A Comprehensive Survey on Methods for Image Integrity

PAOLA CAPASSO[**], University of Salerno, Italy
GIUSEPPE CATTANEO, University of Salerno, Italy
MARIA DE MARSICO, Sapienza University of Roma, Italy

The outbreak of digital devices on the Internet, the exponential diffusion of data (images, video, audio, and text), along with their manipulation/generation also by Artificial Intelligence (AI) models, e.g., Generative Adversarial Networks (GANs), have created a great deal of concern in the field of forensics. A malicious use can affect relevant application domains, which often include counterfeiting biomedical images, and deceiving biometric authentication systems, as well as their use in scientific publications, in the political world, and even in school activities. It has been demonstrated that manipulated pictures most likely represent indications of malicious behavior, such as photos of minors to promote child prostitution or false political statements. Following this widespread behavior, various forensic techniques have been proposed in the scientific literature over time both to defeat these spoofing attacks as well as to guarantee the integrity of the information. Focusing on Image Forensics, which is currently a very hot topic area in Multimedia Forensics, this paper will discuss the whole scenario in which a target image could be modified. The aim of this comprehensive survey will be 1) to provide an overview of the types of attacks and contrasting techniques and 2) to evaluate to what extent the former can deceive prevention methods and the latter can identify counterfeit images. The results of this study highlight how forgery detection techniques, sometimes limited to a single type of real scenario, are not able to provide exhaustive countermeasures and could/should therefore be combined. Currently, the use of neural networks, such as CNNs, is already heading, synergistically, in this direction.

CCS Concepts: • **General and reference** → **Surveys and overviews**;

Additional Key Words and Phrases: Digital Forensics (DF), Image Forensics, Image Forgery Detection (IFD), Active Methods(AM), Passive Methods(PM), Dependent and Independent Techniques, Pixel Non-Uniformity noise (PNU), Photo Response Non-Uniformity (PRNU)

1 INTRODUCTION

With the increasingly pervasive intentional or unintentional manipulation of data (images, video, audio, and text), the focus on forgery/counterfeit detection is growing exponentially [274]. As highlighted in Fig. 1, Multimedia Forensics is a broad disciplinary area that requires a lot of attention in terms of scientific and forensic activities. It bears the great responsibility of producing and disseminating methods to check internet data, which is often manipulated, altered, and even generated, maliciously, with intentional anti-forensics AF techniques (AFTs)[120]. Restricting the scope to Image Forensics, which is currently a hot topic in Multimedia Forensics, the paper will focus on Image Manipulation, which occurs when operations are performed on an image to modify it. In current literature, Image Forgery considers how the entire image is manipulated with malicious intent while in Image

[*]All authors contributed equally to this research.

Authors' addresses: Paola Capasso, pcapasso@unisa.it, pcapasso@unisa.it, University of Salerno, Via Giovanni Paolo II, 132 Fisciano, Salerno, Italy, 84084; Giuseppe Cattaneo, University of Salerno, Via Giovanni Paolo II, 132 Fisciano, Salerno, Italy, 84084, cattaneo@unisa.it; Maria De Marsico, Sapienza University of Roma, Via Salaria 113, 00198 Roma, Rome, Italy, maria.demarsico@uniroma1.it.

1551-6857/2023/11-ART $15.00
https://doi.org/10.1145/3633203

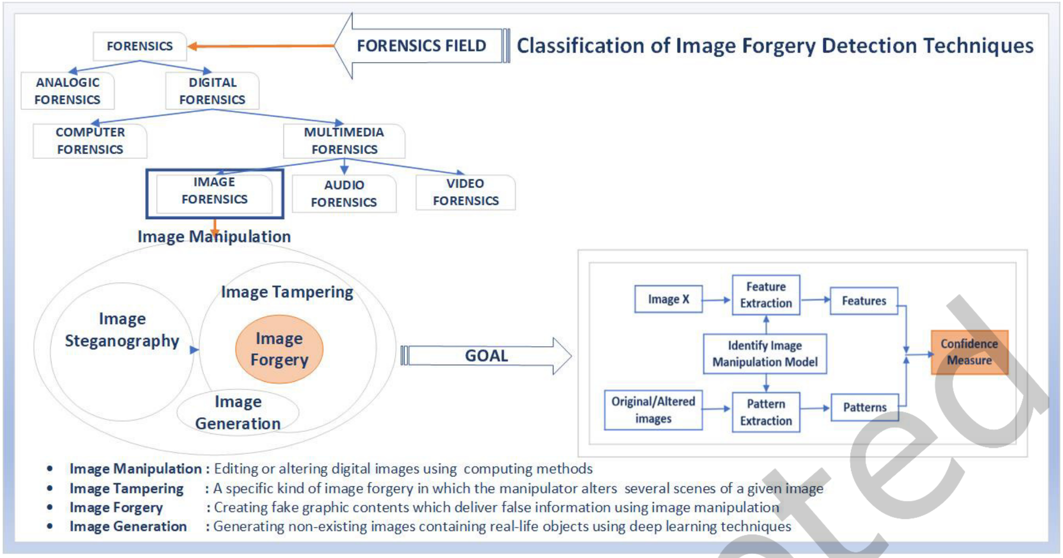


Fig. 1. The Goal of Forgery Detection.

Tampering, only parts of the image are intentionally modified. Image Generation uses computer software or algorithms to produce an image or part of an image simulating real-world scenes. The common denominator of these classes of operations is the malicious intention to violate the integrity of an image to deceive the observer, whereas Steganography has the objective of transporting secret messages from a sender to a recipient. In the latter, the image is modified so that it can store secret information invisible to the human eye, therefore maintaining the original appearance as much as possible. The goal of research in the field of Image Manipulation detection and identification is to examine, analyze, and define an acceptable confidence threshold to ensure data integrity and authenticity. At present, machine learning, and in particular approaches involving deep networks, are playing a supporting role both on the side of the attackers (see GANs[129]), and the defenders (see CNNs [193]), whether they are researchers, Law Enforcement Agencies (LEAs), or in general operators in the forensic sector. Transparent editing operations (manipulation) for tampering, retouching, and enhancement on multimedia objects, which are uploaded or shared through social media or web platforms, alter the original content of the images impeding to still consider them as authentic [247, 309]. However, even without manipulation, two types of artifacts inevitably remain in the image: image acquisition and compression artifacts. The intrinsic properties of these artifacts are essential forensic clues as they differ before and after the manipulation process [179, 198]. All this leads to a lack of a sure and obvious answer on the origin of the image, the user or device capturing it, as well as the truthfulness and originality of the acquired scene. As a consequence, many problems arise in the forensic field, creating a deal of interest in the search for substantial and cutting-edge solutions. The scientific community has unanimously proposed a twofold classification of all the different approaches to assure/verify image integrity. As shown in Fig. 2 "active" technologies usually embed data or signatures into the original image during its digitalization, either in the spatial or frequency domain; "passive" technologies, which are increasingly sophisticated, are based exclusively on digital content and operate without any knowledge of either the original image or pre-defined data or signature, therefore just relying on, e.g., statistical anomalies and/or artifacts. This investigation is a forensic contribution to the general scenario of forgery detection techniques. It will deal with the whole scenario where a target image could be modified. The aim will be 1) to provide an overview of the types of attacks and contrasting techniques and 2) to evaluate to what extent the former can deceive prevention methods and the latter to identify counterfeit images. The widespread diffusion of digital technologies has led, in the forensic field, to a constant increase in cases in which the use of digital evidence has been decisive in identifying the solution. It is easy to understand how their use will soon be pervasive and well-codified within forensic procedures. However, not all the approaches present in the current literature meet the requirements to be exploited in forensic activities [50]. Whenever a method is reproducible and replicable, it can be considered valid in a court and/or in front of a judge, and therefore it is forensic. The evaluation of the Confidence measure to obtain depends only on the common objective of the involved parties. This review has considered this forensic aspect an essential prerogative: all the methods mentioned in the paper have an experimental part, thus appearing as replicable and hence forensically sound. Thanks to the Budapest Convention [269, 322] and according to the reproducibility principle, digital evidence has been made admissible in courts. The Convention and the resulting regulations stipulate that all digital evidence is collected, archived, and presented according to a well-codified and recognized process. Once a scientific method has been identified, it will always be necessary to carry out an experimental evaluation phase before it can become a so-called *Best Practice* and its expected utility can be recognized by also carrying out a technology transfer action to operators in the sector. The European community boasts a network of experts (ENFSI-European Network of Forensics Science Institutes) that promotes knowledge sharing, experience exchange, and the reaching of mutual agreements in the field of forensic sciences through the development and use of good practices and their collection in a devoted manual (ENFSI BPM [1]) also offering a different taxonomy that can inspire further insight into the problems dealt with. Starting from these assumptions as well as current literature, the survey projects itself into an exhaustive search for reliable and forensically sound methodologies to support technological solutions aimed above all at Law Enforcement Agencies (LEAs) and Forensics Personnel. It will represent those treated aspects of the same problem assuming that there are counterfeits but doubting that they are always reproducible in court. This is where *Best Practices* should come into play, by possibly considering a joint use of different techniques having the same forensic purpose.

Other available surveys in literature often focus on specific kinds of forgery and/or detection strategies (see for example [59] on keypoint-based copy-move forgery detection methods or the recent work in [339] about deep learning approaches). This work aims to provide as wide and encompassing an account as possible of existing strategies, orienting readers in this extremely variated field. Many emerging topics like anti-forensic attacks and deepfake would deserve a deeper and wider critical analysis and discussion of open problems, which is beyond the scope of this survey. However, besides mentioning those topics we suggest references that offer related sufficient and thorough insight. Therefore, although methodologies have evolved up to deep learning and CNNs, this survey demonstrates that the basic work done by traditional techniques, which still support and are the basis for neural networks, is still considerable and indispensable. It also wants to represent a testimony of continuity and tries to establish a common line between traditional and non-traditional approaches. It is worth noting how the statistics show the effective use of these techniques [16] in real operative scenarios. The conceptual map below (Fig.2) proposes an updated scheme of real approaches to identify counterfeits.

The rest of the paper is organized as follows. Section 2 formally introduces Image Forgery Detection, the basic Concepts, the Problem Definition, and the Workflow of blind approaches. Section 3 reviews the methods of Forgery Detection proposed in the current literature, and Section 4 presents an evaluation of benchmark datasets fitting this purpose. Section 5 discusses the Research Challenges and Directions. Section 6 draws some conclusions. Finally, due to the broad scope of the subject, contrasting with the journal's strict space restrictions, further insights, examples, and figures have been included in the Online Appendix available for the online version of the paper.

[1]This Best Practice Manual for Digital Image Authentication was funded by the European Union's Internal Security Fund – Police and it is currently available for download: https://enfsi.eu/wp-content/uploads/2021/10/BPM_Image-Authentication _ENFSI-BPM-DI-003-1.pdf

2 FUNDAMENTALS

Image and Video Forensics (or **Forensics**, for short) refers to a specific area of Digital Forensics **(DF**, for short)[43, 255] that deals with the study and analysis of images (and videos) for their validation and use in Forensics [24]. The field of Image Forgery Detection (**IFD**) has developed 1) to combat the problem of image distortion in various application areas such as forensic and criminal investigation, insurance processing, surveillance systems, intelligence services, medical imaging, journalism [214], and 2) to reply to some important and complex technological questions such as determining if an image is authentic, doctored, or computer generated [99].

2.1 What is Image Forgery?

Counterfeiting can be defined as copying something with the intent to deceive; with it becoming a serious crime when it represents the making of realistic and fraudulent imitations of objects and documents to make them to be considered authentic either for profit or to mislead surveillance systems. There is a slight difference in the law between forgery and counterfeiting, with the former referring to forging documents and images, while the latter to material assets such as money, securities, and consumer products. In this article, the two terms, implying intentional illegality, will be used interchangeably to identify deception. The most frequent tasks in photo manipulation are: deleting/hiding a region in the image, adding a new object to the image, and misrepresenting image information [214].

2.2 Problem Definition

According to current literature [111, 213, 228, 312], Forgery Detection (FD) falls into two categories, namely, active and passive techniques (Fig.2). They can only extract forensic evidence if some information exists in the image [102].

Active Approach (AAFD - Active Approach to Forgery Detection) (3.1.1): as the name suggests, active methods of detection (see Fig.2 left-side) focus on the information that is hidden in an image at the time of its acquisition/digitalization. Given an image, the AAFD algorithms aim to detect the source and therefore forgery using

- **1. Watermarking**
- **2. Digital Signatures**
- **3. Cryptography techniques**

for image authenticity confirmation. They require prior knowledge of the elements associated with the original image, digital watermarking, or digital signatures. When checking the image, if the additional information found is incorrect, the image can be identified as tampered with; otherwise, the image is genuine. These approaches require special hardware or software to insert the authentication code inside the image before the image is distributed [225].

Passive Approach (PAFD - Passive Approach to Forgery Detection) (3.1.2): passive forensic techniques (Fig.2 right-side) do not rely on any additional information in the image and aim to find traces left during the image processing phases (acquisition and storage). They extract features from an image to detect the forgery. These so-called "blind methods" can be classified as: **1. Against Tampering Operations**: *Forgery Type-Dependent* or *Forgery Type-Independent*; **2. Based on Intrinsic Regularities & Inconsistencies** ; **3. Handling Natural & Computer Graphic/AI Images**.

2.3 Some Basic Concepts

This section discusses some concepts that have been mentioned in our previous introduction but will not be included anymore in the following. However, it is worth mentioning their role.

Image Generation (IG) encompasses methods that use machine and deep learning-based techniques to produce artificial images containing real-world objects and scenes from an existing data set: generating a fake image does not necessarily imply a forgery. For this, **IG** is not considered to be a part of Image Forgery. However, the advent of DeepFake (from *Deep Learning* and *Fake*) [4, 267] is quickly changing the way IG is regarded by the forensic community [13, 131, 135, 170, 192, 310, 321]. Basically, it refers to a recent manipulation technique allowing to synthesizing of images or videos from scratch, e.g. using Generative Adversarial Networks (GANs) and overimposing them on existing images or videos [134]. For example, it allows counterfeiting the identity of a person in a video/photo.

Image Warping (IW) is the geometric deformation of a single object in a given image. Warping can be used for correcting image distortion as well as for creative purposes.

Image Resizing is simply changing the size of the images without changing the number of pixels. *When an image is resized, its pixel information changes.* For example, if an image is reduced in size, all the unnecessary pixel information will be deleted from the photo editor. When an image is enlarged, the photo editor must create and add new pixel information, based on its best guesses, to achieve a larger size.

2.4 Generalized Workflow of the *Passive (or Blind*) Forgery Detection Process on the Image

In the passive approaches, before even getting to the identification of the kind of counterfeit, the main objective is to classify whether a given image is original (or authentic) or forged. A generalized scheme includes the steps below and is among the most used in the literature [1, 6, 94, 206, 213, 228, 273].

• Image Pre-processing: before dealing with any image, an initial optional step [94], almost always enforced in best practices, is the image pre-processing . Possible operations performed on the image include image filtering, image retouching, cropping, resizing, low-bypass filtering, the transformation from RGB to grayscale, and the modification of DCT coefficients. The choice of this step and the type of operation also depends on the calculation.

• Feature Extraction: given an input image, feature selection provides both a separation between different image classes and a decrease in computational complexity [153]. Of course, more traditional methods extract hand-crafted features that are engineered according to the chosen method and usually play a specific role in the procedure depending on the kind of forgery and the detection strategy. When Deep Learning-based methods are rather involved in the workflow, the feature extraction step is completely demanded by the network, so that the obtained embeddings are autonomously learned by the architecture and lack a precise explanation.

• Feature Matching & Filtering: a classifier, e.g., LDA (Latent Dirichlet Allocation), SVM (Support Vector Machine), or a neural network in general, will be chosen according to the set of features extracted from the previous step. It will determine if the image is original or not [97, 203, 205].

• Image Post-processing operations : tampering operations often involve post-processing operations to smooth the boundaries of tampered regions, to make the final artifact less visually suspectable (active-post-processing) or may be unintentionally introduced to tampered images during data transmission, e.g., JPEG compression, noise adding, and color reduction (passive post-processing) [350]. On the other hand, they can help detect those manipulations, such as location tracking, that might be included in the forged images. To improve the forgery localization several mathematical morphological operations could be performed [123, 228].

3 NOTABLE METHODS OVERVIEW

Digital Image Forgery started to occur a decade after the first image was created in various ways. At present, it exploits various image manipulation software, available for almost all trading platforms. Among the first technical issues to be addressed, the identification of the forgery is especially relevant since the authenticity of the images also follows from it. To achieve this, several FD techniques were used which will be examined in this section (see Fig.2). For the sake of completeness, Table 6 outlines the information. Special attention will be given to forensics-viable methods according to the Budapest Convention.

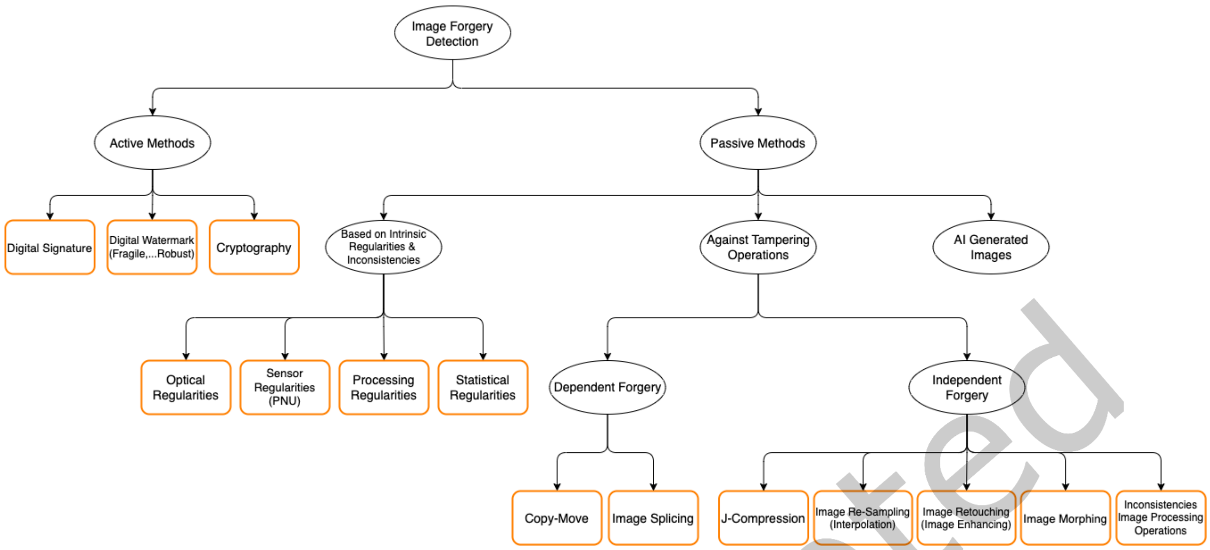


Fig. 2. Conceptual map of Forgery Detection Methods.

3.1 Taxonomy of Digital Forgery Detection Methods

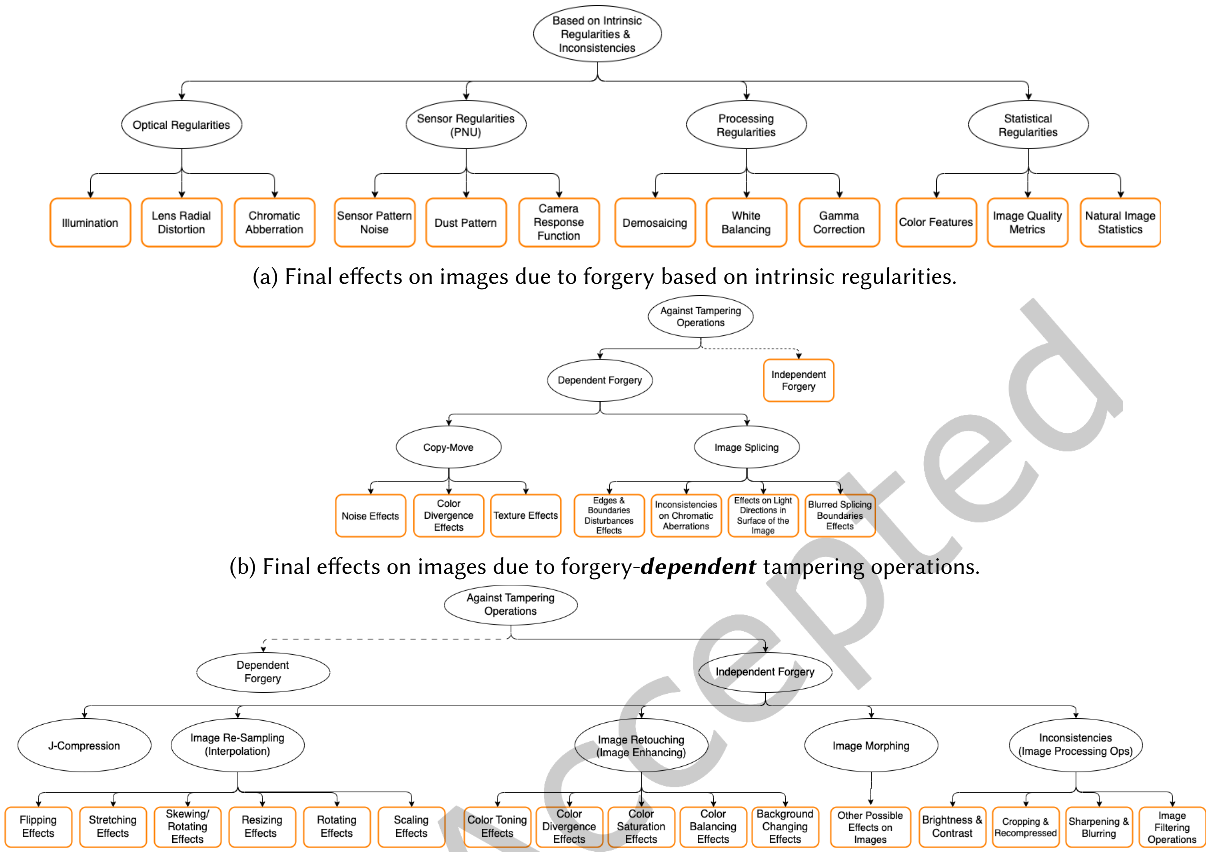
Digital Image Forgery Detection methods aim to detect those manipulations of a digital image that change the semantics of the visual message. As discussed above, the DF techniques are classified into two categories [274]: 3.1.1 **Active** (see Fig.2 (left-side)); 3.1.2 **Passive** (see Fig.2 (right-side)).
This taxonomy depends on the accessibility of the original picture. Each strategy can be further sub-partitioned (Fig.2).

3.1.1 ***Active Methods****.*

Active methods are robust mechanisms for safeguarding the integrity of digital images and exploiting certain information entered into them during the process of image acquisition and digitalization [58]. Alterations in an image are detected by analyzing such embedded (known) data. The main applications of these image authentication methods include intellectual and owner identification. They are classified according to whether they ensure strict integrity, content authentication, and the storage strategy of authentication data (i.e., watermark or external signature). These approaches include Watermarking, Digital Signatures, and conventional Cryptography [139].

• **Digital Watermarking techniques:** A large amount of literature currently deals with the topic [76, 110, 152, 188, 225]. Intuitively, Image Watermarking alters an image by inserting a mark that guarantees its authenticity. Watermarking methods are classified into three categories: *1) fragile watermarks 2) semi-fragile watermarks 3) robust watermarks.*

Fragile watermarking methods only allow a strict integrity check, while *semi-fragile* watermarking methods, based on external signatures, ensure content authentication. The former watermarking methods are highly sensitive to any type of tampering even in the modification of a single bit. The results obtained with these techniques show that they are both robust and secure and are therefore the best solution for copyright protection. The latter semi-fragile watermarking methods can be used for forensic purposes. Through these techniques, the authenticator can distinguish the original images from those whose content is intentionally modified while preserving the content of an image. The results offered by them show that despite their computational complexity, these techniques are secure and robust for all types of counterfeiting attacks. Finally, there are the kinds of *robust*



(a) Final effects on images due to forgery based on intrinsic regularities.

(b) Final effects on images due to forgery-***dependent*** tampering operations.

(c) Final effects on images due to forgery- ***independent*** tampering operations.

Fig. 3. Passive approach: each (sub-figure) represents effects on images due to different types of Forgery.

watermarking algorithms that can survive the content by preserving changes such as compression, noise addition, and filtering, as well as geometric changes such as resize, translation, rotation, cropping, and many more. They are used for ownership authentication [64]. These approaches have a high computational complexity and also offer less embedding capability. Fragile watermarking methods remain the simplest to implement ([271]). In digital watermarking, a specific message (digest) is inserted when an image is captured from a digital device. The watermarking is either "visible" or "invisible ([223]) and is, generally, independent of the image data ([323]). The basic underlying idea is that any attempt to alter the content of an image will also alter the watermark itself. In the following stages, a summary is then extracted from it to verify its legitimacy to compare it with the original digest. The result will indicate whether the image has been modified after acquisition. Therefore, the watermarking techniques consist of two phases: in the first, the image is generated and the watermark is also inserted. In the second stage, once the destination is reached, the watermark is extracted from the image and compared with the initial watermark. These techniques can be broadly classified into two categories depending on the kind of image transformation: 1) the *Spatial Domain* (LSB (Least Significant Bit) [284], SS (Spread Spectrum) [46], RIF (Random Insertion in File) [36]); 2) the *Frequency Domain* (DWT (Discrete Wavelet Transform) [304], DCT (Discrete Cosine

Transform) [95], DFT (Discrete Fourier Transform) [306], SVD (Singular Values Decomposition) [217]). It has been pointed out that the frequency domain methods are more robust than the spatial domain techniques [79].

Advantages: These methods provide authenticated multimedia content and focus on four essential features: robustness, security, capacity, and invisibility. ***Disadvantages:*** 1) Few (and generally expensive) devices have the function to incorporate a watermark in the image acquisition process. 2) These techniques, which require specialized software to incorporate the abstract into the image, are unable to distinguish the legitimate manipulations performed for the enhancement of the image quality (enhancement of contrast, sharpening, etc.) from the illegitimate ones (see [271]).

• **Cryptographic techniques** : Encryption techniques involve two steps: in the encryption stage, the plaintext is converted into ciphertext using a cipher. Conversely, in the decryption stage, the same cipher is used to convert ciphertext to plaintext. Approaches, e.g., classic cryptographically secure hash functions such as MD-4, MD-5 (message digest), CRC-32 (32-bit cyclic redundancy check), and SHA-1 (secure hash algorithms), are just some of the many methods existing in the literature that adopt a common general procedure. Due to the large research field, interested readers are advised to see [127, 194, 323, 328, 329, 336].

•**Digital Signatures techniques**: The validation of the authenticity of digital messages is normally based on a digital signature. Thanks to the valid signature, the recipient can assume that the message belongs to the known sender. The digital signature guarantees that the content is authentic, reliable, and from an authentic source. Applications of these techniques have been found to improve data integrity and image authentication in many industries, and some techniques are combined with watermarking, steganography, and cryptographic techniques [15, 181, 259, 301].

In Conclusion, in active methods, a trustworthy camera calculates a digital watermark or signature from the image at capture time, and any subsequent changes to the image can be detected by checking the value of the digital watermark or digital signature value at the time of its use. The disadvantages of active methods include that digital cameras must be equipped with a watermarking chip or a digital signature chip which, using a private key wired into the camera itself, authenticates each captured image before storing it on the memory card. This implies the definition of a common standard protocol: a requirement that would limit the application of such solutions only to very limited scenarios [254].

3.1.2 ***Passive Methods***. As discussed above, active methods use specially designed digital signatures and watermarking tools in cameras. Passive methods, sometimes known as blind methods, overcome this limitation by exclusively analyzing the binary information of an image[101], relying directly on image statistics, without requiring any prior information on image acquisition. Passive methods fall into three categories: *a) based on Tampering Operations, b) based on Intrinsic Regularities and Inconsistencies* and, *c) coping with Natural & Computer Graphic Images*. The most characteristic is certainly the first and second ones. The first is divided into forgery-dependent and forgery-independent methods [35, 42, 242, 264, 312]: **forgery type-dependent techniques** *depend on the different types of forgery performed on the image* and include methods to detect the most popular kinds of attack copy-move and image slicing; **forgery type -independent techniques** *are independent of the type of attack.*

a. Based on tampering operations

Forgery Type-Dependent Techniques

• **Copy-Move Forgery.** Copy-Move attack refers to forgeries that use a single image to copy a region from it and paste it into the same image to hide or duplicate specific objects. The copied part may or may not be modified. Since it belongs to the same image, its essential properties such as noise, color, and texture do not change, so the final forged image has homogeneous characteristics. This makes it difficult to even locate the forgery. Further operations such as rescaling, filtering, and noise scattering can be applied to hide any traces of the forgery.

Copy-Move Forgery Detection techniques is the process of identifying the occurrence of a copy-move in an image and can be classified into three categories, namely: 1) Brute Force detection 2) Block-based detection and 3) Keypoint-based detection. Due to the computational time complexity of the first category, literature mainly refers to approaches based on blocks and key points.

- 1. Brute Force detection is based on an exhaustive search and autocorrelation technique, which checks for any position change. The exhaustive search examines the corresponding image segment through circular shifts, producing a large number of comparisons. The computational times are relatively high.

- 2. Block-based detection divides the forged image into overlapping or non-overlapping blocks to analyze the block features in the frequency domain.

In the ***Phase of Block Feature Extraction*** (see Fig. 6) several approaches have been applied:
i) Since the Local Binary Patterns (LBP) operator is a texture descriptor for rotation-invariant grayscale images, it is widely used as a grayscale operator. LBP codes can be extracted from blocks beyond block texture verification. The approach in [105] proposed a generic passive image forgery scheme that combines a spatial rich model (SRM) with a textural feature based on the LBP operator. The combination of LBP with co-occurrence matrices makes the model capable of detecting almost all types of forgeries with improved detection accuracy.
ii) The use of the frequency domain, through a signal transform, can carry on the signatures for the image blocks, thus allowing for the identification of duplicate regions. In [215] *Mahmood et al.* used the stationary wavelet transform (SWT) and DCT to detect and localize the copy-move operation in digital images. The SWT allows it to work in both spatial and spectral domains, and the feature vectors are reduced by applying DCT. Dimension reduction processes are widely used to enhance the performance of the frameworks. Table 1 references the most used algorithms.

- 3. Keypoint-based detection. Feature-based or Keypoint-based approaches extract key points from forged images. They use a two-step process of locating and describing the local interest points. Robust local descriptors are constructed which must be invariant to affine alterations. They are not only robust to noise and geometric transformations but also use scale and rotation invariant feature detectors and descriptors. Table 1 lists the main algorithms used in the Feature Extraction phase (see Fig. 5). These methods rely on the identification and selection of high-entropy image regions (i.e. the "key points"): one feature vector per keypoint is then extracted. As a result, fewer feature vectors are estimated, resulting in reduced computational complexity of feature matching and post-processing. Post-processing thresholds are also lower than those of block-based methods. The downside is that the copied regions are not always covered by a satisfactory number of corresponding key points. If the copied regions show little structure, the region may be completely missing. Recently, [331] proposed a key point-based copy-move forgery detection and location technique based on a hierarchical point matching that reduces the number of points to improve the matching process. Feature-based approaches are relatively better than block-based and brute force methods in terms of computational efficiency, complexity, and robustness against many transformations such as scaling, rotation, cropping, etc. [167].

In the ***Phase of Matching and Filtering***, both in Block-based and Keypoint-based detection approaches, in identifying matching amongst the feature descriptors and to reduce the probability of false matches, most authors propose the use of main similarity measures and algorithms such as the Euclidean Distance, Correlation Coefficient, Sorting (lexicographic sorting, KD-tree, radix sort), Hash (counting bloom filters, locality-sensitive hashing), DCT and Sequential Clustering, Best Bin First, 2NNg, 2NN, Clustering (HAC, WPGMC) and others.

In Conclusion, both classes of methods have strengths and limitations. To address the limitation of these methods in flat regions, some approaches (see in [111]) also implemented mixed processes to tackle copy-move tampering detection problems, combining techniques based on features with block-based techniques. The approach in [140] combines the key point-based SIFT method with the block-based method using the dyadic wavelet transform (DyWT). Also in [295] a combination of the two different approaches is proposed by

Table 1. a. Based on tampering operations - 1st Part - Main methods.

A - BASED ON TAMPERING OPERATIONS - 1st PART			
FORGERY TYPE-DEPENDENT TECHNIQUES			
Copy-Move Forgery Detection techniques : Main methods			
Block-based detection			
Algorithms	Ref.	Algorithms	Ref.
Discrete Wavelet Transform (DWT)	[123, 169, 187, 330, 342]	Texture and Intensity	[146, 222, 300, 314]
Singular Value Decomposition (SVD)	[93, 167, 187]	Discrete Cosine Transform (DCT)	[114, 190]
Fourier Transform (Fourier-Mellin Transform)	[33]	Log-Polar Coordinates or transform	[47, 227]
Log-Polar Fast Fourier Transform (LPFFT)	[325]	Radix Sort	[195]
Dyadic Wavelet Transform (DyWT)	[224, 261]	Wiener Filter Wavelet	[70]
Multi-resolution wavelet decomposition	[22]	Principle Component Analysis (PCA)	[256]
Moments Invariant	[209]	Dimension Reduction	[180]
SVD (Singular Value Decomposition)	[187, 317]	KPCA	[21, 86]
Radon Transformation and Phase Correlation	[241]	Local Binary Patterns (LBP)	[317]
Fast Walsh Hadamard Transform (FWHT)	[289]	Zernike Moments	[216, 245, 272]
Keypoint-based detection			
Algorithms	Ref.	Algorithms	Ref.
SIFT (Scale Invariant Feature Transform)	[11, 150, 166, 191]	Principle Component Analysis (PCA)	[286]
ORB (OrientedFAST and rotated BRIEF)	[295]	Harris Corner Detector	[154]
BRISK (Binary Robust Invariant Scalable KPs)	[182]		
Splicing Forgery Detection techniques : Main methods			
Algorithms	Ref.	Algorithms	Ref.
Bispectral Analysis	[98]	Bicoherence magnitude and phase feature	[235]
Inverse camera response functions (CRF)	[115, 240]	Expectation/maximization (EM) algorithm	[74, 230]
Based on the use of the VGG-16 CNN	[178]	Wavelet decomposition-D phase congruency	[97, 115]
Multi-size block discrete cosine transform	[285]	Moment features and Image Quality metrics	[282]
CRF signature	[234, 282]	DCT coefficients and SVM	[202]
Based on DCT and image quality features	[347]	Gray level co-occurrence matrix (GLCM)	[315]
Based on computing the inverse CRF functions	[200]	Hilbert-Huang transform (HHT)	[65, 115, 252]
Planar homography constraint	[345]	Based on Chroma spaces	[349]
Artificial NN, indip. CA, and auto-regres. coeff.	[130, 142]	Based on Sobel edge detc.,deriv. op., Hough transf.	[160]
Based on the image of a person's eyes	[164]	Based on geometry invariants	[147, 148]
Based on statistics of 2-D phase congruency	[97]	Based on natural image model	[285]
Based on a NN architecture called CAU-Net	[250]	Based on a fully convolutional network (FCN)	[275]
Based on a ringed residual U-Net (RRU-Net)	[37]	Based on SVM	[91]
Based on computing the inverse CRF functions	[200]	Locally Planar Irradiance Points and CFR	[149]

extracting the key SIFT points in an image and then combining LPP (Locality Preserving Projection) to obtain low-dimensional feature descriptors.

• **Image Splicing.** Splicing is the process of cutting out a section of an image and pasting it onto the same image or another image. To create a fake image, splicing entails merging a minimum of two images. When images with contrasting bases have been well blended the edges between the spliced regions can be visually imperceptible. Unlike copy-move forgery, in splicing used objects are harvested from more than one image. The splicing, however, disturbs the higher-order Fourier statistics. These insights can then be used as an element to distinguish fakes [115, 237, 238, 348].

Image Splicing Detection is fundamental in Image Forgery Detection[42]. Table 1 lists the main related algorithms.

It appears from the literature that many of the methods mentioned work well when the analyzed image is compressed by a high-quality factor. Otherwise, compression artifacts make it very difficult to spot the fake.

Forgery Type-Independent Techniques

Table 2. a. Based on tampering operations - 2nd Part - Main methods.

A - BASED ON TAMPERING OPERATIONS - 2nd PART			
FORGERY TYPE-INDEPENDENT TECHNIQUES			
J-Compression Detection techniques : Main methods			
Algorithms	Ref.	Algorithms	Ref.
Maximum likelihood estimation to identify what quantization table was used	[96, 253]	Double compression by examining the histograms of the DCT coefficients	[257]
Operations based on DCT coefficient structure	[231]	Histograms of coefficient subbands analysis	[303]
Benford's law statistical model for probability distributions of the block-DCT first digits	[116]	Exploration of conditions under which primary quantization coefficients are identified	[290]
Tampered areas detection in double JPEG2000 compression tampered images	[343]	Mismatch information of BAG as a clue of copy-paste forgery	[189]
Shifted DJPEG with a convolutive model	[262]	Markov process/transition probability matrix	[61]
Probabilities of the first digits of quantized DCT coefficients from alternate current modes	[184]	Classification from the first order statistics of DCT modes of low-frequency DCT coefficient	[252]
Double/multiple quantization effects and CNN-First Quantization Estimation solutions	[25–27, 141, 179, 199]	Detection of either block-aligned or misaligned recompression	[68]
PCA on separate different SFQ noises	[291]	Detection of the presence of NA-JPEG images	[38–40]
Detection via B-G analysis of Jpeg artifacts	[41]	First quantization matrix estimation	[119]
Analysis of the blocking periodicity	[67]	Analysis of the properties of the image blocks	[187]
Maximum likelihood estimation of JPEG quantization steps was developed	[96]	Detection of composites created by JPEG images of different qualities	[100]
Detection of DJPEG images with periodic artifacts of re-quantization and discontinuities	[107]	Analysis of weakness/strength points of the current solutions on DCT and JPEG properties	[28]
Exploration of the image-specific artifacts	[212]	Estimation of the kind of source encoder	[196]
Based on blocking artifacts	[335]	Based on Multi-domain CNN	[12]
Re-Sampling Detection techniques : Main methods			
Algorithms	Ref.	Algorithms	Ref.
Prefiltering/derivation vs. resampling traces	[82]	Detection of adaptive scaling of images	[112]
Relations: rotation angle/frequencies at peaks	[277]	Property of 2°der. of interpolated periodicity of images	[118, 229]
Decomposition and random matrix principles	[311]	EM algorithm to estimate probability maps	[258]
Multidirectional high-pass filters on an image	[248]	Re-sampling detection in JPEG images	[176]
Cyclostationary process	[211]	Zero-crossings of the second difference signal	[260]
ML to distinguish between seam-carved (or seam-inserted) and normal images	[277]	Dual-filtering-based CNN to extract features directly from the images	[251]
Cumulative periodograms	[174, 319]	Radon transformation	[211]
Retouching Detection techniques : Main methods			
Algorithms	Ref.	Algorithms	Ref.
Identify/rebuild gamma correction operations	[51]	Identify the use of histogram equalization	[292, 293]
Two contrast enhancement-based algorithms via histogram peak/gap artifacts analysis	[53]	PRNU-based forgery detection algorithm based on the whole image	[69]
To measure the distortion between two images, the first original and the second processed	[18]	Statistical anomalies through the Laplace modeling of the derivative histogram	[34]
Algorithm vs cut-and-paste image forgery	[197]	Image sharpening detection methods	[351]
Detection of USM sharpening op. in images	[52]	A JPEG-robust forensic method based on CNN	[283]

• **J-Compression.** Editing an image involves loading it, modifying it, and then saving it again. Knowing the history of these compression operations, as well as whether a bitmap image has been previously compressed, is a clue in FD.

Image J-Compression Detection techniques. Table 2 lists the main used methods.

These methods work well for detecting saved images: the problem is when they are rotated, resized, and/or enhanced.

• **Image Re-Sampling.** When spatial transformations such as resizing, rotation, and stretching are applied to a digital image (to a specific object in the image or to all the image content), the type of forgery is known as re-sampling. The resizing of an image changes the dimensions of an object but does not improve the quality of that object. Re-sampling can be performed in different ways: Up/Down-sampling, Mirroring, Skewing, and Seam Carving.

Table 3. a. Based on tampering operations - 3rd Part - Main methods.

A - BASED ON TAMPERING OPERATIONS - 3rd PART			
FORGERY TYPE-INDEPENDENT TECHNIQUES			
Morphing Detection techniques : Main methods			
Algorithms	Ref.	Algorithms	Ref.
De-morphing method without needing a reference image or prior information about the morphing process	[19]	Wavelet domain analysis to gain insight into the spatial-frequency content of a morphed face	[3]
De-morphing generative adversarial network (FD-GAN) to restore the accomplice's facial image	[249]	FM Detection strategy with 3 modules (ICAO-aligned pre-processing, feature extraction, and classification module)	[233]
NN exploiting layer-wise relevance propagation (LRP) to analyze the differences in the decision-making process of the differently trained neural networks	[281]	StirTrace framework towards benchmarking face morphing forgeries extending it by additional scaling functions for the face biometrics scenario	[144]
MAP methodology vs. the Morphing potential attack	[109]	Framework for the Continual Learning Strategies	[45]
Demorphing approach to protecting ABControl systems	[108]	Micro-texture variations extraction using BSIF with SVM	[265]
Morphing attack detection approach based on convolutional neural networks	[280]	Use of transferable features from pre-trained Deep CNN to detect both digital and print-scanned morphed face images	[266]
Discriminative 2D Discrete Wavelet Transform (2D-DWT)	[2]	The Fourier spectrum of sensor pattern noise (FS-SPN)	[344]
Morph detection algorithm based on an analysis of PRNU	[85]	Distribution of Benford features extracted in Jpeg images	[218]
TDA (Topological Data Analysis) approach to detect various known morphing attacks	[156]	Morphing detection by using state-of-the-art facial recognition algorithms based on hand-crafted features and D-CNN	[313]
Detection for FM forgeries on image degradation	[232]	Facial landmarks shifting patterns reference/probe image	[83]
Deep MS Context Aggregation Net for denoised images	[307, 308]	Automated morph detection on pat.-recog. algorithms	[279]
Inconsistencies (Image Processing Operations) Detection techniques: Main methods			
Algorithms	Ref.	Algorithms	Ref.
Classifiers of distortion between original/processed images	[18, 30, 32]	Based on blind deconvolution	[297]
Based on image segmentation techniques	[17]	Based on non-intrusive component forensics	[175, 298]

Image Re-Sampling Detection: To create a fake image, some selected regions need to undergo geometric transformations such as rotate, scale, stretch, skew, flip, and so on. For example: if the face of a person is larger in an image, it should be scaled to the extent that the sizes of the faces are similar in the composite image. This requires re-sampling the image to compose a new sample and adding periodic correlations between pixels in the neighborhood. These transformations leave traces that are not typically present in the original images, and forgery techniques seek to identify such traces that constitute re-sampling cues. The interpolation phase also (e.g., nearest neighbor, bilinear, bicubic) plays an important role in the re-sampling process and introduces non-negligible statistical changes due to the specific periodic correlations in the image. These correlations can be used to recognize falsehoods caused by re-sampling [210, 259]. Table 2 summarizes several elements proposed and combined over time.

• **Image Retouching.** The image retouching forgery aims to enhance an object or image to exhibit or hide a specific feature such as coloring, lighting, or background changing. It is commonly used for aesthetic and

Table 4. b. Based on Intrinsic Regularities & Inconsistencies - Main methods.

B - BASED ON INTRINSIC REGULARITIES & INCONSISTENCIES			
Optical Regularities Detection Detection techniques : Main methods			
Algorithms	Ref.	Algorithms	Ref.
How the direction of a point light source is estimated	[161–165]	Automatic estimation of chromatic and aberration	[126, 162, 337]
Based on the geometric and photometric constraints	[103, 168]	Based on the focus on lens radial distortion	[71]
To calculate the surface normal matrix of the image	[207]	Based on camera lens-distortion correction	[128]
Processing Regularities Detection Detection techniques : Main methods			
Algorithms	Ref.	Algorithms	Ref.
Detection framework of demosaicing regularity	[54, 299]	A 3-layer feedforward backpropagation NN(BPN)	[151]
Sensors Regularities Detection Detection techniques : Main methods			
Algorithms	Ref.	Algorithms	Ref.
Based on imperfections of CCD pixels	[122]	Based on the detection of sensor dust characteristics	[89]
Based on sensor noise	[63, 172, 185]	Based on camera response normality and consistency	[200]
The color filter array (CFA) is examined	[31, 258]	Based on significant noise residual regions	[201]
Based on the PRNU & PNU	[8, 49, 55, 204]	Based on Colour-Decoupled PRNU (CD-PRNU)	[186]
Statistical Regularities Detection techniques : Main Methods			
Algorithms	Ref.	Algorithms	Ref.
Based on binary similarity and image quality measures, higher-order wavelet statistics with SVM Class	[57]	By analyzing image variations using Statistical Process Control	[23]
SVD-based image manipulation detection	[137]	To categorize a camera model	[104, 173]

Table 5. c. Natural & Computer Graphic Images (CGI).

C - NATURAL & COMPUTER GRAPHIC IMAGES (CGI) : MAIN METHODS			
Algorithms	Ref.	Algorithms	Ref.
Edge properties features	[183]	Residual pattern noise	[171]
Statistical moments of 1-D and 2-D characteristic functions	[296]	Color, edge, and texture properties	[80]
An aggregate of existing features	[276]	Features to identify computer-generated images	[87, 88]
Zero connectivity and fuzzy membership	[324]	Progressive randomization	[221]
Models on 1)first-order and higher-order wavelet statistics 2)characteristic function of the image and wavelet subbands	[66, 208]	The combination of three different algorithms based on the geometry, the wavelet, and the cartoon features	[236, 239]

commercial purposes, to enhance or reduce image features, and to create a compelling composite of two images which may require transformations such as rotating, stretching, or scaling, one of the images.

Image Retouching Detection: Many methods have been proposed for the detection of retouched forgeries, which is difficult if the image is significantly changed from the original image. Also, human intervention is often required to interpret the result. Table 2 lists the main related proposals.

• **Image Morphing.** A gradual transformation from one graphical object or image (source) to another graphical object or image (target) is called Image Morphing [155]. Differently from Warping, Image Morphing interpolates two or more graphical objects. It is a combination of image warping and blending techniques to interpolate objects to create a novel one. The basic idea of morphing is to distort the first image into another image by some predefined set of rules. The two basic principles of image morphing are image warping and cross-fading which must be coupled. Obviously, during this transformation, the central image, i.e., the generated one, is the key point of the technology because it decides whether the sequence will look good or not. It is intuitive to think that as the source image evolves, it begins to degrade and the target image evolves with new characteristics. The first images in the sequence will look more like the source. The central image will have the characteristics of both the source and the final images and will be distorted [60].

Image Morphing Attack Detection (MAD): Table 3 lists the basis of the latest generation algorithms and Automated MAD approaches recently proposed [219, 307].

• **Inconsistencies (Image Processing Operations).** An altered image has undergone basic image processing operations (Brightness&Contrast, Cropping&Recompressed, Sharpening&Blurring, and Filtering Operations). Tampering produces inconsistencies in the regular models and the traces of these operations can be useful in identifying forgery.

Image Processing Operations Detection. Table 3 lists the most recently proposed techniques.

b. Based on Intrinsic Regularities & **Inconsistencies.** Image regularities are of different nature, e.g., *Optical, Processing-related, Sensor-related, and Statistical.*

• **Optical Regularities.** Imperfections due to illumination, radial distortion of the lens, and chromatic aberration.

Optical Regularities Detection. Table 4 lists the most recently proposed techniques.

• **Processing Regularities.** Demosaicing, White Balancing, and Gamma Correction.

Processing Regularities Detection. Table 4 lists the most recently proposed techniques.

• **Sensor Regularities (Pixel Non-Uniformity - PNU for short)** . The Source Camera Identification (SCI, for short) techniques identify the intrinsic evidence left in images by the corresponding digital cameras responsible for their acquisitions. It is worth mentioning Sensor Pattern noise (the photo response non-uniformity (PRNU), Dust pattern, Feature Extraction, and Camera Response Function (CRF).

Sensor Regularities Detection. Table 4 lists the most recently proposed techniques.

• **Statistical Regularities.** Color Features, Image Quality Metrics, Natural Image Statistics.

Statistical Regularities Detection. Table 4 lists the most recently proposed techniques.

Methods based on image features do not work well when the image from a camera having a similar CCD [312].

c. Natural & Computer Graphic Images (CGI). Graphic software can generate photorealistic images. A challenging problem is to distinguish between computer-generated photorealistic and real (photographic) images.

Natural & Computer Graphic Image Detection. Table 5 lists the main bases for the proposed algorithms.

3.2 Summary Table: a summary outline

Table 6 reports some essential helpful information for the identification of the main classes of methods in this context.

4 DATASETS AND EVALUATIONS

4.1 Benchmark Image Datasets.

This subsection presents some public benchmark datasets (see Table 7) for the training and evaluation of the PAFD approaches. Each dataset was created for specific forgery attack detection methods. A combination of existing ones can be used for a wide range of applications. However, this requires some preliminary work to create a unified structure with consistent annotations. It is worth underlining that it would be extremely interesting to compare the real performance of methods and their effectiveness in the wild. However, a serious and thorough performance comparison would entail a shared benchmark and widely acknowledged protocols that are presently missing. These requirements represent an engaging challenge for the future, especially assembling a single dataset for all the detection methods.

5 DISCUSSION: LIMITATIONS, CHALLENGES AND OPPORTUNITIES

At present, generative AI techniques [270] and diffusion models [75] are a continuous source of new challenges. These techniques are spreading so quickly and in such a pervasive way that they would deserve much more space than a section herein. We hope that the suggested references can effectively complement the present survey. Diffusion models can be used also for audio synthesis [341]. As can be deduced from Fig. 2, Multimedia Forensics, in addition to Image Forensics, also includes Audio and Video. In particular, following the increasing popularity of DeepFakes, interest in Video Forensics is growing more and more. Currently, Deepfake detection is classified into machine learning-based classical methods, and more recent ones based on deep learning-based (the most widely used), statistical, and blockchain-based techniques [267]. Literature testifies that most deepfake detection research uses DL algorithms looking for inconsistencies in deepfake videos. However, since these are generated through adversarial training (often GANs), their ability to evade AI-based detection systems will improve as they become familiar with new detection methods. The challenge of recognizing them is increasingly difficult. The wide range of forensic video products available nowadays for forensic investigators [157] provides an overview that is not able to tackle all challenges. For a complete discussion of this area of research we suggest referring to exhaustive related works [9, 92, 113, 124, 133, 136, 143, 294, 332, 333].

The main challenge in detecting tampering is represented by the structural changes that occur in digital images. Due to their massive and widespread use in every field of application and considering the speed by which neural networks tackle/propose challenges, research is increasingly projected towards a combined use of traditional techniques with machine learning solutions. In addition to the traditional detection techniques

Table 6. A summary outline of the public forgery type detection methodologies considered in this review.

Rif.	Name	Category	Operation[2]	Class.	Rif.	Name	Category	Operation[2]	Class.
3.1.1	Digital Signature	Active	–	–	3.1.2	Copy-Move	Passive	ATO	Dependent forgery
3.1.1	Digital Watermarking	Active	–	–	3.1.2	Image Splicing	Passive	ATO	Dependent forgery
3.1.1	Cryptography	Active	–	–	3.1.2	J-Compression	Passive	ATO	Independent forgery
3.1.2	Optical Regularities	Passive	BOIR	–	3.1.2	Image Re-Sampling	Passive	ATO	Independent forgery
3.1.2	Source Camera Identification	Passive	BOIR	–	3.1.2	Image Morphing	Passive	ATO	Independent forgery
3.1.2	Processing Regularities	Passive	BOIR	–	3.1.2	Inconsistencies	Passive	ATO	Independent forgery
3.1.2	Statistical Regularities	Passive	BOIR	–	3.1.2	Image Retouching	Passive	ATO	Independent forgery
–	–	–	–	–	3.1.2	Others	Passive	N&CGI	–

[2] ***BOIR:*** Based on intrinsic regularities & inconsistencies. ***ATO:*** Against Tampered Operations. ***N&CGI:***Natural & Computer Graphic Images.

Table 7. List of the Public Forgery Digital Image Datasets.[2]

Ref.	Dataset Name	Year	Forgery Type	Ref.	Dataset Name	Year	Forgery Type
[278]	UCID	2003	For Source Camera Identification purposes	[56]	UniSA TIDE	2014	Tampered color images with different resolutions, splicing operations, blur filtering
[237]	COLUMBIA GRAY	2004	SCI: Splicing, BMP format gray images	[288]	CMH	2015	Copy-move, rotation, resizing, rotation, and resizing
[147]	COLUMBIA COLOUR	2006	Splicing, TIFF format color images	[14]	CVIP	2015	Translation, copy-move, rotation, scaling
[158]	INRIA_Copy Days	2008	Cropping, scaling, jpeg compression, combined strong attacks	[84]	RAISE	2015	SCI: High luminance images, uncompressed images, and camera native images
[90]	SIDD	2008	For Source Camera Identification purposes	[327]	SCUT-FBP	2015	For automatic facial beauty perception
[90]	CASIA v1.0	2009	SCI: Jpeg formatting and splicing (at preprocessing)	[318]	Wattanachote	2015	Seam-carved/seam-inserted images at various quality factors
[90]	CASIA v2.0	2009	SCI: Copy-move and splice images	[338]	Wild WEB	2015	SCI: Cut&paste,copy-move, erase forging
[11, 125]	DRESDEN	2010	SCI: Multiple cameras, multiple file formats, and different visual qualities	[320]	COVERAGE	2016	Copy-move along with interpretations
[20]	BOSS_Bases v0.93	2011	Greyscale, no PGM, multiple camera models, and appropriate raw EIF	[132]	NC	2016	Splice and localization detection, provenance modification
[11]	MICC-2000	2011	SCI: Coloring, copy-move, and jpeg formatting	[177]	RTD v.2.0	2017	Modifications, PRNU signatures, TIFF/PNG formatting, Ground Truth Maps of 3-level
[11]	MICC-F220	2011	SCI: Coloring,copy-move, jpeg-format, images with no mask, lacks post-processing	[287]	VISION	2017	For Source Camera Identification purposes
[41]	Bianchi	2012	Jpeg and TIFF formatting	[5]	DHFI	2018	For Source Camera Identification purposes
[72]	CMEN	2012	Copy-move images, resized images	[121]	KAGGLE	2018	For Source Camera Identification purposes
[72]	IMD	2012	Copy-move images	[132]	MFC	2018	Splicing investigates processing events, source modification camera verification, GAN modifications
[72]	MANIP	2012	Copy-move images	[302]	DSID_DAXING	2019	For Source Camera Identification purposes
[305]	CoMoFoD	2013	Coloring PNG/jpeg formatting,copy-move	[117]	SOCRATES	2019	For Source Camera Identification purposes
[106]	IEEE IFS-TC	2013	Copy-move images and Splicing	[138]	FODB-FORCHHEIM	2020	For Source Camera Identification purposes
[10]	MICC-F600	2013	SCI: Coloring PNG and jpeg formatting, copy-move	[243]	IMD	2020	Multiple-forged advanced GAN, inpainting-forged-images,images-from-2322-device
[77]	CMFDdb grip	2014	Rotation, scaling, jpeg compression	[48]	UNISA2020	2021	For SCI(on PNU): images from multiple conventional digital cameras of the same type

[1] The columns provide the following information for each dataset (from left to right): reference section, name, year, and forgery type.

mentioned above, convolutional neural networks (CNNs, for short) can represent an ambitious and effective solution to detect counterfeits. Touted as one of the most popular deep learning methods, CNN-based approaches are recently gaining success in Digital Image Forensics [12, 29, 62, 73, 78, 145, 220, 268, 316, 346]. In Active Forgery Detection, Kandi et al. in [340] proposed a watermarking technique based on an auto-encoder CNN network for robust non-blind watermarking, that achieves better performance than that of domain transform techniques. On the other hand, in Passive Forgery Detection, a CNN has been used to identify the camera that captured the particular image. Yao et al. in [334] proposed a multi-classifier based on CNNs that subjected images to post-processing attacks such as JPEG compression and adding noise. Several CNN-based approaches deal with copy-move operation [44, 78, 159, 226, 326]. Ouyang et al. in [244] used an adjusted network obtained from an existing trained ImageNet model and obtained a satisfactory performance compared to automatically generated spoofed images, while it does not apply to real spoofed images. Quan et al. in [263] proposed a CNN generic framework to classify images as computer-generated or natural with robust results against resampling (resizing) and JPEG compression. In [7] a useful list of CNN-based techniques with related comparisons is mentioned.

Actually, in the context of image tampering, new proposed solutions based on **Image Anomaly Detection** (IAD) and **Deep Anomaly Detection** are emerging. Anomaly Detection, or Novelty Detection, is referred to as the process of discovering data instances that deviate significantly from the majority of data instances. Due to the complexity of the problem and difficulty of learning, an advanced approach such as Deep Anomaly Detection is currently also required [246]. The work in [81] surveyed the concerns and efforts made so far to optimize and improve Anomaly/Tampering Detection methods. It includes a comprehensive table that summarizes image tampering detection and image anomaly detection datasets fit for purpose. The direction of all these aforementioned efforts introduces the need for a rigorous consideration of new and increasingly complex challenges related to tampered image detection. The most promising trend in terms of research, challenges, and opportunities is the use of machine learning techniques.

6 CONCLUSIONS

The huge diffusion of data (images, video, audio, and text), often uploaded/shared via social media or web platforms, and the possibility of their manipulation/generation also through Artificial Intelligence (AI) models, poses serious problems. Some examples are counterfeiting biomedical images, deceiving biometric authentication systems, cheating in scientific publications, in the political world, and in school activities.

In particular, the Deepfake technique, e.g. photo-realistic video or image content creation via DL methods, with the associated social and legal problems, poses serious threats to the privacy, reputation, and security of the victims. Despite many recent proposals for Deepfake detection, the rapid progress in multimedia technology and the proliferation of application tools continuously pose new challenges calling for a reliable and definitive solution [135]. A side effect is a decreased focus on more traditional forgery techniques, that, however, still represent not completely solved problems.

Whatever the nature of the manipulation, once a digital image represents a crime, it is necessary to detect the forgery. This document has presented a comprehensive overview of current and past research specially developed to list Image Forgery Detection algorithms in the Digital Forensics scenario. The paper overviews the most important methodologies used so far, restricting the scope to cases where the solution is forensic. Taking into account the various other public investigations for the detection of forgery images available in the current literature, it aims to provide a comprehensive longitudinal overview of the entire image-related forensic scenario. As mentioned in the introduction, retracing the fundamental work carried out so far, this investigation aims to represent a testimony of continuity between traditional and non-traditional approaches. We hope this survey will help forensic groups to tackle the detection of existing attacks, and get basic information about the rising ones while providing a compass for a deeper insight. In the future, we plan to move the focus toward deep manipulation detection in the context of deep fake applications.

REFERENCES

[1] Nor Bakiah Abd Warif, Ainuddin Wahid Abdul Wahab, Mohd Yamani Idna Idris, Roziana Ramli, Rosli Salleh, Shahaboddin Shamshirband, and Kim-Kwang Raymond Choo. 2016. Copy-move forgery detection: survey, challenges and future directions. *Journal of Network and Computer Applications* 75 (2016), 259–278.

[2] Poorya Aghdaie, Baaria Chaudhary, Sobhan Soleymani, Jeremy Dawson, and Nasser M Nasrabadi. 2021. Detection of morphed face images using discriminative wavelet sub-bands. In *2021 IEEE International Workshop on Biometrics and Forensics (IWBF)*. IEEE, 1–6.

[3] Poorya Aghdaie, Baaria Chaudhary, Sobhan Soleymani, Jeremy Dawson, and Nasser M. Nasrabadi. 2022. Morph Detection Enhanced by Structured Group Sparsity. In *2022 IEEE/CVF Winter Conference on Applications of Computer Vision Workshops (WACVW)*. 311–320. https://doi.org/10.1109/WACVW54805.2022.00037

[4] Zahid Akhtar. 2023. Deepfakes Generation and Detection: A Short Survey. *Journal of Imaging* 9, 1 (2023), 18.

[5] Omar Al Shaya, Pengpeng Yang, Rongrong Ni, Yao Zhao, and Alessandro Piva. 2018. A new dataset for source identification of high dynamic range images. *Sensors* 18, 11 (2018), 3801.

[6] Amani Alahmadi, Muhammad Hussain, Hatim Aboalsamh, Ghulam Muhammad, George Bebis, and Hassan Mathkour. 2017. Passive detection of image forgery using DCT and local binary pattern. *Signal, Image and Video Processing* 11 (2017), 81–88.

[7] SS Ali, II Ganapathi, NS Vu, SD Ali, N Saxena, and N Werghi. 2022. Image Forgery Detection Using Deeplearning by Recompressing Images. Electronics 2022, 11, 403.

[8] Erwin J Alles, Zeno JMH Geradts, and Cor J Veenman. 2009. Source camera identification for heavily jpeg compressed low resolution still images. *Journal of forensic sciences* 54, 3 (2009), 628–638.

[9] Irene Amerini, Gianmarco Baldini, and Francesco Leotta. 2021. Image and Video Forensics. *Journal of Imaging* 7, 11 (2021). https://doi.org/10.3390/jimaging7110242

[10] Irene Amerini, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, Luca Del Tongo, and Giuseppe Serra. 2013. Copy-move forgery detection and localization by means of robust clustering with J-Linkage. *Signal Processing: Image Communication* 28, 6 (2013), 659–669.

[11] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra. 2011. A SIFT-based forensic method for copy-move attack detection and transformation recovery. *IEEE Transactions on Information Forensics and Security* 6, 3 PART 2 (2011), 1099–1110. https://doi.org/10.1109/TIFS.2011.2129512 cited By 624.

[12] Irene Amerini, Tiberio Uricchio, Lamberto Ballan, and Roberto Caldelli. 2017. Localization of JPEG Double Compression Through Multi-domain Convolutional Neural Networks. In *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*. 1865–1871. https://doi.org/10.1109/CVPRW.2017.233

[13] Muhammad Aoun. 2023. Deep Fake Detection in Social Media Forensic Taxonomy, Challenges, Future Directions. *LC International Journal of STEM (ISSN: 2708-7123)* 4, 1 (2023), 16–26.

[14] Edoardo Ardizzone, Alessandro Bruno, and Giuseppe Mazzola. 2015. Copy–move forgery detection by matching triangles of keypoints. *IEEE Transactions on Information Forensics and Security* 10, 10 (2015), 2084–2094.

[15] Rizky Damara Ardy, Oktaviana Rena Indriani, Christy Atika Sari, Eko Hari Rachmawanto, et al. 2017. Digital image signature using triple protection cryptosystem (RSA, Vigenere, and MD5). In *2017 International Conference on Smart Cities, Automation & Intelligent Computing Systems (ICON-SONICS)*. IEEE, 87–92.

[16] Matthew PJ Ashby. 2017. The value of CCTV surveillance cameras as an investigative tool: An empirical analysis. *European Journal on Criminal Policy and Research* 23, 3 (2017), 441–459.

[17] JANLUK AśS. [n. d.]. DIGITAL IMAGE AUTHENTICATION USING IMAGE FILTERING TECHNIQUES. In *Conference on Scientific Computingpp*, Vol. 236. Citeseer, 244.

[18] I. Avcibas, S. Bayram, N. Memon, M. Ramkumar, and B. Sankur. 2004. A classifier design for detecting image manipulations. In *2004 International Conference on Image Processing, 2004. ICIP '04.*, Vol. 4. 2645–2648 Vol. 4. https://doi.org/10.1109/ICIP.2004.1421647

[19] Sudipta Banerjee, Prateek Jaiswal, and Arun Ross. 2022. Facial De-morphing: Extracting Component Faces from a Single Morph. In *2022 IEEE International Joint Conference on Biometrics (IJCB)*. 1–10. https://doi.org/10.1109/IJCB54206.2022.10007977

[20] Patrick Bas, Tomáš Filler, and Tomáš Pevnỳ. 2011. " Break our steganographic system": the ins and outs of organizing BOSS. In *Information Hiding: 13th International Conference, IH 2011, Prague, Czech Republic, May 18-20, 2011, Revised Selected Papers 13*. Springer, 59–70.

[21] M Bashar, K Noda, N Ohnishi, and K Mori. 2010. Exploring duplicated regions in natural images. *IEEE Transactions on Image Processing* (2010).

[22] Md Khayrul Bashar, Keiji Noda, Noboru Ohnishi, Hiroaki Kudo, Tetsuya Matsumoto, and Yoshinori Takeuchi. 2007. Wavelet-Based Multiresolution Features for Detecting Duplications in Images.. In *MVA*. 264–267.

[23] Philip Bateman, Anthony T. S. Ho, and Alan Woodward. 2009. Image forensics of digital cameras by analysing image variations using Statistical Process Control. In *2009 7th International Conference on Information, Communications and Signal Processing (ICICS)*. 1–5. https://doi.org/10.1109/ICICS.2009.5397649

[24] Sebastiano Battiato, Fausto Galvan, Martino Jerian, and Matteo Salcuni. 2013. Linee guida per l'autenticazione forense di immagini. *Chapter in IISFA Memberbook* (2013).

[25] Sebastiano Battiato, Oliver Giudice, Francesco Guarnera, and Giovanni Puglisi. 2021. Estimating previous quantization factors on multiple JPEG compressed images. *EURASIP Journal on Information Security* 2021, 1 (2021), 1–11.

[26] Sebastiano Battiato, Oliver Giudice, Francesco Guarnera, and Giovanni Puglisi. 2021. First quantization estimation by a robust data exploitation strategy of DCT coefficients. *IEEE Access* 9 (2021), 73110–73120.

[27] Sebastiano Battiato, Oliver Giudice, Francesco Guarnera, and Giovanni Puglisi. 2022. CNN-based first quantization estimation of double compressed JPEG images. *Journal of Visual Communication and Image Representation* 89 (2022), 103635.

[28] Sebastiano Battiato and Giuseppe Messina. 2009. Digital forgery estimation into DCT domain: a critical analysis. In *Proceedings of the First ACM workshop on Multimedia in forensics*. 37–42.

[29] Belhassen Bayar and Matthew C Stamm. 2016. A deep learning approach to universal image manipulation detection using a new convolutional layer. In *Proceedings of the 4th ACM workshop on information hiding and multimedia security*. 5–10.

[30] Sevinç Bayram, İsmail Avcıbaş, Bülent Sankur, and Nasir Memon. 2006. Image manipulation detection. *Journal of Electronic Imaging* 15, 4 (2006), 041102–041102.

[31] S. Bayram, H. Sencar, N. Memon, and I. Avcibas. 2005. Source camera identification based on CFA interpolation. In *IEEE International Conference on Image Processing 2005*, Vol. 3. III–69. https://doi.org/10.1109/ICIP.2005.1530330

[32] Sevinc Bayram, Husrev T Sencar, and Nasir Memon. 2008. Classification of digital camera-models based on demosaicing artifacts. *digital investigation* 5, 1-2 (2008), 49–59.

[33] Sevinc Bayram, Husrev Taha Sencar, and Nasir Memon. 2009. An efficient and robust method for detecting copy-move forgery. In *2009 IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE, 1053–1056.

[34] S Bharathiraja. 2019. Anti-forensics contrast enhancement detection (AFCED) technique in images based on laplace derivative histogram. *Mobile Networks and Applications* 24, 4 (2019), 1174–1180.

[35] Charmil Nitin Bharti and Purvi Tandel. 2016. A survey of image forgery detection techniques. In *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. IEEE, 877–881.

[36] Sharbani Bhattacharya. 2012. Additive watermarking in optimized digital image. *IEEE Beacon, IEEE (Delhi Section) publication in* 31, 1 (2012), 79.

[37] Xiuli Bi, Yang Wei, Bin Xiao, and Weisheng Li. 2019. RRU-Net: The ringed residual U-Net for image splicing forgery detection. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*. 0–0.

[38] Tiziano Bianchi, Alessia De Rosa, and Alessandro Piva. 2011. Improved DCT coefficient analysis for forgery localization in JPEG images. In *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2444–2447.

[39] Tiziano Bianchi and Alessandro Piva. 2011. Detection of non-aligned double JPEG compression with estimation of primary compression parameters. In *2011 18th IEEE International Conference on Image Processing*. 1929–1932. https://doi.org/10.1109/ICIP.2011.6115848

[40] Tiziano Bianchi and Alessandro Piva. 2011. Detection of nonaligned double JPEG compression based on integer periodicity maps. *IEEE transactions on Information Forensics and Security* 7, 2 (2011), 842–848.

[41] Tiziano Bianchi and Alessandro Piva. 2012. Image forgery localization via block-grained analysis of JPEG artifacts. *IEEE Transactions on Information Forensics and Security* 7, 3 (2012), 1003–1017.

[42] Gajanan K. Birajdar and Vijay H. Mankar. 2013. Digital image forgery detection using passive techniques: A survey. *Digital Investigation* 10, 3 (2013), 226–245. https://doi.org/10.1016/j.diin.2013.04.007

[43] Rainer Böhme, Felix C Freiling, Thomas Gloe, and Matthias Kirchner. 2009. Multimedia forensics is not computer forensics. In *Computational Forensics: Third International Workshop, IWCF 2009, The Hague, The Netherlands, August 13-14, 2009. Proceedings 3*. Springer, 90–103.

[44] Luca Bondi, Silvia Lameri, David Güera, Paolo Bestagini, Edward J. Delp, and Stefano Tubaro. 2017. Tampering Detection and Localization Through Clustering of Camera-Based CNN Features. In *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*. 1855–1864. https://doi.org/10.1109/CVPRW.2017.232

[45] Guido Borghi, Gabriele Graffieti, Annalisa Franco, and Davide Maltoni. 2022. Incremental Training of Face Morphing Detectors. In *2022 26th International Conference on Pattern Recognition (ICPR)*. 914–921. https://doi.org/10.1109/ICPR56361.2022.9956395

[46] Anirban Bose and Santi Prasad Maity. 2017. Spread spectrum watermark detection on degraded compressed sensing. *IEEE Sensors Letters* 1, 5 (2017), 1–4.

[47] Sergio Bravo-Solorio and Asoke K. Nandi. 2009. Passive forensic method for detecting duplicated regions affected by reflection, rotation and scaling. In *2009 17th European Signal Processing Conference*. 824–828.

[48] Andrea Bruno, Paola Capasso, Giuseppe Cattaneo, Umberto Ferraro Petrillo, and Riccardo Improta. 2022. A novel image dataset for source camera identification and image based recognition systems. *Multimedia Tools and Applications* (2022), 1–17.

[49] Andrea Bruno, Giuseppe Cattaneo, Umberto Ferraro Petrillo, and Paola Capasso. 2021. PNU Spoofing: a menace for biometrics authentication systems? *Pattern Recognition Letters* 151 (2021), 3–10.
[50] Eric Van Buskirk and Vincent T. Liu. 2006. Digital Evidence: Challenging the Presumption of Reliability. *Journal of Digital Forensic Practice* 1, 1 (2006), 19–26. https://doi.org/10.1080/15567280500541421 arXiv:https://doi.org/10.1080/15567280500541421
[51] Gang Cao, Yao Zhao, and Rongrong Ni. 2010. Forensic estimation of gamma correction in digital images. In *2010 IEEE International Conference on Image Processing*. IEEE, 2097–2100.
[52] Gang Cao, Yao Zhao, Rongrong Ni, and Alex C. Kot. 2011. Unsharp Masking Sharpening Detection via Overshoot Artifacts Analysis. *IEEE Signal Processing Letters* 18, 10 (2011), 603–606. https://doi.org/10.1109/LSP.2011.2164791
[53] Gang Cao, Yao Zhao, Rongrong Ni, and Xuelong Li. 2014. Contrast Enhancement-Based Forensics in Digital Images. *IEEE Transactions on Information Forensics and Security* 9, 3 (2014), 515–525. https://doi.org/10.1109/TIFS.2014.2300937
[54] Hong Cao and Alex C Kot. 2009. Accurate detection of demosaicing regularity for digital image forensics. *IEEE Transactions on Information Forensics and Security* 4, 4 (2009), 899–910.
[55] Paola Capasso, Lucia Cimmino, Andrea F Abate, Andrea Bruno, and Giuseppe Cattaneo. 2022. A PNU-Based Methodology to Improve the Reliability of Biometric Systems. *Sensors* 22, 16 (2022), 6074.
[56] Giuseppe Cattaneo and Gianluca Roscigno. 2014. A possible pitfall in the experimental analysis of tampering detection algorithms. In *2014 17th International Conference on Network-Based Information Systems*. IEEE, 279–286.
[57] Oya Celiktutan, Bülent Sankur, and Ismail Avcibas. 2008. Blind identification of source cell-phone model. *IEEE Trans. Inf. Forensics Secur.* 3, 3 (2008), 553–566.
[58] B Chaitra and PV Bhaskar Reddy. 2019. A study on digital image forgery techniques and its detection. In *2019 International conference on contemporary computing and informatics (IC3I)*. IEEE, 127–130.
[59] Devanshi Chauhan, Dipali Kasat, Sanjeev Jain, and Vilas Thakare. 2016. Survey on keypoint based copy-move forgery detection methods on image. *Procedia Computer Science* 85 (2016), 206–212.
[60] Rahul Chauhan, Preeti Mishra, and RC Joshi. 2020. An overview of digital image forensics: image morphing and forgery detection algorithms. *Information Security and Optimization* (2020), 107–120.
[61] Chunhua Chen, Yun Q Shi, and Wei Su. 2008. A machine learning based scheme for double JPEG compression detection. In *2008 19th international conference on pattern recognition*. IEEE, 1–4.
[62] Jiansheng Chen, Xiangui Kang, Ye Liu, and Z Jane Wang. 2015. Median filtering forensics based on convolutional neural networks. *IEEE Signal Processing Letters* 22, 11 (2015), 1849–1853.
[63] Mo Chen, Jessica Fridrich, Miroslav Goljan, and Jan Lukás. 2008. Determining image origin and integrity using sensor noise. *IEEE Transactions on information forensics and security* 3, 1 (2008), 74–90.
[64] Tao Chen and Hongtao Lu. 2012. Robust spatial LSB watermarking of color images against JPEG compression. In *2012 IEEE Fifth International Conference on Advanced Computational Intelligence (ICACI)*. IEEE, 872–875.
[65] Wen Chen, Yun Q. Shi, and Wei Su. 2007. Image splicing detection using 2D phase congruency and statistical moments of characteristic function. In *Security, Steganography, and Watermarking of Multimedia Contents IX*, Edward J. Delp III and Ping Wah Wong (Eds.), Vol. 6505. International Society for Optics and Photonics, SPIE, 65050R. https://doi.org/10.1117/12.704321
[66] Wen Chen, Yun Q Shi, and Guorong Xuan. 2007. Identifying computer graphics using HSV color model and statistical moments of characteristic functions. In *2007 ieee international conference on multimedia and expo*. IEEE, 1123–1126.
[67] Yi-Lei Chen and Chiou-Ting Hsu. 2008. Image tampering detection by blocking periodicity analysis in JPEG compressed images. In *2008 IEEE 10th Workshop on Multimedia Signal Processing*. 803–808. https://doi.org/10.1109/MMSP.2008.4665184
[68] Yi-Lei Chen and Chiou-Ting Hsu. 2011. Detecting recompression of JPEG images via periodicity analysis of compression artifacts for tampering detection. *IEEE Transactions on Information Forensics and Security* 6, 2 (2011), 396–406.
[69] Giovanni Chierchia, Giovanni Poggi, Carlo Sansone, and Luisa Verdoliva. 2014. A Bayesian-MRF approach for PRNU-based image forgery detection. *IEEE Transactions on Information Forensics and Security* 9, 4 (2014), 554–567.
[70] Hyeokho Choi and R. Baraniuk. 1998. Analysis of wavelet-domain Wiener filters. In *Proceedings of the IEEE-SP International Symposium on Time-Frequency and Time-Scale Analysis (Cat. No.98TH8380)*. 613–616. https://doi.org/10.1109/TFSA.1998.721499
[71] Kai San Choi, Edmund Y. Lam, and Kenneth K. Y. Wong. 2006. Source camera identification using footprints from lens aberration. In *Digital Photography II*, Nitin Sampat, Jeffrey M. DiCarlo, and Russel A. Martin (Eds.), Vol. 6069. International Society for Optics and Photonics, SPIE, 60690J. https://doi.org/10.1117/12.649775
[72] Vincent Christlein, Christian Riess, Johannes Jordan, Corinna Riess, and Elli Angelopoulou. 2012. An evaluation of popular copy-move forgery detection approaches. *IEEE Transactions on information forensics and security* 7, 6 (2012), 1841–1854.
[73] Sara Concas, Gianpaolo Perelli, Gian Luca Marcialis, and Giovanni Puglisi. 2022. Tensor-Based Deepfake Detection In Scaled And Compressed Images. In *2022 IEEE International Conference on Image Processing (ICIP)*. IEEE, 3121–3125.
[74] Valentina Conotter, Giulia Boato, and Hany Farid. 2010. Detecting photo manipulation on signs and billboards. In *2010 IEEE International Conference on Image Processing*. 1741–1744. https://doi.org/10.1109/ICIP.2010.5652906

[75] Riccardo Corvi, Davide Cozzolino, Giada Zingarini, Giovanni Poggi, Koki Nagano, and Luisa Verdoliva. 2023. On the detection of synthetic images generated by diffusion models. In *ICASSP 2023-2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 1–5.
[76] Ingemar Cox, Matthew Miller, Jeffrey Bloom, and Chris Honsinger. 2002. Digital watermarking. *Journal of Electronic Imaging* 11, 3 (2002), 414–414.
[77] Davide Cozzolino, Giovanni Poggi, and Luisa Verdoliva. 2014. Copy-move forgery detection based on patchmatch. In *2014 IEEE international conference on image processing (ICIP)*. IEEE, 5312–5316.
[78] Davide Cozzolino and Luisa Verdoliva. 2016. Single-image splicing localization through autoencoder-based anomaly detection. In *2016 IEEE international workshop on information forensics and security (WIFS)*. IEEE, 1–6.
[79] S. Craver, N. Memon, B.-L. Yeo, and M.M. Yeung. 1998. Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications. *IEEE Journal on Selected Areas in Communications* 16, 4 (1998), 573–586. https://doi.org/10.1109/49.668979
[80] Florin Cutzu, Riad Hammoud, and Alex Leykin. 2005. Distinguishing paintings from photographs. *Computer Vision and Image Understanding* 100, 3 (2005), 249–273.
[81] Kelton A.P. da Costa, João P. Papa, Leandro A. Passos, Danilo Colombo, Javier Del Ser, Khan Muhammad, and Victor Hugo C. de Albuquerque. 2020. A critical literature survey and prospects on tampering and anomaly detection in image data. *Applied Soft Computing* 97 (2020), 106727. https://doi.org/10.1016/j.asoc.2020.106727
[82] Nahuel Dalgaard, Carlos Mosquera, and Fernando Pérez-González. 2010. On the role of differentiation for resampling detection. In *2010 IEEE International Conference on Image Processing*. 1753–1756. https://doi.org/10.1109/ICIP.2010.5652358
[83] Naser Damer, Viola Boller, Yaza Wainakh, Fadi Boutros, Philipp Terhörst, Andreas Braun, and Arjan Kuijper. 2019. Detecting face morphing attacks by analyzing the directed distances of facial landmarks shifts. In *Pattern Recognition: 40th German Conference, GCPR 2018, Stuttgart, Germany, October 9-12, 2018, Proceedings 40*. Springer, 518–534.
[84] Duc-Tien Dang-Nguyen, Cecilia Pasquini, Valentina Conotter, and Giulia Boato. 2015. Raise: A raw images dataset for digital image forensics. In *Proceedings of the 6th ACM multimedia systems conference*. 219–224.
[85] Luca Debiasi, Ulrich Scherhag, Christian Rathgeb, Andreas Uhl, and Christoph Busch. 2018. PRNU-based detection of morphed face images. In *2018 International Workshop on Biometrics and Forensics (IWBF)*. 1–7. https://doi.org/10.1109/IWBF.2018.8401555
[86] Chandan Deep Kaur and Navdeep Kanwal. 2019. An analysis of image forgery detection techniques. *Statistics, Optimization & Information Computing* 7, 2 (2019), 486–500.
[87] Sintayehu Dehnie, Taha Sencar, and Nasir Memon. 2006. Digital image forensics for identifying computer generated and digital camera images. In *2006 International Conference on Image Processing*. IEEE, 2313–2316.
[88] Ahmet Emir Dirik, Sevinç Bayram, Husrev T Sencar, and Nasir Memon. 2007. New features to identify computer generated images. In *2007 IEEE International Conference on Image Processing*, Vol. 4. IEEE, IV–433.
[89] Ahmet Emir Dirik, Husrev Taha Sencar, and Nasir Memon. 2008. Digital single lens reflex camera identification from traces of sensor dust. *IEEE Transactions on Information Forensics and Security* 3, 3 (2008), 539–552.
[90] Jing Dong, Wei Wang, and Tieniu Tan. 2013. Casia image tampering detection evaluation database. In *2013 IEEE China summit and international conference on signal and information processing*. IEEE, 422–426.
[91] Jing Dong, Wei Wang, Tieniu Tan, and Yun Q. Shi. 2009. Run-Length and Edge Statistics Based Approach for Image Splicing Detection. In *Digital Watermarking*, Hyoung-Joong Kim, Stefan Katzenbeisser, and Anthony T. S. Ho (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 76–87.
[92] Ricard Durall, Margret Keuper, and Janis Keuper. 2020. Watch your up-convolution: Cnn based generative deep neural networks are failing to reproduce spectral distributions. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*. 7890–7899.
[93] Brandon Dybala, Brian Jennings, and David Letscher. 2007. Detecting Filtered Cloning in Digital Images. In *Proceedings of the 9th Workshop on Multimedia & Security* (Dallas, Texas, USA) *(MM & Sec '07)*. Association for Computing Machinery, New York, NY, USA, 43–50. https://doi.org/10.1145/1288869.1288877
[94] Mohamed A Elaskily, Heba K Aslan, Osama A Elshakankiry, Osama S Faragallah, Fathi E Abd El-Samie, and Mohamed M Dessouky. 2017. Comparative study of copy-move forgery detection techniques. In *2017 Intl Conf on advanced control circuits systems (ACCS) Systems & 2017 Intl conf on new paradigms in electronics & information technology (PEIT)*. IEEE, 193–203.
[95] Ferda Ernawan and Muhammad Nomani Kabir. 2018. A Robust Image Watermarking Technique With an Optimal DCT-Psychovisual Threshold. *IEEE Access* 6 (2018), 20464–20480. https://doi.org/10.1109/ACCESS.2018.2819424
[96] Zhigang Fan and Ricardo L De Queiroz. 2003. Identification of bitmap compression history: JPEG detection and quantizer estimation. *IEEE Transactions on Image Processing* 12, 2 (2003), 230–235.
[97] Zhen Fang, Shuozhong Wang, and Xinpeng Zhang. 2009. Image Splicing Detection Using Camera Characteristic Inconsistency. In *2009 International Conference on Multimedia Information Networking and Security*, Vol. 1. 20–24. https://doi.org/10.1109/MINES.2009.208
[98] Hany Farid. 1999. *Detecting Digital Forgeries Using Bispectral Analysis*. Technical Report. USA.

[99] Hany Farid. 2004. Creating and Detecting Doctored and Virtual Images: Implications to The Child Pornography Prevention Act. Technical Report TR2004-518, Department of Computer Science, Dartmouth College,2004.
[100] Hany Farid. 2009. Exposing digital forgeries from JPEG ghosts. *IEEE transactions on information forensics and security* 4, 1 (2009), 154–160.
[101] Hany Farid. 2009. Image forgery detection. *IEEE Signal Processing Magazine* 26, 2 (2009), 16–25. https://doi.org/10.1109/MSP.2008.931079
[102] Hany Farid. 2016. *Photo forensics*. MIT press.
[103] Hany Farid and Mary J Bravo. 2010. Image forensic analyses that elude the human visual system. In *Media forensics and security II*, Vol. 7541. SPIE, 52–61.
[104] Giovanni Maria Farinella, Mario Valerio Giuffrida, Vincenzo Digiacomo, and Sebastiano Battiato. 2015. On blind source camera identification. In *Advanced Concepts for Intelligent Vision Systems: 16th International Conference, ACIVS 2015, Catania, Italy, October 26-29, 2015. Proceedings 16*. Springer, 464–473.
[105] Sundus Farooq, Muhammad Haroon Yousaf, and Fawad Hussain. 2017. A generic passive image forgery detection scheme using local binary pattern with rich models. *Computers & Electrical Engineering* 62 (2017), 459–472. https://doi.org/10.1016/j.compeleceng.2017.05.008
[106] Sundus Farooq, Muhammad Haroon Yousaf, and Fawad Hussain. 2017. A generic passive image forgery detection scheme using local binary pattern with rich models. *Computers & Electrical Engineering* 62 (2017), 459–472.
[107] Xiaoying Feng and Gwenaël J. Doërr. 2010. JPEG recompression detection. In *Electronic imaging*.
[108] Matteo Ferrara, Annalisa Franco, and Davide Maltoni. 2017. Face demorphing. *IEEE Transactions on Information Forensics and Security* 13, 4 (2017), 1008–1017.
[109] Matteo Ferrara, Annalisa Franco, Davide Maltoni, and Christoph Busch. 2022. Morphing Attack Potential. In *2022 International Workshop on Biometrics and Forensics (IWBF)*. 1–6. https://doi.org/10.1109/IWBF55382.2022.9794509
[110] Pasquale Ferrara, Tiziano Bianchi, Alessia De Rosa, and Alessandro Piva. 2012. Image forgery localization via fine-grained analysis of CFA artifacts. *IEEE Transactions on Information Forensics and Security* 7, 5 (2012), 1566–1577.
[111] William D. Ferreira, Cristiane B.R. Ferreira, Gelson da Cruz Júnior, and Fabrizzio Soares. 2020. A review of digital image forensics. *Computers & Electrical Engineering* 85 (2020), 106685. https://doi.org/10.1016/j.compeleceng.2020.106685
[112] Claude Fillion and Gaurav Sharma. 2010. Detecting content adaptive scaling of images for forensic applications. In *Media Forensics and Security II*, Nasir D. Memon, Jana Dittmann, Adnan M. Alattar, and Edward J. Delp III (Eds.), Vol. 7541. International Society for Optics and Photonics, SPIE, 75410Z. https://doi.org/10.1117/12.838647
[113] Joel Frank, Thorsten Eisenhofer, Lea Schönherr, Asja Fischer, Dorothea Kolossa, and Thorsten Holz. 2020. Leveraging frequency analysis for deep fake image recognition. In *International conference on machine learning*. PMLR, 3247–3258.
[114] Jessica Fridrich. 2003. Detection of copy-move forgery in digital images. In *Proc. Digital Forensic Research Workshop, 2003*.
[115] Dongdong Fu, Yun Q Shi, and Wei Su. 2006. Detection of image splicing based on Hilbert-Huang transform and moments of characteristic functions with wavelet decomposition. In *Digital Watermarking: 5th International Workshop, IWDW 2006, Jeju Island, Korea, November 8-10, 2006. Proceedings 5*. Springer, 177–187.
[116] Dongdong Fu, Yun Q. Shi, and Wei Su. 2007. A generalized Benford's law for JPEG coefficients and its applications in image forensics. In *Security, Steganography, and Watermarking of Multimedia Contents IX*, Edward J. Delp III and Ping Wah Wong (Eds.), Vol. 6505. International Society for Optics and Photonics, SPIE, 65051L. https://doi.org/10.1117/12.704723
[117] Chiara Galdi, Frank Hartung, and Jean-Luc Dugelay. 2019. SOCRatES: A Database of Realistic Data for SOurce Camera REcognition on Smartphones.. In *ICPRAM*. 648–655.
[118] Andrew C Gallagher. 2005. Detection of linear and cubic interpolation in JPEG compressed images. In *The 2nd Canadian Conference on Computer and Robot Vision (CRV'05)*. IEEE, 65–72.
[119] Fausto Galvan, Giovanni Puglisi, Arcangelo Ranieri Bruna, and Sebastiano Battiato. 2014. First quantization matrix estimation from double compressed JPEG images. *IEEE Transactions on Information Forensics and Security* 9, 8 (2014), 1299–1310.
[120] Simson Garfinkel. 2007. Anti-forensics: Techniques, detection and countermeasures. In *2nd International Conference on i-Warfare and Security*, Vol. 20087. 77–84.
[121] Michael Geiger. 2018. Geiger, Michael, "2018 IEEE Signal Processing Cup: Forensic Camera Model Identification Challenge" (2018).Honors Theses. 1577. (2018).
[122] Zeno J Geradts, Jurrien Bijhold, Martijn Kieft, Kenji Kurosawa, Kenro Kuroki, and Naoki Saitoh. 2001. Methods for identification of images acquired with digital cameras. In *Enabling technologies for law enforcement and security*, Vol. 4232. SPIE, 505–512.
[123] Mehdi Ghorbani, Mohammad Firouzmand, and Ahmad Faraahi. 2011. DWT-DCT (QCD) based copy-move image forgery detection. In *2011 18th International Conference on Systems, Signals and Image Processing*. IEEE, 1–4.
[124] Oliver Giudice, Luca Guarnera, and Sebastiano Battiato. 2021. Fighting deepfakes by detecting gan dct anomalies. *Journal of Imaging* 7, 8 (2021), 128.
[125] Thomas Gloe and Rainer Böhme. 2010. The'Dresden Image Database'for benchmarking digital image forensics. In *Proceedings of the 2010 ACM symposium on applied computing*. 1584–1590.

[126] Thomas Gloe, Karsten Borowka, and Antje Winkler. 2010. Efficient estimation and large-scale evaluation of lateral chromatic aberration for digital image forensics. In *Media Forensics and Security II*, Nasir D. Memon, Jana Dittmann, Adnan M. Alattar, and Edward J. Delp III (Eds.), Vol. 7541. International Society for Optics and Photonics, SPIE, 754107. https://doi.org/10.1117/12.839034

[127] Oded Goldreich and Oded Goldreich. 1999. The foundations of modern cryptography. *Modern Cryptography, Probabilistic Proofs and Pseudorandomness* (1999), 1–37.

[128] Miroslav Goljan and Jessica Fridrich. 2012. Sensor-fingerprint based identification of images corrected for lens distortion. In *Media Watermarking, Security, and Forensics 2012*, Vol. 8303. Spie, 132–144.

[129] Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. 2020. Generative adversarial networks. *Commun. ACM* 63, 11 (2020), 139–144.

[130] E.S. Gopi, N. Lakshmanan, T. Gokul, S. KumaraGanesh, and Prerak.r. Shah. 2006. Digital Image Forgery Detection using Artificial Neural Network and Auto Regressive Coefficients. In *2006 Canadian Conference on Electrical and Computer Engineering*. 194–197. https://doi.org/10.1109/CCECE.2006.277398

[131] Diego Gragnaniello, Davide Cozzolino, Francesco Marra, Giovanni Poggi, and Luisa Verdoliva. 2021. Are GAN generated images easy to detect? A critical analysis of the state-of-the-art. In *2021 IEEE international conference on multimedia and expo (ICME)*. IEEE, 1–6.

[132] Haiying Guan, Mark Kozak, Eric Robertson, Yooyoung Lee, Amy N Yates, Andrew Delgado, Daniel Zhou, Timothee Kheyrkhah, Jeff Smith, and Jonathan Fiscus. 2019. MFC datasets: Large-scale benchmark datasets for media forensic challenge evaluation. In *2019 IEEE Winter Applications of Computer Vision Workshops (WACVW)*. IEEE, 63–72.

[133] Luca Guarnera, Oliver Giudice, and Sebastiano Battiato. 2020. Fighting deepfake by exposing the convolutional traces on images. *IEEE Access* 8 (2020), 165085–165098.

[134] Luca Guarnera, Oliver Giudice, Francesco Guarnera, Alessandro Ortis, Giovanni Puglisi, Antonino Paratore, Linh M. Q. Bui, Marco Fontani, Davide Alessandro Coccomini, Roberto Caldelli, Fabrizio Falchi, Claudio Gennaro, Nicola Messina, Giuseppe Amato, Gianpaolo Perelli, Sara Concas, Carlo Cuccu, Giulia Orrù, Gian Luca Marcialis, and Sebastiano Battiato. 2022. The Face Deepfake Detection Challenge. *Journal of Imaging* 8, 10 (2022). https://doi.org/10.3390/jimaging8100263

[135] Luca Guarnera, Oliver Giudice, Cristina Nastasi, and Sebastiano Battiato. 2020. Preliminary forensics analysis of deepfake images. In *2020 AEIT international annual conference (AEIT)*. IEEE, 1–6.

[136] Luca Guarnera, Oliver Giudice, Matthias Niesner, and Sebastiano Battiato. 2022. On the exploitation of Deepfake model recognition. 2022 IEEE. In *CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*.

[137] Gokhan Gul, Ismail Avcibas, and Fatih Kurugollu. 2010. SVD based image manipulation detection. In *2010 IEEE International Conference on Image Processing*. 1765–1768. https://doi.org/10.1109/ICIP.2010.5652854

[138] Benjamin Hadwiger and Christian Riess. 2021. The Forchheim image database for camera identification in the wild. In *Pattern Recognition. ICPR International Workshops and Challenges: Virtual Event, January 10–15, 2021, Proceedings, Part VI*. Springer, 500–515.

[139] Adil Haouzia and Rita Noumeir. 2008. Methods for image authentication: a survey. *Multimedia tools and applications* 39 (2008), 1–46.

[140] Mohammad Farukh Hashmi, Vijay Anand, and Avinas G. Keskar. 2014. Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform. *AASRI Procedia* 9 (2014), 84–91. https://doi.org/10.1016/j.aasri.2014.09.015 2014 AASRI Conference on Circuit and Signal Processing (CSP 2014).

[141] Junfeng He, Zhouchen Lin, Lifeng Wang, and Xiaoou Tang. 2006. Detecting Doctored JPEG Images Via DCT Coefficient Analysis. In *European Conference on Computer Vision*.

[142] Jonatan Henríquez and Werner Kristjanpoller. 2019. A combined Independent Component Analysis–Neural Network model for forecasting exchange rate variation. *Applied Soft Computing* 83 (2019), 105654. https://doi.org/10.1016/j.asoc.2019.105654

[143] Young-Jin Heo, Woon-Ha Yeo, and Byung-Gyu Kim. 2023. Deepfake detection algorithm based on improved vision transformer. *Applied Intelligence* 53, 7 (2023), 7512–7527.

[144] Mario Hildebrandt, Tom Neubert, Andrey Makrushin, and Jana Dittmann. 2017. Benchmarking face morphing forgery detection: Application of stirtrace for impact simulation of different processing steps. In *2017 5th International Workshop on Biometrics and Forensics (IWBF)*. 1–6. https://doi.org/10.1109/IWBF.2017.7935087

[145] Zahra Hossein-Nejad and Mehdi Nasri. 2022. Clustered redundant keypoint elimination method for image mosaicing using a new Gaussian-weighted blending algorithm. *The Visual Computer* 38, 6 (2022), 1991–2007.

[146] Peter Howarth and Stefan Rüger. 2004. Evaluation of Texture Features for Content-Based Image Retrieval. In *Image and Video Retrieval*, Peter Enser, Yiannis Kompatsiaris, Noel E. O'Connor, Alan F. Smeaton, and Arnold W. M. Smeulders (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 326–334.

[147] Yu-Feng Hsu and Shih-Fu Chang. 2006. Detecting image splicing using geometry invariants and camera characteristics consistency. In *2006 IEEE International Conference on Multimedia and Expo*. IEEE, 549–552.

[148] Yu-Feng Hsu and Shih-Fu Chang. 2007. Image Splicing Detection using Camera Response Function Consistency and Automatic Segmentation. In *2007 IEEE International Conference on Multimedia and Expo*. 28–31. https://doi.org/10.1109/ICME.2007.4284578

[149] Yu-Feng Hsu and Shih-Fu Chang. 2010. Camera Response Functions for Image Forensics: An Automatic Algorithm for Splicing Detection. *IEEE Transactions on Information Forensics and Security* 5, 4 (2010), 816–825. https://doi.org/10.1109/TIFS.2010.2077628

[150] Hailing Huang, Weiqiang Guo, and Yu Zhang. 2008. Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm. In *2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, Vol. 2. 272–276. https://doi.org/10.1109/PACIIA.2008.240

[151] Yizhen Huang and Yangjing Long. 2008. Demosaicking recognition with applications in digital photo authentication based on a quadratic pixel correlation model. In *2008 IEEE Conference on Computer Vision and Pattern Recognition*. IEEE, 1–8.

[152] Muhammad Hussain, Ghulam Muhammad, Sahar Q Saleh, Anwar M Mirza, and George Bebis. 2013. Image forgery detection using multi-resolution Weber local descriptors. In *Eurocon 2013*. IEEE, 1570–1577.

[153] Rabha W Ibrahim, Zahra Moghaddasi, Hamid A Jalab, and Rafidah Md Noor. 2015. Fractional differential texture descriptors based on the Machado entropy for image splicing detection. *Entropy* 17, 7 (2015), 4775–4785.

[154] Meera Mary Isaac and M. Wilscy. 2015. Copy-Move Forgery Detection Based on Harris Corner Points and BRISK. In *Proceedings of the Third International Symposium on Women in Computing and Informatics* (Kochi, India) *(WCI '15)*. Association for Computing Machinery, New York, NY, USA, 394–399. https://doi.org/10.1145/2791405.2791453

[155] Md Baharul Islam, Md. Tukhrejul Inam, and Balaji Kaliyaperumal. 2013. Overview and Challenges of Different Image Morphing Algorithms. *International Journal of Advanced Research in Computer Science and Electronics Engineering* 2 (2013).

[156] Sabah Jassim and Aras Asaad. 2018. Automatic detection of image morphing by topology-based analysis. In *2018 26th European Signal Processing Conference (EUSIPCO)*. IEEE, 1007–1011.

[157] Abdul Rehman Javed, Zunera Jalil, Wisha Zehra, Thippa Reddy Gadekallu, Doug Young Suh, and Md Jalil Piran. 2021. A comprehensive survey on digital video forensics: Taxonomy, challenges, and future directions. *Engineering Applications of Artificial Intelligence* 106 (2021), 104456.

[158] Herve Jegou, Matthijs Douze, and Cordelia Schmid. 2008. Hamming embedding and weak geometry consistency for large scale image search-extended version. (2008).

[159] Jesse S Jin, Changsheng Xu, Min Xu, Dai-Kyung Hyun, Min-Jeong Lee, Seung-Jin Ryu, Hae-Yeoun Lee, and Heung-Kyu Lee. 2013. Forgery detection for surveillance video. In *The Era of Interactive Media*. Springer, 25–36.

[160] Wang Jing and Zhang Hongbin. 2006. Exposing Digital Forgeries by Detecting Traces of Image Splicing. In *2006 8th international Conference on Signal Processing*, Vol. 2. https://doi.org/10.1109/ICOSP.2006.345714

[161] Micah K Johnson and Hany Farid. 2005. Exposing digital forgeries by detecting inconsistencies in lighting. In *Proceedings of the 7th workshop on Multimedia and security*. 1–10.

[162] Micah K Johnson and Hany Farid. 2006. Exposing digital forgeries through chromatic aberration. In *Proceedings of the 8th workshop on Multimedia and security*. 48–55.

[163] Micah K Johnson and Hany Farid. 2007. Exposing digital forgeries in complex lighting environments. *IEEE Transactions on Information Forensics and Security* 2, 3 (2007), 450–461.

[164] Micah K. Johnson and Hany Farid. 2008. Detecting Photographic Composites of People. In *Digital Watermarking* (Guangzhou, China) *(Lecture Notes in Computer Science)*, Yun Q. Shi, Hyoung-Joong Kim, and Stefan Katzenbeisser (Eds.). Springer, 19–33. https://doi.org/10.1007/978-3-540-92238-4_3

[165] Micah K Johnson and Hany Farid. 2008. Detecting photographic composites of people. *Digital watermarking* (2008), 19–33.

[166] Pravin Kakar and N. Sudha. 2012. Exposing Postprocessed Copy–Paste Forgeries Through Transform-Invariant Features. *IEEE Transactions on Information Forensics and Security* 7, 3 (2012), 1018–1028. https://doi.org/10.1109/TIFS.2012.2188390

[167] XiaoBing Kang and ShengMin Wei. 2008. Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics. In *2008 International Conference on Computer Science and Software Engineering*, Vol. 3. 926–930. https://doi.org/10.1109/CSSE.2008.876

[168] Eric Kee and Hany Farid. 2010. Exposing digital forgeries from 3-D lighting environments. In *2010 IEEE International Workshop on Information Forensics and Security*. IEEE, 1–6.

[169] Er Saiqa Khan and Er Arun Kulkarni. 1801. An efficient method for detection of copy-move forgery using discrete wavelet transform. *International Journal on Computer Science and Engineering* 2, 5 (1801), 2010.

[170] Ihtiram Raza Khan, Saman Aisha, Deepak Kumar, and Tabish Mufti. 2023. A Systematic Review on Deepfake Technology. *Proceedings of Data Analytics and Management: ICDAM 2022* (2023), 669–685.

[171] Nitin Khanna, George T-C Chiu, Jan P Allebach, and Edward J Delp. 2008. Forensic techniques for classifying scanner, computer generated and digital camera images. In *2008 IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE, 1653–1656.

[172] Nitin Khanna, Aravind K Mikkilineni, and Edward J Delp. 1740. Forensic camera classification: Verification of sensor pattern noise approach. *Fed Bur Invest* 11, 1 (1740).

[173] M. Kharrazi, H.T. Sencar, and N. Memon. 2004. Blind source camera identification. In *2004 International Conference on Image Processing, 2004. ICIP '04.*, Vol. 1. 709–712 Vol. 1. https://doi.org/10.1109/ICIP.2004.1418853

[174] Matthias Kirchner. 2010. Efficient estimation of CFA pattern configuration in digital camera images. In *Media Forensics and Security II*, Nasir D. Memon, Jana Dittmann, Adnan M. Alattar, and Edward J. Delp III (Eds.), Vol. 7541. International Society for Optics and Photonics, SPIE, 754111. https://doi.org/10.1117/12.839102

[175] Matthias Kirchner and Rainer Bohme. 2008. Hiding Traces of Resampling in Digital Images. *IEEE Transactions on Information Forensics and Security* 3, 4 (2008), 582–592. https://doi.org/10.1109/TIFS.2008.2008214
[176] Matthias Kirchner and Thomas Gloe. 2009. On resampling detection in re-compressed images. In *2009 First IEEE international workshop on information forensics and security (WIFS)*. IEEE, 21–25.
[177] Paweł Korus and Jiwu Huang. 2016. Multi-scale analysis strategies in PRNU-based tampering localization. *IEEE Transactions on Information Forensics and Security* 12, 4 (2016), 809–824.
[178] A Kuznetsov. 2019. Digital image forgery detection using deep learning approach. *Journal of Physics: Conference Series* 1368, 3 (nov 2019), 032028. https://doi.org/10.1088/1742-6596/1368/3/032028
[179] Myung-Joon Kwon, Seung-Hun Nam, In-Jae Yu, Heung-Kyu Lee, and Changick Kim. 2022. Learning JPEG compression artifacts for image manipulation detection and localization. *International Journal of Computer Vision* 130, 8 (2022), 1875–1895.
[180] Aaron Langille and Minglun Gong. 2006. An efficient match-based duplication detection algorithm. In *The 3rd Canadian Conference on Computer and Robot Vision (CRV'06)*. IEEE, 64–64.
[181] Wei-Bin Lee and Tung-Her Chen. 2002. A public verifiable copy protection technique for still images. *Journal of Systems and Software* 62, 3 (2002), 195–204.
[182] Stefan Leutenegger, Margarita Chli, and Roland Y. Siegwart. 2011. BRISK: Binary Robust invariant scalable keypoints. In *2011 International Conference on Computer Vision*. 2548–2555. https://doi.org/10.1109/ICCV.2011.6126542
[183] Alex Leykin and Florin Cutzu. 2003. Differences of edge properties in photographs and paintings. In *Proceedings 2003 International Conference on Image Processing (Cat. No. 03CH37429)*, Vol. 3. IEEE, III–541.
[184] Bin Li, Yun Q. Shi, and Jiwu Huang. 2008. Detecting doubly compressed JPEG images by using Mode Based First Digit Features. In *2008 IEEE 10th Workshop on Multimedia Signal Processing*. 730–735. https://doi.org/10.1109/MMSP.2008.4665171
[185] Chang-Tsun Li. 2010. Source camera identification using enhanced sensor pattern noise. *IEEE Transactions on Information Forensics and Security* 5, 2 (2010), 280–287.
[186] Chang-Tsun Li and Yue Li. 2010. Digital camera identification using Colour-Decoupled photo response non-uniformity noise pattern. In *Proceedings of 2010 IEEE International Symposium on Circuits and Systems*. 3052–3055. https://doi.org/10.1109/ISCAS.2010.5537994
[187] Guohui Li, Qiong Wu, Dan Tu, and Shaojie Sun. 2007. A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD. In *2007 IEEE international conference on multimedia and expo*. IEEE, 1750–1753.
[188] Leida Li, Shushang Li, Hancheng Zhu, Shu-Chuan Chu, John F Roddick, and Jeng-Shyang Pan. 2013. An Efficient Scheme for Detecting Copy-move Forged Images by Local Binary Patterns. *J. Inf. Hiding Multim. Signal Process.* 4, 1 (2013), 46–56.
[189] Weihai Li, Nenghai Yu, and Yuan Yuan. 2008. Doctored JPEG image detection. In *2008 IEEE International Conference on Multimedia and Expo*. 253–256. https://doi.org/10.1109/ICME.2008.4607419
[190] Weihai Li, Yuan Yuan, and Nenghai Yu. 2009. Passive detection of doctored JPEG image via block artifact grid extraction. *Signal Processing* 89, 9 (2009), 1821–1829. https://doi.org/10.1016/j.sigpro.2009.03.025
[191] Yanshan Li, Weiming Liu, Xiaotang Li, Qinghua Huang, and Xuelong Li. 2014. GA-SIFT: A new scale invariant feature transform for multispectral image using geometric algebra. *Information Sciences* 281 (2014), 559–572. https://doi.org/10.1016/j.ins.2013.12.022 Multimedia Modeling.
[192] Yuezun Li, Xin Yang, Pu Sun, Honggang Qi, and Siwei Lyu. 2020. Celeb-df: A large-scale challenging dataset for deepfake forensics. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*. 3207–3216.
[193] Zewen Li, Fan Liu, Wenjie Yang, Shouheng Peng, and Jun Zhou. 2021. A survey of convolutional neural networks: analysis, applications, and prospects. *IEEE transactions on neural networks and learning systems* (2021).
[194] Ching-Yung Lin and Shih-Fu Chang. 1997. Robust image authentication method surviving JPEG lossy compression. In *Storage and Retrieval for Image and Video Databases VI*, Vol. 3312. SPIE, 296–307.
[195] Hwei-Jen Lin, Chun-Wei Wang, and Yang-Ta Kao. 2009. Fast Copy-Move Forgery Detection. *WSEAS Trans. Sig. Proc.* 5, 5 (may 2009), 188–197.
[196] W Sabrina Lin, Steve Tjoa, H Vicky Zhao, and KJ Ray Liu. 2007. Image source coding forensics via intrinsic fingerprints. In *2007 IEEE International Conference on Multimedia and Expo*. IEEE, 1127–1130.
[197] Xufeng Lin, Chang-Tsun Li, and Yongjian Hu. 2013. Exposing image forgery through the detection of contrast enhancement. In *2013 IEEE International Conference on Image Processing*. 4467–4471. https://doi.org/10.1109/ICIP.2013.6738920
[198] Xiang Lin, Jian-Hua Li, Shi-Lin Wang, Alan-Wee-Chung Liew, Feng Cheng, and Xiao-Sa Huang. 2018. Recent Advances in Passive Digital Image Security Forensics: A Brief Review. *Engineering* 4, 1 (2018), 29–39. https://doi.org/10.1016/j.eng.2018.02.008 Cybersecurity.
[199] Zhouchen Lin, Junfeng He, Xiaoou Tang, and Chi-Keung Tang. 2009. Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis. *Pattern Recognition* 42, 11 (2009), 2492–2501. https://doi.org/10.1016/j.patcog.2009.03.019
[200] Zhouchen Lin, Rongrong Wang, Xiaoou Tang, and Heung-Yeung Shum. 2005. Detecting doctored images using camera response normality and consistency. In *2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05)*, Vol. 1. 1087–1092 vol. 1. https://doi.org/10.1109/CVPR.2005.125

[201] Bei-Bei Liu, Yongjian Hu, and Heung-Kyu Lee. 2010. Source camera identification from significant noise residual regions. In *2010 IEEE International Conference on Image Processing*. IEEE, 1749–1752.

[202] Qingzhong Liu and Andrew H. Sung. 2009. A new approach for JPEG resize and image splicing detection. In *MiFor '09*.

[203] Wei Lu, Wei Sun, Ji-Wu Huang, and Hong-Tao Lu. 2008. Digital image forensics using statistical features and neural network classifier. In *2008 International Conference on Machine Learning and Cybernetics*, Vol. 5. IEEE, 2831–2834.

[204] Jan Lukas, Jessica Fridrich, and Miroslav Goljan. 2006. Digital camera identification from sensor pattern noise. *IEEE Transactions on Information Forensics and Security* 1, 2 (2006), 205–214.

[205] Weiqi Luo, Jiwu Huang, and Guoping Qiu. 2006. Robust detection of region-duplication forgery in digital image. In *18th International Conference on Pattern Recognition (ICPR'06)*, Vol. 4. IEEE, 746–749.

[206] Weiqi Luo, Zhenhua Qu, Feng Pan, and Jiwu Huang. 2007. A survey of passive technology for digital image forensics. *Frontiers of Computer Science in China* 1 (2007), 166–179.

[207] Yingda Lv, Xuanjing Shen, and Haipeng Chen. 2011. An improved image blind identification based on inconsistency in light source direction. *The Journal of Supercomputing* 58 (2011), 50–67.

[208] S. Lyu and H. Farid. 2005. How realistic is photorealistic? *IEEE Transactions on Signal Processing* 53, 2 (2005), 845–850. https://doi.org/10.1109/TSP.2004.839896

[209] Babak Mahdian and Stanislav Saic. 2007. Detection of copy–move forgery using a method based on blur moment invariants. *Forensic science international* 171, 2-3 (2007), 180–189.

[210] Babak Mahdian and Stanislav Saic. 2008. Blind authentication using periodic properties of interpolation. *IEEE Transactions on Information Forensics and Security* 3, 3 (2008), 529–538.

[211] Babak Mahdian and Stanislav Saic. 2009. A cyclostationarity analysis applied to image forensics. In *2009 Workshop on Applications of Computer Vision (WACV)*. IEEE, 1–6.

[212] Babak Mahdian and Stanislav Saic. 2009. Detecting double compressed JPEG images. In *International Conferences on Imaging for Crime Detection and Prevention*.

[213] Babak Mahdian and Stanislav Saic. 2010. A bibliography on blind methods for identifying image forgery. *Signal Processing: Image Communication* 25, 6 (2010), 389–399. https://doi.org/10.1016/j.image.2010.05.003

[214] Babak Mahdian and Stanislav Saic. 2010. Blind methods for detecting image fakery. *IEEE Aerospace and Electronic Systems Magazine* 25, 4 (2010), 18–24.

[215] Toqeer Mahmood, Zahid Mehmood, Mohsin Shah, and Tanzila Saba. 2018. A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform. *Journal of Visual Communication and Image Representation* 53 (2018), 202–214.

[216] Khaled Mahmoud and Arwa Husien. 2016. Copy-move forgery detection using zernike and pseudo zernike moments. *Int. Arab J. Inf. Technol.* 13, 6A (2016), 930–937.

[217] Nasrin M. Makbol, Bee Ee Khoo, and Taha H. Rassem. 2016. Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. *IET Image Processing* 10, 1 (2016), 34–52. https://doi.org/10.1049/iet-ipr.2014.0965 arXiv:https://ietresearch.onlinelibrary.wiley.com/doi/pdf/10.1049/iet-ipr.2014.0965

[218] Andrey Makrushin, Tom Neubert, and Jana Dittmann. 2017. Automatic Generation and Detection of Visually Faultless Facial Morphs.. In *VISIGRAPP (6: VISAPP)*. 39–50.

[219] Andrey Makrushin and Andreas Wolf. 2018. An overview of recent advances in assessing and mitigating the face morphing attack. In *2018 26th European Signal Processing Conference (EUSIPCO)*. IEEE, 1017–1021.

[220] Francesco Marra, Diego Gragnaniello, Luisa Verdoliva, and Giovanni Poggi. 2020. A full-image full-resolution end-to-end-trainable CNN framework for image forgery detection. *IEEE Access* 8 (2020), 133488–133502.

[221] Sarah Mercer, Kyle Read Talbot, and Isobel Kai-Hui Wang. 2021. Fake or real engagement–looks can be deceiving. *Student engagement in the language classroom* (2021), 143–162.

[222] Hai Min, Wei Jia, Xiao-Feng Wang, Yang Zhao, Rong-Xiang Hu, Yue-Tong Luo, Feng Xue, and Jing-Ting Lu. 2015. An intensity-texture model based level set method for image segmentation. *Pattern Recognition* 48, 4 (2015), 1547–1562.

[223] Saraju P Mohanty. 1999. Digital watermarking: A tutorial review. *URL: http://www. csee. usf. edu/~ smohanty/research/Reports/WMSurvey1999Mohanty. pdf* (1999).

[224] Ghulam Muhammad, Muhammad Hussain, and George Bebis. 2012. Passive copy move image forgery detection using undecimated dyadic wavelet transform. *Digital investigation* 9, 1 (2012), 49–57.

[225] Saba Mushtaq and Ajaz Hussain Mir. 2014. Digital image forgeries and passive image authentication techniques: a survey. *International Journal of Advanced Science and Technology* 73 (2014), 15–32.

[226] Gul Muzaffer and Guzin Ulutas. 2019. A new deep learning-based method to detection of copy-move forgery in digital images. In *2019 Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT)*. 1–4. https://doi.org/10.1109/EBBT.2019.8741657

[227] AN Myna, MG Venkateshmurthy, and CG Patil. 2007. Detection of region duplication forgery in digital images using wavelets and log-polar mapping. In *International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007)*, Vol. 3. IEEE, 371–377.

[228] Syed Tufael Nabi, Munish Kumar, Paramjeet Singh, Naveen Aggarwal, and Krishan Kumar. 2022. A comprehensive survey of image and video forgery techniques: variants, challenges, and future directions. *Multimedia Systems* 28, 3 (2022), 939–992.

[229] L. Nataraj, A. Sarkar, and B. S. Manjunath. 2009. Adding Gaussian noise to "denoise" JPEG for detecting image resizing. In *2009 16th IEEE International Conference on Image Processing (ICIP)*. 1493–1496. https://doi.org/10.1109/ICIP.2009.5414609

[230] Lakshmanan Nataraj, Anindya Sarkar, and Bangalore S Manjunath. 2010. Improving re-sampling detection by adding noise. In *Media Forensics and Security II*, Vol. 7541. SPIE, 177–187.

[231] Ramesh Neelamani, Ricardo De Queiroz, Zhigang Fan, Sanjeeb Dash, and Richard G Baraniuk. 2006. JPEG compression history estimation for color images. *IEEE Transactions on Image Processing* 15, 6 (2006), 1365–1378.

[232] Tom Neubert. 2017. Face morphing detection: An approach based on image degradation analysis. In *Digital Forensics and Watermarking: 16th International Workshop, IWDW 2017, Magdeburg, Germany, August 23-25, 2017, Proceedings 16*. Springer, 93–106.

[233] Tom Neubert, Christian Kraetzer, and Jana Dittmann. 2019. A Face Morphing Detection Concept with a Frequency and a Spatial Domain Feature Space for Images on EMRTD. In *Proceedings of the ACM Workshop on Information Hiding and Multimedia Security* (Paris, France) *(IH & MMSec'19)*. Association for Computing Machinery, New York, NY, USA, 95–100. https://doi.org/10.1145/3335203.3335721

[234] Tian-Tsong Ng. 2009. Camera response function signature for digital forensics - Part II: Signature extraction. In *2009 First IEEE International Workshop on Information Forensics and Security (WIFS)*. 161–165. https://doi.org/10.1109/WIFS.2009.5386461

[235] T-T Ng and S-F Chang. 2004. A model for image splicing. In *2004 International Conference on Image Processing, 2004. ICIP'04.*, Vol. 2. IEEE, 1169–1172.

[236] Tian-Tsong Ng and Shih-Fu Chang. 2006. An online system for classifying computer graphics images from natural photographs. In *Security, Steganography, and Watermarking of Multimedia Contents VIII*, Vol. 6072. SPIE, 397–405.

[237] Tian-Tsong Ng, Shih-Fu Chang, and Q Sun. [n. d.]. A data set of authentic and spliced image blocks.Tech. Rep. DVMM, Columbia University (2004). ([n. d.]).

[238] Tian-Tsong Ng, Shih-Fu Chang, and Qibin Sun. 2004. Blind detection of photomontage using higher order statistics. In *2004 IEEE International Symposium on Circuits and Systems (ISCAS)*, Vol. 5. V–V. https://doi.org/10.1109/ISCAS.2004.1329901

[239] Tian-Tsong Ng, Shih-Fu Chang, and Mao-Pei Tsui. 2007. Lessons learned from online classification of photo-realistic computer graphics and photographs. In *2007 IEEE Workshop on Signal Processing Applications for Public Security and Forensics*. IEEE, 1–6.

[240] Tian-Tsong Ng and Mao-Pei Tsui. 2009. Camera response function signature for digital forensics - Part I: Theory and data selection. In *2009 First IEEE International Workshop on Information Forensics and Security (WIFS)*. 156–160. https://doi.org/10.1109/WIFS.2009.5386464

[241] Hieu Cuong Nguyen and Stefan Katzenbeisser. 2012. Detection of copy-move forgery in digital images using radon transformation and phase correlation. In *2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. IEEE, 134–137.

[242] Nitish Nirmalkar, Shailesh Kamble, and Sandeep Kakde. 2015. A review of image forgery techniques and their detection. In *2015 international conference on innovations in information, embedded and communication systems (ICIIECS)*. IEEE, 1–5.

[243] Adam Novozamsky, Babak Mahdian, and Stanislav Saic. 2020. IMD2020: A large-scale annotated dataset tailored for detecting manipulated images. In *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision Workshops*. 71–80.

[244] Junlin Ouyang, Yizhi Liu, and Miao Liao. 2017. Copy-move forgery detection based on deep learning. In *2017 10th international congress on image and signal processing, biomedical engineering and informatics (CISP-BMEI)*. IEEE, 1–5.

[245] Junlin Ouyang, Yizhi Liu, and Miao Liao. 2019. Robust copy-move forgery detection method using pyramid model and Zernike moments. *Multimedia Tools and Applications* 78 (2019), 10207–10225.

[246] Guansong Pang, Chunhua Shen, Longbing Cao, and Anton Van Den Hengel. 2021. Deep learning for anomaly detection: A review. *ACM computing surveys (CSUR)* 54, 2 (2021), 1–38.

[247] Cecilia Pasquini, Irene Amerini, and Giulia Boato. 2021. Media forensics on social media platforms: a survey. *EURASIP Journal on Information Security* 2021, 1 (2021), 1–19.

[248] Anjie Peng, Yadong Wu, and Xiangui Kang. 2017. Revealing traces of image resampling and resampling antiforensics. *Advances in Multimedia* 2017 (2017).

[249] Fei Peng, Le-Bing Zhang, and Min Long. 2019. FD-GAN: Face de-morphing generative adversarial network for restoring accomplice's facial image. *IEEE Access* 7 (2019), 75122–75131.

[250] Jin Peng, Yinghao Li, Chengming Liu, and Xiaomeng Gao. 2023. The Circular U-Net with Attention Gate for Image Splicing Forgery Detection. *Electronics* 12, 6 (2023). https://doi.org/10.3390/electronics12061451

[251] Lin Peng, Xin Liao, and Mingliang Chen. 2021. Resampling parameter estimation via dual-filtering based convolutional neural network. *Multimedia Systems* 27 (2021), 363–370.

[252] Tomas Pevny and Jessica Fridrich. 2008. Detection of Double-Compression in JPEG Images for Applications in Steganography. *IEEE Transactions on Information Forensics and Security* 3, 2 (2008), 247–258. https://doi.org/10.1109/TIFS.2008.922456

[253] Tomáš Pevný and Jessica Fridrich. 2008. Estimation of primary quantization matrix for steganalysis of double-compressed JPEG images. In *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, Edward J. Delp III, Ping Wah Wong, Jana Dittmann, and Nasir D. Memon (Eds.), Vol. 6819. International Society for Optics and Photonics, SPIE, 681911. https://doi.org/10.1117/12.759155
[254] Alessandro Piva. 2013. An overview on image forensics. *International Scholarly Research Notices* 2013 (2013).
[255] Mark Pollitt. 2010. A history of digital forensics. In *Advances in Digital Forensics VI: Sixth IFIP WG 11.9 International Conference on Digital Forensics, Hong Kong, China, January 4-6, 2010, Revised Selected Papers 6*. Springer, 3–15.
[256] Alin C Popescu and Hany Farid. 2004. Exposing digital forgeries by detecting duplicated image regions.Computer Science Technical Report TR2004-515. (2004).
[257] Alin C. Popescu and Hany Farid. 2004. Statistical Tools for Digital Forensics. In *Information Hiding*.
[258] Alin C Popescu and Hany Farid. 2005. Exposing digital forgeries by detecting traces of resampling. *IEEE Transactions on signal processing* 53, 2 (2005), 758–767.
[259] Sabyasachi Pramanik, Samir Kumar Bandyopadhyay, and Ramkrishna Ghosh. 2020. Signature image hiding in color image using steganography and cryptography based on digital signature concepts. In *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*. IEEE, 665–669.
[260] Santasriya Prasad and KR Ramakrishnan. 2006. On resampling detection and its application to detect image tampering. In *2006 IEEE International Conference on Multimedia and Expo*. IEEE, 1325–1328.
[261] OM Prathibha, NS Swathikumari, and P Sushma. 2012. Image forgery detection using dyadic Wavelet transform. *Int. J. Electron. Sig. Syst* 2 (2012), 41–43.
[262] Zhenhua Qu, Weiqi Luo, and Jiwu Huang. 2008. A convolutive mixing model for shifted double JPEG compression with application to passive image authentication. In *2008 IEEE International Conference on Acoustics, Speech and Signal Processing*. 1661–1664. https://doi.org/10.1109/ICASSP.2008.4517946
[263] Weize Quan, Kai Wang, Dong-Ming Yan, and Xiaopeng Zhang. 2018. Distinguishing Between Natural and Computer-Generated Images Using Convolutional Neural Networks. *IEEE Transactions on Information Forensics and Security* 13, 11 (2018), 2772–2787. https://doi.org/10.1109/TIFS.2018.2834147
[264] Muhammad Ali Qureshi and Mohamed Deriche. 2015. A bibliography of pixel-based blind image forgery detection techniques. *Signal Processing: Image Communication* 39 (2015), 46–74. https://doi.org/10.1016/j.image.2015.08.008
[265] R. Raghavendra, Kiran B. Raja, and Christoph Busch. 2016. Detecting morphed face images. In *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*. 1–7. https://doi.org/10.1109/BTAS.2016.7791169
[266] R. Raghavendra, Kiran B. Raja, Sushma Venkatesh, and Christoph Busch. 2017. Transferable Deep-CNN Features for Detecting Digital and Print-Scanned Morphed Face Images. In *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*. 1822–1830. https://doi.org/10.1109/CVPRW.2017.228
[267] Md Shohel Rana, Mohammad Nur Nobi, Beddhu Murali, and Andrew H Sung. 2022. Deepfake detection: A systematic literature review. *IEEE access* 10 (2022), 25494–25513.
[268] Yuan Rao and Jiangqun Ni. 2016. A deep learning approach to detection of splicing and copy-move forgeries in images. In *2016 IEEE international workshop on information forensics and security (WIFS)*. IEEE, 1–6.
[269] Karen Reid. 2011. *A practitioner's guide to the European Convention on Human Rights*. Sweet & Maxwell.
[270] K Remya Revi, KR Vidya, and M Wilscy. 2021. Detection of Deepfake Images Created Using Generative Adversarial Networks: A Review. In *Second International Conference on Networks and Advances in Computational Technologies: NetACT 19*. Springer, 25–35.
[271] Christian Rey and Jean-Luc Dugelay. 2002. A survey of watermarking algorithms for image authentication. *EURASIP Journal on Advances in Signal Processing* 2002, 6 (2002), 1–9.
[272] Seung-Jin Ryu, Min-Jeong Lee, and Heung-Kyu Lee. 2010. Detection of copy-rotate-move forgery using Zernike moments. In *Information Hiding: 12th International Conference, IH 2010, Calgary, AB, Canada, June 28-30, 2010, Revised Selected Papers 12*. Springer, 51–65.
[273] Akram Hatem Saber, Mohd Ayyub Khan, and Basim Galeb Mejbel. 2020. A Survey on Image Forgery Detection Using Different Forensic Approaches. *Advances in Science, Technology and Engineering Systems Journal* 5, 3 (2020), 361–370. https://doi.org/10.25046/aj050347
[274] Somayeh Sadeghi, Sajjad Dadkhah, Hamid A Jalab, Giuseppe Mazzola, and Diaa Uliyan. 2018. State of the art in passive digital image forgery detection: copy-move image forgery. *Pattern Analysis and Applications* 21, 2 (2018), 291–306.
[275] Ronald Salloum, Yuzhuo Ren, and C-C Jay Kuo. 2018. Image splicing localization using a multi-task fully convolutional network (MFCN). *Journal of Visual Communication and Image Representation* 51 (2018), 201–209.
[276] Gopinath Sankar, Vicky Zhao, and Yee-Hong Yang. 2009. Feature based classification of computer graphics and real images. In *2009 IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE, 1513–1516.
[277] Anindya Sarkar, Lakshmanan Nataraj, and Bangalore S Manjunath. 2009. Detection of seam carving and localization of seam insertions in digital images. In *Proceedings of the 11th ACM workshop on Multimedia and security*. 107–116.
[278] Gerald Schaefer and Michal Stich. 2003. UCID: An uncompressed color image database. In *Storage and Retrieval Methods and Applications for Multimedia 2004*, Vol. 5307. SPIE, 472–480.

[279] Ulrich Scherhag, Christian Rathgeb, and Christoph Busch. 2018. Towards Detection of Morphed Face Images in Electronic Travel Documents. In *2018 13th IAPR International Workshop on Document Analysis Systems (DAS)*. 187–192. https://doi.org/10.1109/DAS.2018.11

[280] Clemens Seibold, Wojciech Samek, Anna Hilsmann, and Peter Eisert. 2017. Detection of Face Morphing Attacks by Deep Learning. In *Digital Forensics and Watermarking*, Christian Kraetzer, Yun-Qing Shi, Jana Dittmann, and Hyoung Joong Kim (Eds.). Springer International Publishing, Cham, 107–120.

[281] Clemens Seibold, Wojciech Samek, Anna Hilsmann, and Peter Eisert. 2020. Accurate and robust neural networks for face morphing attack detection. *Journal of Information Security and Applications* 53 (2020), 102526. https://doi.org/10.1016/j.jisa.2020.102526

[282] Hanieh Shabanian and Farshad Mashhadi. 2017. A new approach for detecting copy-move forgery in digital images. In *2017 IEEE Western New York Image and Signal Processing Workshop (WNYISPW)*. 1–6. https://doi.org/10.1109/WNYIPW.2017.8356252

[283] Wuyang Shan, Yaohua Yi, Ronggang Huang, and Yong Xie. 2019. Robust contrast enhancement forensics based on convolutional neural networks. *Signal Processing: Image Communication* 71 (2019), 138–146. https://doi.org/10.1016/j.image.2018.11.011

[284] Puneet Kr Sharma. 2012. Rajni: Analysis of image watermarking using least significant bit algorithm. *International Journal of Information Sciences and Techniques (IJIST) Vol* 2 (2012), 95–101.

[285] Yun Q. Shi, Chunhua Chen, and Wen Chen. 2007. A Natural Image Model Approach to Splicing Detection. In *Proceedings of the 9th Workshop on Multimedia & Security* (Dallas, Texas, USA) *(MM & Sec '07)*. Association for Computing Machinery, New York, NY, USA, 51–62. https://doi.org/10.1145/1288869.1288878

[286] BL Shivakumar and S Santhosh Baboo. 2011. Detection of region duplication forgery in digital images using SURF. *International Journal of Computer Science Issues (IJCSI)* 8, 4 (2011), 199.

[287] Dasara Shullani, Marco Fontani, Massimo Iuliani, Omar Al Shaya, and Alessandro Piva. 2017. Vision: a video and image dataset for source identification. *EURASIP Journal on Information Security* 2017, 1 (2017), 1–16.

[288] Ewerton Silva, Tiago Carvalho, Anselmo Ferreira, and Anderson Rocha. 2015. Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes. *Journal of Visual Communication and Image Representation* 29 (2015), 16–32.

[289] Badal Soni, Pradip K. Das, and Dalton Meitei Thounaojam. 2017. Blur Invariant Block Based Copy-Move Forgery Detection Technique Using FWHT Features. In *Proceedings of the International Conference on Watermarking and Image Processing* (Paris, France) *(ICWIP 2017)*. Association for Computing Machinery, New York, NY, USA, 22–26. https://doi.org/10.1145/3150978.3150987

[290] Matthew James Sorell. 2009. Conditions for effective detection and identification of primary quantisation of re-quantized JPEG images. *International Journal of Digital Crime and Forensics (IJDCF)* 1, 2 (2009), 13–27.

[291] Springer 2011. *Tampered region localization of digital color images based on jpeg compression noise*. Springer.

[292] Matthew C. Stamm and K.J. Ray Liu. 2010. Forensic detection of image manipulation using statistical intrinsic fingerprints. *IEEE Transactions on Information Forensics and Security* 5, 3 (2010), 492–506. https://doi.org/10.1109/TIFS.2010.2053202

[293] Matthew C Stamm and KJ Ray Liu. 2010. Forensic estimation and reconstruction of a contrast enhancement mapping. In *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE, 1698–1701.

[294] Dan-Cristian Stanciu and Bogdan Ionescu. 2023. Autoencoder-based Data Augmentation for Deepfake Detection. In *Proceedings of the 2nd ACM International Workshop on Multimedia AI against Disinformation*. 19–27.

[295] Baina Su and Zhu Kaizhen. 2012. Detection of Copy Forgery in Digital Images Based on LPP-SIFT. In *2012 International Conference on Industrial Control and Electronics Engineering*. 1773–1776. https://doi.org/10.1109/ICICEE.2012.469

[296] Patchara Sutthiwan, Jingyu Ye, and Yun Q Shi. 2009. An enhanced statistical approach to identifying photorealistic images. In *Digital Watermarking: 8th International Workshop, IWDW 2009, Guildford, UK, August 24-26, 2009. Proceedings 8*. Springer, 323–335.

[297] Ashwin Swaminathan, Min Wu, and KJ Ray Liu. 2006. Image tampering identification using blind deconvolution. In *2006 International Conference on Image Processing*. IEEE, 2309–2312.

[298] Ashwin Swaminathan, Min Wu, and KJ Ray Liu. 2007. Nonintrusive component forensics of visual sensors using output images. *IEEE Transactions on Information Forensics and Security* 2, 1 (2007), 91–106.

[299] Jun Takamatsu, Yasuyuki Matsushita, Tsukasa Ogasawara, and Katsushi Ikeuchi. 2010. Estimating demosaicing algorithms using image noise variance. In *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*. IEEE, 279–286.

[300] Hideyuki Tamura, Shunji Mori, and Takashi Yamawaki. 1978. Textural Features Corresponding to Visual Perception. *IEEE Transactions on Systems, Man, and Cybernetics* 8, 6 (1978), 460–473. https://doi.org/10.1109/TSMC.1978.4309999

[301] Omar Tayan, Muhammad N Kabir, and Yasser M Alginahi. 2014. A hybrid digital-signature and zero-watermarking approach for authentication and protection of sensitive electronic documents. *The scientific world journal* 2014 (2014).

[302] Huawei Tian, Yanhui Xiao, Gang Cao, Yongsheng Zhang, Zhiyin Xu, and Yao Zhao. 2019. Daxing smartphone identification dataset. *IEEE Access* 7 (2019), 101046–101053.

[303] Steven Tjoa, W Sabrina Lin, H Vicky Zhao, and KJ Ray Liu. 2007. Block size forensic analysis in digital images. In *2007 IEEE International Conference on Acoustics, Speech and Signal Processing-ICASSP'07*, Vol. 1. IEEE, I–633.

[304] Radhika v Totla and KS Bapat. 2013. Comparative analysis of watermarking in digital images using DCT & DWT. *International Journal of Scientific and Research Publications* 3, 2 (2013), 1–4.

[305] Dijana Tralic, Ivan Zupancic, Sonja Grgic, and Mislav Grgic. 2013. CoMoFoD—New database for copy-move forgery detection. In *Proceedings ELMAR-2013*. IEEE, 49–54.

[306] Matthieu Urvoy, Dalila Goudia, and Florent Autrusseau. 2014. Perceptual DFT Watermarking With Improved Detection and Robustness to Geometrical Distortions. *IEEE Transactions on Information Forensics and Security* 9, 7 (2014), 1108–1119. https://doi.org/10.1109/TIFS.2014.2322497

[307] Sushma Venkatesh, Raghavendra Ramachandra, Kiran Raja, and Christoph Busch. 2021. Face morphing attack generation and detection: A comprehensive survey. *IEEE transactions on technology and society* 2, 3 (2021), 128–145.

[308] Sushma Venkatesh, Raghavendra Ramachandra, Kiran Raja, Luuk Spreeuwers, Raymond Veldhuis, and Christoph Busch. 2020. Detecting Morphed Face Attacks Using Residual Noise from Deep Multi-scale Context Aggregation Network. In *2020 IEEE Winter Conference on Applications of Computer Vision (WACV)*. 269–278. https://doi.org/10.1109/WACV45572.2020.9093488

[309] Sebastiano Verde, Cecilia Pasquini, Federica Lago, Alessandro Goller, Francesco De Natale, Alessandro Piva, and Giulia Boato. 2023. Multi-clue reconstruction of sharing chains for social media images. *IEEE Transactions on Multimedia* (2023), 1–15. https://doi.org/10.1109/TMM.2023.3253389

[310] Luisa Verdoliva. 2020. Media forensics and deepfakes: an overview. *IEEE Journal of Selected Topics in Signal Processing* 14, 5 (2020), 910–932.

[311] David Vázquez-Padín and Fernando Pérez-González. 2011. Prefilter design for forensic resampling estimation. In *2011 IEEE International Workshop on Information Forensics and Security*. 1–6. https://doi.org/10.1109/WIFS.2011.6123133

[312] Savita Walia and Krishan Kumar. 2019. Digital image forgery detection: a systematic scrutiny. *Australian Journal of Forensic Sciences* 51, 5 (2019), 488–526. https://doi.org/10.1080/00450618.2018.1424241 arXiv:https://doi.org/10.1080/00450618.2018.1424241

[313] Lukasz Wandzik, Gerald Kaeding, and Raul Vicente Garcia. 2018. Morphing Detection Using a General- Purpose Face Recognition System. In *2018 26th European Signal Processing Conference (EUSIPCO)*. 1012–1016. https://doi.org/10.23919/EUSIPCO.2018.8553375

[314] Junwen Wang, Guangjie Liu, Hongyuan Li, Yuewei Dai, and Zhiquan Wang. 2009. Detection of Image Region Duplication Forgery Using Model with Circle Block. In *2009 International Conference on Multimedia Information Networking and Security*, Vol. 1. 25–29. https://doi.org/10.1109/MINES.2009.142

[315] Wei Wang, Jing Dong, and Tieniu Tan. 2009. Effective image splicing detection based on image chroma. In *2009 16th IEEE international conference on image processing (ICIP)*. IEEE, 1257–1260.

[316] Xinyi Wang, He Wang, Shaozhang Niu, and Jiwei Zhang. 2019. Detection and localization of image forgeries using improved mask regional convolutional neural network. *Mathematical Biosciences and Engineering* 16, 5 (2019), 4581–4593.

[317] Yuan Wang, Lihua Tian, and Chen Li. 2017. LBP-SVD based copy move forgery detection algorithm. In *2017 IEEE international symposium on multimedia (ISM)*. IEEE, 553–556.

[318] Kanoksak Wattanachote, Timothy K Shih, Wen-Lung Chang, and Hon-Hang Chang. 2015. Tamper detection of JPEG image due to seam modifications. *IEEE transactions on information forensics and security* 10, 12 (2015), 2477–2491.

[319] Weimin Wei, Shuozhong Wang, and Zhenjun Tang. 2008. Estimation of rescaling factor and detection of image splicing. In *2008 11th IEEE International Conference on Communication Technology*. IEEE, 676–679.

[320] Bihan Wen, Ye Zhu, Ramanathan Subramanian, Tian-Tsong Ng, Xuanjing Shen, and Stefan Winkler. 2016. COVERAGE—A novel database for copy-move forgery detection. In *2016 IEEE international conference on image processing (ICIP)*. IEEE, 161–165.

[321] PAWAN WHIG et al. 2022. More on Convolution Neural Network CNN. *International Journal of Sustainable Development in Computing Science* 4, 1 (2022).

[322] David Wicki-Birchler. 2020. The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime? *International Cybersecurity Law Review* 1 (2020), 63–72.

[323] Raymond B Wolfgang and Edward J Delp III. 1999. Fragile watermarking using the VW2D watermark. In *Security and Watermarking of Multimedia Contents*, Vol. 3657. SPIE, 204–213.

[324] Qiong Wu, Shao-Jie Sun, Wei Zhu, Guo-Hui Li, and Dan Tu. 2008. Detection of digital doctoring in exemplar-based inpainted images. In *2008 international conference on machine learning and cybernetics*, Vol. 3. IEEE, 1222–1226.

[325] Qiumin Wu, Shuozhong Wang, and Xinpeng Zhang. 2011. Log-polar based scheme for revealing duplicated regions in digital images. *IEEE Signal Processing Letters* 18, 10 (2011), 559–562.

[326] Yue Wu, Wael Abd-Almageed, and Prem Natarajan. 2018. Busternet: Detecting copy-move image forgery with source/target localization. In *Proceedings of the European conference on computer vision (ECCV)*. 168–184.

[327] Duorui Xie, Lingyu Liang, Lianwen Jin, Jie Xu, and Mengru Li. 2015. Scut-fbp: A benchmark dataset for facial beauty perception. In *2015 IEEE International Conference on Systems, Man, and Cybernetics*. IEEE, 1821–1826.

[328] Liehua Xie and Gonzalo R Arce. 1998. A blind wavelet based digital signature for image authentication. In *9th European Signal Processing Conference (EUSIPCO 1998)*. IEEE, 1–4.

[329] Liehua Xie, Gonzalo R Arce, Arianne Lewis, and EB Basch. 2000. Image enhancement towards soft image authentication. In *2000 IEEE International Conference on Multimedia and Expo. ICME2000. Proceedings. Latest Advances in the Fast Changing World of Multimedia (Cat. No. 00TH8532)*, Vol. 1. IEEE, 497–500.

[330] Preeti Yadav and Yogesh Rathore. 2012. Detection of copy-move forgery of images using discrete wavelet transform. *International Journal on Computer Science and Engineering* 4, 4 (2012), 565.

[331] Fan Yang, Jingwei Li, Wei Lu, and Jian Weng. 2017. Copy-move forgery detection based on hybrid features. *Engineering Applications of Artificial Intelligence* 59 (2017), 73–83. https://doi.org/10.1016/j.engappai.2016.12.022

[332] Pengpeng Yang, Daniele Baracchi, Rongrong Ni, Yao Zhao, Fabrizio Argenti, and Alessandro Piva. 2020. A survey of deep learning-based source image forensics. *Journal of Imaging* 6, 3 (2020), 9.

[333] Ziming Yang, Jian Liang, Yuting Xu, Xiao-Yu Zhang, and Ran He. 2023. Masked relation learning for deepfake detection. *IEEE Transactions on Information Forensics and Security* 18 (2023), 1696–1708.

[334] Hongwei Yao, Tong Qiao, Ming Xu, and Ning Zheng. 2018. Robust Multi-Classifier for Camera Model Identification Based on Convolution Neural Network. *IEEE Access* 6 (2018), 24973–24982. https://doi.org/10.1109/ACCESS.2018.2832066

[335] Shuiming Ye, Qibin Sun, and Ee-Chien Chang. 2007. Detecting digital image forgeries by measuring inconsistencies of blocking artifact. In *2007 IEEE International Conference on Multimedia and Expo*. Ieee, 12–15.

[336] Minerva M Yeung and Fred Mintzer. 1997. An invisible watermarking technique for image verification. In *Proceedings of international conference on image processing*, Vol. 2. IEEE, 680–683.

[337] Jun Yu, Scott Craver, and Enping Li. 2011. Toward the identification of DSLR lenses by chromatic aberration. In *Media Watermarking, Security, and Forensics III*, Vol. 7880. SPIE, 373–381.

[338] Markos Zampoglou, Symeon Papadopoulos, and Yiannis Kompatsiaris. 2015. Detecting image splicing in the wild (web). In *2015 IEEE International Conference on Multimedia & Expo Workshops (ICMEW)*. IEEE, 1–6.

[339] Marcello Zanardelli, Fabrizio Guerrini, Riccardo Leonardi, and Nicola Adami. 2022. Image forgery detection: a survey of recent deep-learning approaches. *Multimedia Tools and Applications* (2022), 1–46.

[340] Jishen Zeng, Shunquan Tan, Bin Li, and Jiwu Huang. 2018. Large-Scale JPEG Image Steganalysis Using Hybrid Deep-Learning Framework. *IEEE Transactions on Information Forensics and Security* 13, 5 (2018), 1200–1214. https://doi.org/10.1109/TIFS.2017.2779446

[341] Chenshuang Zhang, Chaoning Zhang, Sheng Zheng, Mengchun Zhang, Maryam Qamar, Sung-Ho Bae, and In So Kweon. 2023. A survey on audio diffusion models: Text to speech synthesis and enhancement in generative ai. *arXiv preprint arXiv:2303.13336* 2 (2023).

[342] Jing Zhang, Zhanlei Feng, and Yuting Su. 2008. A new approach for detecting Copy-Move forgery in digital images. In *2008 11th IEEE Singapore International Conference on Communication Systems*. 362–366. https://doi.org/10.1109/ICCS.2008.4737205

[343] Jing Zhang, Haiying Wang, and Yuting Su. 2008. Detection of Double-Compression in JPEG2000 Images. In *2008 Second International Symposium on Intelligent Information Technology Application*, Vol. 1. 418–421. https://doi.org/10.1109/IITA.2008.83

[344] Le-Bing Zhang, Fei Peng, and Min Long. 2018. Face morphing detection using Fourier spectrum of sensor pattern noise. In *2018 IEEE international conference on multimedia and expo (ICME)*. IEEE, 1–6.

[345] Wei Zhang, Xiaochun Cao, Yanling Qu, Yuexian Hou, Handong Zhao, and Chenyang Zhang. 2010. Detecting and Extracting the Photo Composites Using Planar Homography and Graph Cut. *IEEE Transactions on Information Forensics and Security* 5, 3 (2010), 544–555. https://doi.org/10.1109/TIFS.2010.2051666

[346] Ying Zhang, Jonathan Goh, Lei Lei Win, and Vrizlynn LL Thing. 2016. Image region forgery detection: A deep learning approach. *SG-CRC* 2016 (2016), 1–11.

[347] Zhen Zhang, Jiquan Kang, and Yuan Ren. 2008. An effective algorithm of image splicing detection. In *2008 international conference on computer science and software engineering*, Vol. 1. IEEE, 1035–1039.

[348] Zhen Zhang, GuangHua Wang, Yukun Bian, and Zhou Yu. 2010. A novel model for splicing detection. In *2010 IEEE Fifth International Conference on Bio-Inspired Computing: Theories and Applications (BIC-TA)*. IEEE, 962–965.

[349] Xudong Zhao, Jianhua Li, Shenghong Li, and Shilin Wang. 2011. Detecting Digital Image Splicing in Chroma Spaces. In *Digital Watermarking*, Hyoung-Joong Kim, Yun Qing Shi, and Mauro Barni (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 12–22.

[350] Lilei Zheng, Ying Zhang, and Vrizlynn L.L. Thing. 2019. A survey on image tampering and its detection in real-world photos. *Journal of Visual Communication and Image Representation* 58 (2019), 380–399. https://doi.org/10.1016/j.jvcir.2018.12.022

[351] Nan Zhu, Cheng Deng, and Xinbo Gao. 2017. Image sharpening detection based on multiresolution overshoot artifact analysis. *Multimedia Tools and Applications* 76 (2017), 16563–16580.