Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: an evaluation

Preeti Sharma 1 · Manoj Kumar 2 · Hitesh Sharma 1

Received: 28 March 2022 / Revised: 31 May 2022 / Accepted: 5 September 2022 / Published online: 1 October 2022
© Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
The digital image proves critical evidence in the fields like forensic investigation, criminal investigation, intelligence systems, medical imaging, insurance claims, and journalism to name a few. Images are an authentic source of information on the internet and social media. But, using easily available software or editing tools such as Photoshop, Corel Paint Shop, PhotoScape, PhotoPlus, GIMP, Pixelmator, etc. images can be altered or utilized maliciously for personal benefits. Various active, passive and other new deep learning technology like GAN approaches have made photo-realistic images difficult to distinguish from real images. Digital image tamper detection now focuses on determining the authenticity and consistency of digital photos. The major research problems use generic solutions and strategies, such as standardized data sets, benchmarks, evaluation criteria and generalized approaches. This paper overviews the evaluation of various image tamper detection methods. A brief discussion of image datasets and a comparative study of image criminological (forensic) methods are included in this paper. Furthermore, recently developed deep learning techniques along with their limitations have also been addressed. This study aims to comprehensively analyze image forgery detection methods using conventional and advanced deep learning approaches.

Keywords Digital image forensics · GAN · Copy-move forgery detection · Data-driven methods · Image splicing · Deep learning-based detection techniques

© Manoj Kumar
wss.manojkumar@gmail.com

Preeti Sharma
preetiii.kashyup@gmail.com

Hitesh Sharma
hksharma@ddn.upes.ac.in

1 School of Computer Science, University of Petroleum and Energy Studies (UPES), Dehradun 248007, India
2 Faculty of Engineering and Information Sciences, University of Wollongong in Dubai, Dubai Knowledge Park, Dubai, United Arab Emirates
1 Introduction

Digital image forgery is a very challenging domain that deals with the tempering and manipulation of digital images. It has become a major concern for the whole society. Merriam-Webster described it as “falsely and fraudulently changing a digital picture,” an idea that dates back to 1840. It reproduces images with different parameter values [65]. Serious cases of image forgery are increasing, and this alarms the law and order systems of the world [30]. There are numerous image editing, enhancing, correction, modification, and recreation tools readily available, which encourages the commission of criminal acts.

In fields like forensic investigation, criminal investigation, intelligence systems, medical imaging, insurance claims, and journalism, digital images become critical evidence. This emphasizes the importance of maintaining and detecting the image’s authenticity. As a result, image forgery detection techniques are gaining concern and importance in society [11]. Two incidences of image forgery are discussed in Figs. 1 [90] and 2 [7] and are included here to describe the severity of the issue (Fig. 2).

The incidence listed in Fig. 1 is result of a deep learning-based technology called Deepfakes. It is a latest technology that uses GAN (Generative Adversarial Networks) for making fake images/videos by exchanging one person’s face with another. Forged faces and videos are extensively disseminated on the Internet, moral, societal, and security issues (such as fake news and fraud) may occur. Face manipulation can be accomplished through (i) full face synthesis, (ii) identity exchange, (iii) attribute manipulation, and (iv) expression. GANs are unsupervised generative models that learn the data distribution which are built up of two neural networks, one trained to generate data and the other to distinguish fake from genuine data (thus the “adversarial” element of the model). As new forms of GANs arise at an increasing rate, forensics models’ capacity to recognise new types of forged images is growing more difficult. The ultimate requirement of forensics model generalisation ability is investigated in this paper. When they are required to work with unknown sources/datasets, however, their performance suffers. This problem necessitates the development of a general face forgery detection model that is independent of the software used. The field of digital forensics research is finally focusing on solving more generic problems. As a result, it appears that universal solutions and strategies, such as the creation of

![Fig. 1](image1.png)  
Fig. 1 The doctored image depicting Jeffrey Wong Su En while receiving the award from Queen Elizabeth II, published in Malaysian dailies, and the original picture of Ross Brawn receiving the Order of the British Empire from the Queen (b)
standardized data sets, benchmarks, and evaluation criteria, will be presented in order to achieve the new frameworks while reducing the risk of digital forgeries.

Studies on image forgery suggest that crimes of this nature are mostly done to (1) circulate misleading/false information, (2) gain political influence, and (3) generate unethical publicity and advantages. The propagation of incorrect information needs to be stopped, or some solution is urgently required to address it. Image forensic is a field of digital forensic that deals with image forgery detection and validation. It is an emerging field that seeks to establish the origin and validity of digital media. It works for the detection of the originality of images or videos so that major ramifications on a national and worldwide level due to forgery can be controlled. Digital image forensic ensures the integrity and validity of enormous amounts of data before using them in a variety of circumstances, such as courts of law, forensic, social media, medical fields, etc. that are becoming increasingly vital. It provides techniques divided into two main classes of image forgery detection: a. active image forgery or non-blind image forgery detection; and b. passive or blind image forgery detection, as shown in Fig. 3.

The active class of forgery detection uses two techniques: digital signature and digital watermarking. These approaches require some prior picture information, which could have been embedded in the image at the moment of capture, during image acquisition, or at a later point. In practice, photos created for forensic investigation, such as fingerprint photos, criminal

Fig. 2 A photo from a 2014 art project in Germany that was shared on Facebook in 2020 to falsely claim that the people in the photo were Chinese coronavirus victims

Fig. 3 Active and Passive Techniques for image forgery detection
photos, crime scene photos, and so on, are very unlikely to have a watermark or signature. As a result, active forgery detection techniques have proven to be very useful for forensic examination of digital images. These are not very useful for forensic investigation of digital images. On the other hand, passive forgery detection doesn’t require any pre-embedded information about the image. It works by detecting intrinsic aspects of the image based on the sort of doctoring or identification of the source of the image. This work provides almost a complete guidance of all traditional and modern techniques of forgery detection discussed by different authors. It gives an idea about image forgery, its types, techniques, available datasets, applications, limitations, and its advancement to deep learning at present. This paper provides a good foundation for new researchers to start in this domain and also, the findings discussed as part of the conclusion at the end of the paper would become promising areas of futuristic research.

The remaining section of this review study discusses the classification of active image forgery detection techniques in Section 2. Section 3 discusses the classification of passive forgery detection techniques and comparative studies of the work done in this field, starting from conventional approaches towards current deep learning approaches. In Section 4, details about popularly used image forgery datasets and the limitations of existing deep learning-based approaches are also discussed. Section 5 presents new emerging deep learning-based methods that are currently used in the field of image forensics and the discussion section shows the impact of the study in broader way is included in Section 6 and finally, the conclusion is presented in Section 7.

2 Classification of active image forgery detection

Active image forgery detection involves two major approaches digital watermarking and signatures. These are two techniques used in active forensic techniques to inject legitimate information into images. When there is a doubt regarding the validity of a picture, the embedded authentication information is retrieved to establish the image’s authenticity [7]. It is followed by the limitation of multiple processing steps of digital images. Digital Watermarking and Digital Signature are two basic methods used for Active Image Forgery Detection.

2.1 Digital watermarking

To identify the watermark, apply to pixel data the maximum length of the linear shift register sequence and compute the sequence’s spatial cross-correlation function as well as the picture that is watermarked [61]. This information is added or attached with dynamic picture validation that ensures a validation code at the time the image is produced or transferred. However, fake image capturing or processing tools can alter this information. When a fake photograph resembling an original image is recreated using image editing tools, it either lacks this information or else contains it. Ferrara et al. [24] projected a new forensic tool centered on the interpolation procedure for assessing the original image and forged portions. During forgery detection, the conditional co-occurrence probability matrix (CCPM) is used for detecting third-order statistical features that can also be used to detect picture splicing. Li et al. [56] devised a new method for the detection of copy-move forgeries in which the circular blocks were extracted using the Local Binary Pattern (LBP). It is claimed here that detecting
forgery at different angles of the rotated region is extremely challenging. Hussain et al. [37] proposed a multiresolution Weber Local Descriptors (WLD) method for detecting picture forgeries based on chrominance component characteristics. To identify forgeries, the Support Vector Machine (SVM) classifier and the WLD histogram components are used.

### 2.2 Digital signature

One of the most common ways to detect picture forgery or manipulation is through digital signatures. A digital signature is used to represent the validity of a digital document using a mathematical structure. This is an owner and application-specific utility that embeds authentic user and device information.

This information is added or attached with dynamic picture validation that ensures a validation code at the time the image is produced or transferred. A robust bit is taken from the original picture in the digital signature. A 16*16 pixel block is used to divide a picture. Random matrices of size N with elements evenly divided in the interval [0, 1] are generated using a secret key k. Every random matrix is subjected to a low pass filter regularly to N random smooth patterns. By applying the signing procedure to a digital picture, the system generates a digital signature.

The following are the qualities of a digital signature:

- It is only the sender who can sign the original image and the recipient who can only confirm that signature.
- The signature cannot be falsified by unauthenticated users.
- It provides integrity and avoids

Doke et al. [20] proposed a low phase filter method for acquiring an X random pattern for each random matrix recurrently. Through the signing operation on the image, the model generates a digital signature. The following phases are included in the image signing operation:

- Images are decomposed using parameterized wavelet features.
- Remove the standard digital signature.\`
- Cryptographically, the crypto signature is produced by using the private key and hashing the extracted standard digital signature.\`
- The client receives digital images as well as a cryptographic signature.

Ginesu et al. [31] presented a novel mutual image-based authentication framework. It is a challenge-response scheme that uses a visual password and image scrambling. The software’s application window is divided into k grids, each with h cells. Throughout the user must correctly identify images to pass the image/s selection procedure the k pass image/s chosen at random from the N JPEG images database.

### 3 Experimentation

This section discusses about classification of Passive Image Forgery Detection. It is the most evolving detection scheme that deals with image forgery these days. Picture forensics, also known as passive or blind image forensics, is a method of determining image authenticity and
source without depending on pre-extraction or pre-embedded data [116]. It includes five methods: Pixel-based detection, Format-based detect physical-based detection, Camera-based detection, and Geometry-based detection. These methods further include several detection techniques shown in Figs. 4 and 5.

These are the popular image tampering tricks (device-independent) used to modify/recreate an image for accomplishing evil/criminal intention [15]. Different image processing tools are used to serve the purpose. Passive processes are given into shape with one or more images. The fake image thus produced, although looks authentic, contains intricate traces of inconsistencies, such as overlapping loss of information, distortions, and other artifact fingerprints as clues for Image Forensics.

3.1 Pixel based forgery detection

Pixel-based classification is performed on a pixel-by-pixel basis, using only the spectral information available for that specific pixel. Pixel-based techniques are frequently used to extract low-level features, where the image is classified based on spectral information, and pixels in the overlapping region are misclassified due to class confusion. Copy-move, Image splicing, Image resampling, and Image retouching are major classes of pixel-based forgeries. Various methods for their detection are devised in many previous types of research and are still a hot research area especially using Deep Learning Approaches.

3.1.1 Copy and move based methods

It is one of the most common image tampering techniques, and it’s also one of the most difficult to spot because the cloned image is taken from the same image. A section of an image is copied and pasted to another part of the same picture in Copy-Move image forgery [2]. It consists of two attacks: class-1 copy-move forgery and class 2 copy and creates a forgery. Figure 6a and 6b show an example of class 1 and class 2 attacks [30, 37]. The methods deployed for Copy-Move forgery detections are block-based and key point-based listed below [2].

![Digital Forensic](image)

**Fig. 4** Passive image forgery detection techniques
This technique is frequently used as a process of evil intended image manipulation to change the image message or conceal its portion(s) with the help of another image(s)/digital effects. Image editing features, such as copy, move, duplicate, clone, image merging, and filters are used.

Fig. 5 Classification of various methods of image forgery detection techniques

Fig. 6 a: Copy-Move image forgery (Class-1 type). b: Copy-Create image forgery (Class-2 type)
As a result, the fake image bears distinctive traces of distortion, digital correction, overlapping, and other enhancing effects. Also, the size and shape of the doctored portion can be analyzed to record the image forgery. Lu et al. [60] proposed a new scheme that makes use of the circular domain coverage (ECDC) algorithm. The proposed scheme combines forgery detection methods based on blocks and key points. First, from an entire image, speed-up robust features (SURF) in log-polar space and scale-invariant feature transform (SIFT) are extracted. Second, generalized two nearest neighbors (g2NN) are used to generate a large number of matched pairs. To detect tampered regions Popescu et al. [80] worked upon principal components analysis (PCA) as a feature. Yao et al. [114] detect copy-move forgery using non-negative matrix Factorization. Non-negative matrix factorization (NMF) coefficients are extracted from a list of all blocks after the image is partitioned into fixed-size overlapped blocks. It is worth mentioning that all of the coefficients are quantized before matching, which means that a sub-image can be interpreted with a small amount of data. Rani et al. [85]. This research proposes a pixel-based forgery detection framework for copy-move and splicing-based forgeries. Initially, image data is pre-processed to improve the textural information. For the identification of bogus picture regions, the suggested method estimates multiple attributes using augmented SURF and template matching. The estimated key parameters are compared to the determined threshold value. The CASIA forged picture dataset is used in the evaluation. The upgraded SURF approach has a forgery detection accuracy of 97%, while template matching has a fraud detection accuracy of 100%.

3.1.2 Image-retouching forgery detection methods

It is a very useful approach in magazines and photography in films. Although such modifications are to beautify the image and hence not counted for forging. But we are including it here as it includes changes/manipulations with the originality of the image. The image is upgraded to beautify it, and only particular parts are altered (like removing wrinkles) to produce the final shot. In Fig. 7a, part shows the retouched image while (b) part shows the original image.

These are common enhancement techniques that are comparatively harmless and considered less malicious than other forgery methods. Such manipulations are done using good photo retouching tools to correct or improve a whole image or its portion. They are commonly used as accepted image editing tools in print/web media. Fine retouching works, such as ton

![Fig. 7 a Retouched image and b original image](image-url)
correction, saturation, sharpness, or noise corrections, are so precise that such variations cannot be identified unless checked using sophisticated tools. Xing et al. [111] describe a new algorithm based on an 8-neighborhood quick sweeping technique. The experimental result shows that there is a significant increase in the rate of the image inpainting while maintaining-quality effect. Sundaram et al. [111] presented a review consisting of methods by Wang et al. proposed a universal picture construction in which three critical parameters, such as Area, Shape, and Perimeter, are presented (ASP). Then, by the ASP principles, a Pyramid model based on downsampling in painting (PDI) was presented. The results of the experiments show that by incorporating the PDI model, the performance of existing techniques can be drastically improved. In addition, according to a paper by Bo et al., an image inpainting technique based on a self-organizing map (SOM) is used to find the useful structure information of a ruined image. Kumar et al. [50] examined different pixel- and physics-based counterfeit detection algorithms, as well as a comparative examination of these techniques. Furthermore, imaging devices and processing procedures, no matter how varied they are, contain a constant pattern in the image that, if interfered with, will introduce a departure from the original pattern. This divergence allows one to detect image counterfeiting. It has more accurate forgery detection and has more homogeneous lit surfaces. Some of the methods can be referred from [43, 66].

3.1.3 Image splicing or photomontage forgery detection methods

It is a frequent kind of digital image alteration. Image splicing, often known as image composition, is one kind of tampering. Image splicing is defined as a technique that copies and pastes areas from identical or distinct sources [30]. With this method, an image is recreated/transformed by merging many image(s). The method is also known as image composition in which primary information of each image used in splicing is lost/distorted/damaged as shown in Fig. 8.

The spiciness has two broad classifications and that are (1) Boundary-based Splicing and (2) Region-based Splicing. Forensics approaches are used to identify the tampering tools as well as the nature/regions of distortions present in these fake images. Fan et al. [23] estimate the illuminance of each horizontal and vertical band; they proposed combining five low-level statistics-based algorithms. Based on local illumination estimation, inconsistencies in the illuminant color in the object region were used to detect region splicing frauds. Lyu et al.

Fig. 8 Image splicing forgery
use of local noise inconsistencies to detect small regions damaged by local noise is presented as a blind forgery detection approach. The approach employs non-overlapping blocks and high pass diagonal wavelet coefficients at the highest resolution. To detect spliced forgery, the image was segmented based on homogeneity criterion into many homogeneous sub-regions using a basic area merging technique. The approaches work well on images with uniform noise levels, but they fail when the verified image has the same. Pan et al. [74] make use of local noise inconsistencies to detect small regions damaged by local noise is presented as a blind forgery detection approach. The approach employs non-overlapping blocks and high pass diagonal wavelet coefficients at the highest resolution. To detect spliced forgery, the image was segmented based on homogeneity criterion into many homogeneous sub-regions using a basic area merging technique. The approaches work well on images with uniform noise levels, but they fail when the verified image has the same.

3.1.4 Image resampling forgery detection

It is based on the concept that geometric modifications like stretching, flipping, skewing, rotation scaling, etc. are made to some particular sections in need to generate an amazing forged image. The interpolation stage is crucial in the resampling process since it introduces significant statistical changes. The picture is resampled, which introduces unique periodic correlations. These connections can be put to good use [42]. Figure 9 shows an example of the image resampling method [82]. Wang et al. [111] represented that supervised learning is a powerful and universal approach to deal with the twin challenges of unknown picture statistics and unknown stenographic codes. A pivotal piece of the learning procedure is the determination of low-dimensional instructive features. Liu et al. [57] studied the relationship between surrounding Discrete Cosine Transform (DCT) coefficients and suggested a method for detecting enlarged JPEG images and spliced images, both of which are commonly exploited in photo counterfeiting. The neighboring joint density features of the DCT coefficients are extracted in detail, and the features are then detected using Support Vector Machines (SVM) (Tables 1, 2, 3, 4 and 5).

Fig. 9 Image resampling forgery
| Type of Forgery Detection Area                                                                 | Researchers          | Year | Approach                                                                 | Dataset                              | Performance            |
|------------------------------------------------------------------------------------------------|----------------------|------|--------------------------------------------------------------------------|--------------------------------------|------------------------|
| Detection of copy move and splicing.                                                            | Rao et al. [86]      | 2016 | CNN - SVM                                                                | CASIA, Columbia Gray.                | Accuracy 97.8%         |
|                                                                                                 |                      |      | Input Feature: Pixel values                                              |                                      |                        |
|                                                                                                 |                      |      | Input Size: 128 × 128                                                    |                                      |                        |
|                                                                                                 |                      |      | 1st initialization layer SRM filters                                     |                                      |                        |
|                                                                                                 |                      |      | Location: pixel                                                          |                                      |                        |
| Image splicing localization using a multi-task fully convolutional network.                      | Salloum et al. [91] | 2018 | FCN                                                                      | Ad-hoc, CASIA, Carvalho, Columbia Gray, NIST. | F1 score: 7.9/54.1     |
|                                                                                                 |                      |      | Input Feature: Pixel values                                              |                                      |                        |
|                                                                                                 |                      |      | Input Size: 224 × 224                                                    |                                      |                        |
| Copy-move forgery detection with convolutional kernel network.                                  | Liu et al. [58]      | 2017 | Input Feature: Key points                                               | Ad-hoc, CoMoFoD, ROME patches.       | Accuracy 97.1          |
|                                                                                                 |                      |      | Input Size: 51 × 51                                                      |                                      |                        |
|                                                                                                 |                      |      | Background Architecture: VGG-16                                          |                                      |                        |
|                                                                                                 |                      |      | Location: pixel                                                          |                                      |                        |
| Busternet: Detecting copy-move image forgery with source/target localization.                  | Wu et al. [109]      | 2018 | Input Feature: Pixel values                                              | Ad-hoc, CASIA, MS COCO, CoMoFoD, SUN 2012. | F1 score: 49.3 / 45.6 |
|                                                                                                 |                      |      | Input Size: 256 × 256                                                    |                                      |                        |
|                                                                                                 |                      |      | Background Architecture: VGG-16                                          |                                      |                        |
|                                                                                                 |                      |      | Location: pixel                                                          |                                      |                        |
| Image splice detection via learned self-consistency.                                            | Huh et al. [36]      | 2018 | CNN                                                                      | ad-hoc, Carvalho, Columbia Gray, Realistic (Korus), On-the-wild websites. | MAP 51.0               |
|                                                                                                 |                      |      | Input Feature: EXIF metadata, pixel values                              |                                      |                        |
|                                                                                                 |                      |      | Input Size: 128 × 128                                                    |                                      |                        |
|                                                                                                 |                      |      | Background Architecture: ResNet-v2                                      |                                      |                        |
| Patch-based image inpainting forensics.                                                         | Zhu et al. [88]      | 2018 | Input Feature: High-pass residuals                                       | MIT Place, Ad-hoc.                   | MAP 97.8               |
|                                                                                                 |                      |      | Input Size: 256 × 256                                                    |                                      |                        |
|                                                                                                 |                      |      | Background Architecture: Own                                             |                                      |                        |
|                                                                                                 |                      |      | Location: pixel                                                          |                                      |                        |
|                                                                                                 | Bappy et al. [3]     | 2019 | LSTM                                                                     | IEEE Forensics Challenge, Coverage, Ad-hoc. | Accuracy 94.8 (NIST)  |
| Type of Forgery Detection Area                                                                 | Researchers          | Year | Approach                                                                 | Dataset                      | Performance                             |
|------------------------------------------------------------------------------------------------|----------------------|------|--------------------------------------------------------------------------|------------------------------|-----------------------------------------|
| Image Forgeries Detection with A.K. Hybrid LSTM and encoder–decoder architecture.             | Wu et al. [110]      | 2019 | Multi-branch                                                             | Dresden, Columbia colour, Carvalho, ad-hoc, CASIA, NIST, Coverage. | Accuracy 81.7 (CASIA), 79.5 (NIST)       |
| Detection of image forgeries with anomalous features with Manipulation tracing network.        | Wu et al. [110]      | 2019 | Multi-branch                                                             | Dresden, Columbia colour, Carvalho, ad-hoc, CASIA, NIST, Coverage. | Accuracy 81.7 (CASIA), 79.5 (NIST)       |
| Image inpainting detection based on multi-task deep learning network.                          | Wang et al. [106]    | 2020 | High-pass residuals                                                      | Ad-hoc, MS COCO, ImageNet.   | MAP 97.8                               |
| LSTM-CNN-based detection technique for object removal caused by exemplar-based image inpainting.| Lu et al. [59]       | 2020 | Pixel values                                                             | UCID, Ad-hoc.                | Accuracy 93.6                          |
| Super Pixel Segmentation and Hybrid Feature Point Mapping for Digital Image Forgery Detection  | Reddy [87]           | 2021 | ResNet (CNN Based), SIFT, SURF                                          | Ad-hoc                      | More Robust than conventional methods.  |
| Type of Forgery Detection Area | Researchers | Year | Approach | Dataset | Performance |
|-------------------------------|-------------|------|----------|---------|-------------|
| Detection of Double JPEG compression. | Morgand et al. [67] | 2016 | Special CNN Design: Customized 3x1 kernels Network Depth: 2C-2F Input Feature: DCT features Input Size: 64x64, 128x128, ..., 1024x1024 | UCID | Accuracy: 100.00% |
| Detect tampered images in different image formats. | Zhang et al. [117] | 2016 | Stacked Auto encoder model (SAE) (3 layers) Input Feature: DCT, Image Patch (Colour Space) Input Size: 32x32 | CASIA | Accuracy: 91.09% (Overall Both For JPEG, TIFF) Fall-out: 4.31% Precision: 57.67% Accuracy: 96.30 |
| Aligned and non-aligned double JPEG detection with CNN. | Barni et al. [4] | 2017 | Special CNN Design: N/A Network Depth: 3C-2F Input Feature: Noise residuals or DCT features Input Size: 64x64, 256x256 | RAISE | Accuracy: 99.60 |
| Localization of JPEG double compression with multi-domain CNN | I. Amerini et al. [1] | 2017 | Special CNN Design: Two-branch CNN Network Depth: 2C-2F, 3C-1F Input Feature: DCT features, pixel values Input Size: 64x64 | UCID | Accuracy: 99.48 |
| Detection of Multiple JPEG compression classification with DCT-domain deep convolutional neural networks | Verma et al. [105] | 2018 | Special CNN Design: N/A Network Depth: 4C-3F Input Feature: DCT features Input Size: 128x128 | UCID | Accuracy: 99.48 |
| Double JPEG detection in mixed JPEG quality factors with deep convolutional neural network | Park et al. [75] | 2018 | Special CNN Design: Two-branch CNN Network Depth: 4C-3F, 3F Input Feature: DCT features, quantization tables Input Size: 256x256 | Ad-hoc | Accuracy: 92.76 |
| Double JPEG Compression Detection Based on Noise-Free DCT Coefficients Mixture Histogram Model. | Zhu et al. [119] | 2019 | Special CNN Design: Two-branch R-CNN Network: ResNet 101 network Input Feature: RGB Images, SRM Images Input Size: 8x8, 16x16, 32x32, 64x64 | NIST Nimble 2016 (NIST16), CASIA, COVER, Columbia | F1 Score: NIST16: 0.722 Columbia: 0.697 COVER: 0.437 |
| Type of Forgery Detection Area | Researchers | Year | Approach | Dataset | Performance |
|-------------------------------|-------------|------|----------|---------|-------------|
| Improving Robustness of Image Tampering Detection for Compression | Diallo et al. [17] | 2020 | Special CNN Design: N/A Network Layers: 11 Input Feature: Image Patches, discriminant features Input Size: 64×64 | Dresden | CASIA: 0.408 Accuracy - NIST16: 0.937 Columbia: 0.858 COVER: 0.817 CASIA: 0.795 Known: Accuracy 0.77 TPR 0.68 Unknown: Accuracy 0.63 TPR 0.46 |
| Error Level Analysis for Lossless Image Compression Based Forgery Detection | Sri et al. [97] | 2021 | Network Depth: 3C-2F Input Feature: Noise residuals or DCT features Input Size: 64×64, 256×256 | MICC-F2000, CASIA v2 | Accuracy: 0.99% with both datasets. |
| Type of Forgery Detection Area                                      | Researchers        | Year | Approach                                      | Dataset          | Performance (Camera Model: Efficiency of CNN) |
|-------------------------------------------------------------------|--------------------|------|-----------------------------------------------|------------------|-----------------------------------------------|
| Camera model identification with CNN                              | Tuama et al. [103] | 2016 | CNN                                          | Dresden          | 12:98                                         |
|                                                                  |                    |      | Input Features: High-pass residuals           |                  |                                               |
|                                                                  |                    |      | Initialization: Random init.                 |                  |                                               |
|                                                                  |                    |      | Input Size: 256×256                          |                  |                                               |
| Camera model identification with deep CNN                         | Bondi et al. [6]   | 2016 | CNN – SVN                                     | Ad-hoc, Dresden  | 18:93                                         |
|                                                                  |                    |      | Input Features: Pixel values                 |                  |                                               |
|                                                                  |                    |      | Initialization: Random init.                 |                  |                                               |
|                                                                  |                    |      | Input Size: 64×64                            |                  |                                               |
| Computer Generated Images with Deep Convolutional Neural Networks | Rezende et al. [14]| 2017 | CNN-SVM                                      | ImageNet, Tokuda | Accuracy: 94.1                                |
|                                                                  |                    |      | Input Size: 224×224                          |                  |                                               |
| Photorealistic Computer Graphics Detection using Convolutional Neural Networks | He et al. [35]     | 2017 | CNN                                          | ad-hoc, Columbia CGI, Web images | Accuracy: 98.0 |
|                                                                  |                    |      | Backbone Architecture: ResNet-50            |                  |                                               |
| Detecting forged images and videos with Capsule-forensics        | Nguyen et al. [71] | 2017 | Capsule                                      | MeszoNet, FaceForensics, Rahmouni | Accuracy: 97.0 |
|                                                                  |                    |      | Backbone Architecture: VGG-16               |                  |                                               |
|                                                                  |                    |      | Input Size: 128×128                          |                  |                                               |
| Source Camera Identification on Mobile Devices                   | Obregón et al. [25]| 2019 | CNN-SVM                                      | MICHE-I          | 3:91.1                                        |
|                                                                  |                    |      | Input Features: Pixel values                 |                  |                                               |
|                                                                  |                    |      | Initialization: Random init.                 |                  |                                               |
|                                                                  |                    |      | Input Size: 32×32                            |                  |                                               |
| Camera Model Fingerprint Detection                                | Cozzolino et al. [12]| 2019| Siamese                                      | ad-hoc dataset   | 3:100.0                                       |
|                                                                  |                    |      | Input Features: Pixel values                 |                  |                                               |
|                                                                  |                    |      | Initialization: Random init.                 |                  |                                               |
|                                                                  |                    |      | Input Size: 32×32                            |                  |                                               |
| Camera identification with domain knowledge-driven deep multi-task learning | Ding et al. [18]  | 2019 | Multi-scale CNN                              | Vision, ad-hoc   | 14:97.1                                       |
|                                                                  |                    |      | Input Features: High-pass residuals          |                  |                                               |
|                                                                  |                    |      | Initialization: Random init.                 |                  |                                               |
|                                                                  |                    |      | Input Size: 48×48                            |                  |                                               |
| Limited Labels Classification in Source Camera identification with | Roy et al. [89]    | 2020 | Siamese                                      | Vision (2)       | 10:87.3                                       |
|                                                                  |                    |      | Input Features: Pixel values                 |                  |                                               |
| Type of Forgery Detection Area | Researchers | Year | Approach | Dataset | Performance (Camera Model: Efficiency of CNN) |
|-------------------------------|-------------|------|----------|---------|---------------------------------------------|
| Deep Siamese Network          | Zhang et al. [118] | 2020 | Initialization: Random init. Input Size: 64×64 CNN | ad-hoc | Accuracy 94.2 |
| Locating Difference of Photorealistic Computer Generated Images and Photographic Images. | Gardella et al. [28] | 2021 | Quantisation of DCT coefficient for JPEG compression applied in 8×8 blocks. (Noise based method using Complex camera Processing chain.) | CG-1050 | MCC score for Retouching (0.0915), Colorization (0.1108) and splicing (0.0362) |
| Type of Forgery Detection Area                                                                 | Researchers             | Year | Approach                                                                                                                                  | Dataset            | Accuracy (%)/Performance |
|------------------------------------------------------------------------------------------------|-------------------------|------|------------------------------------------------------------------------------------------------------------------------------------------|-------------------|--------------------------|
| Fake Colorized Image Detection with Channel-wise CNN                                           | Zhuo et al. [120]       | 2018 | TensorFlow  
Input Features: state of the art Steganographic features  
Input Value: True Colour  
Input Size: 256×256, 128×128, and 32×32 | D1                 | Better than FCID-FE and FCID HIST                                             |
| Detection of Median filtering detection with CNN                                              | Tang et al. [101]       | 2018 | Special CNN Design: MLPCONV  
Network Depth: 2 M-3C  
Input Feature: Upscaled values  
Input Size: 64×64, 32×32 | BOSSBase, NRCS, UCID | AUC. 89.96                                |
| JPEG post-processing generic contrast adjustment with CNN                                     | Barni et al. [5]        | 2018 | Special CNN Design: N/A  
Network Depth: 9C-1F  
Input Feature: Pixel values  
Input Size: 64×64 | RAISE              | Accuracy: 92.76                                      |
| Image forensics for color illumination, block and key point based approach                   | Thakur et al. [102]     | 2018 | Hybrid  
DWT, color illumination Algorithm, SLIC Algorithm; SIFT Algorithm, Correlation Coefficient Map generation Algorithm,  
Block Matching Threshold Algorithm, Feature Extraction Algorithm | ad-hoc            | Precision: 97.25%; Recall: 100%; F1: 98.53%        |
| Contrast enhancement forensics based with convolutional neural networks                       | Sun et al. [99]         | 2018 | Special CNN Design: N/A  
Network Depth: 3C-2F  
Input Feature: GLCM  
Input Size: 256×256 | MS COCO           | TPR 99.80                                             |
| Contrast Enhancement Detection based with CNN                                                 | Shan et al. [113]       | 2019 | Special CNN Design: N/A  
Network Depth: 4C-2F  
Input Feature: GLCM  
Input Size: 256×256 | BOSSBASE           | AUC 99.40                                             |
| Image Level Forgery Identification, Pixel Level Forgery Localization with CNN                 | Deng et al. [16]        | 2019 | VGG-CNN  
Input Feature: Pixel values  
Initiation: Random region | Image Manipulation Dataset 1, COCO Dataset | Accuracy: 93% AUC: 79% |

Table 4 Physics-Based Image Forensics: Light Direction (2D), (3D) and Light Environment
| Type of Forgery Detection Area                  | Researchers       | Year | Approach                                                                 | Dataset   | Accuracy (%)/ Performance |
|-----------------------------------------------|-------------------|------|---------------------------------------------------------------------------|-----------|----------------------------|
| Image processing forensics with CNN           | Camacho et al. [9] | 2020 | Input Size: 56×56 Special CNN Design: Special init. For 1st layer Network Depth: 5C-2F Input Feature: Pixel values Input Size: 256×256,64×64 | Dresden   | Accuracy: 93.71            |
| Industrial Object Detection with Physics-Based Rendering | Eversberg et al. [21] | 2021 | RCNN: with 5000 synthetic training images. Input Features: Pixel Values (8-piece batch) Input Size: 640×360 with 25 Epochs. | PASCAL, COCO | AP [0.5:0.95]: 0.642, AP[0.5]: 0.931 (Average Precision) |
| Type of Forgery Detection Area | Researchers | Year | Approach | Dataset | Accuracy (%) | Performance |
|-------------------------------|-------------|------|----------|---------|--------------|-------------|
| Recasting residual-based local descriptors with CNN | Cozzolino et al. [13] | 2017 | CNN - SVM | Ad-hoc | – | |
| Detection and localization of image forgeries using resampling features and deep learning | Bunk et al. [8] | 2017 | LSTM | NIST 16 | Accuracy: 94.9 | |
| Detection of GAN-Generated Fake Images over Social Networks | Marra et al. [64] | 2018 | Conventional and Deep Learning | ad-hoc | Accuracy: 95 | |
| Satellite Image Forgery Detection and Localization Using GAN and One-Class Classifier | Yarlagadda et al. [115] | 2018 | GAN, One Class SVN | Landsat Science program | 0.972 (Detection), 0.974 (Localization) | |
| Detecting and segmenting manipulated facial images and videos | Nguyen et al. [68] | 2019 | AE-CNN | FaceForensics, FaceForensics++ | Accuracy: 90.3, 90.4 | |
| Digital face manipulation | Hashmi et al. [34] | 2020 | CNN | ad-hoc | AUC 99.7 | |
| Classifying deepfakes - OC-FakeDect | Khalid et al. [45] | 2020 | VAE | FaceForensics++ | Accuracy: 98.2 | |
| Detection of swapped face | Ding [19] | 2020 | CNN | ad-hoc | Accuracy: 99.9 | |
| Type of Forgery Detection Area | Researchers | Year | Approach | Dataset | Accuracy (%)/Performance |
|------------------------------|-------------|------|----------|---------|--------------------------|
| Detection of handcrafted facial image manipulations as well as GAN-generated facial images. | Lee et al. [55] | 2021 | SFFNV3 (Shallow Fake Face Net) | Handcrafted Facial Manipulation (HFM) dataset | For input size: 256 X 256, F1-score: 70.18, AUC: 72.52 For input size: 128 X 128, F1-score: 66.19, AUC: 69.61 |

Background Architecture: ResNet18
Input Size: 224 X 224

Detection of handcrafted facial image manipulations as well as GAN-generated facial images. | | | | | |

Background Architecture: CNN
Input Size: 128 X 128, 256 X 256.
3.2 Compression based forgery detection

Forgery detection can be made difficult by the alteration of a forged image for compression and other purposes. Forgery detection is difficult using JPEG picture compression. JPEG stands for Joint Photographic Experts Group. However, some JPEG compression features are used in forensics analysis to detect tampering traces [79]. JPEG quantization based, double JPEG compression based, multiple JPEG compression based, and JPEG blocking based approaches are all examples of these techniques. Specific compression algorithms introduce statistical correlation, which is useful for detecting image counterfeiting. Huang [76] described a technique for detecting double JPEG compression that makes use of a quantization matrix. Kee et al. [30] described a method for determining whether or not a picture has been edited by using the camera signature of a JPEG image.

In light of the belief that when the block-wise DCT is handled in line with the primary JPEG compression grid, its coefficients will display an integer periodicity. Bianchi et al. suggested an approach for detecting non-aligned double JPEG compression. For modeling of images, Rani et al. [84] develop a steganalysis metric based on a Gaussian distribution. The distribution of DCT coefficients is modeled using a Gaussian distribution model, and a ratio of two Fourier coefficients of the distribution of DCT coefficients is quantified. This derived steganalysis metric is compared to three stenographic methods: LSB (Least Significant Bit), SSIS (Spread Spectrum Image Steganography), and the Steg-Hide tool, which is based on a graph-theoretic approach. Different classification approaches, such as SVM, are used to classify picture features datasets.

3.2.1 JPEG quantization method

The image that we will supply in JPEG (joint photographic expert group) format, in which the initial image is converted into an RGB image to brightness or chromatic space. These figures fluctuate depending on the low and high points. These JPEG compression speeds are represented by 192 values that show the channels of the RGB color system. The quantization that the DCT achieves Methods of (discrete cosine transformation) [95].

3.2.2 Double JPEG quantization and JPEG blocking method

Images must be uploaded into a program that will be used to manipulate them, and then saved again. We can infer from the fact that the vast majority of photographs are stored in JPEG encoding that only genuine images are stored in JPEG encoding. Encoding JPEG images in lossy mode results in particular patterns that do not appear in photos that are compressed in a single pass. Double JPEG compression creates patterns that can be exploited as indicators of manipulation or tampering [33, 72]. The Discrete Cosine Transform is the foundation of JPEG compression. As the JPEG image is made up of 8 × 8-pixel image blocks that have been converted and quantized independently, the patterns emerge at the boundary of nearby blocks in the form of horizontal and vertical edges. A doctored image may have these blocking patterns altered. To reduce file size in Y’CbCr color space, these JPEG blocks use a typical factor for digital image compression: 8 by 8-pixel blocks [117].
3.2.3 -based forgery detection

When we capture a photo with a digital camera, the image passes from the sensor to the memory, where it goes through a series of processing stages that include quantization, color correlation, gamma correction, white balancing, filtering, and JPEG compression. These processing phases, from image capture to image stored in memory, may vary depending on the camera model and camera antiques. These methods are based on this standard. Chromatic aberration, color filter array, camera response, and sensor noise are the four types of approaches that can be used [7]. Geradts [29] stated that if a portion of an image has a common intensity of lighting faults in pixels, they are only visible in darker or lighter areas. Because of the varying wavelengths of light, the lens bent it to different degrees. Defects in pixels are caused by temperature. A few post-processing manipulations, such as image, contrast, compression, blurring, and so on, can also help to eliminate incorrect pixels. Due to the exorbitant expense of many sensors, several manufacturers employed only one sensor to capture a natural color scene. As a result, color filter arrays (CFA) are frequently used in sensors to restrict the wavelength band that reaches the CCD array. Few projection algorithms have been proposed for full-resolution color vision reconstruction [83]. Some artifacts in cameras can be used to enhance photographs taken with conventional cameras. This type of picture forensics can be done using a variety of approaches. Typical cameras are being replaced by low-cost cameras. Images are captured in everyday life using cameras from companies such as Leica, Sony, Fujifilm, Pentax, Panasonic, Canon, Nikon, and others that use wavelengths that reach inside a CCD array.

3.2.4 Chromatic aberration

Chromatic aberration occurs from an optical system’s failure to concentrate light perfectly on different wavelengths. Lateral chromatic aberration, as an expansion/contraction of the color channels with each other, expresses itself in a first-order approximation. This aberration is often disrupted and cannot be constant in the entire image while manipulating an image [38]. One disadvantage of this method is that to obtain a global assessment of the entire image, the majority of the image must be real. On the other hand, if a large portion of the image is forged, the overall estimation of the image is wrong and may produce false findings. It also produces good results when the image is of high quality since chromatic aberration may be better modeled with high-quality photographs [69].

3.2.5 Color filter Array

A digital color image is made up of three channels, each of which contains samples from several color bands, such as red, green, and blue. The vast majority of digital cameras come with either a single charge-coupled device (CCD) or a pair of complementary charge-coupled devices (CCDs) color sensors using a metal-oxide-semiconductor (CMOS). A color filter array is used to create images (CFA) [81]. The most commonly seen Bayer array is a three-color CFA that is widely used that uses three color filters Red, Blue, and Green [104].
3.2.6 Source camera abbreviation

Digital image source identification is a type of technology that determines the picture source only based on the image itself, without any knowledge of the image creation equipment. Signal processing is used to do this. The forensic investigator can use the source camera identification to figure out what kind of camera was used to capture the image under inquiry. When digital content is presented as a silent witness, it is critical [112].

3.2.7 Sensor imperfection

Many forensic applications, such as matching an image to a specific camera, revealing malicious image manipulation and processing, and determining an approximate age of a digital photograph. Imperfections of digital imaging sensors can serve as unique identifiers, just as human fingerprints or skin blemishes. Defects caused by manufacturing flaws, physical processes occurring inside the camera, and environmental factors are among the many types of defects that forensic analysts are interested in [26].

3.3 Physics-based forgery detection

Natural images are typically taken in a variety of lighting situations. As a result, in splicing processes, the lighting of a forged zone may differ from the original (where two or more images are used to create a forged image). In physics-based approaches, light source discrepancies between certain objects in the scene are employed to reveal tampering evidence. Images are blended at the time of modification in this process, which is captured under a variety of lighting conditions. It can be difficult to match up the lighting state when using these photographs. The blended photos illumination discrepancy could be used to demonstrate the tempered areas of image counterfeiting. For the first time, Stojkovic et al. [98] proposed a solution to these problems. They devise a method for evaluating the side of a lighting source in the first degree of freedom to demonstrate the effects of tampering. Kumar et al. [53] proposed an approach that works for photographs with any sort of item present in the scene, i.e. it is not restricted to human faces and image selection of same intensity regions. The suggested technique identifies the manipulated object and returns the angle of incidence concerning the light source direction by analyzing the lighting parameters. On an image dataset composed of various sorts of modified images, the exhibited solution achieves a forgery recognition rate of 92%.

3.3.1 Light environment

It is a physics-based image forgery detection that looks for lighting anomalies in complex natural lighting. When splicing items from multiple photos, it’s tough to achieve physically constant illumination, and research demonstrates that such errors are difficult to detect with human eyes [73]. Lighting-based forensic can be categorized as simple directional lighting, 2D complex lighting and 3 D complex lighting discussed further in Light Direction (2D and 3D). The last two methods work by first recovering the lighting environment, which is represented by a group of spherical harmonics coefficients, and then comparing the coefficients estimated from different parts of the image [22]. The lighting in the scene is sophisticated, in that a large number of lights can be put in arbitrary positions, resulting in a variety of complex lighting.
situations. Nirmalkar et al. [72] explain how to estimate a low-parameter representation of such complex illumination conditions. Kumar et al. [54] suggested a strategy for detecting image alteration utilizing complicated lighting-based analysis. For photos obtained under one or more light sources, this approach yields satisfactory counterfeit detection results. We calculated elevation angles for certain objects about various light sources in the scene. The approach discovers light sources and elevation angles by using pixels from a certain location. The acquired results from the suggested technique are compared to verify the resilience to identifying tampering in synthetic images while taking precomputed and source direction into account.

3.3.2 Light direction (2D)

This method deals with the estimation of the area in which the light source’s 2D location is located. This area is referred to as the “Light Zone” (LZ). This calculation is based on the shadow area that has been calculated for the current image. Shadow segmentation is based on the previously estimated shadow area and the currently estimated Light Zone [78]. Stojkovic et al. [98] present a method for displaying the results of a fabricated part of an image that is based on a light direction anomaly. Using blind identification methods, the above method was used to estimate the picture’s plane normal matrix. Forgery detection accuracy was found to be 87.33% in this model. The approach proposed by Kumar et al. [51] detects image fraud by exploiting discrepancies in the light source direction. Initially, surface normal is generated using a surface texture profile on the input image during the preprocessing step. The RED band is primarily utilized to gather surface texture information and to perform surface normal calculations. The incidence angle $\theta_i$ is calculated for various image patches using the estimated lighting profile and normal. The $\theta_i$ angle is the estimated angle between the picture object and the direction of the light source. The inconsistency of $\theta_i$ values is utilized as proof of tampering, and it has been discovered to be capable of identifying modified items in an image.

3.3.3 Light direction (3D)

This method is based on the surface reflection model of the image which uses convexity and constant reflectance as two parameters. It detects forgery especially Face forgery by taking occlusion geometry and surface texture information into major consideration. To estimate the 3D lighting SH (spherical harmonics) coefficients, it recreates the 3D face model from some face photos and uses the 3D normal information [77]. Kee et al. [44] describe a low-dimensional model for assessing the 3-D lighting environment. It evaluates model parameters based on a single image. Fan et al. [22] focuses on lighting-related forensics. It demonstrates how to use a simple counter-forensic method to deceive a forgery detection based on 2D lighting factors. For forensics, this intermediate result supports the application of more complex 3D lighting factors. Such a study route necessitates at least a rough approximation of the suspect object’s 3D surface. Kumar et al. [49] suggested a study that demonstrates a cutting-edge forgery detection system based on lighting fingerprints available in digital photos. Any alteration of the image(s) results in distinct fingerprints, which can be used to confirm the image(s)’ integrity after the analysis. This technique employs several processes to determine the intensity and structural information. The Laplacian approach is used to extract dissimilar features from an image, which is then followed by surface normal estimation. Using this information, the light’s source direction is calculated in terms of angle $w$. By recognizing
distinct fingerprints based on illumination factors, the suggested technique offers an efficient tool for digital image forgery detection.

### 3.4 Geometric based forgery detection

Geometric constraints are used in forgery detection systems that utilize perspective views. These techniques are further divided into intrinsic camera parameters-based techniques (such as focal length, main point, aspect ratio, and skew), metric measurement-based techniques, and multiple view geometry-based techniques [52]. In real photographs, for example, the primary point (the intersection of the optical axis and the image plane) lies at the image’s center. When a small section of an image is moved or translated (copy-move example), or two or more photos are combined (splicing example), keeping the image’s main point in the correct perspective becomes problematic [27]. Johnson et al. [39] review and recommend many projective geometry tools, including a method for rectifying planar surfaces and the capacity to make real-world measurements from a planar surface. The first method makes use of polygons with well-defined shapes. The second method is based on the concept of vanishing points, which can be one or two in number on a plane. Every approach estimates the world-to-image transformation, which can be used to remove planar distortions and perform measurements.

#### 3.4.1 Camera intrinsic parameters

Scale factor, focal length, lens distortion, skew, and principal point are the intrinsic parameters of a camera. This allows mapping the camera coordinates to the pixel coordinates. This mapping is a 3D to 2D mapping and lies upon many independent parameters [100]. Internal parameters estimated from a non-tampered image should be consistent across the image. As a result, variations in these parameters across the image are used to detect tampering [107]. Ng et al. [70] review and recommend many projective geometry tools, including a method for rectifying planar surfaces and the capacity to make real-world measurements from a planar surface. The first method makes use of polygons with well-defined shapes. The second method is based on the concept of vanishing points, which can be one or two in number on a plane. Every approach estimates the world-to-image transformation, which can be used to remove planar distortions and perform measurements.

#### 3.4.2 Metric measurement

Metric measurements can be taken from a planar surface after rectifying the image. There are three methods for rectifying planar surfaces when using perspective projection. Only a single image is used by each method. The first method requires the knowledge of known-shape polygons, the second method is based on two or more vanishing points, and the third requires two or more coplanar circles that can be used to recover the image to world transformation, allowing metric measurements to be taken on the plane. Metric measurements help to detect the region of interest even if it lies out of the reference plane. [108]. Points on a plane, X, in the world coordinate system are imaged to the image plane with coordinates x, given by: \( x = HX \).

Both points are homogeneous 3-vectors in their respective reference systems. Four or more points with known coordinates X and x are required to solve for the projective transformation matrix H. The estimation of H is determined up to an unknown scale factor. This scale factor
must be determined from a single image and a known length on the world plane. The image is warped according to $H^{-1}$ with a known $H$ to produce a rectified image from which measurements can be taken. Nirmalkar et al. [72] review and recommend many projective geometry tools, including a method for rectifying planar surfaces and the capacity to make real-world measurements from a planar surface. The first method makes use of polygons with well-defined shapes. The second method is based on the concept of vanishing points, which can be one or two in number on a plane. Estimates the world-to-image transformation in each approach, allowing planar distortions to be removed and measurements to be taken.

### 3.4.3 Multi-view geometry

It is defined as a method for detecting picture composites by enforcing two-view geometrical constraints on image pairs: H and F constraints, where H denotes the planar homographic matrix and F is the fundamental matrix.

**H constraint** occurs when a camera rotates for an angle, corresponding points $x1$ and $x2$ on two image planes are related by: $x2 = K[R | 0]X = KRK^{-1}x1$.

**F Constraint** occurs when a camera moves in general and points are not coplanar. A Fundamental Matrix, F, can be used to connect them using a point $x1$ on one image to a line $l1$ on the other represented as $x2Tl1 = x2TFx1$ where $x2$ corresponds to $x1$ [68].

### 4 Limitations of existing deep learning-based approaches and different open-access forensic datasets

There are certainly major issues where the deep learning approaches are also struggling hard and that can become the base for future research:-.

#### 4.1 Lack of optimal model of image forgery model

Most of the models suffer from cumbersome algorithms fitted with wrong classifiers. Such frameworks lead to poor/faulty performance. Choice of the dataset (or its unavailability) is also a criterion where the models suffer. Overall, a faulty image forgery detection model is often seen to fail due to extra time consumption and expensiveness. Moreover, procedures in Deep learning Image Forgery Detection vary a lot from one another, in terms of pre-processing, training, and human decision analytical phase.

#### 4.2 Lack of accuracy of automated forgery prediction

Even today, this aspect is still chiefly dependent on the classifiers. They often perform poorly in case of detecting intricate forgeries, such as Deep Fakes. Selection of initiation mode and detection location (pixel/region) become incompatible with one another during the analysis phase. Thus, automation for this phase cannot be ideally achieved. Rather, in almost every case they need an expert to intervene in the process.
4.3 Lack of availability of deep learning-based good tools

It is found that Deep Learning-Based Image Forgery Detections work efficiently only in limited areas, such as device detection, copy-moving detection, etc. Moreover, the experimental results are heavily dependent on dataset selection and utilization.

4.4 Lack of cost-effectiveness

Most of the mechanisms as categorized in the study are costly due to the inclusions of classifiers, high-end training algorithms, and computational issues. In Image Forensics, the existing dataset plays a major role for model training and development purposes. There are different types of datasets available to accompany these analyses, such as Dataset of original information, such as UCID dataset, RAISE dataset, Vision Dataset, etc. Dataset of Manipulated information, such as CASIA V1, CASIA V2 dataset, MICC-F220 dataset, etc. as shown in Table 6.

5 Modern Deep learning-based forgery detection techniques

This section defines the most prevailing, demanding, and modern detection techniques used in the world nowadays in the field of forensic sciences. Joudar et al. [40] proposes a new optimization model for kernels redundancy reduction in CNN. Fernandes et al. [41] proposed that a particle swarm optimization-based algorithm could be used to search for the most effective convolutional neural networks.

5.1 Deep fakes

Other than the conventional methods as described above, there are more complicated image forgeries done nowadays. An emerging Artificial Intelligence-based trick is Deepfakes done using Specific Datasets (human faces, shapes, figures, etc.) assisted Neural Net techniques capable of region/face detection and neat modification [10]. Deep fakes are images/videos in which one person’s face has been convincingly replaced by a computer-generated face that often resembles a second person. Sharma et al. [93, 94] explores an innovative method for

| Dataset       | Image size               | Format  | Color | Original/Tampered |
|---------------|--------------------------|---------|-------|-------------------|
| Columbia Gray | 128*128                  | BMP     | NO    | 933/912           |
| Columbia color| 757*568/1152*768         | TIFF    | YES   | 183/180           |
| CASIA v1.0    | 384*256                  | JPEG    | YES   | 800/921           |
| CASIA v2.0    | 240*160/900*600          | TIFF/JPEG | YES | 7491/5123         |
| MICC-F220     | 722*480/800*600          | JPEG    | YES   | 110/110           |
| MICC-F2000    | 2048*1536                | JPEG    | YES   | 1300/700          |
| IMD           | 3000*2300                | JPEG/PNG| YES  | 48/48             |
| MICC-F600     | 800*533/3888*2952        | JPEG/PNG| YES  | 440/160           |
| CoMoFoD       | 512*512                  | JPEG/PNG| YES  | 5200/5200         |
| Wild Web      | Various                  | Various | YES   | 0/10646           |
| COVERAGE      | Various                  | TIFF    | YES   | 100/100           |
determining an individual’s emotional state by analysing the shape of their lips at various points in time.

5.2 Anti-forensics

Anti-computer forensics, also known as counter-forensics, are methods of preventing forensic analysis. Through the drawbacks as present in deep learning-based Image Forensics approaches, such as adversarial attacks where the Convoluted Neural Network (CNN) Model of Image Forensics is poor, smarter tricks are developed that can bypass the deep learning detection systems. Examples are, Jacobian-based Saliency Map Attack (JSMA), Fast Gradient Sign Method (FGSM), etc. [32].

5.3 Image source location(location forensic approaches)

Image source location based forensic approaches discusses into three categories. Camera artifacts based, Imaging property based and Sensor imperfection based source locations.

5.3.1 Camera artifact based source location

Based on every camera specification, lens and CFA produce some amount of aberration that can be analyzed from a digital image, and accordingly, the image capturing device can be located. Works in this area include choi et al. [92] who implemented Devernay’s line extraction method and proposed an image source location approach based on lens aberration analysis. Van and others used Support Vector Machine (SVM) as a model training scheme to analyze Chromatic aberration as a fingerprint for locating the correct image source.

5.3.2 Sensor imperfection based source location

Three major sensor defects aid the Image Forensic Experts to locate the Image Source. These are fixed pattern noise (FPN), Photo Response Non-Uniformity (PRNU), and pixel defects. Lukas and others worked based on pattern noise as exhibited through FPN and PRNU and made a comparative study on locating the correct image source. Koppanati [46, 47, 48] highlights a novel model for the encryption of multimedia data on cloud and using LFSR which uses of the RGB channels to encrypt data with the assistance of Logistic Map and Linear Feedback Shift Register. The authors Mantri et al. [62] propose a Pre-Encryption and Identification Technique in order to detect crypto-ransomware attacks at the pre-encryption level (PEI).

5.3.3 Imaging property-based source location

Coding and post-processing features as present in recognized digital image capturing devices are evidence for identifying actual Image Sources. Taking this fact as a working rule, Kharrazi et al. used pre-storage color processing and size corrections as fingerprints to locate the actual image capturing device. His model utilized SVM as a training scheme. Keeping security related to transmission and storage, Manupriya et al. [63] proposes an encryption technique called $V \oplus$ SEE which requires less bandwidth and CPU than AES and DES.
6 Discussion

High-speed internet access and free high-processing digital editing tools (image) worsen the problem of digital resource authenticity. Due to social networking sites, it’s difficult to find the source of digital resources. Finding the history (flow) of digital resources is crucial. Identifying forgeries and digital asset modifications to improve information clarity is difficult. The biggest challenge is identifying the few operations done on digital assets to improve clarity without changing their meaning or origin. New set of digital acquisition, processing, and tools and their accessible availability, widespread transmissions via social networking sites over the internet, and open source software have all contributed to a substantial and demanding problem of digital forgeries. Digital forensic is a new discipline that’s trying to figure out where digital media came from and how accurate it is. It detects the originality of photos or films, allowing for the management of enormous implications on a national and global scale caused by forgery done using Active, Passive or other deep learning based approaches including GAN the new and advance one in this field. The field of digital forensics research is finally focusing on solving more generic problems. As a result, it appears that universal solutions and strategies, such as the creation of standardized data sets, benchmarks, and evaluation criteria, generalized techniques will be required in order to achieve the new frameworks while reducing the risk of digital forgeries.

7 Conclusion

This paper critically reviews the broad classification of image forgery detection techniques. A comprehensive overview of active and passive forgery methods is analyzed by systematically surveying the literature. This study finds a wide scope of Deep Learning based methods in Passive Image Forgeries, ranging from pixel-based to geometric-based detection. Smarter algorithms are implemented to locate tampering in the fake face images as found in Deep Fake forgery. Future research in this field can be assisted using a variety of open-access datasets like CASIA V1, CASIA V2, MICC-F2000, CoMoFoD, etc. The paper concludes that advanced image forensics should incorporate more advanced methodologies that minimize executable time and operational cost. Key constraints like (1) accuracy of detection, (2) feature dimensionality, and (3) Robustness against a high degree of post-processing (4) High computational complexity (5) Vulnerability to multiple attacks such as rotation, scaling, JPEG compression, blurring, and brightness control, etc. (4) A large number of false matches with a regular backdrop are issues which require further studies. In a nutshell, despite deep learning methods showing wonderful results, there is still room for improvement to deal with more intense forgeries arising in today’s world.

In term of future work it appears that universal solutions and strategies, such as the creation of standardized data sets, benchmarks, and evaluation criteria, new deep generative techniques are extremely required in order to achieve the generalized solutions of detection of digital forgeries. Benchmarks for forged and unforged data sets are needed to evaluate collaborative research. Creation of open access data sets that are applicable for all possible forgeries such as copy paste, compositing, splicing, photomontage, blending, matting etc. is also promising area to explore in order to determine, analyse, and comprehend the usefulness of existing and future research studies. Designing more advance, generalized and robust forgery prevention and detection approaches that work efficiently for wild scenarios will be key research area to deal with more intense forgeries in future.
Data availability  Data is available on request.

Declarations

Conflict of interest  The authors have no conflict of interest.

References

1. Amerini I, Uricchio T, Ballan L, Caldelli R (2017) Localization of JPEG double compression through multi-domain convolutional neural networks. In: 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), pp 1865–1871. https://doi.org/10.1109/CVPRW.2017.233
2. Ansari MD, Ghera SP, Tyagi V (2014) Pixel-based image forgery detection: a review. IETE J Educ 55(1):40–46
3. Bappy JH, Simons C, Nataraj L, Manjunath BS, Roy-Chowdhury AK (2019) Hybrid lstm and encoder–decoder architecture for detection of image forgeries. IEEE Trans Image Process 28(7):3286–3300
4. Barni M, Bondi L, Bonettini N, Bestagini P, Costanzo A, Maggini M, Tondi B, Tubaro S (2017) Aligned and non-aligned double JPEG detection using convolutional neural networks. J Vis Commun Image Represent 49:153–163
5. Barni M, Costanzo A, Nowroozi E, Tondi B (2018) CNN-based detection of generic contrast adjustment with JPEG post-processing. In: 2018 25th IEEE International Conference on Image Processing (ICIP), pp 3803–3807. https://doi.org/10.1109/ICIP.2018.8451698
6. Bondi L, Baroffio L, Güera D, Bestagini P, Delp EJ, Tubaro S (2016) First steps toward camera model identification with convolutional neural networks. IEEE Signal Process Lett 24(3):259–263
7. Bourouis S, Alroobaee R, Alharbi AM, Anejany M, Rubaiee S (2020) Recent advances in digital multimedia tampering detection for forensics analysis. Symmetry 12(11):1811
8. Bunk J, Bappy JH, Mohammed TM, Nataraj L, Flenner A, Manjunath BS, ..., Peterson L (2017) Detection and localization of image forgeries using resampling features and deep learning. In: 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), pp 1881–1889. https://doi.org/10.1109/CVPRW.2017.235
9. Camacho IC, Wang K (2021) Data-dependent scaling of CNN’s first layer for improved image manipulation detection. In: Digital Forensics and Watermarking: 19th International Workshop, IWDW 2020, Melbourne, VIC, Australia, November 25–27, 2020, Revised Selected Papers. Springer Nature, vol. 12617, p 208. https://doi.org/10.1007/978-3-030-69449-4_16
10. Castillo Camacho I, Wang K (2021) A comprehensive review of Deep-learning-based methods for image forensics. J Imaging 7(4):69
11. Chaitra B, Reddy PVB (2019) A study on digital image forgery techniques and its detection. In: 2019 International Conference on contemporary Computing and Informatics (IC3I), pp 127–130. https://doi.org/10.1109/IC3I46837.2019.9055573
12. Cozzolino, D, Verdoliva, L (2020) Noiseprint: A CNN-based camera model fingerprint. IEEE Trans Inf Forensics Secur 15:144–159. https://doi.org/10.1109/TIFS.2019.2916364
13. Cozzolino D, Poggi G, Verdoliva L (2017) Recasting residual-based local descriptors as convolutional neural networks: an application to image forgery detection. In: Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security, pp 159–164. https://doi.org/10.1145/3082031.3083247
14. De Rezende ER, Ruppert GC, Theophilo A, Tokuda EK, Carvalho T (2018) Exposing computer generated images by using deep convolutional neural networks. Signal Process Image Commun 66:113–126
15. Ding X, Chen Y, Tang Z, Huang Y (2019) Camera identification based on domain knowledge-driven deep multi-task learning. IEEE Access 7:25878–25890. https://doi.org/10.1109/ACCESS.2019.2897360
16. Ding X, Raziei Z, Larson EC, Olinick EV, Krueger P, Hahsler M (2020) Swapped face detection using deep learning and subjective assessment. EURASIP J Inf Secur 2020(1):1–12
17. Doke KK, Patil SM (2012) Digital signature scheme for image. Int J Comput Appl 49(16):1–6
21. Eversberg L, Lambrecht J (2021) Generating images with physics-based rendering for an industrial object detection task: realism versus domain randomization. Sensors 21(23):7901
22. Fan W, Wang K, Cayre F, Xiong Z (2012) 3D lighting-based image forgery detection using shape-from-shading. In: 2012 Proceedings of the 20th European Signal Processing Conference (EUSIPCO), pp 1777–1781
23. Fan Y, Carré P, Fernandez-Maloigne C (2015) Image splicing detection with local illumination estimation. In: 2015 IEEE International Conference on Image Processing (ICIP), pp 2940–2944. https://doi.org/10.1109/ICIP.2015.7351341
24. Ferrara P, Bianchi T, De Rosa A, Piva A (2012) Image forgery localization via fine-grained analysis of CFA artifacts. IEEE Trans Inf Forensic Secur 7(5):1566–1577
25. Freire-Obregon D, Narducci F, Barra S, Castrillon-Santana M (2019) Deep learning for source camera identification on mobile devices. Pattern Recogn Lett 126:86–91
26. Fridrich J (2013) Sensor defects in digital image forensic. In: Digital image forensics (pp. 179–218). Springer, New York, NY, USensor
27. Gaharwar GKS, Nath PVV, Gaharwar RD (2015) Comprehensive Study of Different Types Image Forgeries. Int J Sci Technol Manag 6:146–151
28. Gardella M, Musé P, Morel JM, Colom M (2021) Forgery detection in digital images by multi-scale noise estimation. J Imaging 7(7):119
29. Geradts ZJ, Bijhold J, Kieft M, Kuroswa K, Kuroki K, Saitoh N (2001) Methods for identification of images acquired with digital cameras. In enabling technologies for law enforcement and security. Int Soc Opt Photonics 4232:505–512
30. Gill NK, Garg R, Doegar EA (2017) A review paper on digital image forgery detection techniques. In: 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp 1–7. https://doi.org/10.1109/ICCCNT.2017.8203904
31. Ginesu G, Giusto DD, Onali T (2006) Mutual image-based authentication framework with JPEG2000 in wireless environment. EURASIP J Wirel Commun Netw 2006:1–14
32. Glorot X, Bordes A, Bengio Y (2011) Deep sparse rectifier neural networks. In: Proceedings of the Fourteenth International Conference on Artificial Intelligence and Statistics, in Proceedings of Machine Learning Research 15:315–323. https://proceedings.mlr.press/v15/glorot11a.html
33. Gupta A, Saxena N, Vasistha SK (2013) Detecting copy-move forgery using DCT. Int J Sci Res Publ 3:5
34. Hashmi MF, Anand V, Keskar A (2014) Copy-move image forgery detection using an efficient and robust method combining un-decimated wavelet transform and scale invariant feature transform. AASRI Procedia 9:84–91. https://doi.org/10.1016/j.aasri.2014.09.015
35. He P, Li H, Wang H, Zhang R (2020) Detection of computer graphics using attention-based dual-branch convolutional neural network from fused color components. Sensors 20(17):4743
36. Huh M, Liu A, Owens A, Efros AA (2018) Fighting fake news: image splice detection via learned self-consistency. In: Proceedings of the European Conference on Computer Vision (ECCV), pp 101–117
37. Hussain M, Qasem S, Bebis G, Muhammad A, Mathkour H (2015) Evaluation of image forgery detection using multi-scale weber local descriptors. Int J Artif Intell Tools 24(4):1540016
38. Johnson MK, Farid H (2006) Exposing digital forgeries through chromatic aberration. In: Proceedings of the 8th workshop on Multimedia and security, pp 48–55. https://doi.org/10.1145/1161366.1161376
39. Johnson MK, Farid H (2006) Metric measurements on a plane from a single image. Computer Science Technical Report TR2006-579. https://digitalcommons.dartmouth.edu/cs/tr/288
40. Joudar NE, Ettouil M (2021) KRR-CNN: kernels redundancy reduction in convolutional neural networks. Neural Comput & Appl 1–12
41. Junior FEF, Yen GG (2019) Particle swarm optimization of deep neural networks architectures for image classification. Evol Comput Evolut 49:62–74
42. Kashyap A, Parmar RS, Agrawal M, Gupta H (2017) An evaluation of digital image forgery detection approaches. arXiv: preprint arXiv: 1703.09968. https://doi.org/10.48550/arXiv.1703.09968
43. Kaur A, Rani J (2016) Digital Image Forgery and Techniques of Forgery Detection. Int J Tech Res Sci 1(4):18–24 [Online]. Available: www.ijtrs.com
44. Kee E, Farid H (2010) Exposing digital forgeries from 3-D lighting environments. In: 2010 IEEE International Workshop on Information Forensics and Security, pp 1–6. https://doi.org/10.1109/WIFS.2010.5711437
45. Khalid H, Woo SS (2020) OC-FakeDect: classifying deepfakes using one-class variational autoencoder. In: 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), pp 2794–2803. https://doi.org/10.1109/CVPRWS50498.2020.00336
46. Koppanati RK, Kumar K (2020) P-MEC: polynomial congruence-based multimedia encryption technique over cloud. IEEE Consum Electron Mag 10(5):41–46. https://doi.org/10.1109/MCE.2020.3003127
47. Koppanati RK, Qamar S, Kumar K (2018) SMALL: secure multimedia technique using logistic and LFSR. In: 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), pp 1820–1825. https://doi.org/10.1109/ICCONS.2018.8662840
48. Koppanati RK, Kumar K, Qamar S (2021) E-MOC: an efficient secret sharing model for multimedia on cloud. In: Tripathi M, Upadhyaya S (eds) Conference Proceedings of ICDLAIR2019. Lecture Notes in Networks and Systems, vol 175. Springer, Cham. https://doi.org/10.1007/978-3-030-67187-7_26
49. Kumar M, Srivastava S (2018) Image tampering detection based on inherent lighting fingerprints. In: In computational vision and bio inspired computing (pp. 1129–1140). Springer, Cham
50. Kumar M, Srivastava S (2019) Image forgery detection based on physics and pixels: a study. Australian J Forensic Sci 51(2):119–134
51. Kumar M, Srivastava S (2019) Image authentication by assessing manipulations using illumination. Multimed Tools Appl 78(9):12451–12463
52. Kumar BS, Karthi S, Karthika K, Cristin R (2018) A systematic study of image forgery detection. J Comput Theor Nanosci 15(8):2560–2564
53. Kumar M, Rani A, Srivastava S (2019) Image forensics based on lighting estimation. Int J Image Graph 19(03):1950014
54. Kumar M, Srivastava S, Uddin N (2019) Forgery detection using multiple light sources for synthetic images. Australian J Forensic Sci 51(3):243–250
55. Lee S, Tariq S, Shin Y, Woo SS (2021) Detecting handcrafted facial image manipulations and GAN-generated facial images using shallow-FakeFaceNet. Appl Soft Comput 105:107256
56. Li L, Li S, Zhu H, Chu SC, Roddick JF, Pan JS (2013) An efficient scheme for detecting copy-move forged images by local binary patterns. J Inf Hiding Multim Signal Process 4(1):46–56
57. Liu Q, Sung AH (2009) A new approach for JPEG resize and image splicing detection. In: Proceedings of the First ACM workshop on Multimeida in forensics, pp 43–48. https://doi.org/10.1145/1631081.1631092
58. Liu Y, Guan Q, Zhao X (2018) Copy-move forgery detection based on convolutional kernel network. Multimed Tools Appl 77(14):18269–18293
59. Lu M, Niu S (2020) A detection approach using LSTM-CNN for object removal caused by exemplar-based image inpainting. Electronics 9(5):858
60. Lu S, Hu X, Wang C, Chen L, Han S, Han Y (2022) Copy-move image forgery detection based on evolving circular domains coverage. Multimed Tools Appl: 1–26. https://doi.org/10.1007/s11042-022-12755-w
61. Mahalakshmi SD, Vijayalakshmi K, Priyadharsini S (2012) Digital image forgery detection and estimation by exploring basic image manipulations. Digit Invest 8(3–4):215–225
62. Mantri A, Singh N, Kumar K, Dahiya S (2022) Pre-encryption and identification (PEI): an anti-crypto ransomware technique. IETE J Res:1–9
63. Manupriya P, Sinha S, Kumar K (2017) V⊕ SEE: video secret sharing encryption technique. In: 2017 Conference on Information and Communication Technology (CICT), pp 1–6. https://doi.org/10.1109/INFOCOMTECH.2017.8340639
64. Marra F, Gragnaniello D, Cozzolino D, Verdoliva L (2018) Detection of Gan-generated fake images over social networks. In: 2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), pp 384–389. https://doi.org/10.1109/MIPR.2018.00084
65. Meena KB, Tyagi V (2019) Image Forgery Detection: Survey and Future Directions. In: Image forgery detection: survey and future directions. In data, engineering and applications (pp. 163–194). Springer, Singapore
66. Mohite VD, Athawale U, Athawale S, Vidyapeeth B, Mumbai N (2019), “Survey on Recent Image Forgeries and their Detection Methods. Int J Res Eng Appl Manag, 02, (pp. 885–892) (JREAM)
67. Morgand A, Tamaazousti M, Bartoli A (2018) A geometric model for specularity prediction on planar surfaces with multiple light sources. IEEE Trans Vis Comput Graph 24(5):1691–1704. https://doi.org/10.1109/TVCG.2017.2677445
68. Morgand A, Tamaazousti M, Bartoli A (2021) A Multiple-View Geometric Model for Specularity Prediction on Non-Uniformly Curved Surfaces. arXiv preprint arXiv:2108.09378. https://doi.org/10.48550/arXiv.2108.09378
69. Mushraq S, Mir A (2014) Digital image forgeries and passive image authentication techniques: a survey. Int J Adv Sci Technol 73:15–32. https://doi.org/10.14257/ijast.2014.73.02
70. Ng TT, Chang SF, Hsu J, Xie L, Tsui MP (2005) Physics-motivated features for distinguishing photographic images and computer graphics. In: Proceedings of the 13th annual ACM international conference on Multimedia, pp 239–248. https://doi.org/10.1145/1101149.1101192
71. Nguyen HH, Yamagish J, Echizen I (2019) Capsule-forensics: using capsule networks to detect forged images and videos. In: ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp 2307–2311. https://doi.org/10.1109/ICASSP.2019.8682602
72. Nirmalkar N, Kamble S, Kakde S (2015) A review of image forgery techniques and their detection. In: 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), pp 1–5. https://doi.org/10.1109/ICIIECS.2015.7193177
73. O'Brien JF, Farid H (2012) Exposing photo manipulation with inconsistent reflections. ACM Trans Graph 31(1):4–1
74. Pan X, Zhang X, Lyu S (2011) Exposing image forgery with blind noise estimation. In: Proceedings of the thirteenth ACM multimedia workshop on Multimedia and security, pp 15–20. https://doi.org/10.1145/2037252.2037256
75. Park, J, Cho, D, Ahn, W, Lee, HK (2018) Double JPEG detection in mixed JPEG quality factors using deep convolutional neural network. In proceedings of the European conference on computer vision (ECCV) (pp. 636-652)
76. Pawlak Z, Tusk M, Kuna S, Strohbusch F, Fox MF (1984) pH dependence of hydrogen bonding in complexes between trimethyl-N-oxide and pentachlorophenol and trifluoroacetic acid in acetonitrile. J Chem Soc Faraday Trans 1: Phys Chem Condensed Phases 80(7):1757–1768
77. Peng B, Wang W, Dong J, Tan T (2016) Optimized 3D lighting environment estimation for image forgery detection. IEEE Trans Inf Forensic Secur 12(2):479–494
78. Pine, J, Nicolas, H (2001) Estimation 2d illuminant direction and shadow segmentation in natural video sequences. In proceedings of VLBV (p. 197)
79. Pinel JM, Nicolas H, Bris CL (2001) Estimation of 2D illuminant direction and shadow segmentation in natural video sequences. Proceedings of VLBV, pp 197–202
80. Popescu, AC, Farid, H (2004) Exposing digital forgeries by detecting duplicated image regions. Tech. The report, TR2004-515, dep. Comput. Sci. Dartmouth Coll. Hanover, new Harmsph., no. 2000,( pp. 1–11) [online]. Available: http://os2.zemris.fer.hr/ostalo/2010_marceta/Diplomski_files/102.pdf. Accessed 20 Aug 2021
81. Popescu AC, Farid H (2005) Exposing digital forgeries in color filter array interpolated images. IEEE Trans Signal Process 53(10):3948–3959
82. Qureshi MA, Deriche M (2014) A review on copy move image forgery detection techniques. In: 2014 IEEE 11th International Multi-Conference on Systems, Signals & Devices (SSD14), pp 1–5. https://doi.org/10.1109/SSD.2014.6808907
83. Raja A (2021) Active and Passive Detection of Image Forgery: A Review Analysis. IJERT- Proc 9(5):418–424
84. Rani A, Kumar M, Goel P (2016) Image modelling: a feature detection approach for Steganalysis. In international conference on advances in computing and data sciences (pp. 140-148). Springer, Singapore
85. Rani A, Jain A, Kumar M (2021) Identification of copy-move and splicing based forgeries using advanced SURF and revised template matching. Multimed Tools Appl 80(16):23877–23898
86. Rao Y, Ni J (2016) A deep learning approach to detection of splicing and copy-move forgeries in images. In: 2016 IEEE International Workshop on Information Forensics and Security (WIFS), pp 1–6. https://doi.org/10.1109/WIFS.2016.7823911
87. Reddy V, Vaghdevi K, Kolli D (2021) Digital image forgery detection using SUPER pixel segmentation and HYBRID feature point mapping. European J Molecular Clin Med 8(2):1485–1500
88. Rohde LE, Clausell N, Ribeiro JP, Goldraich L, Netto R, Dec GW, … Polanczyk CA (2005) Health outcomes in decompensated congestive heart failure: a comparison of tertiary hospitals in Brazil and United States. Int J Cardiol 102(1):71–77
89. Roy A, Chakraborty RS, Sameer VU, Naskar R (2017) Camera source identification using discrete cosine transform residue features and ensemble classifier. In: CVPR workshops, pp 1848–1854. https://doi.org/10.1109/CVPRW.2017.231
90. Saber AH, Khan MA, Mejbel BG (2020) A survey on image forgery detection using different forensic approaches. Adv Sci Technol Eng Syst J 5(3):361–370
91. Salloum R, Ren Y, Kuo CCIJ (2018) Image splicing localization using a multi-task fully convolutional network (MFCN). J Vis Commun Image Represent 51:201–209
92. San Choi K, Lam EY, Wong KK (2006) Source camera identification using footprints from lens aberration. In: Proc. SPIE 6069, Digital Photography II, 60690J (10 February 2006). https://doi.org/10.1117/12.649775
93. Sharma S, Kumar K (2018) Guess: genetic uses in video encryption with secret sharing. In: Proceedings of 2nd international conference on computer vision & image processing (pp. 51-62). Springer, Singapore
94. Sharma S, Kumar K, Singh N (2017) D-FES: Deep facial expression recognition system. In: 2017 Conference on Information and Communication Technology (CICT), pp 1–6. https://doi.org/10.1109/INFOCOMTECH.2017.8340635
95. Singh MsN, Joshi S (2016) Digital image forensics: progress and challenges. In: Proceedings of 31st National convention of Electronics and Telecommunication Engineers, Researchgate (October 2015)
96. Shiwei L, Xunyu P, Xing Z (2014) Exposing region splicing forgeries with blind local noise estimation [J]. Int J Comput Vis 110(2):202–221
97. Sri CG, Bano S, Deepika T, Kola N, Pranathi YL (2021) “Deep Neural Networks Based Error Level
Analysis for Lossless Image Compression Based Forgery Detection,” 2021 Int Conf Intell Technol CONIT
2021, pp. 1–8, 2021, https://doi.org/10.1109/CONIT51480.2021.9498357.
98. Stojkovic A, Shopovska I, Luong H, Aelterman J, Jovanov L, Philips W (2019) The effect of the color
filter array layout choice on state-of-the-art demosaicing. Sensors 19:3215. https://doi.org/10.3390/
s19143215
99. Sun JY, Kim SW, Lee SW, Ko SJ (2018) A novel contrast enhancement forensics based on convolutional
neural networks. Signal Process Image Commun 63:149–160
100. Swapna P, Krouglicof N, Gosine R (2010) A novel technique for estimating intrinsic camera parameters in
geometric camera calibration. In: CCECE 2010, pp 1–7. https://doi.org/10.1109/CCECE.2010.5575238
101. Tang H, Ni R, Zhao Y, Li X (2018) Median filtering detection of small-size image based on CNN. J Vis
Commun Image Represent 51:162–168
102. Thakur A, Jindal N (2018) Image forensics using color illumination, block and key point based approach.
Multimed Tools Appl 77(19):26033–26053
103. Tuama A, Comby F, Chaumont M (2016) Camera model identification with the use of deep convolutional
neural networks. In: 2016 IEEE International Workshop on Information Forensics and Security (WIFS), pp
1–6. https://doi.org/10.1109/WIFS.2016.7823908
104. U. S. Patent, “United States Patent (19),” (1976)
105. Verma V, Agarwal N, Khanna N (2018) DCT-domain deep convolutional neural networks for multiple
JPEG compression classification. Signal Process Image Commun 67:22–33
106. Wang X, Niu S, Wang H (2021) Image inpainting detection based on multi-task deep learning network.
IETE Tech Rev 38(1):149–157
107. Wu L, Wang Y (2011) Detecting image forgeries using geometric cues. In: Computer Vision for Multimedia
Applications: Methods and Solutions. IGI Global, pp 197-217. https://doi.org/10.4018/978-1-60960-024-2.ch012
108. Wu L, Cao X, Zhang W, Wang Y (2012) Detecting image forgeries using metrology. Mach Vis Appl
23(2):363–373
109. Wu Y, Abd-Almageed W, Natarajan P (2018) Busternet: detecting copy-move image forgery with source/
target localization. In: 15th European Conference, Munich, Germany, September 8–14, Proceedings, Part
VI. https://doi.org/10.1109/78-3-030-01231-1_11
110. Wu Y, AbdAlmageed W, Natarajan P (2019) Mantra-net: manipulation tracing network for detection and
localization of image forgeries with anomalous features. In: Proceedings of the IEEE/CVF Conference on
Computer Vision and Pattern Recognition (CVPR), pp 9543–9552
111. Xu J, Feng D, Wu J, Cui Z (2009) An image inpainting technique based on 8-neighborhood fast sweeping
method. In: 2009 WRI International Conference on Communications and Mobile Computing, pp 626–630.
https://doi.org/10.1109/CMMC.2009.369
112. Xu B, Wang X, Zhou X, Xi J, Wang S (2016) Source camera identification from image texture features.
Neurocomputing 207:131–140
113. Yang P (2021) Dual-domain fusion convolutional neural network for contrast enhancement forensics.
Entropy 23(10):1318
114. Yao H, Qiao T, Tang Z, Zhao Y, Mao H (2011) Detecting copy-move forgery using non-negative matrix
factorization. In: 2011 Third International Conference on Multimedia Networking and Security, pp 591–594.
https://doi.org/10.1109/MINES.2011.104
115. Yarlagadda SK, Güera D, Bestagini P, Maggie Zhu F, Tubaro S, Delp EJ (2018) Satellite image forgery
detection and localization using Gan and one-class classifier. Electron Imaging 2018(7):214–211
116. Zhang X, Wang X (2018) Digital image encryption algorithm based on elliptic curve public cryptosystem.
IEEE Access 6:70025–70034
117. Zhang Y, Goh J, Win LL, Thing VL (2016) Image region forgery detection: a Deep learning approach.
SG-CRC 2016:1–11
118. Zhang RS, Quan WZ, Fan LB, Hu LM, Yan DM (2020) Distinguishing computer-generated images from
natural images using channel and pixel correlation. J Comput Sci Technol 35(3):592–602
119. Zhou P, Han, X, Morariu, VI, Davis, LS (2018) Learning rich features for image manipulation detection.
In: Proceedings of the IEEE conference on computer vision and pattern recognition, pp 1053–1061. https://
doi.org/10.48550/arXiv.1805.04953
120. Zhuo L, Tan S, Zeng J, Lit B (2018) Fake colorized image detection with channel-wise convolution based
deep-learning framework. In: 2018 Asia-Pacific Signal and Information Processing Association Annual
Summit and Conference (APSIPA ASC), pp 733–736. https://doi.org/10.23919/APSIPA.2018.8659761

Publisher’s note Springer Nature remains neutral with regard to jurisdictional claims in published maps and
institutional affiliations.