International Journal of Safety and Security Engineering
Vol. 14, No. 5, October, 2024, pp. 1505-1515
Journal homepage: http://iieta.org/journals/ijsse

Deep Learning Methods for Copy Move Image Forgery Detection: A Review

Bilal Benmessahel

Faculty of technology, UFAS 1 University, Setif 19000, Algeria

Corresponding Author Email: Bilal.benmessahel@gmail.com

https://doi.org/10.18280/ijsse.140518

Received: 18 February 2024
Revised: 12 April 2024
Accepted: 26 June 2024
Available online: 31 October 2024

Keywords:
image, forgery, passive method, deep learning, copy move

ABSTRACT

The widespread and easy-to-use digital tools for manipulating images have made it easier for people to tamper with images, which have increased the number of false or fraudulent images that are shared over the internet and social networks. The massive issue of image forgery requires practical and accurate solutions. In response, a number of deep learning and computer vision techniques have been created to identify digital picture forgeries. This review paper gives a new viewpoint by highlighting recent developments and the need for updated insights, in contrast to previous reviews on deep learning techniques for image forgery detection. This study focuses on how current algorithms employ different deep learning techniques to obtain more accurate results by analyzing the state-of-the-art in deep learning-based copy-move image forgery detection (CMFD). Notably, this review provides a comprehensive classification of the most recent deep learning-based copy-move image forgery detection methods and also gives a succinct summary of deep learning detection techniques. Additionally, the study gives a new comparison between different deep learning algorithms for CMFD and explores widely-used datasets for image forgery detection, enabling a thorough understanding of the problem through a comprehensive analysis and synthesis of the existing literature. Further, this review aims to identify new directions, fill in knowledge gaps, and encourage further research in this important area.

1. INTRODUCTION

In recent years, the importance of detecting image forgery has increased significantly in the real world due to the ease with which a particular image can be altered and shared on social media, leading to the spread of fake news and rumors worldwide [1-3]. Detecting image forgery has become a significant challenge for image forensics due to the availability of sophisticated image manipulation software. Although there have been several traditional approaches for detecting image forgery described in the literature, they tend to focus on extracting simple traits and are designed to address specific types of fraud. However, with the advancement of deep learning techniques, deep learning-based algorithms have gained popularity for detecting fake images. These methods involve building a model that automatically extracts critical features for classification rather than relying on statistical or geometrical computations. Compared to traditional methods, deep learning techniques have demonstrated excellent results in detecting image modifications.

The research on deep learning-based copy-move image forgery detection has important applications in cyber security, computer vision, and digital forensics. For example, CMFD can improve digital evidence processing in forensics, helping law enforcement prosecute cybercrimes and increasing accuracy. Also, it may be used for computer vision problems such as picture identification and object detection, which will result in stronger algorithms. Further, CMFD can help build sophisticated cyber security procedures and solutions that guard sensitive data and guarantee reliable communications by detecting and stopping digital picture manipulation. These cross-disciplinary effects demonstrate the importance and wider application of CMFD.

The purpose of this study is to give researchers an overview of how copy move image forgery research has developed over the last several years and to indicate potential directions for future research. With the use of some insightful comparisons between deep learning-based classifiers and conventional approaches, this study will present performance evaluation, with a focus on the most popular passive detecting copy-move forgeries with deep learning techniques.

The majority of the existing surveys on picture forensics [3-13] centered on traditional feature-based techniques. Recent studies [4, 10] have a specific perspective or scope than ours. Yang et al. [10] categorize the proposed techniques in the literature to two categories: unsupervised and supervised techniques with a special focus on “Deep fake detection techniques”. In fact, this paper employs a wide range of the most recent deep learning techniques to detect forged copies in images. We try also to have a larger coverage than other previous surveys, which have devoted their evaluations to describe and analyze the solutions for one or more specific issues, such as image source identification [10], camera identification [13], and computer-generated picture detection [14].

The remainder of the paper is structured as follows: Section II provides a classification of CMFD techniques and types of picture forgery detection. Section III follows, which presents a description of the copy move image manipulation. Section IV gives an overview of the principal of deep learning based CMFD. Section V presents the traditional and the deep learning methods. Section VI gives keys concepts used in deep learning for CMFD. Section VII reviews the deep learning methods. In section VIII, gives a conclusion that summarize the paper.

2. CLASSIFICATION OF IMAGE FORGERY DETECTION

Due to a rise of criminal activity, image forgery has become a crucial issue that demands attention [15]. Users are now able to transform image content with the use of picture editing software without being able to tell one altered photo from another with the naked eye, which gives them the ability to disseminate misleading information. Furthermore, achieving authenticity and integrity is the main objective of forgery detection in the digital age.

The growth of digital photo fraud has led to a wide variety of image forgeries methods. There are essentially two ways in digital photo forensics: active approaches and passive approaches. Both are composed of several ways, as seen in Figure 1.

2.1 Active approach

In an active method, the digital picture has to pass through some sort of pre-processing, such as adding digital signatures while the image is being made or including a watermark. In fact, this would restrict their use. The two primary active protection methods, as something that is included into photos as they are received, are digital watermarking [16] and signature. If particular information cannot be recovered from the acquired image, we can tell the image has been altered.

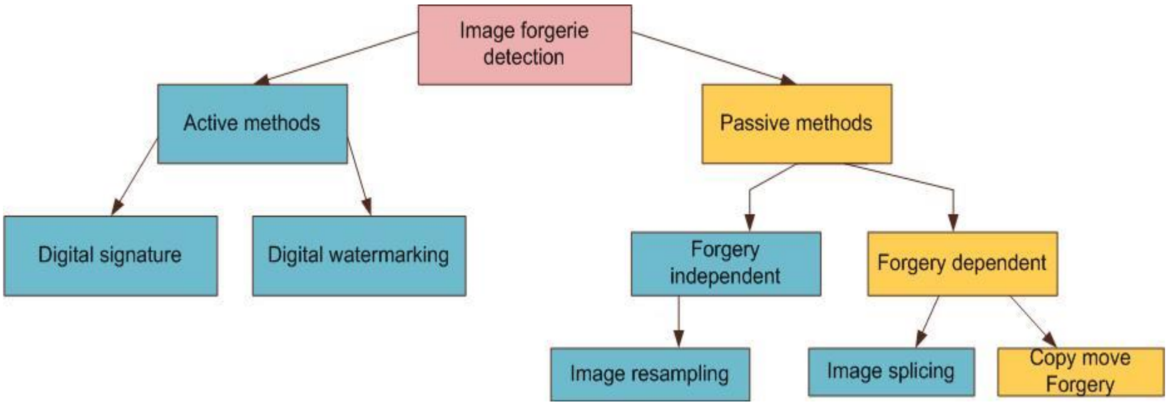

Figure 1. Image forgery techniques

2.2 Passive approach

The passive approach, sometimes referred as the blind approach, is a technique for photograph authentication that just needs the image itself and no prior information of the photograph.

When compared to the active strategy, the passive approach is more challenging since we don't take into account any signatures or watermarks in the image. Format-based or pixel-based techniques are examples of passive approaches. The subcategories of passive method include copy move and copy splicing techniques. Copy move detection technique is one of the most difficult tasks to complete since the duplicated source is included in the same picture, giving both the source and destination areas identical image characteristics. Whereas in splicing technique the source and destination are in two different pictures, in contrast. A piece of the first picture is duplicated and pasted to a second picture to create a copy splice forgery, which results in a fabricated image. The forgery region can be subject to picture alterations such translation, rotation, flipping, and scaling.

3. COPY-MOVE FORGERY

Copy-move image forging is a widely used and uncomplicated method of altering images. This technique involves copying a part of an image and pasting it elsewhere in the same picture. Since the pasted portion comes from the original image, its significant characteristics like color, noise, and texture remain unaltered, making it more difficult to detect this type of image forgery.

The objective of detecting copy-move forgery is to recognize any replicated portions in an image being analyzed, which could suggest an attempt to commit fraud. Copy-move alterations can be classified as "simple", "affine", or "complicated" forgeries, depending on the level of difficulty involved in the copying process.

1. Simple cloning: simple or plain cloning involves copying and pasting a section of an image to a different location without any modifications. This type of cloning can be done using basic picture editing software and is straightforward.

2. Affine cloning: is a type of image tampering that involves altering a portion of an image through scaling and rotation using affine transformations. This results in a new portion of the image that is transformed in a way that is different from the original portion. Affine cloning is similar to plain copy-move tampering and can be easily carried out using image editing software that supports affine transformations.

3. Complex cloning: refers to a more intricate method of altering a replicated section of an image, often involving further processes like blending the edges, estimating diffusion, altering colors, or employing other advanced techniques for image manipulation. Accomplishing complex cloning requires the use of advanced image editing software. Figure 2 illustrates a case of copy-Move forgery, where the left image depicts a manipulated version of the original image on the right, which initially featured three missiles. The forged image

on the left has four missiles, which is an example of the type of alteration that can occur in this type of forgery. Figure 3 gives the number of research papers produced in Springer and IEEE between the years 2016 and 2024.

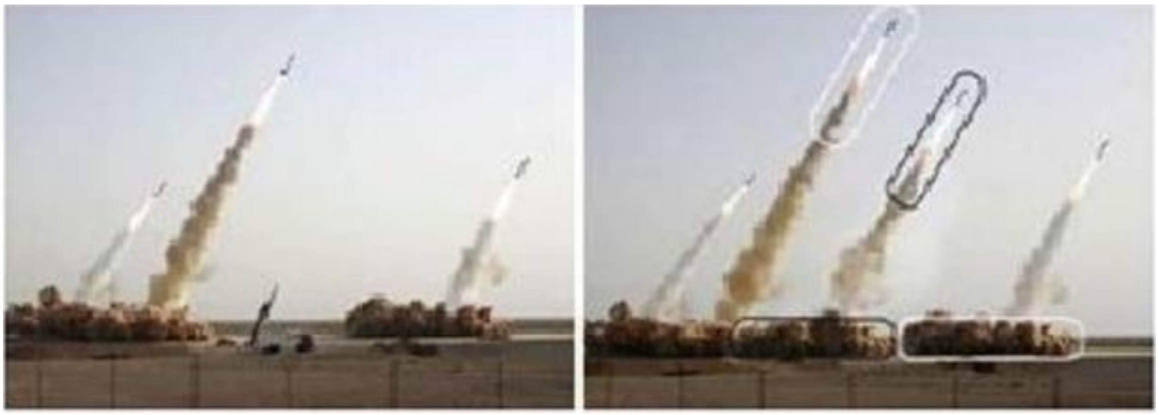

Figure 2. Copy-move forgery example: (left) original image with 3 missiles (right) forged image with 4 missiles

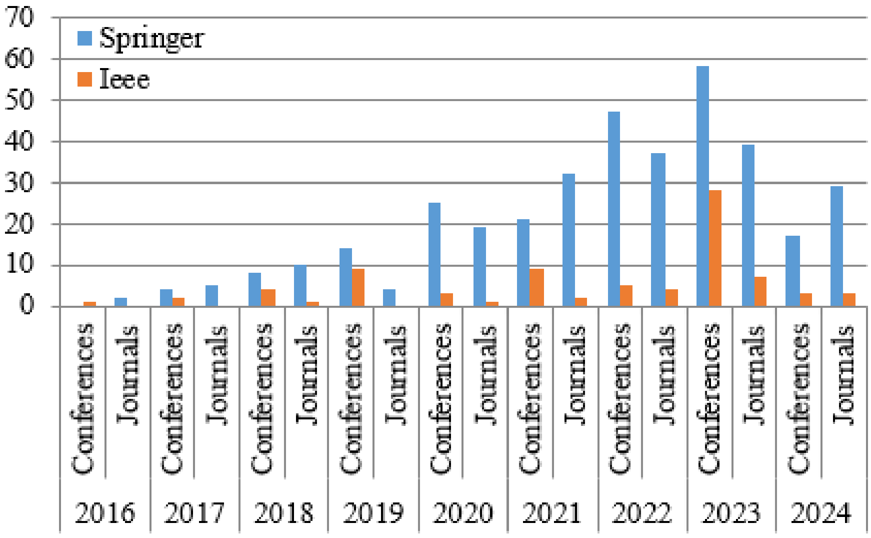

Figure 3. The number of research papers in the field of image forgery detection between 2016 and 2024 in Springer and IEEE

4. DEEP LEARNING PRINCIPALE FOR CMFD

In order to detect copy-move forgeries with high accuracy, the fundamental idea behind deep learning techniques for CMFD is to use deep neural networks to automatically learn and extract discriminative features from digital images. Below is a description of the main Steps:

4.1 Training phase

The first step in this phase is to enter the training dataset, which contains both authentic and altered images. Subsequently, picture pre-processing step ensures dataset homogeneity by standardizing and improving image quality. The modified images are then passed to feature extraction using deep learning techniques to uncover distinct patterns suggestive of copy-move manipulation. The collected features are then passed to further processing in order to improve their representation and normalization and get them ready for classification.

4.2 Testing phase

In the testing phase, the suspect image is given as an input. Then the same steps are made to the input image using methods similar to the training phase.

4.3 Deep learning classification algorithm

After the training and testing phases, the retrieved features are analyzed and the integrity of the image is verified using a deep learning classification algorithm. The classification algorithm assesses the image's patterns and characteristics by feeding the extracted features into the trained model prepared in the training phase. It then assigns a probability or confidence score that indicates the possibility of copy-move manipulation. The image is categorized using this score, which is vital in detecting copy-move forgeries and maintaining the integrity of digital content.

4.4 Classification and decision

After all previous steps, a decision-making process that use predetermined thresholds or criteria for classifying a picture either authentic or fake.

The Figure 4 illustrates the different steps of Deep learning CMFD.

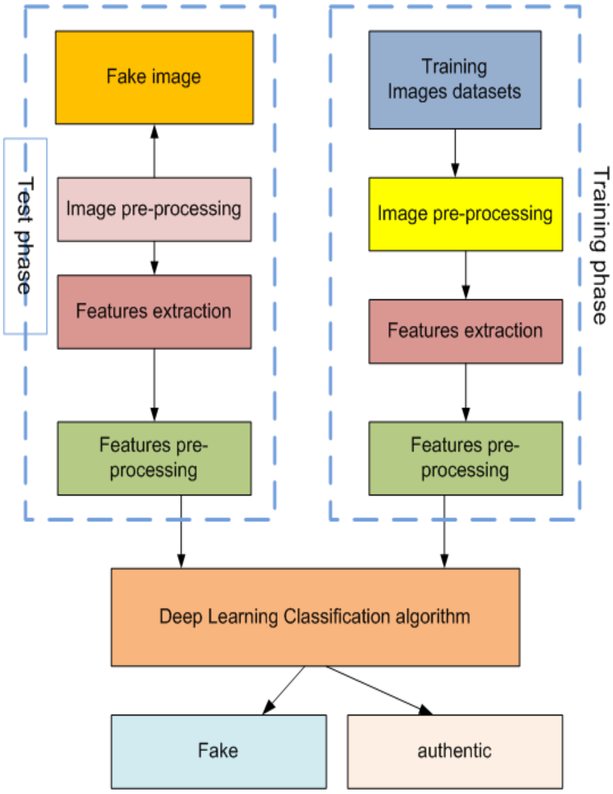

Figure 4. Deep learning steps for CMFD

5. TRADITIONAL VS DEEP LEARNING METHODS FOR CMFD

In the literature the CMFD methods are classified in two categories:

5.1 Traditional methods

In Traditional or image processing based method, there are three main types of traditional methods used for detecting copy-move forgery, namely key points-based (pixel based), overlapping block-based and object based. The overlapping block-based method involves breaking up suspect images into overlapping blocks in order to analyze the similarity of their features and detect any tampered regions. This can be done using techniques such as PCA [17], DCT [18], Zernike [19], and dense-field [20]. While effective, these algorithms are computationally expensive and not suitable for detecting geometric modifications.

On the other hand, key point-based techniques such as SIFT [21], SURF [22], triangle [23] and ORB [24], are more resistant to geometric deformation, but may not work well on areas of the image that are smooth. These methods extract robust key point features and use similarity matching to identify tampered regions.

In the object-based copy-move image forgery detection locates and examines duplicate objects in a picture. Using object detection algorithms, it begins with object detection and then uses techniques to extract characteristics from an object, such as texture, color, and form. After that, related areas in the image are identified by comparing the retrieved characteristics across it. This object-focused method works well for identifying forgeries where entire objects are duplicated and repositioned inside the picture.

The different CMFD categories are illustrated in Figure 5.

Also a comparative table between Traditional and DL approached for CFMD is given in Table 1.

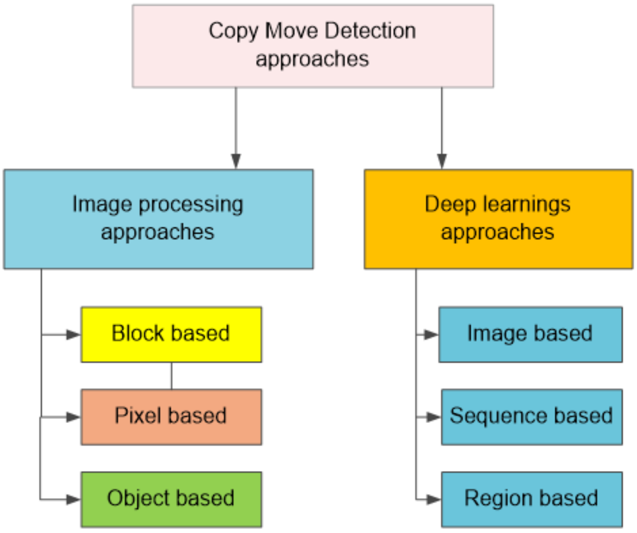
Copy Move Detection approaches
Image processing approaches
Deep learnings approaches
Block based
Pixel based
Object based
Image based
Sequence based
Region based

Figure 5. CMFD categories

Table 1. Traditional methods vs deep learning methods

	Traditional Methods	**Deep Learning Methods**
Avantages	-Resistant to geometric deformations -Effective on smooth areas of images -Well-established and understood techniques -Suitable for specific types of forgery detection	-Automatically learn complex patterns -Reduced need for manual feature engineering -High accuracy with large datasets -Flexibility to adapt to various forgery techniques
Limits	-Computationally intensive -Limited effectiveness on complex tampering -Not suitable for detecting all types of forgery -Manual feature engineering required	-High computational requirements -Need for large amounts of labeled data -Vulnerable to overfitting and dataset biases -Interpretability and explainability challenges

5.2 Deep learning methods

In the CMFD literature, three main approaches are used in deep learning based CMFD: image-based, sequence-based, and region-based. In the image-based approach CNN is used to analyse the full image to extract and match features, suitable for detecting large duplicated regions. Whereas in the sequence-based approach RNNs or Long Short Term Memory networks to capture temporal relationships and identify forgeries with sequential patterns. Finally in the region-based method, which works well for intricate forgeries involving several very small copied segments, divides the image into smaller patches, takes features from each segment, and matches comparable segments.

From another point of view, the proposed approaches base on deep learning for copy-move detection are classified into two subcategories:

5.2.1 Approaches using custom models

These approaches are based on the creation and training of custom deep learning models specifically for copy-move detection tasks. Techniques such as CNN, DNN, and RNN are the most used for this purpose. For example, CNNs are good at spotting replicated regions in faked photos because they are good at collecting spatial hierarchies of characteristics. CNNs and DNNs have powerful capabilities in feature extraction, but they may need a significant amount of processing power. RNNs are mostly made for sequential data, however because they concentrate on temporal links, they might not be the best option for copy-move detection.

5.2.2 Approaches using a model with transfer learning

On the other hand, these methods use transfer learning and pre-trained deep learning models to tackle copy-move detection tasks. Transfer learning is the process of optimizing previously learned models usually CNNs built on substantial datasets like ImageNet to cope with particular objectives like copy-move detection. This method gives excellent performance in CMFD. Transfer learning makes successful feature extraction and classification possible by utilizing the information embodied in pre-trained models. This improves the identification of duplicated portions in forged photos.

6. KEYS CONCEPTS USED IN DEEP LEARNING CMFD

Three concepts on which Deep Learning CMFD techniques are based:

Image artifacts: Undetected irregularities and anomalies that occur when digital images are manipulated which are the result of noise, compression, or modification are known as image artifacts. The irregularities between the original and replicated areas of the picture in terms of texture, color, lighting, or spatial layout are some examples of these artifacts. The deep learning methods use the neural networks capacity to recognize and evaluate these small imperfections, which facilitate the detection of manipulated areas in the fake image.

Attention mechanisms: Used to improve the deep learning models through offering them with the ability to concentrate on pertinent areas of the picture while avoiding irrelevant and noisy areas. These processes enable the model to focus on certain regions of the picture, and improve the capacity to identify pertinent information and produce precise predictions. Object recognition is a common use example of attention techniques. Using combined spatial attention method, the models are able to dynamically change their focus to different portions of the picture based on the presence of objects or patterns of interest. This improves detection accuracy overall and enables more accurate item localization.

Transfer learning: Transfer learning is a machine learning approach in which a model trained for one job is adapted or transferred to perform a related task. Transfer learning is used in deep learning CMFD approaches to fine-tune pre-trained neural networks that have acquired representations of broad image properties from a large dataset for the specialized objective of detecting copy-move fraud. Transfer learning enables deep learning models to efficiently identify and categorize copy move forgeries with minimum of data using pre-training expertise. This strategy considerably minimizes the requirement for considerable training data and processing resources while boosting the detection model's performance and generalizability.

7. DEEP LEARNING METHODS REVIEW

The success of computer vision techniques based on deep learning [10, 25], along with advancements in GPU technology, has led researchers to explore the use of Deep Learning models for detecting image tampering. Deep Learning involves two main stages - feature extraction and classification - and is capable of automatically learning abstract and complex patterns required to identify manipulated areas in images. This approach offers several advantages, such as reducing the time and effort needed to detect hand-crafted features in altered photos. However, training Deep Learning models can be challenging due to the high computational requirements and the need for large amounts of data. Convolutional Neural Networks (CNNs), Deep Neural Networks (DNNs) [26] and Recurrent Neural Networks (RNNs) are some examples of the various Deep Learning models available for this task.

Barad and Goswami [27] carried out a study utilizing deep learning techniques to identify manipulated images. They also evaluated the methods used to verify the authenticity of photographs using publicly available databases.

Wu et al. [28] introduced a deep learning-based architecture called BusterNet for detecting copy move picture fraud. This method is end-to-end trainable and consists of two branches. The first branch identifies manipulation areas using visual artifacts, while the second branch finds copy/move locations based on visual similarities. The authors also provided simple techniques to use out-of-domain datasets and an effective training process for BusterNet. Their extensive research revealed that BusterNet outperformed traditional copy move algorithms by a significant margin.

The importance of utilizing deep learning-based algorithms on publically accessible datasets to identify manipulation in photos was covered by Manjunatha and Patil [29]. They discussed the techniques for passive picture forensic analysis and emphasized upcoming difficulties in creating a system for the identification of altered photos.

Rao and Ni [30] suggested a CNN-based architecture in a different research for the identification of fake digital images. They suggested that the pre-processing phase is directly affected by the first layer of the CNN model. It looks for problems that result from manipulation. SVM was used for the detection phase.

Zhan et al. [31] proposed a transfer learning method that utilizes pre-trained weights from the AlexNet model and an SVM classifier to reduce the time needed for training. The performance of the model was good. Another approach based on transfer learning was developed by Doegar et al. [32], which benefited from previous knowledge obtained through the steganalysis model. With this method, they achieved an average accuracy of 97.36%.

Bi et al. [33] proposed a technique called the Ringed Residual U-Net (RRU-Net) for detecting image forgeries. Their approach involves using an end-to-end image segmentation network to identify manipulations without the need for pre- or post-processing. The RRU-Net architecture is designed to mimic the processes used by the human brain for consolidation and recollection, which can improve the ability of a CNN to learn. By using residual propagation to remember input feature information in a CNN, the authors were able to overcome the problem of gradient degradation. The final output of the RRU-Net combines the remaining answer with the response characteristic, enabling it to distinguish between real and fake areas in an image. Experimental results showed that the proposed technique outperformed existing conventional methods.

In the research [31], another study was introduced that offered a comprehensive solution based on deep neural networks for identifying copy-move fraud. To accomplish this, a convolutional feature extractor was utilized to analyse the input image and extract block-like characteristics, with the VGG16 feature extractor being used. In order to enhance the image resolution, bilinear up-sampling was used. The main limitation of the proposed model was that it did not perform well on images with only textures.

Another recent DL technique for identifying and locating forged areas in compressed pictures is presented in study [34]. The proposed approaches use the EfficientNet model. An effective feature extraction and classification are made using optimization algorithms such as SPOA, CDT, and TAS together with quality criteria. The effectiveness of the proposed approaches is demonstrated by evaluation on CASIA datasets.

The work [35] presents CAMU-Net, an inventive CMFD technique that successfully detects copy-move fraud inside images. Using the VGG16 architecture, the approach use four-step, the first stage, Hierarchical Feature Extraction (HFE_Stage), extracts multi-scale features that capture both global semantics and local details. To improve the accuracy of forgery detection, the ensuing Hierarchical Feature Matching (HFM_Stage) hierarchically matches features. By concentrating on key regions at various sizes through the use of a coordinate attention mechanism, the Coordinate Attention-based Resource Allocation (CARA_Stage) improves matching maps. Lastly, to improve the detection of copy-move forgeries, the Multi-scale Feature Fusion-based Up-sampling (MFFU_Stage) combines data from several scales. During these phases, CAMU-Net outperforms both conventional and deep learning-based techniques in identifying locations in photos where copy-move forgeries are present.

An end-to-end trainable copy-move fusion strategy for CMFD is presented in the work [36], which combines CNN architecture with the benefits of CenSurE keypoint detection. By employing a data-driven approach, the technique is able to detect and localize copy-move forgeries in a variety of picture contexts by continuously updating its learning through training data. The method enables forgery detection across many copy-move attack types, such as basic, post-processed, and geometrically modified forgeries, alos it cane cope with other image processing modifications, by combining CNN features with CenSurE keypoints. The method has strong performance in a range of textures for pictures and gives accurate results under various attack condition.

In the paper [37], skip connections, cycle learning rates (CLR), and a deep CNN-based model named ResNet-101 are coupled to address the issue of exploding and vanishing gradients in CMFD. To demonstrate the efficacy of the model, the work is trained and assessed using datasets such MICC-F600, MICC-F2000, MICC-F220, and CoMoFoD v2. With accuracy rates of up to 97.75% for CoMoFoD v2 after just 5 epochs and 96.09%, 97.63%, and 96.87% for MICC-F220, MICC-F600, and MICC-F2000, respectively, after 10 epochs, the suggested method outperforms the state-of-the-art models currently in operation.

A cmapraison between various deep learning-based methods for detecting copy-move forgery is presented in Table 2.

Table 2. Comparative analysis of deep learning approaches for copy-move detection

	Approaches Using Custom Models	Approaches Using Model with Transfer Learning
Avantages	-Designed and trained only for certain copy-move detection applications -Can be optimized for unique copy-move alterations for a particular type of forgeries -Potentially can give high performance with a proper optimization	-Using pre-trained models decreases the computational cost -Can deal with data scarcity using transfer learning -Pre-trained models gives good results for features extraction and classification
Limits	-Training and development require significant huge expertise and resources -Might consume a large computational resource -Insufficient regularization might lead to overfitting -Can give low performance with new and complex types of copy-move forgeries	-Without substantial fine-tuning, it is possible that copy-move forgeries will not be captured in their entirety -Performance is highly dependent on the quality and relevance of pre-trained models -Less flexible than specific models -The fine-tuning procedure can be time-consuming and labor costly

8. COMPARATIVE AND REVIEW ANALYSIS

The comparison between deep learning-based CMFD solutions with respects to different approaches such as custom or transfer learning models and techniques such as image based or sequence base with respect to various datasets, a variety of methodological strategies and performance results are shown. Techniques like CNN+Simple Linear Iterative clustering and CNN, which use transfer learning from pre-trained models like VGG16, yield outstanding accuracies exceeding 99% on datasets MICC-F220 and synthetic datasets, respectively. On the MICC-F220/MICC-F2000 and NIST Nimble 2016 datasets, for example, custom models like CNN+LSTM and CKN demonstrate competitive performance with F1 scores of 0.5997 and accuracies of 94.86%, respectively. It's interesting to note that techniques like SRM-CNN + SVM and BusterNet demonstrate great accuracies of 98.04% and 96.84% on the UCID and CASIA V1.0 datasets, respectively, without the need for transfer learning, demonstrating the efficacy of well-built custom models.

In another point of view and based on several datasets such as CASIA II, COVERAGE, and CoMoFoD, some solutions for example CNN, Residual, and AR-Net, present comparatively modest performance, with F1 scores of 50.09% and accuracies of 94.26%. In summary, with the conducted research highlights how model design, transfer learning, and dataset properties affect CMFD solutions effectiveness in digital forensics applications.

Table 3. Recent contributions using deep learning-for copy move image forgery detection

Ref.	Deep Learning Approach	Based Model	Localization	Datasets	Results
[30]	SRM-CNN + SVM	Custom model	no	CASIA V1.0	Accuracy = 98.04%
[31]	BusterNet	transfer learning (VGG16)	yes	CASIA and CoMoFoD	F1 =49.26%
[34]	CNN	EfficientNet	yes	CASIA1, CASIA2	Accuracy 98.03%
[35]	CAMU-Net	No transfer learning	No	CASIA2	AUC 87.3%
[36]	CNN	VGG16	yes	GRIP, CASIA1, CASIA2 , MICC-F220	F1 score 96.86 %
[37]	CNN	ResNet-101	yes	MICC-F600, MICC-F2000, MICC-F220, and CoMoFoD v2.	Accuracy 97.75%
[38]	CKN	Custom model	No	MICC-F220 and MICC-F2000	F1 = 0.5997
[39]	CNN	transfer learning (ImageNet)	no	OXFORD	Test Error 2.43 %
[40]	CNN + LSTM	Custom model	no	NIST Nimble 2016	Accuracy = 94.86%
[41]	MFR-CNN	Custom model	yes	UCID	Accuracy = 96.84%
[42]	CNN	Custom model	no	Synthesized dataset	Accuracy = 99.10%
[43]	CNN	transfer learning (VGG16)	yes	CASIA V2.0	F1 = 75.72
[44]	CNN + Siamese Net	transfer learning (Resnet V1)	yes	CASIA and CoMoFoD	-
[45]	AR-Net	transfer learning (VGG16)	yes	Synthesized CASIA II COVERAGE CoMoFoD	F1 =50.09
[46]	Residual and CNN	transfer learning (VGG16)	no	CoMoFoD	Accuracy =94.26%
[47]	InceptionNet	transfer learning (InceptionNet)	no	CASIA	Accuracy =64.29%
[48]	AlexNet	transfer learning (AlexNet)	yes	GRIP	F1=0.93
[49]	CNN+Simple Linear Iterative Clustering	transfer learning (VGG16)	yes	MICC-F220	Accuracy 99.11

Table 4. Datasets used in copy move forgery detection

Dataset	Original/Forged	Format	Size
ST Nimble 17	2667/1410	JPEG, NEF, BMP, PNG, TIFF	60 × 120; 8000 × 5320
Coverage	100/100	C-TIFF	400 × 486
NIST Nimble 16	560/564	L-JPEG	500 × 500; 5616 × 3744
IEEE IFS-TC	1050/1150	C-PNG	1024 × 768; 3000 × 2500
CASIA1	750/975	JPG	384 × 256
CASIA1	7491/5123	JPG, BMP, TIF	320 × 240 – 800 × 600
MICC-F220	110/110	JPG	480 × 722 – 1070 × 800
MICC-F600	40/160	JPG, PNG	722 × 480 – 800 × 600
MICC-F2000	1300/700	JPG	2048 × 1536
SATs-130	10/120	JPG	various
CMFD	0/48	JPG, PNG	various
CoMoFoD	4800/4800	JPG, PNG	various
Korus	220/220	TIF	1920 × 1080
OXFORD	8189	JPG	256× 256
Extended IMD2020	35,000/ 35,000	JPEG, PNG	722×480 to 800×600 pixels
NISL-FIM	1300/700	JPEG	2048 × 1536 pixels
SUN	108,754	JPEG	120,000 pixels
GRIP	80	JPEG, PNG	768 × 1024 or 1024 ×768 pixels
FAU	48	JPEG	3000 × 2000 pixels
CMH JPEG compression	108	JPEG	768 × 1024

Also, the significant discoveries resulting from a comprehensive examination of numerous research publications on the subject of detecting copy-move forgery using deep learning are listed above.

1) Most techniques for detecting forgery are reliant on manually created methods of extracting features, which can

vary greatly depending on the individual. However, with the development of deep learning techniques, it is now possible to automatically extract features. By adopting deep learning, potential human error can be eliminated, and the efficiency of the model can be improved while reducing the time complexity.

2) The localization task of analysing an image focuses on identifying small details, whereas the tampering detection task concentrates on identifying larger, overall changes in the image. It is more challenging to pinpoint the exact area that has been altered in an image through localization compared to detecting whether the image has been tampered with in a broader sense. Few research approaches have successfully identified the precise location of the modified region.

3) Researchers evaluate the effectiveness of tampering detection algorithms using a variety of parameters, including accuracy, precision, recall, F-measure, and others. To compare how well various tampering detection systems, common criteria should be applied.

4) The tampering detection algorithms are evaluated by using a database of both original and modified photos. To accurately assess the algorithms, the database should include a wide variety of original photo types and tampering methods. Although there are publicly available datasets for image altering, their small size limits the use of tampering detection methods based on deep learning.

5) The approach of deep learning relies heavily on data, but when it comes to datasets for copy-move forgery, they are typically limited in size. Consequently, many deep learning researchers resort to using artificially manipulated images as a substitute for training data. These synthetic images are created by altering the tampered area through various transformations, including scaling and rotation by different degrees. Three commonly used copy-move forgery datasets are CoMoFoD, CASIA 2, and COVERAGE, with their details presented in Table 3 and Table 4.

9. RESULTS AND FUTURE CHALLENGES

Deep learning showed a powerful and effective tool for CMFD. In the flowing points some achieved results and future challenge:

9.1 Results

Best accuracy: Deep learning based solutions can give best accuracy in detecting copy-moved manipulations compared to traditional methods. All that is due to their capacity to recognize complex patterns and relations in pictures that are difficult to extract using manually created features.

Robustness: Deep learning models can be more robust to various manipulations like rotation, compression, and noise addition, which forgers often employ to disguise their edits. This is due to the model's ability to learn these variations during training.

Automation: Deep learning approaches can automate the copy-move detection process, reducing the need for manual analysis by forensic experts. This saves time and resources.

9.2 Challenges

Deep learning-based copy-move detection still has several challenges and issues despite the encouraging outcomes:

Big datasets: deep learning models training need a significant amount of data comprising both authentic and fake pictures. Collecting such big datasets can be very expensive.

Computational cost: running deep learning model need powerful and sophisticated hardware which can be costly. The accessibility to such hardware may be not easy.

Manipulation techniques: As image manipulation tools advance, CMFD becomes increasingly challenging and deep learning model-based solutions must be updated and improved on a regular basis to keep up with forgers' inventive ways of creating ever-more-complex forgeries.

Interpretability: It might be challenging to comprehend how deep learning models arrive at judgments because to their complexity. This might provide a challenge in forensic environments when it's crucial to offer context for a finding.

10. CONCLUSIONS

To sum up, this study gives a complete overview of deep learning methods in the detection of copy-move image forgery. By analyzing current research closely, we have revealed how effective deep learning is compared to traditional techniques for identifying areas within images that have been tampered with. The findings reveal that, it is important to embrace advanced approaches when dealing with emerging threats of image manipulation. Its practical implications are enormous as it will help us fight the menace. Law enforcement agencies, digital media companies and related stakeholders can improve their capabilities by incorporating these deep learning-based forgery detection models into their existing forensic tools and image analysis software i.e., enhance their ability to deter against digital misinformation and maintain the reliability of visual content. In addition, it will be crucial to show how these methods work through testing them on real-world based situations while also looking at ways on how they can be rolled out widely.

It is worth noting some limitations that should be considered in interpreting and generalizing this research which provides valuable insights on the use of Deep Learning Techniques for Copy-Move Image Forgery Detection.

The first challenge lies in the scope of dataset employed for training and validation. Although such representative datasets like MICC and CoMoFoD have been used to develop deep networks, they may not completely portray the complexity and variability present in real life situations due to limited diversity and size of the dataset. The deep learning models' performance also depends on factors such as dataset bias, imbalanced class distributions, variations in image quality and resolution among others.

Moreover, these evaluation metrics used to gauge the effectiveness of forgery detection models do not give a true picture of everything about them. Accuracy, precision and recall are some quantifiable ways by which different studies evaluate model performances but might not show how well the model works with unseen data or are sensitive enough for subtle instances of forgery. Additionally, there are significant computational resources required for training and testing deep learning models that could be challenging when it comes to scalability and practical deployment in resource-starved environments.

The other limitation is that it's not easy to detect image forgery due to its complexity. Image forgery detection tasks are so complicated and may involve many types of tampering techniques that require domain-specific knowledge to get accurate results. While deep learning approaches have shown potential in dealing with these challenges, there is still a need for further research to explore hybrid methods where deep learning is combined with traditional image processing techniques and domain expertise.

In view of these constraints, future investigations could be guided toward overcoming these hurdles and coming up with stronger and more dependable systems for detecting fakes that can be used in practical life situations. Additionally, efforts at dataset quality improvement, better evaluation methodologies, and model efficiency optimization will play a critical role in pushing forward the state-of-the-art of copy-move image forgery detection.

REFERENCES

[1] Piva, A. (2013). An overview on image forensics. International Scholarly Research Notices, 2013(1): 496701. https://doi.org/10.1155/2013/496701

[2] Agarwal, S., Farid, H., Gu, Y., He, M., Nagano, K., Li, H. (2019). Protecting world leaders against deep fakes. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops, pp. 38-45.

[3] Bharti, C.N., Tandel, P. (2016). A survey of image forgery detection techniques. In 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, pp. 877-881. https://doi.org/10.1109/WiSPNET.2016.7566257

[4] Castillo Camacho, I., Wang, K. (2021). A comprehensive review of deep-learning-based methods for image forensics. Journal of Imaging, 7(4): 69. https://doi.org/10.3390/jimaging7040069

[5] Rocha, A., Scheirer, W., Boult, T., Goldenstein, S. (2011). Vision of the unseen: Current trends and challenges in digital image and video forensics. ACM Computing Surveys (CSUR), 43(4): 1-42. https://doi.org/10.1145/1978802.1978805

[6] Stamm, M.C., Wu, M., Liu, K.R. (2013). Information forensics: An overview of the first decade. IEEE Access, 1: 167-200. https://doi.org/10.1109/ACCESS.2013.2260814

[7] Birajdar, G.K., Mankar, V.H. (2013). Digital image forgery detection using passive techniques: A survey. Digital Investigation, 10(3): 226-245. https://doi.org/10.1016/j.diin.2013.04.007

[8] Zheng, L., Zhang, Y., Thing, V.L. (2019). A survey on image tampering and its detection in real-world photos. Journal of Visual Communication and Image Representation, 58: 380-399. https://doi.org/10.1016/j.jvcir.2018.12.022

[9] Asghar, K., Habib, Z., Hussain, M. (2017). Copy-move and splicing image forgery detection and localization techniques: A review. Australian Journal of Forensic Sciences, 49(3): 281-307. https://doi.org/10.1080/00450618.2016.1153711

[10] Yang, P., Baracchi, D., Ni, R., Zhao, Y., Argenti, F., Piva, A. (2020). A survey of deep learning-based source image forensics. Journal of Imaging, 6(3): 9. https://doi.org/10.3390/jimaging6030009

[11] Verdoliva, L. (2020). Media forensics and deepfakes: An overview. IEEE Journal of Selected Topics in Signal Processing, 14(5): 910-932. https://doi.org/10.1109/JSTSP.2020.3002101

[12] Zhang, Z., Wang, C., Zhou, X. (2018). A survey on passive image copy-move forgery detection. Journal of Information Processing Systems, 14(1): 6-31. https://doi.org/10.3745/JIPS.02.0078

[13] Wu, J., Feng, K., Tian, M. (2020). Review of imaging device identification based on machine learning. In Proceedings of the 2020 12th International Conference on Machine Learning and Computing, Shenzhen, China, pp. 105-110. https://doi.org/10.1145/3383972.3384037

[14] Ni, X., Chen, L., Yuan, L., Wu, G., Yao, Y. (2019). An evaluation of deep learning-based computer generated image detection approaches. IEEE Access, 7: 130830-130840. https://doi.org/10.1109/ACCESS.2019.2940383

[15] Gupta, S., Mohan, N. (2018). Color channel characteristics (CCC) for efficient digital image forensics. Engineering, Technology & Applied Science Research, 8(1): 2555-2561. https://doi.org/10.48084/etasr.1744

[16] Sanivarapu, P.V., Rajesh, K.N.V.P.S., Hosny, K.M., Fouda, M.M. (2022). Digital watermarking system for copyright protection and authentication of images using cryptographic techniques. Applied Sciences, 12(17): 8724. https://doi.org/10.3390/app12178724

[17] Huang, D.Y., Huang, C.N., Hu, W.C., Chou, C.H. (2017). Robustness of copy-move forgery detection under high JPEG compression artifacts. Multimedia Tools and Applications, 76: 1509-1530. https://doi.org/10.1007/s11042-015-3152-x

[18] Mahmood, T., Nawaz, T., Irtaza, A., Ashraf, R., Shah, M., Mahmood, M.T. (2016). Copy-move forgery detection technique for forensic analysis in digital images. Mathematical Problems in Engineering, 2016(1): 8713202. https://doi.org/10.1155/2016/8713202

[19] Ryu, S.J., Lee, M.J., Lee, H.K. (2010). Detection of copy-rotate-move forgery using Zernike moments. In Information Hiding: 12th International Conference, IH 2010, Calgary, AB, Canada, pp. 51-65. https://doi.org/10.1007/978-3-642-16435-4_5

[20] 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. https://doi.org/10.1109/TIFS.2015.2455334

[21] Costanzo, A., Amerini, I., Caldelli, R., Barni, M. (2014). Forensic analysis of SIFT keypoint removal and injection. IEEE Transactions on Information Forensics and Security, 9(9): 1450-1464. https://doi.org/10.1109/TIFS.2014.2337654

[22] Shivakumar, B.L., Baboo, S.S. (2011). Detection of region duplication forgery in digital images using SURF. International Journal of Computer Science Issues, 8(4): 199-205.

[23] Ardizzone, E., Bruno, A., Mazzola, G. (2015). Copy–move forgery detection by matching triangles of keypoints. IEEE Transactions on Information Forensics and Security, 10(10): 2084-2094. https://doi.org/10.1109/TIFS.2015.2445742

[24] Zhu, Y., Shen, X., Chen, H. (2016). Copy-move forgery detection based on scaled ORB. Multimedia Tools and

Applications, 75: 3221-3233. https://doi.org/10.1007/s11042-014-2431-2

[25] Alsheikhy, A., Said, Y., Barr, M. (2020). Logo recognition with the use of deep convolutional neural networks. Engineering, Technology & Applied Science Research, 10(5): 6191-6194. https://doi.org/10.48084/etasr.3734

[26] Khan, H.R., Hasan, M.A., Kazmi, M., Fayyaz, N., Khalid, H., Qazi, S.A. (2021). A holistic approach to Urdu language word recognition using deep neural networks. Engineering, Technology & Applied Science Research, 11(3): 7140-7145. https://doi.org/10.48084/etasr.4143

[27] Barad, Z.J., Goswami, M.M. (2020). Image forgery detection using deep learning: A survey. In 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, pp. 571-576. https://doi.org/10.1109/ICACCS48705.2020.9074408

[28] Wu, Y., Abd-Almageed, W., Natarajan, P. (2018). Busternet: Detecting copy-move image forgery with source/target localization. In Computer Vision – ECCV 2018: 15th European Conference, Munich, Germany, pp. 170-186. https://doi.org/10.1007/978-3-030-01231-1_11

[29] Manjunatha, S., Patil, M.M. (2021). Deep learning-based technique for image tamper detection. In 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, pp. 1278-1285. https://doi.org/10.1109/ICICV50876.2021.9388471

[30] Rao, Y., Ni, J. (2016). A deep learning approach to detection of splicing and copy-move forgeries in images. In 2016 IEEE International Workshop on Information Forensics and Security (WIFS), Abu Dhabi, United Arab Emirates, pp. 1-6. https://doi.org/10.1109/WIFS.2016.7823911

[31] Zhan, Y., Chen, Y., Zhang, Q., Kang, X. (2017). Image forensics based on transfer learning and convolutional neural network. In Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security, Philadelphia Pennsylvania, USA, pp. 165-170. https://doi.org/10.1145/3082031.3083250

[32] Doegar, A., Dutta, M., Gaurav, K. (2019). CNN based image forgery detection using pre-trained AlexNet model. International Journal of Computational Intelligence & IoT, 2(1).

[33] Bi, X., Wei, Y., Xiao, B., Li, W. (2019). RRU-Net: The ringed residual U-Net for image splicing forgery detection. In 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Long Beach, CA, USA, pp. 30-39. https://doi.org/10.1109/CVPRW.2019.00010

[34] Bhowal, A., Neogy, S., Naskar, R. (2024). Deep Learning-based forgery detection and localization for compressed images using a hybrid optimization model. Multimedia Systems, 30(3): 128. https://doi.org/10.1007/s00530-024-01336-6

[35] Zhao, K., Yuan, X., Liu, T., Xiang, Y., Xie, Z., Huang, G., Feng, L. (2024). CAMU-Net: Copy-move forgery detection utilizing coordinate attention and multi-scale feature fusion-based up-sampling. Expert Systems with Applications, 238: 121918. https://doi.org/10.1016/j.eswa.2023.121918

[36] Diwan, A., Roy, A.K. (2024). CNN-keypoint based two-stage hybrid approach for copy-move forgery detection. IEEE Access, 12: 43809-43826. https://doi.org/10.1109/ACCESS.2024.3380460

[37] Vaishali, S., Neetu, S. (2024). Enhanced copy-move forgery detection using deep convolutional neural network (DCNN) employing the ResNet-101 transfer learning model. Multimedia Tools and Applications, 83(4): 10839-10863. https://doi.org/10.1007/s11042-023-15724-z

[38] Liu, Y., Guan, Q., Zhao, X. (2018). Copy-move forgery detection based on convolutional kernel network. Multimedia Tools and Applications, 77: 18269-18293. https://doi.org/10.1007/s11042-017-5374-6

[39] Ouyang, J., Liu, Y., Liao, M. (2017). Copy-move forgery detection based on deep learning. In 2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI), Shanghai, China, pp. 1-5. https://doi.org/10.1109/CISP-BMEI.2017.8301940

[40] Bunk, J., Bappy, J.H., Mohammed, T.M., Nataraj, N., Flenner, A., Manjunath, B.S., Chandrasekaran, S., Roy-Chowdhury, A.K., Peterson, L. (2017). Detection and localization of image forgeries using resampling features and deep learning. In 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Honolulu, HI, USA, pp. 1881-1889. https://doi.org/10.1109/CVPRW.2017.235

[41] Chen, J., Kang, X., Liu, Y., Wang, Z.J. (2015). Median filtering forensics based on convolutional neural networks. IEEE Signal Processing Letters, 22(11): 1849-1853. https://doi.org/10.1109/LSP.2015.2438008

[42] Bayar, B., Stamm, M.C. (2016). A deep learning approach to universal image manipulation detection using a new convolutional layer. In Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security, Vigo Galicia Spain, pp. 5-10. https://doi.org/10.1145/2909827.2930786

[43] Wu, Y., Abd-Almageed, W., Natarajan, P. (2018). Image copy-move forgery detection via an end-to-end deep neural network. In 018 IEEE Winter Conference on Applications of Computer Vision (WACV), Lake Tahoe, NV, USA, pp. 1907-1915. https://doi.org/10.1109/WACV.2018.00211

[44] Barni, M., Phan, Q.T., Tondi, B. (2020). Copy move source-target disambiguation through multi-branch CNNs. IEEE Transactions on Information Forensics and Security, 16: 1825-1840. https://doi.org/10.1109/TIFS.2020.3045903

[45] Zhu, Y., Chen, C., Yan, G., Guo, Y., Dong, Y. (2020). AR-Net: Adaptive attention and residual refinement network for copy-move forgery detection. IEEE Transactions on Industrial Informatics, 16(10): 6714-6723. https://doi.org/10.1109/TII.2020.2982705

[46] Thakur, R., Rohilla, R. (2019). Copy-move forgery detection using residuals and convolutional neural network framework: A novel approach. In 2019 2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC), Greater Noida, India, pp. 561-564. https://doi.org/10.1109/PEEIC47157.2019.8976868

[47] Zhong, J.L., Pun, C.M. (2019). An end-to-end dense-inceptionnet for image copy-move forgery detection. IEEE Transactions on Information Forensics and Security, 15: 2134-2146.

https://doi.org/10.1109/TIFS.2019.2957693

[48] Muzaffer, G., Ulutas, G. (2019). A new deep learning-based method to detection of copy-move forgery in digital images. In 2019 Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT), Istanbul, Turkey, pp. 1-4. https://doi.org/10.1109/EBBT.2019.8741657

[49] Agarwal, R., Verma, O.P. (2020). An efficient copy move forgery detection using deep learning feature extraction and matching algorithm. Multimedia Tools and Applications, 79(11): 7355-7376. https://doi.org/10.1007/s11042-019-08495-z