-spread adoption in forensics investigations and availability in commercial software.

The technique is used in two principal applications: source attribution, and forgery localization. The former allows to either confirm or identify the device that was used to capture a given photograph. It involves correlation of the expected device signature with its estimate from the investigated image. The method can effectively work with large-scale datasets, as confirmed by an evaluation covering 6,896 devices representing 150 camera models [87]. Forgery localization based on sensor signatures relies on local correlation of the signatures to identify specific areas with potential mismatch. In addition to generation of pixel-wise tampering localization maps, analysis of the PRNU signature can also be used to estimate parameters of resizing or cropping [88].

4.3.2. Analysis techniques

Due to multiplicative character of PRNU, the expected correlation of the signatures varies with local image intensity [61]. Moreover, in highly textured areas noise estimation algorithms cannot fully separate image content from the sensor noise leading to signature contamination and deterioration of the correlation statistics. As a result, local analysis is typically aided by a predictor, which estimates the expected correlation based on local image features. Alternatively, locally shifted versions of the signature can be used as a baseline, leading to self-normalized scores, like peak-to-correlation energy (PCE) [87] or correlation to circular correlation norm (CCN) [89]. However, in tampering localization these measures seem to perform sub-optimally.

Fig. 6 shows example tampering localization results for different variants of local signature analysis: (a) standard normalized correlation field; (b) peak-to-correlation energy (PCE); (c) tampering probability estimated from the PCE; (d) tampering probability from a Bayesian formulation with a correlation predictor. Due to relatively large analysis window size (I used the most common 129×129 px windows for all considered variants), PRNU-based localization is unable to detect small forgeries. Moreover, it tends to work poorly in highly-textured dark areas. An obvious gap in correlation strength between solid and textured areas can be clearly observed in the correlation fields shown in Fig. 6.

In order to address these limitations many researchers have focused on improving the quality of sensor noise estimation. Various techniques have been reported including: (a) adoption of more reliable denoising (e.g., BM3D [90]); (b) equalization of the spectrum of the PRNU [91]; (c) retaining only its phase information [89]; (d) attenuation of strong components bleeding from image content [92]; (e) suppression of color interpolation artifacts based on color filter array's structure [93]; (f) content-adaptive prediction of

noise-free pixel values [94]; (g) locally adaptive DCT filtering [95]. A recent empirical evaluation of various approaches is available in [96].

Improvements in the localization procedure include: (a) adoption of random field models [90,97]; (b) computation of the correlation scores for manually-defined image segments [98]; (c) use of guided image filtering [99]; (d) adoption of multi-scale analysis strategies [100]. All of these techniques aim at improving localization capabilities for small forgeries. While considerable improvements with respect to the original algorithm have been obtained, the issue is still subject to ongoing research.

4.3.3. Fundamental limitations

As already mentioned, reliability of sensor noise estimates is severely limited for dark and textured content. Hence, such images (or areas thereof) do not allow for reliable PRNU analysis, especially in the presence of further post-processing. Additionally, collection of sufficiently discriminative detection statistics requires relatively large analysis windows. Following the recommendation of the original authors, most localization algorithms use a fixed window size of 129×129 px which is already too large to detect small forgeries. A recent evaluation of multi-scale strategies confirmed that this size delivers good balance in overall performance but is overly conservative in favorable areas [100]. While the situation can be improved using some of the techniques discussed in Section 4.3.2, it is unlikely that the performance gap could be eliminated.

Despite good robustness of the PRNU, reliable analysis requires synchronization between the signatures. Hence, care needs to be taken when dealing with images that have been resampled, cropped [88], or corrected for lens distortion [101]. Usually some form of brute-force search is adopted.

4.3.4. Available software

Sensor noise analysis techniques (either tampering identification or source attribution) are implemented in commercially available forensics software including Amped Authenticate [102], Verifeyed [103], Pizarro [104], and Forensic Pathways Image Analyzer [105]. Academic implementations are also available for sensor noise estimation [106], signature matching [106], and various tampering localization strategies [100,107].

4.3.5. Known vulnerabilities & attacks

There are two main attacks on sensor noise verification systems. The first involves removal of the signature with the aim of image anonymization [108]. Some of the proposed techniques include patch-based desynchronization attacks [109] or enforced seam carving [110].

The second scenario involves malicious insertion of a signature, which may be performed in combination with the first (to attack source attribution) or separately (to attack forgery localization). In the first case, re-inserted signatures may be detected by a triangle test [111] which exploits vestigial correlations with stolen images. However recent study suggests that by carefully choosing signature insertion strength, the attacker can significantly increase his chances of success [112].

In case of forgery localization, there are no reported defenses against the re-insertion attack. An attacker in possession of the camera may produce an arbitrarily high-quality signature and discard any intermediate images in the process. The correlation predictor from the original analysis method will even help to determine the strength of signature insertion for each image area. To the best of my knowledge, successful detection of this attack has not yet been reported.

4.4. Noise level traces

4.4.1. General information & analysis capabilities

In addition to sensor pattern noise, image forgeries may also be revealed by inconsistencies in local noise levels. This trace combines joint influence of the sensor characteristics, the current ISO setting, and prospective post-processing (e.g., denoising). Noise level analysis is primarily used in splicing detection. While the algorithms will typically yield a map of local noise variances, there is no automatic method to map the results to tampering probabilities. Hence, localization using this trace is a semi-supervised problem.

4.4.2. Analysis techniques

One of the most popular algorithms for splicing detection based on noise level traces was proposed by Mahdian and Saic [113]. Their method performs noise level-based image segmentation. The algorithm proceeds by estimating noise variance within small image blocks. Neighboring blocks with similar noise levels are then merged to form larger segments. The method operates under a Gaussian noise assumption.

Pan et al. proposed a different method for local noise variance estimation [114]. Their approach builds upon an observation that kurtosis of band-pass filtered natural images should concentrate around a constant value. The algorithm yields response maps with pixel-level resolution. It is effective only if the tampered area exceeds 10% of the image and the noise strength exceeds 10 dB.

While both of the above algorithms assumed the additive white Gaussian noise model, a recent method by Yao et al. [115] was designed to work with intensity-dependent noise (similar to PRNU). The authors discuss a noise level function (NLF) which aims to better fit noise characteristics with possible variations of standard deviation with image intensity. The NLF is estimated from a Bayesian maximum a posteriori (MAP) formulation, while including constraints stemming from the camera response function (CRF, see Section 4.6).

4.4.3. Limitations & known vulnerabilities

By definition, noise level estimation algorithms are sensitive to variations in the local noise variance. Hence, carefully prepared forgeries where similar noise level is maintained, will not be detected. Existing algorithms were evaluated mostly on synthetic forgeries with carefully controlled strength of artificially inserted noise, and on naive splicing forgeries without explicit care about noise level consistency. Further work is required to validate their potential on high-quality forgeries. At this moment, it would also seem that designing efficient anti-forensic techniques should be fairly straightforward. However, I am not aware of existing studies of this problem.

4.4.4. Available software

Noise level consistency is a simple forensic trace with available commercial implementations. Relevant tools are available in Amped Authenticate [102], and Pizarro [104]. An academic implementation of the algorithm proposed by Mahdian and Saic [113] can be found in the Image Forensics Toolbox [116].

4.5. Demosaicing traces

4.5.1. General information & analysis capabilities

In order to capture color images, most digital cameras adopt the Bayer color filter array (CFA) which makes each pixel capture either red, green, or blue components of the incoming light.[4] A full

[4] There exist many variations of color-capture technologies including different filter colors (e.g., CMY – cyan, magenta, yellow), various color arrangements, or even

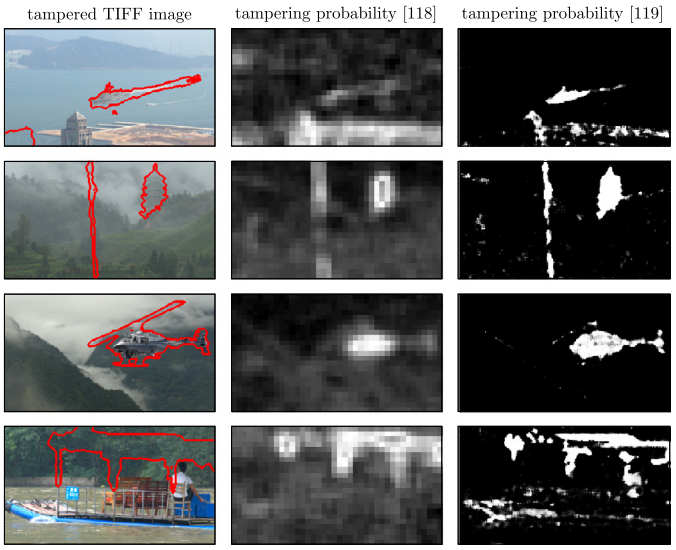

Fig. 7. Example results of tampering localization by local analysis of CFA interpolation; successive columns represent the tampered image, localization result by Dirik and Memon [118], and localization result by Ferrara et al. [119].

resolution color image is obtained by color interpolation, known as *demosaicing*. Periodic structure of the CFA leads to periodic interpolation artifacts that can be expected in pristine digital photographs [117]. Image forgeries can be revealed by analyzing local discrepancies, e.g., locally missing interpolation, or locally different CFA structure. Potential forgeries may also be detected by comparing an estimate of the CFA structure with the one reported in image meta-data.

Presence of demosaicing artifacts is a useful indicator for source attribution. Not only can it be used for distinguishing between certain camera models, but also allows to distinguish digital photographs from computer generated imagery.

4.5.2. Analysis techniques

Estimation of the current CFA structure can be easily performed by sub-sampling and re-demosaicing the image according to various filter configurations and choosing the one that yields the lowest reconstruction error. Kirchner proposed an algorithm that can estimate the CFA structure more efficiently by means of a single linear filtering operation [120].

Presence of periodic interpolation artifacts can be verified by Fourier transform analysis [117], where characteristic peaks can be observed. However, this method requires large image blocks and is not suitable for precise tampering localization. In order to address this issue, Dirik and Memon proposed a forensic feature based on the ratio between variances of prediction residues in interpolated and non-interpolated pixels [118]. The authors use analysis windows of size 96×96 px. Most recently, Ferrara et al. [119] also considered the variance of prediction errors, but used a Gaussian mixture model to fit two conditional density functions. A naive Bayesian rule was then used to compute the tampering probability. Although the algorithm can operate on image blocks as small as 2×2 px, the authors recommended to aggregate scores from several neighboring blocks for better performance.

Example localization results for the most recent algorithms [118,119] are shown in Fig. 7. It can be observed that the method by Ferrara et al. [119] delivers better localization resolution and tends to yield more confident results. In this example, I used block aggregation to obtain effective localization resolution of 8×8 px blocks, which was reported to yield the best performance.

4.5.3. Fundamental limitations

Despite very precise localization ability, CFA interpolation artifacts constitute a relatively simple feature which lacks both robustness and security. Traces of periodic interpolation are easily destroyed by JPEG compression, even with the highest quality levels. Hence, this trace is applicable almost exclusively for never-compressed photographs. Moreover, existing methods assume that the camera uses the standard Bayer CFA and a non-adaptive demosaicing algorithm. For some cameras these conditions are violated which may lead to false positive errors, or completely unreliable localization maps.

4.5.4. Available software

The commercially available Amped Authenticate [102] can analyze interpolation artifacts, including the periodic ones from CFA interpolation. Academic implementations of the most recent methods proposed in [118,119] are publicly available online [116,121].

4.5.5. Known vulnerabilities & attacks

Due to relative simplicity of CFA interpolation, its analysis can be attacked both by straightforward re-interpolation of sub-sampled color channels, and by more advanced CFA synthesis algorithms [122] which can deliver higher image fidelity. It is also possible to either remove or synthesize CFA artifacts by standard gradient descent driven by a CFA-based forensic feature [123].

4.6. In-camera processing traces

Without post-processing, pixel intensities could be expected to be linearly proportional to the amount of light actually measured by the senor. However, such a representation is poorly suited to the logarithmic perception of a human vision system and digital cameras employ non-linear post-processing to enhance final image quality. The mapping, referred to as a camera response function can be estimated and analyzed for inconsistencies to reveal a forgery. The method proposed by Hsu and Chang performs this by comparing response functions between different image segments [124]. While the algorithm aims at forgery detection, some localization clues may be inferred from the automatically obtained segmentation.

Swaminathan et al. proposed to use blind deconvolution to estimate a filter that could model both in-camera and external post-processing [125]. Hence, their approach aims to learn low-level characteristics of authentic images acquired by a specific camera. While the method is aimed at detecting specific post-processing operations, it may also be used for tampering localization by revealing local inconsistencies from the expected camera model.

While the above studies have reported good results in targeted academic evaluation, I am not aware of any large-scale evaluation on realistic forgeries. To the best of my knowledge, none of these techniques is currently implemented in commercial forensic analysis software.

4.7. JPEG compression traces

4.7.1. General information & analysis capabilities

Despite its old age, JPEG [132,133] remains the dominant image codec for digital photographs. It is used by default in most digital cameras and Web services such as photo galleries, or social networks. Even though many professionals and advanced enthusiasts may prefer to capture RAW images, final edited versions of their

filter-less sensors that directly capture full-resolution RGB components (e.g., the Foveon X3 sensor). Nevertheless, the RGB Bayer CFA remains dominant on the market.

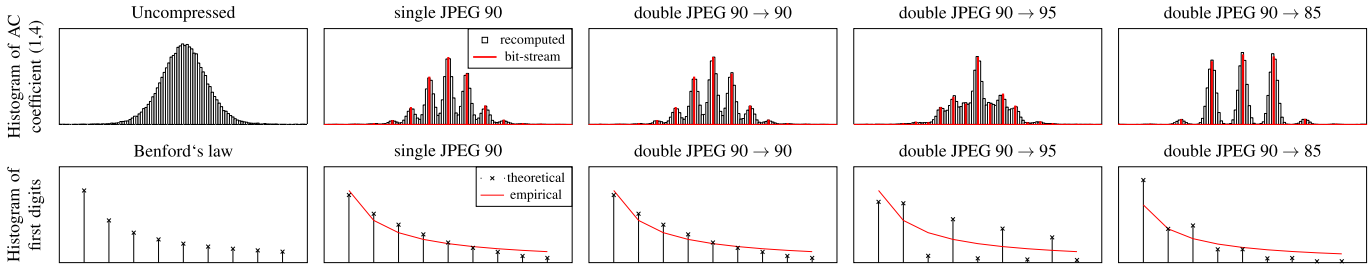

Fig. 8. Impact of multiple JPEG compressions on selected transform-domain traces: (top) 1-order statistics of DCT coefficient (1,4) in the luminance channel; (bottom) first digit statistics for DCT coefficient (1,2) in the luminance channel and the expected Benford's law model; note significant changes in behavior when the quality level changes (4th and 5th columns); note also the difference between DCT coefficient statistics extracted from a JPEG bit-stream (red peaks in the top row) and recomputed from a decoded spatial representation (black bars). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

photographs will be converted to JPEG anyway – either for archiving or publication. This makes JPEG-based traces one of the most important tools in digital image forensics.

The codec operates on non-overlapping image blocks of size 8×8 px. Each block is transformed to spectral domain by discrete cosine transform (DCT), and the obtained coefficients are quantized according to a *quantization table*. The table specifies 64 quantization steps, for various horizontal-vertical frequencies, which can be adjusted to control the desired image quality or file size.[5] The JPEG standard does not define the quantization tables, which can be customized by camera or software manufacturers. A popular approach to control the rate-distortion trade-off involves specification of a general formula to compute the quantization table based on a single *quality level*. Such an approach is used, e.g., by a popular, free implementation from the independent JPEG group (IJG) [133].

Since different software and hardware manufacturers often use customized quantization tables, it is straightforward to verify the investigated file against a database of known tables. However, due to the ease of re-compression and meta-data editing, such analysis may not be reliable. In some cases, it may be possible to detect original image parameters by sophisticated statistical analysis. For example, it is possible to detect traces of JPEG compression or even estimate the involved quantization matrix from an uncompressed bitmap representation [134,135]. Furthermore, analysis of complex JPEG-based traces allows to distinguish the number of compression steps that the image has undergone. Popular decision criteria include uncompressed vs. compressed, and singly vs. doubly compressed images. Traces of multiple compression indicate that the image has been re-saved, but not necessarily tampered with. However, local inconsistencies of image compression history clearly indicate malicious editing.

4.7.2. Analysis techniques

Analysis of JPEG compression traces can be performed both in the spatial and in the transform domain. Since image blocks are processed independently, excessive compression leads to *blocking artifacts* – a regular grid of size 8×8 px which reveals the original division structure in the spatial domain. In case of malicious tampering, the regular structure of this grid may be locally disturbed. Li et al. proposed a technique which exploits this phenomenon for tampering localization [126]. The algorithm automatically generates a tampering map which clearly shows areas where the local blocking grid diverges from the global one.

Transform domain analysis relies on the expected statistics of DCT coefficients which can reveal traces of multiple JPEG compression. Fig. 8 shows the behavior of two popular traces for images with various compression histories: (top) distribution (1-st order statistic) of a selected DCT coefficient; (bottom) first digit statistics of a selected DCT coefficient [136]. It can be observed that both traces are sensitive to compression quality changes between subsequent compressions and can be used for construction of effective classifiers. Typically multiple DCT coefficients are used to improve reliability.

In uncompressed digital images, the distribution of AC coefficients (top row in Fig. 8) follows a generalized Gaussian distribution. When an image is compressed for the first time, the coefficients are quantized, but the envelope of the distribution is still followed (see red peaks in 2nd column). When subsequent compression occurs, the behavior changes depending on the image quality settings. Characteristics peaks or valleys can be observed when the second quality level differs from the first one (4th and 5th columns). Based on this behavior, various forensic features may be constructed.

Lin et al. proposed an algorithm that estimates conditional probabilities based on empirical distribution of the AC coefficients [127]. The final decision is made by a naive Bayes classifier. The algorithm was subsequently improved by Bianchi et al. who recognized that the empirical distribution is essentially a mixture of an authentic and altered components [128]. The approach was further extended in a follow-up study, which considers separately cases of aligned and misaligned JPEG blocking grid [129]. The discussed algorithms generate tampering localization maps with resolution of 8×8 px blocks.

Another efficient tampering localization approach is to consider mode-based first digit features (MBFDF), i.e., first digit statistics obtained separately for various DCT frequencies [131]. A machine learning classifier, e.g., a support vector machine (SVM), can be trained to distinguish between different compression histories. Such an approach has been reported to deliver good accuracy in detecting image splicing across various compression configurations [130,131]. However, for the sake of reliable first digit statistics, it operates on larger sliding windows. A recent study of multi-scale strategies compares its efficiency for various window sizes, ranging from 16×16 to 128×128 px [130].

Fig. 9 shows example tampering localization results for all of the discussed algorithms [126–130] and various double compression cases. It can be observed that AC coefficient analysis can deliver very precise localization, however its reliability decreases when successive quality levels are similar. MBFDF analysis appears to perform better in such situations, but needs to use larger blocks for reliable statistics. The window size in the illustrated example was 64×64 px.

4.7.3. Fundamental limitations

Most of existing techniques for tampering localization based on local compression inconsistencies work relatively well if the second quality level is greater than for the original image. If the quality level difference is sufficient, reliable localization can be performed

[5] Due to different visual impact of brightness and color information, the JPEG standard actually uses two such tables for the luminance and chrominance channels of the YC_bC_r color space.

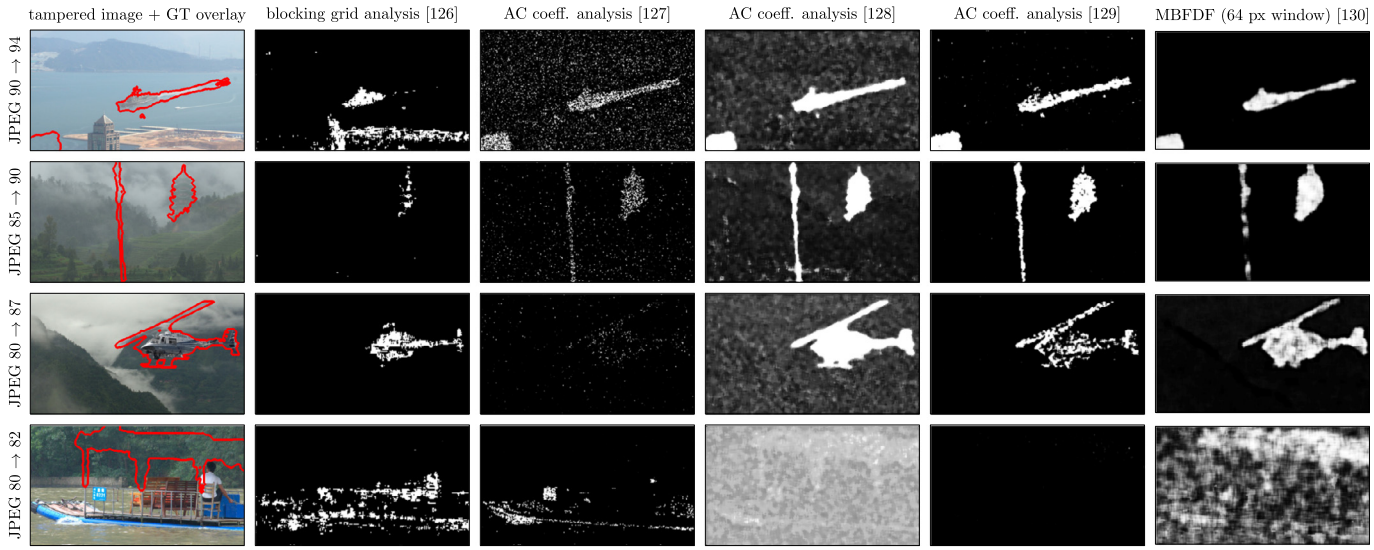

Fig. 9. Example forgery localization results that expose compression inconsistencies in four 2 Mpx images with the use of five popular algorithms: blocking grid (BG) analysis [126]; DCT coefficient analysis [127–129]; and MBFDF analysis [130,131]. Ground truth tampering map is overlaid in red on the tampered image (1st column); output maps indicate local tampering probability.

even for 8×8 px windows. If the second quality level is lower, performance drops significantly and much larger windows are required for adequate results [130]. Performance drops even further if the second quality level is the same as the original one. Although relevant methods exist to detect such cases [137,138], I am not aware of algorithms capable of forgery localization. Hence, reliable tampering localization with JPEG-based traces is still an active research topic.

4.7.4. Known vulnerabilities & attacks

The described analysis techniques can be defeated with the use of anti-forensics. Stamm et al. described a method to conceal traces of JPEG image forgery by restoring the expected 1st order statistics of DCT coefficients with the use of a controlled pseudo-random dither [139–141]. However, the method leaves traces on its own, which makes it possible to detect the use of anti-forensics [142]. An academic implementation of the above anti-forensics technique is publicly available online [143]. Similar considerations are also available for first digit statistics restoration [144–146].

The most recent algorithm for JPEG compression anti-forensics uses a 3-stage optimization that minimizes a total variation (TV)-based objective [147]. The method successfully defeats state-of-the-art forensic detectors and renders existing localization schemes ineffective (see supplementary materials to [147] for relevant localization-oriented results). To the best of my knowledge, detection of this anti-forensic technique remains an open problem.

4.7.5. Available implementations & software

Several implementations of JPEG-based forgery localization algorithms are available. Commercial software with relevant functionality includes Amped Authenticate [102] and Pizarro [104,148]. Publicly available academic implementations include Matlab code from the original authors [121], and from the Image Forensics Toolbox [12,116]. The state-of-the-art anti-forensics algorithm by Fan et al. [147], also has a publicly available Matlab implementation [149].

4.8. Meta-data analysis

Original photographs acquired with digital cameras are typically accompanied by meta-data, a (key, value) description of the image, acquisition conditions, camera settings, etc. The most popular meta-data standards include the EXIF (exchangeable image file format), and XMP (extensible metadata platform). Although this information can be easily removed or modified, it may provide invaluable insights about the image's processing history. Kee et al. [150] constructed a signature which captures the variance in JPEG quantization tables, Huffman codes, thumbnails, and EXIF meta-data. They demonstrate that their signature is highly distinct across 1.3 million images acquired by 773 cameras and smart-phones. It can be used to support source attribution and prospective tampering detection.

Some meta-data fields can deliver invaluable insights even in isolation. Popular image editors attach editor information, or even editing history (e.g., in the `Exif.Image.Software` or `Xmp.xmpMM.History` keys). The `Exif.Thumbnail` key contains a miniature of the image for quicker access to the content in a photo preview context. Some editors either do not update the thumbnail, or append a new one. As a result, forgeries may be revealed by comparing the full size image with the embedded miniature(s). Such capabilities are delivered by both commercial forensics software like Amped Authenticate [102], and open source tools like Ghiro [151]. Manual analysis can also be performed with plethora of meta-data tools for photographers (e.g., the popular exiftool [152]).

A recent study has shown that the values of certain EXIF parameters may be estimated from image content. Specifically, the method discussed by Fan et al. [153] is capable of detecting brightness and contrast adjustments based on statistical analysis of image noise. Each EXIF parameter is represented as a weighted sum of statistical noise features. Significant difference between the estimated and the explicitly reported parameters can serve as an indicator of image manipulation.

Even if standard meta-data like EXIF or XMP is stripped from the photo, valuable insights may be obtained from irremovable syntax elements of the JPEG format. The quantization tables used by various hardware and software manufacturers tends to differ and can be used to get a hint about the coder that produced the image. An open source image forensics tool *JPEG Snoop* [154] contains a large database of known quantization tables and can deliver detailed information about the utilized JPEG compression settings.

4.9. Natural image models

Conventional forensic traces exploit the effects of specific steps in the photo acquisition pipeline. Researchers have also explored general low-level features that aim to capture the complex characteristics of natural images, as captured by digital cameras. So far, two main approaches have been proposed in the context of tampering localization, i.e., pixel co-occurrence features adopted from digital steganography [155], and Gaussian mixture models [156]. Such features have been reported to accurately discriminate image splicing [155,156], various post-processing operations [156], and even images captured by different camera models [62]. However, at this point adoption of such features remains experimental due to the *source mismatch* problem. It remains challenging to train universal models that would retain high classification accuracy if testing data does not match training data. This is a considerable limitation given that even images taken with different ISO settings may be considered as coming from a different source [157]. The sensitivity, however, will depend on the technique at hand and the issue requires further study.

Low-level natural image models have also been used for distinguishing between digital photographs and computer generated images, and also between originally captured images and prospective forgeries re-captured from a computer screen. Many existing methods follow the standard approach of low-level image features, followed by a support vector machine classifier. An efficient method based on learning dictionaries of edge profiles has recently been proposed by Thongkamwitoon et al. [63]. Their approach achieves good performance based on only two features: edge spread width and approximation error from a learned sparse representation. Recapture detection is a binary decision problem and cannot be used to localize the forgery. It is also applicable in the field of biometrics for countering spoofing attacks [158].

Since natural image models build upon existing low-level features and standard machine learning methods, various implementations may be found online. Academic implementations of popular steganographic features and ensemble classifiers can be obtained from [106]. I am not aware of any publicly available pre-trained forensic models. To the best of my knowledge, such features are not available in any commercial forensics software.

4.10. Forgery traces

Previously discussed techniques rely on discrepancies in specific traces of the photo acquisition pipeline. An alternative approach involves looking for traces of known forgeries. Image editing may include general post-processing (e.g., resampling, filtering, or contrast and brightness adjustments) as well as localized malicious changes (e.g., splicing, copy-move, inpainting). Selected representative methods for detecting these operations are discussed in successive sub-sections.

4.10.1. Copy-move forgeries

A copy-move forgery involves replacement of selected image fragments with other fragments from the same image. Typically, such operation is used for duplication of an existing object, but may also be used for object removal by masking it with surrounding background. In contrast to more sophisticated exemplar-based inpainting, a copy-move forgery typically involves a larger continuous region that undergoes a rigid transformation (with optional post-processing).

Detection of copy-move forgeries is one of the most active research topics in the forensics literature, and has already resulted in multiple efficient algorithms. A review of the variety of existing methods is out of scope of this work. Interested readers are referred to a recent experimental evaluation covering many popular methods [159]. Here, I briefly discuss two generic classes of detection algorithms, and summarize the most recent propositions of their further improvement.

Two main approaches to copy-move detection include: (a) patch-based techniques; (b) key-point-based techniques. The former consider small image patches, and attempt to match each patch to a different one based on some compact content representation, e.g., rotation or scale invariant moments. A cluster of neighboring patches matched to the same source region indicates a potential copy-move forgery. The most important drawback of patch-based techniques consists in their considerable computational complexity. Key-point-based techniques address this limitation by considering rotation and scale-invariant features located in characteristic points of the image, e.g., SIFT or SURF key-points [160]. However, these methods tend to perform poorly in solid areas, where key-points are sparse.

Recently proposed improvements for copy-move detection include incorporation of content segmentation [135], behavioral knowledge space (BKS) fusion [161], fast approximations of the patch-match algorithm [162], and multi-scale analysis [163]. These techniques bring improvements both in terms of computational complexity, and robustness to post-processing.

A key limitation of existing detectors is that by itself, copy-move detection methods cannot distinguish between either naturally occurring self-similarity or even the original and the cloned objects. Additional forensic detectors will be required for this purpose, e.g., sensor noise (Section 4.3) or resampling detectors (Section 4.10.4).

In contrast to previously discussed traces, detection of copy-move forgeries relies on perceptually significant components of image content. Apart from manual editing of the copied objects, I am not aware of automatic tools that could prevent detection of such forgeries in a general case. Key-point based detectors can be attacked by either SIFT key-point insertion or removal [164]. An example Matlab implementation of such an mechanism can be found at [165]. A forensic analysis of the impact of this attack can be found [166]. Patch-based detection methods remain unaffected.

Overall, existing techniques exhibit high maturity and deliver reliable results in varied conditions. Detection algorithms are implemented in commercially available software such as Amped Authenticate [102] and Pizarro [104,148]. Academic implementations for the most recent techniques are also freely available [167–170].

4.10.2. Splicing

Image splicing resembles copy-move forgeries, but the object of interest is copied from a different image. In general, the donor image may have been acquired by a different camera and hence some additional low-level traces are likely to reveal the forgery. Many of the discussed techniques will be effective in detecting and localizing a splicing forgery, including PRNU-based senor noise verification (Section 4.3), JPEG-based traces (Section 4.7), and many others.

A popular approach to splicing detection involves employing natural image models (e.g., pixel co-occurrence features) and training a classifier to distinguish authentic image regions from the ones with a splicing boundary [171]. However, such an approach suffers from the source mismatch problem. Moreover, many datasets available for training contain examples of naive splicing, where the boundary is very sharp and lacks alpha matting or any other masking. At the moment it is not clear whether such an approach would be effective in detecting professionally prepared forgeries.

Some scholars have also proposed unsupervised learning methods, which attempt to identify two distinct natural image models within a single image. Proposed approaches range from expec-

tation maximization (EM)-based clustering [172] to autoencoder-based reconstruction error evaluation [173]. Despite early promising results, these techniques are still experimental. Potential problems include dealing with natural content variations (e.g., sky vs. ground texture) and same-camera tampering sources. I am not aware of publicly available implementations.

4.10.3. Inpainting

Inpainting is an image restoration technique that allows for filling holes in the image. While early approaches were capable of filling only small scratches, or masking sensor defects, the most recent exemplar-based techniques can effectively remove even large objects. Such functionality is available not only in modern professional photo editors, but also in standalone, easy-to-use applications for smart-phones and tablets, e.g., *Touch Retouch* [174].

Exemplar-based inpainting can be viewed as a semi-automatic sophisticated version of a copy-move forgery, where patches are taken from various image regions and blended together for better visual results. Chang et al. [175] proposed an automatic algorithm for detecting such forgeries. In principle the detection method is similar to copy-move forgery detection. The algorithm identifies suspected regions based on perceptually similar image patches. Finally, heuristic rules are used to remove false alarms. To the best of my knowledge, a public implementation of this algorithm is not available.

4.10.4. Resampling

Resampling is a necessary operation when an image undergoes an affine transformation like rescaling, rotation, etc. Since insertion of a foreign object into an image is likely to require at least size adjustments, resampling will necessarily be involved and its traces may indicate a potential forgery. Resampling introduces periodic artifacts manifested by characteristic peaks in a 2-dimensional Fourier spectrum of signal derivative [176]. Adoption of Radon transform allows to detect more general cases of rotation and skewing [177].

The above studies focused on re-sampling detection and did not thoroughly study the impact of analysis window size which is important in tampering localization. Mahdian and Saic used fixed windows of 128×128 px which are too large for detection of small forgeries. A subsequent study has shown that some types of re-sampling, e.g., up-sampling, can be detected by simple high-pass filtering on small image blocks which reveals missing high-frequency components in up-sampled regions of the image [178]. The authors considered both the standard JPEG blocking grid of size 8×8 and a more flexible wavelet transform. In a recent preliminary study Bunk et al. proposed a deep-learning-based framework for re-sampling detection and considered analysis windows between 64×64 px and 128×128 px [179].

Algorithms for detecting traces of resampling are available in the Amped Authenticate [102] and Pizarro [104,148] software. Kirchner and Böhme analyzed three effective methods for hiding the traces of re-sampling: (a) median filtering; (b) geometric distortion with edge modulation; (c) a dual-path approach with different transformation of low-frequency and high-frequency components [180].

4.10.5. Filtering

While global filtering does not necessarily indicate malicious changes to the image content, its detection is important since it may affect the operation of other forensic detectors. This is particularly true for non-linear filters, like the median filter, which is known to affect resampling detectors [180]. Some research also aims to study the joint impact of various global operations, which leads to a deeper understanding of complex processing chains. Conotter et al. studied the case of filtered JPEG images and provided a statistical model for post-processed DCT coefficients [181].

In contrast to unintentional, global post-processing, presence of localized filtering is an important indicator of possible malicious modifications (and also prospective efforts to hide it). Swaminathan et al. studied modeling both in-camera and out-camera post-processing by estimating an image filter with blind deconvolution [125] (see also Section 4.6). They demonstrated that this approach can be used for reliable detection of popular operations like blurring, contrast enhancement, median filtering, etc.

An efficient dedicated technique for detecting localized median filtering was described by Yuan [182], who proposed to construct 5 sub-sets of forensic features to capture different aspects of local dependencies introduced by the filter. These sub-sets are then combined for better performance. The algorithm delivers superior classification accuracy, even when dealing with small image blocks and JPEG-compressed images. The author reported good classification results for block sizes ranging from 16×16 px to 64×64 px, depending on JPEG compression settings. The strongest evaluated quality level was 95.

Chen et al. recently proposed an alternative approach which employs two new feature sets computed in the image difference domain [183]. Compared to previous methods, the new algorithm is more robust to JPEG compression and noise. The authors used analysis windows of size 32×32 px when dealing with uncompressed images, and 64×64 px when the filtered image is post-processed – either by lossy compression or Gaussian noise. A reference academic implementation of this approach is freely available online [184].

Some filtering operations, like contrast enhancement, may also be detected by observing peaks and holes in the image histogram [185]. However, such traces can be efficiently covered up with relevant anti-forensics. The algorithm proposed by Barni et al. [186] involves an optimization procedure for histogram remapping with distortion constraints. The algorithm has a publicly available academic implementation [187]. Anti-forensic techniques also exist for covering traces of median filtering [188]. However, similarly to JPEG-based traces, its use can be detected [189].

4.11. Localization protocols & trade-offs

Local analysis of forensic traces allows to discover inconsistencies characteristic of malicious localized editing. The most common approach involves sliding window analysis, either in an overlapping or non-overlapping manner. Due to statistical nature of many forensic traces, larger window sizes are preferred in order to ensure statistical sufficiency. However, excessively large windows are discouraged as they severely limit the localization resolution and overlook small forgeries. Hence, the choice of analysis window size constitutes an important trade-off in forensic analysis.

Existing detectors differ significantly with respect to their optimal window size. Analysis of CFA traces has been reported to yield good performance with effective resolution of 8×8 px blocks. Detectors of JPEG traces typically operate on windows ranging from 8×8 to 64×64 px. Verification of sensor pattern noise requires even larger windows, with the prevailing choice of 129×129 px. Such windows are already too large for many small or irregularly-shaped forgeries, which motivates seeking better localization protocols.

One way of improving the localization performance involves modeling interactions between neighboring image blocks. The problem can be formulated as a Markov random field, where the final decision is reached by minimizing an energy function with both local preference and interaction terms. As a result, local decisions are no longer independent and confident detector's responses may be propagated to other regions of the image where the foren-

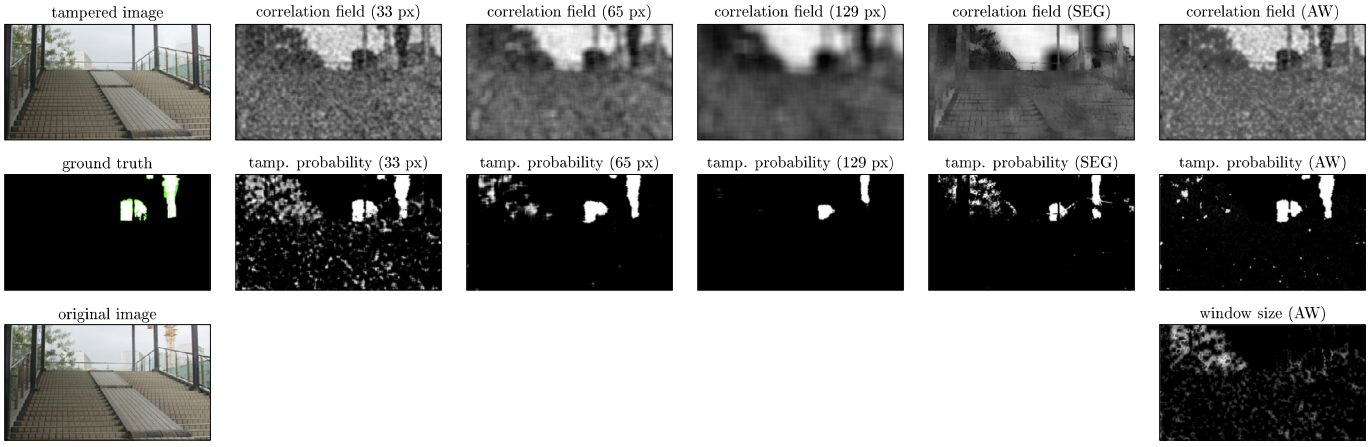

Fig. 10. Example tampering localization results for various multi-scale strategies; the segmentation-guided (SEG) and adaptive-window (AW) strategies (columns 5 and 6) were able to improve shape representation with respect to the standard 129 px window (column 4); at the same time, they were less affected by noise than conventional analysis with smaller windows (e.g., the 33 px window in column 2).

sic feature may be unreliable [90]. Adoption of random fields is still a relatively new approach in tampering localization, and there are no universally accepted models. Depending on the forensic feature at hand, either a generative Markov [90] or a conditional random field [97,100] may be used. It would appear that the latter is often more suitable, as it is more universal and relies on relaxed independence assumptions. A recent study of sensor noise-based localization seems to support this observation [97]. Further considerations include neighborhood interaction models, which may differ in the range of included interactions and their prospective adaptation strategies [190].

Another possible approach is to use manually delineated segments. Chierchia et al. have shown that small forgeries can be detected in this way even with large-window detectors like sensor noise verification [98]. Unfortunately, accurate manual segmentation may be excessively time-consuming and even impossible in case of object removal forgeries with no natural boundaries. A follow up study proposed to address this limitation with guided filtering [99]. The reported results demonstrated clear benefits for smaller forgeries, but virtually no improvement for the ones of the order of 129×129 px or larger. In a recent study, Korus and Huang developed a similar segmentation-guided strategy, but observed consistent improvement also for larger forgeries [100].

Instead of relying on a single fixed window size, tampering localization can also benefit from *multi-scale analysis* [130]. This localization strategy, recently proposed by Korus and Huang, involves forensic analysis with windows of various sizes, and subsequent fusion of the obtained multi-scale candidate maps into a single final decision map. Such an approach aims to combine the benefits of small-scale and large-scale analysis. The original paper studied the problem for MBFDF-based JPEG splicing localization, and demonstrated that a dedicated fusion algorithm obtained better results than any individual candidate window. In a follow-up study, the fusion scheme was generalized to PRNU-based sensor noise verification, and extended with content-adaptive neighborhood interactions [100]. The approach was also compared with alternative multi-scale strategies: (a) a segmentation-guided strategy (SEG) which adapts the shape and size of analysis windows to local segmentation results; (b) adaptive-window strategy (AW) which dynamically changes the window size based on local image content.

Example tampering localization results for various multi-scale strategies used with the PRNU detector are shown in Fig. 10. Columns 2–4 show traditional single scale results with square analysis windows of size 33, 65, and 129 px, respectively. It can be observed that the standard 129 px window leads to coarse detection which poorly reflects the actual shape of the forgery. More accurate results were obtained with smaller windows at the cost of increased noise level. Both of the mentioned SEG and AW multi-scale strategies were able to detect the shape more accurately with only minor deterioration of image-wide noise. Overall, multi-scale analysis is still a new technique in digital image forensics, and further work is needed to validate its benefits for various traces. Existing studies addressed MBFDF traces [130] and PRNU-based sensor noise verification [100]. A recent preliminary study has shown promising results with deep-learning-based splicing detection [191]. A similar approach was also recently proposed for active integrity protection based on robust hash functions [28] (see Section 2.2).

Multi-scale effects can also be observed in multi-clue localization. In case of big differences in analysis window size between the employed detectors (e.g., when CFA and PRNU analyses are performed), the identified regions will differ considerably in shape. Such results will require cross-referencing the identified regions with actual image objects. One possible approach to address this problem is to employ adaptive neighborhood interactions in a random field model [190]. This allows to exploit information about existing image objects leading to improved shape representation and easier detection of small forgeries. At the same time, such an approach does not suffer from object removal forgeries, where the adaptation mechanism falls back to standard, nearly uniform interactions. Further work may be required to extend the approach to more diverse forensic detectors.

Academic implementations of various multi-scale localization strategies [100] can be found online [107]. The provided Matlab toolbox includes a random field model that can also be used for standard single-scale localization with arbitrary detectors. Alternatively, publicly available solvers for general random field models are also available, e.g., the UGM toolbox for Matlab [192].

4.12. Decision fusion protocols

Due to their simplicity, many forensic traces exhibit: (a) limited robustness to lossy compression or global post-processing, (b) questionable security due to the ease of their re-introduction by an attacker. Nevertheless, preparation of a convincing forgery which aims to maintain consistency of all forensic traces is a challenging problem requiring expert knowledge. Hence, reliable forensic analysis requires a multi-clue approach, which aims to reach the final decision by looking at many independent traces. Decision fusion in digital image forensics is an emerging research direction, which has been studied primarily for binary detection problems.

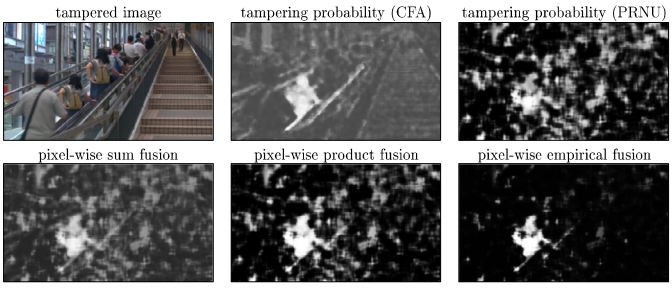

Fig. 11. Example result of pixel-wise decision fusion based on CFA and PRNU analysis; even naive pixel-wise combination rules allow to improve upon individual candidate probability maps.

Three general approaches to the fusion problem include: (a) feature-level fusion; (b) measurement-level fusion; (c) decision-level fusion. The former involves training a single classifier in a concatenated feature space. Due to exponential growth of the training set, such an approach is often impractical. The remaining approaches rely on the outputs of individual forensic detectors, which are trained separately. The measurement-level fusion can be expected to yield somewhat better performance as it allows to capture the confidence level of individual interim decisions.

Two sophisticated frameworks with measurement-level fusion have been proposed based on fuzzy logic [193] and Dempster-Shafer Theory of Evidence (DSTE) [194]. The DSTE can be seen as a generalization of Bayesian probability with enhanced handling of decision uncertainty. Both of the above frameworks provide systematic mechanisms for dealing with compatibility of interim decisions of individual forensic detectors. A recent study discussed possible extension of the DSTE approach to tampering localization [195], but the problem requires further work.

In tampering localization, decision fusion is still an open problem, and most of the reported systems rely on naive pixel-wise application of simple combination rules, or simple heuristics for candidate map selection [196,197]. A recent comparative study has demonstrated that standard product fusion and simple map summation deliver best results among a variety of pixel-wise combination rules [198]. However, due to possible multi-scale effects in multi-clue detectors (see Section 4.11), pixel-wise fusion is clearly sub-optimal. The detected regions will need to be cross-referenced with semantically meaningful objects in the image. A promising approach has recently been discussed based on content-adaptive conditional random fields [190]. However, further work in this direction is required.

An example result of pixel-wise decision fusion is shown in Fig. 11. The image was tampered by means of a copy-move forgery involving duplication of a person on the escalator. The image was subsequently analyzed with CFA and PRNU detectors leading to noisy tampering probability maps. Combination of these candidate maps gives better results, where the tampered region is more easily visible. The figure shows three pixel-wise combination strategies: (left) map summation; (middle) product fusion; (right) empirical fusion based on previously collected joint response statistics [190].

4.13. Future challenges

In addition to the open problems discussed in Sections 4.1–4.12, digital image forensics will need to face rapid advancements in the field of computational imaging. We are currently on a verge of a revolution in digital camera design with two important contenders: (a) light-field photography; (b) multi-sensor and multi-lens cameras. The former relies on capturing not only the intensity, but also the direction of incoming rays. Light-field cameras (e.g., the Lytro Illum [199]) allow for much more versatile post-capture customization, including changing the depth of field, which leads to potentially significant variations in the image content. The fundamentally different image acquisition pipeline will render many existing forensic traces useless. New techniques will be required for forensic analysis of such images.

At first sight, multi-sensor cameras rely on a mostly unaffected acquisition pipeline (Fig. 5). However, the pipeline has a separate instance for each of the lens-sensor pairs, and the final photograph is obtained via image fusion. Multi-sensor cameras range from simple 2-lens setups (commonly seen in high-end smart-phones) up to sophisticated systems with several-dozen sensors. A common 2-lens setup involves two nearly identical cameras, where one is stripped of the CFA in order to deliver a full-resolution luminance component with better low-light performance. Such solutions are integrated into popular smart-phones like LG G5, Huawei P9 and P10, or Xiaomi Mi6. To the best of my knowledge, behavior of existing forensic traces has not yet been evaluated for such camera setups.

In the above 2-sensor configuration it may be expected that some existing techniques may work with only minor modifications. Sensor noise verification is a good example. Some of the reported photo source attribution systems already use combined camera fingerprints to reduce computational complexity [200]. This suggests that it might be possible to effectively deal with mixed fingerprints. However, further work in this direction will be required.

Unfortunately, more sophisticated multi-sensor setups will most likely invalidate many existing forensic traces. A good example is the coming Light L16 camera [201] which is based on a 16-sensor setup with varying focal lengths. Depending on the photo settings, the camera activates various groups of sensors, looking into different directions of the scene. Arbitrary values of focal length are obtained by fusing images stemming from a few fixed lengths provided by the lenses. This variability of sensor activation will invalidate even the most mature approach of sensor noise verification. Moreover, the proprietary *Polar Fusion Engine* responsible for combining interim images is a software module that will evolve over time. Hence, any prospective forensic traces may be affected by a simple firmware update. Designing efficient techniques for working with such cameras is an important problem for future research.

5. Image phylogeny techniques

5.1. General information & analysis capabilities

The problem of image phylogeny is an emerging research direction aiming to recover the relationships and processing history of various versions of an image [202–204]. In case of a forgery, the identified alternative copies may be used as a reference during authentication. Depending on the application at hand, it may be necessary to first identify candidate, near-duplicated images within a larger photo collection. An example application involves analysis of digital photographs that accompany news items online and in social media. Once the images are identified, they are registered by finding either cropping parameters, an affine transform, or a more general homographic projection. Registered images are then normalized with respect to their brightness, color and compression levels. Finally, the images are compared by computing pixel-wise residuals that can also reveal local changes in the image content.

Image phylogeny techniques aim to recover a tree that represents the editing history of an image. If the input set of near-duplicate images contains similar, but distinct photographs (e.g., taken in a different moment in time or with a different camera), it may be more appropriate to recover a forest, i.e., a set of trees that correspond to distinct image clusters [203]. This approach may require some user interaction to determine the number of

clusters [202]. The ability to automatically recover the number of clusters is the subject of ongoing research [205].

5.2. Analysis techniques

Image phylogeny techniques rely on the following general steps: (a) finding near-duplicate images in a large photo collection; (b) image registration; (c) image normalization (brightness, color, compression); (d) image comparison and generation of a (dis)similarity matrix; (e) clustering; (f) phylogeny tree/forest reconstruction. Most of these steps correspond to well-known problems from computer vision and computational imaging. Near-duplicate images can be obtained with a plethora of algorithms for robust image retrieval, including solutions based on robust hash functions described in Section 2.2. Image registration is commonly performed by means of SIFT/SURF feature extraction followed by RANSAC for finding the homographic projection. Image normalization also relies on popular algorithms like the color transfer technique. The following step of image clustering can be performed with unsupervised learning methods like manifold learning or spectral clustering [205].

The novelty of image phylogeny consists in the problem of reconstructing a tree/forest of inter-image relationships. The tree is built based on an asymmetric dissimilarity matrix obtained as a result of image comparison. The utilized distance metric is computed from pixel-wise residuals of registered and normalized images. The phylogeny tree can be obtained by the Oriented-Kruskal algorithm that recovers the minimal spanning tree [206]. The core of computational complexity resides in computing the dissimilarity matrix. In order to allow for operation on large image sets, it becomes necessary to consider sparse matrices with appropriate heuristics for on-demand dissimilarity computation [202].

5.3. Fundamental limitations & open problems

While image phylogeny allows to recover the relationships between near-duplicate images and observe how the image was changed over time, it does not answer questions about image integrity. Other techniques will need to be used to validate the integrity of the original (root) image. Hence, image phylogeny is not an end-to-end solution and is aimed at supporting the decisions made by a human analyst (or a more comprehensive image authentication system).

Furthermore, to the best of my knowledge, there are no algorithms that would allow to cross-reference semantic content from separate trees in a forest. For example, if the same event is covered by multiple photographers, the footage from each one could be authenticated based on the corresponding footage from the others. However, such decisions still need to be made manually – at least until scene understanding algorithms reach the necessary level of sophistication.

Phylogeny techniques could also be used for finding donor images where potentially spliced objects may have been taken from. Such algorithms could significantly improve the detection and history of image composition. The issue has recently been discussed by Oliveira et al. [207] who extend the problem of image phylogeny to handle the inherent issues of multiple parenting.

5.4. Available implementations & software

As already discussed, selected sub-problems in image phylogeny rely on various algorithms from computer vision and computational imaging. Hence, implementations of popular building blocks, like image registration, are widely available (e.g., in Matlab or in OpenCV [208]). Selected algorithms for phylogeny tree and forest reconstruction have publicly available academic implementations provided by the authors along with their original papers [209].

6. Alternative experimental techniques

The techniques described in Sections 2–4 represent the most mature approaches to digital image authentication, both from the perspective of active protection and passive verification. However, researchers are still working on alternative ways of addressing the problem. Naveh and Tromer recently described a prototype of an image authentication system based on a Proof-Carrying Data paradigm [210]. Their approach involves definition of a set of allowed image transformations, which generate a proof of authenticity on each processing step. While the technique remains experimental at this stage, it possesses certain interesting properties. The generated proofs can be verified quickly with constant complexity, and reveal no knowledge about the processing history, or the parameters of individual steps.

Li et al. proposed a novel technique based on fixed point theory [211]. The method involves constructing a transformation of digital images with sparsely distributed fixed points that serve as fragile valid images. The authors designed an effective algorithm to project an arbitrary image to the closest fixed-point image. Depending on the transformation, the scheme can deliver either fragile or semi-fragile authentication capabilities.

7. Tools & resources

This section summarizes some of the resources available within the multimedia security community. I briefly introduce publicly available datasets and comprehensive image forensics toolkits. Due to the lack of standardized datasets and publicly available tools for active protection techniques, I focus on passive image forensics.

7.1. Datasets

The digital image forensics community has prepared a number of datasets for evaluating tampering detection and localization systems (Table 1). The datasets differ significantly in quality and diversity of included forgeries. Most of them feature copy-move and naive splicing forgeries, which require relatively little effort and can be generated (semi-)automatically. Some of the most notable copy-move forgery datasets include: (a) the Friedrich–Alexander University (FAU) dataset used in a recent large-scale evaluation of various approaches [159,216]; (b) the COVERAGE dataset which focuses on difficult cases with naturally occurring self-similarity [217].

Popular CASIA [223] and Columbia [224] image splicing datasets are aimed at forgery detection and do not include pixel-level ground truth data. The first version of the CASIA dataset, as well as both CISDE and CUISDE datasets from Columbia contain mainly automatically generated or crudely performed splicing forgeries without blending or alpha matting. As a result, they feature sharp boundaries between authentic and spliced regions which do not appear realistic and cannot be expected in practical forgery cases. The first CASIA dataset was also reported to contain design flaws consisting in non-uniformly chosen JPEG quality settings, which led to overestimated detection capabilities [222]. The second CASIA dataset is a significant step forward both in the number of tampered images and in their realism. However, the dataset is still of mixed quality and features many crude and obvious modifications.

Since preparation of high-quality realistic forgeries is time-consuming, there are few datasets with such images. The most notable include: (a) the image corpus from the image forensics challenge organized by the IEEE Information Forensics and Security Technical Committee (IFS-TC) [215]; (b) realistic people insertion and face forgery dataset by Carvalho et al. [69,213]; (c) a recent realistic forgery dataset by Korus and Huang [21,100]. All

Table 1
Summary of publicly available image tampering datasets. Acronyms: copy-move forgery dataset (CMD); realistic forgery dataset (RFD).

Dataset	Forgery types	# images[a]	Resolution	Image format	Ground truth	Extra materials	Remarks	URL
Wild Web	Various realistic	10,646 in total (80 confirmed forgeries)	Varied	JPG/PNG/GIF/BMP/TIFF	Pixel-level	n/a	Req. registration	[212]
RFD (Carvalho)	Realistic (people)	100 pairs	2048×1536	PNG	Pixel-level	Face coordinates, illuminant maps	n/a	[213]
RFD (Fontani)	Various realistic	69 O + 69 T	320×480–5184×3456	JPG	Image-level, bounding-box	n/a	n/a	[214]
IFS-TC challenge (phase 1)	Various realistic	Train: 1,050 O + 450 T; Test: 5,713	1024×768	PNG (with possible JPEG history)	Pixel-level	n/a	n/a	[215]
RFD (Korus)	Various realistic	220 pairs	1920×1080	Uncompressed TIFF	Pixel-level	PRNU signatures	3-level ground-truth with collateral damage	[21]
FAU CMD	Copy-move	48 O + forgeries	2362×1581–3888×2592	JPG/PNG	Pixel-level	Scripts for generating forgeries, alpha masks for copied objects	Forgeries generated on demand	[216]
COVERAGE	Copy-move	100 pairs	486×400	TIFF	Pixel-level, sep. source & copy	n/a	Focuses on self-similar objects	[217]
GRIP CMD	Copy-move	80 pairs	1024×768	PNG	Pixel-level, just copy	Perl generation scripts, alpha masks for copied objects	n/a	[218]
CoMoFoD	Copy-move	200 O + forgeries	512×512	PNG/JPG	Pixel-level, source & copy	n/a	Larger version req. registration	[219]
CMD (Ardizzone)	Copy-move	50 T	1024×768	BMP	Pixel-level, source & copy	More post-processed images	Naively pasted; varied post-processed subsets	[220]
MICC F8	Copy-move	8 T	800×532–2048×1536	JPG	Image-level	n/a	n/a	[221]
MICC F220	Copy-move	110 O + 110 T	722×480–800×600	JPG	Image-level	n/a	n/a	[221]
MICC F600	Copy-move	440 O + 160 T	800×533–3888×2592	JPG/PNG	Pixel-level	n/a	n/a	[221]
MICC F2000	Copy-move	1,300 O + 700 T	2048×1536	JPG	Image-level	n/a	n/a	[221]
CASIA 1.0	Naive splicing & copy-move	800 O + 921 T	384×256	JPG	Image-level	n/a	Req. registration; Possibly flawed [222]	[223]
CASIA 2.0	Splicing & copy-move	7,491 O + 5,123 T	240×160–800×600	BMP/JPG/TIFF	Image-level	n/a	Req. registration	[223]
CISDE	Naive splicing	912 O + 933 T	128×128	BMP grayscale	Image-level	n/a	Req. registration	[224]
CUISDE (Uncompressed)	Naive splicing	180 O + 180 T	757×568–1152×768	TIFF/BMP	Edge masks	n/a	Req. registration	[224]

[a] Number of included images: Original (O); Tampered (T).

datasets include diverse forgery cases, and provide accurate pixel-level ground truth masks. The latter also includes sensor noise signatures of the involved cameras.

A large-scale challenge that addresses various problems in digital image forensics has recently been organized by NIST [14]. The image corpus contains an impressive number of nearly 17,800 test cases, and a separate set of world images which may have been involved in preparing some of the forgeries. This is the largest image forensics dataset to date. However, it is not freely available and was only provided to the participants of the challenge.

In addition to the datasets with content forgeries, there are also two collections of original, full-resolution digital photographs. The Dresden image database [225] contains over 14,000 JPEG images captured by 73 digital cameras representing 25 unique models. While the dataset was primarily intended for evaluation of source attribution schemes, it is also commonly used for synthetic evaluation in tampering detection/localization studies. A recently published RAISE [226] dataset contains 8,156 RAW images captured by 3 cameras. The current version of the dataset contains duplicated images, and should be pruned before use.

7.2. Commercial & community forensics software

Many of the discussed techniques are already implemented in commercial systems for forensic image analysis. The most comprehensive solution is *Amped Authenticate* (re-branded and available in some markets as *Axon Detect*) [102] which provides tools for convenient manual inspection of image data as well as automatic detectors of many forensic traces, e.g.: sensor noise verification (Section 4.3); JPEG compression anomalies (Section 4.7); and copy-move detection (Section 4.10.1). Automatic forensic detectors are also available in the *Verifeyed* system [103]. In addition to a standalone desktop application, *Verifeyed* also provides a Web service for remote verification of image integrity. A recently presented system *Pizarro* [104,148] implements both conventional forensic detectors, as well as selected image restoration algorithms (e.g., super-resolution, or JPEG artifact removal). A low-cost image forensics toolkit *PhotoDetective* has recently been developed as a result of a successful Kickstarter campaign [227]. The application offers basic tools including lighting direction estimation, compression consistency verification, or meta-data and quantization table analysis.

Open source tools do not provide such comprehensive functionality, but can work well for selected authentication problems. *Ghiro* [151] is a Web application for batch analysis of image meta-data in the forensics context. It includes features like meta-data extraction and analysis, matching against known editing signatures, verification of image-thumbnail consistency, or visualization of image acquisition coordinates. *JPEG Snoop* [154] is a small dedicated application that allows to extract detailed information about JPEG compression settings. The program contains an extensive database of known compression signatures for many cameras and image editors. A free web application *Forensically* [228] delivers a fairly comprehensive toolkit for basic forensic analysis. Available tools include an image magnifier, copy move detection, noise level consistency verification, and meta-data analysis (with thumbnail and JPEG parameters).

Academic implementations of selected algorithms can also be found in supplementary materials to scientific papers. These algorithms are typically provided to ensure research reproducibility and should not be considered as ready-to-use solutions. I have collected known implementations along with the description of individual forensic traces in Section 4. A collection of several popular algorithms can be found in the *Image Forensics Toolbox* for Matlab [116]. The authors have also provided a Web interface, an *Image Verification Assistant*, which allows to run the analysis online [229]. The application presents an interactive view of the generated localization maps and allows to export a report to a PDF document.

8. Summary & discussion

Development of techniques for protection or verification of digital image integrity has been an active research topic for nearly two decades. Available solutions have evolved from general image-agnostic signatures, through sophisticated active protection mechanisms capable of tampering localization and content recovery, up to passive forensic methods that analyze imperceptible telltales left in the image during its acquisition or subsequent post-processing. An emerging field of image phylogeny aims to reconstruct the editing history of digital images from a set of near-duplicate copies. Such an approach gives invaluable context to the investigated images and may support the authentication process beyond integrity verification.

Unfortunately, none of existing methods delivers an ideal and comprehensive solution to real-world image authentication problems. In order to give an accessible general perspective on the capabilities and the limitations of individual approaches, I've summarized this information in Table 2. Note that the table refers to general classes of methods and not to specific algorithms or their implementations. For this reason, and for the sake of presentation clarity, the table inherently contains certain simplifications and generalization. As a result, this summary should be viewed with the perspective of general tendencies and broad expectations towards specific approaches. The lack of certain features may stem either from technical limitations of the involved traces or methods, or simply from the lack of such functionality in scientific communications. For more detailed information, the readers are referred to corresponding sections of this survey, and to the original research papers.

The main limitation of active protection techniques consists in the necessity to prepare a protected image upon its acquisition. This is an unrealistic requirement for many applications, and may be feasible mainly for controlled work-flows. Moreover, current experience of leading camera manufacturers demonstrates that correct deployment of such methods is non-trivial, as protection keys may be extracted from the acquisition device. However, due to complex post-processing that is currently common in digital photography, active protection techniques may still be considered as a viable approach. Protection may be applied to the final images regardless of their processing history, and the authentication procedure will verify image integrity with respect to that point in time. Hence, such protection will essentially require a further shift of trust from the acquisition device to the photographer.

In some applications active protection and passive verification can coexist. Once the final image is protected and saved as a JPEG file for archiving or future dissemination, both the embedded signature and relevant forensic traces (e.g., JPEG traces, or post-processing traces) can be used for image authentication. It would be interesting to analyze the potential for such joint analysis. Intelligently designed watermarks can facilitate forensic analysis, as demonstrated in a recent interesting study which constructed telltale watermarks for precisely counting JPEG compression steps [230].

Forensic techniques allow us to reason about image integrity based on our extensive knowledge of the photo acquisition pipeline. Unfortunately, these acquisition-based traces are often destroyed either during post-processing or re-compression. As a result, despite massive interest from the research community, few techniques have reached sufficient maturity for use in regular forensic practice. A recent evaluation on Web images has demonstrated unreliable performance of existing detectors [12] in uncontrolled con-

Table 2
High-level summary of the features provided by available protection and verification techniques.

Method/trace	Maturity[a]	Reference data carrier	Source attribution[b]	Robustness	Geometry recovery	Localization resolution	Recovery (quality)	Automaticity[c]	Remarks	Attack difficulty[d]	Software[e]
Signature verification											
Generic crypt. signatures	High	Meta-data	–	No	No	–	–	A	Only binary decision	Hard	C
Robust signatures	High	Meta-data	–	Yes	Possible	Variable	–	A	Loc. resolution vs. hash length	Hard	–
Distributed source coding	Low	Ext. server	–	Yes	Yes	Precise	–	A	Needs an external server	–	–
Authentication watermarking											
Fragile watermarking	High	Content	–	No	No	Very precise	–	A	Key rotation needed	Hard	–
Semi-fragile watermarking	High	Content	–	Yes	Possible	Precise-Medium	–	A	Key rotation needed	Hard	–
Self-recovery	High	Content	–	No	No	Very precise	High	A	Key rotation needed	Hard	A
Semi-fragile self-recovery	Low	Content	–	Yes	No	Medium	Coarse	A	Key rotation needed	Hard	–
Forensic analysis : physical and optical integrity											
Lighting	High	–	–	Yes	No	Object-level	–	M/S	Direction or color	Artistic	A
Shadows	Low	–	–	Yes	No	Object-level	–	M/S	Needs simple lighting	Artistic	–
Geometry & perspective	Medium	–	–	Yes	No	Object-level	–	M/S	Sensitive to camera position	Artistic	–
Chromatic aberration	High	–	–	Yes	Yes	Coarse	–	A	Compensated by cameras	Easy	–
Radial lens distortion	Low	–	–	Yes	No	Edge-level	–	A	Compensated by cameras	Easy	–
Blur (motion/DoF)	Low	–	–	Yes	No	Medium	–	S	Problems with mixed blur	Artistic	–
Forensic analysis : digital acquisition integrity											
Sensor noise	High	–	D	Yes	Yes	Medium–Coarse	–	A	Needs per-camera models	Easy	C/A
Noise level	Medium	–	–	Limited	No	Precise–Medium	–	S/A	Tampered/authentic ambiguity	Easy	C/A
Demosaicing	Medium	–	M/C	Limited	No	Very precise	–	A	Often assume simple demosaicing	Easy	C/A
In-camera processing	Low	–	M/C	Limited	No	Segment-level/Coarse	–	A	Learns a camera processing model	–	–
JPEG traces	High	–	–	Yes	No	Precise–Medium	–	A	Problems for JPEG quality $Q_2 \leq Q_1$	Easy	C/A
Meta-data & thumbnail	High	–	M/C	Yes	Yes	Coarse (thumb.)	Thumbnail	A	Easily removable/editable	Easy	C/O
Natural image models	Medium	–	M/C/R	Limited	No	Precise–Medium	–	A	Source mismatch problem	–	A
Forensic analysis : processing & forgery traces											
Copy move	High	–	–	Yes	No	Precise, object-level	–	A	Source/target ambiguity	Artistic	C/A
Splicing	High	–	–	Limited	No	Medium	–	A	Source mismatch problem	Artistic	A
Inpainting	Low	–	–	No	No	Medium–Coarse	–	A	Problems for small forgeries	Artistic	A
Resampling	High	–	–	Limited	No	Very precise–Coarse	–	A	Easier for up-sampling	Easy	–
Filtering	High	–	–	Yes	No	Precise–Coarse	–	A	Performance depends on the filter	Easy	C/A
Contextual information analysis											
Image phylogeny	Medium	–	–	Yes	Yes	Very precise	Root image	S	Requires a set of near-duplicate images and further analysis	–	A

[a] Perceived maturity stems from the volume of available studies, recency, availability of software, etc.
[b] Source attribution: (D) device; (M) camera model; (C) computer graphics detection; (R) re-capture detection.
[c] Automaticity: (A) automatic; (S) semi-automatic or supported; (M) manual.
[d] Attack difficulty based on reported vulnerabilities: (Hard) hard to perform, no publicly available software; (Easy) easy to implement or automatic software available; (Artistic) requires manual artistic skills.
[e] Publicly available software: (A) academic; (C) commercial; (O) open-source.

ditions. Hence, analysis of Web images seems to proceed towards image phylogeny [202], and reconstruction of image dissemination and processing history from various copies available online. This observation seems to be supported by a recent large-scale evaluation in the Nimble challenge organized by NIST. Conventional acquisition-based traces delivered poor performance, and reliable results were obtained only after identifying the original image among a million of possible candidates [15]. Unfortunately, it is typically not known which image is the original one, or whether it is available at all.

Acquisition-based forensic traces are better suited to image authentication in near-acquisition conditions, e.g., when analyzing a full-resolution image, allegedly representing unaltered capture of a digital camera. Such is the case, e.g., in photo journalism where newspapers may demand original images from their photographers. Even in this case, however, passive analysis may be challenging. Many of the reported traces are very simple and can be re-introduced to a forged image by a skillful attacker. It is currently believed that it is difficult to prepare a convincing forgery that could conceal all traces. Hence, a lot of hope is directed towards decision fusion methods that could integrate multiple sources of evidence. However, such techniques are still in their early stage, especially for tampering localization problems.

Despite extensive research efforts, the research community still does not have a solid understanding of what is most useful in practical forensic analysis. There are no widely accepted evaluation protocols or performance measures and the existing ones may poorly reflect on the actual utility of the localization results [190]. Existing studies adopt simple pixel-wise measures like true/false positive/negative rates, precision, recall, accuracy, or F_1 measure. Such metrics are inherently sub-optimal as they ignore spatial relationships in the localization map. Distribution of errors may change the meaning of the result and impact the utility of the detector's response map to the analyst. Similar issues have already been studied in the context of image segmentation [231–233], but have not yet been incorporated to best-practices in forensic evaluation protocols.

Another considerable difficulty in digital forensics research resides in the lack of proper datasets. Apart from the singular well-defined problem of copy-move detection, where reasonable forgery samples with arbitrary post-processing may be generated automatically based on templates, there are no large-scale datasets with realistic forgeries that could be studied in similarly varied conditions. Preparing high-quality forgeries that could potentially be faced during high-profile investigations requires large amounts of time and skills. The recently launched MediFor program sponsored by DARPA aims to address this issue and provide a large-scale dataset for the forensics community [13].

Finally, in the nearest future digital image forensics will need to face the challenge of rapid developments in computational imaging. Among problems with increasingly sophisticated editing techniques, it will it be necessary to deal with multi-sensor acquisition which starts to get traction in the smart-phone market. It will be important to design techniques that can work not only for static 2-sensor setups but also in complex, dynamic multi-sensor systems. If such setups will indeed invalidate most of existing acquisition-based traces, we will need to rethink our current approach to ensuring digital image integrity.

References

[1] Adobe Sensei, http://www.adobe.com/sensei.html, visited 11 Apr. 2017.
[2] FaceApp, https://www.faceapp.com/, visited 11 Apr. 2017.
[3] Adobe Sky Replace, https://research.adobe.com/sky-replace/, visited 11 Apr. 2017.
[4] F. Luan, S. Paris, E. Shechtman, K. Bala, Deep photo style transfer, arXiv preprint arXiv:1703.07511, 2017.
[5] Xiaomi Selfie Beautification, http://www.businessinsider.com/xiaomi-selfie-beautification-2015-2?IR=T, visited 11 Apr. 2017.
[6] V. Schetinger, M. Oliveira, R. da Silva, T. Carvalho, Humans are easily fooled by digital images, arXiv preprint arXiv:1509.05301, 2015, https://arxiv.org/abs/1509.05301.
[7] Nikon image authentication software, http://imaging.nikon.com/lineup/software/img_auth/, visited 9 Apr. 2017.
[8] Canon's original data security kit, http://www.canon.co.jp/imaging/osk/osk-e3/index.html, visited 9 Apr. 2017.
[9] I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, Digital Watermarking and Steganography, 2nd edition, Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2007.
[10] J. Fridrich, M. Goljan, Images with self-correcting capabilities, in: Proc. of IEEE Int. Conf. Image Process, 1999, http://dx.doi.org/10.1109/ICIP.1999.817228.
[11] P. Blythe, J. Fridrich, Secure digital camera, in: Digital Forensic Research Workshop, 2004, pp. 11–13.
[12] M. Zampoglou, S. Papadopoulos, Y. Kompatsiaris, Large-scale evaluation of splicing localization algorithms for web images, Multimed. Tools Appl. 76 (4) (2017) 4801–4834, http://dx.doi.org/10.1007/s11042-016-3795-2.
[13] DARPA media forensics program, http://www.darpa.mil/program/media-forensics, visited 24 May 2017.
[14] NIST Nimble Image Forensics Challenge 2017, https://www.nist.gov/itl/iad/mig/nimble-challenge-2017-evaluation.
[15] J. Brogan, P. Bestagini, A. Bharati, A. Pinto, D. Moreira, K. Bowyer, P. Flynn, A. Rocha, W. Scheirer, Spotting the difference: context retrieval and analysis for improved forgery detection and localization, arXiv preprint arXiv:1705.00604, https://arxiv.org/abs/1705.00604.
[16] Scientific Working Group Imaging Technology, Best practices for image authentication, https://www.swgit.org/pdf/Section%2014%20Best%20Practices%20for%20Image%20Authentication?docID=39, version 1.1, 2013.01.11.
[17] M. Stamm, M. Wu, K. Liu, Information forensics: an overview of the first decade, IEEE Access 1 (2013) 167–200, http://dx.doi.org/10.1109/access.2013.2260814.
[18] A. Piva, An overview on image forensics, in: ISRN Signal Processing, 2013, 496701, http://dx.doi.org/10.1155/2013/496701.
[19] G.K. Birajdar, V.H. Mankar, Digital image forgery detection using passive techniques: a survey, Digit. Investig. 10 (3) (2013) 226–245, http://dx.doi.org/10.1016/j.diin.2013.04.007.
[20] M.A. Qureshi, M. Deriche, A bibliography of pixel-based blind image forgery detection techniques, Signal Process. Image Commun. 39 (2015) 46–74.
[21] Realistic Forgery Dataset, http://kt.agh.edu.pl/~korus/downloads/dataset-realistic-tampering/.
[22] G.L. Friedman, The trustworthy digital camera: restoring credibility to the photographic image, IEEE Trans. Consum. Electron. 39 (4) (1993) 905–910, http://dx.doi.org/10.1109/30.267415.
[23] OpenSSL, https://www.openssl.org/.
[24] Motorola MTP6750 Tetra Portable Radio, https://www.motorolasolutions.com/en_xa/products/dimetra-tetra/terminals/portable-terminals/mtp6000/mtp6750.html, visited 14 Apr. 2017.
[25] Photo Proof by KeeeX, https://keeex.me/solutions/mobile/photo-proof/, visited 13 Apr. 2017.
[26] Canon original data security system compromised: ElcomSoft discovers vulnerability, https://www.elcomsoft.com/PR/canon_101130_en.pdf, 2010, visited 13 Apr. 2017.
[27] Elcomsoft discovers vulnerability in Nikon's image authentication system, https://www.elcomsoft.com/PR/nikon_110428_en.pdf, 2011, visited 13 Apr. 2017.
[28] C.P. Yan, C.M. Pun, Multi-scale difference map fusion for tamper localization using binary ranking hashing, IEEE Trans. Inf. Forensics Secur. 12 (9) (2017) 2144–2158, http://dx.doi.org/10.1109/TIFS.2017.2699942.
[29] S.-H. Han, C.-H. Chu, Content-based image authentication: current status, issues, and challenges, Int. J. Inf. Secur. 9 (1) (2010) 19–32, http://dx.doi.org/10.1007/s10207-009-0093-2.
[30] V. Monga, M. Mihcak, Robust and secure image hashing via non-negative matrix factorizations, IEEE Trans. Inf. Forensics Secur. 2 (3) (2007) 376–390, http://dx.doi.org/10.1109/tifs.2007.902670.
[31] C. Lin, S. Chang, A robust image authentication method distinguishing JPEG compression from malicious manipulation, IEEE Trans. Circuits Syst. Video Technol. 11 (2) (2001) 153–168, http://dx.doi.org/10.1109/76.905982.
[32] J. Fridrich, M. Goljan, Robust hash functions for digital watermarking, in: Proc. Int. Conf. Information Technology: Coding and Computing, 2000, pp. 178–183, http://dx.doi.org/10.1109/ITCC.2000.844203.
[33] A. Swaminathan, Y. Mao, M. Wu, Robust and secure image hashing, IEEE Trans. Inf. Forensics Secur. 1 (2) (2006) 215–230, http://dx.doi.org/10.1109/TIFS.2006.873601.
[34] O. Altun, G. Sharma, M. Celik, M. Bocko, A set theoretic framework for watermarking and its application to semifragile tamper detection, IEEE Trans. Inf. Forensics Secur. 1 (4) (2006) 479–492, http://dx.doi.org/10.1109/TIFS.2006.885018.

[35] Y. Mao, M. Wu, Unicity distance of robust image hashing, IEEE Trans. Inf. Forensics Secur. 2 (3) (2007) 462–467, http://dx.doi.org/10.1109/tifs.2007.902260.

[36] pHash – the Open Source Perceptual Hash Library, http://www.phash.org/, visited 13 Apr. 2017.

[37] Y.C. Lin, D. Varodayan, B. Girod, Image authentication using distributed source coding, IEEE Trans. Image Process. 21 (1) (2012) 273–283, http://dx.doi.org/10.1109/TIP.2011.2157515.

[38] X. Zhang, S. Wang, Fragile watermarking with error free restoration capability, IEEE Trans. Multimedia 10 (8) (2008), http://dx.doi.org/10.1109/TMM.2008.2007334.

[39] X. Zhang, S. Wang, Statistical fragile watermarking capable of locating individual tampered pixels, IEEE Signal Process. Lett. 14 (10) (2007) 727–730, http://dx.doi.org/10.1109/LSP.2007.896436.

[40] P. Meerwald, A. Uhl, Watermarking of raw digital images in camera firmware, IPSJ Trans. Comput. Vis. Appl. 2 (2010) 16–24, http://dx.doi.org/10.2197/ipsjtcva.2.16.

[41] P. Korus, J. Bialas, A. Dziech, Towards practical self-embedding for JPEG-compressed digital images, IEEE Trans. Multimed. 17 (2) (2015) 157–170, http://dx.doi.org/10.1109/TMM.2014.2368696.

[42] P. Korus, J. Białas, A. Dziech, Iterative filtering for semi-fragile self-recovery, in: IEEE Int. Workshop Inf. Forensics and Security, 2014, pp. 36–41, http://dx.doi.org/10.1109/WIFS.2014.7084300.

[43] H. He, F. Chen, H.-M. Tai, T. Kalker, J. Zhang, Performance analysis of a block-neighborhood-based self-recovery fragile watermarking scheme, IEEE Trans. Inf. Forensics Secur. 7 (1) (2012) 185–196, http://dx.doi.org/10.1109/TIFS.2011.2162950.

[44] Y. Huo, H. He, F. Chen, Alterable-capacity fragile watermarking scheme with restoration capability, Opt. Commun. 285 (2012) 1759–1766, http://dx.doi.org/10.1016/j.optcom.2011.12.044.

[45] M.J. Holliman, N.D. Memon, Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes, IEEE Trans. Image Process. 9 (3) (2000) 432–441, http://dx.doi.org/10.1109/83.826780.

[46] H. He, J. Zhang, H. Tai, Self-recovery fragile watermarking using block-neighborhood tampering characterization, in: Information Hiding, in: Lect. Notes Comput. Sci., vol. 5806, Springer, 2009, pp. 132–145.

[47] C. Chang, Y. Fan, W. Tai, Four-scanning attack on hierarchical digital watermarking method for image tamper detection and recovery, Pattern Recognit. 41 (2) (2008) 654–661, http://dx.doi.org/10.1016/j.patcog.2007.06.003.

[48] H. He, J. Zhang, Cryptoanalysis on majority-voting based self-recovery watermarking scheme, in: Proc. Int. Conf. on Multimedia Information Networking and Security, 2009, http://dx.doi.org/10.1109/MINES.2009.218.

[49] P. Korus, A. Dziech, Efficient method for content reconstruction with self-embedding, IEEE Trans. Image Process. 22 (3) (2013) 1134–1147, http://dx.doi.org/10.1109/TIP.2012.2227769.

[50] P. Korus, A. Dziech, Adaptive self-embedding scheme with controlled reconstruction performance, IEEE Trans. Inf. Forensics Secur. 9 (2) (2014) 169–181, http://dx.doi.org/10.1109/TIFS.2013.2295154.

[51] X. Zhang, S. Wang, Z. Qian, G. Feng, Self-embedding watermark with flexible restoration quality, Multimed. Tools Appl. 54 (2011) 385–395, http://dx.doi.org/10.1007/s11042-010-0541-z.

[52] X. Zhang, S. Wang, Z. Qian, G. Feng, Reference sharing mechanism for watermark self-embedding, IEEE Trans. Image Process. 20 (2) (2011) 485–495, http://dx.doi.org/10.1109/TIP.2010.2066981.

[53] X. Zhang, Z. Qian, Y. Ren, G. Feng, Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction, IEEE Trans. Inf. Forensics Secur. 6 (4) (2011) 1223–1232, http://dx.doi.org/10.1109/TIFS.2011.2159208.

[54] S. Sarreshtedari, M.A. Akhaee, A source-channel coding approach to digital image protection and self-recovery, IEEE Trans. Image Process. 24 (7) (2015) 2266–2277, http://dx.doi.org/10.1109/TIP.2015.2414878.

[55] A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, A secure and improved self-embedding algorithm to combat digital document forgery, Signal Process. 89 (12) (2009) 2324–2332, http://dx.doi.org/10.1016/j.sigpro.2009.02.001.

[56] X. Zhu, A.T. Ho, P. Marziliano, A new semi fragile image watermarking with robust tampering restoration using irregular sampling, Signal Process., Image Commun. 22 (5) (2007), http://dx.doi.org/10.1016/j.image.2007.03.004.

[57] Aucom surveillance system with watermarking-based protection, http://www.aucom.com.au/page/Complete-Packages/4-Security-Camera-Kit.htm, visited 22 May 2017.

[58] H. Kruegle, CCTV Surveillance: Video Practices and Technology, Butterworth-Heinemann, 2011.

[59] I.J. Cox, G. Doërr, T. Furon, Watermarking is not cryptography, in: Y. Shi, B. Jeon (Eds.), Digital Watermarking, in: Lect. Notes Comput. Sci., vol. 4283, Springer, Berlin, Heidelberg, 2006, pp. 1–15, http://dx.doi.org/10.1007/11922841_1.

[60] P. Korus, Homepage, http://kt.agh.edu.pl/~korus/.

[61] M. Chen, J. Fridrich, M. Goljan, J. Lukas, Determining image origin and integrity using sensor noise, IEEE Trans. Inf. Forensics Secur. 3 (1) (2008) 74–90, http://dx.doi.org/10.1109/TIFS.2007.916285.

[62] F. Marra, G. Poggi, C. Sansone, L. Verdoliva, A study of co-occurrence based local features for camera model identification, Multimed. Tools Appl. (2016) 1–17, http://dx.doi.org/10.1007/s11042-016-3663-0.

[63] T. Thongkamwitoon, H. Muammar, P.L. Dragotti, An image recapture detection algorithm based on learning dictionaries of edge profiles, IEEE Trans. Inf. Forensics Secur. 10 (5) (2015) 953–968, http://dx.doi.org/10.1109/TIFS.2015.2392566.

[64] J. Fridrich, Digital image forensics, IEEE Signal Process. Mag. 26 (2) (2009) 26–37, http://dx.doi.org/10.1109/MSP.2008.931078.

[65] H. Farid, Image forgery detection, IEEE Signal Process. Mag. 26 (2) (2009) 16–25, http://dx.doi.org/10.1109/MSP.2008.931079.

[66] A. Ho, S. Li, Handbook of Digital forensics of Multimedia Data and Devices, John Wiley & Sons, 2015.

[67] H. Sencar, N. Memon, Digital Image Forensics – There is More to a Picture than Meets the Eye, Springer, 2013.

[68] M.K. Johnson, H. Farid, Exposing digital forgeries in complex lighting environments, IEEE Trans. Inf. Forensics Secur. 2 (3) (2007) 450–461, http://dx.doi.org/10.1109/TIFS.2007.903848.

[69] T. Carvalho, C. Riess, E. Angelopoulou, H. Pedrini, A. Rocha, Exposing digital image forgeries by illumination color classification, IEEE Trans. Inf. Forensics Secur. 8 (7) (2013) 1182–1194, http://dx.doi.org/10.1109/TIFS.2013.2265677.

[70] W. Zhang, X. Cao, J. Zhang, J. Zhu, P. Wang, Detecting photographic composites using shadows, in: Proc. IEEE Int. Cong. Multimedia and Expo, IEEE, 2009, pp. 1042–1045, http://dx.doi.org/10.1109/icme.2009.5202676.

[71] Q. Liu, X. Cao, C. Deng, X. Guo, Identifying image composites through shadow matte consistency, IEEE Trans. Inf. Forensics Secur. 6 (3) (2011) 1111–1122, http://dx.doi.org/10.1109/tifs.2011.2139209.

[72] V. Conotter, G. Boato, H. Farid, Detecting photo manipulation on signs and billboards, in: IEEE Int. Conf. Image Process, 2010, pp. 1741–1744, http://dx.doi.org/10.1109/ICIP.2010.5652906.

[73] W. Zhang, X. Cao, Y. Qu, Y. Hou, H. Zhao, C. Zhang, Detecting and extracting the photo composites using planar homography and graph cut, IEEE Trans. Inf. Forensics Secur. 5 (3) (2010) 544–555, http://dx.doi.org/10.1109/TIFS.2010.2051666.

[74] H. Yao, S. Wang, Y. Zhao, X. Zhang, Detecting image forgery using perspective constraints, IEEE Signal Process. Lett. 19 (3) (2012) 123–126, http://dx.doi.org/10.1109/lsp.2011.2182191.

[75] M. Iuliani, G. Fabbri, A. Piva, Image splicing detection based on general perspective constraints, in: Proc. IEEE Int. Conf. Information Forensics and Security, IEEE, 2015, pp. 1–6, http://dx.doi.org/10.1109/wifs.2015.7368598.

[76] C. Riess, M. Unberath, F. Naderi, S. Pfaller, M. Stamminger, E. Angelopoulou, Handling multiple materials for exposure of digital forgeries using 2-d lighting environments, Multimed. Tools Appl. (2016) 1–18, http://dx.doi.org/10.1007/s11042-016-3655-0.

[77] B. Peng, W. Wang, J. Dong, T. Tan, Optimized 3D lighting environment estimation for image forgery detection, IEEE Trans. Inf. Forensics Secur. 12 (2) (2017) 479–494, http://dx.doi.org/10.1109/TIFS.2016.2623589.

[78] Illumination color classification (c++ code), https://github.com/tiagojc/IBTSFIF.

[79] 3D lighting environment estimation (Matlab code), https://github.com/bomb2peng/CASIA_3Dlighting.

[80] M. Johnson, H. Farid, Exposing digital forgeries through chromatic aberration, in: Proc. ACM Workshop on Multimedia and Security, 2006, pp. 48–55, http://dx.doi.org/10.1145/1161366.1161376.

[81] H.R. Chennamma, L. Rangarajan, Image splicing detection using inherent lens radial distortion, arXiv preprint arXiv:1105.4712, 2011, https://arxiv.org/abs/1105.4712.

[82] P. Kakar, N. Sudha, W. Ser, Exposing digital image forgeries by detecting discrepancies in motion blur, IEEE Trans. Multimed. 13 (3) (2011) 443–452, http://dx.doi.org/10.1109/tmm.2011.2121056.

[83] M.P. Rao, A.N. Rajagopalan, G. Seetharaman, Harnessing motion blur to unveil splicing, IEEE Trans. Inf. Forensics Secur. 9 (4) (2014) 583–595, http://dx.doi.org/10.1109/TIFS.2014.2302895.

[84] K. Bahrami, A.C. Kot, L. Li, H. Li, Blurred image splicing localization by exposing blur type inconsistency, IEEE Trans. Inf. Forensics Secur. 10 (5) (2015) 999–1009, http://dx.doi.org/10.1109/TIFS.2015.2394231.

[85] O. Mayer, M. Stamm, Anti-forensics of chromatic aberration, in: SPIE/IS&T Electronic Imaging, International Society for Optics and Photonics, 2015, 94090M, http://dx.doi.org/10.1117/12.2182457.

[86] M.P. Rao, S.M. Prabhu, A. Rajagopalan, G. Seetharaman, Camouflaging motion blur: art or science?, in: Proc. Indian Conf. Computer Vision Graphics and Image Processing, ACM, 2014, p. 84, http://dx.doi.org/10.1145/2683483.2683568.

[87] M. Goljan, J. Fridrich, T. Filler, Large scale test of sensor fingerprint camera identification, in: IS&T/SPIE Electronic Imaging, 2009, p. 72540I, http://dx.doi.org/10.1117/12.805701.

[88] J.F.M. Goljan, Camera identification from scaled and cropped images, in: SPIE – Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents, 2008.

[89] X. Kang, Y. Li, Z. Qu, J. Huang, Enhancing source camera identification performance with a camera reference phase sensor pattern noise, IEEE

Trans. Inf. Forensics Secur. 7 (2) (2012) 393–402, http://dx.doi.org/10.1109/TIFS.2011.2168214.
[90] G. Chierchia, G. Poggi, C. Sansone, L. Verdoliva, A Bayesian-MRF approach for PRNU-based image forgery detection, IEEE Trans. Inf. Forensics Secur. 9 (4) (2014) 554–567, http://dx.doi.org/10.1109/TIFS.2014.2302078.
[91] X. Lin, C. Li, Preprocessing reference sensor pattern noise via spectrum equalization, IEEE Trans. Inf. Forensics Secur. 11 (1) (2016) 126–140, http://dx.doi.org/10.1109/TIFS.2015.2478748.
[92] C.T. Li, Source camera identification using enhanced sensor pattern noise, IEEE Trans. Inf. Forensics Secur. 5 (2) (2010) 280–287, http://dx.doi.org/10.1109/TIFS.2010.2046268.
[93] Y. Hu, C. Jian, C.T. Li, Using improved imaging sensor pattern noise for source camera identification, in: Proc. of IEEE Int. Conf. on Multimedia & Expo, 2010, pp. 1481–1486.
[94] X. Kang, J. Chen, K. Lin, P. Anjie, A context-adaptive SPN predictor for trustworthy source camera identification, Int. J. Image Video Process. 2014 (1) (2014) 1–11, http://dx.doi.org/10.1186/1687-5281-2014-19.
[95] A. Lawgaly, F. Khelifi, Sensor pattern noise estimation based on improved locally adaptive DCT filtering and weighted averaging for source camera identification and verification, IEEE Trans. Inf. Forensics Secur. 12 (2) (2017) 392–404, http://dx.doi.org/10.1109/tifs.2016.2620280.
[96] M. Al-Ani, F. Khelifi, On the SPN estimation in image forensics: a systematic empirical evaluation, IEEE Trans. Inf. Forensics Secur. 12 (5) (2017) 1067–1081, http://dx.doi.org/10.1109/TIFS.2016.2640938.
[97] S. Chakraborty, M. Kirchner, Prnu-based image manipulation localization with discriminative random fields, in: IS&T Electronic Imaging: Media Watermarking, Security and, Forensics, 2017, http://dx.doi.org/10.2352/issn.2470-1173.2017.7.mwsf-333.
[98] G. Chierchia, S. Parrilli, G. Poggi, L. Verdoliva, C. Sansone, PRNU-based detection of small-size image forgeries, in: Proc. of Int. Conf. on Digital Signal Processing, 2011, http://dx.doi.org/10.1109/ICDSP.2011.6004957.
[99] G. Chierchia, D. Cozzolino, G. Poggi, C. Sansone, L. Verdoliva, Guided filtering for PRNU-based localization of small-size image forgeries, in: Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing, 2014, pp. 6231–6235, http://dx.doi.org/10.1109/ICASSP.2014.6854802.
[100] P. Korus, J. Huang, Multi-scale analysis strategies in PRNU-based tampering localization, IEEE Trans. Inf. Forensics Secur. 12 (4) (2017) 809–824, http://dx.doi.org/10.1109/TIFS.2016.2636089.
[101] M. Goljan, J. Fridrich, Sensor-fingerprint based identification of images corrected for lens distortion, in: Proc. SPIE 8303, Media Watermarking, Security, and Forensics, 2012, http://dx.doi.org/10.1117/12.909659.
[102] Axon Detect, https://www.axon.com/products/detect, visited 18 Apr. 2017.
[103] Verifeyed, http://verifeyed.com/documentation/, visited 18 Apr. 2017.
[104] Pizarro, http://pizzaro.utia.cas.cz/, visited 18 Apr. 2017.
[105] Forensic Pathways Image Analyzer, http://www.forensic-pathways.com/forensic-image-analyser/, visited 18 Apr. 2017.
[106] DDE laboratory, http://dde.binghamton.edu/, visited Sept. 2015.
[107] Multi-scale forensic analysis toolbox, https://github.com/pkorus/multiscale-prnu, visited 18 Apr. 2017.
[108] A. Karakücük, A. Dirik, H. Sencar, N. Memon, Recent advances in counter PRNU based source attribution and beyond, in: SPIE/IS&T Electronic Imaging, 2015, 94090N, http://dx.doi.org/10.1117/12.2182458.
[109] J. Entrieri, M. Kirchner, Patch-based desynchronization of digital camera sensor fingerprints, Electron. Imaging 2016 (8) (2016) 1–9, http://dx.doi.org/10.2352/issn.2470-1173.2016.8.mwsf-087.
[110] S. Bayram, H.T. Sencar, N.D. Memon, Seam-carving based anonymization against image & video source attribution, in: Proc. IEEE Int. Workshop Multimedia Signal Processing, 2013, pp. 272–277, http://dx.doi.org/10.1109/mmsp.2013.6659300.
[111] M. Goljan, J. Fridrich, M. Chen, Defending against fingerprint-copy attack in sensor-based camera identification, IEEE Trans. Inf. Forensics Secur. 6 (1) (2011) 227–236, http://dx.doi.org/10.1109/TIFS.2010.2099220.
[112] F. Marra, F. Roli, D. Cozzolino, C. Sansone, L. Verdoliva, Attacking the triangle test in sensor-based camera identification, in: IEEE Int. Conf. Image Processing, 2014, pp. 5307–5311, http://dx.doi.org/10.1109/icip.2014.7026074.
[113] B. Mahdian, S. Saic, Using noise inconsistencies for blind image forensics, Image Vis. Comput. 27 (10) (2009) 1497–1503.
[114] X. Pan, X. Zhang, S. Lyu, Exposing image splicing with inconsistent local noise variances, in: IEEE Int. Conf. Computational Photography, 2012, pp. 1–10, http://dx.doi.org/10.1109/iccphot.2012.6215223.
[115] H. Yao, S. Wang, X. Zhang, C. Qin, J. Wang, Detecting image splicing based on noise level inconsistency, Multimed. Tools Appl. (2016) 1–23, http://dx.doi.org/10.1007/s11042-016-3660-3.
[116] Image forensics toolbox for Matlab, https://github.com/MKLab-ITI/image-forensics, visited 18 Apr. 2017.
[117] A. Popescu, H. Farid, Exposing digital forgeries in color filter array interpolated images, IEEE Trans. Signal Process. 53 (10) (2005) 3948–3959, http://dx.doi.org/10.1109/TSP.2005.855406.
[118] A. Dirik, N. Memon, Image tamper detection based on demosaicing artifacts, in: Proc. of IEEE Int. Conf. on Image Processing, 2009, pp. 1497–1500, http://dx.doi.org/10.1109/ICIP.2009.5414611.
[119] P. Ferrara, T. Bianchi, A. Rosa, A. Piva, Image forgery localization via fine-grained analysis of CFA artifacts, IEEE Trans. Inf. Forensics Secur. 7 (5) (2012) 1566–1577, http://dx.doi.org/10.1109/TIFS.2012.2202227.
[120] M. Kirchner, Efficient estimation of CFA pattern configuration in digital camera images, in: IS&T/SPIE Electronic Imaging, International Society for Optics and Photonics, 2010, p. 754111, http://dx.doi.org/10.1117/12.839102.
[121] Multimedia forensics – communications & signal processing laboratory, http://lesc.det.unifi.it/en/node/187, visited 18 Apr. 2017.
[122] M. Kirchner, R. Böhme, Synthesis of color filter array pattern in digital images, http://dx.doi.org/10.1117/12.805988, 2009.
[123] M. Iuliani, S. Rossetto, T. Bianchi, A. De Rosa, A. Piva, M. Barni, Image counter-forensics based on feature injection, in: IS&T/SPIE Electronic Imaging, International Society for Optics and Photonics, 2014, 902810, http://dx.doi.org/10.1117/12.2042234.
[124] Y.F. Hsu, S.F. Chang, Camera response functions for image forensics: an automatic algorithm for splicing detection, IEEE Trans. Inf. Forensics Secur. 5 (4) (2010) 816–825, http://dx.doi.org/10.1109/TIFS.2010.2077628.
[125] A. Swaminathan, M. Wu, K.R. Liu, Digital image forensics via intrinsic fingerprints, IEEE Trans. Inf. Forensics Secur. 3 (1) (2008) 101–117, http://dx.doi.org/10.1109/tifs.2007.916010.
[126] W. Li, Y. Yuan, N. Yu, Passive detection of doctored JPEG image via block artifact grid extraction, Signal Process. 89 (9) (2009) 1821–1829, http://dx.doi.org/10.1016/j.sigpro.2009.03.025.
[127] Z. Lin, J. He, X. Tang, C.K. Tang, Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis, Pattern Recognit. 42 (11) (2009) 2492–2501, http://dx.doi.org/10.1016/j.patcog.2009.03.019.
[128] T. Bianchi, A. De Rosa, A. Piva, Improved DCT coefficient analysis for forgery localization in JPEG images, in: Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing, 2011, pp. 2444–2447, http://dx.doi.org/10.1109/icassp.2011.5946978.
[129] T. Bianchi, A. Piva, Image forgery localization via block-grained analysis of JPEG artifacts, IEEE Trans. Inf. Forensics Secur. 7 (3) (2012) 1003–1017, http://dx.doi.org/10.1109/TIFS.2012.2187516.
[130] P. Korus, J. Huang, Multi-scale fusion for improved localization of malicious tampering in digital images, IEEE Trans. Image Process. 25 (3) (2016) 1312–1326, http://dx.doi.org/10.1109/TIP.2016.2518870.
[131] I. Amerini, R. Becarelli, R. Caldelli, A. Del Mastio, Splicing forgeries localization through the use of first digit features, in: Proc. of IEEE Int. Workshop on Inf. Forensics and Security, 2014, http://dx.doi.org/10.1109/WIFS.2014.7084318.
[132] G.K. Wallace, The JPEG still picture compression standard, IEEE Trans. Consum. Electron. 38 (1) (1992), xviii–xxxiv.
[133] Independent JPEG Group, http://www.ijg.org/, visited 18 Apr. 2017.
[134] C. Pasquini, F. Pérez-González, G. Boato, A Benford–Fourier JPEG compression detector, in: IEEE Int. Conf. Image Process, 2014.
[135] J. Li, X. Li, B. Yang, X. Sun, Segmentation-based image copy-move forgery detection scheme, IEEE Trans. Inf. Forensics Secur. 10 (3) (2015) 507–518, http://dx.doi.org/10.1109/TIFS.2014.2381872.
[136] B. Li, Y. Shi, J. Huang, Detecting doubly compressed JPEG images by using mode based first digit features, in: Proc. of IEEE Workshop on Multimedia Signal Processing, 2008, pp. 730–735, http://dx.doi.org/10.1109/MMSP.2008.4665171.
[137] F. Huang, J. Huang, Y.Q. Shi, Detecting double JPEG compression with the same quantization matrix, IEEE Trans. Inf. Forensics Secur. 5 (4) (2010) 848–856, http://dx.doi.org/10.1109/tifs.2010.2072921.
[138] J. Yang, J. Xie, G. Zhu, S. Kwong, Y.Q. Shi, An effective method for detecting double JPEG compression with the same quantization matrix, IEEE Trans. Inf. Forensics Secur. 9 (11) (2014) 1933–1942, http://dx.doi.org/10.1109/tifs.2014.2359368.
[139] M.C. Stamm, S.K. Tjoa, S. Lin, K.R. Liu, Undetectable image tampering through JPEG compression anti-forensics, in: Proc. IEEE Int. Conf. Image Processing, IEEE, 2010, pp. 2109–2112, http://dx.doi.org/10.1109/icip.2010.5652553.
[140] M.C. Stamm, K.R. Liu, Anti-forensics of digital image compression, IEEE Trans. Inf. Forensics Secur. 6 (3) (2011) 1050–1065, http://dx.doi.org/10.1109/tifs.2011.2119314.
[141] P. Comesana-Alfaro, F. Pérez-González, Optimal counterforensics for histogram-based forensics, in: Proc. IEEE Int. Conf. Acoust., Speech, and Signal Process, 2013, pp. 3048–3052, http://dx.doi.org/10.1109/icassp.2013.6638218.
[142] G. Valenzise, V. Nobile, M. Tagliasacchi, S. Tubaro, Countering JPEG anti-forensics, in: Proc. IEEE Int. Conf. Image Processing, 2011, pp. 1949–1952, http://dx.doi.org/10.1109/icip.2011.6115854.
[143] M. Stamm, Anti-forensic dither (Matlab code), http://ece.drexel.edu/stamm/research_code/JPEG_AF_Code.rar.
[144] C. Pasquini, G. Boato, JPEG compression anti-forensics based on first significant digit distribution, in: IEEE Int. Workshop Multimedia Signal Processing, IEEE, 2013, pp. 500–505, http://dx.doi.org/10.1109/mmsp.2013.6659339.
[145] M. Kirchner, S. Chakraborty, A second look at first significant digit histogram restoration, in: IEEE Int. Workshop Information Forensics and Security, IEEE, 2015, pp. 1–6, http://dx.doi.org/10.1109/wifs.2015.7368578.
[146] C. Pasquini, P. Comesana-Alfaro, F. Pérez-González, G. Boato, Transportation-theoretic image counterforensics to first significant digit histogram foren-

sics, in: IEEE Int. Conf. Acoustics, Speech and Signal Processing, 2014, pp. 2699–2703, http://dx.doi.org/10.1109/icassp.2014.6854090.
[147] W. Fan, K. Wang, F. Cayre, Z. Xiong, JPEG anti-forensics with improved tradeoff between forensic undetectability and image quality, IEEE Trans. Inf. Forensics Secur. 9 (8) (2014) 1211–1226, http://dx.doi.org/10.1109/TIFS.2014.2317949.
[148] J. Kamenicky, M. Bartos, J. Flusser, B. Mahdian, J. Kotera, A. Novozamsky, S. Saic, F. Sroubek, M. Sorel, A. Zita, et al., Pizzaro: forensic analysis and restoration of image and video data, Forensic Sci. Int. 264 (2016) 153–166, http://dx.doi.org/10.1016/j.forsciint.2016.04.027.
[149] W. Fan, JPEG compression anti-forensics (Matlab code), http://www.cs.dartmouth.edu/~wfan/documents/AFJPG-TIFS14.tar.gz, visited 11 May 2017.
[150] E. Kee, M.K. Johnson, H. Farid, Digital image authentication from JPEG headers, IEEE Trans. Inf. Forensics Secur. 6 (3) (2011) 1066–1075, http://dx.doi.org/10.1109/TIFS.2011.2128309.
[151] Ghiro, http://www.getghiro.org/, visited 18 Apr. 2017.
[152] P. Harvey, ExifTool, https://sno.phy.queensu.ca/phil/exiftool/.
[153] J. Fan, H. Cao, A. Kot, Estimating EXIF parameters based on noise features for image manipulation detection, IEEE Trans. Inf. Forensics Secur. 8 (4) (2013) 608–618, http://dx.doi.org/10.1109/tifs.2013.2249064.
[154] JPEG Snoop, http://www.impulseadventure.com/photo/jpeg-snoop.html, visted 18 Apr. 2017.
[155] X. Qiu, H. Li, W. Luo, J. Huang, A universal image forensic strategy based on steganalytic model, in: ACM Information Hiding and Multimedia Security Workshop, 2014, pp. 165–170, http://dx.doi.org/10.1145/2600918.2600941.
[156] W. Fan, K. Wang, F. Cayre, General-purpose image forensics using patch likelihood under image statistical models, in: Proc. of IEEE Int. Workshop on Inf. Forensics and Security, 2015, http://dx.doi.org/10.1109/wifs.2015.7368606.
[157] P. Bas, Steganography via cover-source switching, in: IEEE Int. Workshop Inf. Forensics Security, 2016, pp. 1–6, http://dx.doi.org/10.1109/WIFS.2016.7823905.
[158] J. Galbally, S. Marcel, J. Fierrez, Biometric antispoofing methods: a survey in face recognition, IEEE Access 2 (2014) 1530–1552, http://dx.doi.org/10.1109/access.2014.2381273.
[159] V. Christlein, C. Riess, J. Jordan, C. Riess, E. Angelopoulou, An evaluation of popular copy-move forgery detection approaches, IEEE Trans. Inf. Forensics Secur. 7 (6) (2012) 1841–1854, http://dx.doi.org/10.1109/TIFS.2012.2218597.
[160] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra, A sift-based forensic method for copy-move attack detection and transformation recovery, IEEE Trans. Inf. Forensics Secur. 6 (3) (2011) 1099–1110, http://dx.doi.org/10.1109/TIFS.2011.2129512.
[161] A. Ferreira, S. Felipussi, C. Alfaro, P. Fonseca, J. Vargas-Muñoz, J.A. dos Santos, A. Rocha, Behavior knowledge space-based fusion for copy–move forgery detection, IEEE Trans. Image Process. 25 (10) (2016) 4729–4742, http://dx.doi.org/10.1109/tip.2016.2593583.
[162] D. Cozzolino, G. Poggi, L. Verdoliva, Efficient dense-field copy&move forgery detection, IEEE Trans. Inf. Forensics Secur. 10 (11) (2015) 2284–2297, http://dx.doi.org/10.1109/TIFS.2015.2455334.
[163] E. Silva, T. Carvalho, A. Ferreira, A. Rocha, Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes, J. Vis. Commun. Image Represent. 29 (2015) 16–32, http://dx.doi.org/10.1016/j.jvcir.2015.01.016.
[164] Y. Li, J. Zhou, A. Cheng, X. Liu, Y.Y. Tang, Sift keypoint removal and injection via convex relaxation, IEEE Trans. Inf. Forensics Secur. 11 (8) (2016) 1722–1735, http://dx.doi.org/10.1109/TIFS.2016.2553645.
[165] Matlab code for sift keypoint removal, https://github.com/YuanmanLi/github-SIFT-Keypoint-Removal-and-Injection-RDG-TPKI.
[166] A. Costanzo, I. Amerini, R. Caldelli, M. Barni, Forensic analysis of SIFT keypoint removal and injection, IEEE Trans. Inf. Forensics Secur. 9 (9) (2014) 1450–1464, http://dx.doi.org/10.1109/TIFS.2014.2337654.
[167] SIFT-based copy-move detection (Matlab code), https://github.com/lambertoballan/sift-forensic, visited 20 Apr. 2017.
[168] GRIP Image Processing Research Group, http://www.grip.unina.it/research/83-image-forensics/90-copy-move-forgery.html, visited 20 Apr. 2017.
[169] BKS-based Copy-move Detection (Matlab code), https://github.com/anselmoferreira/bks-copy-move-detection, visited 20 Apr. 2017.
[170] Multi-scale Copy-move Detection (C++ code), https://github.com/anselmoferreira/copy-move-detection, visited 20 Apr. 2017.
[171] H. Li, W. Luo, X. Qiu, J. Huang, Image forgery localization via integrating tampering possibility maps, IEEE Trans. Inf. Forensics Secur. 12 (5) (2017) 1240–1252, http://dx.doi.org/10.1109/tifs.2017.2656823.
[172] D. Cozzolino, G. Poggi, L. Verdoliva, Splicebuster: a new blind image splicing detector, in: Proc. of IEEE Int. Workshop on Inf. Forensics and Security, 2015, http://dx.doi.org/10.1109/wifs.2015.7368565.
[173] D. Cozzolino, L. Verdoliva, Single-image splicing localization through autoencoder-based anomaly detection, in: Proc. IEEE Int. Workshop Inf. Forensics and Security, IEEE, 2016, http://dx.doi.org/10.1109/wifs.2016.7823921.
[174] A. Soft, Touch Retouch, http://adva-soft.com/products/touch-retouch/, visited 21 Apr. 2017.
[175] I. Chang, J. Yu, C. Chang, A forgery detection algorithm for exemplar-based inpainting images using multi-region relation, Image Vis. Comput. 31 (1) (2013) 57–71, http://dx.doi.org/10.1016/j.imavis.2012.09.002.
[176] M. Kirchner, Fast and reliable resampling detection by spectral analysis of fixed linear predictor residue, in: Proc. ACM workshop on Multimedia and Security, ACM, 2008, pp. 11–20, http://dx.doi.org/10.1145/1411328.1411333.
[177] B. Mahdian, S. Saic, Blind authentication using periodic properties of interpolation, IEEE Trans. Inf. Forensics Secur. 3 (3) (2008) 529–538, http://dx.doi.org/10.1109/TIFS.2004.924603.
[178] S. Prasad, K.R. Ramakrishnan, On resampling detection and its application to detect image tampering, in: Proc. of IEEE Int. Conf. on Multimedia & Expo, 2006, pp. 1325–1328, http://dx.doi.org/10.1109/icme.2006.262783.
[179] J. Bunk, J. Bappy, T. Mohammed, L. Nataraj, A. Flenner, B. Manjunath, S. Chandrasekaran, A. Roy-Chowdhury, L. Peterson, Detection and localization of image forgeries using resampling features and deep learning, arXiv preprint arXiv:1707.00433, https://arxiv.org/abs/1707.00433.
[180] M. Kirchner, R. Bohme, Hiding traces of resampling in digital images, IEEE Trans. Inf. Forensics Secur. 3 (4) (2008) 582–592, http://dx.doi.org/10.1109/tifs.2008.2008214.
[181] V. Conotter, P. Comesana, F. Pérez-González, Forensic detection of processing operator chains: recovering the history of filtered JPEG images, IEEE Trans. Inf. Forensics Secur. 10 (11) (2015) 2257–2269, http://dx.doi.org/10.1109/TIFS.2015.2424195.
[182] H.D. Yuan, Blind forensics of median filtering in digital images, IEEE Trans. Inf. Forensics Secur. 6 (4) (2011) 1335–1345, http://dx.doi.org/10.1109/TIFS.2011.2161761.
[183] C. Chen, J. Ni, J. Huang, Blind detection of median filtering in digital images: a difference domain based approach, IEEE Trans. Image Process. 22 (12) (2013) 4699–4710, http://dx.doi.org/10.1109/tip.2013.2277814.
[184] GLF features for median filtering forensics, https://github.com/ChenglongChen/GLF_Features_for_Median_Filtering_Forensics, visited 23 May 2017.
[185] M. Stamm, K.R. Liu, Blind forensics of contrast enhancement in digital images, in: Proc. IEEE Int. Conf. Image Processing, IEEE, 2008, pp. 3112–3115, http://dx.doi.org/10.1109/icip.2008.4712454.
[186] M. Barni, M. Fontani, B. Tondi, A universal technique to hide traces of histogram-based image manipulations, in: ACM Int. Workshop Multimedia and Security, ACM, 2012, pp. 97–104, http://dx.doi.org/10.1145/2361407.2361424.
[187] V. Laboratory, A universal technique to hide traces of histogram-based image manipulations, http://clem.dii.unisi.it/~vipp/files/software/UniversalHistogramAntiForensics.rar.
[188] Z. Wu, M.C. Stamm, K.R. Liu, Anti-forensics of median filtering, in: IEEE Int. Conf. Acoustics, Speech and Signal Processing, IEEE, 2013, pp. 3043–3047, http://dx.doi.org/10.1109/icassp.2013.6638217.
[189] H. Zeng, T. Qin, X. Kang, L. Liu, Countering anti-forensics of median filtering, in: IEEE Int. Conf. Acoustics, Speech and Signal Processing, IEEE, 2014, pp. 2704–2708, http://dx.doi.org/10.1109/icassp.2014.6854091.
[190] P. Korus, J. Huang, Evaluation of random field models in multi-modal unsupervised tampering localization, in: Proc. of IEEE Int. Workshop on Inf. Forensics and Security, 2016, http://dx.doi.org/10.1109/wifs.2016.7823898.
[191] Y. Liu, Q. Guan, X. Zhao, Y. Cao, Image forgery localization based on multi-scale convolutional neural networks, arXiv preprint arXiv:1706.07842, https://arxiv.org/abs/1706.07842.
[192] M. Schmidt, UGM: a Matlab toolbox for probabilistic undirected graphical models, http://www.cs.ubc.ca/~schmidtm/Software/UGM.html, 2011.
[193] M. Barni, A. Costanzo, Dealing with uncertainty in image forensics: a fuzzy approach, in: Proc. of IEEE Int. Conf. on Acoustics, Speech and Signal Processing, 2012, pp. 1753–1756, http://dx.doi.org/10.1109/ICASSP.2012.6288238.
[194] M. Fontani, T. Bianchi, A. De Rosa, A. Piva, M. Barni, A framework for decision fusion in image forensics based on Dempster–Shafer theory of evidence, IEEE Trans. Inf. Forensics Secur. 8 (4) (2013) 593–607, http://dx.doi.org/10.1109/TIFS.2013.2248727.
[195] P. Ferrara, M. Fontani, T. Bianchi, A. De Rosa, A. Piva, M. Barni, Unsupervised fusion for forgery localization exploiting background information, in: Proc. IEEE Int. Conf. Multimedia & Expo Workshops, 2015, http://dx.doi.org/10.1109/ICMEW.2015.7169770.
[196] L. Gaborini, P. Bestagini, S. Milani, M. Tagliasacchi, S. Tubaro, Multi-clue image tampering localization, in: Proc. of IEEE Int. Workshop on Inf. Forensics and Security, 2014, pp. 125–130, http://dx.doi.org/10.1109/WIFS.2014.7084315.
[197] L. Verdoliva, D. Cozzolino, G. Poggi, A feature-based approach for image tampering detection and localization, in: Proc. of IEEE Int. Workshop on Inf. Forensics and Security, 2014, http://dx.doi.org/10.1109/wifs.2014.7084319.
[198] D. Cozzolino, F. Gargiulo, C. Sansone, L. Verdoliva, Multiple classifier systems for image forgery detection, in: Image Analysis and Processing, in: Lect. Notes Comput. Sci., vol. 8157, 2013, pp. 259–268, http://dx.doi.org/10.1007/978-3-642-41184-7_27.
[199] Lytro Illum Camera, https://illum.lytro.com/illum, visited 24 Apr. 2017.
[200] S. Bayram, H.T. Sencar, N. Memon, Sensor fingerprint identification through composite fingerprints and group testing, IEEE Trans. Inf. Forensics Secur. 10 (3) (2015) 597–612, http://dx.doi.org/10.1109/tifs.2014.2385634.
[201] Light L16 Camera, https://light.co/camera, visited 24 Apr. 2017.
[202] Z. Dias, S. Goldenstein, A. Rocha, Large-scale image phylogeny: tracing image ancestral relationships, IEEE Multimed. 20 (3) (2013) 58–70, http://dx.doi.org/10.1109/mmul.2013.17.

[203] F. Costa, M. Oikawa, Z. Dias, S. Goldenstein, A. de Rocha, Image phylogeny forests reconstruction, IEEE Trans. Inf. Forensics Secur. 9 (10) (2014) 1533–1546, http://dx.doi.org/10.1109/TIFS.2014.2340017.
[204] Z. Dias, S. Goldenstein, A. Rocha, Toward image phylogeny forests: automatically recovering semantically similar image relationships, Forensic Sci. Int. 231 (1) (2013) 178–189, http://dx.doi.org/10.1016/j.forsciint.2013.05.002.
[205] M. Oikawa, Z. Dias, A. Rocha, S. Goldenstein, Manifold learning and spectral clustering for image phylogeny forests, IEEE Trans. Inf. Forensics Secur. 11 (1) (2016) 5–18, http://dx.doi.org/10.1109/TIFS.2015.2442527.
[206] Z. Dias, A. Rocha, S. Goldenstein, Image phylogeny by minimal spanning trees, IEEE Trans. Inf. Forensics Secur. 7 (2) (2012) 774–788, http://dx.doi.org/10.1109/tifs.2011.2169959.
[207] A. Oliveira, P. Ferrara, A. De Rosa, A. Piva, M. Barni, S. Goldenstein, Z. Dias, A. Rocha, Multiple parenting identification in image phylogeny, in: IEEE Int. Conf. Image Process, IEEE, 2014, pp. 5347–5351, http://dx.doi.org/10.1109/icip.2014.7026082.
[208] Open source computer vision library, http://opencv.org/.
[209] Image phylogeny methods (c++ code), http://repo.recod.ic.unicamp.br/public/projects, visited 13 July 2017.
[210] A. Naveh, E. Tromer, Photoproof: cryptographic image authentication for any set of permissible transformations, in: IEEE Symp. Security and Privacy, IEEE, 2016, pp. 255–271, http://dx.doi.org/10.1109/sp.2016.23.
[211] X. Li, X. Sun, Q. Liu, Image integrity authentication scheme based on fixed point theory, IEEE Trans. Image Process. 24 (2) (2015) 632–645, http://dx.doi.org/10.1109/tip.2014.2372473.
[212] Wild Web Dataset, http://mklab.iti.gr/project/wild-web-tampered-image-dataset.
[213] Record research group's datasets, https://recodbr.wordpress.com/code-n-data/.
[214] VIPP Realistic Forgery Dataset, http://clem.dii.unisi.it/~vipp/files/datasets/DEMPSTER_SHAFER_FORENSICS.zip.
[215] IFS-TC Image Forensics Challenge, http://ifc.recod.ic.unicamp.br/.
[216] Copy-Move Forgery Dataset, https://www5.cs.fau.de/research/data/image-manipulation/.
[217] COVERAGE – Copy-Move Forgery Database with Similar but Genuine Objects, https://github.com/wenbihan/coverage.
[218] GRIP Copy-move Forgery Dataset, http://www.grip.unina.it/research/83-image-forensics/88-forgery-detection-pm.html.
[219] CoMoFoD, http://www.vcl.fer.hr/comofod/.
[220] Copy-move Forgery Dataset, https://www.researchgate.net/publication/281781572_Copy_Move_Forgery_Dataset.
[221] MICC Copy-move Forgery Dataset, http://lci.micc.unifi.it/labd/2015/01/copy-move-forgery-detection-and-localization/.
[222] G. Cattaneo, G. Roscigno, A possible pitfall in the experimental analysis of tampering detection algorithms, in: Proc. IEEE Int. Conf. Network-Based Information Systems, 2014, pp. 279–286, http://dx.doi.org/10.1109/nbis.2014.82.
[223] CASIA Datasets, http://forensics.idealtest.org/.
[224] Columbia DVMM Image Splicing Datasets, http://www.ee.columbia.edu/ln/dvmm/newDownloads.htm.
[225] T. Gloe, R. Böhme, The Dresden image database for benchmarking digital image forensics, Journal of Digital Forensic Practice 3 (2–4) (2010) 150–159, http://dx.doi.org/10.1145/1774088.1774427.
[226] D.T. Dang-Nguyen, C. Pasquini, V. Conotter, G. Boato, RAISE – a raw images dataset for digital image forensics, in: Proc. of ACM Multimedia Systems, 2015, http://dx.doi.org/10.1145/2713168.2713194.
[227] PhotoDetective: Image Forensic Toolkit, http://metainventions.com/photodetective.html.
[228] Forensically, https://29a.ch/photo-forensics/.
[229] Image Verification Assistant, http://reveal-mklab.iti.gr/reveal/.
[230] M. Carnein, P. Schöttle, R. Böhme, Telltale watermarks for counting JPEG compressions, Electron. Imaging 2016 (8) (2016) 1–10, http://dx.doi.org/10.2352/ISSN.2470-1173.2016.8.MWSF-072.
[231] A. Cavallaro, E.D. Gelasca, T. Ebrahimi, Objective evaluation of segmentation quality using spatio-temporal context, in: IEEE Int. Conf. Image Process, 2002, http://dx.doi.org/10.1109/icip.2002.1038965.
[232] E.D. Gelasca, T. Ebrahimi, On evaluating video object segmentation quality: a perceptually driven objective metric, IEEE J. Sel. Top. Signal Process. 3 (2) (2009) 319–335, http://dx.doi.org/10.1109/jstsp.2009.2015067.
[233] E.D. Gelasca, T. Ebrahimi, M. Farias, M. Carli, S.K. Mitra, Towards perceptually driven segmentation evaluation metrics, in: IEEE Computer Vision and Pattern Recognition Workshop, 2004, http://dx.doi.org/10.1109/cvpr.2004.465.

Paweł Korus received his M.Sc. and Ph.D. degrees in telecommunications (both with honors) from the AGH University of Science and Technology in 2008, and in 2013, respectively. From 2015 to 2017 he has been a post-doctoral researcher with the College of Information Engineering, Shenzhen University, Shenzhen, China. He is currently an assistant professor with the Department of Telecommunications, AGH University of Science and Technology, Krakow, Poland.

His research interests include various aspects of multimedia security & image processing, with particular focus on digital image forensics, content authentication, digital watermarking & information hiding. In 2015 he received a scholarship for outstanding young scientists from the Polish Ministry of Science and Higher Education.