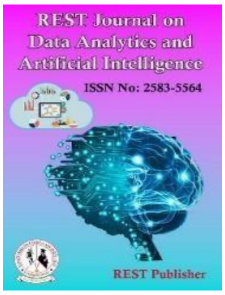
REST Journal on Data Analytics and Artificial Intelligence

Vol: 3(2), June 2024

REST Publisher; ISSN: 2583-5564

Website: http://restpublisher.com/journals/jdaai/

DOI: https://doi.org/10.46632/jdaai/3/2/18



A Comparative Study of Deep Learning and Transfer Learning Approaches for Image Forgery Detection

[*]Kuppampati Sowmya Sri, S.M. Nigar

Gokula Krishna College of Engineering, Andhra Pradesh, India.

**Corresponding author:sowmyasree.siva@gmail.com*

Abstract *- The rapid growth of online activities such as commerce, education, research, and virtual conferences has led to a greater reliance on digital images as primary information sources on social media and other platforms. The extensive use, combined with the ease of modification via image-editing software, highlights the crucial need for effective image forgery detection tools. Traditional detection methods based on handcrafted features have grown less efficient, prompting the introduction of deep learning-based approaches, many of which combine transfer learning with pre-trained models to improve detection efficiency and shorten training time. This research presents a comprehensive evaluation of image forgery detection algorithms, categorizing them as classical, deep learning, and transfer learning frameworks. The study compares deep learning with transfer learning methods, assessing their strengths in feature extraction, classification, and detection accuracy. The findings indicate that, while transfer learning models are particularly effective at feature extraction using pre-trained architectures, deep learning remains superior for classification tasks. This insight intends to help academics construct high-accuracy, efficient models for detecting various forms of forgeries. Combining pre-trained models for feature extraction and deep learning for classification is the best option for real-time digital forensics, increasing detection accuracy and processing speed.*

Keywords: *Image Forgery Detection, Deep Learning Techniques, Image Tampering, Feature Extraction, Public Image Forgery Datasets.*

I. INTRODUCTION

Images are vital across various domains, such as medicine, education, digital forensics, sports, scientific research, and the media, where they function as key sources of information. Nonetheless, the accessibility of advanced editing software like Photoshop, GIMP, and CorelDRAW, in addition to mobile programs like Photo Hacker, has rendered the creation of modified or counterfeit photographs uncomplicated. Verifying the legitimacy of a photograph is essential, particularly when utilized as evidence in judicial proceedings. Image manipulation, defined as any modification of a digital image, includes forgeries techniques that modify an image's content to convey a misleading story. Image tampering, a type of forgerie, alters particular components inside an image—either by duplicating and relocating elements from the same image (copy-move tampering) or by including elements from a different image (image splicing).

Techniques for detecting image forgery are categorized into two main approaches: *active* and *passive*. Active approaches entail incorporating supplementary information, like digital watermarks, during image capture or modification, which subsequently facilitates the identification of alterations. Passive methods, referred to as "blind approaches," identify modifications without depending on embedded information. They examine the intrinsic characteristics of the image to detect indications of alteration. Passive approaches can be further categorized according to the specific sort of forgery they target, including compression, re-sampling, copy-move manipulation, or splicing. Copy-move and splicing forgeries are notably difficult to detect visually, requiring specialized procedures for accurate identification—essential for digital image forensics. In contrast to active approaches such as watermarking, passive methods tend to be more versatile yet pose significant hurdles in detecting manipulation. Various methodologies for identifying image manipulation have been suggested based on these findings, as depicted in Figure 1.

Active (Non-blind) Approaches and Passive (Blind) Approaches are the two main categories into which the Figure 1 shows a classification of several picture forgery detection techniques. These two approaches reflect somewhat distinct ways of spotting picture modification depending on whether they rely on additional embedded data or just examine the intrinsic characteristics of the image. Active (Non-blind) Approaches are methods that utilize auxiliary data that is embedded within an image to aid in the identification of any modifications. Typically, these methods incorporate either Digital Watermarking or Digital Signature. Unique identifiers or watermarks are embedded within the image during the acquisition or editing stage in digital watermarking. One can confirm the image's legitimacy later on by using these markers. Digital signatures are thus cryptographic elements included in the image to enable the authentication and integrity verification. In controlled contexts where integrating this knowledge is practical, active techniques are successful; yet, their relevance is limited by the need for previous intervention during image production or editing.

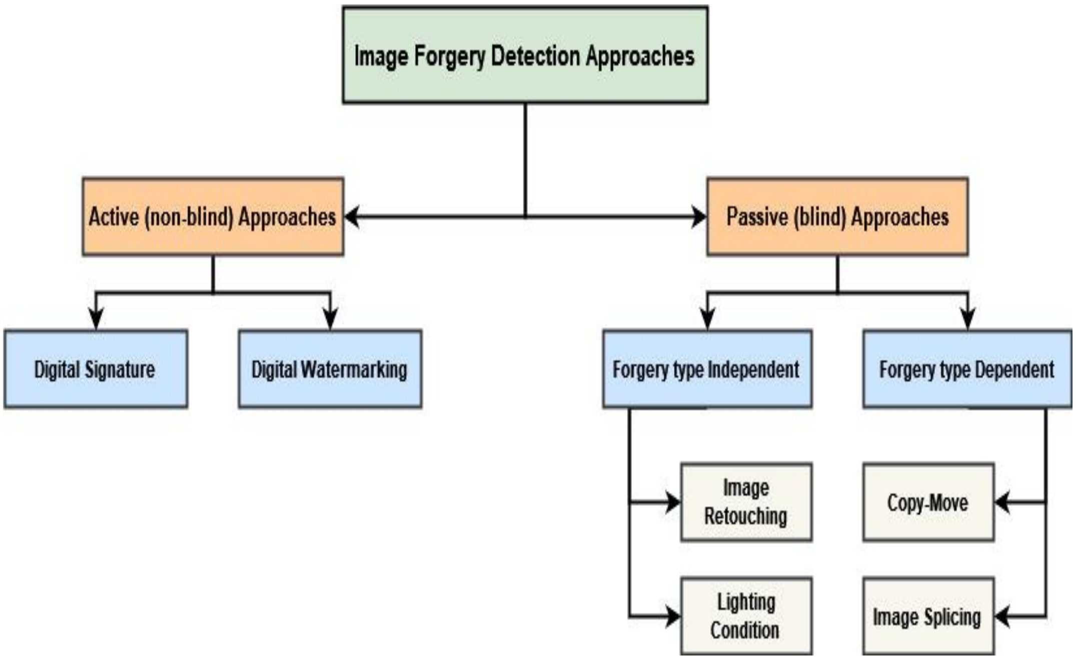


FIGURE 1. Classification of Forgery Detection Techniques (FDT).

Passive, or blind, methods, on the other hand, are more flexible for a wide range of uses especially when working with photos devoid of watermarks or signatures since they depend on no pre-existing embedded information inside the image. Further divisions among passive techniques are forgery-dependent and forgery-type independent ones. Among the particular forms of tampering that underlie forging type-dependent techniques are copy-move and image splicing. While in image splicing parts from several photographs are joined, in copy-move forging sections of an image are replicated within the same image to fool viewers. These methods require various detection strategies that are adapted to the particular characteristics of each type of manipulation.

Passive techniques in the forgery-type independent category are intended to identify alterations that could jeopardize an image's overall visual characteristics without relying on specific modification patterns. Changes in clarity, texture, and colour are frequently identified during image retouching. The Lighting Condition study detects any changes to image illumination due to the potential for modified images to have unusual lighting patterns or shadows. These forgery-type independent approaches assist digital forensics in identifying minor manipulations.

2. DIGITAL IMAGE FORGERY DETECTION STRATEGIES

Digital Image Forgery Detection (IFD) is a binary classification task focused on determining whether an image is forged or authentic. A typical framework for blind or passive IFD follows a structured process comprising several key stages, as outlined in Figure 2.

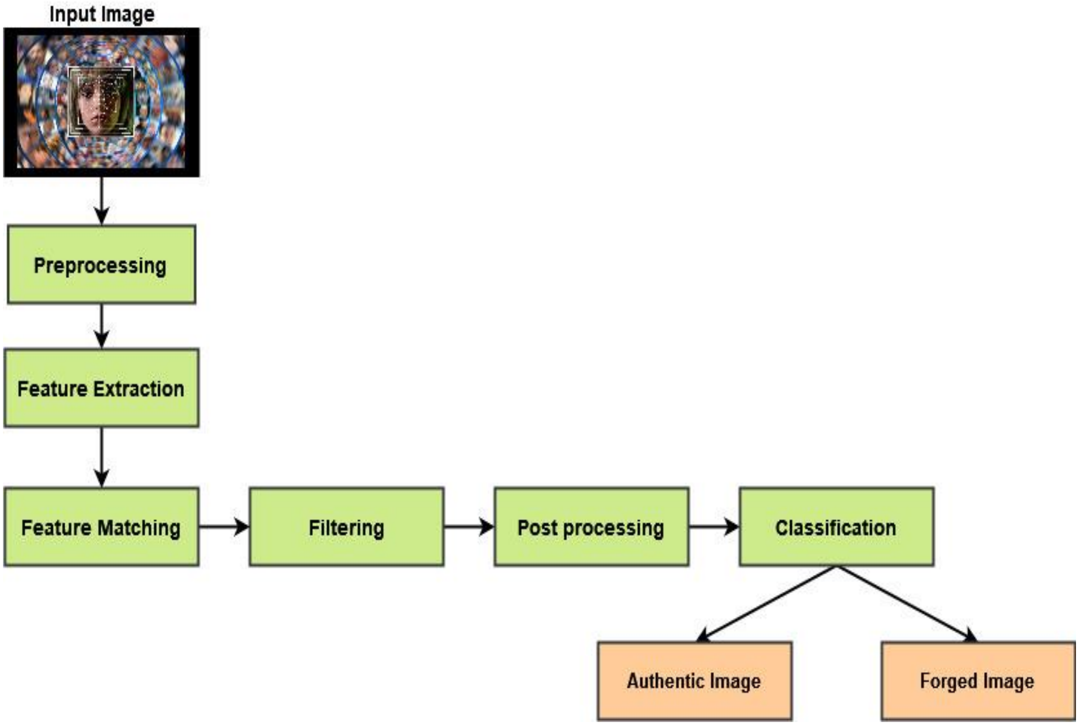


FIGURE 2. Block diagram for IFD

Preprocessing: In this initial phase, various preparatory operations are applied to the image to enhance feature extraction. These may include converting the image from RGB to grayscale, performing histogram equalization, and applying smoothing filters, all aimed at standardizing the image for the subsequent analysis.

Feature Extraction: Next, distinctive features are extracted that can differentiate between authentic and forged images. Informative and manipulation-sensitive features are selected to maximize detection accuracy, ensuring that these characteristics are highly indicative of image tampering.

Feature Matching: During this phase, feature vectors from different regions of the image are compared to identify potential similarities. In block-based methods, for example, rectangular regions are analyzed for matching features, which helps in detecting inconsistencies. This comparison plays a critical role in determining whether the image shows signs of tampering.

Filtering: Not all feature vectors contribute meaningfully to the analysis; some may produce false positives in terms of similarity. Thus, a filtering step is applied to exclude irrelevant feature vector pairs and retain only those that genuinely indicate potential forgery.

Classification: In this step, a trained classifier is used to assign the image to one of the two classes—either forged or authentic. The classifier's decision is based on the previously extracted and filtered features, aiming to accurately distinguish between tampered and genuine images.

Post-processing: After classification, additional analysis can be performed for further insights. For instance, image forgery localization is a post-processing step that highlights specific areas of forgery within the image, providing more detailed information about the tampering after the image has been identified as forged.

Numerous comprehensive reviews of Digital Image Forgery Detection techniques have been conducted, organizing these methods based on the feature extraction and classification techniques they employ. Digital image forgery detection algorithms are broadly categorized into two main groups: Machine Learning Techniques and Deep Learning Techniques, as illustrated in Figure 3.

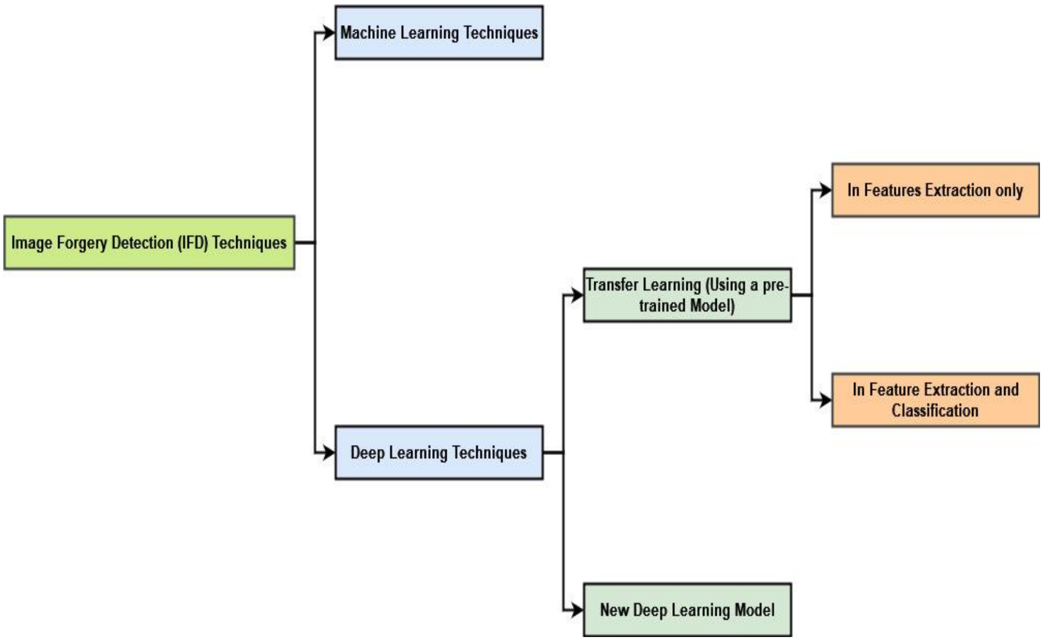

Machine Learning Techniques
Image Forgery Detection (IFD) Techniques
In Features Extraction only
Transfer Learning (Using a pre-trained Model)
In Feature Extraction and Classification
Deep Learning Techniques
New Deep Learning Model

FIGURE 3. Types of IFD

3. CONVENTIONAL TECHNIQUES

Copy-Move Interference Detection entails identifying a region within an image, duplicating it, and repositioning it elsewhere in the same image, resulting in highly linked duplicated portions. The steps for Detection of Copy-Move Tampering in Image is shown in Figure 4. The objective of copy-move detection approaches is to find duplicated regions by examining similarities or distances between characteristics taken from various segments of the image. Researchers employ two methodologies for this detection: (i) segmenting the image into small blocks and extracting features from each block, or (ii) pinpointing keypoints throughout the image and extracting features from each keypoint. By analysing features block-by-block or keypoint-by-keypoint, corresponding pairings can be recognised, validating the existence of duplicated areas and suggesting manipulation. These strategies are efficacious when the duplicated region is sufficiently extensive to encompass many blocks or keypoints, facilitating trustworthy comparison.

Image Fusion Detection, conversely, refers to the process of spotting forgeries in which segments of numerous photographs are amalgamated into a singular composite. In contrast to copy-move forgery, picture splicing does not contain replicated areas within the same image, rendering it more difficult to identify. Detection approaches depend on recognizing indicators left post-tampering, including edge discontinuities, illumination inconsistencies, geometric anomalies, and camera-specific attributes. For instance, edges at the spliced boundaries may appear artificial, or lighting throughout areas may be inconsistent. Researchers such as Johnson and Farid employ techniques to compute illumination trajectories inside a picture; discrepancies in these trajectories may indicate manipulation. Furthermore, when JPEG images are altered and subsequently re-saved, double quantization (DQ) artifacts may manifest as a result of numerous compression processes. Popescu and Farid have devised techniques for identifying double-compressed JPEG photos, so offering additional proof of manipulation.

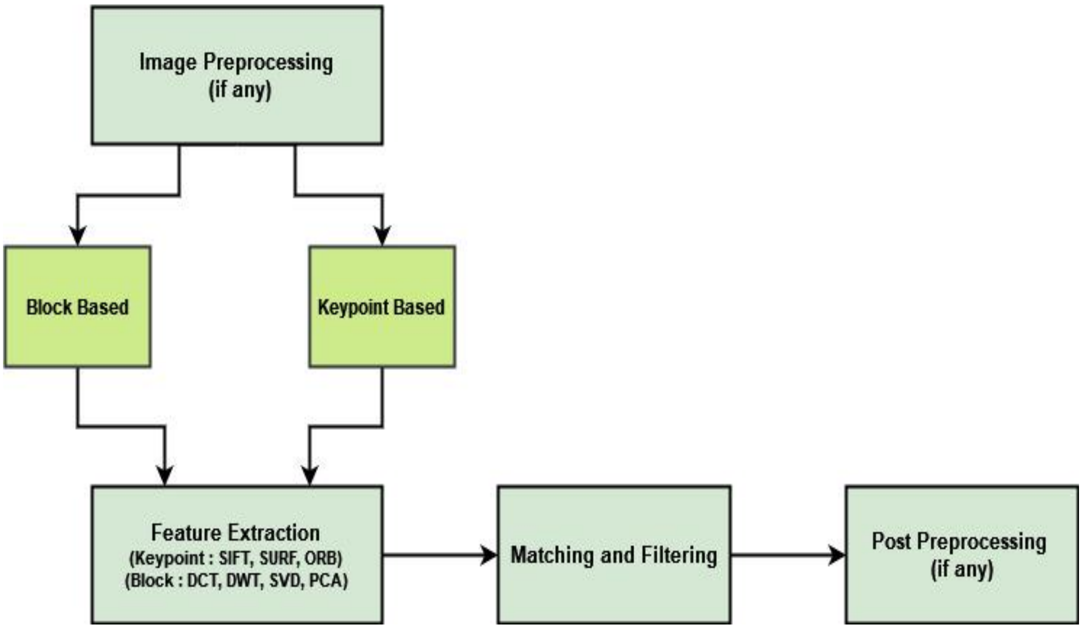


FIGURE 4. Steps in Copy-Move Tampering in Image

4. DEEP LEARNING TECHNIQUES

Techniques for Image Forgery Detection (IFD) based on deep learning markedly diverge from conventional IFD algorithms. In these methodologies, a deep neural network (DNN) is engineered to do both feature extraction and classification inside. The DNN independently collects essential information from input photos and classifies them with high precision, utilising well-initialized weights and optimised network parameters during training. These attributes, referred to as deep learning-based features, are obtained directly from the network layers, thereby obviating the necessity for human feature engineering. In certain cases, handcrafted features are incorporated into the DNN to diminish training duration and improve accuracy, facilitating a more efficient and effective detection process.

In recent years, various new algorithms for image fraud detection have emerged, each with its methodology for detecting manipulated material in digital photos. One such approach is the automatic picture splicing forgery detection scheme described in [10], which makes use of feature extraction based on color filter array analysis. After extracting features, Principal Component Analysis (PCA) is used to minimize dimensionality and improve the detection process' efficiency. Another notable contribution comes from [11], which proposes a constrained R-CNN model for image modification detection. This model employs a coarse-to-fine method, starting with a learnable manipulation feature extractor. The technique performs well in distinguishing modified regions, demonstrating deep learning's ability to deal with complex forgeries. The dual-encoder UNet (D-Unet), described in [12], is a very excellent network for identifying picture splicing forgeries. This architecture incorporates two encoders, one for learning picture fingerprints and distinguishing between tampered and authentic regions, and the other for providing directional information to improve learning and detection capabilities. Another important breakthrough is the Progressive Spatio-Channel Correlation Network (PSCC-Net), announced in [13], which uses a two-path processing method. The top-down path collects both local and global characteristics, whereas the bottom-up path focuses on manipulation detection and mask estimation. This dual-path approach allows for accurate localization of tampered areas in photos [14].

In [15], researchers created the Multi-Domain Learning Convolutional Neural Network, a real-time forensic approach that takes advantage of periodicity patterns in both original and changed photos. This method uses a multi-domain loss function to improve the recognition of deep learning features. In addition, [16] suggested a strategy for detecting and localizing image splicing that combines a CNN-based local feature descriptor with a fully linked conditional random field. This method is supplemented with a novel initialization methodology for the first convolutional layer based on the spatial rich model (SRM), which effectively improves splice localization. Further advancements include the hybrid features and semantic reinforcement network (HFSRNet) reported in [17], which uses encoding-decoding principles, Long Short-Term Memory (LSTM), and rotating residual units to improve detection accuracy. This network also uses semantic reinforcement to help distinguish between tampered and authentic parts. Another effective approach, integrating camera model identification (CMI) and IFD, is proposed in [18]. This CNN-based model is adept at managing typical picture modifications, particularly those found in photographs shared online, after training with a combination of compressed and uncompressed images.

Recent advances in Copy-Move Forgery Detection (CMFD) are illustrated in [19], in which a deep learning strategy uses CNNs to gain hierarchical feature representations for exact tampering detection. [20] introduces a CNN model with multi-scale input and numerous convolutional stages that is organised into encoder and decoder blocks to effectively capture and process features. Other contributions include [21] a lightweight deep learning model for double image compression scenarios, [22] a CNN model for real-time splicing detection, and [23] a comprehensive CNN framework with multiresolution hybrid features. This framework combines RGB and noise streams with a tamper-guided dual self-attention (TDSA) module that directs the network's attention to tampered areas for precise segmentation. Furthermore, in [24], a boundary-to-pixel direction (super-BPD) technique is paired with a deep CNN for copy-move IFD and localisation, which improves edge detection accuracy. A streamlined CNN approach developed in [25] is simple and effective at detecting copy-move forgeries with high accuracy.

These studies illustrate the ongoing progress and diversification of strategies for detecting image forgeries. Each method provides useful insights into maintaining digital picture integrity, with solutions ranging from splicing detection to copy-move forgery detection and localization. As technology advances, these creative approaches strengthen the landscape of digital forensics and contribute to the overarching goal of preserving image authenticity.

5. TRANSFER LEARNING STRATEGIES

The advancements in digital image forgery detection have seen the development of numerous methods leveraging deep learning architectures. In [26], researchers introduced a deep learning-based approach for detecting image splicing, beginning with preprocessing the input image using a technique called 'Noiseprint' to extract noise residuals. Following this, the ResNet-50 model was utilized as a feature extractor, and the extracted features were classified using an SVM classifier. Another notable method, described in [27], employs stacked autoencoders (SAE) across various image compression levels, using pre-trained CNN models like VGG16 and AlexNet to serve as feature extractors. The method capitalizes on the activations from the fully connected layers of these CNN models to enhance detection accuracy.

Research in [28] introduced an image forgery detection technique that combines color illumination and semantic segmentation to achieve pixel-level classification, using a fine-tuned VGG-16 model to classify images as genuine or manipulated. Similarly, a robust model tailored for image splicing detection is presented in [29], where grayscale conversion and Total Variation Distance (TVD) analysis are first applied. Feature extraction is then conducted using VGG16, GoogLeNet, and DenseNet201, and the classification process is carried out with SVM, naïve Bayes, and KNN classifiers. Another method, described in [30], adopts a decision fusion approach using CNN models like ResNet-18, ResNet-50, and ResNet-101. Pre-trained weights are initially used to evaluate image tampering, and fine-tuned weights help in comparing the results, enhancing the model's performance.

In the area of copy-move forgery detection, [31] introduced two distinct approaches. Model1 features a custom-designed architecture, while Model2 uses transfer learning with VGG-16. To address the generalization challenge in forgery detection, the architecture was trained on one dataset and evaluated on multiple others, enhancing its applicability across diverse datasets. Another multiple-image splicing detection method was proposed in [32], which utilizes Mask R-CNN with MobileNet V1 as a lightweight backbone model. Depth-wise separable convolution was used to minimize computational load, improving processing speed without sacrificing accuracy. Additionally, a multimodal deep learning-based network was introduced in [33], utilizing DCNN for initial forgery detection followed by part-based image retrieval, with InceptionV3 playing a critical role in feature extraction.

Further contributions include an image splicing detection technique described in [34], which consists of preprocessing, feature extraction using a pre-trained AlexNet model, and classification via Canonical Correlation Analysis (CCA) for binary classification. In [35], a blind IFD technique employed a ResNet-conv backbone with Mask-RCNN for feature extraction, exploring ResNet-50 and ResNet-101 architectures. Another innovative approach, described in [36], utilizes a feature fusion-based technique combining RGB color space and luminance channels, extracting local binary feature maps and feeding them into ResNet-18 for further analysis. Lastly, an IFD model based on AlexNet with batch processing and softmax activation was introduced in [37], while [38] explored the use of resource-efficient models like SmallerVGGNet and MobileNetV2, which are optimized for forgery detection on embedded devices, particularly in cases involving transformations like brightness changes, blurring, noise, cropping, and rotation.

In [39], a blind image splicing detection technique was introduced, utilizing a deep convolutional residual network architecture based on ResNet-50, initialized with ImageNet weights, and excluding fully connected layers for classification. This approach focuses on extracting essential image features while maintaining a streamlined network structure. Additionally, [40] presented a method that processes image batches and incorporates YOLO weights into a CNN using the ResNet50v2 architecture, allowing for a robust comparative analysis with existing forgery detection techniques. Another significant contribution, the Optimal Deep Transfer Learning Copy Move Forgery Detection (ODTLCMFD) technique, is detailed in [41]. This method employs MobileNet with a political optimizer (PO) for feature extraction and integrates an enhanced bird swarm algorithm (EBSA) for classification optimization, using a least square support vector machine (LS-SVM) with the Multiclass Support Vector Machine (MSVM) approach to boost classification accuracy. Finally, [42] proposed a detection strategy for both copy-move and splicing forgeries by using three CNN models: Error Level Analysis (ELA), VGG16, and VGG19, where preprocessing at a specific compression rate helped to optimize model training.

Comparison of DLand TL methods

Traditional Convolutional Neural Networks (CNN) and transfer learning are distinguished by their respective data requirements, learning processes, and knowledge transfer. Figure 5 demonstrates the distinctions between the two. The Traditional CNN approach commences with a substantial dataset from Domain A on the left. The model is capable of capturing intricate patterns and features that are unique to the dataset by undergoing a comprehensive learning process on this extensive dataset. The model accurately classifies images within the same domain by utilizing the learned features it has acquired after training. Computationally intensive and time-consuming to train, conventional CNNs necessitate substantial quantities of data for effective learning.

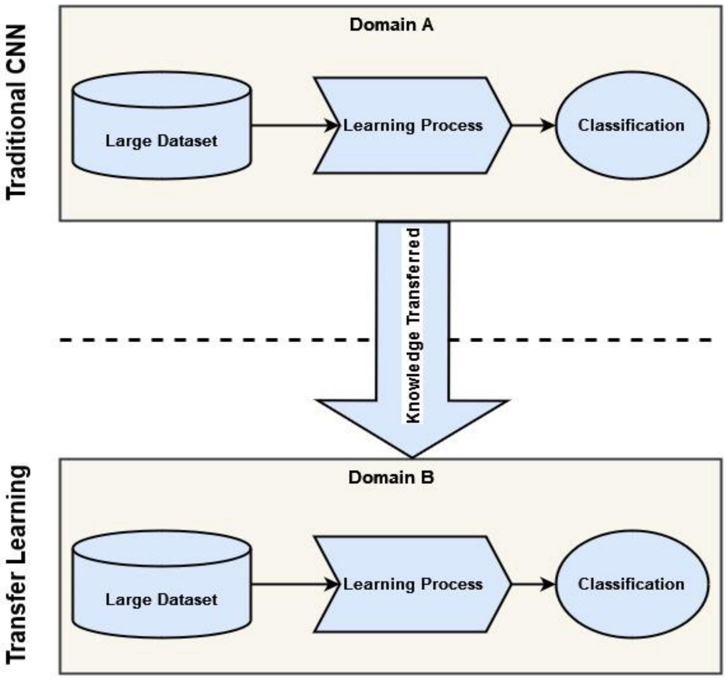


FIGURE 5. DL Vs TL

The Transfer Learning approach, depicted on the right, resolves the issue of inadequate data availability by repurposing knowledge acquired in a distinct field. Initially, a CNN model is trained on a large dataset from Domain A and subsequently applied to a new task in Domain B, which has a small dataset. The knowledge acquired in Domain A is transferred, thereby reducing the necessity for exhaustive training on the smaller dataset of Domain B. This transfer of knowledge enables the model to classify data in Domain B with increased accuracy and reduced training time by utilising the features that have been previously acquired, rather than starting from blank. This method is particularly advantageous in scenarios where the acquisition of substantial labeled datasets is either challenging or expensive. In digital image forgery detection, deep learning and transfer learning algorithms exhibit significant potential, each with distinct strengths and applications. Deep learning techniques depend on extensive neural network designs, like CNNs and bespoke models, engineered to autonomously extract characteristics from photos and identify alterations. Methods such as D-Unet for splicing detection [43], the Progressive Spatio-Channel Correlation Network (PSCC-Net) for localization [44], and multi-domain learning convolutional neural networks [45] illustrate deep learning's ability to manage intricate feature extraction and classification within a unified framework. Deep learning algorithms, through the acquisition of hierarchical features, excel at collecting complex subtleties frequently overlooked by conventional, handmade features. These methods are predominantly end-to-end, necessitating solely labelled data and an appropriate network architecture for optimal operation.

Conversely, transfer learning techniques utilize pre-trained models, typically initialized on extensive datasets such as ImageNet, which are subsequently refined for the specific objective of forgery detection. Examples include employing ResNet-50 for splicing detection following Noiseprint preprocessing [46] and utilizing VGG16 for detecting pixel-level manipulations [47]. Transfer learning can markedly decrease the time and computer resources needed for training, as these models inherently include general image properties. Methods such as Optimal Deep Transfer Learning Copy Move Forgery Detection (ODTLCMFD) [48] and the incorporation of pre-trained YOLO weights into a CNN utilizing ResNet50v2 architecture [49] highlight the adaptability of transfer learning for particular forgery detection applications. Transfer learning methods utilize features from extensive datasets to facilitate quicker convergence, frequently requiring a smaller sample, therefore proving invaluable in data-scarce situations.

Both strategies encounter challenges and limitations. Deep learning methodologies sometimes necessitate extensive, annotated datasets for optimal performance, which can be challenging to get in the realm of counterfeit detection. They are computationally demanding, necessitating substantial processing power for training. Moreover, these approaches may encounter difficulties with generalization, since they are prone to overfitting the specific training dataset, hence constraining their efficacy on novel or unencountered forging types. Transfer learning mitigates certain challenges by minimizing data requirements; nonetheless, it continues to encounter problems in adapting pre-trained models to the domain-specific characteristics inherent to forgeries. Some counterfeit artifacts may be insufficiently represented in broad datasets like ImageNet, resulting in unsatisfactory feature extraction for sophisticated operations such as splicing or copy-move forgeries. Moreover, transfer learning models frequently necessitate meticulous adjustment to prevent the transfer of extraneous information from the source domain, potentially resulting in suboptimal performance.

Both deep learning and transfer learning methodologies encounter difficulties in identifying subtle forgeries or those that include intricate alterations, such as geometric distortions and fluctuating lighting conditions. Ensuring effective detection across various compression levels, image formats, and noise levels continues to be a prevalent challenge. Resolving these problems will probably necessitate hybrid models that integrate the feature extraction capabilities of deep learning with the efficiency of transfer learning, alongside additional study into dataset augmentation and the refinement of model architectures to enhance generalization and detection accuracy.

6. CONCLUSION

This survey paper provides a comprehensive overview of digital image forgery detection techniques, offering a classification of forgery methods and a detailed examination of various approaches used in detecting image tampering. Starting with traditional techniques, which rely on handcrafted features and are often limited to specific types of manipulations, we discussed how these methods laid the foundation for more advanced techniques. The review then shifts to deep learning-based methods, which leverage neural networks to autonomously extract and classify complex features within images, demonstrating higher accuracy and adaptability across various types of forgeries, including copy-move and splicing. The paper also highlights the emerging role of transfer learning approaches, where pre-trained models are adapted to the forgery detection domain. By using pre-trained architectures such as ResNet, VGG, and MobileNet, transfer learning enables faster model convergence and reduces data requirements, making it suitable for scenarios with limited labeled forgery data. This paper contrasts deep learning and transfer learning methods, emphasizing that while deep learning excels in capturing complex features directly from data, transfer learning offers efficiency by leveraging knowledge from general-purpose datasets. The strengths and limitations of each approach were analyzed, demonstrating that both methods offer unique advantages in digital forensics but face challenges with generalization, data requirements, and computational costs.

Finally, this survey identifies common challenges in digital image forgery detection, such as handling diverse manipulation types, ensuring robustness across different image qualities, and improving detection accuracy under limited data availability. Moving forward, there is a need for hybrid models that can combine the adaptability of deep learning with the efficiency of transfer learning, along with expanded, high-quality datasets that represent a broader range of forgery types. The findings of this paper contribute to a better understanding of the current landscape in forgery detection, providing a foundation for future advancements in preserving the authenticity and integrity of digital images.

REFERENCES

[1]. Zanardelli, Marcello, et al. "Image forgery detection: a survey of recent deep-learning approaches." Multimedia Tools and Applications 82.12 (2023): 17521-17566.

[2]. Guo, Xiao, et al. "Hierarchical fine-grained image forgery detection and localization." Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2023.

[3]. Guillaro, Fabrizio, et al. "Trufor: Leveraging all-round clues for trustworthy image forgery detection and localization." Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2023.

[4]. Zeng, Nianyin, et al. "DPMSN: A dual-pathway multiscale network for image forgery detection." IEEE Transactions on Industrial Informatics (2024).

[5]. Khalil, Ashgan H., et al. "Enhancing digital image forgery detection using transfer learning." IEEE Access 11 (2023): 91583-91594.

[6]. Sharma, Preeti, Manoj Kumar, and Hitesh Sharma. "Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: an evaluation." Multimedia Tools and Applications 82.12 (2023): 18117-18150.

[7]. Maashi, Mashael, et al. "Modelling of Reptile Search Algorithm with Deep Learning Approach for Copy Move Image Forgery Detection." IEEE Access (2023).

[8]. Zhu, Jiaying, et al. "Learning Discriminative Noise Guidance for Image Forgery Detection and Localization." Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 38. No. 7. 2024.

[9]. Pham, Nam Thanh, and Chun-Su Park. "Toward deep-learning-based methods in image forgery detection: A survey." IEEE Access 11 (2023): 11224-11237.

[10]. 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

[11]. 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.

[12]. 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 andLocalization," Computer Vision and Pattern Recognition (cs.CV),Cornell University, arXiv, 2020.

[13]. 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.

[14]. Yu, Zeqin, et al. "DiffForensics: Leveraging Diffusion Prior to Image Forgery Detection and Localization." Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2024.

[15]. 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.

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

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

[18]. 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.

[19]. 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.

[20]. 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.

[21]. 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.

[22]. 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.

[23]. 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

[24]. 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.

[25]. 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.

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

[27]. 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.

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

[29]. 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

[30]. 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.

[31]. 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,

[32]. 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

[33]. 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.

[34]. 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

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

[36]. 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

[37]. 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

[38]. 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.

[39]. 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.

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

[41]. 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

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

[43]. 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.

[44]. 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.

[45]. 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.

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

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

[48]. 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.

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