INTERNATIONAL JOUNAL OF: SCIENCE RESEARCH AND TECHNOLOGY

TIMBOU-AFRICA ACADEMIC PUBLICATIONS
INTERNATIONAL JOURNAL, NOVEMBER, 2022 EDITIONS
VOL. 11 NO. 9 ISSN: 2623-7861

GENERAL-PURPOSE IMAGE TAMPERING DETECTION TECHNIQUES: A REVIEW OF RECENT ADVANCES

ABDULKADIR MAIGARI TURAKI; FATIMA AHMED ABUBAKAR; AHMAD ATIKA JIBRIN; SUBERU YUSUF; & SUNUSI ABDULHAMID DANTATA

Department of Computer Science, Federal Polytechnic Bauchi, Bauchi State, Nigeria.

ABSTRACT

Image tampering is the action of adding or removing important features from an image to change its semantic meaning for illegal or malicious purposes. The development of sophisticated computers and image editing software has made the tampering of digital images easy and undetectable by the human visual system. As a result, the tampering of images for malicious purposes is now rampant in our society leading to many ethical and moral consequences,

INTRODUCTION

In recent times, digital media including images have become the principal means of conveying information due to their expressive potentials and the ease of distribution, acquisition, and storage [1]. The efficacy of digital images in conveying information has made them more preferable than text information as a means of communication. Consequently, it is becoming common more than ever to see an image representing a prime source of evidence in legal proceedings, crime investigations, and, a source of information by mass media and publishing agencies. However, the nature of the digital image has raised a lot of questions in most of these positive aspects where they are utilized. Digital images can be easily altered to convey false or misleading information. The advent of sophisticated computers and user-friendly image editing software allows anyone with rudimentary image editing skills to alter them easily without leaving behind any human perceptible traces [2]. Thus, image modifications for harmful reasons have become commonplace in our society, resulting in a lot of ethical and moral consequences, such as the spread of fake news, erroneous verdicts, and reputational damage among others [3]. Therefore, it is necessary to develop strategies and methods to allow the verification of the

such as the spread of fake news, wrong verdicts, and damage of reputation among others. For these reasons, it is important to have tools that can help us determine the authenticity of digital media. The earliest methods for detecting image tampering focused on detecting specific image tampering, they could not be used for detecting multiple image tampering. However, practical image tampering often involves multiple tampering operations. To address this problem, recent studies in image tampering detection have focused on designing general purpose or universal approaches capable of detecting more than one image tampering type. This paper presents a comprehensive literature review of the recent development in general-purpose or universal image tampering detection techniques. The paper discusses and summaries recent general-purpose image tampering detection approaches, along with a detailed discussion on the datasets and evaluation metrics used. Comparative analysis of the performance of the reviewed methods, some discussion on the challenges faced by the current methods, and scopes for future directions are also presented in this review. The main goal of this paper is to help fellow and prospective researchers in digital image forensic by collecting the current trends, challenges, and some future direction in the development of general-purpose image tampering detection methods.

Keywords: image tampering; general purpose; tampering detection; image forensics; review

authenticity of digital images before using them to make crucial decisions.

To determine the authenticity and processing history of digital images, numerous image manipulation detection methods have been developed recently. The existing methods work based on the idea that each image manipulation operation creates unique traces that change the underlying statistics of an original image uniquely. As a result, to detect image tampering, researchers devised algorithms that recover these traces and utilize them to identify if and how an image is tampered with. Although these methods have been successful in detecting several types of image manipulations, such as median filtering [4], contrast enhancement [5], JPEG compression [6], copy-move [7], and image splicing [8], they cannot identify more than one type of image tampering. The disadvantages of these techniques are that they require multiple tests to determine if an image is altered or genuine [3]. Thus, methods capable of identifying multiple image manipulation operations are required.

To address these limitations, recent studies in image tampering detection have concentrated on building general-purpose techniques capable of detecting multiple types of image manipulation. Several general-purpose image tampering detection techniques [9-11] based on handcrafted features such as Spatial Rich Model (SRM) [12], Local Binary Pattern (LBP) [13], etc. have been proposed, with outstanding results. Moreover, with the success of deep learning methods, particularly CNN, in many visual identification tasks, current image forensics researchers [14-16] also seek to use the strength of deep learning methods to solve the problem of digital image tampering detection. The deep learning approaches can extract and learn image manipulation fingerprints from images automatically. Thus, their performances are significantly superior to that of earlier approaches.

This paper presents a comprehensive literature review of the recent developments in general-purpose or universal image tampering detection techniques. The paper discusses and summaries recent general-purpose image tampering detection methodologies, along with a detailed discussion on the commonly used datasets and evaluation metrics. Finally, a comparison of the performance of the reviewed methods, some discussion on the challenges faced by the current methods, and scopes for future directions are also discussed. Several related reviews [17-21] have been proposed in the literature, however, to the best of our knowledge, this is the first review focusing entirely on recent general-purpose image tampering detection methods. Our goal is to help fellow and prospective researchers in digital image forensic by compiling the current trends, challenges, and some future direction in the development of general-purpose image tampering detection methods.

Digital Image Tampering Techniques

In the context of digital image forensics, image tampering refers to any manipulation or alteration in an image to change its semantic meaning for illegal or malicious purposes [1,22]. Although digital images can be manipulated by photo editing tools to correct some flaws in the image or to make it look more perfect, however, if such actions are aimed at removing or creating objects that never existed for malicious purposes, such modification is considered as image tampering. The advent of high-performance photo editing software such as Photoshop and GIMP has made digital image tampering relatively easier, anyone with basic photo editing skills can tamper with the original information of an image. As a consequence, digital image tampering has now become ubiquitous in our daily lives leading to serious moral, ethical and legal issues [9]. Digital image tampering can be broadly categorized into **content changing tampering** (e.g. copy move and splicing) and content **preserving tampering** (e.g. Median Filtering and resampling) [23].

However, practical tampering often involves both tampering types. The content preserving tampering such as median filtering is used for smoothening the boundaries of the tampered regions in content changing tampering such as copy-move to make the traces of image tampering less visually detectable [22]. In this section, we first present the different types of content changing tampering followed by some content preserving tampering operations often used for hiding image tampering artifacts reported in the literature. Figure x. illustrates the different types of image tampering techniques.

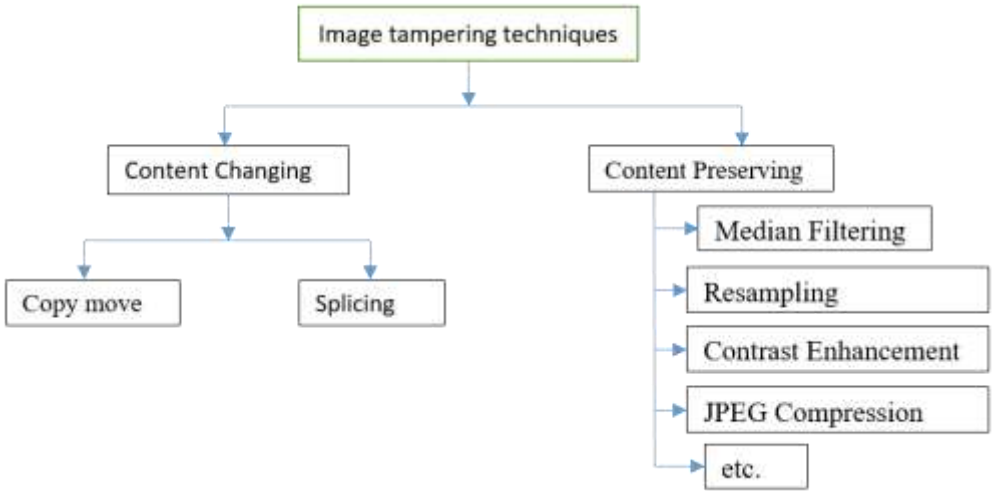

FIGURE 1. CLASSIFICATION OF IMAGE TAMPERING TECHNIQUES

Copy Move: One of the straightforward methods of altering the semantic meaning of a digital image is by removing an unwanted scene or object from the given image or creating a scene or object that never existed. In such circumstances, the forger needs to replace the region of the object removed or introduce a new object or scene in the image. A typical solution here is to copy a portion of the same image and paste it on the region where an object was removed or where a new object needs to be created [1]. When an image is tampered with by copying and pasting portions from the same image to either delete an object or create an object that never existed, such type of image tampering is known as copy-move [23]. Copy move, also known as cloning, is the most common and most studied image tampering. When carried out perfectly, it is usually difficult to detect copy-move visually as it does not leave behind any visual perceptible artifacts. To create a convincing copy-move tampering, the forger often performs some post-processing operations (content preserving tampering) such as filtering and geometric transformation (resize, rotate or translate) on the copied region to make it match

perfectly with its new surroundings. These operations hide the traces of copy-move making it difficult to be detected [24].

Splicing: Splicing, also known as cut and paste, is performed by copying a portion from a source image and pasting it into a target image to form a composite image. Unlike copy-move which usually involves a single image, splicing involves two or more images [1]. Splicing operations are very likely to introduce some inconsistencies between the characteristics of the pasted region and the rest of the image. Detecting splicing is usually performed by studying these inconsistencies. However, splicing detection is often more challenging than copy-move as the inconsistencies introduced are visually less perceptible than traces introduced by copy-move [25].

In-painting: In-painting is the action of drawing or filling some missing content on the image to fill the holes or gaps left by the object removal operation. This is achieved by exploiting the information in the region surrounding the holes. The hole is gradually filled from the periphery to the center resulting in a perceived continuity in the whole image [redi]. In-painting alters the original image and the tampered region. The tampered region usually have distinct noise, lighting, and compression rate when compared to the rest of the same image [26].

Resampling: Resampling is one of the most common image post-processing operations performed by applying geometric transforms such as rotation and scaling to an image. Resampling can hide the traces of the previous tampering such as copy-move or splicing [27]. The resampling process, however, produces fingerprints in the image histogram, and thus provides a useful clue for image tampering detection. Resampling in itself is not a type of image tampering, however, most forgers use it as a means of creating a convincing image tampering. For example, when performing image splicing, rotation, scaling or translation may be used to ensure that the spliced region matched perfectly on the new image [28].

Median Filtering: Median filtering is a widely used de-noising and smoothing post-processing operation which is often used to erase image tampering traces and statistical traces of blocking artifacts introduced by JPEG compression [29]. The application of median filtering may interfere with or diminish subtle traces of the previous manipulation and this may decrease the reliability of forensics methods [30]. Therefore, the detection of median filtering is a crucial step in revealing the processing history of an image under investigation.

Contrast Enhancement: Contrast enhancement is also a post-processing operation used to alter the illumination effect of an image to increase its quality. Contrast enhance is performed through histogram equalization, which involves remapping the intensity values in the input image so that the output image has a uniform distribution of intensities

[31]. Contrast enhancement can also be used by forgers to change the semantic meaning of an image or to conceal the traces of image manipulation. Thus, contrast enhancement detection plays a vital role in the forensics analysis of digital images.

Image Tampering Detection Techniques

Image tampering detection methods have become a requirement of the present time as image tampering is increasing every day. Image tampering is the action of adding or removing important features from an image to change its semantic meaning for illegal or malicious purposes [32]. Digital image tampering detection mechanisms aim to detect such modifications or tampering. Image tampering detection approaches can be broadly grouped into two different categories, active methods and passive methods [33-34]. Figure 2 shows a hierarchical organizational structure for image tampering detection methods, stressing the difference between active and passive approaches.

Active Methods: In the active approaches also known as data hiding approaches, a digital image is authenticated by inserting some relevant information such as watermarks or digital signature in the image at the time of capture [33]. The active approaches are very effective since any attempt to tamper with the image will inevitably destroy the inserted watermarks or digital signature. However, since inserting watermarks or digital signatures requires a specialized imaging device, these approaches have gained little application/utilization. Therefore, the passive approaches also known as blind approaches are now regarded as the most preferred approaches for image tampering detection tasks.

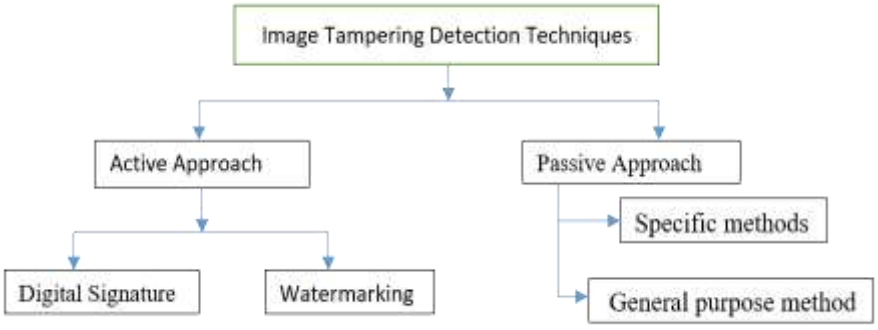

Figure 2. classification of image tampering detection techniques

Passive Methods: The passive approaches work in the absence of watermarks or digital signatures i.e. does not rely on previous information to determine if and how an image is tampered, but operate on the assumption that image tampering operations leave behind some traces and inevitably destroy some inherent properties of an image which can be

extracted and analyzed to determine the origin of a digital image and the integrity of its content [34]. The passive image tampering methods can be further classified into two classes, namely, tampering specific and general-purpose methods [35]. The tampering specific or dependent methods are designed to detect a specific type of image tampering. Most of these methods are tailored toward the detection of the two major content changing image tampering i.e. copy move and splicing [36]. On the other hand, the general-purpose or universal image tampering detection methods are designed to detect multiple types of image tampering by looking for general inconsistencies in images that appear due to tampering operations [37]. To create convincing tampering, often some post-processing and geometric transformation operations such as median filtering, JPEG compression, and resampling are applied to copy moved regions or spliced regions to smooth the boundaries of the tampered regions. A more general technique that could detect multiple types of image tampering can be built by analyzing the effect of post-processing and geometric transformation operations performed independent of the kind of tampering [22]. The general-purpose approaches provide universal strategies to perform image forensics irrespective of the type of tampering.

The remainder of this paper is organized as follows. Section 2 presents the commonly used datasets by the reviewed methods. Section 3 discusses and summarizes the recent methods in general-purpose image tampering detection. The evaluation metrics along with the comparison of the review methods are presented in section 4. Finally, the challenges along with future scopes and conclusions are added in sections 5 and 6, respectively.

General Purpose Image Tampering Detection Datasets

Unlike the specific image tampering detection approaches, there are no benchmark datasets for evaluating the general-purpose image tampering detection approaches. Therefore, the researchers need to prepare a dataset of both the original and tampered images from authentic and uncompressed image datasets for training and evaluating their models. In this way, researchers can recreate different image tampering operations and conduct experiments on an adequate and customized dataset. Several authentic image datasets have been used as the primary data source for the training and evaluation of general-purpose image tampering detection approaches. Some of these datasets were originally intended to benchmark camera model identification and image steganalysis techniques, while others to evaluate and benchmark content-based image retrieval and object detection models. In this section, we present a review of the major sources of datasets used for synthesizing the datasets used for training and evaluating the general-purpose image tampering approaches from the literature

One of the first and widely used datasets for the purpose of general-purpose image forensic is the Uncompressed Image Database (UCID) [38]. The UCID dataset was released in 2003 to serve as a benchmark dataset for evaluating image retrieval, image compression, and color quantization techniques. The dataset consists of over 1300 uncompressed images of size 384 × 512 or 512 × 384 in TIFF format together with a ground truth of a series of query images with corresponding models that an ideal Content-Based Image Retrieval (CBIR) algorithm would retrieve. All the images in UCID were captured using a single camera and comprises images on a variety of topics including natural scenes and man-made objects, both indoors and outdoors. Owing to the uncompressed format, the UCID dataset has been employed in many specific and general-purpose image tampering detection systems as a source for synthesizing training and evaluation datasets.

Another dataset with a wide application in the development of general–purpose image forensic approach is the BOSSBASE [39] dataset. Released in 2010 originally for research in image steganalysis field, the BOSSbase database today forms a major source of datasets used in synthesizing the training and evaluation datasets for both specific and general-purpose image tampering detection techniques. The dataset consists of a training set and testing set along with the HUGO algorithm that can be used to create the steganography images. The training dataset consists of 10,000 grayscale cover images with a dimension of 512 × 512. The testing set consists of 1000 grayscale images with a dimension of 512 × 512. The raw images were captured using 7 different cameras and stored in PGM format.

Another dataset that has gained wide applications in the synthesis of the training and evaluation datasets of general-purpose image tampering detection models is the Dresden image dataset. The Dresden image dataset was released in 2010 by [40] specifically to develop and benchmark camera-based digital forensic approaches. The dataset contains more than 14,000 authentic images of various resolutions captured with 73 different cameras drawn from 25 different models to ensure that device-specific and model-specific characteristics can be disentangled and studied separately.

The Raw Image Database (RAISE) [41] dataset is a wide collection of authentic and diverse image datasets intended to serve as a common benchmark for comparing, testing, and evaluating present and future generation forensic algorithms. The dataset contains 8156 uncompressed high-resolution images of various sizes, depicting different scenarios and subjects. The dataset is properly annotated and is publicly available together with accompanying metadata. It comprises 4 subsets called RAISE-1K, RAISE-2K, RAISE-3K, and RAISE-4K. RAISE dataset has been used by several authors to create different image

tampering for the training and evaluation of general-purpose image tampering models, thus, it's also a powerful resource for general image tampering researchers.

The IEEE Information Forensics and Security Technical Committee (IFS-TC) image forensic datasets were released in 2013 during an image forensic challenge [42]. The datasets consist of both original and tampered images involving two tampering techniques, namely, image splicing and copy-move. Each tampered image was accompanied by a ground-truth binary map that depicted the tampered region in the image. The dataset consists of 500 tampered images and 1,000 authentic (original) images, all of which are of the same size and in PNG format. While this dataset was specifically designed for evaluating and benchmarking copy-move and image splicing detection models, it has also been used by several authors as a primary data source for training and evaluating general-purpose image tampering detection approaches.

The Microsoft Common Object in Context (MS COCO) dataset [43] originally intended for advancing the state of the art in object recognition has also been used to create different image forgeries for the training and evaluation of general image tampering detection approaches. The dataset comprises over 300k images of complex everyday scenes containing common objects in their natural context in JPEG format and it comes along with the class annotation and segmentation annotation.

Other datasets that are used for synthesizing the training and evaluation datasets of general-purpose image tampering include NRCS [44], SZUBase [45-46], Kaggle Camera Model Identification (KCMI) dataset [60], and images from different cameras. The NRCS database contains 2,728 JPEG compressed images. The database was created by the United States Department of Agriculture and includes high-resolution photographs from a wide range of agricultural categories. SZUBase is a dataset collected in [46] with 40000 grayscale images of size 512 × 512. The KCMI dataset was released by Kaggle in collaboration with IEEE in 2018 during a camera model identification challenge organized by the duo. The dataset was captured using 10 different camera models with 275 images from each device.

Table 1 provides a summary of the datasets used in the training and evaluation of general-purpose image tampering techniques. In particular, the table presents the dataset names, released year, image size, format, original purpose of the datasets and the number of samples in each of the datasets.

Table 1. Summary of the datasets used in the literature of general-purpose image tampering detection. The "L", "C", and "U" in the **format** column correspond to Lossy compression, Lossless compression, and Uncompressed, respectively.

S/N	Dataset Name	Release Year	Image size	Format	Purpose	Number of samples
1	Dresden [40]	2010	Various	L-JPEG, U-NEF	Digital image forensic	25137
2	BOSSbase [39]	2010	512x512	U-PGM	Image Steganography	10,000

3	UCID [38]	2004	Various	U-TIFF	image retrieval, compression and color quantization	1338
4	RAISE [41]	2015	Various	C-TIFF, U-NEF	Image Forensic	8156
5	IEEE-IFS-TC [42]	2013	Various	C-PNG	Image Forensic	1050/1150
6	SZUbase [45]		512x512		Image Steganography	-
7	NRCS [44]	2004	1500x2100	U-TIFF, L-JPEG		11,036
8	Kaggle Camera [60]	2018	Various	L-JPEG, C-TIFF	Camera Model Identification	2750
9	MS COCO [43]	2014	Various	L-JPEG	Object detection and segmentation	328k

General Purpose Image Tampering Detection Methods

General-purpose image tampering approaches are employed to detect multiple or a group of image tampering operations. These techniques are generally based on, detecting the traces left behind during the post-processing or geometric transformations operations and the general disturbance in images that may appear due to image tampering operations [22]. The methods used for detecting general-purpose image tampering can be categorized into two classes, namely, handcrafted features and deep learning-based methods, which are discussed in this section. Fig 3. Shows the general architecture of image tampering detection systems based on handcrafted (top) and deep learning (bottom) methods. The forward and backward arrows in the bottom flowchart indicate forward and backward propagation directions. We use "Conv." and "FC" to represent Convolution and Fully Connected layers, respectively.

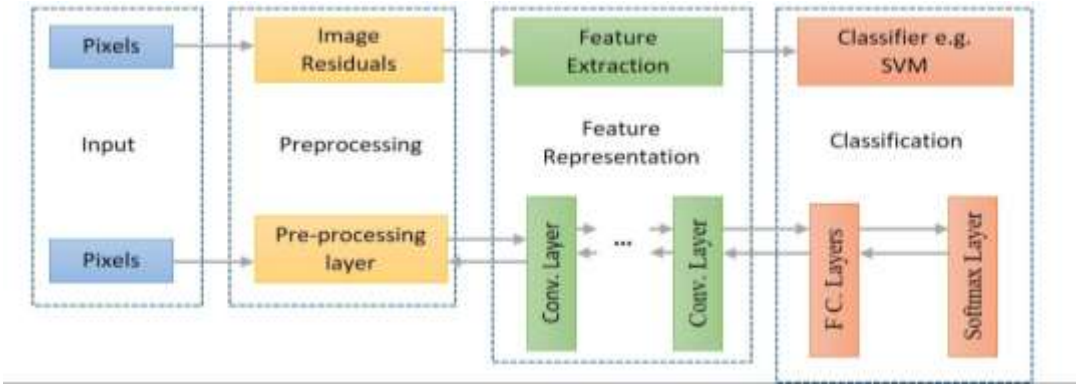

FIGURE 3. ARCHITECTURES OF IMAGE TAMPERING DETECTION SYSTEMS

Handcrafted Feature-Based Methods

Handcrafted methods or the traditional methods extract intrinsic statistical properties artificially from input images and most often employ machine learning algorithms for classification. The handcrafted methods mainly build image tampering detection methods in two steps: feature extraction and classification [37]. In the feature extraction step, a set of handcrafted features is extracted from each image to capture the impact of image tampering operations. In the classification step, classifiers such as SVM or ensemble classifiers are learned based on the extracted features. The design of good discriminative features is the key step in this approach and largely impacts the detection performance. Thus, several studies have proposed the use of different discriminative features, which are discussed in this subsection.

The first general-purpose image forensics method utilizing this technique was proposed by Qiu et al. [9] where they suggested the use of steganalytic features such as LBP (Local Binary Pattern) and SRM (spatial rich model) in the design of a general-purpose image tampering system. The proposed method modeled image tampering detection problems as steganography and evaluate LBP and SRM steganalytic features on the detection of five types of image manipulation operations, including Gaussian blurring, gamma correction, lossy JPEG compression, median filtering, and re-sampling. The method achieves high detection accuracies in detecting individual and multiple tampering operations.

The work of Fan et al. [47] introduced a general purposed image manipulation detection approach where image manipulation fingerprints are learned from Gaussian mixture model (GMM) parameters of small image patches processed by different image manipulation operations. The proposed method can detect a tampered image by comparing the average patch log-likelihood values calculated on overlapping image patches under different GMMs of original and tampered images. Six tampering operations, median filtering, Gaussian filtering, WGN (White Gaussian Noise), UnSharp Masking (USM), JPEG Compression, and resampling are considered in the study. The proposed model shows excellent performance in detecting both individual and multiple image tampering on small and large images.

Li et al. [10] also proposed a universal image tampering approach using residual-based features and powerful steganalytic features called the Spatial Rich Model (SRM). The technique is based on SRM features, extracted from image residual, obtained from the original input image using high pass filtering technique. Using this approach, they were able to obtain universal feature sets which they used in building the proposed model. The technique was able to detect multiple image tampering operations and some anti-forensics operations effectively and universally.

In [11], Farooq *et al.* investigated and demonstrated the performance of SRM and LBP in detecting multiple image tampering. They embedded LBP in SRM sub-models to capture detailed statistics of the quantized version of image noise residuals. The extracted features were used for classification using an ensemble classifier. Synthesized datasets from the first IEEE IFS-TC image forensics challenge [42] were used for the experiment. The experimental results demonstrate that using LBP in conjunction with the SRM feature makes the model capable enough to detect almost all types of forgeries with an accuracy of 98.4%.

Peng *et al.* [48] designed a universal feature set for multi-purpose image forensics capable of detecting different kinds of image manipulation operations concurrently using residual-based features. To remove the effect of image content on the robustness of the proposed features, they introduced a residual group with several high pass filtered residuals from which a partial correlation coefficient is exploited. The partial correlation coefficient is then combined with the autoregressive coefficient and transition probability to form the proposed composite feature sets which are used to measure how manipulations affect the pixel neighborhood correlations in a linear and non-linear fashion. The composite feature set is then fed to a multi-classifier which performs the final classification. The proposed method achieved excellent performance in identifying several image manipulations.

The summary of the handcrafted methods, their targeted image tampering, features used, classifiers and performances are listed in Table 2.

Table 2. Comparative analysis of general-purpose image tampering methods using handcrafted techniques

S/N	Methods	Targeted Tampering	Feature	Classifier	Dataset	Performance
1	[9]	Gaussian blurring, gamma correction, lossy JPEG compression, median filtering, and re-sampling.	LBP and SRM	Ensemble Classifier	IEEE IFS-TC Image forensic database	Acc= 96.89% (SRM), Acc= 92.24% (LBP)
2	[47]	median filtering, Gaussian filtering, WGN (White Gaussian Noise), UnSharp Masking (USM), JPEG Compression and resampling	Patch likelihood of different Gaussian Mixture Model (GMM) of original and tampered images	Decision threshold	Images from 4 different cameras	Acc => 92.67%

3	[10]	Gamma correction, Histogram equalization, Unsharp masking sharpening, Mean filtering, Gaussian filtering, Median filtering, Wiener filtering, up-sampling, down-sampling, and JPEG compression	Residual based features + SRM	Ensemble classifier	Bossbase	Acc = 98.41%
4	[11]	Gaussian Blurring, Gamma Correction, JPEG Compression, Median Filtering, Up sampling, Down sampling, Contrast Enhancement, Cropping, Copying, and Image Splicing	LBP with SRM	Ensemble classifier	IEEE IFS-TC image forensics datasets	Acc = 98.40%
5	[48]	Gaussian blurring, median filtering, re-sampling, and JPEG compression	Residual based features	Multi-classifier	BOSSbase and RAISE databe	Acc = 95.20%

Although the handcrafted methods have yielded promising results, the extraction of handcrafted features suffers from high computational costs and their performance can be severely affected by post-processing operations such as JPEG compression and resampling. Moreover, since the feature extraction and classification steps are disconnected, they can not be optimized simultaneously. This implies that the guidance from the classification step will not be used to extract useful features in the feature extraction phase. Thus, it is desirable to develop a multi-purpose image tampering approach that can learn effective and robust features adaptively with joint feature extraction and classification steps.

Deep Learning-Based Methods

In recent times, deep learning has attracted increasing attention due to its satisfactory results in several image processing and computer vision applications [49]. Inspired by these successes, the forensics community has recently focused on applying deep learning-based methods for general-purpose image tampering detection. Unlike the handcrafted feature-based methods, the deep learning methods directly learn effective features automatically from the input images through convolution, pooling, and activation operations, and the feature extraction and classification steps can be optimized simultaneously.

In a quest for better general-purpose image tampering detection methods, several methods utilizing the deep learning method have been proposed recently. For example, the work of Bayar and Stamm, [3] presented a universal image manipulation detection technique that utilizes a deep learning approach. The proposed method is based on a new convolution layer called "constrained convolution layer", capable of suppressing image content to learn image manipulation operation directly from data. Their method could effectively detect specific and multiple image manipulation operations in both uncompressed and compressed images format, and it showed superiority over SRM based general-purpose image manipulation approaches.

Tant *et al.* [50] illustrated a CNN and nearest-neighbor interpolation-based multipurpose image manipulation method. The nearest neighbor interpolation is employed in the preprocessing layer to magnify the input images to enlarge the differences between image manipulation operations. In the network design, the authors used multi-scale convolutional layers in the first few layers to learn hierarchical representations for different image tampering operations. However, since the multi-scale Conv layers are generally a highly non-linear function of the input, the mlpconv layers are employed to improve the network's nonlinear modeling capability. Moreover, they employed shortcut connections between the mlpconv layers to increase the depth of their network and at the same time preventing information loss. The proposed model is used for the detection of Median filtering, Mean Filtering, Gaussian Filtering, Contrast Enhancement, resampling, and JPEG compression in small image blocks. The method achieves high accuracies of 93.77% and 95.91% in 32x32 and 64x64 image blocks, respectively.

In [51], Boroumond and Fridrich introduced a method for detecting the processing history of an image that could correctly detect multiple processing operations. It is based on CNN with an IP layer accepting statistical moments of feature maps. The proposed CNN model was trained in three phases. The first phase involved training a "moment extractor" module on small images (512×512) which was then used in Phase II to extract moments from all (arbitrarily sized) training images. In the last phase, the IP layers were trained to map the extracted moments to tampering operation classes. Four types of processing operations were considered: low-pass filtering (blurring), high-pass filtering (sharpening), de-noising (content-adaptive low-pass filtering), and tonal adjustments, such as histogram equalization, gamma correction, and contrast enhancement. The proposed model could correctly classify images of different sizes and shows robustness against JPEG compression.

In [52], the authors proposed a universal image forensics method based on a deep Siamese Convolutional neural network. The proposed method takes as input a pair of image patches and decides whether they are identically or differently processed. Five

image tampering operations, Gaussian Blurring, Median Filtering, Resampling, Noise Addition, and Gamma Corrections were considered and the experimental results demonstrate that the proposed method could detect both known and unknown image tampering operations with high detection accuracies.

Chen *et al.* [53] presented a method that can simultaneously detect 11 different types of image manipulations based on densely connected convolutional neural networks. The approach replaced the standard convolution layers in CNN with a dense connectivity pattern of denseNet [54] to strengthen the transmission of features related to image manipulation detection. The approach achieves high accuracies on different datasets and shows robustness against JPEG compression.

In [55], the authors described a multiple image tampering technique based on CNN and frequency domain features of image residuals. The authors designed a two-layer CNN that extracts frequency-domain features of image residuals derived from the input images. The extracted features are used to classify seven different types of image manipulations using softmax and extremely randomized tree classifiers.

Camacho and Wang [56] proposed a general-purpose image manipulation approach that introduced a new initialization technique in the first layer of CNN to address the challenging nature of general-purpose image manipulation detection. The authors presented a method for creating random high-pass filters that could operate without constraints, based on the groundbreaking work of the famous Xavier initialization [57]. The method obtained high detection accuracies for image tampering such as median filtering, Additive White Gaussian Noise (AWGN), and resampling in both binary as well as multiclass classifications.

In a related work to their previous work, the authors of [56] recently proposed a data-dependent scaling strategy for first-layer filters initialized by various algorithms [58]. The proposed method took into account natural image statistics and was able to ensure that the amplitude (i.e., variance) of data flow in a CNN remained stable, which was useful for general-purpose image manipulation detection. A comparative study on the output variance of the different initialization algorithms before and after applying the proposed data-dependent scaling approach shows that the proposed method worked well with the different initialization approaches and different CNN architectures when tested on the task of detecting both individual and multiple image tampering operations.

The authors in [14] proposed a multi-purpose image tampering approach based on reinforcement learning that could design a deep neural network automatically without manual intervention. The method consists of a learning agent which is trained to choose layers of CNN sequentially according to the Q. Learning algorithm [59] within a tailored state-action search space designed to learn suitable network, the e-greedy strategy, and

experience replay for searching an optimal network and speeding up the search process, respectively. The proposed model is evaluated on a dataset generated from SZUbase [45-46] image database. The method obtains an average detection accuracy of 88.62% on the detection of the eleven image tampering operations.

Aminu and Agwu [15] presented a general-purpose image tampering detection approach based on CNN and Local Optimal Oriented Pattern (LOOP). The LOOP is employed in the preprocessing layer to capture the different tampering traces that might be introduced by different tampering operations. The Proposed CNN is then fed the LOOP maps from the preprocessing layer, which extracts and learns the representations of different image tampering traces. The final classification is then performed by three classifiers, softmax, xgboost, and Extra Tree. Five tampering operations including, Contrast Enhancement, Median Filtering, Gaussian Blurring, Gamma Correction, and JPEG Compression were considered in the study. The method achieves high detections rates in both individual and multiclass image tampering detection. However, the performance of the proposed model degrades in JPEG compressed and small images.

In [16], the authors designed a general-purpose image tampering detection approach based on deep learning. They proposed the use of residual dense blocks in building their model to exploit the local dense connections and global residual learning for better classification. The network input and high-level hierarchical features produced by proposed residual dense blocks are fused globally for better information propagation throughout the entire network. The architecture achieved overall detection accuracies of 95.09% and 97.31 % for BOSSBase [39] and Dresden [40] datasets, respectively in multiple image tampering detection.

Ali *et al.* proposed a deep learning method in [61] that could identify several instances of image manipulation based on double compression artefacts. The proposed model was trained utilizing the difference between the original and corresponding recompressed images. The technique recognized both image splicing and copy moves and had an overall validation accuracy of 92.23 %.

The authors of [62] proposed a multi-scale residual deep CNN technique for general-purpose image tampering detection. The proposed approach uses a multi-scale residual module for adaptably extracting image tampering artifacts from the input images and feature extraction blocks intended to extract high-level image tampering artifacts from the output of the multi-scale residual module. With overall accuracies of 97.07% and 97.48% on the Bossbase and Dresden datasets, respectively, the proposed approach could detect six separate image tampering operations.

In [63], the authors introduced a general-purpose technique for detecting image tampering and manipulation operation chains that was based on CNN and a recent local

feature descriptor called LOOP. The authors combine the discriminative powers of the local feature descriptor and the feature extraction capabilities of CNN in order to create a powerful general-purpose image tampering detection method.

Table 3 provide a summary of the various general-purpose image tampering detection methods using deep the learning techniques. In particular, the table highlights the targeted image tampering, features, network type, and datasets used by each method alongside the performance of each method with respect to tampering detection accuracy.

Although the deep learning approaches have improved on the performance of the handcrafted approaches, they often fail in the presence of anti-forensics methods and their performances degrades in the JPEG compressed and low-resolution images. Thus, the development of general-purpose image tampering approaches that will be robust against anti-forensics methods and JPEG compression remains an open challenge.

Table 3. Comparative analysis of general-purpose image tampering methods using deep learning techniques

S/N	Methods	Targeted image Tampering	Feature	Network Type	Dataset	Performance
1	[3]	Median filtering, Gaussian Blurring, resampling, JPEG Compression, and AWGN	Prediction error filters	CNN - ERT	IEEE IFS-TC image forensics, 34 new camera models, and Dresden database	Acc = 99.97%
2	[50]	Median filtering, Mean Filtering, Gaussian Filtering, Contrast Enhancement, resampling, and JPEG compression	Deep Features	CNN- Nearest Neighbor interpolation Algorithm	BOSSbase, UCID database, and NRCS	Accuracies of 93.77% and 95.91% in 32x32 and 64x64 image blocks, respectively.
3	[51]	Low-pass filtering (blurring), high-pass filtering (sharpening), de-noising (content-adaptive low-pass filtering), and tonal	Deep features	CNN	BOSSbase	Acc = 97.99%

		adjustments, such as histogram equalization, gamma correction, and contrast enhancement.				
4	[52]	Gaussian Blurring, Median Filtering, Resampling, Noise Addition, and Gamma Corrections	Deep Features	Deep Siamese - CNN	Dresden	Acc =99.64%
5	[14]	Median filtering, Wiener Filtering, Average Filtering, Gaussian Blurring, Unsharp masking, Gamma Correction, Histogram Equalization JPEG Compression, JPEG 2000, scaling, rotation and	Deep Features	Auto-Generated CNN with Reinforcement Learning	SZUbase, BOSSbase and UCID.	Acc = 88.62%
6	[15]	Gamma Correction, Median Filtering, Gaussian Blurring, JPEG Compression, and Contrast Enhancement	Local Features and Deep features	CNN-ET, XGBOOST	IEEE Image Forensics Database, BOSSbase and MS COCO database	Acc = 99.81%
7	[53]	Median filtering, Wiener Filtering, Average Filtering, Gaussian Blurring, Unsharp masking, Gamma Correction, Histogram Equalization JPEG Compression, JPEG	Deep features	Dense - CNN	Image from diff cameras, BOSSbase, and UCID	Acc = 98.08%

		2000, scaling, rotation and				
8	[55]	Average filtering, Gaussian filtering Laplacian filtering, Median filtering Rescaling operation, Rotation operation, and Wiener filtering	Frequency domain features of image residuals	CNN - ERT	IEEE IFS-TC image forensics and others	Acc = 84.52% (32x32) , Acc = 81.64% (64x64)
9	[56]	Median filtering, Gaussian blurring, Additive Gaussian noise, Resampling, and JPEG compression	Deep Features	Different CNN architectures	Dresden	Acc= 96.45 (conv. Based Scaling) and Acc = 96.42 (covariance based scaling)
10	[58]	Median filtering, Gaussian blurring, Additive Gaussian noise, Resampling, and JPEG compression	Deep Features	CNN	Dresden	Acc = 99.67
11	[16]	Median filtering, Gaussian Blurring, resampling, JPEG Compression and AWGN	Deep Features	Residual Dense-CNN	Dresden and BOSSbase	Acc = 95.09 (BOSSbase), Acc = 97.31 (Dressden)
12	[61]	Copy move and Image slicing	Image difference	CNN	CASIA 2.0	Acc = 92.23
13	[62]	Additive White Guassian Noise (AWGN), Median Filtering, Gaussian Blurring, Resampling, JPEG Compression, and Contrast Enhancement	Prediction error filters	Multiscale Residual Deep CNN	Dresden and BOSSbase	Acc=97.07 (Bossbase), Acc = 97.48% (Dresden)

14	[63]	Gamma Correction, Median Filtering, Gaussian Blurring, JPEG Compression, and Contrast Enhancement	Deep Features	CNN-ET and CNN- XGBOOST	IEEE Image Forensics Database, BOSSbase and MS COCO database	Acc = 99.15%

Performance Evaluation Metrics

Deciding on a particular performance metric may depend on many factors, including the forensic problem and the nature of datasets to be used. Since there are no benchmark datasets for training and evaluating the general-purpose approaches, researchers usually generate synthetic images from available datasets. These synthesized datasets consist of both the tampered and original images in an equal proportion. While these may not be the case in real-world scenarios, the majority of the general-purpose image tampering approaches are trained and evaluated with datasets consisting of an equal number of each class. Therefore, the accuracy and confusion metrics are the most preferred metrics in evaluating the general-purpose image tampering detection approaches. However, in an experimental setting with imbalanced data from different classes, the accuracy metric in general results in biased value and thus is not preferred.

The image tampering detection model's accuracy is defined as the percentage of correctly classified samples among all samples which can be formulated as in equation (1).

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \quad (1)$$

where TP, TN, FP, and FN stand respectively for true positive, true negative, false positive, and false negative numbers of classified samples.

The confusion matrix shown in table 4 is a table used to describe the performance of a classification model on a set of test data for which the true values are given. True positive (TP) and true negative (TN) are the correct predictions made by the model while False positive (FP) and false-negative (FN) are the errors made by the model. All the four terms used in computing the accuracy above are drawn from the confusion matrix as can be seen in the mathematical formulations. The accuracy metrics is used for measuring the predictive performance of a model in individual image tampering while the confusion matrix measures the performance of models in multiple image tampering or a group of image tampering detection. Although other metrics such as recall, precision and AUC have been used in individual image tampering detections, they have gained little or no applications in the design of general purpose image tampering detection methods.

Table 4. confusion matrix

	Predicted Positive Class	Predicted Negative Class
Actual Positive class	True Positive (TP)	False Negative (FN)
Actual Negative class	False Positive (FP)	True Negative (TN)

Performance Analysis

This section provides a comparative analysis of the performance of both the handcrafted and deep learning-based approaches for general-purpose image tampering detection with respect to the detection accuracy. Figures 4 and 5 illustrate the accuracies achieved by various handcrafted and deep learning-based general-purpose image tampering techniques respectively. The maximum accuracy in the handcrafted approaches is achieved by [10], whereas the method of [3] achieved the highest accuracy in the deep learning-based approaches. The Deep learning techniques are found to be more robust than the handcrafted feature-based techniques with respect to detection accuracies as they are capable of automatically learning and extracting image tampering clues directly from input images without the need for complex pre-processing steps associated with the handcrafted approaches which may introduce noise that may interfere with the needed image tampering artifacts. Moreover, since the feature extraction and classification phase of the deep learning approaches are connected, insights from the classification phase can be used to guide feature extraction in the feature extraction phase. However, the deep learning approach requires a huge amount of data, more computational resources, and training time as compared to the handcrafted-based methods.

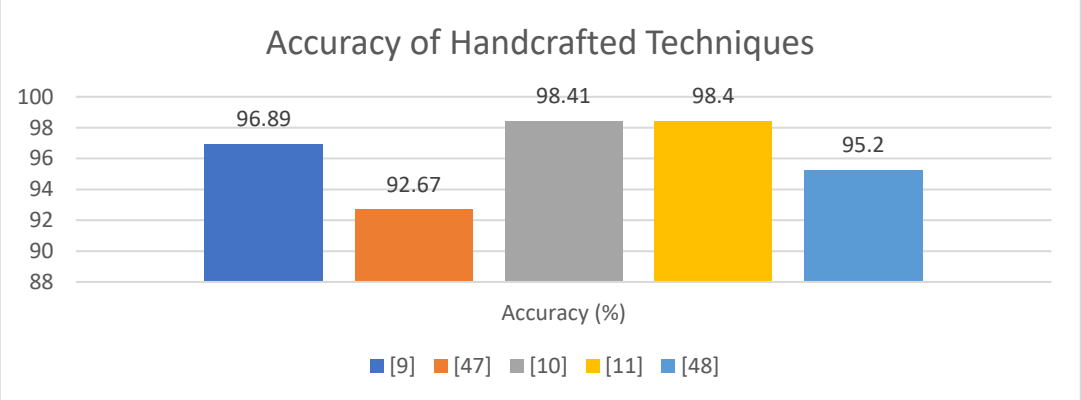

Figure 4. General purpose image tampering detection accuracy comparison between different handcrafted methods

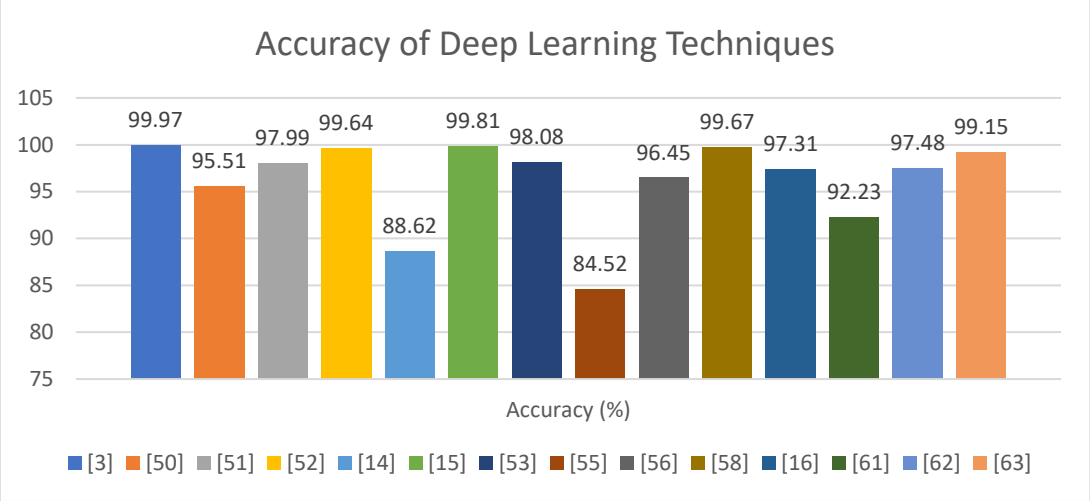

Figure 5. General purpose image tampering detection accuracy comparison between different deep learning methods

Research Challenges and Future Scopes

From the above review, it is clear that a lot still needs to be done in this field and various challenges need to be addressed. A major challenge of the existing general-purpose image tampering detection approaches is that they failed in the presence of anti-forensics methods. Thus, efforts can be directed at strengthening the robustness of the current general-purpose image tampering approaches and the development of methods capable of detecting both image tampering operations and anti-forensics methods. Furthermore, another future direction worth exploring is the extension of general-purpose image tampering detection to other media, specifically videos. Videos today are even more powerful information carriers than images in communication and are often used as evidence in trials. Therefore, the development of robust general-purpose video tampering detection approaches can represent an interesting area for new digital forensic researchers. Finally, dataset selection is also a significant factor in the evaluation of the general-purpose image tampering detection methods. Unlike the specific image tampering approaches, there are no prepared benchmark datasets for evaluating the general-purpose approaches. Image tampering operations such as median filtering, scaling, JPEG compression, contrast enhancement, and Gaussian blurring, etc. are performed during pre-processing phase using different data sources. This leads to the use of different datasets by different authors. In such a case, the experiments cannot be repeated efficiently and the obtained results cannot be generalized easily. Thus, the accuracy claimed by various studies cannot be compared as they have used different datasets, scaling, and compression schemes. Therefore, efforts can also be directed

toward the creation of a benchmark dataset that will contain all the known image tampering operations.

Conclusions

In this paper, we have elaborated on the methods, datasets, and evaluation metrics used in recent times for developing general-purpose image tampering detection solutions. Other existing reviews have focused on both tampering specific methods and other forms of image tampering. None of them covered a detailed review of general-purpose or universal image tampering detection methods. Hence, this paper discusses and summaries recent general-purpose image tampering detection approaches, along with a detailed discussion on the datasets and evaluation metrics used. Comparative analysis of the performance of the review methods, some discussion on the challenges, and the scopes for future directions are also presented in this review. From the review, it can be concluded that the deep learning approaches provide better solutions than the traditional methods and are the most widely used methods in recent times.

References

Redi, J. A.; Taktak, W.; Dugelay, J. L. Digital image forensics: a booklet for beginners. *Multimedia Tools and Applications* **2011**, 51,133-162.

Bayar, B.; Stamm, M.C. A deep learning approach to universal image manipulation detection using a new convolutional layer. *In Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security* **2016**, 5 -10.

Bayar, B.; Stamm, M.C. Constrained convolutional neural networks: A new approach towards general purpose image manipulation detection. *IEEE Transactions on Information Forensics and Security* **2018,** 11, 2691-2706.

Tang, H.; Ni, R.; Zhao, Y.; Li, X. Median Filtering Detection of Small-Size Image based on CNN. *J. Vis. Commun. Image R.* **2018.**

Sun, J. Y.; Kim, S. W.; Lee, S. W.; Ko, S. J. A novel contrast enhancement forensics based on convolutional neural networks. *Signal Processing: Image Communication* **2018**.

Harish, A. N.; Verma V.; Khanna, N. Double JPEG Compression Detection for distinguishable blocks in images with same Quantization matrix. *2020 IEEE 30th International Workshop on Machine Learning for Signal Processing (MLSP)* **2020**, pp. 1-6.

Abdalla, Y.; M.T. Iqbal, M. T.; Shehata, M. Copy-Move Forgery Detection and Localization Using a Generative Adversarial Network and Convolutional Neural-Network. *Information* **2019**, 9, 286.

Rao, Y.; J. Ni, J.; H. Zhao, H. Deep Learning Local Descriptor for Image Splicing Detection and Localization. *IEEE Access* **2020**, 8, 25611-25625.

Qiu, X.; Li, H.; Luo, W.; and Huang J. A universal image forensics strategy based on steganalytic model. *In Proceedings of the 2nd ACM workshop on Information hiding and multimedia security* **2014**, 165-170

Li, H.; Luo, W.; Qiu, X.; Huang, J. Identification of various image operations using residual-based features. *IEEE Trans. Circ. Syst. Video Technol.* **2018**, 31–45.

Sundus, F.; Yousaf, M. H.; Hussain, F. A generic passive image forgery detection scheme using local binary pattern with rich models. *Computers & Electrical Engineering* **2017**, 62, 459-472.

Fridrich, J.; Kodovsky, J. Rich models for steganalysis of digital images. *IEEE Transactions on Information Forensics and Security* **2012,** 7, 868–882.

Ojala, T.; Pietikinen, M.; D. Harwood, D. Performance evaluation of texture measures with classification based on Kullback discrimination of distributions. *In Proc. ICPR*, **1994**.

Wei, Y.; Chen, Y.; Kang, X.; Wang, Z.J.; Xiao, L. Auto-generating neural networks with reinforcement learning for multi-purpose image forensics. In *2020 IEEE International Conference on Multimedia and Expo (ICME)* **2020**, 1-6.

Aminu, A.A.; Agwu, N.N. General Purpose Image Tampering Detection Using Convolutional Neural Network and Local Optimal Oriented Pattern (Loop). *Signal & Image Processing: An International Journal (SIPIJ)* **2020,** *Vol*, 12. 13-32.

Singh, G.; Goyal, P. GIMD-Net: An effective General-purpose Image Manipulation Detection Network, even under anti-forensic attacks. In *2021 International Joint Conference on Neural Networks (IJCNN)* **2021** (pp. 1-8).

Camacho, I.C.; Wang, K. A Comprehensive Review of Deep-Learning-Based Methods for Image Forensics. Journal of Imaging **2021**, 7, 69.

Ferreira, W.D.; Ferreira, C.B.; da Cruz Júnior, G.; Soares, F. A review of digital image forensics. *Computers & Electrical Engineering* **2020**, *85*, 106685.

Khudhair, Z.N.; Mohamed, F.; Kadhim, K.A. A Review on Copy-Move Image Forgery Detection Techniques. In *Journal of Physics* **2021**, 012010.

Kaur, H.; Jindal, N. Image and video forensics: A critical survey. *Wireless Personal Communications* **2020**, 1-22.

Saber, A.H.; Khanl, M.A.; Mejbel, B.G. A survey on image forgery detection using different forensic approaches. *Advances in Science, Technology and Engineering Systems Journal* **2020**, 5, 361-370.

Lilei, Z.; Z. Ying Z.; Vrizlynn, L. L. A Survey on Image Tampering and Its Detection in Real-world Photos. *Journal of Visual Communication and Image Representation* **2019**, 58, 380-399.

Farid, H. A survey of image forgery detection. *IEEE Signal Process Mag* **2009**, 2, 16–25.

Piva, A. An overview on image forensics. *International Scholarly Research Notices* (*ISRN*) 2013.

Thakur, R.; Rohilla, R. Recent advances in digital image manipulation detection techniques: A brief review. *Forensic Science International* **2020**, 312, p.110311.

Bourouis, S.; Alroobaea, R.; Alharbi, A.M.; Andejany, M.; Rubaiee, S. 2020. Recent advances in digital multimedia tampering detection for forensics analysis. *Symmetry* **2020**, 12(11), 1811.

Cao, G.; Zhou, A.; Huang, X. Song, G.; *et al,* "Resampling detection of recompressed images via dual-stream convolutional neural network," *arXiv preprint arXiv: 1901.04637* **2019**.

Bunk, J.; Bappy, J. H.; Mohammed, T. M.; *et al.* Detection and localization of image forgeries using resampling features and deep learning. *In: Computer Vision and Pattern Recognition Workshops (CVPRW), IEEE Conference* **2017**. 1881–1889.

Yu, L.; Zhang, Y.; Han, H.; Zhang, L.; Wu, F. Robust median filtering forensics by CNN-based multiple residuals learning. *IEEE Access* **2019**, 7, pp.120594-120602.

Aminu, A. A.; Agwu, N. N.; Obianuju, N. Median Filtering Forensics Based on convolutional neural network and local optimal oriented patterns. *International Journal of Computer Application 2020,* 175, 42-51.

Sun, J.Y.; Kim, S.W.; Lee, S.W.; Ko, S.J. A novel contrast enhancement forensics based on convolutional neural networks. *Signal Processing: Image Communication* **2018**, 63, 149-160.

Manjunatha, S.; M. M. Patil, M. M. Deep learning based techniques for image tamper detection. *Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)* **2021**, pp. 1278-1285

Kakar, P. Passive Approaches for Detecting Digital Image Forgery. *PhD Thesis*, *Nanyang Technological University* **2012**.

Al-Qershi, O.M.; Khoo, B.E. Passive detection of copy-move forgery in digital images: state-of-the-art. *Forensic Sci Int* **2013**, 231:284–295.

Gupta, S.; Mohan, N.; and Kaushal, P. Passive image forensics using universal techniques: a review. *Artificial Intelligence Review* **2021**, pp.1-51.

Gupta, A.; Singhal, D. A Simplistic Global Median Filtering Forensics Based on Frequency Domain Analysis of Image Residuals. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) **2019**, 15(3), 1-23.

Qian, Y.; Dong, J.; Wang, W.; Tan, T. Deep learning for steganalysis via convolutional neural networks. In *Media Watermarking, Security, and Forensics* **2015**, 9409, 94090J

Schaefer, G.; Stich, M. UCID-An uncompressed color image database. In proceedings of the SPIE: Storage and Retrieval Methods and Applications for Multimedia 2004; 472-480.

Bas, P.; Filler, T.; Pevny, T. Break our steganographic system: The ins and outs of organizing BOSS. *In Proceedings of the International Workshop on Information Hiding, Prague, Czech Republic* **2011**, 59–70.

Gloe, T.; Bohme, R. The Dresden image database for benchmarking digital image forensics. *In Proceedings of the ACM Symposium on Applied Computing, Sierre, Switzerland* **2010**, 1584–1590.

Dang-Nguyen, D.T.; Pasquini, C.; Conotter, V.; Boato, G. RAISE: A raw images dataset for digital image forensics. In Proceedings of the ACM Multimedia Systems Conference, Portland, OR, USA, 18–20 March 2015; pp. 219–224.

IEEE IFS-TC. IEEE IFS-TC Image Forensics Challenge Dataset. 2014. Available online: http://ifc.recod.ic.unicamp.br/fc.website/ index.py (accessed on 2 August 2021).

Lin, T.; Maire, M.; Belongie, S.; Hays, J.; Perona, P.; Ramanan, D.; Dollár, P.; Zitnick, C.L. Microsoft COCO: Common objects in context. In Proceedings of the European Conference on Computer Vision, Zurich, Switzerland, 6–12 September 2014; pp. 740–755.

NRCS, U: 'Natural resources conservation service photo gallery, United States department of agriculture', 2014. Available at http://plants.usda.gov/

Yang, J.; Ruan, D.; Huang, J.; Kang, X.; and Shi, Y. An embedding cost learning framework using gan. *IEEE Transactions on Information Forensics and Security* **2020**, 15, 839–851.

Tang, W.; Tan, S.; Li, B.; Huang, J. Automatic stenographic distortion learning using a generative adversarial network. *IEEE Signal Processing Letters* **2017**, 24, 1547–1551.

Fan, W.; Wang K., Cayre, F. General-purpose image forensics using patch likelihood under image statistical models. In Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS'15) **2015**, 1–6.

Peng, A.; Deng, K.; Luo, S.; and Zeng, H. Multi-Purpose Forensics of Image Manipulations Using Residual-Based Feature. *Cmc-computers materials & continua* **2020**, 65(3), 2217-2231.

Liao, x.; li, k. zhu, x.; ray liu, k. j. robust detection of image operator chain with two-stream convolutional neural network. *ieee journal of selected topics in signal processing* **2020**, 14.

Tang, H.; Rongrong, N.; Yao, Z; Xiaolong L. Detection of various image operations based on CNN. In *2017 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)* **2017**, 1479-1485.

Boroumand, M.; Fridrich, F. Deep learning for detecting processing history of images. *Society for Imaging Science and Technology* **2018**.

Anitruddha, M.; Singh, J.; Tomar, Y. S.; Bora. P. K. Universal image manipulation detection using deep siamese convolutional neural network. *arXiv preprint arXiv:1808.06323* (**2018**).

Chen, Y.; Xiangui, K.; Yun, Q. S.; Wang, Z. J. A multi-purpose image forensic method using densely connected convolutional neural networks. *Journal of Real-Time Image Processing* **2019**, 16, 725-740.

Huang, G.; Liu, Z.; Maaten, L.; Weinberger, K.Q. densely connected convolutional networks. *In: Proc. IEEE Conf. on computer vision and pattern recognition, Hawaii, USA*, 2017, 77–86.

Singhal, D.; Gupta, A.; Tripathi, A.; Kothari, R. CNN-based multiple manipulation detector using frequency domain features of image residuals. *ACM Transactions on Intelligent Systems and Technology (TIST)* **2020**, *11*, 1-26.

Camacho, I.C.; Wang, K. A simple and effective initialization of CNN for forensics of image processing operations. *In Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, Paris, France*, **2019**, 73, 107–112

Glorot, X.; Bengio, Y. Understanding the difficulty of training deep feed-forward neural networks. *In Proceedings of the International Conference on Artificial Intelligence and Statistics, Sardinia, Italy* **2010**, 249–256.

Camacho, I.C.; Wang, K. Data-dependent scaling of CNN's first layer for improved image manipulation detection. *In Proceedings of the International Workshop on Digital-forensics and Watermarking, New York, NY, USA* **2020**, 1–15.

Watkins, C. J. C. H. Learning from delayed rewards. 1989.

IEEE Signal Processing Society. IEEE's Signal Processing Society—Camera Model Identification Competition. 2018. Available online: https://www.kaggle.com/c/sp-society-camera-model-identification (accessed on 2 August 2021).

Ali, S. S., Iyyakutti, I. G.; Ngoc-Son, V.; Syed, D. A.; Neetesh, S.; and Naoufel W. Image forgery detection using deep learning by recompressing images. *Electronics 2022,* vol.11, no. 3.

Rana, K.; Gurinder, S.; and Puneet, G. MSRD-CNN: Multi-Scale Residual Deep CNN for General-Purpose Image Manipulation Detection. *IEEE Access* 10 (2022), 41267-41275.

Aminu, A. A.; Nwojo, N. A.; Steve, A. and Muhammed, K. A. Detection of image manipulation with convolutional neural network and local feature descriptors. *TELKOMNIKA (Telecommunication Computing Electronics and Control)* 2022, vol. 20, no. 3, 629-637