Informatics Bulletin, Faculty of Computers and Artificial Intelligence, Helwan University
Published Online ***Vol 6 Issue 2, July 2024***
(https://fcihib.journals.ekb.eg)

# Image Forgery Detection Using Deep Learning: A Comparative Study

Ashgan H. Khalil[1], Atef Z. Ghalwash[1], Hala A. Elsayed [1], Gouda I. Salama[2].
[1] Computer Science Dept., Faculty of Computers and Artificial Intelligence, Helwan University, Cairo, Egypt
[2] Depart. of Computer Engineering, MTC, Cairo, Egypt
Corresponding author: Ashgan H. Khalil (e-mail: Ashganheissen_csp@fci.helwan.edu.eg).

***Abstract*—In recent years, there has been a significant increase in online activities, including business meetings, education, research, and virtual conferences. As a result, digital images have become the main source of information that can be shared and visualized on social media, in addition, it's easy to forge these images using image-editing software, and it's essential to detect image forgery for such images. So, it becomes essential to introduce an efficient image forgery detection technique to classify these images as either authentic or forged. In the past few years, deep learning-based techniques have achieved remarkable results in the field of image forgery detection IFD, most of them used transfer learning with the help of pre-trained models aiming to reduce time in the training and detection phase. This paper presents a comparative study of various image forgery detection techniques, it explores the techniques based on new deep learning models and techniques based on transfer learning models with the help of pre-trained models. The study aims to provide insights into the performance of different techniques used in deep learning and pre-trained models in image forgery detection, which may guide any researcher to present a useful model, that can detect multiple image forgery types simultaneously with improved detection accuracy and minimal detection time. The discussed results suggest the use of pre-trained models in the feature extraction phase only. and recommend using deep learning in classification.**

**Keywords: Copy-Move · Image forgery detection (IFD) techniques · Image Splicing · Transfer learning.**

## I. Introduction

The tampering of a digital image is called digital image forgery, these forged images cannot be detected by the naked eye. These images are the primary sources of spreading fake news in the market and spreading misleading information in society to influence the public with the help of various social media platforms such as Facebook, Twitter, etc. [1], [2]. These forgeries are done using editing tools that are available and free of cost with some advanced software such as GNU, GIMP, and Adobe Photoshop [3]. Such forgeries can be detected using digital image forgery algorithms and techniques, these algorithms are used in image security especially when the original content is unavailable [4].

The paper is organized as follows: The classification of digital image forgery is covered in section II. Section III discusses the digital image forgery detection techniques in detail. Section IV presents a comparative study of deep learning techniques and transfer learning techniques. Section V analyzes the comparison results between deep learning and transfer learning techniques, Section VI has the conclusion and future work.

## II. Digital Image Forgery Classification

Digital image forgery means adding unusual patterns to the original images that cause a heterogeneous manner in the form of image properties and unusual distribution of image features. Digital image forgeries appeared in different forms like copy move forgery and other morphological applications on images such as splicing, retouching, resampling, and morphing in addition to images created by graphical applications. Figure 1 shows the classification of digital image forgery [4]. Digital image forgery can be classified as active and passive approaches as follows:

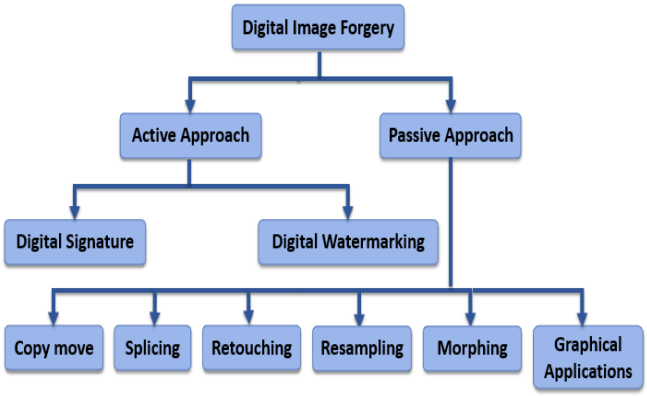


Figure 1: Digital Image Forgery Classification

### *A. Active/Non-blind Method*

In active approaches, primary knowledge about the image is necessary for the verification process. The inserted information within the picture is employed to find the basis of that picture or to observe the modification in that picture, it consists of two types: digital signatures and digital watermarking. Digital signatures insert some subsidiary data obtained from images, by the end of the acquisition process, and digital watermarks are inserted in images during image attainment or during the dispensation phase. The disadvantage of active methods is that they are introduced in images during the record utilizing special equipment. Therefore, primary knowledge about images is essential [5].

*B. Passive/Blind Method*

Passive image forgery detection methods exploit the information retained during different stages of digital image capture and storage to identify any tampering. Unlike active methodologies, passive approaches do not rely on prior knowledge about the image. Instead, they exploit the fact that tampering actions alter the informational content of the image, thereby enabling effective tampering detection [5].

**Copy move** forgery is utilized by taking a section or object in an image and adding it again in the image itself but in another location to iterate a specific scene in the image. Copy-move forgery is the most difficult type to detect, this difficulty is presented in copying an object or part of the image with the same properties and same feature distribution and pasting it in the same image. This image forgery method makes the final tampered image have the same homogenous context, it does not have distortions, noise, or heterogeneity features like coloring changes, shadows, edging, or any other features used as evidence of tampering [4] [6]. An experienced forger can also apply some post-processing techniques after CMF processes such as rotation, scaling, JPEG compression, etc., which makes the detection further difficult and complex. Hence, the foremost most important point in this detection method is the feature extraction which is invariant to these above post-processing operations [3].

**Splicing forgery** can be done by adding or merging two images or groups of images to produce an unprecedented image [4]. The source images used to create a spliced image may have different color temperatures, illumination conditions, and noise levels based on various factors. Forger always applies average filtering or some other related image processing operation as postprocessing like resizing, cropping, rotating, and retouching each of the source images to match the visual conditions or shape and size of the target image so that the forged image can look realistic and make splicing boundaries smooth and less visually different from its surrounding [7].

**Retouching forgery** is the process of enhancing an image to conceal or exhibit specific features like illumination, coloration, contrast enhancement, and background coloring altering. Retouching forgery includes the visual quality enhancement of the image. In the resampling forgery, the original image is resized to distort the actual content of the image [4].

**Resampling Forgery** is based on changing the dimensionality of a specific part or object in the image to display it in a misleading view. **Morphing forgery** is the process of combining two various scenes of two various images to create an unprecedented scene. Finally, the last forgery type is applied by creating a total image using graphical software; the produced image does not belong to reality [4]. The major types of tampering are Copy Move, Image Splicing, and Image Retouching (IR)) [5].

## III. Digital Image Forgery Detection Techniques

Digital Image Forgery Detection is a binary classification task, with the objective of the method to classify the image as either forged or authentic. A general structure for blind or passive IFD is given below which involves the following major steps summarized in Figure 2 [5].

**Preprocessing:** This step involves applying some operations on the image before the feature extraction process, such as the conversion of the image from RGB to grayscale, histogram equalization, smoothing, etc.

**Feature extraction:** The features of each class are extracted which can differentiate among them. Certain features are then selected which are more informative and sensitive to image manipulation.

**Feature matching:** The step of feature matching involves the matching of the feature vectors of different regions, e.g., the rectangular regions in block-based methods, which are similar to each other, which ends with the detection process if the image is original or forged.

**Filtering:** Some feature vectors might not be similar but still give a positive result in terms of similarity and thus have to be filtered out from the actual feature vector pairs that are similar.

**Classification:** This step classifies the image as belonging to either of the class: forged or authentic image, using a trained classifier.

**Post-processing:** Image forgery localization is one of the examples of post-processing operation which gives additional information about the forgery in the image after being classified as forged.

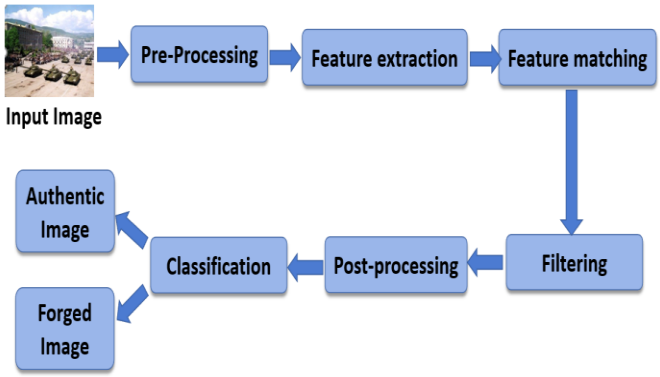


Figure 2: The general structure of the image forgery detection techniques

Many comprehensive reviews of Digital Image Forgery Detection Techniques are presented by collecting various types according to feature extraction techniques and classification techniques used. Digital image forgery detection algorithms can be grouped into: Machine learning techniques, and Deep learning techniques as shown in Figure 3.

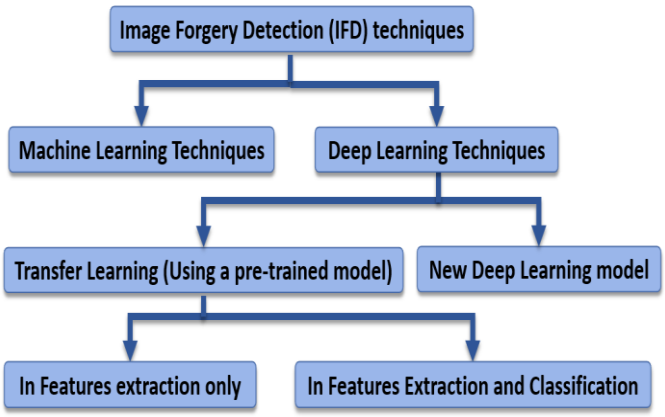


Figure 3: Image forgery detection techniques (IFD)

### *A. Image Forgery Detection Techniques (IFD) Based on Machine Learning*

Image Forgery Detection IFD techniques have two phases, feature extraction, and classification. The feature extraction phase is the major phase in the IFD. Generally based on the feature extraction mechanisms, the IFD techniques can be categorized as hand-crafted feature-based and deep learning feature-based. Hand-crafted features are the traditional features used in image processing or computer vision that are used in extracting features. Common hand-crafted feature extraction mechanisms like adaptive speeded-up robust features (SURF), Discrete Wavelet Transform (DWT), Integer Wavelet Transform (IWT), Patched Local Vector Pattern (LVP), Principal Component Analysis (PCA), 'Histogram of Oriented Gradients (HoG), feature and Mode Based First Digit Feature (MBFDF). Discrete Cosine Transform (DCT) and Local Binary Pattern (LBP) etc., these features can be used to distinguish between authentic and forged images [7]. The collected data are subjected to the fused feature extraction framework [8].

In machine learning-based IFD techniques, the feature extraction phase in machine learning IFD uses common hand-crafted feature extraction mechanisms, as mentioned before. In the classification phase, one of the machine learning algorithms is used like Logistic Regression, Naive Bayes, K-Nearest Neighbors (KNN), Decision Tree, and Support Vector Machines. (SVM) to classify whether the image is authentic or forged.

After surveying many existing Copy-move algorithms, most of the existing CMFD algorithms based on Hand-crafted features are very robust to most post-processing operations. However, it fails for other operations especially in contrast change [9].

The major limitations in traditional IFD are due to the various processes applied over the original image before pasting it over the same image to hide forgery. Most of the techniques have a high computational cost compared to the existing deep learning methods [3].

### *B. Image Forgery Detection Techniques Based on Deep Learning*

Deep learning-based IFD techniques differ from the two previous types of IFD techniques, the deep neural network is designed in which the feature extraction phase and the classification phase can be done through the network. The deep neural network DNN can extract the important features and accurately classify the image based on good starting weights and good tuning of the network parameters during the training time. Here the features are called deep learning-based features, which means that the features are extracted from the deep network itself. In some cases, the hand-crafted features are fed to the DNN to reduce the training time and aim for an improved accuracy rate [7].

Deep learning networks can overcome the limitations of traditional or hand-crafted features and can learn a very large number of features automatically [7]. In deep learning-based image detection methods, a large number of authentic and tampered images are fed to the models for tamper detection [10]. Deep Learning networks have been proven effective in finding complex hidden patterns in the data which can differentiate the forged part from the original image by building an appropriate neural network [11].

Some authors performed feature extraction and classification as a single module, whereas many authors use existing Convolutional Neural Networks (CNN) as a feature extractor, and then feature classification is applied explicitly, and postprocessing operation is mainly applied for the localization [7]. The accuracy of different deep learning-based IFD techniques is above 85% and reaches up to 99% [12]. For all activities or problems that machine learning algorithms were not able to solve, deep learning can solve them easily. ML algorithms are very related to DL [13].

Several deep learning-based techniques exhibit a high degree of accuracy in detecting image forgeries. In [8], an image tampering detection framework was designed, encompassing two distinct but interconnected phases: a feature extraction phase and the tamper detection phase. During the feature extraction phase, an extensive set of diverse features, including SURF, DWT, LVP, PCA, HoG, and MBFDF, were meticulously extracted. These extracted features were then employed as inputs for an optimized CNN. Then Sealion Customized Firefly algorithm (SCFF), was applied to fine-tune the CNN's weights.

Building on this foundation, [11] introduced a modified iteration of the U-Net Image Segmentation Model, augmented with the inclusion of L2 regularization, to reduce model complexity and curtail the total number of parameters, addressing overfitting issues and improve the overall accuracy and the F1 score of the model. In [14] the authors proposed an alternative approach to image forgery detection, commencing with the extraction of low-level features from two input streams: one representing the spatial image and the other depicting a high-pass filtered residual image.

In [15], researchers introduced an automated image splicing forgery detection scheme that leveraged a unique approach. This method involved feature extraction based on the analysis of the color filter array (CFA). Following the feature extraction process, a crucial dimensionality reduction step was executed using Principal Component Analysis (PCA) that enhances the overall efficiency of the detection process. [16] proposed Constrained R-CNN for image manipulation detection that adopted a comprehensive coarse-to-fine approach, commencing with a learnable manipulation feature extractor, the proposal network demonstrated its effectiveness in distinguishing manipulated regions.

In [17], a network known as the dual-encoder UNet (D-Unet) was introduced as a formidable tool for detecting image splicing forgeries. This network comprised two encoders, one unfixed specialized in learning image fingerprints to differentiate between tampered and non-tampered regions, and the other fixed to provide critical directional information that greatly facilitated the network's learning and detection capabilities. In [18], the Progressive Spatio-Channel Correlation Network (PSCC-Net) was developed. PSCC-Net adopted a novel two-path processing approach: a top-down path that extracted both local and global features, and a bottom-up path responsible for detecting image manipulation and estimating manipulation masks.

Researchers in [19], introduced a real-time image forensic method known as the multi-domain learning convolutional neural network (MDL-CNN). This method harnessed the periodicity property present in both original and modified images. To enhance the recognition ability of deep learning features, a multi-domain loss function was devised. In [20], an image splicing detection and localization scheme was proposed that relied on a local feature descriptor learned by a deep CNN. An innovative initialization technique for the first convolutional layer, based on the spatial rich model (SRM), was introduced, and a splicing localization scheme was developed, integrating the CNN model with a fully connected conditional random field (CRF.

In [21], researchers introduced the hybrid features and semantic reinforcement network (HFSRNet), a network architecture founded on encoding and decoding principles. This approach incorporated LSTM with resampling features. Consolidated features derived from rotating residual units were utilized to maximize the distinction between untampered and tampered regions. Additionally, semantic reinforcement was implemented to enhance performance. [22] proposed a robust framework encompassing camera model identification (CMI) and IFD. Based on CNN, this model was adept at handling various common manipulations often encountered when sharing images online. The training process involved a mixture of different qualities of compressed and uncompressed images, resulting in a versatile and effective system.

In [23], the authors developed a deep learning method tailored for Copy-Move Forgery Detection (CMFD). CNN was harnessed to acquire hierarchical feature representations from input images, facilitating the detection of tampered and original images with precision. [24] presented a deep CNN model characterized by multi-scale input and multiple stages of convolutional layers. The model was organized into two key blocks: In the encoder block, feature maps extracted from convolutional layers at multiple stages were fused and down-sampled. In the decoder block, extracted feature maps underwent further fusion and sampling.

The authors in [25] introduced a robust deep learning-based system designed for identifying image forgeries within the context of double image compression. The model was trained using disparities between an image's original and recompressed versions, offering a lightweight and rapid solution for forgery detection. Researchers in [26] proposed a CNN model tailored for real-time detection of splicing forged images. This streamlined model featured a modest number of parameters, comprising just four convolutional layers and four max-pooling layers, rendering it highly suitable for resource-constrained environments.

The authors in [27] unveiled an end-to-end comprehensive CNN framework that seamlessly integrated multiresolution hybrid features drawn from both RGB and noise streams, learning visual artifacts and compression inconsistencies. A pivotal innovation was the tamper-guided dual self-attention (TDSA) module, meticulously designed to steer the network's focus towards tampered regions and effectively segment them from the image. In [28], an approach to copy-move IFD and localization introduced. This method hinged on the concept of super boundary-to-pixel direction (super-BPD) segmentation, complemented by the utilization of a deep CNN (DCNN). The workflow commenced with the employment of segmentation techniques, fostering stronger connections among identical image blocks. Subsequently, the DCNN was deployed to extract features and localization process. Image BPD information used to optimize the edges of the approximately detected image, further enhancing accuracy. [29] proposed a streamlined and lightweight CNN model tailored for the automatic detection of copy-move forgery. Despite its simplicity, this model achieved remarkable detection accuracy rates, underscoring the efficacy of its design in identifying manipulated content.

These studies underscore the continual innovation and diversification of techniques within the realm of image forgery detection, each contributing to the broader landscape of digital image integrity preservation.

### *C. Image Forgery Detection Techniques Based on Transfer Learning*

Transfer learning is to takes the knowledge from the previously trained model (features, weights, etc.) which is trained by a large dataset (ImageNet database which consists of 1.2 million images with 1000 categories in the case of AlexNet) to solve the problem of the new target domain, as illustrated in Figure 4. It keeps the knowledge learned from domain A and applies it in domain B. To train the model on the target data through transfer learning, weights from the pre-trained model

are used as initializers, instead of initializing the model with random weights, this helps to accelerate the training speed [30].

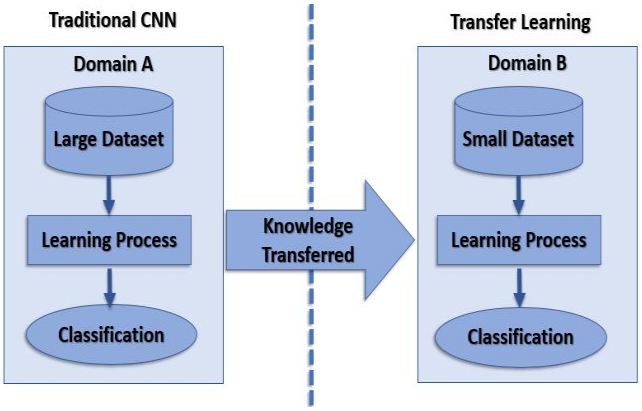


Figure 4: Traditional CNN vs. Transfer Learning

Deep learning-based methods require large data to train the model. However, the image-splicing datasets that are available in the public domain do not have a large number of images. The lack of availability of sufficient data to train a deep learning model has motivated the concept of transfer learning. Transfer learning allows solving a similar problem by transferring the knowledge of any existing well-trained deep learning model. In this way, instead of training the new deep learning model from scratch, just utilize the weights of pre-trained models [2].

The pre-trained model saves a lot of time, which is consumed by the training process, and it reduces the dimensionality, it reduces the number of parameters, which reduces the chance of overfitting. The major advantage of transfer learning is that it works on small data and retains models with it [13].

A variety of pre-trained CNN models have emerged, such as AlexNet [31], VGGNet [32], ResNet [33], GoogleNet [34], DenseNet [35], Xception [36], SENet [37], Siamese Network [38] as well as Caffe. The AlexNet architecture consists of eight layers, of which five are convolutional layers and three are fully connected layers, it introduces support for multiple GPUs, which were required for larger datasets like ImageNet [39]. VGG-16 model trained on over a million images from the ImageNet database. The network model is 16 layers deep and can discriminate many types of images into their respective classes [40]. VGGNet has much fewer parameters; the small convolution filters allow it to have a greater number of weight layers, thus improving performance [39].

ResNet is a CNN trained on the ImageNet dataset which makes a balance between computational complexity and performance [41]. ResNet-18 is 18 layers deep with 11.7 million parameters. ResNet-50 with 50 layers deep with 25.6 million parameters. ResNet-101 is 101 layers deep with 44.6 million parameters. ResNet networks can classify the images into up to 1000 categories [42]. The GoogLeNet model helps to improve the use of calculation resources inside the network. Its crafted design allows for increased network depth and width while keeping the computation budget constant. The DenseNet201 model has classified over a million images from the ImageNet database [40].

In the following, various image forgery detection techniques based on transfer learning were discussed. In [2], a deep learning-based method for detecting image splicing was proposed. Initially, the input image was preprocessed using a technique called 'Noiseprint' to obtain the noise residual. Next, the popular ResNet-50 network was employed as a feature extractor. Finally, the obtained features were classified using the SVM classifier. [12] introduced a compelling strategy that harnessed the power of stacked autoencoders (SAE) across diverse image compression scenarios. Notably, pre-trained models were judiciously enlisted to serve as adept image feature extractors. The method ingeniously leveraged the activations derived from the fully connected layers of esteemed CNN models such as VGG16 and AlexNet.

The research by [13] introduced a method for detecting and pinpointing image forgeries, leveraging color illumination and semantic segmentation techniques. The approach incorporated fine-tuned VGG-16 with two distinctive classes, enabling pixel-level classification of images as genuine or manipulated. Furthermore, [40] presented a deep-learning model tailored for image splicing detection. Their process began with grayscale conversion and subsequently applied Total Variation Distance (TVD) analysis to the images. Feature extraction was conducted using three pre-trained CNN models, VGG16, GoogLeNet, and DenseNet201, while classification was achieved through the deployment of three robust classifiers, SVM, naïve Bayes, and KNN.

In [42], a decision fusion system was introduced, employing Residual Exploitation-based CNN models such as ResNet-18, ResNet-50, and ResNet-101 for decision integration. Initially, the pre-trained weights of these models were utilized to assess image tampering. Subsequently, fine-tuned weights were employed to compare the tampering results against the pre-trained model's performance. In [43], two distinct approaches were presented for detecting copy-move forgery using deep learning. Model1 featured a custom-designed architecture, while Model2 harnessed transfer learning with VGG-16. To enhance generalization, the study utilized images from eight diverse open-access datasets. The architecture was trained on one dataset but evaluated across multiple datasets, addressing the challenge of broader applicability in forgery detection.

A multiple image splicing forgery detection method using Mask R-CNN was proposed in [44], with a MobileNet V1 network serving as the lightweight backbone model to extract features from the input image. Depth-wise separable convolution was employed to reduce network capacity. The model reduced network calculation parameters and sped up the detection process without compromising accuracy. In [45], a universal deep learning-based network was introduced, featuring a multimodal system with two steps: initial forgery detection using DCNN (Deep Convolutional Neural Network) followed by part-based image retrieval. InceptionV3 played a pivotal role in extracting essential features.

Meanwhile, in [46], researchers proposed an image splicing detection method based on deep learning, which consisted of three distinct stages: (1) preprocessing involving RGB image conversion and image size adjustment, (2) feature extraction utilizing the pre-trained AlexNet model, and (3) classification where the generated feature representation was leveraged to train a Canonical Correlation Analysis (CCA) classifier for binary classification (authentic/forged). In [47], a blind IFD technique was introduced, which introduced a backbone architecture for deep learning named ResNet-conv used to create the initial feature map for training the Mask-RCNN network. The Mask-RCNN model was employed in conjunction with the ResNet model to extract the initial feature map. Two different ResNet architectures, ResNet-50 and ResNet-101, were explored.

In [48], a feature fusion-based approach was proposed, leveraging both the RGB color space and luminance channels that utilized handcrafted features based on color characteristics and deep features derived from the image's luminance channel to identify patterns conducive. Local binary feature maps were input into the pre-trained ResNet-18 model to generate a 512-D feature vector. The classification process was carried out using a shallow neural network. In [49], an IFD model based on the AlexNet framework was introduced by incorporating batch, and utilizing a softmax activation function in the final layer for classification purposes. Meanwhile, [50] explored two deep learning models, namely, SmallerVGGNet and MobileNetV2, which are resource-efficient frameworks suitable for digital image forgery detection on embedded devices. The modified version of MobileNetV2 is effective in detecting copy-move forgery, especially when dealing with changes in brightness, blurring, and noise, as well as detecting geometric transformations such as cropping and rotation.

In [51], proposed a blind image splicing detection technique employing a deep convolutional residual network architecture as its foundation, that initialized using ImageNet weights and utilized the ResNet-50 architecture for extracting initial image features, with the fully connected layers excluded for classification purposes. [52] introduced an approach that took image batches as input and incorporated YOLO weights into a CNN, using the ResNet50v2 architecture. They conducted a comparative analysis between their proposed system and existing methods for image forgery detection.

A DCT-based multi-task learning network named FBI-Net In [53], a forgery localization method was introduced, utilizing a fully convolutional encoder-decoder architecture with a ResNet-18 backbone. This architecture comprised three encoders with shared parameters. Additionally, a Dilated Frequency Self-Attention Module (DFSAM) was incorporated into the bridge layer to recalibrate the fused features and enhance their representation. In [54], researchers introduced a lightweight model that employed mask R-CNN with MobileNet to detect both copy-move and image-splicing forgeries. They conducted experiments using seven diverse datasets dedicated to copy-move and splicing forgery detection.

[55] presented the Optimal Deep Transfer Learning Copy Move Forgery Detection (ODTLCMFD) technique, which involved a deep learning model for target image classification and an enhanced bird swarm algorithm (EBSA) for classification optimization. The MobileNet model, coupled with a political optimizer (PO), facilitated feature extraction, while least square support vector machine (LS-SVM) model,

employing the Multiclass Support Vector Machine (MSVM) technique, enhanced classification performance. In [56], an approach for detecting copy-move and splicing image forgery was introduced using three distinct CNN models: ELA (Error Level Analysis), VGG16, and VGG19. A preprocessing technique was applied to obtain images at a specific compression rate, which were then used for model training.

Furthermore, [57] presented an automated deep learning-based fusion model, known as DLFM-CMDFC, designed for detecting and localizing copy-move forgeries. This model combined generative adversarial networks (GANs) and densely connected networks (DenseNets). The outputs of these two components were merged within the DLFM-CMDFC framework, creating a layer for encoding input vectors with the initial layer of an extreme learning machine (ELM) classifier. The weight and bias values of the ELM model were fine-tuned using the artificial fish swarm algorithm (AFSA).

## IV. Comparative study for Deep Learning based Techniques and Transfer Learning based Techniques

A comparison between the different image forgery detection techniques based on deep learning is done and concluded in Table 1, taking into consideration the year of publication, the forgery type: (splicing, copy-move, both of them or all image forget types), preprocessing techniques done before extracting the features, feature extraction technique, classification techniques, the dataset used in training and testing the model and the performance evaluation of the used technique. Table 2 illustrates a comparison between the different image forgery detection techniques based on transfer learning with the same considerations taken in the previous comparison shown in Table 1.

Table 1: Comparison between Image Forgery Detection Techniques Based on Deep Learning

| Reference | Forgery Type | Pre-Processing | Feature Extraction Technique | Classification Technique | Dataset | Evaluation |
|---|---|---|---|---|---|---|
| Mohassin Ahmad, 2021, [8] | Splicing, Copy-move, Noise inconsistency, double Compression | Resize the image to 256 x 256, calculate the histogram, compute the standard deviation | (SURF), (DWT), (LVP), (PCA), (HoG), (MBFDF) | (CNN) fine-tuned with (SCFF) | MICC-F220, Columbia, DJPEG, | **Accuracy=** 97.64% |
| Qureshi, 2021, [11] | Splicing + Copy-move | Not Exist | Image Segmentation Model U-Net + L2 regularization | Image Segmentation Model U-Net + L2 regularization | CasiaV2.0 | **F1 score=** 0.9614 |
| Li Haodong, 2021, [14] | Image tampering and localization | Not Exist | Spatial stream + Residual stream | An adapted Mask R-CNN framework | COCO (Training) NIST16, Coverage, CASIAv2, Columbia, IMD2020 (Testing) | **F1-scores=** 0.895 (NIST16) |
| Hussien Nadheer, 2020, [15] | Splicing | Not Exist | CFA + feature reduction + PCA | A deep belief network-based classifier | CISDED | **Precision=** 95.05%, **Recall=** 94.05%, **True Positive rate=** 94.05%, **Accuracy=**98.197% |
| Chao Yang, 2020, [16] | Splicing, copy-move, object removal | Resize the input image | LMFE | Constrained R-CNN + RPN-A | COCO (Training) NIST16, COVERAGE, Columbia (Testing) | **F1-score** is increased by 28.4%, 73.2%, 13.3% on the NIST16, COVERAGE, Columbia |
| Bi Xiuli, 2020, [17] | Splicing | Not Exist | Dual-encoder UNet + spatial pyramid global-feature extraction module | Global insight of D-Unet | CASIA, COLUMB, NIST'16 | **Precision**= 0.96, **Recall**=0.901, **F-score=**0.93 (COLUMB) |
| Liu Xiaohong, 2021, [18] | Splicing, Copy-move, object removal | Not Exist | PSCC-Net (top-down path) | PSCC-Net (bottom-up path) | Columbia, Coverage, CASIA, NIST16, real-world dataset: IMD20 | **AUC=** 99.65, **F1=** 97.12, **EER=** 2.83, **TPR** = 95.65% |
| Yang, Bin, 2020, [19] | Splicing, Copy-move | Not Exist | MDL-CNN | MDL-CNN | BOSSbase 1.01 + laboratory database | **Average accuracy** = 95%. |
| Rao Yuan, 2020, [20] | Splicing | Not Exist | SRM | CNN CRF + SVM | CASIA v2.0, Columbia gray DVMM, DSO-1 | **Accuracy** = 97.5%. |
| Chen Haipeng, 2021, [21] | Splicing, Copy-move, Object removal | Reasonable sampling + divide the image into non-overlapping patches + Use Laplacian filter + (FFT) | LSTM | HFSRNet | NIST16, COVERAGE, CASIA | **Accuracy=** 98.9%, **F1-score=** 0.918, **AUC=** 0.954 |
| Diallo Boubacar, 2020, [22] | Forged image | The image is divided into non-overlapping patches. | CMI | CNN+ clustering algorithm | DIF–CMI | **Accuracy** = 90% |
| MohamedA. Elaskily, 2020, [23] | Copy-Move | Resize the input images without cropping | six CNV layers, each followed by a max-pooling layer | CNN | (MICC-F220, MICC-F2000, MICC-F600) + SATs-130 | **Accuracy=** 100% |
| Ankit Jaiswal, 2021, [24] | Copy-Move | Scale the input images half-sampled multiple times to the dimension of 16 × 16 | CNN (Encoder + decoder) | CNN | CoMoFoD, CMFD | **Accuracy:** CoMoFoD= 98.39%, CMFD= 98.78% |
| Syed Sadaf, 2022, [25] | Splicing + copy move | Image Double compression | Difference between image and recompressed version + CNN | CNN | CASIA v2.0 | **Accuracy=** 92.3% |
| Hosny Khalid M, 2023, [26] | Splicing | Resize the input images to 222 x 222 | CNN | CNN | CASIAv1, CASIAv2, CUISDE | **Accuracy:** CASIAV1=99.1%, |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | CASIAV2=99.3%, CUISDE=100% |
| Fengyong Li, 2022, [27] | Splicing, Copy-Move | Calculate Noise Map | RGB stream + noise stream | End-to-end fully CNN + (TDSA) | NIST16, CASIA, COLUMBIA | **Accuracy:** NIST16=98.4%, COLUMBIA=97.7% |
| Qianwen Li, 2022, [28] | Copy-Move | Image Segmentation | DCNN | SD-Net: (super-BPD) +DCNN: | USCISI, CoMoFoD, CASIAv2 | CoMoFoD: **P**=59.11, **R**=57.69, **F**=50.77 CASIAv2: **P**=57.48, **R**=51.25, **F**=48.06 |
| Saboor Koul, 2022, [29] | Copy-Move | Not Exist | CNN | CNN | MICC-F2000 | **Accuracy**= 97.52% |

Table 2: Comparison between Image Forgery Detection Techniques Based on Transfer Learning in the last four years

| **Reference** | **Forgery Type** | **Pre-Processing** | **Feature extraction Technique** | **Classification Technique** | **Dataset** | **Evaluation** |
|---|---|---|---|---|---|---|
| Tyagi Meena, 2021, [2] | Splicing | Noiseprint | ResNet-50 | SVM | CUISDE | **Accuracy =**97.24%. |
| Bibi Sumaira, 2021, [12] | Every type of forgery and compressed image | Not Exist | AlexNet and VGG16 | The Ensemble Subspace Discriminant classifier | CASIAv1, CASIAv2 | **Accuracy:** JPEG images =95.9% TIFF images= 93.3% |
| Abhishek,2021, [13] | Splicing + Copy-move | Resize Images for VGGnetwork + Semantic segmentation + Color illumination | VGG-16 | VGG-16 | GRIP, DVMM, CMFD, BSDS300 | **Accuracy** = 98%, |
| Almawas Latifa, 2020, [40] | Splicing | Convert images into grayscale + TVD applied | VGG16, GoogLeNet, DenseNet201 | SVM, naïve Bayes, KNN | CASIAv1, CASIAv2 | **Accuracy=** 88.6%, **Sensitivity** = 92.05%, **Specificity=** 85.7% (CASIAv2+ DenesNet201, classified with KNN classifier) |
| Amit Doegar, 2021, [42] | Tampered images with geometrical and transformation attacks | Resize the input image 224 × 224. | ResNet-18, ResNet-50, ResNet-101 | SVM | MICC-F220 | **Accuracy=** 99.09%, |
| Rodriguez-Ortega, 2021, [43] | Copy-move | Not Exist | Model1: Customized CNN Model2: VGG-16 | Model1: Customized CNN Model2: VGG-16 | Coverage, CG-1050v1, CG-1050v2, MICC-F220, MICC-F2000, CMFD, CASIAv1, CASIAv2. | **Accuracy:** Model1=68% Model2=78% |
| Kadam Kalyani, 2021, [44] | Multiple Splicing | Not Exist | MobileNet V1 | Mask R-CNN | MISD (customize database) | **Average Precision=**82% |
| Jabeen Saira, 2021, [45] | Splicing + Copy-move | Not Exist | DNN + InceptionV3 | DNN + InceptionV3 | CASIAv2, CoMoFoD, NIST 2018 | **Accuracy:** CASIA-V2=93.04%, CoMoFoD+CASIA-V2=88.90%, CoMoFoD + CASIA-V2 +NIST 2018=89.01% |
| Taha Ahmed Ismail, 2021, [46] | Splicing | RGB image conversion | AlexNet | CCA classifier | CASIAv1 | **Accuracy=** 98.79% |
| Ahmed Belal, 2020, [47] | Splicing | Use Xavier_normal and He_normal initialization techniques | Mask R-CNN + ResNet-50, ResNet-101 | Mask R-CNN + ResNet-50, ResNet-101 | MISD, CASIAv1, WildWeb, Columbia Gray | **Average Precision**: MISD=82%, CASIAv1=74%, WildWeb=81%, Columbia Gray=86%. **F1-Score**= MISD=67%, CASIAv1=64%, WildWeb=68%, Columbia Gray=61% |
| Savita Wali, 2021, [48] | Splicing | Not Exist | 648-D Markov-based features from the quaternion | Shallow Neural Network | CASIAv1, CASIAv2 | **Accuracy:** CASIAv1=99.3% CASIAv2=97.94% |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | discrete cosine transform of the image + The luminance channel of YCbCr color space used from the Local Binary Pattern of the image + ResNet-18 | | | |
| Samir Soad, 2020, [49] | All image forgery types | Not Exist | AlexNet model by using batch normalization | AlexNet | CASIAv2, CASIAv1, DVMM, NIST | **Accuracy =**98.176% |
| Abbas Muhammad Naveed, 2021, [50] | Copy-move | Resize the input image: SmallerVGGNet 96x96, MobileNetV2 224x224 | SmallerVGGNet, MobileNetV2 | SmallerVGGNet, MobileNetV2 | CoMoFoD, MICC-F2000, CASIAv2 | **Accuracy**: SmallerVGGNet= 87%, MobileNetV2= 85% |
| Souradip Nath, 2021, [51] | Splicing | Not Exist | ResNet-50 | ANN based binary classifier | CASIAv2 | **Accuracy=** 96% |
| Haq Ul, 2022, [52] | Splicing | Divide the images into patches | ResNet50v2+ YOLO weights CNN | ResNet50v2+ YOLO weights CNN | CASIAv1, CASIAv2 | **Accuracy=** 99.3% |
| A-ROM GU, 2022, [53] | Splicing, Copy-move | Apply DCT | DFSAM | ResNet-18 | CASIAv1, CASIAv2, Carvalho, Columbia, Coverage, IMD2020 | **Average of IoU**= 70.99% and **F1-score=** 76.98% |
| Kalyani Dhananjay Kadam, 2022, [54] | Splicing, Copy-move | Not Exist | Mask R-CNN with MobileNet V1 | Mask R-CNN with MobileNet V1 | COVERAGE, CASIAv1, CASIAv2, MICCF220, MICCF600, MICCF2000, COLUMBIA | Copy-move: **F1-score:** MICC F600=70% **Average Precision**: MICC F2000, COVERAGE=90% Splicing: **F1-score:** CASIA1.0=64% **Average Precision**: COLUMBIA=90% |
| Kumar, 2023, [55] | Copy-move | Not Exist | PO + MobileNet | EBSA + LS-SVM | MICC-F220, MICCF-2000, MICC-F600 | **Accuracy**: MICC-F220, MICC-F2000 =98.6%, MICC-F600=98.3% |
| Devjani Mallick, 2022, [56] | Splicing+ Copy-move | Image normalization, resize images 128x128 | ELA | CNN, VGG16, VGG19 | CASIAv2.0 + NC2016 | **Accuracy**: CNN=70.6%, VGG16=71.6%, VGG19=72.9% |
| Krishnaraj N, 2022, [57] | Copy-move | Not Exist | GANs + DenseNet | ELM classifier | MNIST, CIFAR-10 | MNIST: **Precision**=95.42%, **Recall**=95.89%, **Accuracy**=95.42%, **F-score**=95.82%, CIFAR-10: **Precision**=97.27%, **Recall**=96.46%, **Accuracy**=96.94%, **F-score**=96.06%. |

## V. Analyzing the comparison results between Deep Learning based and Transfer Learning based Techniques

Upon analyzing the outcomes of the comparison among research studies conducted from 2020 until the present, focusing on two contemporary image forgery detection techniques, deep learning-based and transfer learning-based approaches, it was evident that a larger number of research studies opted for the utilization of pre-trained models with transfer learning, surpassing those that exclusively employed deep learning methods, as illustrated in Figure 5. This preference can be attributed to the imperative demand for extensive datasets within the realm of image forgery detection for training purposes, a resource that remains limited in availability. Transfer learning effectively solves this challenge, as previously described. Furthermore, the experimental results of these studies prove that by using the pre-trained model, they substantially improved both training and detection times, as they mentioned.

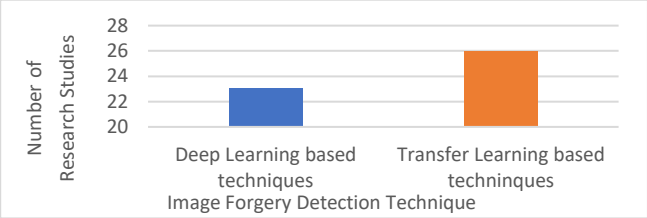


Figure 5: The count of research studies conducted from 2020 to the present on image forgery detection techniques employing deep learning and transfer learning.

After examining the detection accuracy rates achieved by deep learning and transfer learning-based Image Forgery Detection (IFD) techniques, we selected the top ten studies that exhibited the highest detection accuracy rates for both methodologies. Upon calculating the average accuracy, it became evident that both approaches yielded an approximate accuracy rate of around 98%, with only a marginal difference between them. Interestingly, the research studies focusing on transfer learning techniques emphasized their ability to attain not only high accuracy but also low training time, reduced detection time, and minimized computational costs. This observation has led researchers to employ pre-trained models with slight modifications rather than designing new deep-learning models from scratch.

Turning our attention to the specific types of image forgery under investigation, as delineated in Figure 6, we observed that a greater number of studies were dedicated to splicing as opposed to copy-move detection in both techniques. This highlights the need for increased research efforts in the realm of copy-move detection. Furthermore, there is a notable dearth of studies addressing the detection of splicing and copy-move forgery together at the same time, and need more studies.

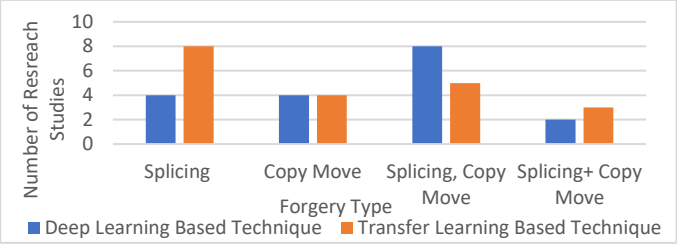


Figure 6: Number of research studies done for each image forgery type from 2020 till now.

Upon a thorough analysis of these research studies, it becomes apparent that the average detection accuracy rate for splicing consistently surpasses that of copy-move in both techniques, as illustrated in Figure 7. This phenomenon can be attributed to the relatively straightforward nature of splicing yields higher accuracy levels. This is because splicing comes from two distinct images introducing noticeable disparities in the properties of the two images rather than copy move which originates from a single source image, resulting in replicated properties throughout that pose a greater challenge for accurate detection.

Furthermore, the detection of splicing and copy-move forgery together affects their detection accuracy rates as depicted in Figure 7. This underscores the need for the development of innovative and refined techniques capable of simultaneously identifying both splicing and copy-move forgeries with a heightened degree of accuracy, mirroring real-life scenarios.

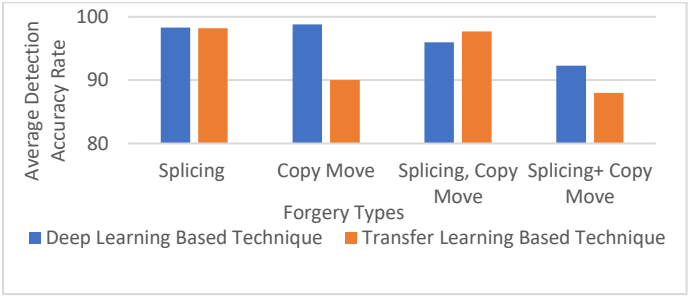


Figure 7: The average detection accuracy rates for each type of forgery in both deep learning-based and transfer learning-based approaches.

In the pursuit of time efficiency with transfer learning-based IFD, various studies adopted different strategies. Some chose to employ the pre-trained model with transfer learning only during the feature extraction phase, while others extended its usage to both feature extraction and classification phases. Figure 8 provides a comparative analysis between these approaches, highlighting that the number of studies utilizing a pre-trained model just for feature extraction was lower than those employing it for both feature extraction and classification.

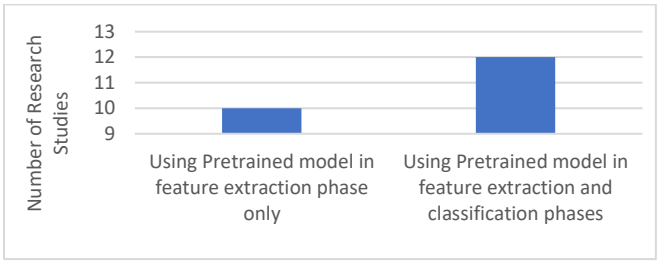


Figure 8: A comparison between the number of studies that exclusively utilized a pre-trained model in the feature extraction phase and those that employed it in both the feature extraction and classification phases.

The studies employing a pre-trained model solely during the feature extraction phase demonstrate a higher average detection accuracy rate in comparison to those utilizing a pre-trained model for both feature extraction and classification phases. This disparity is evident in Figure 9 and has prompted recent research endeavors to consider the use of pre-trained models exclusively for feature extraction while employing alternative classification techniques.

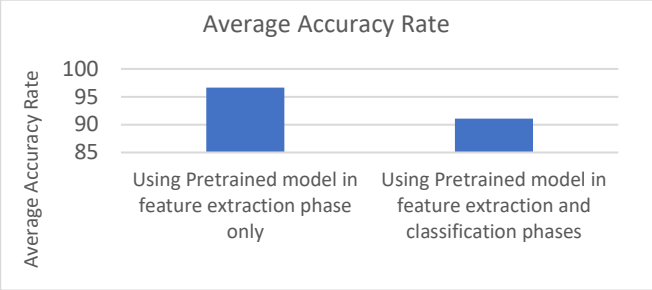


Figure 9: Average detection accuracy rate for studies that used the pre-trained model in the feature extraction phase only compared with others that used the pre-trained model in both feature extraction and classification phases

This divergence in performance may be attributed, in part, to the fact that some of these studies focus on the detection of various forgery types, including copy-move, splicing, combined copy-move and splicing, and facial forgery. As previously demonstrated, these specific forgery types tend to exhibit lower detection accuracy rates, thus impacting the overall average detection accuracy rate.

Therefore, to take advantage of transfer learning and also avoid any overfitting problem, the pre-trained ResNet-50 network is used as a feature extractor, it has a simple and robust architecture [2]. VGG-16 shows good accuracy using a smaller number of epochs [58]. The naïve Bayes classifier provided good specificity with the DenesNet201 model. The KNN classifier achieved the highest accuracy and sensitivity, so it is preferable for detecting authentic images. The high feature dimensionality made the classification task difficult. The best-observed accuracy results for image-splicing detection came from using CASIA v2.0 with DenesNet201 classified with the KNN classifier [40]. Initialization with ImageNet weights provided better results [47]. The utilization of the residual exploitation-based CNN models leads to the reduction of the number of false matches, thereby reducing the false-positive rate and increasing the accuracy of the approach. The fusion-based approach gives more accuracy [42].

## VI. Conclusion

In this paper, various IFD techniques have been surveyed and discussed, and a comparison between deep learning and transfer learning IFD techniques is made. Also, a set of pre-trained models used in transfer learning is mentioned. Multiple tampering operations are performed on the image and the post-processing operations are done to erase the traces left behind by the tampering operation, which makes it more difficult to detect the tampering. In addition, a comparison of different methods for detecting image forgeries is discussed, examining both new deep-learning approaches and techniques utilizing transfer learning with pre-trained models. The goal is to offer insights into the effectiveness of these methods in detecting various types of image forgery. The findings aim to aid researchers in developing models that can accurately detect multiple types of image forgery simultaneously while minimizing detection time.

The results indicate that pre-trained models are best suited for the feature extraction phase only, and can be supported with the traditional feature extraction technique for improving the accuracy, while deep learning is recommended for classification tasks.

In the future, creating a universal model that detects multiple image forgery techniques and overcomes all the constraints and computational complexity is important. Deep learning-based techniques should be designed to develop robust image forgery detectors that can work under different challenging situations and detect the forged videos that may be created by merging several videos. Using reinforcement learning will improve the results.

**References**

[1] K. D. Kadam, S. A., and K. K., "Multiple Image Splicing Dataset (MISD): A Dataset for Multiple Splicing," Data, MDPI, 2021.

[2] Tyagi, K. B. Meena, and Vipin, "A Deep Learning based Method for Image Splicing Detection," Journal of Physics: Conference Series, 2021.

[3] R. Agarwal, O. P. Verma, A. Saini, A. Shaw, and R. Patel, "The Advent of Deep Learning-Based," Innovative Data Communication Technologies and Application, Springer Nature Singapore Pte Ltd. 2021, 2021.

[4] M. A. Elaskily, M. H. Alkinani, A. Sedik, and M. M. Dessouky, "Deep learning based algorithm (ConvLSTM) for Copy Move Forgery Detection," Journal of Intelligent & Fuzzy Systems, 14 September 2021.

[5] A. Mohassin and K. Farida, "Digital Image Forgery Detection Approaches: A Review," Applications of Artificial Intelligence in Engineering, Algorithms for Intelligent Systems, Springer Nature Singapore Pte Ltd. 2021, 2021.

[6] A. Belal, "Detection and localization of forgeries in digital images", A PhD Dissertation Submitted to Electrical and Computer Engineering Department, University of Victoria, 2020.

[7] K. B. Meena and V. Tyagi, "Image Splicing Forgery Detection Techniques: A Review," Springer Nature Switzerland AG 2021, 2021.

[8] F. K. Mohassin Ahmad, "A novel image tamper detection approach by blending forensic tools and optimized CNN: Sealion customized firefly algorithm," Multimedia Tools and Applications, Springer Science+Business Media, LLC, Springer Nature 2021, 29 August 2021.

[9] Ismail Taha Ahmed, B. T. Hammad, and N. Jamil, "A comparative analysis of image copy-move forgery detection algorithms based on hand and machine-crafted features," Indonesian Journal of Electrical Engineering and Computer Science, vol. 22, no. 2, p. pp. 1177~1190, May 2021.

[10] R. Thakur and R. Rohilla, "Recent Advances in Digital Image Manipulation Detection Techniques: A Brief Review," Forensic Science International, Elsevier, 24 April 2020.

[11] Qureshi, M. M. Qureshi, and M. Ghalib, "Image Forgery Detection & Localization Using Regularized U-Net," Springer Nature Singapore Pte Ltd. 2021, 2021.

[12] S. Bibi, A. Abbasi, I. U. Haq, S. W. Baik, and A. Ullah, "Digital Image Forgery Detection Using Deep Autoencoder and CNN Features," Human-centric Computing and Information Sciences, um. Cent. Comput. Inf. Sci. (2021)/, HCIS., 2021.

[13] N. J. Abhishek, "Copy move and splicing forgery detection using deep convolution neural network, and semantic segmentation," Multimedia Tools and Applications (2021), Springer, 2021.

[14] H. Li, X. Chen, P. Zhuang, and B. Li, "Image Tampering Localization Using Unified Two-Stream Features Enhanced with Channel and Spatial Attention," Springer Nature Switzerland AG, 2021.

[15] N. Y. Hussien, R. O. Mahmoud, and H. H. Zayed, "Deep Learning on Digital Image Splicing Detection Using CFA Artifacts," International Journal of Sociotechnology and Knowledge Development (IJSKD), 2020.

[16] Y. Chao, L. Huizhou, L. Fangting, B. Jiang and Z. Hao, "Constrained R-CNN: A General Image Manipulation Detection Model," 2020 IEEE International Conference on Multimedia and Expo (ICME), IEEE, 2020.

[17] X. Bi, Y. Liu, B. Xiao, W. Li, C.-M. Pun, G. Wang, and X. Gao, "D-Unet: A Dual-encoder U-Net for Image Splicing Forgery Detection and Localization," Computer Vision and Pattern Recognition (cs.CV), Cornell University, arXiv, 2020.

[18] X. Liu, Y. Liu, J. Chen and X. Liu, "PSCC-Net: Progressive Spatio-Channel Correlation Network for Image Manipulation Detection and Localization," Computer Vision and Pattern Recognition, Cornell University,arXiv:2103.10596 (cs), 2021.

[19] B. Yang, Z. Li, and T. Zhang, "A real-time image forensics scheme based on multi-domain learning," Journal of Real-Time Image Processing (2020), Springer, 2020.

[20] Y. RAO, J. NI, and H. ZHAO, "Deep Learning Local Descriptor for Image Splicing Detection and Localization," Digital Object Identifier, IEEE Access, 2020.

[21] H. Chen, C. Chang, Z. Shi, and Y. Lyu, "Hybrid features and semantic reinforcement network for image," Multimedia Systems, Springer Nature 2021, 2021.

[22] B. Diallo, T. Urruty, P. Bourdon and C. Fernandez-Maloigne, "Robust forgery detection for compressed images using CNN supervision," Forensic Science International: Reports, ELSEVIER, 2020.

[23] A. E. Mohamed, A. E. Heba, A. Sedik, M. D. Mohamed, E. B. G. M., O. A. Elshakankiry, K. A. A. M., K. A. Heba, S. F. Osama, and A. E.-S. F. E., "A novel deep learning framework for copy-move forgery detection in images," Multimedia Tools and Applications, # Springer Science+Business Media, LLC, part of Springer Nature 2020, Springer, 2020.

[24] Ankit, K. Jaiswal, and S. Rajeev, "Detection of Copy-Move Forgery in Digital Image Using Multi-scale, Multi-stage Deep Learning Model," Neural Processing Letters, part of Springer Nature 2021, Springer, August 2021.

[25] A. Syed Sadaf, G. Iyyakutti Iyappan, V. Ngoc-Son, A. Syed Danish and S. Neetesh, "Image Forgery Detection Using Deep Learning by Recompressing Images," Electronics, MDPI, 2022.

[26] K. M. Hosny, A. M. Mortda, N. A. Lashin and M. M. Fouda, "A New Method to Detect Splicing Image Forgery Using Convolutional Neural Network," Applied Science, MDPI, 2023.

[27] L. Fengyong, P. Zhenjia, W. Weimin, L. Jing, and Q. Chuan, "Image Forgery Detection Using Tamper-Guided Dual Self-Attention Network with Multiresolution Hybrid Feature," Security and Communication Networks, Hindawi, 2022.

[28] L. Qianwen, W. Chengyou, Z. Xiao and Q. Zhiliang, "Image copy-move forgery detection and localization based on super-BPD segmentation and DCNN," Scientific Reports, Scopus, 2022.

[29] Saboor Koul, M. Kumar, S. S. Khurana, and F. Mushtaq, "An efficient approach for copy-move image forgery detection using convolution neural network," Multimedia Tools and Applications, Springer, 2022.

[30] W. H. Khoh, Y. H. Pang, A. B. J. Teoh, and S. Y. Ooi, "In-air hand gesture signature using transfer learning and its forgery attack," Applied Soft Computing, ELSEVIER, 2021.

[31] A. Krizhevsky, I. Sutskever, and Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," In Advances in Neural Information Processing Systems; MIT Press: Cambridge, MA, USA, p. pp. 1097–1105., 2012.

[32] S. Karen and Z. Andrew, "Very Deep Convolutional Networks For Large-Scale Image Recognition," Published as a conference paper at ICLR 2015, arXiv, Cornell University, Computer Science, Computer Vision and Pattern Recognition (cs.CV), 10 Apr 2015.

[33] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," In Proceedings of the IEEE Conference on computer vision and pattern recognition, Las Vegas, NV, USA, p. 770–778, 27–30 June 2016.

[34] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke and A. Rabinovich, "Going deeper with convolutions," In Proceedings of the IEEE Conference on Computer Vision and Pattern, p. pp. 1–9, 7–12 June 2015.

[35] G. Huang, Z. Liu, L. Van Der Maaten and K. Weinberger, "Densely connected convolutional networks," In Proceedings of the IEEE conference on computer vision and pattern recognition, Honolulu, HI, USA, p. pp. 4700–4708, 21–26 July 2017.

[36] F. X. Chollet, "Deep learning with depthwise separable convolutions," In Proceedings of the IEEE conference on computer vision and pattern recognition, Honolulu, HI, USA, p. pp. 1251–1258, 21–26 July 2017.

[37] S. Chopra, R. Hadsell, and Y. LeCun, "Learning a Similarity Metric Discriminatively, with Application to Face Verification," In Proceedings of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05) IEEE Computer Society: Washington, DC, USA, p. pp. 539–546., 2005.

[38] J. Gu, Z. Wang, J. Kuen, L. Ma, A. Shahroudy, B. Shuai, T. Liu, X. Wang, G. Wang, J. Cai, and e. al, "Recent advances in convolutional neural networks," Pattern Recognit, p. 354–377, 2018.

[39] Arora, C. Khushi, and Monika, "Automatic Facial Forgery Detection Using Deep Neural Networks," Advances in Interdisciplinary Engineering: Select Proceedings of FLAME 2020, Springer, 2020.

[40] L. Almawas, A. Alotaibi, and H. Kurdi, "Comparative performance study of classification models for image splicing detection," The 15th International Conference on Future Networks and Communications (FNC) August 9–12, 2020, Leuven, Belgium, ScienceDirect, Procedia Computer Science 175 (2020), ELSEVIER, 2020.

[41] Y. Pengpeng, B. Daniele, R. Ni, Y. Zhao, F. Argenti, and A. Piva, "A Survey of Deep Learning-Based Source Image Forensics," Journal of Imaging, MDPI, 2020.

[42] D. Amit, H. Srinidhi, G. M. Siddesh, K. G. Srinivasa and D. Maitreyee, "Cloud-Based Fusion of Residual Exploitation-Based Convolutional Neural Network Models for Image Tampering Detection in Bioinformatics," BioMed Research International, Hindawi, April 2021.

[43] Y. Rodriguez-Ortega, D. M. Ballesteros and D. Renza, "Copy-Move Forgery Detection (CMFD) Using Deep Learning for Image and Video Forensics," journal of imaging, MDPI, 2021,.

[44] K. KADAM, S. AHIRRAO, K. K., and S. S., "Detection and Localization of Multiple Image Splicing using MobileNet V1," Computer Vision and Pattern Recognition, Cornell University, arXiv, 2021.

[45] S. Jabeen, U. G. Khan, R. Iqbal, M. Mukherjee, and J. Lloret, "A deep multimodal system for provenance filtering with universal forgery detection and localization," Multimedia Tools and Applications (2021), Springer Science+Business Media, LLC, part of Springer Nature, 2021.

[46] A. I. Taha, H. B. Tareq, and J. Norziana, "Effective Deep Features for Image Splicing Detection," 2021 IEEE 11th International Conference on System Engineering and Technology (ICSET), IEEE, pp. 189-193, 6 Nov. 2021.

[47] B. Ahmed, T. A. Gulliver, and S. alZahir, "Image splicing detection usingmask-RCNN," Signal, Image and Video Processing (2020), Springer, 2020.

[48] W. SAVITA, K. KUMAR, K. MUNISH and G. XIAO-ZHI, "Fusion of Handcrafted and Deep Features for Forgery Detection in Digital Images," Digital Object Identifier, IEEE Access, July 2021.

[49] S. Samir, E. Emary, K. El-Sayed and H. Onsi, "Optimization of a Pre-Trained AlexNet Model for Detecting and Localizing Image Forgeries," Information 2020, MDPI, 2020.

[50] M. N. Abbas, M. S. Ansari, M. N. Asghar, N. Kanwal, T. O`Neill and B. Lee, "Lightweight Deep Learning Model for Detection of Copy-move Image Forgery with Post-processed Attacks," 19th World Symposium on Applied Machine Intelligence and Informatics (SAMI) 2021 IEEE, 2021.

[51] R. N. Souradip Nath, "Automated image splicing detection using deep CNN-learned features and ANN-based classifier," Signal, Image and Video Processing (2021), Springer Nature 2021, 2021.

[52] U. Haq, Q. Emad, Z. Tanveer, and A. Abdulrazaq, "Deep Learning-Based Digital Image Forgery Detection System," Applied Science, MDPI, 2022.

[53] G. A-ROM, N. J. U-HYEON, and L. A. SANG-CHUL, "FBI-Net: Frequency-Based Image Forgery Localization via Multitask Learning With Self-Attention," IEEE Access, 2022.

[54] D. K. Kalyani, A. Swati, and K. Ketan, "Efficient Approach towards Detection and Identification of Copy Move and Image Splicing Forgeries Using Mask R-CNN withMobileNet V1," Computational Intelligence and Neuroscience, Hindawi, 2022.

[55] Kumar, C. D. P. Sundaram, and S. Saravana, "Metaheuristics with Optimal Deep Transfer Learning Based Copy-Move Forgery Detection Technique," Intelligent Automation & Soft Computing, Tech Science Press, Scopus, 2023.

[56] M. Devjani, S. Mantasha, G. Anuja, and M. Tabassum, "Copy Move and Splicing Image Forgery Detection using CNN," ICACC, EDP Sciences, 2022.

[57] N. Krishnaraj, B. Sivakumar, K. Ramya, T. Yuvaraja and R. T. and Amruth, "Design of Automated Deep Learning-Based Fusion Model for Copy-Move Image Forgery Detection," Computational Intelligence and Neuroscience, Hindawi, 2022.

[58] Qurat-ul-ain, N. Nida, A. Irtaza and N. Ilyas, "Forged Face Detection using ELA and Deep Learning Techniques,"," 2021 International Bhurban Conference on Applied Sciences and Technologies (IBCAST), pp. pp. 271-275, 2021.

[59] Kaushal, S. G. N. Mohan, and Priyanka, "Passive image forensics using universal techniques: a review," Springer Nature B.V. 2021, 16 July 2021.