Bilad Alrafidain Journal for Engineering Science and Technology
https://doi.org/10.56990/bajest/2025.040112
ISSN: 2073-9524
Pages:137-154

Copy-Move Image Forgery Detection Using Deep Learning Approaches: An Abbreviated Survey

Zainab Shawkat Ibrahim[1], Taha Mohammed Hasan[2*]
[1,2] Department of Computer Science, College of Science, University of Diyala, Iraq, 32001
scicompms222303@uodiyala.edu.iq[1], dr.tahamh@uodiyala.edu.iq [2]

Abstract
Images play a fundamental role in digital media, and altering digital images can present a significant risk since it contributes to disseminating false information. The rapid advancement of technology in digital image forensics has significantly improved the quality of forged images to the extent that many forgeries are now indistinguishable. Digital image authenticity and reliability are becoming more significant as evidence. Some people invalidate photos by adding or removing sections. Therefore, image forgery detection and localization are crucial. Image manipulation techniques have made this a major computer vision issue. Images can be obtained from many origins and may appear in multiple formats. Consequently, passive techniques for detecting image forgeries are generally favored, which do not necessitate prior knowledge about an image. The prevalent forms of passive image forgery detection encompass the identification of copy-move and image-splicing forgeries. Recently, deep learning techniques have become prevalent in image manipulation detection. These techniques demonstrated superior accuracy to traditional approaches due to their ability to extract features from images effectively. This study comprehensively examines deep learning methodologies utilized in detecting copy-move forgery, and it has mostly focused on studies conducted in recent years, and data sets commonly used in detecting copy-move forgery have been mentioned. This abbreviated survey concluded that combining conventional image processing methods with pre-trained CNN approaches could leverage the strength of both, exhibit significant efficiency, and decrease the requirement for labeled image datasets. Furthermore, utilizing ensemble techniques to integrate multiple approaches improves overall forgery detection performance.

Keywords: Passive approach, Digital image, Copy-move forgery, Deep learning, CNN.

Article history: ***Received:*** *31 Jul 2024;* ***Accepted:*** *29 Aug 2024;* ***Published:*** *15 Mar 2025*

1. Introduction

The development of powerful picture editing and processing technologies has made it simple and visually invisible to manipulate digital photos. When a phony image cannot be recognized from a real one by visual inspection, certain legitimate problems could arise. It poses many difficulties for media forensics [1]. Digital photographs provide crucial evidence in various industries, including forensic inquiry, criminal investigation, intelligence systems, medical imaging, insurance claims, and media. This highlights the significance of maintaining and determining the legitimacy of the image. Image forgery detection systems are becoming increasingly important in [2], as a result, maintaining the integrity and authenticity of digital photographs has grown difficult and is no longer a given. Digital photographs without forensic investigation are not admissible as evidence in a court of law [3].

* Corresponding author: dr.tahamh@uodiyala.edu.iq

ISSN: 2073-9524
Pages:137-154

Image manipulation is a technique used to counterfeit photos to hide information. In general, there are two types of image forgery detection techniques: active and passive image forgery [4] and [5]. Fig. 1 shows the further classification of both types. In an active image integrity technique, the user adds data to the image, which is then removed at the recipient's end to verify the accuracy of the data [6], in this approach, a computerized watermark or signature is added to an image; this can be done manually or automatically by the acquisition device. With digital watermarking, certain data, known as a message digest, is inserted into the image while it is being captured. Later stages of the process remove this data from the image to verify its legitimacy. This extracted data is examined to determine whether it changes; if it does, this indicates that the image was edited after the image capture process. The first stage of the two-phase method involves embedding the message digest in the image. The message digest is retrieved and compared with the acquired watermark in the second stage, which occurs after the image has arrived at its destination [7].

Passive approach Image forgery detection, often called a blind approach, is frequently difficult in image processing. The stream-of-passive approach analyses an image's contents and structure to confirm its reliability or authenticity without any embedded signatures or watermarks [3]. The most prevalent passive approaches are copy-move forgery, image splicing forgery, and retouching forgery [5], as mentioned in Fig. 1. A portion of a picture is duplicated and moved about within the same image, called the copy move. Combining two or more photos to create a new image is called splicing [8]; retouching a photograph includes changing the lighting, blurring, and texture. Fashion photography and many other commercial applications employ image retouching [9].

This paper offers an abbreviated survey of deep learning-based copy-move image forgery detection. The fundamental contributions of this survey are as follows:

1. Presenting a review of the recently used deep learning methodologies, especially CNNs, and stating their effectiveness in detecting copy-move forgery in digital images.
2. Providing an abbreviated and effortless explanation of state-of-the-art works concerning copy-move image forgery detection using CNNs in the last five years (from 2019 to 2023).
3. Analyzing the details of the implemented techniques, datasets, and the results of covered works.
4. Presenting the most commonly utilized datasets in the field of digital image forensics.

The structure of this study is as follows: Section 2 discusses deep learning methods. Section 3 discusses copy-move forgery based on deep learning. Section 4 discusses a comparative study of copy-move forgery detection approaches. Section 5 presents commonly available datasets. Section 6 presents a discussion. Section 7 presents an analysis of image forgery datasets. Finally, Section 8 concludes the work.

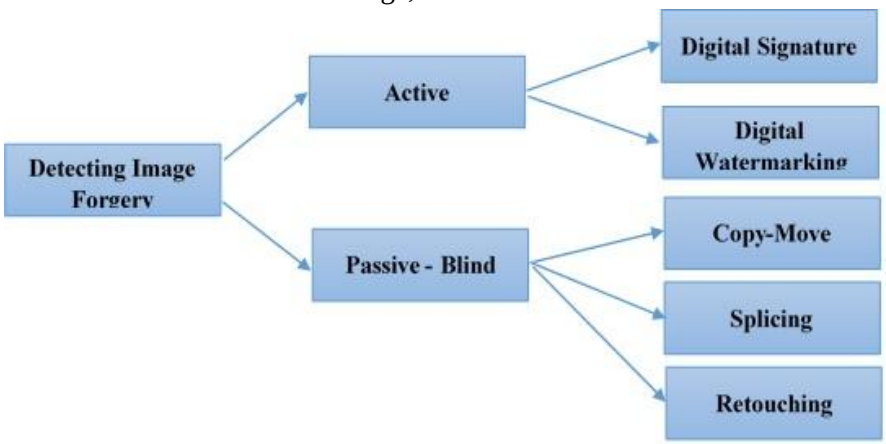

Fig. 1 Image forgery detection techniques.

ISSN: 2073-9524
Pages:137-154

2. Deep Learning Methodologies

Deep learning (DL) methodologies have become widely employed across several domains of study due to their inherent capacity to autonomously acquire features and attain notable levels of accuracy in classification tasks.

In the work of Thakur and Rohilla [10], Deep Learning has several models, including Convolutional Neural Networks (CNN), Deep Neural Networks (DNN), and Recurrent Neural Networks (RNN). Among these models, CNN is the most frequently used deep learning model. The convolutional layer of CNN functions as a discriminator and an extractor [11]. Quick developments in computing capabilities, including processor power, memory space, and power consumption, have improved the efficiency and cost-effectiveness of computer vision applications. DL improves image classification, semantic segmentation, and object recognition for computer vision researchers [8].

DL-based techniques have gained significant importance in the contemporary environment. Several early studies, inspired by the success of residual-based machine learning methods, proposed CNN architectures that were designed to extract residual feature patterns [11]. CNNs currently have deeper layers of neurons for analyzing more complicated information. CNN and deep learning's biggest benefit is that they can automatically learn relevant features, which is harder than feature building. Today, computer vision and digital image processing employ CNN and deep learning [12].

The CNN architecture has many layers, including the convolutional, max-pooling, flattening, and complete connection layers.

- The convolutional layer: The first layer of the CNN architecture is responsible for extracting features from the input image. Typically, the earliest layers of a neural network are responsible for extracting low-level features, such as edges, lines, and corners. Conversely, the last layers of the network are designed to extract high-level features, such as forms. The present layer does convolution operations on the input data by using sliding windows referred to as filters. Each layer produces a feature map. Filters link local locations in CNN networks. Thus, each first hidden layer neuron is coupled to a tiny input neuron region. Every layer's input is filtered, and the feature map's depth equals the number of filters. Filters and weight sharing lower CNN training parameters [13].
- Max-pooling layer: CNN networks commonly include a pooling layer after each convolution layer. This layer shrinks feature maps. Therefore, it decreases the number of parameters to learn and network calculation. The layer's most used functions are maximum and average. Maximum pooling sends the biggest pixel in each window to the output, whereas average pooling sends the average of the pixels in the window. The output depth matches the input depth in the pooling layer, which applies to all input depths [13].
- Fully connected layer: One or more completely linked levels finish the CNN network. A completely linked layer links all neurons in the preceding and next layers. In reality, this layer scores network output [13].

3. Copy-Move Forgery Detection Based on Deep Learning

Copy-move forgery is a frequently employed and relatively simple method of tampering with images. This technique involves duplicating an image's specific region, known as the source region, as shown in Fig. 2. The duplicated region is then subjected to various preprocessing techniques such as scaling, rotating, or colour adjustment. Ultimately, the altered region is pasted onto another region, the target region, within the same image [14]. This specific type of forgery presents significant challenges in terms of detection. Typically, this attack has two general objectives: 1) concealing certain events or regions inside the image and 2) augmenting the number of entities inside the image to amplify an occurrence lacking substantial significance [15].

The copy-move forgery detection (CMFD) involves hand-crafted features and machine-crafted (deep learning). The former may be categorized into three primary approaches: block-based, keypoint-

ISSN: 2073-9524
Pages:137-154

based, and hybrid. Block-based techniques employ several methods for feature extraction, such as the Fourier transform and DCT (Discrete Cosine Transform). A keypoint-based approach such as SIFT (Scale Invariant Feature Transform) and SURF (Speed-UP Robust Features) [16].

The performance of conventional CMFD approaches is generally adequate. Nevertheless, their 1) capacity to deal with assaults is limited, 2) A high computational cost afflicts the methods above, 3) the ability to handle specific types of forgeries is limited, and 4) the inability to identify many fake areas at once [15].

The second deep learning-based approach can immediately acquire and enhance the hierarchical feature representations to detect image fakes [17]. In a deep learning model, the network layer receives images directly and automatically learns features from the image content. However, when it comes to detecting image tampering, the focus shifts from learning content-based characteristics to learning and using the traces that remain after the tampering operation has been conducted on the image. These traces are then used to categorize the image as legitimate or tampered with [10].

Fig. 2 Copy-Move forgery, (left side) forged image, and (right side) original image.

4. Comparative Analysis

This section primarily discusses the methodologies employed in prior studies for identifying copy-move fraud in photos by utilizing deep learning algorithms. Additionally, the dataset employed in this research is described, and the accuracy metrics achieved in each study are outlined. Table 1 displays the results of the survey of approaches for detecting forgeries that are based on DL.

Agarwal et al. [18] proposed Deep learning for detecting copy-move forgery. This system divides the input image into patches based on colour similarity during pre-processing. Simple Linear Iterative Clustering (SLIC) segments the input image and extracts features from segmented patches for processing. The author used VGGNet (Visual Geometry Group-net) to extract multi-scale features from segmented patches. VGGNet extracts features to identify copied regions regardless of whether they are rotated, scaled, or compressed. Finally, the depth

ISSN: 2073-9524
Pages:137-154

of each patch pixel is recreated after feature extraction for block comparison. This is done through adaptive patch-matching. Each segmented patch is compared. Most suspected tampered areas are detected during this comparison, and the matching key locations are combined with host image segmented patches. It shows the input images' forged regions. It outputs the modified area after identifying it. The suggested deep learning-based method has the potential to reduce computing time and improve the accuracy of detecting duplicated areas.

Abdalla et al. [19] proposed an end-to-end deep learning CNN for a copy-move forgery detection approach. Input, convolutional, fully connected, classification, and output layers comprise the proposed CNN, each with various convolutional filters. This approach increases feature extraction in copy-move forgery detection models, which improves speed. CNN learning capabilities increase output outcomes, therefore increasing input samples and training cycle improves them. CNNs detect copy-move forgeries cheaply than traditional methods. Finally, CNN may employ several input images, improving model accuracy.

Thakur and Rohilla [10] introduced an approach for detecting splicing and copy-move forgeries. This strategy uses the median filter residual of the second order and the Laplacian filter residual (LFR) as combined input to CNN architecture, which draws inspiration from VGGNet. This CNN aims to categorize images as either legitimate or tampered with accurately. Before being inputted into the convolutional neural network, the image undergoes a pre-processing stage. In the preprocessing stage, the images undergo a resizing operation to dimensions of 128x128. Also, they are converted to grayscale before calculating their filtering residuals. The experimental outcomes demonstrate the efficacy of the suggested methodology and give a much higher level of accuracy when compared to many other approaches.

Abdalla et al. [20] presented a deep convolutional and adversarial fusion processing model for copy forgery detection. The network was created with a two-branch and a merge-unit design. CNN and generative adversarial networks (GAN) are used in the two branches to effectively localize and identify copy and transfer forgery regions. After conducting experiments on data sets, the results showed the effectiveness of the proposed model for localizing the forgery area and detecting tampering. Moreover, it is worth noting the ability of the proposed technique to generalize its outputs to forgeries of different sizes than those taken into account during the training steps.

Muzaffer and Ulutas [21], the authors proposed a deep learning architecture for identifying and localizing copy-move, replacing conventional feature extraction methods. The methodology utilizes the pre-trained AlexNet convolutional neural network to extract features from sub-blocks of the image. Subsequently, the process of matching them is executed, followed by the subsequent removal of erroneous matches.

Kuznetsov [22], the author proposed developing a CNN model to effectively identify and accurately localize counterfeit instances within images of remote sensing data. The neural network model incorporates sliding windows of varying sizes in this methodology to generate feature maps. These feature maps are then used for localization. The suggested designs provide superior quality values compared to other methodologies, yet there is a need for improvement in terms of computation speed.

Thakur and Jindal [23] used a method for detecting CMF and splicing forgery in images by a hybrid approach that combines copy-move and splicing forgery detection techniques. The suggested method employs a machine learning-based colour illumination approach. A deep convolutional neural network (DCNN) is utilized to distinguish between authentic and manipulated images. The deep neural network (DNN) is evaluated utilizing a minimal image batch size. The last step uses a machine learning technique based on colour lighting to recognize cases of passive forgery within publicly available datasets. Two processes are involved in this process, namely, the categorization of images and the identification of the manipulated area. The proposed technique shows superior performance over all datasets.

ISSN: 2073-9524
Pages:137-154

Elaskily et al. [24], the authors utilized a methodology for identifying Copy_move Forgery (CMF) by utilizing deep learning techniques. The suggested model uses a Convolutional Neural Network (CNN) with Convolutional Long Short-Term Memory (CovLSTM) networks. The proposed approach involves extracting features of the image using a series of Convolutional (CNVs) layers, ConvLSTM layers, and pooling layers. These extracted features are then used for feature conformability and the detection of copy-move forgeries. This model has been utilized on four existing datasets, which have been merged to make novel datasets that serve the purpose of generalization experiments and address the issue of overfitting. The method achieves a high level of accuracy, gaining 100% when using a total of 100 epochs.

Singhal and Ranga [6], proposed a model's primary emphasis on identifying copy-move forgery and splicing forgery which employs four consecutive convolution and pooling layers, each with different parameters. In the CNN architecture, a filter is used on every convolutional layer, and each layer is started with specific weights and a bias. The proposed model includes a hidden layer after four convolutional layers and a pooling layer. Ultimately, an output layer is utilized for decision-making processes. Also, the issue of overfitting was addressed by including a dropout layer between the hidden layer and the output layer. There is still a long way to go in this area, and much more research can be done to discover better algorithms that detect forged images efficiently.

Abbas et al. [25] introduced centers on conducting experiments with two cutting-edge deep learning models: Some of the commonly used architectures are SmallerVGGNet (derived from VGGNet) and MobileNetV2. That means the SVGGNet CNN framework was built as an improved version of the VGGNet architecture to be used for specific tasks. The first and primary planned goal was to solve the problem of time and resources taken by a heavyweight and a deep model. Further was the objective of creating a CNN framework that corresponds to the nature of a focused deep learning model. MobileNetV2, created for devices with little memory, is a (CNN) that integrates depth-wise separable convolutions. This approach permits the formation of a lightweight CNN that is acceptable for embedded tools and systems. The researchers employed a method known as fine-tuning. This included creating a new fully connected (FC) layer, denoted as the model head, and exchanging the previously trained FC layer with it. In terms of accuracy and TPR measures, the SVGGNet and MobileNetV2 models were performance similarly. Therefore, in a resource-limited setting, the submitted adaptation of the MobileNetV2 model for networks is an effective solution that is both computationally efficient and dependable while also arriving at high levels of accuracy for the intended objective.

Rao et al. [26], the authors suggested image fraud detection and localization techniques. They proposed an attention model using a conditional random field (CRF) to characterize local correlation among neighboring pixels to detect forged and real image borders. The proposed attention model generates attention maps from receptive fields at different dimensions using four attention modules with varying semantics. The created attention maps reduce noise and emphasize valuable areas by multiplying the input feature element-wise, helping the network extract more discriminative and generalizable features around fabricated borders. They create a forgery forensic technique using Atrous spatial pyramid pooling (ASPP) to construct a fine-grained tampering probability map for detection and localization. The suggested approach's greater generalization is shown by extensive experimentation on many public datasets.

Liang et al. [27] suggested a network called Pyramid Correlation Network (PCNet) to detect copy-move forgeries. The primary objective of this network is to acquire a comprehensive and detailed representation of images via the use of a pyramid-cascaded correlation architecture. The PCNet model demonstrates commendable performance in the detection of large-region tampering samples, as well as exceptional performance in detecting small-region or medium-region tampering samples, but this model suffers from computational complexity.

ISSN: 2073-9524
Pages:137-154

Abhishek and Jindal [28] utilized color illumination, deep CNNs, and semantic segmentation techniques for detecting and localizing image forgeries. Colour illumination is employed to implement a colour map after the pre-processing stage. The transfer learning methodology is employed to train the VGG-16 model utilizing a deep convolutional neural network architecture, specifically to classify two distinct classes. The algorithm in question is designed to classify the pixels of images as either authentic or forged. After categorization, forgery localization begins. Classifying an image involves anticipating its fabrication. Localization shows where image forgery is active. This was a difficult task solved by utilizing transfer learning DCNN and semantic segmentation. Transfer learning's ability to retrain models with little data is its main benefit.

Goel et al. [29], the authors suggested applying a novel dual-branch convolutional neural network in a passive copy move forgery detection system that is based on deep learning to distinguish between authentic and fake images. The convolutional neural network with dual branches is designed to extract multi-scale information by utilizing different kernel sizes in each branch. The fusion of retrieved multi-scale features is then conducted to attain high accuracy, precision, and recall scores. The effectiveness of the suggested design is supported by thorough result analysis and comparison analysis, which demonstrate its superiority over the other architecture in terms of performance scores, computing time, and complexity.

Rhee [30] presented the development of a ground truth image for detecting Copy-Move regions. The deep neural networks employed in this work include Resnet50, Resnet18, Mobilenetv2, Xception, Inceptionresnetv2, and Deep Lab v3plus, which are state-of-the-art CNN models known for their outstanding performance in image classification and semantic segmentation tasks. The Resnet50 and Resnet18 models, often employed for the task of image classification, are transformed into a series of models, which is mostly utilized for semantic segmentation. These models show novel designs and possess the combined attributes of image classification and semantic segmentation.

Qazi et al. [31], the authors utilized deep learning techniques to detect counterfeit images accurately, in which ResNet50v2 is used as the foundational model. Additionally, they utilized the YOLO CNN weights for transfer learning. This technique facilitated the training of the model by allocating significant weights. The authors used pre-trained weights from the YOLO CNN object detection model to initialize their suggested architecture based on ResNet50v2. This approach significantly reduced costs during training. The model was initialized using pre-existing weights that included valuable information. One advantage of this approach is that it effectively lessens the required training time by utilizing a ResNet-based architecture.

Li et al. [32] proposed SD-Net to handle the issue of low precision in the detection outcome of most image copy_move forgery detection (CMFD) techniques based on convolutional neural networks (CNN). SD-Net merges super boundary-to-pixel direction (super-BPD) segmentation with deep CNN (DCNN) to improve the detection and localization of image copy-move forgeries. The utilization of segmentation technology serves to optimize the correlation between identical or comparable image blocks, hence enhancing the precision of detection. Additionally, deep convolutional neural networks (DCNN) are employed to extract visual features, substituting traditional, manually designed characteristics with automatically learned features. The employment of a feature pyramid enhances resilience against scaling attacks. Furthermore, the BPD information is employed as a method to enhance the edges of the first detected images, resulting in the acquisition of the ultimate detected image. The experimental results demonstrated that the SD-Net had effective detection and localization capabilities for various types of forgeries, including rotated and scaled ones. Notably, the model performed particularly well in detecting large-scale scaling forgeries. In comparison to alternative methodologies, the SD-Net exhibits superior accuracy in localization and demonstrates robustness when subjected to a range of post-processing

ISSN: 2073-9524
Pages:137-154

techniques, including but not limited to brightness alterations, contrast modifications, colour reduction, picture blurring, JPEG compression, and noise adding.

Zainal et al. [33], the authors introduced a unique approach to identifying copy_move forgery recognition (CMFR) via deep learning (DL) and hybrid optimization techniques. The suggested system is based on the integration of the hybrid Grey Wolf Optimization and African Buffalo Optimization (GWO-ABO) algorithms utilizing the CNN approach. This scheme, referred to as GWO-ABO-CNN, serves as the essential framework for this research. The scheme that has been created utilizes convolution layers and pooling layers to extract image attributes. Subsequently, these attributes are compared and employed to detect copy_move forgery (CMF).

Kwon et al. [34], the authors fundamentally focused on checking for JPEG compression artifacts that continue beyond the process of image acquisition and subsequent editing. They put forth a CNN that leverages discrete cosine transform (DCT) coefficients, which retain compression artifacts, to identify certain regions in an image that have undergone alteration. CNNs are unable to effectively capture the distribution of discrete cosine transform (DCT) coefficients due to the inherent nature of convolution operations that discard spatial coordinates, which play a crucial role in representing DCT coefficients. The execution of this method is notably superior to conventional techniques and deep neural network approaches when it comes to identifying and precisely identifying manipulated areas.

Aria et al. [15], presented a deep-learning strategy called QDL-CMFD, an image quality-independent method designed to identify forgery. The technique known as QDL-CMFD utilizes generative adversarial networks (GANs) to rise the quality of images, while CNNs are utilized to detect forgeries. This study presents a customized dual-branch CNN structure, including two distinct subnetworks: a manipulation detection subnetwork and a similarity detection subnetwork. In disparity with prevailing methodologies, QDLCMFD can concurrently identify several instances of the falsified area while also discerning the origin and destination of the forgery. Moreover, QDL-CMFD exhibits robustness against many pre-processing and post-processing threats. The system has exceptional efficacy in detecting low-quality manipulated images and small regions. A no-reference image quality assessment (NR-IQA) module evaluates the input picture's quality and improves it if it's low-resolution, which makes copy-move forgery detection difficult. This evaluation retrieves scene characteristics, including normalized local luminance coefficient statistics, and maps the quality score out of feature space. The Optimized Super-Resolution Generative Adversarial Network (OSRGAN) module upgrades images with distortion or low resolution.

Ganapathi et al. [35], the authors introduced an end-to-end deep neural network methodology for detecting image fraud, employing two subnetworks to extract characteristics from spatial and frequency domains at several resolutions. The researchers integrated channel attention into their methodology with the subnet-works to get attention-aware characteristics on manipulated areas. The derived features of CA-HRNet are based on spatial domains with different resolutions, whereas the derived features of CA-DCTNet are based on the frequency domain. Integrating these two characteristics facilitates the localization of manipulated sections at the pixel level. Incorporating channel attention has yielded improved outcomes compared with other cutting-edge methodologies.

Tinnathi and Sudhavani [36] proposed an approach for improving copy-move forgery detection utilizing an updated Grey Wolf Optimization (GWO) algorithm with the AlexNet model. To begin with, a super pixel clustering technique is utilized to do patch segmentation in the manipulated images. Moreover, this study proposes an improved Grey Wolf Optimization (GWO) algorithm combined with the AlexNet model to extract features from segmented patches of different sizes. These features are then employed to reconstruct the dense depth of the image pixels. This operation eases the matching of fake areas with authentic areas. Finally, a patch-matching algorithm capable of adapting to several scenarios is

ISSN: 2073-9524
Pages:137-154

utilized to accurately identify the areas of concern within the manipulated photos. The experimental outcome demonstrates that the suggested improved Grey Wolf Optimization (GWO) based AlexNet model effectually identifies and localizes the faked areas, even in salt and pepper noise, Gaussian noise, blurring, rotation, and enhancement. The proposed model can detect many cases of forgery and identify small faked portions, even when the tampered image is smooth.

Jaiswal et al. [4], presented the development of a deep learning CNN model that utilizes multi-scale input and incorporates many stages of convolutional layers. The layers above are partitioned into two components, namely the encoded block and the decoder block. In the encoder block, the feature maps obtained from the convolutional layers of various stages are merged and down-sampled. Similarly, the decoder block combines and performs up-sampling on the retrieved feature maps. The final feature map identifies pixels as forged or non-forged by applying a sigmoid activation function. The model has undergone training and validation using two distinct datasets that are publicly accessible. This work employs both image-level analysis and pixel-level analysis. The second dataset exhibits limited images available for training the model. The lower performance observed in the second dataset can be attributed to this underlying cause.

Mallick et al. [37] introduced a unique methodology for identifying instances of copy-move and splicing picture forgeries. The proposed strategy employs a CNN that incorporates three distinct models: ELA (Error Level Analysis), VGG16, and VGG19. The approach utilizes a pre-processing technique to acquire images at a specific compression rate. These images are employed to train the model, and the images are categorized as either original or fake. However, a substantial amount of work must be undertaken in picture forgery detection. It is anticipated that neural networks will be able to identify manipulated images, irrespective of their level of complexity. The potential for enhancing the VGG19 training model exists by expanding the dataset and utilizing high-performance computer equipment.

Kadam et al. [8] introduced a lightweight model, Mask R-CNN with MobileNet, to detect and identify instances of copy-move and image-splicing frauds. A comparison study was conducted between the proposed work and ResNet-101 on seven distinct standard datasets. The total setup exhibited computational efficiency superior to that of ResNet-101. Based on experimental findings, it has been shown that the suggested methodology successfully achieves a harmonious equilibrium between efficiency and computational expenses when compared to ResNet-101. Additionally, it can determine the proportion of falsified content inside a specific area of an image.

Katiyar and Bhavsar [38], presented a comprehensible methodology for detecting picture manipulation, specifically targeting two distinct forms of image forgery and employing three CNN models for analysis. The outcome indicates that identifying forgeries may be clarified even when only tiny portions of tampered content are inside typical natural images. The essential emphasis of their study was to prioritize the side of interpretability rather than just pursuing exceptional performance. Moreover, their results clarified that a composite model, which embodies learning two distinct classes of forgeries, can produce suitable outcomes in random forgeries. This differs from late studies focusing exclusively on facial forgeries inside deep fakes. Acknowledging that the investigation of interpretability may be expanded to other networks, potentially leading to improved performance, is vital. This concept is significant for image-based classifiers that aim to localize forgeries.

Krishnaraj et al. [39] introduced a fusion model, the Deep Learning-based Fusion Model for Copy_move Detection and Localization (DLFM-CMDFC), which employs automated deep learning techniques. The DLFM-CMDFC technique is a novel approach that integrates the concepts of generative adversarial networks (GANs) and densely connected networks (DenseNet). The DLFM-CMDFC approach integrates the two outputs to form a layer that encodes the input vectors alongside the first layer of an extreme learning machine (ELM) classifier. Furthermore, the ELM model's weight and bias

ISSN: 2073-9524
Pages:137-154

parameters are effectively calibrated using the artificial fish swarm method (AFSA). The outputs of the networks are sent as input to the merging unit. A fabricated image is employed to discern the disparities between the input and target regions. The experimental findings demonstrated that the suggested model outperforms recently developed methodologies.

Manjunatha and Patil [40], presented a proficient method for detecting tampering through resampling features and CNNs. In the suggested model, Range Spatial Filtering (RSF)-CNN, the image undergoes a preprocessing step and is split into patches of uniform size. The resampling characteristics are extracted within each patch utilizing affine transformation and the Laplacian operator. These characteristics include scaling, noise, rotations, additions, and manipulations. The outcomes exhibit that the RSF-CNN approach for tampering detection exhibits much greater accuracy than other methods. An experiment examined the computational complexity of numerous tampering detection systems. The measurement of computational complexity is based on the temporal duration required to identify manipulated areas. The researchers observe that the RSF-TD method displays a notable reduction in calculation time compared to alternative approaches.

Hosny et al. [41] presented a convolutional neural network (CNN) architecture that aims to detect copy-move image fakes authoritatively. The design that has been suggested exhibits computational efficiency, as it incorporates an appropriate configuration of convolutional and max-pooling layers. The technique consists of three distinct steps: preprocessing, feature extraction, and classification. The results from experiments consistently demonstrate the significant superiority of the proposed model when compared to other algorithms, namely in terms of accuracy and TT (total time).

Maashi et al. [42] used deep transfer learning-based CM forgery detection (RSADTL-CMFD). The current model employs a Neural Architectural Search Network (NASNet) to extract important and discriminative features from input photos for forgery detection. We tune hyperparameters with the reptile search algorithm (RSA) to improve NASNet performance. This approach optimizes network hyperparameters, allowing the model to adapt to forgery detection tasks and perform well swiftly. Finally, extreme gradient boosting (XGBoost) classifies image areas as genuine or manipulated/forged using deep learning network features. An exhaustive comparison investigation showed that RSADTL-CMFD outperformed other methods. The RSADTL-CMFD technique enables the real-time identification of the CM areas.

Khalil et al. [43] utilized deep learning and transfer learning to identify two forms of digital picture counterfeiting simultaneously. The suggested method finds the compressed quality of the forged region, which usually differs from the remainder of the image. A deep learning-based model is proposed to detect digital image forgery by calculating the difference between the original image and its compressed version to produce a featured image for the pre-trained model to train after removing its classifier and adding a fine-tuned classifier. Eight binary classification pre-trained models are compared. After comparing evaluation metrics, charts, and graphs, the strategy employing the customized eight pre-trained models beats state-of-the-art methodologies. The approach with the pre-trained model MobileNetV2 offers the best detection accuracy with fewer training parameters and faster training time. Based on network specifications, MobileNet, DenesNet, and VGG16 have the lowest computational cost. For an image forgery detection system with the greatest detection accuracy and the least computing costs and training time, the MobileNet pre-trained model is suggested.

Nirmalapriya et al. [44], aimed to create a system that detects digital picture counterfeiting using the recently proposed Aquila Sine Cosine Algorithm. This hybrid deep learning method uses a Deep Convolutional Neural Network (DCNN) and Squeeze Net to identify digital picture counterfeiting. The created ASCA approach updates the weight of the DCNN and Squeeze Net, reducing detection process training time and computing complexity. ASCA is also created by merging the Aquila Optimizer (AO) update routines with the sine-cosine algorithm. employed a copy_move forgery detection dataset, the

ISSN: 2073-9524
Pages:137-154

hybrid deep learning classifier classifies the output as authentic or fake.

Zhang et al. [14] introduced a unique Convolutional Neural transformer generative Adversarial Network (CNN-T GAN) to localize copy-move forgeries and distinguish between the source and destination. The generator consists of three main components: a CNN branch, a transformer branch, and many feature coupling layers. The CNN and transformer branches extract local features and global representations of the copy-move regions. Feature coupling layers are specifically developed to facilitate the integration of features within two distinct branches. A training process is implemented where both the generator and the discriminator are iteratively taught to optimize the efficiency. The suggested technique has been empirically demonstrated to exhibit superior performance to other methods, i.e., CMFL and CMSTD, across three widely utilized copy-move forgery datasets.

Table 1: Comparative Analysis of Deep Learning- Based Copy-Move Forgery Detection.

References	Deep learning models	Dataset	Metrics					
			F-measure	Precision	Recall	TPR	FPR	Accuracy
Agarwal [18]	Simple Linear Iterative Clustering, VGG Net	MICC-F220 dataset	91.8	98.026	89.583	-	0.75	95
Abdalla [19]	CNN	Combination of MICC-F600, CIFAR-10, and Oxford buildings	0.8835	0.6963	0.8042	-	-	90
Thakur and Rohilla [10]	Uses median filter residual And CNN	CoMoFoD dataset	-	-	-	-	-	95.97
		BOSSBase dataset	-	-	-	-	-	94.26
Younis Abdalla et al. [20]	CNN, GAN	CIFAR-10 MNIST	0.8835	0.6963	0.8042	100	0	~95%
Muzaffer and Ulutas [21]	CNN, AlexNet	GRIP dataset	0.93	-	-	-	-	-
Kuznetsov [22]	CNN	CMFD, Casia v2.	0.77	0.71	0.84	-	-	-
Thakur and Jindal [23]	DL(DCNN), ML(SVM)	CASIA1.0	-	-	-	-	-	0.99
		CASIA2.0	-	-	-	-	-	0.98
		BSDS300	-	-	-	-	-	0.98
		DVMM	-	-	-	-	-	0.97
		CMFD	-	-	-	-	-	0.99
Elaskily et al. [24]	CNN, Convolutional Long Short-Term Memory (CovLSTM) networks.	MICC-F220	-	-	-	100	zero	1.0
		MICC-F2000	-	-	-	97.6	1.1	98.89
		MICC-F600	-	-	-	100	1.9	98.14
		Combined databases	-	-	-	100	2.95	97.13
Singhal and Ranga [6]	CNN	CASIA v1.0 database	0.84	0.81	0.79	-	-	86.4
Abbas et al.[25]	Small VGGNet	CoMoFoD, MICC-F2000, CASIA ITDE 2.0	-	-	-	0.87	0.13	0.87
	MobileNetV2		-	-	-	0.85	0.19	0.85

ISSN: 2073-9524
Pages:137-154

Rao et al. [26]	CNN with multi-semantic attention model	DSO-1	-	0.957	-	-	-	-
		Coverage	-	0.729	-	-	-	-
		CASIA1	-	0.610	-	-	-	-
		CASIA2	-	0.617	-	-	-	-
		Average	-	0.669	-	-	-	-
Peng Liang et al. [27]	Deep learning Pyramid correlation network (PCNet)	USCISI	-	-	-	-	-	-
		CASIA	77.61	79.31	75.43	-	-	-
		CoMoFoD	78.45	77.46	79.46	-	-	-
Abhishek and Jindal [28]	DCNN and Semantic Segmentation	GRIP, DVMM, CMFD, BSDS300	0.82468	-	-	-	-	0.98224
Nidhi Goel et al. [29]	novel dual branch CNN architecture	MICC-F2000	0.94	0.89	1.0	-	-	0.96
Rhee [30]	CNN	CoMoFoD, CVI, GRIP, CASIA, COVERAGE, MICC-F600, and CPH	0.6608	-	0.9350	-	-	0.9523
Qazi et al. [31]	ResNet50; YOLO CNN	CASIA_v1, CASIA_v2 dataset	-	-	-	-	-	99.3%
Li et al. [32]	SD-Net, DCNN, VGG16	USCISI, CoMoFoD	50.77	59.11	57.69	-	-	-
		CASIA II.	48.06	57.48	51.25	-	-	-
Zainal et al. [33]	Grey Wolf Optimization and African Buffalo Optimization using CNN	MICC-F600	99.9	-	-	98.6	1.04	98.2
		SATs-130	1.0	-	-	99	2.84	100
		MICC-F220	1.0	-	-	1.0	0	1.0
		NC16 SP	55.62	68.76	-	-	-	-
		Columbia SP	93.97	95.87	-	-	-	99.61
		GRIP (CM)	76.45%	91.87%	-	-	-	99.46
		CoMoFoD (CM)	14.01	21.46	-	-	-	98.68
		Coverage (CM)	41.27	53.76	-	-	-	93.00
Aria et al. [15]	Generative Adversarial Networks and CNN	CASIA TIDE v2.0	77.35	89.23	81.68	-	-	-
		CoMoFoD	52.86	66.46	67.15	-	-	-
		CMFD dataset	97.83	97.02	96.50	-	-	-
Ganapathi et al., [35]	CA-HRNet extracts the spatial domain features, and CA-DCTNet extracts the frequency domain features using HRNet	CASIA v2	-	-	-	-	-	88.16
		NIST	-	-	-	-	-	86.41
		Fantastic Reality	-	-	-	-	-	91.76
		Carvalho	-	-	-	-	-	81.56
		Columbia	-	-	-	-	-	90.56
Tinnathi and Sudhavani [36]	Super pixel clustering and Enhanced Grey Wolf Optimizer based AlexNet	MICC-F600	99.64	98.58	98.48	-	-	99.66
		MICCF2000	98.50	97.61	97.21	-	-	99.75
		GRIP datasets	99.40	98.93	97.13	-	-	98.48

ISSN: 2073-9524
Pages:137-154

Ankit Kumar Jaiswal et al. [4]	Deep CNN	CoMoFoD	0.9655	0.9794	0.9520	-	-	0.9382
		CMFD	0.9794	0.9794	0.9794	-	-	0.9722
Devjani Mallick et al. [37]	CNN with Error Level Analysis	CASIA- 2.0, NC2016	-	-	-	-	-	70.6
	VGG16		-	-	-	-	-	71.6
	VGG19		-	-	-	-	-	72.9
Kalyani Dhananjay Kadam et al. [8]	Mask R-CNN with MobileNet, a lightweight mode	COVERAGE	0.61	0.90	0.63	-	-	-
		CASIA 2.0	0.68	0.60	0.66	-	-	-
		MICC F220	0.67	0.90	0.75	-	-	-
		MICC F600	0.70	0.70	0.68	-	-	-
		MICC F2000	0.64	0.90	0.80	-	-	-
		CASIA 1.0	0.64	0.70	0.68	-	-	-
		COLUMBIA	0.61	0.90	0.63	-	-	-
Ankit Katiyar and Bhavsar [38]	CNN · Grad-CAM ·	COCO dataset and Inpainting dataset(M1) Copy-Move dataset(M2) M3= (M1&M2)	-	-	-	-	-	M1= 0.80 M2= 0.70 M3=0.69
Krishnaraj et al. [39]	Deep Learning-Based Fusion Model	MNIST, COCO datasets	96.06	97.27	96.46	-	-	-
Manjunatha and Patil [40]	Resampling features and CNN	(MICC), D0 dataset	99.28	98.84	98.08	-	-	-
Hosny [41]	CNN	MICC-F2000	1.0	1.0	1.0	-	-	1.0
		MICC-F600	1.0	1.0	1.0	-	-	1.0
		MICC-F220	1.0	1.0	1.0	-	-	1.0
Maashi [42]	Reptile Search Algorithm with a Deep Transfer Learning	MNIST, CIFAR-10	97.65	97.62	97.39	-	-	-
Khalil et al. [43]	VGG16	CASIA 2.0	0.94	93.93	93.71	-	-	93.83
	VGG19		0.95	94.81	94.73	-	-	94.77
	ResNet50		0.95	94.50	94.69	-	-	94.61
	Reset101		0.94	93.36	94.00	-	-	93.60
	ResNet152		0.93	93.49	93.12	-	-	93.43
	MobileNetV2		0.94	94.21	94.74	-	-	94.69
	Xception		0.93	92.92	92.96	-	-	92.88
	DenseNet		0.94	94.03	94.10	-	-	94.14
Nirmalapriya et al. [44]	Deep CNN and Squeeze Net using Aquila Sine Cosine Algorithm (ASCA).	CMFD, JPEG seam-carving forgery dataset	-	-	-	0.95	-	0.980
Zhang et al. [14]	CNN-Transformer-Generative Adversarial Network	USCISI	90.82	96.28	98.22	-	-	98.66
		CASIA2.0	63.42	87.45	93.87	-	-	97.15
		CoMoFoD	83.42	91.06	96.45	-	-	98.44

ISSN: 2073-9524
Pages:137-154

5. Commonly Available Forgery Datasets

The dataset consists of both legitimate and counterfeit images and is necessary for assessing the effectiveness of the image tampering method. Table 2 presents a comprehensive overview of the commonly available datasets.

Table 2: Common Image Forgery Datasets.

Dataset	Size	Type of forgery	Format	Forged images: Authentic images
CASIA V1.0 [45]	384×256	Copy-move & splicing forgery	JPEG	800:921
CASIA V2.0 [45]	240×160 ,900×600	Copy-move & splicing forgery	JPEG, TIFF	7491:5123
MICC-F220 [46]	722×480, 800×600	Copy-move	JPEG	110:110
MICC-F2000 [46]	2048×1536	Copy-move	JPEG	700:1300
MICC-F600 [46]	800×533, 3888×2592	Copy-move	JPEG, PNG	160:440
USCISI [47]	320 × 240–640 × 575	Copy-move	PNG	100,000/-
Korus [48]	1920 × 1080	Copy-move, Splicing	TIF	220:220
CoMoFoD [49]	512×512	Copy-move	JPEG, PNG	5200:5200
COVERAGE [50]	2048 × 1536	Copy-move	TIF	100:100
GRIP [51]	768×1024	Copy-move	PNG	3440:80

6. Discussion

In recent times, research in detecting image fraud has been rapidly expanding, especially focusing on passive or blind images with copy-move forging techniques. Important aspects were identified by a thorough study of many research publications.

Hence, there is a significant need for a high-quality technique to detect copy-move areas in modified images. The dataset in Image Forensics is crucial for training and developing models. Various types of datasets are accessible for these investigations, including the CoMoFoD dataset, the Columbia dataset, and the Vision Dataset. The dataset contains manipulated information, including CASIA V1, CASIA V2, MICC-F220, MICC-F600, and MICC-F2000 datasets. Researchers evaluate tampering detection algorithms using several metrics, including accuracy, precision, recall, and F-measure. Compare the performance of several tampering detection algorithms using similar criteria (measures).

This research may be directed towards expanding forgery detection algorithms to identify forgeries in audio and visual applications. While deep learning algorithms are commonly employed for identifying digital image fraud, these models seem intricate. In the future, simpler and more precise deep learning models might become the basis for study.

The detection of copy-move forgeries utilizing deep learning approaches encompasses various challenges:

1. Developed editing tools can perfectly blend copied parts with the original images, minimizing perceptible inconsistencies. In addition, forgeries of high quality can contain the slightest or even invisible artifacts, making them harder to detect.
2. Deep learning approaches require training using huge genuine and forged image datasets;

ISSN: 2073-9524
Pages:137-154

however, these required datasets are not always available. Moreover, most existing datasets are imbalanced, affecting the training process.

3. Various forgeries hold varying features, making it difficult for a single deep-learning approach to classify all kinds efficiently.

4. Applying copy-move forgery detection systems in real-time is difficult owing to high computation necessities.

5. Deep learning approaches must be robust to common transformations of digital images (like resizing and compression), that may influence classification accuracy.

6. Typically, deep-learning approaches work as "black-boxes", offering a limited understanding of classifying images as genuine or forged. Therefore, the classification approaches should be improved to be interpretable and gain more trust.

7. Analysis of Image Forgery Datasets

Selecting a suitable dataset is crucial in digital image forensics. A comprehensive dataset must include all conceivable sorts of manipulated images that the classifier may encounter. The classifier's robustness and performance are significantly influenced by the image dataset utilized. The image dataset must be extensive in both the quality and number of images.

Using standard and common datasets would be easier for researchers. There are various forgery detection datasets. The MICC is the oldest and most widely used dataset for forgery detection. This dataset has three subsets: MICC-F220, F600, and F2000. This dataset's counterfeit images were made using copy-move with geometric adjustments, including rotation and scale. It has some drawbacks: forgery images are not post-processing. In evaluation metrics in MICC220 and MICC2000, subsets are image-based because there are no ground truth images. The CoMoFod datasets as big images are unsuitable for sluggish programming languages and block-based approaches.

These datasets lack geometric transformation parameters. CASIA is the most popular public JPEG, splicing, and copy-move dataset. CASIA comes in two variants. CASIA V1.0 and CASIA V2.0. Images in forgery regions have been post-processed using blurring. The drawback of the CASIA dataset is the lack of ground-truth images. The COVERAGE dataset has drawbacks:

The dataset contains 100 original and 100 counterfeit photos. Forgery images are not post-processed, the copy-move regions are big, making it easier to detect, and each image has two ground truth images: one showing the duplicated region and the other showing the pasted region.

8. Conclusion

Our study on deep learning copy-move forgery detection illuminated the advances and problems in this vital field of digital image forensics. Key survey findings are as follows: first, deep learning advances: convolutional neural networks (CNNs) have shown potential in detecting digital image copy-move forgeries. Forensic analysts benefit from these algorithms' ability to learn complicated patterns and features. Secondly, diversity challenges: accurate deep learning models require varied, large, and thorough datasets. Thirdly, improved detection accuracy depends on feature extraction approaches. Fourthly, deep learning model robustness and generalization are crucial. Building robust models against adversarial attacks and image quality, compression, and manipulation variations is difficult. Finally, for practical implementation, scalability and computational efficiency are essential. Researchers are optimizing deep learning models for forensic applications to make them cheaper and more accessible.

More potential future works should be adopted to detect copy-move forgery using deep learning; such as enhancing, investigating more sophisticated CNN structures, or even incorporating attention mechanisms to improve the accuracy of forgery detection. Additionally, it is significant to utilize further data sources to improve the approach's performance. Furthermore, generalized approaches should be developed to detect various kinds of forgeries across various datasets. Eventually, it will be significant to provide real-time processing on mobile platforms by improving the efficiency of forgery detection using deep-learning approaches.

ISSN: 2073-9524
Pages:137-154

Conflict of Interest

The authors declare that there are no conflicts of interest regarding the publication of this manuscript.

References

[1] Hussain, I. Tan, S. Li, B. Qin, X. Hussain, D. and Huang, J. (2021). A novel deep learning framework for double JPEG compression detection of small size blocks. J. Vis. Commun. Image Represent, 80, 103269.

[2] Sharma, P. Kumar, M. and Sharma, H. (2023). Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: an evaluation. Multimedia. Tools Appl., 82(12), 18117–18150.

[3] Abidin, A. B. Z. Majid, H. B. A. Samah, A. B. A. and Hashim, H. B. (2019). Copy-move image forgery detection using deep learning methods: A review. International Conference on Research and Innovation in Information Systems (ICRIIS), 1-6.

[4] Jaiswal, A. K. and Srivastava, R. (2022). Detection of Copy-Move Forgery in Digital Image Using Multi-scale, Multi-stage Deep Learning Model. Neural Process. Lett., 54(1).

[5] Jain, I. and Goel, N. (2021). Advancements in image splicing and copy-move forgery detection techniques: A survey. In 2021 11th international conference on cloud computing, Data Science & Engineering (confluence), 470-475.

[6] Singhal, S. and Ranga, V. (2021). Passive authentication image forgery detection using multilayer CNN. In: Mobile Radio Communications and 5G Networks: Proceedings of MRCN 2020. Springer Singapore, 140, 237–249.

[7] Waleed, J. Abdullah, D. A. and Khudhur, M. H. (2018). Comprehensive Display of Digital Image Copy-Move Forensics Techniques. International Iraqi Conference on Engineering Technology and its Applications, IICETA 2018, 155–160

[8] Kadam, K. D. Ahirrao, S. and Kotecha, K. (2022). Efficient Approach towards Detection and Identification of Copy Move and Image Splicing Forgeries Using Mask R-CNN with MobileNet V1," Computational Intelligence and Neuroscience, 6845326.

[9] Raja, A. (2021). Active and Passive Detection of Image Forgery: A Review Analysis. International Journal of Engineering Research & Technology (IJERT), 9(5), 418–424.

[10] Thakur, R. and Rohilla, R. (2019). Copy-Move Forgery Detection using Residuals and Convolutional Neural Network Framework: A Novel Approach. 2019 2nd Int. Conf. Power Energy Environ. Intell. Control. PEEIC 2019, 561–564.

[11] Manjunatha, S. and Patil, M. M. Deep learning-based technique for image tamper detection. In 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 1278–1285.

[12] Doegar, A. Dutta, M. and Kumar, G. (2018). CNN based Image Forgery Detection using pre-trained AlexNet Model. Proc. Int. Conf. Comput. Intell. IoT 2018, 402–407.

[13] Mehrjardi, F. Z. Latif, A. M. Zarchi, M. S. and Sheikhpour, R. (2018). A survey on deep learning-based image forgery detection. Pattern Recognition (2023), 109778.

[14] Zhang, Y., Zhu, G., Wang, X., Luo, X., Zhou, Y., Zhang, H., & Wu, L. (2022). CNN-transformer based generative adversarial network for copy-move source/target distinguishment. *IEEE Transactions on Circuits and Systems for Video Technology*, *33*(5), 2019-2032.

[15] Aria, M. Hashemzadeh, M. and Farajzadeh, N. (2022). QDL-CMFD: A Quality-independent and deep Learning-based Copy-Move image forgery detection method. Neurocomputing, 511, 213–236.

[16] Rodriguez-Ortega, Y. Ballesteros, D. M. and Renza, D. (2021). Copy-move forgery detection (Cmfd) using deep learning for image and video forensics. Journal of imaging, 7(3), 59.

[17] Rao, Y. Ni, J. and Zhao, H. (020). Deep Learning Local Descriptor for Image Splicing Detection and Localization. IEEE Access, 8, 25611–25625.

[18] Agarwal, R. (2019). An Efficient Method of Copy Move Forgery Detection Using a Deep

ISSN: 2073-9524
Pages:137-154

Learning based Feature Extraction and Matching Algorithm by Ritu Agarwal. Multimed. Tools Appl., 79(11), 7355–7376.

[19] Abdalla, Y. (2019). Convolutional Neural Network for Copy-Move. Symmetry (Basel)., 1–17.

[20] Abdalla, Y. Tariq Iqbal, M. and Shehata, M. (2019). Copy-move forgery detection and localization using a generative adversarial network and convolutional neural network. Information, 10(9), 286.

[21] Muzaffer, G. and Ulutas, G. (2019). A new deep learning-based method to detect copy-move forgery in digital images. In 2019 Scientific Meeting on Electrical-Electronics and Biomedical Engineering and Computer Science, EBBT 2019, 1-4.

[22] Kuznetsov, A. (2020). On deep learning approach in remote sensing data forgery detection. Proc. ITNT 2020 - 6th IEEE Int. Conf. Inf. Technol. Nanotechnol., 14–17.

[23] Thakur, A. and Jindal, N. (2020). Hybrid deep learning and machine learning approach for passive image forensic. IET Image Process., 14 (10).

[24] Elaskily, M. A. Alkinani, M. H. Sedik, A. and Dessouky, M. M. "Deep learning-based algorithm (ConvLSTM) for Copy Move Forgery Detection. J. Intell. Fuzzy Syst., 40(3), 4385–4405.

[25] Abbas, M. N. Ansari, M. S. Asghar, M. N. Kanwal, N. O'Neill, T. and Lee, B. (2021). Lightweight Deep Learning Model for Detection of Copy-Move Image Forgery with Post-Processed Attacks. SAMI 2021 - IEEE 19th World Symp. Appl. Mach. Intell. Informatics, Proc., 125–130.

[26] Rao, Y. Ni, J. and Xie, H. (2021). Multi-semantic CRF-based attention model for image forgery detection and localization. Signal Processing, 183, 108051.

[27] Liang, P. et al., (2021). Copy-Move Forgery Detection Based on Pyramid Correlation Network. Converter, 3, 745–755.

[28] Abhishek and Jindal, N. (2021). Copy moves and splicing forgery detection using deep convolution neural network, and semantic segmentation. Multimed. Tools Appl., 80(3), 3571–3599.

[29] Goel, N. Kaur, S. and Bala, R. (2021). Dual branch convolutional neural network for copy moves forgery detection. IET Image Process., 15(3), 656–665.

[30] Rhee, K. H. (2022). Generation of Novelty Ground Truth Image Using Image Classification and Semantic Segmentation for Copy-Move Forgery Detection. IEEE Access, 10, 2783–2796.

[31] Qazi, E. U. H. Zia, T. and Almorjan, A. (2022). Deep Learning-Based Digital Image Forgery Detection System. Applied Sciences, 12(6), 2851.

[32] Li, Q. Wang, C. Zhou, X. and Qin, Z. (2022). Image copy-move forgery detection and localization based on super-BPD segmentation and DCNN. Scientific Reports, 12(1), 1–12.

[33] Zainal, A. G. Kaur, C. Al Ansari, M. S. Borda, R. F. C. Nageswaran, A. and El-Aziz, R. M. A. (2022). Recognition of Copy Move Forgeries in Digital Images using Hybrid Optimization and Convolutional Neural Network Algorithm. (IJACSA) International Journal of Advanced Computer Science and Applications, 13(12),301–311.

[34] Kwon, M. J. Nam, S. H. Yu, I. J. Lee, H. K. and Kim, C. (2022). Learning JPEG Compression Artifacts for Image Manipulation Detection and Localization. International Journal of Computer Vision, 130(8), 1875–1895.

[35] Ganapathi, I. I. Javed, S. Ali, S. S. Mahmood, A. Vu, N. S. and Werghi, N. (2022). Learning to localize image forgery using end-to-end attention network. Neurocomputing, 512, 25–39.

[36] Tinnathi S. and Sudhavani, G. (2022). Copy-Move Forgery Detection Using Super Pixel Clustering Algorithm and Enhanced GWO Based AlexNet Model. Cybern. Inf. Technol., 22(4), 91–110.

[37] Mallick, D. Shaikh, M. Gulhane, A. and Maktum, T. (2022). Copy Move and Splicing Image Forgery Detection using CNN. ITM Web Conf., 44, 03052.

[38] Katiyar, A. and Bhavsar, A. (2022). Image Forgery Detection with Interpretability. 2022, arXiv preprint arXiv.

ISSN: 2073-9524
Pages:137-154

[39] Krishnaraj, N. Sivakumar, B. Kuppusamy, R. Teekaraman, Y. and Thelkar, A. R. (2022). Design of Automated Deep Learning-Based Fusion Model for Copy-Move Image Forgery Detection. Computational Intelligence and Neuroscience.

[40] Manjunatha S. and Patil, M. M. (2022). Efficient resampling features and convolution neural network model for image forgery detection. Indones. J. Electr. Eng. Comput. Sci., 25(1) 183–190.

[41] Hosny, K. M. Mortda, A. M. Fouda, M. M. and Lashin, N. A. (2022). An Efficient CNN Model to Detect Copy-Move Image Forgery. IEEE Access, 10, 48622–48632.

[42] Maashi M. et al., (2023). Modeling of Reptile Search Algorithm with Deep Learning Approach for Copy Move Image Forgery Detection. IEEE Access, 11, 87297–87304.

[43] Khalil, A. H. Ghalwash, A. Z. Elsayed H. A., Salama, G. I. and Ghalwash, H. A. (2023). Enhancing Digital Image Forgery Detection Using Transfer Learning. IEEE Access, 11, 91583–91594.

[44] Nirmalapriya, G. Maram, B. Lakshmanan, R. and Navaneethakrishnan, M. (2023). ASCA-squeeze net: Aquila sine cosine algorithm enabled hybrid deep learning networks for digital image forgery detection. Comput. Secur., 128: 103155.

[45] Dong, J. Wang, W. and Tan, T. (2013). Casia image tampering detection evaluation database. 2013 IEEE China summit and international conference on signal and information processing. IEEE, 2013.

[46] Amerini, Irene, et al. (2011). A sift-based forensic method for copy-move attack detection and transformation recovery. IEEE transactions on information forensics and security 6.3 (2011): 1099-1110.

[47] u, Y., Abd-Almageed, W., and Natarajan, P. (2018). Busternet: Detecting copy-move image forgery with source/target localization. In Proceedings of the European conference on computer vision (ECCV), 168-184.

[48] Korus, P. (2017). Digital image integrity–a survey of protection and verification techniques. Digital Signal Processing, 71, 1-26.

[49] Tralic, D., Zupancic, I., Grgic, S., and Grgic, M. (2013). CoMoFoD—New database for copy-move forgery detection. In Proceedings ELMAR-2013, IEEE, 49-54.

[50] Wen, B., Zhu, Y., Subramanian, R., Ng, T. T., Shen, X., and Winkler, S. (2016). COVERAGE—A novel database for copy-move forgery detection. In 2016 IEEE international conference on image processing (ICIP),161-165.

[51] Cozzolino, D., Poggi, G., & Verdoliva, L. (2015). Efficient dense-field copy–move forgery detection. IEEE Transactions on Information Forensics and Security, 10(11), 2284-2297.