symmetry

MDPI

Article

Recent Advances in Digital Multimedia Tampering Detection for Forensics Analysis

Sami Bourouis [1,2,*], Roobaea Alroobaea [1], Abdullah M. Alharbi [3] and Murad Andejany [3] and Saeed Rubaiee [3]

[1] Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, P.O. Box 11099, Taif 21944, Saudi Arabia; r.robai@tu.edu.sa

[2] LR-SITI Laboratoire Signal Image et Technologies de l'Information, ENIT, Université de Tunis El Manar, Tunis 1002, Tunisia

[3] Department of Industrial and Systems Engineering, College of Engineering, University of Jeddah, Jeddah 21589, Saudi Arabia; amealharbi@uj.edu.sa (A.M.A.); mbazzar@uj.edu.sa (M.A.); salrubaiee@uj.edu.sa (S.R.)

* Correspondence: s.bourouis@tu.edu.sa

Received: 17 September 2020; Accepted: 28 October 2020; Published: 1 November 2020

Abstract: In the digital multimedia era, digital forensics is becoming an emerging area of research thanks to the large amount of image and video files generated. Ensuring the integrity of such media is of great importance in many situations. This task has become more complex, especially with the progress of symmetrical and asymmetrical network structures which make their authenticity difficult. Consequently, it is absolutely imperative to discover all possible modes of manipulation through the development of new forensics detector tools. Although many solutions have been developed, tamper-detection performance is far from reliable and it leaves this problem widely open for further investigation. In particular, many types of multimedia fraud are difficult to detect because some evidences are not exploited. For example, the symmetry and asymmetry inconsistencies related to visual feature properties are potential when applied at multiple scales and locations. We explore here this topic and propose an understandable soft taxonomy and a deep overview of the latest research concerning multimedia forgery detection. Then, an in-depth discussion and future directions for further investigation are provided. This work offers an opportunity for researchers to understand the current active field and to help them develop and evaluate their own image/video forensics approaches.

Keywords: digital forensics; multimedia tampering; image/video processing; data mining; pattern recognition; taxonomy; survey

1. Introduction

Recent technological developments have exponentially increased the amount of visual data (billions of images and videos) generated every day on the web and by social networks. Facebook, Twitter, YouTube and Instagram are the most popular online websites enabling people to upload and share billions of pictures.Nowadays, social media websites are playing a more important role in our daily life. They help users to express themselves, make new friendships and share their interests and ideas with others. The eighth annual report "social media in the Middle East: 2019 in review" [1–5] states that social media continues to be the top news source for Arab people and it is important for their lives. More than seven out of ten Arabs use Facebook, and every day, nine out of ten young Arabs use at least one social media channel [4,5]. Active social media users in Saudi Arabia are growing rapidly. Over 38% of the Saudi population are active users of social media. From 2018 to the present day, Saudi Arabia remains one of the world's largest markets for YouTube and Snapchat (e.g., more than 15.65 million users for only Snapchat) (Social Media in the Middle East: 2019 in Review: Available at: SSRN: https://ssrn.com/abstract=3517916 or http://dx.doi.org/10.2139/ssrn.3517916) [6]. The social and political impact of disseminated medias on the WWW is unquestionable, especially with the contribution of social networks in shaping the current political and social arena. To make online news more attractive and easier to consume for public audiences, most of them are associated with numerous images or videos. They represent a substantial part of the information circulated in our quotidian communications as well, e.g., newspapers and social websites. Information with multimedia content is also disseminated rapidly. Adults in some Arab countries like in Tunisia (80%), Jordan (92%), and Lebanon (79%) almost agreed that even though high-tech made users more knowledgeable, it made them easier to manipulate [7]. As a result, it is increasingly important to ensure the integrity and authenticity of the vast volumes of data before using them in many situations such as courts of law. Unfortunately, despite the benefits of technological progress, it can evoke many risks, particularly those related to systems and files security. Recently, much fake news has been widely reported on social media about coronavirus (COVID-19). Indeed, wrong remedies and conspiracy theories have affected the Internet with a dangerous strain of misinformation. False media can circulate faster and more easily across social media and the Internet. Therefore, the proliferation of incorrect information that is not useful or even harmful can hamper the public health response and worsen social unrest and division. As an example, in January 2020, thousands of Facebook posts showed a fake photo (taken from an art project in 2014 in Germany) falsely claiming that the people in this picture were victims of coronaviruses in China (see Figure 1). A large number of rumours in the form of images and video clips circulating on the web regarding the virus COVID-19 makes the task of distinguishing between fake and true stories and news increasingly difficult. Therefore, the World Health Organization (WHO) decided to warn people with a list of twenty false stories about coronavirus.

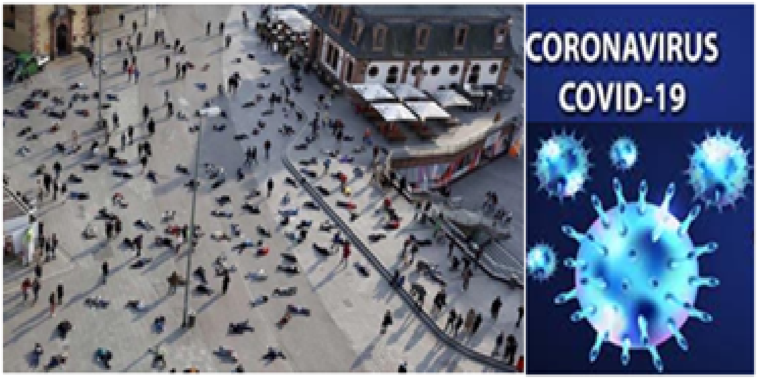
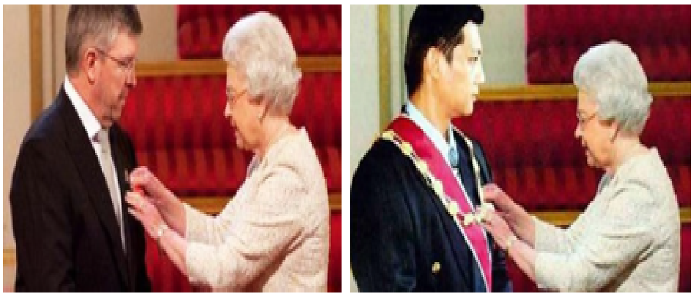


Figure 1. A photograph of an art project in 2014 in Germany that got shared on Facebook in 2020 to falsely claim that the people in this photo were coronavirus victims in China.

Nowadays, digital multimedia forensics has become an emerging research field. It has received considerable attention aiming at determining the origin and potential authenticity of digital media. For instance, image authenticity is important in many social areas, such as: in the medical field, physicians make critical decisions based on digital images; in law-reinforcement agencies and in courtrooms, the trustworthiness of photographs has an essential role where they could be used as evidence. In today's digital age, the fast development of powerful and low-cost editing tools facilitate the manipulation of digital media such as adding or removing parts and objects from images and videos leaving little or no sign of manipulation. Subsequently, this manipulated media will spread quickly and can have serious consequences, on both a national and an international scale. Moreover, it is too difficult to guarantee their integrity and authenticity, as shown in Figure 1, which represents an instance of tampering. With the rapid advances of high-resolution digital cameras and the availability of sophisticated editing software, such as Adobe Photoshop, Pixar and Corel PaintShop, one can easily modify the content of photos without leaving any obvious perceptual sign of manipulation. Unfortunately, they are blurring the line between real and faked multimedia content. The improper use of such editing tools allowing the diffusion of fake and misrepresented medias on social networks is becoming a grave rising problem since they have put the integrity of digital media further at stake. Indeed, counterfeiters repeatedly try to exploit these tools to hide and conceal images and videos and then use them to misinterpret information which can spread very fast and can have disastrous consequences, potentially at a national and international scale. They can also lead to fast-growing issues as decreasing the trustworthiness on many real applications. The big challenge is that it becomes very difficult for a viewer to judge the authenticity of a given image or video. The manipulation of digital media generally known as digital tampering is a horror to individuals (faked sequence of videos of celebrities), to societies (provocative faked images aiming certain ethnicity or religion), to journalism (reporters' post-manipulation of images), to insurance companies and to scientific journals. Tampering becomes a worry for governments, public and private enterprises and for individuals' private lives. Hence, the world is immersed in a serious challenge to address immediately the problem of spreading fraudulent photos and videos. An example of image tampering is depicted in Figure 2 where a Malaysian politician (Jeffrey Wong Su) is facing eviction from his party after faking snaps showing he was seen being knighted by the Queen of England in July 2010.



(**a**) original image (**b**) tampered image

Figure 2. Example of digital tampering image.

Recently, some interesting works have been looking into media authentication but the huge and complex multimedia volume to be analysed makes the design of successful multimedia tampering detection algorithm hard. Research in this field is far from offering robust and universal solutions, leaving the door wide open to further contributions. In the recent past, most of the efforts have been devoted to static tampering detection, but dynamic tempering detection has not received a lot of attention because of the complexity of the dynamic scene analysis and the computational cost. It turns out that this problem becomes more difficult with video forensics. In fact, severe issues create new challenges to the success of video tampering detection, such as the complexity of the dynamic scene analysis, the computational cost, the presence of occlusions, the changes in perspective, the multiple scales, the varying lighting conditions, and the spatio-temporal features extraction challenge (e.g., color, texture, shape, structure, layout, and motion). All these issues motivate the need of studying this hot area of research. Detecting malicious manipulation in digital media is still relevant today, since distinguishing manipulated from original images is increasingly difficult as new sophisticated image forgery approaches are revealed. As smart forgeries are hard to detect, a reliable digital tampering detection system is becoming increasingly important in the fields of public security. It is also important for other areas such as criminal, forensics investigation, intelligence services, insurance, journalism, scientific research, medical imaging and surveillance. An example of digital video tampering showing a modification in the content of a given video sequence downloaded from the Internet is given in Figure 3. In this particular example, some cars are copied and pasted into the same frames where the top row shows the authentic frames and the bottom row shows their tampered version, respectively.

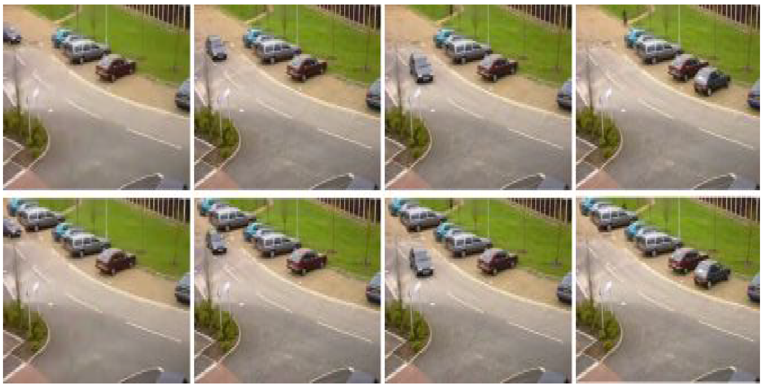


Figure 3. Example of intra-frame object duplication: original sequence (**top**) and forged sequence (**bottom**).

Our focus in this manuscript is to examine this area of research and to provide for the reader a useful reference related to the current studied topic. Moreover, an understandable taxonomy and a deep survey of main published works are presented as well. The organization of this manuscript is organized as follows. A taxonomy related to the current field of research is given in the next section. Then, a deep overview presenting main existing approached for multimedia tampering detection is presented in Section 3. Section 4 provides useful information regarding well-known datasets and benchmarks for both image and video tampering detection. Finally, we suggest a deep discussion and future directions for the problem studied here.

2. Taxonomy

In the following, a comprehensible taxonomy related to digital forensics and multimedia tampering detection is introduced. Brief and essential information are presented as well for the beginner to understand the current topic of research.

2.1. Digital Multimedia Forensics

Nowadays, digital sources are increasingly used to make necessary decisions. This is particularly clear in the field of digital forensic, where one can describe a crime scene through images and videos. The main problem is that it becomes difficult to detect manipulations given that many existing sophisticated editing software form a serious threat to the security. Hence, to cope with this problem, it is crucial to devise new powerful methods that support one to decide on the truthfulness of a given medium (image or video). Consequently, digital multimedia forensics and investigation has emerged as one of the most important security fields. Digital multimedia forensics combines technology, methodology and applications in order to provide trust in different media and to find digital evidences before, when and after a cybernetic security attack has occurred. In particular, the active digital forensics (starts after the detection of incident and before the incident closure) deals with the live data acquisition in order to ensure that relevant and admissible live evidence is available. The live identification, acquisition, preservation and response steps are essential to ensure efficient data collection. The live data gathering from networks causes several difficulties like data volume, data interdependencies, and network throughput speed. One more challenging problem is that of ensuring the reliability of evidences that must be considered with high priority in any judicial inquiry. The reliability deals essentially with the improvement of the authenticity and veracity of the evidence. These two criteria must not be questionable in the court in order to keep the evidence admissibility. Any digital data forgery in the collected data may lead to wrong investigation ending and cause evidences to be discredited in the court law. More generally, since new crime and criminal profiling techniques are more and more based on mining the rich multimodal digital data, their models and profiling will be also inaccurate if these resources are altered or fabricated. Today's digital forensics has become an emerging research field due to the large amount of generated multimedia files.

Digital forensics has received considerable attention, for both governmental and non-governmental organizations and departments, aiming at determining the origin and potential authenticity of digital media. It aims at restoring the lost trust in images and videos by uncovering digital counterfeiting techniques. For instance, image authenticity is important in many social areas, such as: in the medical field, physicians make critical decisions based on digital images; in law-reinforcement agencies and in courtrooms, the trustworthiness of photographs has an essential role where they could be used as evidence. In the literature, several deployed image forensic tools are able to determine the integrity of images. Despite this, authenticating digital images, validating their contents and semantics, and detecting forgeries are some of the critical challenges to date. It is a difficult problem given that manual tampering detection is computationally expensive and automating this process is a necessity. Recently, many scientific researchers expect to implement effective tools to respond to the overwhelming spread of photos/videos on social networks that threaten stability, even in societies and countries, and threaten their security system. However, it is not easy to distinguish between original (authentic) and fake multimedia content. Furthermore, no system yet exists which effectively and accurately accomplishes a generic image tampering detection task. Most existing efforts in this line of research still lack in-depth discussions on robustness against skillful forgers, who are professionals and have a good amount of knowledge of forensic tools and approaches.

2.2. Multimedia Tampering

Image (or video) tampering can be defined as the action of "adding or removing important features from an image (or video) without leaving any obvious traces of tampering" [8]. Generally, the most common applied tampering operations are: (i) deleting (or hiding) a region in the image, (ii) adding a new object into the image, and (iii) misrepresenting the image information (e.g., resizing an object within the image). Despite this problem of digital forensics that has attracted much attention, however, most research in this area still lacks rigorous and solid results and discussions. In addition, several methods have apparent limitations and are difficult to be optimally employed.

2.3. Tampering Tttacks

There are various kinds of tampering attacks being applied to images and videos. Some of them are commonly used by attackers like copy-move, slicing, re-sampling, resizing, noise variations and/or blurring, retouching, JPEG compression, luminance non-linearities and lighting inconsistencies. Here, we briefly describe the main attacks that are often used.

- Copy-move (cloning): This is one of the commonly applied attacks given its simplicity and effectiveness. It concerns all techniques that manipulate an image by copying certain region(s) and pasting them into another place on the same image (or video). As a result, some details will be hidden as well as others being duplicated in the same image.
- Splicing: This involves replacing some image (or video) objects from one or more different images (or videos) into another image (or video) in order to generate a composite image (forged). The inserted parts disturb the pattern of the new image (or video), thus, detecting this kind of tampering deals with exploiting patterns and any presence of statistical correlation distortions. It is one of the most aggressive and frequently used attacks.
- Re-sampling: This is defined as the process of applying some geometric transformations (like scaling, rotation or skewing operations) or any interpolation algorithms in order to create a malicious transformed image or a portion of image and therefore a visually convincing forgery by, for example, increasing or decreasing the image size.
- Retouching: This attack is used in order to enhance the visual quality of the image, for instance, by adding onto brightness. It is usually applied as a post-processing operation of image tampering. In this case, the original image (or video) will not be modified significantly, but only a few reductions in certain properties and characteristics of the image.

- Inpainting: This is the process of drawing some missing content over the image or video using, for example, the "brush" software tool in order to repair damage. As a result, this operation can alter the original image and the faked part takes distinct features (noise, lighting, luminosity and compression rate) from the rest of the parts in the same image or frame-video. It is noted that it is possible to detect this type of attack with the same techniques for copy-move attack detection.
- Other tampering attacks: There are other types of operations, such as filtering, cropping or histogram adjustments, which are often applied without malevolent intention.

The following table (Table 1) gives a general overview of some kinds of tampering attacks and how it is possible to address them using techniques derived from image processing and computer vision fields. More details are given in the following sections.

Table 1. Multimedia tampering techniques and their vulnerabilities.

Attack Type	**Tampering Detection Technique**
Copy-move (cloning)	Block matching, Discrete Cosine Transform (DCT), Principle Component Analysis (PCA), Autocorrelation
Splicing	Bi-spectral analysis, bi-coherence analysis, noise variation estimation, higher order statistics.
Re-sampling	Statistical approaches (EM-algorithm.)
Double JPEG compression	JPEG artifact estimation (frequency analysis)
Editing (luminance, noise nonlinearities)	EM-algorithm, higher order statistics
Multimedia enhancement	Blind statistical estimators (blur estimator, noise estimation, geometry transform estimation)
Geometric transformation (translation, rotation, scaling, skewing, reflection)	Provide spatial information between copied blocks and its neighbors
Post-processing (JPEG/MPEG compression, noise, blurring)	Eliminate any noticeable indications of manipulation especially sharp edges

2.4. Active Tampering Detection

Active methods, known also as data hiding methods, are derived from digital watermarking field. Digital watermarking and signature tools ensure data authenticity, like preventing the illegal copying of images from the Internet [9–11]. The process of watermarking is based on inserting (embedding) a secondary data (digital watermark) into an image or video. Although many active methods have been published in the literature, they present many problems such as: (i) they are impractical to embed digital watermarks in all images, and therefore, digital watermarking is limited in its ability to ensure authenticity. (ii) Not all devices embed a digital watermark, and people do not like using devices containing an embedded watermark. (iii) In the case of a compressed image, fragile watermarks can be easily destroyed. On the other hand, there are millions of digital images and videos on the web without a digital signature or watermark, and therefore it is not practical to adopt active methods to examine the authentication of unmarked digital images.

2.5. Passive Tampering Detection

Passive techniques work without any prior information on the authentic data. They can detect manipulation by exploiting the content-based features of images and videos (i.e., the statistical visual information). Verifying the integrity of digital media and detecting traces of tampering without using any pre–embedded information has proven to be effective for digital forensics (like the case of scene crime analysis). The integrity can be verified passively in order to identify traces like cloning, sampling, re-sampling, and inconsistencies in lighting. Such a process is able to ensure the future protection of the authenticity and credibility of digital data. To perform passive tampering detection, various criteria must be considered in order to develop robust multimedia forensic tools (see Figure 4) such as pixel-based, physically-based, camera-based, format-based, and geometric-based tools [12]. It is also possible to categorize existing detection methods into two main categories: intra-tampering and inter-tampering for both cases images and videos.

- Pixel-based methods: emphasize the use of pixel properties and the correlation between pixels (in spatial or transformed domain) for detecting anomalies (such as copy-move or splicing).
- Camera-based methods: they use several evidences such as the camera's model, artifacts and other features like camera sensors, lens, or some postprocessing steps including gamma correction, quantization, and filtering. These features help in detecting tampering.
- Format-based methods: exploit especially statistical correlations introduced by lossy compression scheme for such formats (like JPEG format) which are considered important clues for the presence of some manipulations. These techniques allow the detection of tampering in compressed media.
- Geometry-based methods: exploit the relative position of the object with respect to the camera as indication for further forgery detection process.
- Physics-based methods: take advantages of the inconsistencies between tampering scenes and physical objects in terms of differences in illumination, light, camera, and object size. These evidences are used to detect anomalies and forgeries.

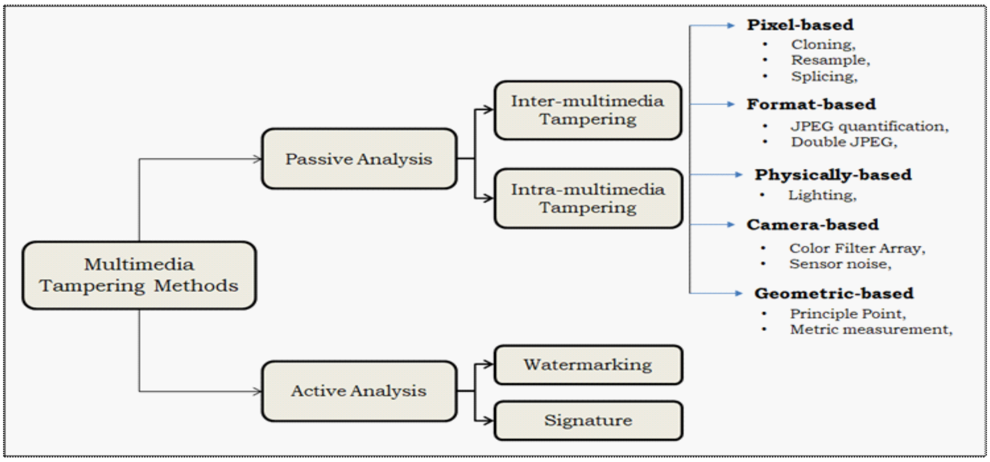


Figure 4. General classification of multimedia tampering detection methods.

2.6. Intra- and Inter-Multimedia Tampering

In this case, objects are clipped or replaced with duplicates in order to mask other objects. This category focuses on detecting manipulations performed at the same input source (images or videos). To discover such a manipulation, it would be possible to examine the similarity between matched clusters of pixels. However, this task would be very costly in computation time, as matching clusters of pixels would become infeasible when the size increases. Moreover, it would be difficult to achieve good accuracy in the case of minor modification like noise addition [8,13–15].

For inter-multimedia tampering, objects from different images or videos are used to tamper other images and/or videos. For example, regions from another image are superimposed on a specific region in the current image. In this case, alteration is performed by means of cloning from a secondary source (e.g., image, or patches from different images) and its detection is carried out by checking the consistency of image properties [8,16–23].

3. Digital Media Forensics Detection: Overview

Several promising methods have been developed in the literature to solve the problem of digital media tampering [24–29]. From a methodological point of view, different disciplines such as data mining, image/video processing, computer vision, and pattern recognition can be involved to address this hot research topic.

3.1. Copy-Move Image Tampering Detection

We recall that the problem of tampering detection has been studied for decades. Typically, image tampering detection methods have focused on the problems of copy-move detection (CMD) [30,31] and splicing detection [12]. Intuitively, these passive methods tend to exploit and analyze image characteristics (features) in order to find traces or similar patches (see Table 2).

Table 2. Summary of notable tampering image detection techniques.

Tampering Type	Tampering Detection Method
Copy-move detection	Discrete Cosine Transform (DCT) [32,33] Geometric Moments [34,35] Fourier–Mellin Transform (FMT) [36,37] Singular Value Decomposition (SVD) [38] Zernike moments [39,40] Wavelet Transform [41,42] Scale-invariant Feature Transform (SIFT) [15,43] Speeded Up Robust Features (SURF) [44]
Splicing detection	DCT per Block [45] Color Filter Array (CFA) artifacts [46] Photo Response Non-uniformity (PRNU) [47–49] Blur inconsistency [50]

Several surveys have been carried out on this hot topic and recently some papers reviewed several image tampering detection techniques [12,28,51]. Most copy-move tampering detection (CMTD) techniques share some common procedures and steps, which are: Feature Extraction and Feature Matching. The feature extraction step has the role of extracting relevant information that describes the treated image. Conventional feature extraction techniques reported in the literature are based on frequency transforms (discrete wavelet transform (DWT), DCT, PCA), polar transform (Fourier–Mellin transform (FMT)), moment transform (Hu, Zernike), local invariant keypoints, or texture (local binary pattern (LBP), Gabor transform). These features are often extracted from overlapping or non-overlapping blocks (i.e., image regions). Then, this is followed by a matching step to determine similarities between extracted features which result in detecting suspected regions. In general, matching stage is performed on the basis of the divided blocks or extracted keypoints. For instance, SIFT keypoints are matched using distance measure withing a clustering process that cluster closest points into similar groups. It is also important to mention that many of the data reduction techniques (e.g., SVD, PCA) are frequently and simultaneously applied within feature extraction step to reduce the dimensionality space and the computational complexity. In particular, singular value decomposition (SVD) is one of the methods often used thanks to its robustness with respect to geometric properties, rotation, filtering, and scaling. It turned out to have higher overall performance compared to other techniques like principal component analysis (PCA) and locally linear embedding (LLE). Furthermore, there is sometimes a need for a post-processing step to be applied in order to remove outliers from matched regions and to refine the final detection result. Many CMTD methods have been proposed so far and can follow either the block-based or keypoint-based principle. The general principle of CMTD detection process is depicted in Figure 5.

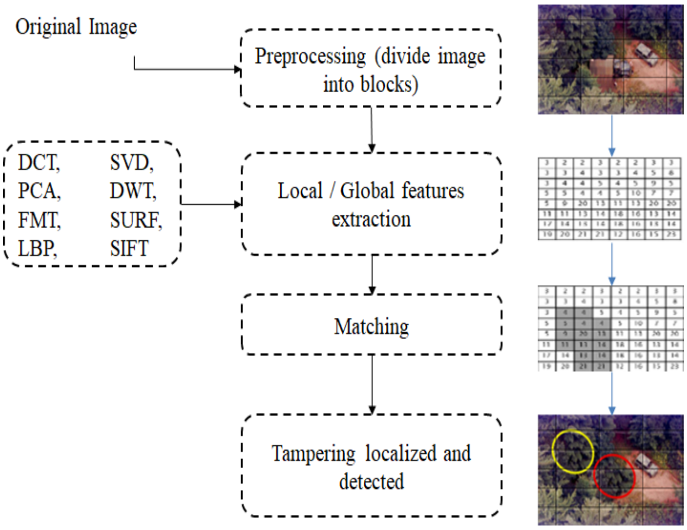

Original Image
Preprocessing (divide image into blocks)
DCT, SVD,
PCA, DWT,
FMT, SURF,
LBP, SIFT
Local / Global features extraction
Matching
Tampering localized and detected

Figure 5. General process of copy-move image tampering detection.

3.1.1. Block-Based Detection Techniques

In the state of the art, there is a significant number of publications regarding block-based techniques. The key idea here is to exploit the similarity measure between different blocks (representing image regions). Thus, an input image will be divided into overlapping or non-overlapping blocks, and each block is represented with a suitable descriptor vector which is calculated on the basis of some transforms. Finally, the suspected region is identified using a feature matching procedure. Visual descriptors were calculated using various techniques including, but not limited to, the following transforms: discrete cosine transform (DCT) [32,33], PCA (see, for example, some illustrations in Figures 6 and 7), singular value decomposition (SVD) [38], histogram of oriented gradients (HOG), geometric moments [34,35], Zernik moments [39,40], wavelet transform [41] and Fourier–Mellin transform [36,37]. It is well known that the computing of these transforms is time-consuming. In [52], authors proposed to detect copy-move tampering in color images with fractional quaternion cosine transform. The same problem was recently addressed in [42] through stationary wavelets transform (SWT), as well as local binary pattern variance (LBPV) method. The authors studied the algorithm's performance with respect to CoMoFoD and Kodak (KLTCI) datasets. Later, the same authors employed DCT with the same transform SWT and matching techniques, in order to reduce the feature vectors dimension and therefore enhancing the detection accuracy [53]. Recently, Gaussian–Hermite moments were applied for copy-move tampering detection [54]. Indeed, each image is divided into several blocks and the underlying Gaussian–Hermite moments descriptors are estimated to be used in the forgery detection process. Other geometric moments have been developed and investigated in this context, such as Zernike, moments to localize duplicated regions in [39,40] and Fourier–Mellin transforms to discover small manipulations [37]. Recently, neural network method and its variants have been applied for image falsification detection like the convolutional neural network (CNN) in [55,56] and the deep neural network (DNN) in [57].

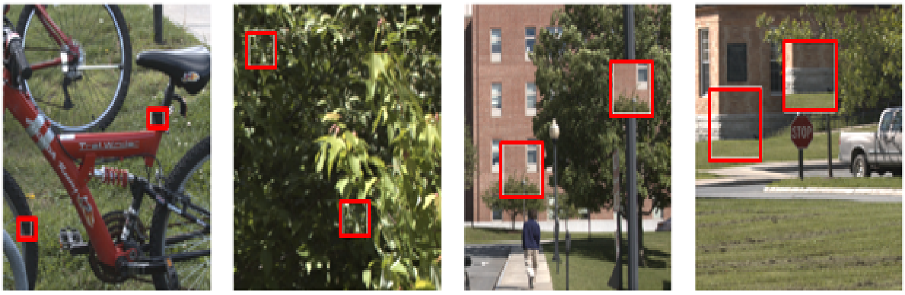


Figure 6. Duplicated regions detection based on DCT: Results obtained with the method in [16].

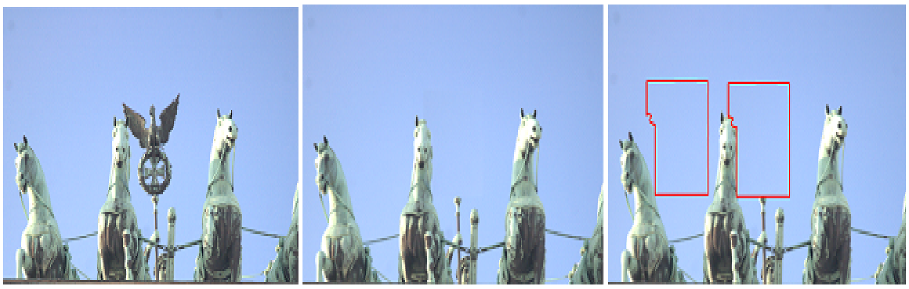


Figure 7. Copy-move attack detection: original image (**left**), tampered image (**middle**) and result after detection (**right**). Results obtained with the method in [33].

3.1.2. Keypoints-Based Detection Techniques

The keypoints-based detection methods are an alternative to the blocks-based ones. Local keypoints (high-entropy image regions) represent local extreme points and are extracted with different techniques. Among these techniques, we can cite, for example, the scale-invariant feature transform (SIFT) [15,43], Harris corner points [58], and speeded up robust features (SURF) [44]. SURF is one of the most efficient feature extractors based mainly on the SIFT detector. It is able to detect points of interest from images using the determinant of the Hessian matrix. SURF is invariant against different geometric transformations, such as translation, rotation, scale, lighting, and contrast [59]. It is noted that sometimes SURF surpasses the feature detector SIFT and many other visual feature extractors in terms of effectiveness, precision, and speed. An illustration of the SURF extraction process is given in Figure 8. In the case of fake images detection, during the matching step, we generally look for groups of similar keypoints which probably reflect the duplicated regions. The grouping process is performed with any clustering algorithm like the nearest neighbor (NN) search and the hierarchical clustering algorithm. Some interesting related works are proposed using interest point detector, as in [15,60]. The latter is based on the scale invariant feature transform (SIFT) [61] to localize duplicated regions in copy-move image forgery. Splicing forgery is also addressed with keypoints-based features in [62], where a symmetry matching method is implemented to deal with reflection-based attacks. This method has shown that it is capable of improving the results obtained in [15].

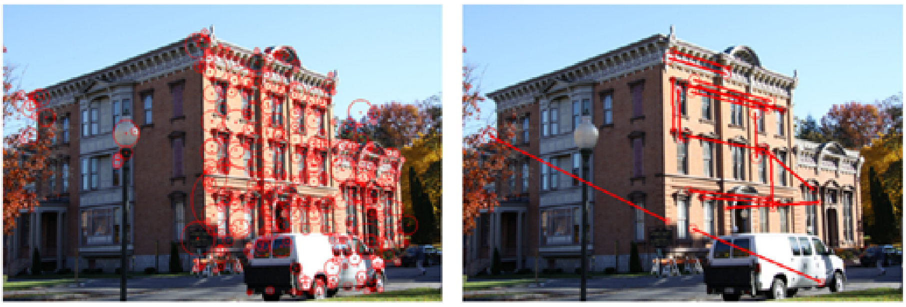


Figure 8. Example of Keypoints extraction (**left** image) using SURF detector and keypoints matching (**right** image) on tampered images.

Duplication tampering detection with local keypoints features is also addressed. Indeed, an adaptive non-maximal suppression keypoint detector and DAISY Descriptor are developed in [63,64]. SIFT features are used via a hierarchical matching strategy in [65] in order to improve the accuracy of duplication detection and to solve the drawback of keypoints matching. A copy-move image tampering detection algorithm based on a hybrid framework including both block-based and keypoint features is developed in [66]. An effective approach based on a voting process to deal with copy-move forgeries under several geometric transformations (i.e., resizing, rotation and compression) is presented in [67]. An example of obtained results for copy-move tampering detection using the SURF Keypoints-based technique is given in Figure 9. In another work [68], authors introduced a copy-move forgery based on a histogram of orientated gradients. Oriented key-points and Scaled ORB features are investigated in [69] as well. RANSAC algorithm is used also in this context to eliminate all possible false matched key-points. In [70], a hybrid method for forensics detection is introduced based on both cellular automata (CA) and local binary patterns (LBP). The main goal is to reduce as much as possible the complexity of extracting texture features using CA rules. In [71], a copy-move detection algorithm is implemented based on both region and texture (LBP) visual features. The method is evaluated on the basis of several image datasets, notably ASIA. Another work is developed allowing fast tampering detection in [72] using the criteria of local bidirectional coherency error. In fact, feature correspondences are refined on the basis of iteration over the improved coherency sensitive search.

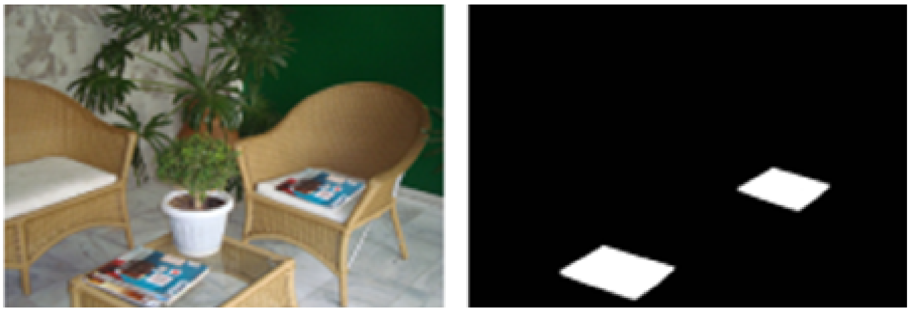


Figure 9. Copy-move tampering detection using SURF Keypoints-based technique: tampered image (**left**) and result of tampering detection(**right**). Results were obtained based on the method in [67].

Data mining and statistical machine learning methods have been applied with success for digital tampering detection. This class of approaches offers the possibility of developing evolving systems, allowing both supervised and unsupervised datasets categorization into authentic and forged classes. They make it possible to discover the relationships between data and to exploit the information present in a database. In particular, statistical mixture models instances have attracted great interest in pattern recognition, data mining and machine learning fields [73–77]. Mixture models provide high flexibility to model both images and videos and to identify different types of forgery attacks based on local or global visual features. Some promising works based on mixture models have been successfully developed for the present problem [78,79]. Indeed, the problem of image inpainting detection was solved through a hybrid generative/discriminative framework in [79]. The authors implemented new probabilistic support vector machine (SVM) kernels to improve detection precision and overcome the disadvantages of conventional SVM kernels (like linear kernel and RBF). These kernels take advantage of the intrinsic structure of the dataset and are generated from statistical mixture model named as "bounded generalized Gaussian mixture model (BGGMM)". Another robust method based on statistical mixture models was also developed in [78]. Indeed, a Bayesian algorithm for finite inverted dirichlet mixture model is proposed since it allows high flexibility for images modelling. Moreover, an inference method based on the Markov chain Monte Carlo sampling technique (MCMC) is implemented instead of a frequentist approach in order to improve the accuracy. It is noted that there are many other promising mixture models that can be extended and used with success for tampering detection. These statistical models have shown interesting results for many other applications related to pattern recognition and computer vision [80–82]. Another recent work allows multiple copy move forgery detection with symmetry-based local features, proposed in [83].

3.2. Splicing Tampering Detection

Unlike copy-move detection approaches, splicing tampering detection approaches are able to detect suspected regions coming from other sources. Splicing tampering is the process of copying a region from one image and pasting it into another different image. In this case, two or more images are involved to cause misleading. In general, the process of detecting spliced images includes the inspection of various inconsistencies between authentic and forged regions. Some blind detection approaches solve this problem by searching for fingerprints from different cameras [84,85] or by analyzing sensor noise [86]. Indeed, the source of images is identified with various artifacts such as interpolation artifacts, defective pixels, color filter array, lens aberration, and JPEG compression artifacts. In recent years, some studies focused on identifying the source camera devices (device brand) in order to determine the image integrity. These works share basically common steps such as describing the device's model with a set of features, training the developed classifier based on the extracted features, and finally predicting the image source class [87,88]. It is noted that many of the underlying methods have apparent limitations in distinguishing between devices of the same brand.

On the other hand, the identification of the camera source is handled with various possible patterns and artifacts such as photo response non-uniformity (PRNU), which is considered to be unique to a particular camera. Furthermore, this pattern has been increasingly studied by several scholars [47–49] and it has been found that it is capable of discriminating each single camera with geat precision whatever the brand. The PRNU signal can be estimated by tiny imperfections of imaging camera. It demonstrated that it is one of the stable and useful fingerprint for sensors identification. The pioneer work that estimated the PRNU signal from an image was published in [89]. The absence of PRNU is used as a clue for PRNU-based splicing detection methods. Recently, some researchers improved the identification of the camera's model using PRNU-based methods [48,49] and different formats of image as well. For example, in [48], authors proposed to neglect the influence of unwanted artifacts for the reference pattern noise which results in enhancing the accuracy and reducing the false identification rate. In [90], an effective method was also proposed for tamper detection based on image hashing as well as physical unclonable function (PUF). The estimation of the PRNU from RAW data to identify source device is determined in different ways as detailed in [84,91,92]. In [91,92], raw data is used to distinguish different devices from the same camera model and not to identify different device models. This issue is addressed in [84] where a probabilistic algorithm for PRNU estimation is developed to model the raw data as a Poisson process using the MLE approach. Thus, the proposed PRNU estimate is applied to identify different camera's models. The noise can also be used as a promising feature to recognize authentic images [86] because any captured image by any sensor will generate specific noise. Therefore, noise is considered to be a favorable clue to reveal splicing tampering. Composite image detection (or splicing) is also treated with feature inconsistency in each image component [93–96]. For instance, digital tampering is treated by constructing noise level functions [96]. In conclusion, we noticed that although some works yielded good results, others produced many false positives and did not do well in localizing the tampering.

3.3. Toward Hybrid Methods

Despite the fact that some studies have been proposed to deal with copy-move tampering detection and that they have reported promising results, many of them do not achieve high performance. We summarize in this section the main drawbacks of several related methods.

- As image tampering detection is a hard problem, the computational time is relatively high for block-based techniques, given that all pixels or extracted features must be examined per block. Sometimes, large-scaling distortion is undetectable. In contrast, the feature-based techniques have less computational complexity. Thus, solving the trade-off speed–accuracy is now a challenging problem.

- Determining the best nd optimal feature extraction algorithm is not easy and final results are highly dependent on the used technique, which can be a keypoint-based or block-based technique.
- In many cases, the existing methods in the literature fail to detect particularly small duplicate regions (caused by copy-move operation), and therefore the accuracy will be very low.
- Some methods fail to locate multiple duplicated regions.
- In general, keypoint-based techniques cannot address the smoothing tampering.
- Sometimes, block-based methods are more accurate than keypoint-based ones in identifying the shapes of duplicated regions.
- Both the keypoint features and block-based matching have difficulties in accurately detecting the smoothed shape region.
- Most copy-move detection methods are unable to detect different types of attack at the same time (e.g., compression, scaling, and noise addition, copy-move and duplication).
- It is too difficult that just one single image tampering detection method or algorithm can reveal entirely forged images. Thus, involving several methodologies and abilities is highly recommended.
- Some tampering detectors may be misled by counter-intrusive processes created by counterfeiting.

To address the above limitations, researchers made a lot of effort to avoid the weakness of each method alone and to take advantage of their strength together [97,98]. Most of the newly developed ideas focus on combining both keypoint-based features and block-based matching techniques into the same hybrid framework. For instance, a passive detection with a hybrid method is proposed in [98], based on keypoints features analysis for triangle shapes rather than standard blocks. In this case, objects are characterized by a connected triangles. Detector methods like SIFT and Harris are applied for local keypoints features extraction. Combining several detectors based on fusion rules is a promising methodology and allows the use of complementary properties to address a hard problem like multimedia tampering detection. Nevertheless, traditional fusion methods can fail to completely tackle this challenge, since they often do not take into account some properties like the spatial dependence (neighboring pixels) and the intrinsic properties of the image. These properties can be considered as important clues and evidences for digital forensics. Another promising work dealing with this aspect through a decision-making process approach was published in [99]. Indeed, authors examined the drawbacks of traditional fusing methods by developing an effective behaviour knowledge space representation (BKS) for copy-move modelling and detection. Recently, a hybrid method was developed that exploits local visual features [100] to improve block-based copy-move tampering detection. In fact, SURF features are calculated on each block instead of calculating them on the entire image. The same authors proposed another work based on SIFT feature and density-based clustering algorithm to increase the performance of tampering detection. An illustration of such a result is given in Figure 10.

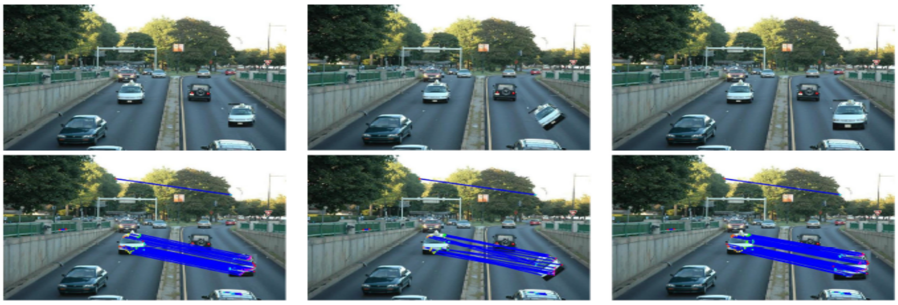


Figure 10. Tampering detection using SIFT Keypoints-based technique: tampered image (**top**) and result of tampering detection (**bottom**) [101].

3.4. Video Tampering Detection

In this section, we report some relevant and recent works developed for video tampering detection. Many of these works are able to detect suspicious objects or frames based on digital video characteristics. To date, several implemented methods focus on identifying inter-frame or intra-frame tampering [22,102–112]. Intra-frame-based methods can occur in either a spatial or spatio-temporal domain (like frames copy-move or splicing). However, the inter-frame based methods (see Figure 11) takes place in the temporal domain (like frame insertion, removal and duplication). One of the pioneering works in this area has dealt with the so-called frame duplication detection [113], by taking into account the correlation information between successive frames. Different types of attacks and counterfeits can occur to disappear and remove video evidence. Thus, effective clues must be exploited to uncover these counterfeits including for instance velocity and physical inconsistencies [103,107], motion residuals [111], and statistical-contour features [109].

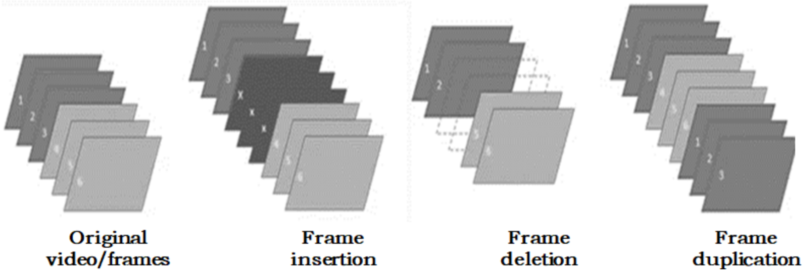


Figure 11. Example of attacks related to inter-frame tampering.

In general, video tampering is detected by verifying spatial alterations such as frame compression [114,115] or temporal modifications such as frame addition or deletion [116,117]. Among the passive forensics' techniques, double compression is one of the substantial clues for video tampering detection. When handling compressed video, attackers follow certain steps to modify this video by first decoding this video, then by manipulating it and finally by recompressing it. This scenario is well illustrated in Figure 12. Obviously, this scenario will leave traces and footprints that can be exploited as valuable information for forensic analysis [118–122]. Some studies have addressed the problem of double compression detection including, but not limited to, the one in [118], which is based on the use of efficient spatio-temporal features evaluated on the basis of local motion vector field.

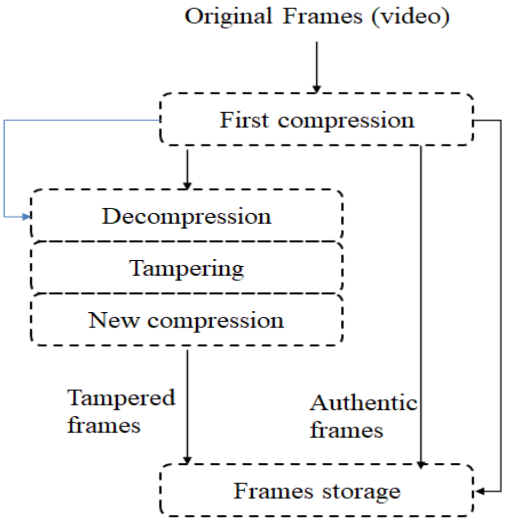


Figure 12. Basic scenario of tampering compressed video.

Solving the video tampering problem is not obvious and one may consider the correlation between a video's frames as an important factor. Only few studies have focused on detecting the frame duplication [108,109,123,124]. For instance, in [123], authors exploit the correlation of singular value decomposition features between authentic and suspicious frames and the frame duplication attack is detected using a similarity analysis-based method. In [109], motion residual features in each frame are considered to identify manipulated frames. Another passive technique [108] is based on the extraction of statistical features and the classification of these features into positive samples or negative ones. Visual features are derived from wavelet-based moment and average gradient intensity, and the extraction process is based on the concept of the adjustable width object boundary (AWOB). The detection of frame duplication is handled differently as well, in particular with the SIFT descriptor and the model bag-of-words (BoW) [125]. This technique can only find duplicated frames and not other forms of attacks. Other works addressed various types of attacks simultaneously such as frame deletion and frame insertion using, for example, histogram of oriented gradients (HOG) features [126]. In this particular work, authors exploit the so-called motion energy image to extract the image-edge and then to locate both frame duplication and shuffling manipulations.

The extraction of efficient spatio-temporal features remains the main challenge for most researchers in order to determine duplicated frames with high precision. For instance, the singular value decomposition (SVD) is performed in conjunction with the Euclidean similarity measure in [123]. DCT was also exploited to create a set of features. For example, the standard deviation of residual frames is used to pick some frames from the video sequence and then the DCT entropy is exploited in detecting inter-frame duplication [23]. In [127], the authors utilized DCT to create a set of features for each frame, and then to discover the presence of forgery using the correlation coefficient. This method provides good results but the computational time is too expensive.

Videos can be forged with the temporal splicing operation as well. To address this kind of tampering, a detector was designed in [128]. It assesses whether a video was temporally interpolated by calculating the temporal correlation among video frames. This detector has been improved later by taking advantage of the edge-intensity in order to pick out the presence of video frame-rate up-conversion [129]. The authors studied as well the Kaufman adaptive moving average (KAMA) to separate authentic frames from interpolating ones. Other clues and traces, notably video noise-based correlation, have also been examined to conduct counterfeit videos detection [130]. Their work is based on the exploitation of the extracted noise residual as a robust feature characteristics and the use of block-level correlation technique. They model the distribution of correlation of temporal noise residue in a tampered video as a Gaussian mixture model (GMM). However, their approach greatly depends on the noise reduction technique. Indeed, when the noise intensities of the original and tampered regions are different, it fails to reduce the noise accurately and can miss some forgeries because of the calculation error of noise residual. It should be noted that conventional Gaussian-based mixture models (GMM) are popular tools allowing acceptable results for modeling univariate data; nevertheless, they fail to fit various complex shapes. Other alternative mixture models including, but not limited to, the generalized GMM may be a more attractive choice for data modelling [76,77,81]. The latter is able to provide more flexibility to better adapt the form of non-Gaussian data than the conventional Gaussian distribution (GMM). A different approach is presented in [131], in which the noise level function (NLF) is used to detect suspicious regions in static scene recorded from video. The authors deal with linear and nonlinear NLFs as noise's inconsistency to detect forged regions. In the same context, pixel prediction error is analyzed to conduct forgery detection. It is calculated from spatially collocated frames in a group of pictures (GOP) [132].

Recently, some attractive passive video tampering detection techniques have been implemented [133–136]. Among them, there are approaches that take advantage of statistical models which are applied with success in this context [135,136]. On the other hand, an automatic technique based on the noise-level variation is presented in [133]. Indeed, the motion-compensated frame rate up-conversion was exploited as well for malicious detection purposes like counterfeiting frame rate.

This problem is also treated in [134], where the residual signal is defined as an indication to locate interpolated forged frames. Wavelet-based moment and average gradient intensity were also estimated in conjunction with the concept of adjustable width object boundary (AWOB) and the SVM classifier in order to identify positive samples (original videos) and negative samples (tampered videos) [108]. We have noticed that many studies have indicated that the performance of their algorithms deteriorates when it comes, for example, to processing high quality compressed videos. In addition, they are unable to locate all possible interpolated frames and are unable to recover texture details for multiple video cases [129,133]. The other point is that most inter-frame techniques are expensive and cannot detect multiple attacks at the same time.

4. Forensics Multimedia Datasets

4.1. Datasets

In the state of the art, a number of public datasets are accessible for multimedia tampering and can be served as a benchmarked dataset for performance evaluation. Some metrics are also required to validate the obtained results with respect to the ground truth. In the following, we provide a concise description of well-known available datasets.

- MICC-F220 dataset [15]: It is collected by 220 images: 110 are original images and 110 tampered. They represent different scenes like animals, plants, and artifacts.
- MICC-F2000 dataset [15]: This publicly accessible database contains in total 2000 images, where 1300 are authentic and the other 700 are tampered with.
- CoMoFoD dataset [137]: It is composed of 260 image sets, where each set includes the original image, a colored/binary mask and the tampered image. Several post-processing activities have been performed on this dataset. Overall, 200 original images with resolution (512 × 512) are post-processed to generate a total number of 10,400 images. The remaining 60 original images have a large resolution of (3000 × 2000) and are post-processed as well, to have a total number of 3120 images.
- Wild web-tampered image dataset [138]: It is a very large collection of tampered images from the web and social media sources, accompanied by a ground truth annotation masking the representation of the location of the forgery.
- CASIA-v2.0 dataset [139]: It is an available dataset for tampered image detection evaluation. It is composed of 7491 color authentic images and 5123 manipulated ones (spliced and/or blurred) of different large sizes, from 240 × 160 to 900 × 600. Certain original images are acquired from the well-known Corel dataset.
- CISD dataset [140]: It is a public collection for splicing detection with 1845 images provided by the lab DVMM at Columbia University. There are 933 authenticated images and the other 912 are faked blocks of size 128 × 128 pixels. Two fundamental operations are performed to create spliced images: crop-and-paste operations from the same source image or two different images.
- Multimedia forensics challenge (MFC) datasets [141]: It is a very large collection of digital media (images and videos) forensics challenge (MFC) evaluations. There are about 176,000 original images and 11,000 original videos, where more than 100,000 are manipulated images and 4000 are manipulated videos.
- Realistic tampering dataset [142]: This dataset contains 220 color authentic and 220 realistic forged images with size of 1920 × 1080 pixels. Images are captured by different cameras (Sony, Canon, Nikon D7000, Nikon D90).
- FaceForensics++ dataset [143]: It is a large scale publicly tampered video dataset composed of 1000 tampered face videos and 1000 authentic videos. Authentic videos were extracted from YouTube and social media. Each manipulated source video has an original counterpart.

- VTD dataset [144]: This video tampering dataset (VTD) is composed of 26 tampered videos and 26 original counterparts which are downloaded from YouTube. The forged video files are obtained as follows: 10 sequences based on splicing attacks, 6 based on an inter-frame forgery and 10 based on copy–move attacks. Each sequence contains between 420 and 480 frames.

Table 3 summarizes several publicly available datasets for both image and videos tampering detection. These datasets can be used by researchers for evaluation purposes.

Table 3. Summary of notable public datasets related to image and video tampering detection.

Dataset	Description
MICC-F600 [15]	Used for image copy-move tampering detection: (110 original, 110 tampered) where the image size is 800 × 533.
MICC-F2000 [15]	Used for image copy-move tampering detection: (1300 original, 700 tampered) where the image size is: 2018 × 1536.
CISD [140]	Used for image splicing detection: (933 original, 912 tampered) where the image size is: 128 × 128.
UCID [145]	Used for image retouching detection: contains 1338 images.
CMH [67]	Used for image copy-move tampering detection: (108 original, 108 tampered) where the image size is: 845 × 634.
Wild Web tampered [138]	Very large collection of tampered images from the Web
CUISDE [146]	Used for image splicing detection: (180 original, 181 tampered) where the image size is (757 × 568).
CASIA-v1.0 [139]	Used for color image splicing detection: (800 original, 921 tampered) where the image size is (374 × 256).
CASIA-v2.0 [139]	Used for color image splicing detection: (7491 original, 5123 tampered) where the image size is (240 × 160 and 900 × 600).
CMFDA [29]	Used for image copy-move tampering detection: contains 48 images with JPEG compression
CoMoFoD [137]	Used for image copy-move tampering detection: (200 original, 60 tampered) where the image size is (512 × 512).
MFC [141]	Used for both images and videos forensics challenge. (176,000 original images, 100,000 tampered) and (11,000 original videos, 4000 tampered videos).
VTD [144]	Used for video forgery detection: (26 original videos, 26 tampered videos).
FaceForensics++[143]	Used for video tampering detection: (1000 original videos, 1000 tampered videos).
SULFA [147]	Used for video tampering detection: (10 original videos, 10 tampered videos).

4.2. Evaluation Metrics

For tampering detection assessment, several metrics can be used. The commonly used metrics are true positive rate (TPR) and false positive rate (FPR). Tampered images are designated as positive samples, and original (or authentic) ones as negative samples.

- True positive rate (TPR) = $TP/(TP+FN)$ =

$$\frac{\#Images\ detected\ as\ tampered\ being\ tampered}{tampered\ images}$$

- False positive rate (FPR) = $FP/(FP+TN)$ =

$$\frac{\#Images\ detected\ as\ tampered\ being\ authentic}{authentic\ images}$$

The performance can be also evaluated through other metrics such as the precision (or accuracy), true negative rate (or specificity), Matthews correlation coefficient (MCC), ROC curves and F1 score.

- True Negative Rate (specificity) = $TN/(TN+FP)$.
- False Negative Rate (FNR) = $TN/(FP+TN)$.
- Accuracy = $(TN+TP)/(TP+FP+TN+FN)$.
- MCC=$(TN \times TP\breve{}FP \times FN)/\sqrt{(TP+FP)(TP+FP)(TN+FN)}$.
- F1= $2TP/(2TP+FN+FP)$.

The correct detection is designed by true positives (TP); the number of false positives (FP) (i.e., if the authentic is detected as tamper); and the number of false negatives (FN) (i.e., if the tamper is detected as authentic). The performance of any developed algorithm is considered satisfactory if it achieved high detection accuracy and low FPR and FNR.

5. Discussions and Conclusions

Passive multimedia tampering detection is one of the fastest-growing scientific research fields. In this manuscript, we have focused on the main recent state-of-the-art approaches that detect both image and video forgery. There are primarily two scenarios for forgery detection: block-based or keypoint-based. Such a process might involves two steps: visual feature extraction and matching steps. Common block-based techniques often use global features instead of local descriptors like DCT, DWT, Fourier transform and other frequency transforms which are robust against blur, noise, and JPEG/MPEG compression. Regarding matching processes, they frequently utilize lexicographical and KD-tree as sorting techniques. The role of this step is to improve the computational complexity especially when looking for duplicate blocks, which results in quickly locating similar blocks (or features). Many works have studied as well the complexity by considering specific conventional and classical techniques, such as PCA and SVD. They help to guarantee the reliability of any counterfeit detection algorithm while maintaining a reasonable calculation time. On the other hand, it is important to note that the block-based category has a limited capacity when dealing with global features which are sensitive to the invariance property against geometric transformations, such as scaling, rotation and projection. Therefore, these descriptors lack the capability to find all possible similar blocks (i.e., authentic and forged blocks). This issue still results in low overall detection performance. Consequently, as to improve the tapering detection, future directions have to be directed to investigate more effective hybrid descriptors and matching methods, including but not limited to, geometric moments (e.g., Fourier–Mellin transform) and texture-based features.

Tampering detection techniques based on keypoint features are also considered popular among other techniques. They are based generally on efficient local visual features like SIFT and SURF which has led, in many cases, to high performance. It is also known that these techniques have proven to be effective against geometric transformations such as scaling, rotation and translation. Nevertheless, this kind of approach fails to identify especially highly textured manipulated regions or frames in a video sequence. In addition, local descriptors do not have the capability to distinguish between authentic similar regions and forged ones, which results in high false-positive rate notable when handling smoothed images and/or videos. It should also be noted that the keypoint features are incapable to determine the shape region between the extracted points, which makes it possible to achieve poor results. On the other hand, keypoint-based methods can be considered very expensive in terms of time complexity because they treat a huge amount of points during the matching process and this is for each image and video. Therefore, it is important to propose new suitable methodologies if one wants to process complex and smooth multimedia data. It is also recommended to find robust techniques that allow one to reduce the computation time (by carefully reducing the number of local features) without degrading the detection performance. Thus, the question here is how to determine the minimum and sufficient number of invariant keypoints describing the desired image and allowing us to discover regions of altered texture.

In the recent past years, most of the efforts have been devoted to static image tampering detection, but video (dynamic) tempering has not received a lot of attention. The main reasons are related to the complexity of the dynamic scene analysis, the computational cost, the presence of occlusions, the changes in perspective, the multiple scales, the varying lighting conditions, and the spatio-temporal features extraction challenge (e.g., color, texture, shape, structure, layout, and motion). Some researchers thought that it would be easy to exploit and extend the techniques used in the case of images to the more complex case of video fraud. Still, some types of forgery cannot be detected since there is no consideration of the temporal fact in a video, which is the relationship between frames. For example, a simple duplication remains hidden due to the fact that each frame appears authentic if tested separately. Moreover, it is hard to detect a simple replacement given that each frame seems to be authentic if we consider that frames are independent. For the case of spatio-temporal doctoring detection, scientific research is just getting started, and the prevention task is not yet well studied. Recently, only few works have been looking into video authentication, but the detection performance is far from being reliable. In addition, most of the proposed methods ignore the rich spatio-temporal content of videos, which can be very helpful. In fact, these methods consider a video as a set of independent frames, so they ignore the spatial and temporal relationships between these frames. Research in this field is far from offering robust solutions.

In summary, various techniques and studies in literature have been developed to address the hard problem of digital multimedia tampering detection and many of them have reported promising results, however, the detection performance is far from being reliable (in terms of number of false positives). Many of these approaches are generally less effective, especially when dealing with homogeneous areas and when we want to maintain robustness to rotation, scaling, blurring, noisy images, and compression with loss. It is also important to say that despite the importance of the online aspect, not all the proposed video counterfeit detection techniques work effectively in an online manner and many of them have limitations when handling a large number of video sequences (big data). In addition, it is important that further research studies the temporal relationship property between frames in order to increase the spatio-temporal forgery detection. This objective could be achieved if one considers the success of advanced and modern methods derived from computer vision, data mining and machine learning fields. For example, statistical learning approaches allow the efficient modelling of large-scale of information and then they could be a good alternative for both image and video tampering detection. Regarding the complexity of extracting several features from the video, this issue can be tackled by adopting feature selection procedures. It is worth noting that for digital tampering detection, providing more information could improve the expected results. Indeed, specific objects are distinguished and characterized on the basis of their characteristics (shape, colour, texture). Then, considering the fact that some characteristics (or descriptors) are more relevant than others which are called "informative descriptors", it will be more practical to use only these informative descriptors instead of applying all possible descriptors. The irrelevant characteristics can be only noise, thus not effective to describe accurately the desired objects. Selecting only the most relevant spatio-temporal features is particularly important and plays a primary role in improving the accuracy of manipulation detection algorithms and decreasing the computational time. Addressing these issues will certainly help achieve high performance in terms of real-time tampering detection. In addition, exploring these challenges could open the door to more effective contributions.

Author Contributions: Conceptualization, S.B. and R.A.; methodology, A.M.A.; software, M.A.; validation, S.B., R.A. and S.R.; formal analysis, S.B.; investigation, S.R.; resources, R.A.; data curation, A.M.A.; writing–original draft preparation, S.B.; writing–review and editing, R.A. and S.R. and R.A.; supervision, M.A.; project administration, M.A.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Radcliffe, D.; Abuhmaid, H. Social Media in the Middle East: 2019. 2020, in press.
2. Available online: https://www.techradar.com/news/twitter-announces-expansion-to-mena-video-content-with-over-16-partnerships (accessed on 4 April 2020).
3. Available online: https://www.statista.com/statistics/315405/snapchat-user-region-distribution/ (accessed on 4 April 2020).
4. Available online: http://www.mideastmedia.org/survey/2019/chapter/social-media/ (accessed on 4 April 2020).
5. Available online: https://www.thinkwithgoogle.com/intl/en-145/getting-know-youtubes-biggest-middle-eastern-audience-millennials/ (accessed on 4 April 2020).
6. Radcliffe, D.; Abuhmaid, H. Social Media in the Middle East: 2019 in Review. 12 January 2020. Available online: https://ssrn.com/abstract=3517916 (accessed on 4 April 2020). [CrossRef]
7. Available online: https://www.pewresearch.org/internet/2019/05/13/publics-in-emerging-economies-worry-social-media-sow-division-even-as-they-offer-new-chances-for-political-engagement/ (accessed on 4 April 2020).
8. Fridrich, A.J.; Soukal, B.D.; Lukáš, A.J. Detection of copy-move forgery in digital images. In Proceedings of the Digital Forensic Research Workshop, Cleveland, OH, USA, 6–8 August 2003.
9. Celik, M.U.; Sharma, G.; Saber, E.; Tekalp, A.M. Hierarchical watermarking for secure image authentication with localization. *IEEE Trans. Image Process.* **2002**, *11*, 585–595. [CrossRef] [PubMed]
10. Meerwald, P.; Uhl, A. Survey of wavelet-domain watermarking algorithms. In *Security and Watermarking of Multimedia Contents III*; International Society for Optics and Photonics: Bellingham, WA, USA, 2001; pp. 505–516.
11. Hartung, F.; Kutter, M. Multimedia watermarking techniques. *Proc. IEEE* **1999**, *87*, 1079–1107. [CrossRef]
12. Farid, H. Image forgery detection. *IEEE Signal Process. Mag.* **2009**, *26*, 16–25. [CrossRef]
13. Lin, H.J.; Wang, C.W.; Kao, Y.T. Fast copy-move forgery detection. *WSEAS Trans. Signal Process.* **2009**, *5*, 188–197.
14. Huang, H.; Guo, W.; Zhang, Y. Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm. In Proceedings of the PACIIA IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Wuhan, China, 19–20 December 2008; pp. 272–276.
15. Amerini, I.; Ballan, L.; Caldelli, R.; Bimbo, A.D.; Serra, G. A SIFT-Based Forensic Method for Copy-Move Attack Detection and Transformation Recovery. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 1099–1110. [CrossRef]
16. Popescu, A.C.; Farid, H. Exposing digital forgeries by detecting duplicated image regions. In *Dartmouth College, Computer Science, Technology Report, TR2004-515*; Dartmouth College: Hanover, NH, USA, 2004; pp. 1–11.
17. Mahdian, B.; Saic, S. Detection of copy–move forgery using a method based on blur moment invariants. *Forensic Sci. Int.* **2007**, *171*, 180–189. [CrossRef]
18. Farid, H.; Lyu, S. Higher-order Wavelet Statistics and their Application to Digital Forensics. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, CVPR, Madison, WI, USA, 6–22 June 2003; p. 94.
19. Pevný, T.; Fridrich, J.J. Detection of Double-Compression in JPEG Images for Applications in Steganography. *IEEE Trans. Inf. Forensics Secur.* **2008**, *3*, 247–258. [CrossRef]
20. Johnson, M.K.; Farid, H. Exposing Digital Forgeries in Complex Lighting Environments. *IEEE Trans. Inf. Forensics Secur.* **2007**, *2*, 450–461. [CrossRef]
21. Qu, Z.; Luo, W.; Huang, J. A convolutive mixing model for shifted double JPEG compression with application to passive image authentication. In Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, ICASSP, Las Vegas, NV, USA, 31 March–4 April 2008; pp. 1661–1664.
22. Liu, Y.; Huang, T. Exposing video inter-frame forgery by Zernike opponent chromaticity moments and coarseness analysis. *Multimed. Syst.* **2017**, *23*, 223–238. [CrossRef]
23. Fadl, S.M.; Han, Q.; Li, Q. Authentication of surveillance videos: Detecting frame duplication based on residual frame. *J. Forensic Sci.* **2018**, *63*, 1099–1109. [CrossRef] [PubMed]
24. Thakur, R.; Rohilla, R. Recent advances in digital image manipulation detection techniques: A brief review. *Forensic Sci. Int.* **2020**, *312*, 110311. [CrossRef]

25. Teerakanok, S.; Uehara, T. Copy-Move Forgery Detection: A State-of-the-Art Technical Review and Analysis. *IEEE Access* **2019**, *7*, 40550–40568. [CrossRef]
26. Lin, X.; Li, J.H.; Wang, S.L.; Liew, A.W.C.; Cheng, F.; Huang, X.S. Recent Advances in Passive Digital Image Security Forensics: A Brief Review. *Engineering* **2018**, *4*, 29–39. [CrossRef]
27. Meena, K.B.; Tyagi, V. Image forgery detection: Survey and future directions. In *Data, Engineering and Applications*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 163–194.
28. Warif, N.B.A.; Wahab, A.W.A.; Idris, M.Y.I.; Ramli, R.; Salleh, R.; Shamshirband, S.; Choo, K.R. Copy-move forgery detection: Survey, challenges and future directions. *J. Netw. Comput. Appl.* **2016**, *75*, 259–278. [CrossRef]
29. Christlein, V.; Riess, C.; Jordan, J.; Riess, C.; Angelopoulou, E. An Evaluation of Popular Copy-Move Forgery Detection Approaches. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 1841–1854. [CrossRef]
30. Khan, S.; Khan, K.; Ali, F.; Kwak, K. Forgery Detection and Localization of Modifications at the Pixel Level. *Symmetry* **2020**, *12*, 137. [CrossRef]
31. Li, J.; Li, X.; Yang, B.; Sun, X. Segmentation-Based Image Copy-Move Forgery Detection Scheme. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 507–518.
32. Alahmadi, A.A.; Hussain, M.; Aboalsamh, H.; Muhammad, G.; Bebis, G.; Mathkour, H. Passive detection of image forgery using DCT and local binary pattern. *Signal Image Video Process.* **2017**, *11*, 81–88. [CrossRef]
33. Luo, W.; Huang, J.; Qiu, G. Robust Detection of Region-Duplication Forgery in Digital Image. In Proceedings of the 18th International Conference on Pattern Recognition (ICPR 2006), Hong Kong, China, 20–24 August 2006; pp. 746–749.
34. Wang, X.; Liu, Y.; Xu, H.; Wang, P.; Yang, H. Robust copy-move forgery detection using quaternion exponent moments. *Pattern Anal. Appl.* **2018**, *21*, 451–467. [CrossRef]
35. Prakash, C.S.; Kumar, A.; Maheshkar, S.; Maheshkar, V. An integrated method of copy-move and splicing for image forgery detection. *Multimed. Tools Appl.* **2018**, *77*, 26939–26963. [CrossRef]
36. Zhong, J.; Gan, Y. Detection of copy–move forgery using discrete analytical Fourier–Mellin transform. *Nonlinear Dyn.* **2016**, *84*, 189–202. [CrossRef]
37. Li, W.; Yu, N. Rotation robust detection of copy-move forgery. In Proceedings of the International Conference on Image Processing, ICIP 2010, Hong Kong, China, 26–29 September 2010; pp. 2113–2116.
38. Zhao, J.; Guo, J. Passive forensics for copy-move image forgery using a method based on DCT and SVD. *Forensic Sci. Int.* **2013**, *233*, 158–166. [CrossRef]
39. Cozzolino, D.; Poggi, G.; Verdoliva, L. Efficient Dense-Field Copy-Move Forgery Detection. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2284–2297. [CrossRef]
40. Ryu, S.; Kirchner, M.; Lee, M.; Lee, H. Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1355–1370.
41. Bashar, M.; Noda, K.; Ohnishi, N.; Mori, K. Exploring duplicated regions in natural images. *IEEE Trans. Image Process.* **2010**. [CrossRef] [PubMed]
42. Mahmood, T.; Irtaza, A.; Mehmood, Z.; Mahmood, M.T. Copy–move forgery detection through stationary wavelets and local binary pattern variance for forensic analysis in digital images. *Forensic Sci. Int.* **2017**, *279*, 8–21. [CrossRef]
43. Pan, X.; Lyu, S. Region Duplication Detection Using Image Feature Matching. *IEEE Trans. Inf. Forensics Secur.* **2010**, *5*, 857–867. [CrossRef]
44. Xu, B.; Wang, J.; Liu, G.; Dai, Y. Image copy-move forgery detection based on SURF. In Proceedings of the 2010 International Conference on Multimedia Information Networking and Security, Nanjing, China, 4–6 November 2010; pp. 889–892.
45. Bianchi, T.; Piva, A. Image Forgery Localization via Block-Grained Analysis of JPEG Artifacts. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 1003–1017. [CrossRef]
46. Ferrara, P.; Bianchi, T.; Rosa, A.D.; Piva, A. Image Forgery Localization via Fine-Grained Analysis of CFA Artifacts. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 1566–1577. [CrossRef]
47. Valsesia, D.; Coluccia, G.; Bianchi, T.; Magli, E. User Authentication via PRNU-Based Physical Unclonable Functions. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 1941–1956. [CrossRef]
48. Lin, X.; Li, C. Preprocessing Reference Sensor Pattern Noise via Spectrum Equalization. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 126–140. [CrossRef]

49. Li, R.; Li, C.; Guan, Y. A compact representation of sensor fingerprint for camera identification and fingerprint matching. In Proceedings of the 2015 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2015, South Brisbane, QL, Australia, 19–24 April 2015; pp. 1777–1781.
50. Bahrami, K.; Kot, A.C.; Li, L.; Li, H. Blurred Image Splicing Localization by Exposing Blur Type Inconsistency. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 999–1009. [CrossRef]
51. Lanh, T.V.; Chong, K.; Emmanuel, S.; Kankanhalli, M.S. A Survey on Digital Camera Image Forensic Methods. In Proceedings of the 2007 IEEE International Conference on Multimedia and Expo, ICME 2007, Beijing, China, 2–5 July 2007; pp. 16–19.
52. Chen, B.; Yu, M.; Su, Q.; Li, L. Fractional quaternion cosine transform and its application in color image copy-move forgery detection. *Multimed. Tools Appl.* **2019**, *78*, 8057–8073. [CrossRef]
53. Mahmood, T.; Mehmood, Z.; Shah, M.; Saba, T. A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform. *J. Vis. Commun. Image Represent.* **2018**, *53*, 202–214. [CrossRef]
54. Meena, K.B.; Tyagi, V. A copy-move image forgery detection technique based on Gaussian-Hermite moments. *Multimed. Tools Appl.* **2019**, *78*, 33505–33526. [CrossRef]
55. Abdalla, Y.E.; Iqbal, M.T.; Shehata, M.S. Convolutional Neural Network for Copy-Move Forgery Detection. *Symmetry* **2019**, *11*, 1280. [CrossRef]
56. Song, C.; Zeng, P.; Wang, Z.; Li, T.; Qiao, L.; Shen, L. Image Forgery Detection Based on Motion Blur Estimated Using Convolutional Neural Network. *IEEE Sens. J.* **2019**, *19*, 11601–11611. [CrossRef]
57. Zhong, J.; Pun, C. An End-to-End Dense-InceptionNet for Image Copy-Move Forgery Detection. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2134–2146. [CrossRef]
58. Chen, L.; Lu, W.; Ni, J.; Sun, W.; Huang, J. Region duplication detection based on Harris corner points and step sector statistics. *J. Vis. Commun. Image Represent.* **2013**, *24*, 244–254. [CrossRef]
59. Bay, H.; Ess, A.; Tuytelaars, T.; Gool, L.V. Speeded-Up Robust Features (SURF). *Comput. Vis. Image Underst.* **2008**, *110*, 346–359. [CrossRef]
60. Zandi, M.; Aznaveh, A.M.; Talebpour, A. Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 2499–2512. [CrossRef]
61. Lowe, D.G. Distinctive Image Features from Scale-Invariant Keypoints. *Int. J. Comput. Vis.* **2004**, *60*, 91–110. [CrossRef]
62. Warif, N.B.A.; Wahab, A.W.A.; Idris, M.Y.I.; Salleh, R.; Othman, F. SIFT-Symmetry: A robust detection method for copy-move forgery with reflection attack. *J. Vis. Commun. Image Represent.* **2017**, *46*, 219–232. [CrossRef]
63. Guo, J.; Liu, Y.; Wu, Z. Duplication forgery detection using improved DAISY descriptor. *Expert Syst. Appl.* **2013**, *40*, 707–714. [CrossRef]
64. Yu, L.; Han, Q.; Niu, X. Feature point-based copy-move forgery detection: Covering the non-textured areas. *Multimed. Tools Appl.* **2016**, *75*, 1159–1176. [CrossRef]
65. Liu, L.; Ni, R.; Zhao, Y.; Li, S. Improved SIFT-Based Copy-Move Detection Using BFSN Clustering and CFA Features. In Proceedings of the 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2014, Kitakyushu, Japan, 27–29 August 2014; pp. 626–629.
66. Pun, C.; Yuan, X.; Bi, X. Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1705–1716.
67. Silva, E.; de Carvalho, T.J.; Ferreira, A.; Rocha, A. Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes. *J. Vis. Commun. Image Represent.* **2015**, *29*, 16–32. [CrossRef]
68. Lee, J.; Chang, C.; Chen, W. Detection of copy-move image forgery using histogram of orientated gradients. *Inf. Sci.* **2015**, *321*, 250–262. [CrossRef]
69. Zhu, Y.; Shen, X.; Chen, H. Copy-move forgery detection based on scaled ORB. *Multimed. Tools Appl.* **2016**, *75*, 3221–3233. [CrossRef]
70. Tralic, D.; Grgic, S.; Sun, X.; Rosin, P.L. Combining cellular automata and local binary patterns for copy-move forgery detection. *Multimed. Tools Appl.* **2016**, *75*, 16881–16903. [CrossRef]
71. Isaac, M.M.; Wilscy, M. Image forgery detection using region - based Rotation invariant Co-occurrences among adjacent LBPs. *J. Intell. Fuzzy Syst.* **2018**, *34*, 1679–1690. [CrossRef]

72. Bi, X.; Pun, C. Fast copy-move forgery detection using local bidirectional coherency error refinement. *Pattern Recognit.* **2018**, *81*, 161–175. [CrossRef]
73. Fan, W.; Sallay, H.; Bouguila, N.; Bourouis, S. A hierarchical Dirichlet process mixture of generalized Dirichlet distributions for feature selection. *Comput. Electr. Eng.* **2015**, *43*, 48–65. [CrossRef]
74. Najar, F.; Bourouis, S.; Bouguila, N.; Belghith, S. Unsupervised learning of finite full covariance multivariate generalized Gaussian mixture models for human activity recognition. *Multim. Tools Appl.* **2019**, *78*, 18669–18691. [CrossRef]
75. Bourouis, S.; Zaguia, A.; Bouguila, N.; Alroobaea, R. Deriving Probabilistic SVM Kernels From Flexible Statistical Mixture Models and its Application to Retinal Images Classification. *IEEE Access* **2019**, *7*, 1107–1117. [CrossRef]
76. Channoufi, I.; Bourouis, S.; Bouguila, N.; Hamrouni, K. Image and video denoising by combining unsupervised bounded generalized gaussian mixture modeling and spatial information. *Multim. Tools Appl.* **2018**, *77*, 25591–25606. [CrossRef]
77. Najar, F.; Bourouis, S.; Zaguia, A.; Bouguila, N.; Belghith, S. Unsupervised Human Action Categorization Using a Riemannian Averaged Fixed-Point Learning of Multivariate GGMM. In Proceedings of the Image Analysis and Recognition—15th International Conference, ICIAR, Povoa de Varzim, Portugal, 27–29 June 2018; pp. 408–415.
78. Bourouis, S.; Mashrgy, M.A.; Bouguila, N. Bayesian learning of finite generalized inverted Dirichlet mixtures: Application to object classification and forgery detection. *Expert Syst. Appl.* **2014**, *41*, 2329–2336. [CrossRef]
79. Alharbi, A.; Alhakami, W.; Bourouis, S.; Najar, F.; Bouguila, N. Inpainting forgery detection using Hybrid Generative/Discriminative approach based on Bounded Generalized Gaussian mixture model. *Appl. Comput. Inform.* **2019**. [CrossRef]
80. Alroobaea, R.; Rubaiee, S.; Bourouis, S.; Bouguila, N.; Alsufyani, A. Bayesian inference framework for bounded generalized Gaussian-based mixture model and its application to biomedical images classification. *Int. J. Imaging Syst. Technol.* **2020**, *30*, 18–30. [CrossRef]
81. Najar, F.; Bourouis, S.; Bouguila, N.; Belghith, S. A Fixed-Point Estimation Algorithm for Learning the Multivariate GGMM: Application to Human Action Recognition. In Proceedings of the IEEE Canadian Conference on Electrical & Computer Engineering, CCECE, Quebec, QC, Canada, 13–16 May 2018; pp. 1–4.
82. Bourouis, S.; Channoufi, I.; Alroobaea, R.; Rubaiee, S.; Andejany, M.; Bouguila, N. Color object segmentation and tracking using flexible statistical model and level-set. *Multimed. Tools Appl.* **2020**, 1–23. [CrossRef]
83. Vaishnavi, D.; Subashini, T.S. Application of local invariant symmetry features to detect and localize image copy move forgeries. *J. Inf. Secur. Appl.* **2019**, *44*, 23–31. [CrossRef]
84. Mehrish, A.; Subramanyam, A.V.; Emmanuel, S. Robust PRNU estimation from probabilistic raw measurements. *Signal Process. Image Commun.* **2018**, *66*, 30–41. [CrossRef]
85. Hou, J.; Lee, H. Detection of Hue Modification Using Photo Response Nonuniformity. *IEEE Trans. Circuits Syst. Video Technol.* **2017**, *27*, 1826–1832. [CrossRef]
86. Zeng, H.; Zhan, Y.; Kang, X.; Lin, X. Image splicing localization using PCA-based noise level estimation. *Multimed. Tools Appl.* **2017**, *76*, 4783–4799. [CrossRef]
87. Sameer, V.U.; Sarkar, A.; Naskar, R. Source camera identification model: Classifier learning, role of learning curves and their interpretation. In Proceedings of the International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 22–24 March 2017; pp. 2660–2666.
88. Roy, A.; Chakraborty, R.S.; Sameer, V.U.; Naskar, R. Camera Source Identification Using Discrete Cosine Transform Residue Features and Ensemble Classifier. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, CVPR, Honolulu, HI, USA, 21–26 July 2017; pp. 1848–1854.
89. Lukás, J.; Fridrich, J.J.; Goljan, M. Digital camera identification from sensor pattern noise. *IEEE Trans. Inf. Forensics Secur.* **2006**, *1*, 205–214. [CrossRef]
90. Cao, Y.; Zhang, L.; Zalivaka, S.S.; Chang, C.; Chen, S. CMOS Image Sensor Based Physical Unclonable Function for Coherent Sensor-Level Authentication. *IEEE Trans. Circuits Syst.* **2015**, *62*, 2629–2640. [CrossRef]
91. Qiao, T.; Retraint, F.; Cogranne, R.; Thai, T.H. Source camera device identification based on raw images. In Proceedings of the 2015 IEEE International Conference on Image Processing, ICIP 2015, Quebec City, QC, Canada, 27–30 September 2015; pp. 3812–3816.
92. Thai, T.H.; Retraint, F.; Cogranne, R. Camera model identification based on the generalized noise model in natural images. *Digit. Signal Process.* **2016**, *48*, 285–297. [CrossRef]

93. Lyu, S.; Pan, X.; Zhang, X. Exposing Region Splicing Forgeries with Blind Local Noise Estimation. *Int. J. Comput. Vis.* **2014**, *110*, 202–221. [CrossRef]
94. Hu, W.; Dai, J.; Jian, J. Effective composite image detection method based on feature inconsistency of image components. *Digit. Signal Process.* **2015**, *39*, 50–62. [CrossRef]
95. Yao, H.; Wang, S.; Zhang, X.; Qin, C.; Wang, J. Detecting Image Splicing Based on Noise Level Inconsistency. *Multimed. Tools Appl.* **2017**, *76*, 12457–12479. [CrossRef]
96. Pun, C.; Liu, B.; Yuan, X. Multi-scale noise estimation for image splicing forgery detection. *J. Vis. Commun. Image Represent.* **2016**, *38*, 195–206. [CrossRef]
97. Chihaoui, T.; Bourouis, S.; Hamrouni, K. Copy-move image forgery detection based on SIFT descriptors and SVD-matching. In Proceedings of the 2014 1st International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), Sousse, Tunisia, 17–19 March 2014; pp. 125–129.
98. Ardizzone, E.; Bruno, A.; Mazzola, G. Copy-Move Forgery Detection by Matching Triangles of Keypoints. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2084–2094. [CrossRef]
99. Ferreira, A.; Felipussi, S.C.; Alfaro, C.; Fonseca, P.; Vargas-Munoz, J.E.; dos Santos, J.A.; Rocha, A. Behavior Knowledge Space-Based Fusion for Copy-Move Forgery Detection. *IEEE Trans. Image Process.* **2016**, *25*, 4729–4742. [CrossRef]
100. Soni, B.; Das, P.K.; Thounaojam, D.M. Geometric transformation invariant block based copy-move forgery detection using fast and efficient hybrid local features. *J. Inf. Secur. Appl.* **2019**, *45*, 44–51. [CrossRef]
101. Soni, B.; Das, P.K.; Thounaojam, D.M. Keypoints based enhanced multiple copy-move forgeries detection system using density-based spatial clustering of application with noise clustering algorithm. *IET Image Process.* **2018**, *12*, 2092–2099. [CrossRef]
102. Stamm, M.C.; Lin, W.S.; Liu, K.J.R. Temporal Forensics and Anti-Forensics for Motion Compensated Video. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 1315–1329. [CrossRef]
103. Wu, Y.; Jiang, X.; Sun, T.; Wang, W. Exposing video inter-frame forgery based on velocity field consistency. In Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2014, Florence, Italy, 4–9 May 2014; pp. 2674–2678.
104. Sitara, K.; Mehtre, B.M. Digital video tampering detection: An overview of passive techniques. *Digit. Investig.* **2016**, *18*, 8–22. [CrossRef]
105. Bestagini, P.; Fontani, M.; Milani, S.; Barni, M.; Piva, A.; Tagliasacchi, M.; Tubaro, S. An overview on video forensics. In Proceedings of the 20th European Signal Processing Conference, EUSIPCO 2012, Bucharest, Romania, 27–31 August 2012; pp. 1229–1233.
106. Singh, R.D.; Aggarwal, N. Video content authentication techniques: A comprehensive survey. *Multimed. Syst.* **2018**, *24*, 211–240. [CrossRef]
107. Conotter, V.; O'Brien, J.F.; Farid, H. Exposing Digital Forgeries in Ballistic Motion. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 283–296. [CrossRef]
108. Richao, C.; Gaobo, Y.; Ningbo, Z. Detection of object-based manipulation by the statistical features of object contour. *Forensic Sci. Int.* **2014**, *236*, 164–169. [CrossRef]
109. Chen, S.; Tan, S.; Li, B.; Huang, J. Automatic Detection of Object-Based Forgery in Advanced Video. *IEEE Trans. Circuits Syst. Video Technol.* **2016**, *26*, 2138–2151. [CrossRef]
110. Yao, Y.; Shi, Y.; Weng, S.; Guan, B. Deep Learning for Detection of Object-Based Forgery in Advanced Video. *Symmetry* **2018**, *10*, 3. [CrossRef]
111. Zhang, D.; Yang, G.; Li, F.; Wang, J.; Sangaiah, A.K. Detecting seam carved images using uniform local binary patterns. *Multimed. Tools Appl.* **2020**, *79*, 8415–8430. [CrossRef]
112. Zhang, D.; Yin, T.; Yang, G.; Xia, M.; Li, L.; Sun, X. Detecting image seam carving with low scaling ratio using multi-scale spatial and spectral entropies. *J. Vis. Commun. Image Represent.* **2017**, *48*, 281–291. [CrossRef]
113. Wang, W.; Farid, H. Exposing Digital Forgeries in Interlaced and Deinterlaced Video. *IEEE Trans. Inf. Forensics Secur.* **2007**, *2*, 438–449. [CrossRef]
114. Milani, S.; Bestagini, P.; Tagliasacchi, M.; Tubaro, S. Multiple compression detection for video sequences. In Proceedings of the 14th IEEE International Workshop on Multimedia Signal Processing, MMSP 2012, Banff, AB, Canada, 17–19 September 2012; pp. 112–117.
115. He, P.; Jiang, X.; Sun, T.; Wang, S. Detection of double compression in MPEG-4 videos based on block artifact measurement. *Neurocomputing* **2017**, *228*, 84–96. [CrossRef]

116. Bian, S.; Luo, W.; Huang, J. Exposing Fake Bit Rate Videos and Estimating Original Bit Rates. *IEEE Trans. Circuits Syst. Video Technol.* **2014**, *24*, 2144–2154. [CrossRef]
117. Gironi, A.; Fontani, M.; Bianchi, T.; Piva, A.; Barni, M. A video forensic technique for detecting frame deletion and insertion. In Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2014, Florence, Italy, 4–9 May 2014; pp. 6226–6230.
118. He, P.; Jiang, X.; Sun, T.; Wang, S. Double compression detection based on local motion vector field analysis in static-background videos. *J. Vis. Commun. Image Represent.* **2016**, *35*, 55–66. [CrossRef]
119. Kang, X.; Liu, J.; Liu, H.; Wang, Z.J. Forensics and counter anti-forensics of video inter-frame forgery. *Multimed. Tools Appl.* **2016**, *75*, 13833–13853. [CrossRef]
120. Yu, L.; Wang, H.; Han, Q.; Niu, X.; Yiu, S.; Fang, J.; Wang, Z. Exposing frame deletion by detecting abrupt changes in video streams. *Neurocomputing* **2016**, *205*, 84–91. [CrossRef]
121. Zheng, J.; Sun, T.; Jiang, X.; He, P. Double H.264 Compression Detection Scheme Based on Prediction Residual of Background Regions. In Proceedings of the Intelligent Computing Theories and Application—13th International Conference, Liverpool, UK, 7–10 August 2017; pp. 471–482.
122. Li, Q.; Wang, R.; Xu, D. Detection of double compression in HEVC videos based on TU size and quantised DCT coefficients. *IET Inf. Secur.* **2019**, *13*, 1–6. [CrossRef]
123. Yang, J.; Huang, T.; Su, L. Using similarity analysis to detect frame duplication forgery in videos. *Multimed. Tools Appl.* **2016**, *75*, 1793–1811. [CrossRef]
124. Wang, W.; Farid, H. Exposing digital forgeries in video by detecting duplication. In Proceedings of the 9th Workshop on Multimedia & Security, MM&Sec, Dallas, TX, USA, 20–21 September 2007; pp. 35–42.
125. Ulutas, G.; Ustubioglu, B.; Ulutas, M.; Nabiyev, V.V. Frame duplication detection based on BoW model. *Multimed. Syst.* **2018**, *24*, 549–567. [CrossRef]
126. Fadl, S.; Han, Q.; Qiong, L. Exposing video inter-frame forgery via histogram of oriented gradients and motion energy image. *Multidimens. Syst. Signal Process.* **2020**, *31*, 1365–1384. [CrossRef]
127. Singh, G.; Singh, K. Video frame and region duplication forgery detection based on correlation coefficient and coefficient of variation. *Multimed. Tools Appl.* **2019**, *78*, 11527–11562. [CrossRef]
128. Bestagini, P.; Battaglia, S.; Milani, S.; Tagliasacchi, M.; Tubaro, S. Detection of temporal interpolation in video sequences. In Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2013, Vancouver, BC, Canada, 26–31 May 2013; pp. 3033–3037.
129. Yao, Y.; Yang, G.; Sun, X.; Li, L. Detecting video frame-rate up-conversion based on periodic properties of edge-intensity. *J. Inf. Secur. Appl.* **2016**, *26*, 39–50. [CrossRef]
130. Hsu, C.C.; Hung, T.Y.; Lin, C.W.; Hsu, C.T. Video forgery detection using correlation of noise residue. In Proceedings of the 2008 IEEE 10th Workshop on Multimedia Signal Processing, Cairns, QLD, Australia, 8–10 October 2008; pp. 170–174.
131. Kobayashi, M.; Okabe, T.; Sato, Y. Detecting Forgery From Static-Scene Video Based on Inconsistency in Noise Level Functions. *IEEE Trans. Inf. Forensics Secur.* **2010**, *5*, 883–892. [CrossRef]
132. Subramanyam, A.V.; Emmanuel, S. Pixel estimation based video forgery detection. In Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2013, Vancouver, BC, Canada, 26–31 May 2013; pp. 3038–3042.
133. Li, R.; Liu, Z.; Zhang, Y.; Li, Y.; Fu, Z. Noise-level estimation based detection of motion-compensated frame interpolation in video sequences. *Multimed. Tools Appl.* **2018**, *77*, 663–688. [CrossRef]
134. Ding, X.; Yang, G.; Li, R.; Zhang, L.; Li, Y.; Sun, X. Identification of Motion-Compensated Frame Rate Up-Conversion Based on Residual Signals. *IEEE Trans. Circuits Syst. Video Technol.* **2018**, *28*, 1497–1512. [CrossRef]
135. Bourouis, S.; Al-Osaimi, F.R.; Bouguila, N.; Sallay, H.; Aldosari, F.M.; Mashrgy, M.A. Video Forgery Detection Using a Bayesian RJMCMC-Based Approach. In Proceedings of the 14th IEEE/ACS International Conference on Computer Systems and Applications, AICCSA 2017, Hammamet, Tunisia, 30 October–3 November 2017; pp. 71–75.
136. Bourouis, S.; Al-Osaimi, F.R.; Bouguila, N.; Sallay, H.; Aldosari, F.M.; Mashrgy, M.A. Bayesian inference by reversible jump MCMC for clustering based on finite generalized inverted Dirichlet mixtures. *Soft Comput.* **2019**, *23*, 5799–5813. [CrossRef]
137. Tralic, D.; Zupancic, I.; Grgic, S.; Grgic, M. CoMoFoD—New database for copy-move forgery detection. In Proceedings of the ELMAR, Zadar, Croatia, 25–27 September 2013; pp. 49–54.

138. Zampoglou, M.; Papadopoulos, S.; Kompatsiaris, Y. Large-scale evaluation of splicing localization algorithms for web images. *Multimed. Tools Appl.* **2017**, *76*, 4801–4834. [CrossRef]
139. Dong, J.; Wang, W.; Tan, T. CASIA Image Tampering Detection Evaluation Database. In Proceedings of the 2013 IEEE China Summit and International Conference on Signal and Information Processing, ChinaSIP, Beijing, China, 6–10 July 2013; pp. 422–426.
140. Ng, T.T.; Chang, S.F.; Sun, Q. *A Data Set of Authentic and Spliced Image Blocks*; ADVENT Technical Report; Columbia University: New York, NY, USA, 2004; pp. 203–2004.
141. Guan, H.; Kozak, M.; Robertson, E.; Lee, Y.; Yates, A.N.; Delgado, A.; Zhou, D.; Kheyrkhah, T.; Smith, J.; Fiscus, J. MFC datasets: Large-scale benchmark datasets for media forensic challenge evaluation. In Proceedings of the IEEE Winter Applications of Computer Vision Workshops (WACVW), Waikoloa Village, HI, USA, 7–11 January 2019; pp. 63–72.
142. Korus, P.; Huang, J. Multi-Scale Analysis Strategies in PRNU-Based Tampering Localization. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 809–824. [CrossRef]
143. Rössler, A.; Cozzolino, D.; Verdoliva, L.; Riess, C.; Thies, J.; Nießner, M. FaceForensics++: Learning to Detect Manipulated Facial Images. In Proceedings of the 2019 IEEE/CVF International Conference on Computer Vision, ICCV, Seoul, Korea, 27 October–2 November 2019; pp. 1–11.
144. Al-Sanjary, O.I.; Ahmed, A.A.; Sulong, G. Development of a video tampering dataset for forensic investigation. *Forensic Sci. Int.* **2016**, *266*, 565–572. [CrossRef]
145. Schaefer, G.; Stich, M. UCID: An uncompressed color image database. In *Storage and Retrieval Methods and Applications for Multimedia 2004*; International Society for Optics and Photonics: Bellingham, WA, USA, 2003; Volume 5307, pp. 472–480.
146. Hsu, Y.; Chang, S. Detecting Image Splicing using Geometry Invariants and Camera Characteristics Consistency. In Proceedings of the 2006 IEEE International Conference on Multimedia and Expo, ICME 2006, Toronto, ON, Canada, 9–12 July 2006; pp. 549–552.
147. Available online: https://http://sulfa.cs.surrey.ac.uk/forged.php (accessed on 4 April 2020).

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.