Journal of Cyber Security
DOI: 10.32604/jcs.2022.032915
Article

Tech Science Press

Deep Learning Based Image Forgery Detection Methods

Liang Xiu-jian[1,2,*] **and Sun He**[2]

[1]Engineering Research Center of Digital Forensics, Ministry of Education, Nanjing University of Information Science and Technology
[2]School of Computer Science, Nanjing University of Information Science & Technology, Nanjing, 210044, China
*Corresponding Author: Liang Xiu-jian. Email: therxjl@163.com
Received: 01 May 2022; Accepted: 01 June 2022

Abstract: Increasingly advanced image processing technology has made digital image editing easier and easier. With image processing software at one's fingertips, one can easily alter the content of an image, and the altered image is so realistic that it is illegible to the naked eye. These tampered images have posed a serious threat to personal privacy, social order, and national security. Therefore, detecting and locating tampered areas in images has important practical significance, and has become an important research topic in the field of multimedia information security. In recent years, deep learning technology has been widely used in image tampering localization, and the achieved performance has significantly surpassed traditional tampering forensics methods. This paper mainly sorts out the relevant knowledge and latest methods in the field of image tampering detection based on deep learning. According to the two types of tampering detection based on deep learning, the detection tasks of the method are detailed separately, and the problems and future prospects in this field are discussed. It is quite different from the existing work: 1) This paper mainly focuses on the problem of image tampering detection, so it does not elaborate on various forensic methods. 2) This paper focuses on the detection method of image tampering based on deep learning. 3) This paper is driven by the needs of tampering targets, so it pays more attention to sorting out methods for different tampering detection tasks.

Keywords: Digital image forensics; image tampering detection; deep learning; image splicing detection; copy-move detection

1 Introduction

Digital images are an indispensable part of news reports, medical images, diplomatic justice, scientific research and other fields in the information age. People take digital images through digital devices and hope that the photos can truly record real scenes that happen in real life. However, with the development of multimedia technology and image processing technology, it becomes easier to process digital images. The hidden dangers of image security follow, which will undoubtedly bring negative effects to all aspects of society, resulting in a serious crisis of trust. In 2018, in an interview with the

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

National Broadcasting Company (NBC), Russian President Vladimir Putin officially responded to the "bear riding image" that was widely circulated on the Internet: Fig. 1, left, Putin's fake image of riding a bear is actually obtained after tampering with the real image of the horse on the right. It is worth noting that with the development of technology, image tampering for the purpose of transmitting false information has become more and more imperceptible, and can even be faked. Therefore, some important digital image application fields, such as news media, security detection, forensic forensics and other scenarios, should strengthen the detection of image authenticity, and timely find the traces of digital image tampering to ensure the authenticity of digital images.

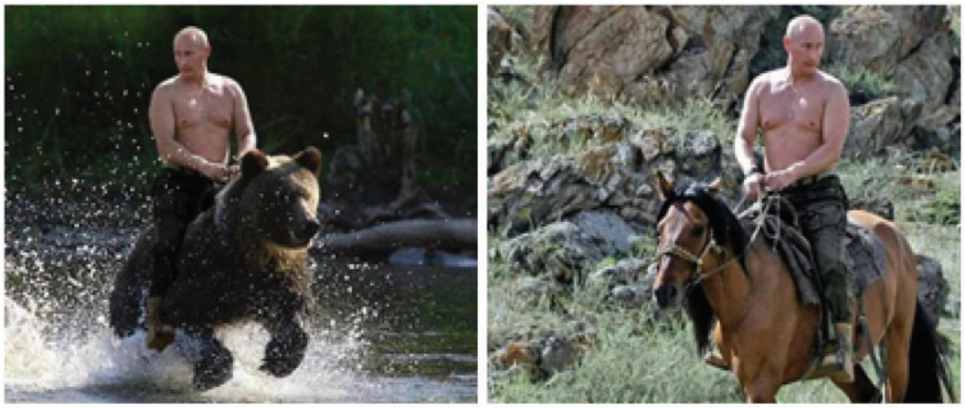

Figure 1: False and real images of "Putin riding a bear"

AlexNet [1] was born in 2012. With the successful application of deep learning in the field of computer vision, since 2016, more and more researchers have tried to apply deep learning methods to the field of image forensics [2–4]. But compared with the tasks in the conventional computer vision field, there are big differences: **1) The recognition target is different**: the image forensics field needs the model to recognize the tampered area of the image; **2) The statistical features are different**: the image forensics task needs to pay attention to the subtle changes of the tampering boundary; **3) Post-processing effects are different**: the image post-processing technology greatly damages the tampering clues of the image.

So far, many image forgery detection methods based on deep learning have emerged, and the performance of forensic methods has been greatly improved. In general, digital image forensics based on deep learning mainly has the following two tasks [5]: **1) Tampering method detection**: It is necessary to identify the tampering method of image content, mainly including splicing, copying-moving, computer generation, multiple **2) Location of tampered area**: It is necessary to locate the tampered area in the false image, and there are two ways to output the content, one is output in the way of bounding box, the other is in the form of binary mask.

In contrast to some existing reviews on digital forensics [6–8], the classification perspective and the focus of our paper are quite different from the existing work: 1) This paper focuses on the image tampering detection problem, and thus does not dwell on various forensic methods including image traceability forensics and image tampering localization. 2) This paper focuses on the detection method of image tampering based on deep learning, and does not invest too much in traditional tampering detection methods. 3) This paper is driven by the demand of tampering targets, and therefore focuses more on the organization of methods for different tampering detection tasks rather than on the classification of deep network architectures.

2 Relevant Knowledge

With the rapid development of network communication and multimedia technology, the security risks of digital images are becoming more and more serious. Therefore, forensic research on digital image tampering becomes very important. At present, the modification methods of digital images [9] mainly include: image manipulation, which refers to the collection of all operations performed on digital images through computer software, also known as image editing. Image forgery, which is a subset of image processing, refers to the modification of images in order to convey deceptive information. Image tampering involves changing part of an image in order to hide an object in the scene, or to add a new object. The relationship between the three image modification methods is shown in Fig. 2.

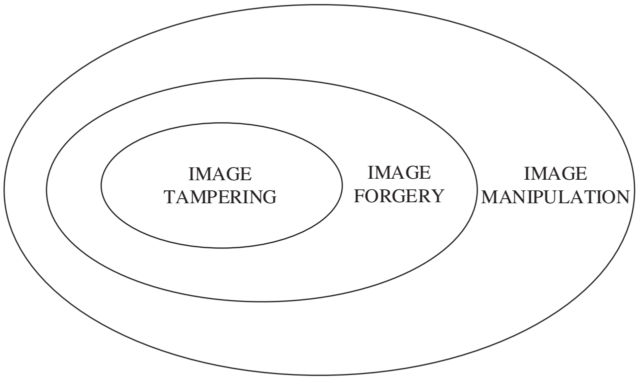

Figure 2: The relationship between the three image modification methods

2.1 Image Tampering Technology

To forensically investigate the tampering of digital images, we first need to understand what are the methods of tampering with digital images. A more comprehensive summary and classification of the tampering methods of digital images was made by Linna [10]. In this paper, we combine the increasingly innovative tampering methods in recent years and classify the specific tampering methods of digital images into eight major categories. A brief description of each of these eight major categories of tampering methods is given below.

(1) **Composited**, a compositing operation is the process of combining parts of images into a single image to create an erroneous visual effect on the viewer.

(2) **Re-touched**, which mainly refers to the use of image editing tools to beautify, stretch and skin the content of the image, so as to achieve the purpose of hiding some important details of the image or repairing some broken images. It is widely used in more and more image editing tools such as Photoshop.

(3) **Computer Generated**, these are images that are generated in specialized software using computer code. With the progress of science and technology, computer-generated pictures can already reach the degree of falseness.

(4) **Morphed**, which is to gradually change an image into another image. We first find out the feature points between the two images, and then superimpose the two images with different weights to obtain different intermediate images, so as to obtain a tampered image with the features of both images.

(5) **Enhanced**, mainly by changing the brightness, light, contrast and color level of the image, in order to highlight some areas of the image. This method usually does not involve a change in the content of the image, but only to enhance the overall appreciation of the image.

(6) **Painted**, which is an image drawn by drawing software (such as Photoshop and CAD) or other drawing tools. Tamperers are good at using such images for some commercial promotional activities, which bring some trouble to people's life.

(7) **Rebroadcast**, which refers to the use of photo acquisition tools to obtain new digital images by secondary acquisition of images that are needed but difficult to obtain. The images obtained after secondary acquisition can deceive people and be used by unscrupulous people to do improper things.

(8) **Stego Image**, which is to hide the image or text that needs to be transmitted or hidden in a carrier image, so that the transmitter or the witness cannot judge through the carrier image itself whether it has hidden information other than the image itself, thus achieving the purpose of secure transmission of secret information.

2.2 Image Forensic Technology

The forensic technology of digital image tampering is mainly to identify the authenticity, integrity and origin of the image by analyzing the characteristics of the digital image. In other words, the forensic technology of digital image tampering mainly judges whether the content of the image is real after the image is generated from the imaging device, whether the image has been tampered with, and what kind of device is it generated from.According to the analysis of some existing achievements, the forensic technology of digital image tampering is mainly divided into active forensics technology and passive forensics technology. The specific classification is shown in Fig. 3. Next, this article will introduce the classification and methods of image forensics in detail.

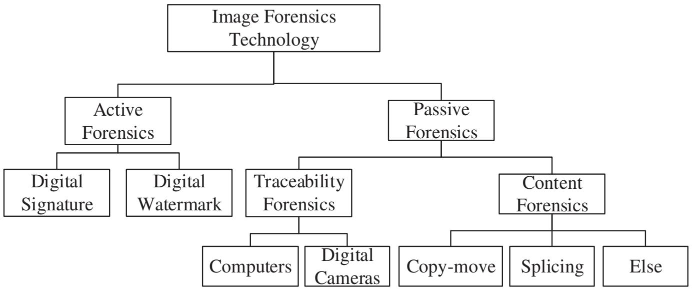

Figure 3: Classification of forensic techniques for digital image tampering

2.2.1 Image Active Forensics Technology

The main feature of active image forensics is the need to embed secret information in the image beforehand [11], and the receiver receives the image and then extracts a watermark or digital signature to determine whether the image has been tampered with by judging the condition of the watermark or signature.

In 1994, Schyndel defined the concept of "digital watermark" for the first time and proposed an encryption technique that embeds cryptographic information in images invisible to the human eye. Digital watermarking contains two main parts: watermark embedding module, and watermark extraction and verification module. As shown in Fig. 4:

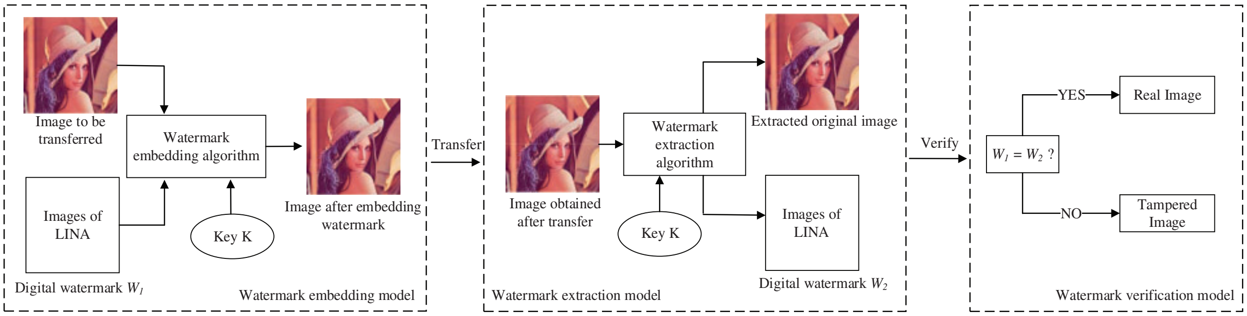
Image to be transferred
Watermark embedding algorithm
Image after embedding watermark
Images of LINA
Key K
Digital watermark W_1
Watermark embedding model
Transfer
Image obtained after transfer
Watermark extraction algorithm
Extracted original image
Key K
Images of LINA
Digital watermark W_2
Watermark extraction model
Verify
$W_1 = W_2$?
YES
Real Image
NO
Tampered Image
Watermark verification model

Figure 4: Flow of digital watermarking active forensics algorithm [12]

The principle of digital signature technology is similar to that of digital watermark technology, and the digital signature-based image active forensics technology merges the image and its digest encryption to form a digital signature. When verifying the authenticity of an image, the abstract is extracted from the image and a digital signature is generated, and the image is judged by comparing the digital signature to determine whether it has been tampered with. The specific process is shown in Fig. 5.

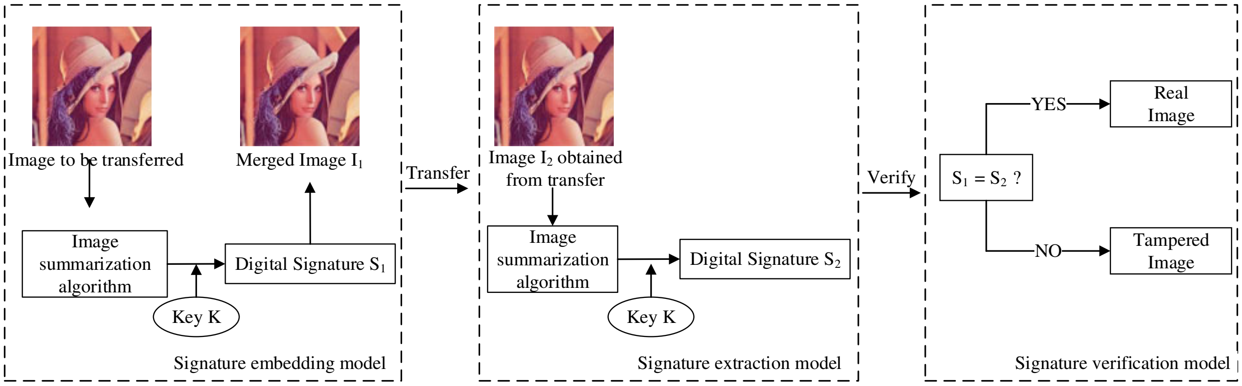
Image to be transferred
Merged Image I_1
Image summarization algorithm
Digital Signature S_1
Key K
Signature embedding model
Transfer
Image I_2 obtained from transfer
Image summarization algorithm
Digital Signature S_2
Key K
Signature extraction model
Verify
$S_1 = S_2$?
YES
Real Image
NO
Tampered Image
Signature verification model

Figure 5: Flow of digital signature active forensic algorithm [13]

However, in practical applications, due to various reasons, the watermark may not be embedded in the image in time, which will affect the use of the image. Therefore, the passive forensics technology of digital image tampering has become a research direction with great research value at home and abroad.

2.2.2 Image Passive Forensics Technology

Passive image forensics [14] is also known as digital image Blind Forensics, where the "blind" means that the forensics can be performed directly from the image without a pre-embedded digital watermark or signature, which is more widely applicable compared to active forensics.

Image traceability forensics refers to identifying the acquisition device of an unknown image. Lukas [15] et al. were the first to propose a pattern noise approach to identify the source of an image, and in the paper, source identification was performed for nine different devices with a recognition rate of 100%. Swaminathan et al. [16,17] used CFA (Color Filter Array) interpolation as a method and then used SVM to classify' images generated by 19 different devices and the accuracy could reach 85%. san

Choi [18] et al. extracted the linear distortion in the images for image sources for identification, and the accuracy can reach 92% by classifying three device images. The current artificial intelligence generated images are prevalent , and the main identification methods proposed earlier are: current identification methods based on imaging devices [19,20], geometric features [21] and statistical features [22,23].

Deep learning methods can regard passive image forensics as object detection problems and anomaly detection problems [8]. In recent years, more scholars hope to take advantage of the self-adaptability of deep learning methods to enable deep learning models to automatically extract effective features. However, due to the fact that the data set is too small and the tampering methods are various, this is still the main problem of deep learning methods in images. Most of the current image tampering is to modify the image content, such as stitching [24,25], copy-move [26–28], image restoration [29,30], etc. The following will describe the data set evaluation indicators.

2.3 Data Set and Evaluation Indicators

2.3.1 Data Set

Collecting and constructing image datasets suitable for tampering localization tasks is not an easy task. In tasks such as image tampering detection, it is often possible to generate large amounts of data using programs that batch process images, but it is difficult to obtain a high-quality dataset of tampered images using similar methods. This is because the images in the dataset are supposed to objectively reflect the actual tampering situation, which requires that the modifications made in the original image should indeed distort its semantics and that the resulting image should not contain obvious visual anomalies. At the same time, to assist in the training of the classifier, corresponding pixel-level labels need to be provided for each tampered image. This in turn makes it difficult to directly collect a potentially large number of tampered images in the network as a dataset. In summary, a more desirable approach to construct tampered image datasets is to generate tampered images manually under controlled conditions [31]. Currently, some publicly available tampered image datasets exist, and the relevant information is summarized in Tab. 1.

Table 1: Publicly used commonly used tampered image datasets

Name	Time	Image format	Image size	Number (True/False)	Tampering methods
NLPR-LSCGB [32]	2021	PNG, JPG	512 × 512–6000 × 4000	71168/71186	Computer-Generated
IMD 2020 [33]	2020	PNG, JPG	193 × 260–4437 × 2958	37010/37010	Multiple Operations
DEFACTO [34]	2019	TIF	240 × 320–640 × 640	-/229000	Multiple Operations
FantasticReality [35]	2019	JPG	280 × 800–6000 × 4000	16592/19423	Splicing
MFC 19 [36]	2019	RAW, PNG, BMP, JPG, TIF	160 × 120–2624 × 19680	10279/5750	Multiple Operations
MFC 18 [37]	2018	RAW, PNG, BMP, JPG, TIF	128 × 104–7952 × 5304	14156/3265	Multiple Operations
PS Battle [38]	2018	PNG, JPG	130 × 60–10000 × 8558	11142/102028	Multiple Operations

(Continued)

Table 1: Continued

Name	Time	Image format	Image size	Number (True/False)	Tampering methods
NIST NC 17 [37]	2017	RAW, PNG, BMP, JPG	160 × 120–8000 × 5320	2667/1410	Multiple Operations
Coverage [39]	2016	TIF	400 × 486	100/100	Copy-Move
NIST NC 16 [37]	2016	JPG	500 × 500–5616 × 3744	560/564	Splicing, Copy-Move
RFD-Korus [40]	2016	TIF	1920 × 1080	220/220	Splicing, Copy-Move
Wild Web [41]	2015	PNG, BMP, JPG, GIF	72 × 45–3000 × 2222	90/9657	Real Cases
CASIA v1 [42]	2013	JPG	384 × 256	800/921	Splicing, Copy-Move
CASIA v2 [43]	2013	JPG, BMP, TIF	240 × 160–900 × 600	7200/5123	Splicing, Copy-Move
CoMoFoD [44]	2013	PNG, JPG	512 × 512–3000 × 2000	260/260	Copy-Move
DSO-1 [45]	2013	PNG	2048 × 1536	100/100	Splicing
IEEE IFS-TC [46]	2013	PNG	1024 × 768–3000 × 2500	1050/1150	Splicing, Copy-Move

It is worth noting that deep learning-based approaches require high data size, and data volumes in the tens of thousands. Therefore, in some deep learning-based image tampering localization efforts other datasets are also used to automate the generation of a large number of tampered images as training data [47,48], but the quality of such automatically generated tampered images is not high. As far as the available literature is concerned, several datasets such as MSCOCO [49], Deresden [50], ImageNet [51], MITPlaces [52], and SUN [53] are commonly used as raw material for automatically generated tampered images.

2.3.2 Evaluation Indicators

As mentioned earlier, image tampering localization is actually a pixel-level binary classification problem. Therefore, the performance of the tampering model can be measured by the commonly used classification evaluation metrics. The commonly used evaluation metrics include Accuracy (ACC), F1-score, Area Under the Curve (AUC), Matthews Correlation Coefficient (MCC), and Intersection over Union (IoU). Intersection over Union (IoU), etc.

3 Splicing Tampering Detection Based on Deep Learning

3.1 Splicing Detection Based on Single Tampering

The image stitching operation refers to stitching a part of the donor image into the source image to generate a new tampered image. Compared with other image content tampering detection, image stitching detection is simpler, because different images have different feature information, the comparison between the stitched area and the real area is usually obvious, and there are relatively more features that can be used.

In 2016, Zhang et al. [54] applied deep learning techniques to image passive forensics for the first time and proposed a deep learning image forensics method based on Daubechies wavelet features. The tampered region was relatively roughly localized and the recognition accuracy was low. Long et al. [55] had proposed a full convolutional network for semantic segmentation task in 2015, which achieved pixel-level classification. Inspired by this, in 2017, Salloum et al. [56] proposed a multi-task image passive forensic framework (MFCN) based on edge reinforcement for pixel-level tampered region segmentation.

Since image stitching and tampering is to stitch together two different image regions, how to distinguish the source of the donor image is a key issue. In 2021, Niu et al. [57] proposed an end-to-end system for stitching detection and localization of Double-JPEG images. It can also distinguish regions from different donor images. The proposed method can work in a wide variety of settings, including aligned and unaligned dual JPEG compression, with superior performance compared to baseline methods working under similar conditions.

Almost all of the above methods use deep network models, and these methods require dense pixelated image data to train the network. On the one hand, it is impractical to construct a training set to represent the myriad of tampering possibilities. On the other hand, this method is often limited in social media platforms or commercial applications. In 2022, Agrawal et al. [58] proposed a method of Self-Supervised Image Signature Learning (SISL) to train a splice detection localization model from image frequency transformation, as shown in Fig. 6. Experiments demonstrate that the model can produce performance similar to or better than multiple existing methods on standard datasets without relying on labels or metadata.

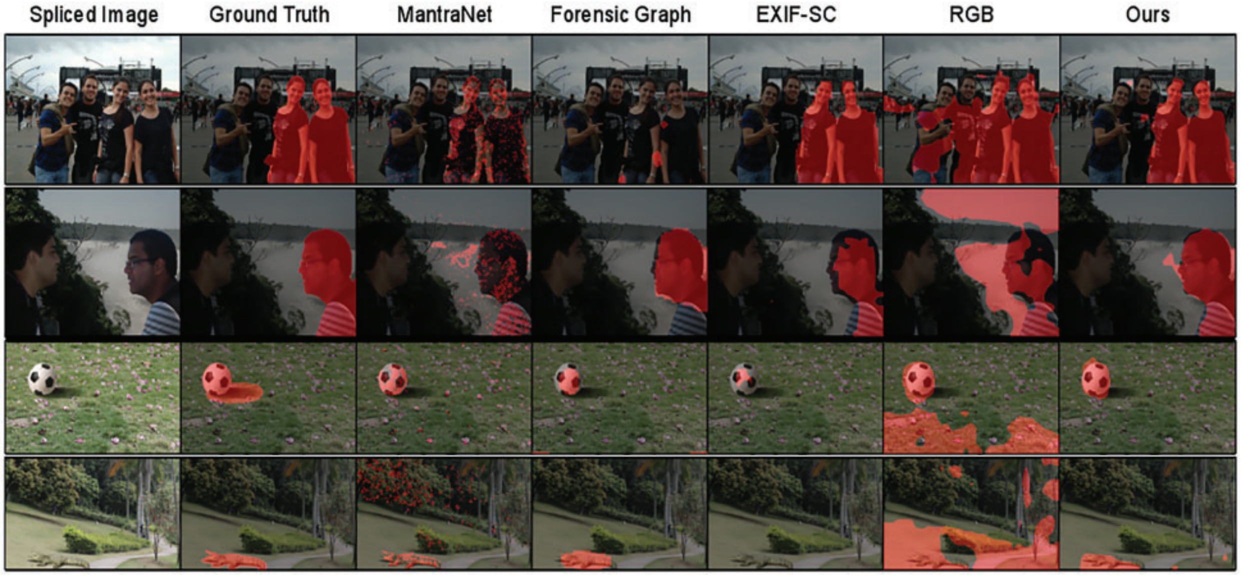

Figure 6: Comparison of detection and localization effects between SISL and other methods [58]

3.2 Splicing Detection Based on Constraint Image

Due to the complexity and diversity of current tampering techniques, it is difficult to extract effective generic features from a single image for learning, so Wu et al. [59] extended the stitching detection task: the original single tampered image detection task was extended to a source and donor image similarity matching task called constrained image stitching detection task (CISD).

Yue Wu et al. proposed a structure called deep matching verification network (DMVN) [59]. It is worth mentioning that the authors introduce the Attention idea at the end of the framework to extract the tampered region features again for visual consistency verification based on the obtained mask, which further improves the region segmentation accuracy. Although the accuracy of detection methods based on Convolutional Neural Network (CNN) has been improving, the performance of existing detection methods is still unsatisfactory. 2019 Bi et al. [60] proposed a Ringed Residual U-Net (RRU-Net) based on the existing U-Net [61], as shown in Fig. 7.The residual propagation recalls the feature information of the source and donor images to solve the gradient degradation problem in the deep network; the residual feedback consolidates the input feature information to make the similarity of image attributes between the source and donor image tampered regions more obvious. And the F1-score reaches 84.1% on CASIA v2, and the F1-score performance is 91.5% on COLUMB [62].

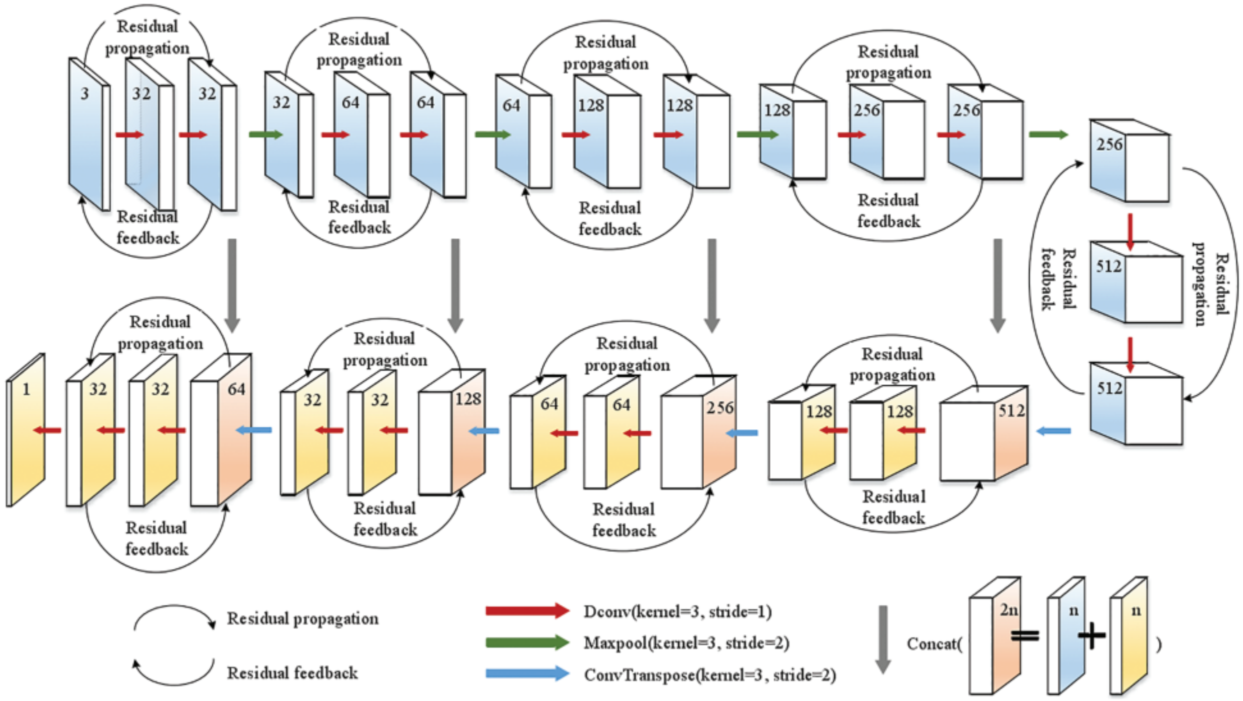

Figure 7: RRU-Net network structure [61] (numbers represent the number of features)

Inspired by the Deep Matching Verification Network (DMVN) [59] of Yue Wu et al., Liu et al. [63] proposed a Deep Matching Model (DAMC) based on atrous convolution in 2019, which also uses tampered images and feeds. volume image as input. The model is based on the GAN [64] framework and is divided into DMAC network, category detection network and area localization network. Compared with DMVN, the model further improves the recognition accuracy.

4 Copy-move Tampering Detection Based on Deep Learning

An image copy-paste operation refers to copying an area of an image and pasting it into the same image. Often, copy-paste operations are used to mask an area in an image to make it difficult to distinguish between real and fake. This tampering method is the same as stitching, both tampering with the content of the image, but the detection difficulty is much higher than that of stitching technology. Because the copy-paste operation is an internal operation of the same image, the real area and the tampered area are very similar in statistical properties, so the inherent properties of the imaging device and most of the image statistical characteristics cannot be used. Currently, image copy-paste detection techniques can be divided into two categories: 1) based on region boundary artifacts, and 2) based on region similarity.

4.1 Copy-move Detection Based on Region Boundary

The image after copy-paste operation usually has boundary artifacts between the tampered area and the boundary of the real area, which is very different from the real image. The detection method based on boundary artifact is to use convolutional network to extract image boundary information, and then classify it through machine learning classifier.

In 2016, Rao et al. [4] applied the deep learning method to the copy-paste operation detection task for the first time. Experiments show that this method can effectively learn boundary artifact features, capture boundary abnormal information, and achieve high classification accuracy. In 2017, Ouyang et al. [65] proposed a copy-paste detection method based on convolutional neural network. Since the amount of copy-paste dataset is too small, the model is first pre-trained on ImageNet, and then the network parameters are fine-tuned using smaller copy-paste training samples, and the final model achieves true and false image classification.In 2020 Kumar et al. [66] used deep semantic image painting and copy-move forgery algorithms to create a synthetic forgery dataset. And use an unsupervised domain adaptation network to detect copy-move forgery behaviors in new domains by mapping the feature space of the synthesized datasets, improving the F1-scores of the CASIA and CoMoFoD datasets to 80.3% and 78.8%, respectively.

Although the method based on region boundary artifact is more in line with human visual habits, it is very difficult for deep learning networks to extract such small boundary artifact information. Therefore, the recognition model using this method can only complete the true and false classification of images, and cannot achieve pixel-level region segmentation.

4.2 Copy-move Detection Based on Regional Similarity

The essence of the copy-stitch operation is to copy an area of an image and paste it into the same image. The image generated by this tampering method must contain two identical regions, so researchers propose a detection method based on regional similarity, which is very similar to the Constrained Image Splicing Detection (CISD) task in the splicing detection problem.

In 2018, Wu et al. [67] proposed an image copy-paste forgery detection framework. This method realizes pixel-level copy-paste task detection for the first time, and the recognition accuracy exceeds that of traditional detection methods. Soon Wu et al. [68] further extended this framework, combining the strengths of boundary artifact-based methods and region similarity methods, and proposed BusterNet, which can detect source targets and tampered targets, as shown in Fig. 8. The model is divided into Mani-Det branch and Simi-Det branch. It is worth noting that the model fuses the features of the Mani-Det branch and the Simi-Det branch, and then classifies the two similar regions at the pixel level to accurately predict the source target and the tampered target. Experiments show that the method has good robustness and achieves the best results on multiple datasets.

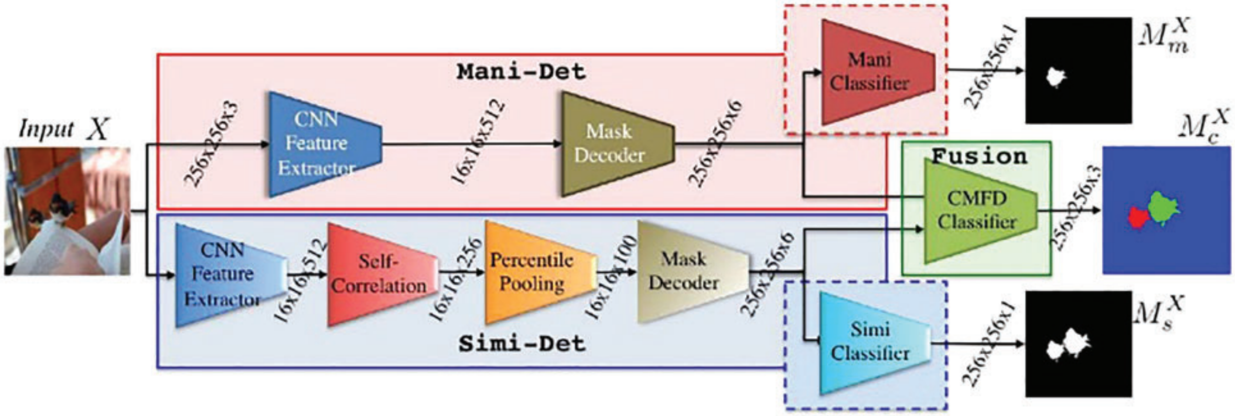

Figure 8: BusterNet network structure [68]

However, the above parallel deep neural network approach still suffers from 1) the necessity to ensure that both branches correctly locate regions; 2) the Simi-Det branch only uses VGG16 with four pooling layers to extract single-level and low-resolution features. In 2021, Chen et al. [69] innovatively proposed a serial deep neural network approach by introducing two successively constructed sub-networks: the replication-move similarity detection network (CMSDNet) and source/target region differentiation network (STRDNet) ensured the correct identification of both branches; by removing the last pooling layer in VGG16, atrous convolution was introduced to preserve the field of view of the filter after removing the fourth pooling layer; STRDNet was designed to obtain similar regions directly from CMSDNet that are identified as tampered and untampered regions at the image level.

5 Conclusion

This paper summarizes the image forgery localization method based on deep learning. In particular, we comb these methods by the network architecture they use. It can be seen that different network architectures have their own characteristics and advantages, which provide a variety of choices for the design of tamper location methods for different specific problems. Deep learning technology is still developing, which brings a lot of challenges and opportunities to image forgery positioning. This paper also introduces datasets and performance evaluation metrics commonly used in image forgery localization, and discusses current issues and some possible research directions in this field. This helps readers to fully grasp the research trend in the field of image forgery location.

Looking forward to the future, we will continue to explore the long road of fighting against image tampering and forgery, and constantly enrich the technical equipment library of digital image forensics to escort the security of multimedia information.

Funding Statement: This work is supported by Key Projects of Innovation and Entrepreneurship Training Program for College Students in Jiangsu Province of China (202210300028Z).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Krizhevsky, I. Sutskever and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," *Commun. ACM*, vol. 60, no. 6, pp. 84–90, 2017, (June 2017). https://doi.org/10.1145/3065386.

[2] J. Bunk, "Detection and localization of image forgeries using resampling features and deep learning," in *2017 IEEE Conf. on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pp. 1881–1889, 2017, https://doi.org/10.1109/CVPRW.2017.235.

[3] N. Huang, J. He and N. Zhu, "A novel method for detecting image forgery based on convolutional neural network," in *2018 17th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications/12th IEEE Int. Conf. on Big Data Science and Engineering (TrustCom/BigDataSE)*, pp. 1702–1705, 2018, https://doi.org/10.1109/TrustCom/BigDataSE.2018.00255.

[4] Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," in *2016 IEEE Int. Workshop on Information Forensics and Security (WIFS)*, pp. 1–6, 2016, https://doi.org/10.1109/WIFS.2016.7823911.

[5] S. Walia and K. Kumar, "Digital image forgery detection: A systematic scrutiny," *Australian Journal of Forensic Sciences*, vol. 51, no. 5, pp. 488–526, 2019.

[6] P. Korus, "Digital image integrity, A survey of protection, and verification techniques," *Digital Signal Process Ing*, vol. 71, pp. 126, 2017.

[7] L. Verdoliva, "Media forensics and deep fakes: A no study on the influence of the temperature on the performance of the system," *IEEE. Journal of Selected Topics in Signal. Processing*, 2020, vol. 14, no. 5, pp. 910–932, 2020.

[8] I. Castillo Camacho and K. Wang, "A comprehensive review of deep learning-based methods for image forensics," *Journal of Imaging*, vol. 7, no. 4, pp. 69, 2021.

[9] L. Zheng, Y. Zhang and V. L. Thing, "A survey on image tampering and its detection in real-world photos," *Journal of Visual Communication and Image Representation*, vol. 58, pp. 380–399, 2019.

[10] R. Y. Wang, B. L. Chu, Z. Yang, Zhou Linna, "A Review of Visual Depth Forgery Detection Technology," *Chinese Journal of Image and Graphics*, vol. 27, no. 1, pp. 43–62, 2022.

[11] D. A. Warbhe, R. V. Dharaskar and V. M. Thakare, "Computationally efficient digital image forensic method for image authentication ⋆," *Procedia Computer Science*, vol. 78, no. 464–470, 2016.

[12] C. Kumar, A. Singh and P. Kumar, "A recent survey on image watermarking techniques and its application in e-governance," *Multimedia Tools and Applications*, vol. 77, pp. 3597–3622, 2018.

[13] A. S. Kittur and A. R. Pais, , " Batch verification of digital signatures: Approaches and challenges," *Journal of Information Security and Applications*, vol. 37, pp. 15–27, 2017.

[14] Z. J. Barad and M. M. Goswami, "Image forgery detection using deep learning: A survey," in *2020 6th Int. Conf. on Advanced Computing and Communication Systems (ICACCS)*, pp. 571–576, 2020, https://doi.org/10.1109/ICACCS48705.2020.9074408.

[15] J. Lukas, J. Fridrich and M. Goljan, "Digital camera identification from sensor pattern noise," *In IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 205–214, 2006, https://doi.org/10.1109/TIFS.2006.873602.

[16] A. Swaminathan, M. Wu and K. J. R. Liu, "Nonintrusive component forensics of visual sensors using output images," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 1, pp. 91–106, 2007, https://doi.org/10.1109/TIFS.2006.890307.

[17] A. Swaminathan, M. Wu and K. J. Ray Liu, "Component forensics of digital cameras: A non-intrusive approach," in *2006 40th Annual Conf. on Information Sciences and Systems*, pp. 1194–1199, 2006, https://doi.org/10.1109/CISS.2006.286646.

[18] E. Y. Lam, S. C. Kai and K. Y. Wong, "Automatic source camera identification using the intrinsic lens radial distortion," *Optics Express*, vol. 14, no. 24, pp. 11551–65, 2006.

[19] A. C. Gallagher and T. Chen, "Image authentication by detecting traces of demosaicing," in *2008 IEEE Computer Society Conf. on Computer Vision and Pattern Recognition Workshops*, pp. 1-8, 2008, https://doi.org/10.1109/CVPRW.2008.4562984.

[20] A. E. Dirik, S. Bayram, H. T. Sencar and N. Memon, "New features to identify computer generated images," in *2007 IEEE Int. Conf. on Image Processing*, pp. IV-433–IV-436, 2007, https://doi.org/10.1109/ICIP.2007.4380047.

[21] T. Ng, S. F. Chang and J. Hsu, "Physics-motivated features for distinguishing photographic images and computer graphics," in *Proc. of the ACM Int. Conf. on Multimedia*, F, 2005.

[22] Y. Wang and P. Moulin, "On discrimination between photorealistic and photographic images," in *2006 IEEE Int. Conf. on Acoustics Speech and Signal Processing Proc.*, pp. II–II, 2006, https://doi.org/10.1109/ICASSP.2006.1660304.

[23] W. Chen, Y. Q. Shi and G. Xuan, "Identifying computer graphics using HSV color model and statistical moments of characteristic functions," in *2007 IEEE Int. Conf. on Multimedia and Expo*, pp. 1123–1126, 2007, https://doi.org/10.1109/ICME.2007.4284852.

[24] Y. Q. Shi, C. Chunhua and C. Wen, "A natural image model approach to splicing detection," in *Proc. of the 9th Workshop on Multimedia and Security*, pp. 51–62, 2007.

[25] W. Wang, J. Dong and T. Tan, "Effective image splicing detection based on image chroma," in *2009 16th IEEE Int. Conf. on Image Processing (ICIP)*, pp. 1257–1260, 2009, https://doi.org/10.1109/ICIP.2009.5413549.

[26] Fridrichaj and Soukalbd, "Detection of copy move forgery in digital images," in *Proc. of the Digital Forensic Research Workshop*, 2003.

[27] J. Li, X. Li, B. Yang and X. Sun, "Segmentation-based image copy-move forgery detection scheme," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 507–518, 2015, https://doi.org/10.1109/TIFS.2014.2381872.

[28] L. Zijian and R. qiuqi, "Detection of copy move based on LPP and improved SIFT," *Signal Processing*, vol. 33, no. 4, pp. 589–594, 2017. (in Chinese).

[29] J. H. Bappy, C. Simons, L. Nataraj, B. S. Manjunath and A. K. Roy-Chowdhury, "Hybrid LSTM and encoder–Decoder architecture for detection of image forgeries," *In IEEE Transactions on Image Processing*, vol. 28, no. 7, pp. 3286–3300, 2019, https://doi.org/10.1109/TIP.2019.2895466.

[30] Y. Wu, W. AbdAlmageed and P. Natarajan, "ManTra-Net: Manipulation tracing network for detection and localization of image forgeries with anomalous features," in *2019 IEEE/CVF Conf. on Computer Vision and Pattern Recognition (CVPR)*, pp. 9535–9544, 2019, https://doi.org/10.1109/CVPR.2019.00977.

[31] L. Haodong, Z. Peiyu and L. Bin, "A survey on deep learning based digital image tampering loculi," *Journal of Signal Processing*, vol. 5, no. 12, pp. 2278–2301, 2021, https://doi.org/10.16798/j.iSSN.10030530.2021.

[32] W. Bai, Z. Zhang and B. Li, "Large-scale CG images benchmark, NLPR-LSCGB," https://github.com/wmbai/LSCGB.

[33] A. Novozámský, B. Mahdian and S. Saic, "IMD2020: A large-scale annotated dataset tailored for detecting manipulated images," in *2020 IEEE Winter Applications of Computer Vision Workshops (WACVW)*, pp. 71–80, 2020, https://doi.org/10.1109/WACVW50321.2020.9096940.

[34] G. Mahfoudi, B. Tajini, F. Retraint, F. Morain-nicolier, J. L. Dugelay *et al.,* "DEFACTO: Image and face manipulation dataset," in *2019 27th European Signal Processing Conf. (EUSIPCO)*, pp. 1–5, 2019, https://doi.org/10.23919/EUSIPCO.2019.8903181.

[35] V. Kniazv, Knyazv and F. Remondino, "The point where reality meets fantasy: Mixed adversarial generators," *Advances in Neural in Detection Formation Processing Systems. ALAA*, pp. 215–226, 2019.

[36] MFC2019 [EB/OL]. https://www.nist.gov/itl/iad/MigMediaForensicsChallenge20190.2019.

[37] G. Haiying, M. Kozak and E. Robertson, "MFC datasets: Large scale bench mark datasets for media forensic challenge evaluation," in *Proc. of the IEEE Winter Conf. on Applications of Computer Vision Workshops*, Waikoloa, HI, USA. IEEE, pp. 63–72, 2019.

[38] S. Heller, L. Rossetto and H. Schuldt, "The PS battles the dataset an image collection for image manipulation detection [EB/OL]," arxiv preprint arxiv: 1804.04866, 2018.

[39] W. Bihan, Z. Ye and Subramanianr, "COVERAGE–A novel data base for copy move for gery detection," in *Proc. of the IEEE Int. Confer Phoenix*, AZ, USA, IEEE, pp. 161–165, 2016.

[40] P. Korus and J. Huang, "Evaluation of random field models in multi-modal unsupervised tampering localization," in *2016 IEEE Int. Workshop on Information Forensics and Security (WIFS)*, pp. 1–6, 2016, https://doi.org/10.1109/WIFS.2016.7823898.

[41] M. Zampogloum, S. Papadopoulos and Y. Kompatsiaris, "Detecting image splicing in the wild (WEB)," in *Proc. of the IEEE Int. Conf. on Multimedia and Expo Workshops*, Turin, Italy. IEEE, pp. 1–6, 2015.

[42] J. Dong, W. Wang and T. Tan, "CASIA image tampering detection evaluation database," in *2013 IEEE China Summit and Int. Conf. on Signal and Information Processing*, pp. 422–426, 2013, https://doi.org/10.1109/ChinaSIP.2013.6625374.

[43] G. Cattaneo and G. Roscigno, "A possible pitfall waniex peri mental analysis of tampering detection algorithms," in *Proc. of the 17th Int. Conf. on Network Based Information Systems*, Salerno, Italy, IEEE, pp. 279–286, 2014.

[44] D. Tralic, I. Zupancic, S. Grgic and M. Grgic, "Comofod — New database for copy-move forgery detection," *Proceedings ELMAR-2013*, pp. 49–54, 2013.

[45] T. J. de Carvalho, C. Riess, E. Angelopoulou, H. Pedrini and A. de Rezende Rocha, "Exposing digital image forgeries by illumination color classification," *In IEEE Transactions on Information Forensics and Security*, vol. 8, no. 7, pp. 1182–1194, 2013, https://doi.org/10.1109/TIFS.2013.2265677.

[46] IEEEIFS TC Image Forensics Challenge Dataset [EB/OL]. http://ifc.recod.ic.unicamp.br/fc.website/inDex.py. 2014.

[47] D. Afchar, V. Nozick, J. Yamagishi and I. Echizen, "MesoNet: A compact facial video forgery detection network," in *2018 IEEE Int. Workshop on Information Forensics and Security (WIFS)*, pp. 1–7, 2018, https://doi.org/10.1109/WIFS.2018.8630761.

[48] P. Zhou, X. Han, V. I. Morariu and L. S. Davis, "Learning rich features for image manipulation detection," in *2018 IEEE/CVF Conf. on Computer Vision and Pattern Recognition*, pp. 1053–1061, 2018, https://doi.org/10.1109/CVPR.2018.00116.

[49] T. Y. Lin, Mairem and Belongies, "Microsoft," in *Computer Vision ECCV 2014*, Cham: Springer International Publishing, pp. 740–755, 2014.

[50] T. Gloe and R. Böhme, "The 'Dresden image database' for bench marking digital image forensics," in *Proc. of the ACM Symp. on Applied Computing. Si Erre*, Switzerland. New York: ACM Press, pp. 1584–1590, 2010.

[51] J. Deng, W. Dong, R. Socher, L. -J. Li, K. Li *et al.,* "ImageNet: A large-scale hierarchical image database," in *2009 IEEE Conf. on Computer Vision and Pattern Recognition*, pp. 248–255, 2009, https://doi.org/10.1109/CVPR.2009.5206848.

[52] Z. Bolei, Lapedrizaa and X. Jianxiong "Learning deep features for scene recognition using places the database," *Advances in Neural Information Process Ing Systems*, vol. 27, pp. 487–495, 2014.

[53] Ehingerka "The database: Large scale scene recognition from abbey to zoo," in *Proc. of the IEEE Conf. on Computer Vision and Pattern Recognition*, San Francisco, CA, USA. IEEE, pp. 3485–3492, 2010.

[54] Y. Zhang, J. Goh and L. Win "Image region forgery detection: A deep learning approach," *Proceedings of the SG-CRC, F*, 2016.

[55] J. Long, E. Shelhamer and T. Darrell, "Fully convolutional networks for semantic segmentation," in *2015 IEEE Conf. on Computer Vision and Pattern Recognition (CVPR)*, pp. 3431–3440, 2015, https://doi.org/10.1109/CVPR.2015.7298965.

[56] R. Salloum, Y. Ren, C. J. Kuo, "Image splicing localization using a multi-task fully convolutional network (MFCN) ⋆," *Journal of Visual Communication & Image Representation*, vol. 51, pp. 201–9, 2017.

[57] Y. Niu, B. Tondi, Y. Zhao, R. Ni and M. Barni, "Image, splicing detection, localization and attribution via JPEG primary quantization matrix estimation and clustering," *IEEE Trans. Inf. Forensics Secur*, vol. 16, pp. 5397–5412, 2021.

[58] S. Agrawal, P. Kumar and S. Seth, "SISL: Self-supervised image signature learning for splicing detection and localization," arXiv preprint arXiv:2203.07824, 2022.

[59] Y. wu, W. Abd-almageed and P. Natarajan, “Deep matching and validation network: An end-to-end solution to constrained image splicing localization and detection,” in *Proc. of the 25th ACM International Conference on Multimedia*, F, 2017. ACM.

[60] X. Bi, Y. Wei, B. Xiao and W. Li, “RRU-Net: The ringed residual U-net for image splicing forgery detection,” in *2019 IEEE/CVF Conf. on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pp. 30–39, 2019, https;//doi.org/10.1109/CVPRW.2019.00010.

[61] O. Ronneberger, P. Fischer and T. Brox. “U-Net: Convo-lutional networks for biomedical image segmentation,”. in *Int. Conf. on Medical Image Computing and Computer-Assisted Intervention*, Springer, pp. 234–241, 2015.

[62] Y. -F. Hsu and S. -F. Chang, “Detecting image splicing using geometry invariants and camera characteristics consistency,” in *Multimedia and Expo, 2006 IEEE Int. Conf.*, IEEE, pp. 549–552.

[63] Y. Liu, X. Zhu, X. Zhao and Y. Cao, “Adversarial learning for constrained image splicing detection and localization based on atrous convolution,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 10, pp. 2551–2566, 2019, https://doi.org/10.1109/TIFS.2019.2902826.

[64] I. Goodfellow, J. P. Abadie and M. Mirza, “Generative adversarial nets,” in *Proc. of the Advances in Neural Information Processing Systems*, F, 2014.

[65] J. Ouyang, Y. Liu and M. Liao, “Copy-move forgery detection based on deep learning,” in *2017 10th Int. Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, pp. 1–5, 2017, https://doi.org/10.1109/CISP-BMEI.2017.8301940.

[66] A. Kumar, A. Bhavsar and R. Verma, “Syn2real: Forgery classification via unsupervised domain adaptation,” in *2020 IEEE Winter Applications of Computer Vision Workshops (WACVW)*, pp. 63–70, 2020, https://doi.org/10.1109/WACVW50321.2020.9096921.

[67] Y. Wu, W. Abd-Almageed and P. Natarajan, “Image copy-move forgery detection via an end-to-end deep neural network,” in *2018 IEEE Winter Conf. on Applications of Computer Vision (WACV)*, pp. 1907–1915, 2018, https://doi.org/10.1109/WACV.2018.00211.

[68] Y. Wu, W. Abd-almageed, P. natarajan, “Buster Net: Detecting copy-move image forgery with source/target localization,” in *Proc. of the European Conf. on Computer Vision (ECCV)*, F, 2018.

[69] B. Chen, W. Tan, G. Coatrieux, Y. Zheng and Y. -Q. Shi, “A serial image copy-move forgery localization scheme with source/Target distinguishment,” *IEEE Transactions on Multimedia*, vol. 23, pp. 3506–3517, 2021, https://doi.org/10.1109/TMM.2020.3026868.