2020 6th International Conference on Advanced Computing & Communication Systems (ICACCS)

Image Forgery Detection using Deep Learning: A Survey

Zankhana J. Barad
Department of Information Technology
Dharmsinh Desai University
Nadiad, INDIA
zank.barad@gmail.com

Mukesh M. Goswami
Department of Information Technology
Dharmsinh Desai University
Nadiad, INDIA
mukesh.goswami@gmail.com

***Abstract*— The information is shared in form of images through newspapers, magazines, internet, or scientific journals. Due to software like Photoshop, GIMP, and Coral Draw, it becomes very hard to differentiate between original image and tampered image. Traditional methods for image forgery detection mostly use handcrafted features. The problem with the traditional approaches of detection of image tampering is that most of the methods can identify a specific type of tampering by identifying a certain features in image. Nowadays, deep learning methods are used for image tampering detection. These methods reported better accuracy than traditional methods because of their capability of extracting complex features from image. In this paper, we present a detailed survey of deep learning based techniques for image forgery detection, outcomes of survey in form of analysis and findings, and details of publically available image forgery datasets.**

Keywords*— *Image Tampering, Block-based approaches, Key points based approaches, Deep Learning

I. INTRODUCTION

Nowadays, images play a vital role in several fields like medical, education, digital forensics, sports, scientific research, news media, etc. and they are used as one of the main sources of information. Due to software like Photoshop, GIMP, Coral Draw and android applications like photo hacker, it is very easy to create a forged image. The genuineness of image becomes very crucial in the cases where the image is used as a proof in court of law.

Image manipulation is any type of operation that is performed on digital images by using any software, it is also referred as image editing. Image forgery is the technique to modify the content of an image which contradicts with some fact happened in past. Image tampering is a type of image forgery which replaces some content of an image with new content. If the new content is copied from the same image itself then it is called copy-move tampering and if the new content is copied from different image then it is called image splicing.

The image manipulation detection approaches can be classified into two: (i) Active and (ii) Passive. In active approach, additional information (such as digital watermark) is embedded in the image during the image acquisition stage or at some later stage by authorized person. The active approach uses this embedded information for manipulation detection. The passive approaches do not depend on the additional information for forgery detection. These approaches are also referred as "blind approaches" as the approaches do not use additional information for forgery detection. The passive approaches extract the features from the image and use these features for forgery detection. The passive approaches can be classified the forgery type independent approaches aim to detect other forgeries such as compression and re-sampling.

Passive forgery type dependent approaches for forgery detection can be categorized into: (i) copy-move and (ii) splicing. The images which are manipulated by these two approaches are very hard to identify by human. Therefore, it becomes very essential to detect these two kinds of forgeries and also it will be useful for digital image forensics. Unlike active image forgery approaches, e.g., watermarking, passive techniques are more useful, but they are more challenging. Wang et al. [1] used the tampering clues for classification of passive approaches for tampering detection. Generally digital forgery doesn't leave any visual clues of what is tampered with but it may change some statistics of an image and based on this belief these techniques work on an image. Some copy-move detection approaches are evaluated by Christlein et al. [2] and some cut-paste detection techniques are evaluated by Zambpglou et al. [3]. In context of this fact, different image tampering detection approaches have been suggested by researchers. The approaches are given in Figure 1.

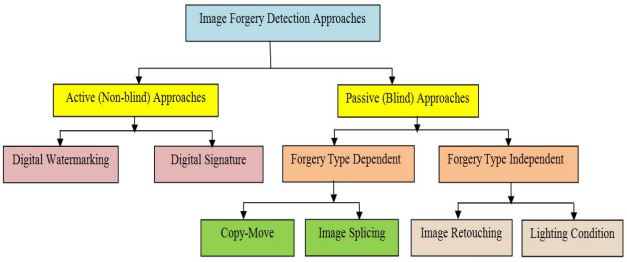

Fig. 1. Classification of Image Forgery Detection Approaches

The structure of this paper is as follows. Section II discusses about the traditional techniques for copy-move and splicing detection. Section III discusses about the deep

learning based approaches for image forgery detection. Section IV presents analysis and findings. Section V discusses about available image forgery datasets. Finally Section VI presents conclusion.

II. Traditional Techniques

A. Copy-Move Tampering Detection

In copy-move tampering, a region (of any size) from the image is selected to perform copy-move operation and it is pasted to some other part of the same image. So there will be very high correlation between these two regions. The objective of the copy-move tampering detection method is to detect duplicated regions in the given image. The similarities (correlation) or distance between features extracted from two different regions of the image indicate the duplication.

Researchers have applied two approaches to extract region-wise features from the image: (i) the image is divided into small regions, referred as blocks, and features for each block are extracted which is first proposed in [4] (ii) the keypoints from the entire image is identified and features for each keypoint are extracted. The extracted features are compared block-wise or keypoint-wise for generating matched blocks pairs or matched keypoints pairs. If matched pairs found among two regions then it conforms the duplication and the image can be classified as tampered image. These techniques presume that the tampered region is big enough to accommodate multiple blocks or keypoints. The general steps for detection of copy-move forgery are presented in Figure 2.

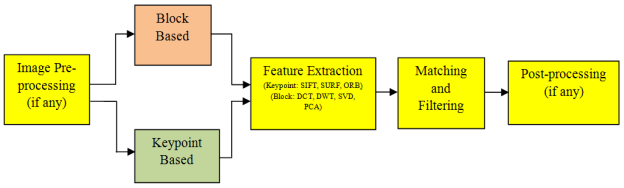

Fig. 2. General Steps for Detection of Copy-Move Tampering in Image

B. Image Splicing Detection

Image splicing is composite of two or more images. Copy-move tampering involves region duplication which is absent in case of image splicing. This makes localization of image splicing a difficult task as compared to detection of copy-move. The image splicing detection methods are based on the clues that are left after tampering process. The examples of common tampering clues are discontinuity in edge, inconsistency arise due to lighting condition, geometric situation and camera. The region which is copied in image leaves an abnormal artifacts on the edges of tampered region, referred as edge discontinuity [5]. Different cameras have different characteristics, so that images taken from different cameras have different properties and based on this clue tampering can be confirmed. Generally, the lighting effect of two images is not always same, there may be little difference between them. So the tampered region may have inconsistent lighting with other regions of the image that is lighting inconsistency. Johnson and Farid [6], [7] suggested to calculate the lighting path of various objects in an image. The conflict among the calculated paths decides the presence of tampering. When an forger chooses a JPEG image for tampering and saves the tampered image, then due to two compression operations, the tampered image will have double quantization (DQ) effect. Popescu and Farid [8] developed tools for the identification of double compressed JPEG images. All these clues indicate tampering in the image.

III. Deep Learning Based Techniques

Both block based and keypoints based methods use hand-crafted features (DCT [4], DWT [9], [10], PCA [11], SIFT [12], [13], SURF [14], [15] etc.) for forgery detection. Development of the GPU technologies and the success of Deep Learning (DL) [16] techniques in the domain of computer vision motivated the researchers to apply DL models for image forgery detection. DL combines features (low/mid/high level) extraction and classification phases. The technique is data-driven and capable of automatically learning abstract and complex features, necessary to identify tampered regions. Moreover, it also saves time and energy required to find hand-crafted features from tampered images. However, training of deep learning models is hard and requires high computational power and very large amount of data. There are many models of DL such as Convolutional Neural Networks (CNN), Deep Neural Network (DNN) and Recurrent Neural Network (RNN). Convolutional Neural Networks (CNN) is popular amongst these DL models. CNN has the convolution layer which acts as a discriminator and feature extractor.

Generally, CNNs extract features based on image content rather than extracting image manipulation features. Bayar et al. [17] proposed new convolutional layer that learns image manipulation features by suppressing image content. This layer considers the local structural relationship between pixels instead of considering the content of an image, because manipulation alters some local relationships. This can detect multiple tampering in an image. One problem with any detection method is that it cannot give satisfactory results for multiple tampering attacks. In addition, to locate the tampered region, most of the work is done targeting only JPEG images where the tampered region is detected using clue left by number of JPEG compression operations. Zhang et al. [16] suggested two step mechanism for detection of forged images. In the first step, they divided the image into patches and then Stacked Auto encoder model is used to learn the features for each patch. In the second step, the contextual information is added to each patch to get accurate results.

Salloum et al. [18] proposed the solution to localize image splicing using Multi-task Fully Convolutional Network (MFCN). They used FCN VGG-16 with skip connection as the base network. It is proved that Multi-task FCN (MFCN) achieves better performance than single-task FCN (SFCN) because SFCN provides coarse localization output in few cases. Reference [18] proposed the MFCN with two output branches. From these two branches, one is used for learning the surface label information and other branch is used for learning the tampered region boundary. Although this method has shown some performance degradation on post-processing operations but still it performed better than some existing

techniques. One approach to localize double JPEG compression using multi-domain convolutional neural network is proposed by Amerini et al. [19]. Multi-domain CNN consists of one CNN based on spatial domain, one CNN based on frequency domain and fully connected layers. Spatial domain-based CNN takes an input of n*n sized patches of RGB color channels. It is composed of two convolutional blocks and two fully connected layers.

TABLE I. COMPARATIVE STUDY OF DEEP LEARNING BASED METHODS FOR IMAGE TAMPERING DETECTION

Paper	Type of Tampering Targeted	Features	# Layers	Model	Dataset	Performance Metric
Bayar et al. [17]	Gaussian blurring, Median filtering, Resampling AWGN,	Prediction error filters	8 (proposed new convolution layer, 2 convolutional layers, 2 max-pooling layers and 3 fully connected layers)	CNN	Collected from 12 different camera models	Accuracy 99.10%
Zhang et al. [16]	Cut-paste, Copy-move	3-level 2D Daubechies wavelet decomposition	---	Stacked-Auto-encoders (SAE)	CASIA v1.0, CASIA v2.0, Columbia	Accuracy 91.09%
Salloum et al. [18]	Image Splicing	Surface probability map and edge probability map	---	Multi-task fully convolution network (MFCN)	Columbia, CASIA v1.0, CASIA v2.0, Carvalho	F1-Score 0.54(CASIA v1.0) 0.61(Columbia) MCC Score 0.52(CASIA v1.0) 0.47(Columbia)
Amerini et al. [19]	Double JPEG compression, Cut-paste	R,G,B Features and histogram of DCT	---	Multi-domain CNN	UCID (1338 Images)	Accuracy 95%
Chen et al. [20]	Median filtering, Cut-paste	Median filter residuals	9 (1 filter layer, 5 convolutional layers, 3 fully connected layers)	CNN	15352 images (NRCS Photo Gallery, BOSSbase 1.01, UCID, Dresden, BOSS RAW)	Accuracy 85.14%
Bondi et al. [21]	Cut-paste	Camera model features	11 (4 convolutional layers, 3 max-pooling layers, 2 fully connected layers, 1 ReLU layer, 1 Softmax layer)	CNN	Dresden Image Database (16k images from 26 different cameras)	Detection Accuracy 81% Localization Accuracy 82%
Cozzolino and Verdoliva [22]	Cut-paste	Noise residual features	---	Autoencoder	Images from 7 devices, 6 smartphones and a camera	F-Measure 0.41(basic) 0.37(with post-processing)
Rao and Ni [23]	Copy-move, Cut-paste	Hierarchical representation from color Images	10 (8 convolutional layers, 2 pooling layers, 1 fully connected layer)	CNN	CASIA v1.0, CASIA v2.0, Columbia gray DVMM	Accuracy 98.04%(CASIA v1.0) 97.83%(CASIA v2.0) 96.38%(DVMM)
Wu et al. [24]	Copy-move	Features from VGG16	---	BusterNet (Deep Neural Network)	CASIA v2.0, CoMoFoD dataset	
Bi et al. [25]	Cut-paste	Image residuals	---	Ringed Residual U-Net (RRU-Net)	CASIA, COLUMB	Accuracy (Image) 76% F-measure (pixel) 0.84: CASIA 0.91: COLUMB
Wang et al. [26]	Copy-move, Cut-paste	Residual Convolution Network ResNet-101	---	Mask Regional Convolution Neural Network (Mask R-CNN)	Cover, Columbia	Average Precision 93% (for Cover) 97% (for Columbia)

Frequency domain-based CNN takes DCT coefficients for each patch as input. Frequency domain-based CNN comprises two convolutional layers followed by two pooling layers and three full connections. Multi-domain CNN joins the outputs coming from fully connected layers of these two networks and it classifies the patch into one of three classes: uncompressed, single or double compressed.

Detecting median filtering from image is very challenging task when size of the image is small and when the image is compressed. To deal with this challenge, Chen et al. [20] proposed a CNN based approach which extracts median filtering residuals from image. The first layer of CNN is a filter layer which reduces the interference arise due to presence of the edges and textures. The removal of interference helps model to investigate the traces left by median filtering. The approach was tested on a dataset of 15352 images, obtained by composition of five image datasets.

A spliced image may consists of traces of multiple devices. To detect tampering based on the traces left by different camera models, Bondi et al. [21] presented a CNN based approach which extracts the features relating to camera model from image patches. Clustering technique is used to analyze the extracted features and based on that it classifies the image as either forged or authentic. The approach was tested on a dataset of 2000 images obtained from different camera models.

The use of noise residual features for image forgery detection and localization is proposed in [22]. The CNN is used for extracting noise residual based features from the image and SVM is used for classification. Rao et al. [23] proposed CNN for image copy-move and splicing detection. The first convolution layer of the CNN is used for pre-processing operation to find out the effects produced by tampering operations. The CNN was trained on labelled path samples from the training images. Then this pre-trained CNN was applied on test images and SVM classifier was used for the detection of tampering. To detect copy-move forgery, Wu et al. [24] proposed two branch DNN architecture called BusterNet which is capable of generating manipulation mask. In this architecture, one branch is used for detection of tampered regions which takes input image, extracts features using CNN, upsamples feature map using Mask Decoder and generates mask using binary classifier. And the other branch is used for the detection of cloned regions which takes input image, uses CNN to extract features, Self-Correlation module to compute feature similarity, Percentile Pooling to collect useful statistics, Mask Decoder for up sampling of feature map, and Binary Classifier to generate binary copy-move mask. Then this fusion module takes inputs from both branches and makes the final copy-move forgery prediction. The proposed approach was evaluated on two datasets: CASIA v2.0 and CoMoFoD.

One CNN-based method called Ringed Residual U-Net (RRU-Net), which is end-to-end image segmentation network, is proposed by Bi et al. [25] for image splicing detection. RRU-Net aims to improve learning way of CNN through recall and consolidation mechanism of human brain. The residual propagation is used to recall the input feature information to solve the degradation problem in the deeper network; the residual feedback consolidates the input feature information to differentiate between the authenticate and forged regions. The RRU-Net was tested on CASIA and COLUMBIA datasets. The model is used by Wang et al.

[26] to detect and locate image forgeries. The model was tested on Cover and Columbia datasets. The model was capable to detect both copy-move and splicing forgeries. The survey of DL based forgery detection methods are presented in Table 1.

IV. Analysis and Findings

The following are important points found after detail analysis of different research papers.

(1) The tampering detection task focuses on the coarse grained analysis whereas localization task focuses on fine grained analysis of the image. Localization of the tampered region in an image is more challenging than tampering detection. There are many techniques proposed by researchers for detection of tampering and only few of these can localize the tampered area.

(2) The traditional methods (both block based and keypoints based methods) use hand-crafted features for tampering detection. The DL technique is capable to learn abstract and complex features, required for identification of tampered regions, automatically. The DL models can be used for (i) binary classification of the input image in to authentic (original) or tampered classes and (ii) localization of tampered regions. Researchers found that CNN models obtained high accuracy in both classification of tampered images and generating fine grained mask for localization of tampered regions. However, training deep networks is hard and requires high computational power and a large size dataset.

(3) Since the person performing the analysis of the tampered image is not aware of the forgery type performed on the original image, the use of a specific detection technique may not work. There is a requirement of a forgery detection technique which would detect the forgery of any type.

(4) Different criteria (accuracy, precision, recall, F-measure, Receiver Operator Characteristics - ROC Curve, MCC, IoU etc.) are used by researchers for measuring the performance of the tampering detection algorithms. The common criteria (measures) should be used for comparing the performance of different tampering detection algorithms.

(5) The performance of the tampering detection algorithms is evaluated on the database consisting of original (authentic) and tampered images. For proper evaluation of the algorithms, the database should contain as many kinds of original images and variety of different tampering attacks as possible. Many image tampering datasets are available publically. However, the size of these datasets is not adequate and puts limitation for DL based tampering detection approaches.

V. Analysis of Image Forgery Datasets

The dataset, composing of authenticate and forged images, is required to evaluate the performance of the image tampering algorithm. There are two types of image tampering algorithms: (i) algorithms generate binary output (as original/tampered at image level), without localization of tampered region and (ii) algorithms generate localization of tampered region (at pixel level).

For algorithms generating binary output, to differentiate between original and tampered images in the dataset, generally, the original images are marked with label "0" and tampered image with label "1". This type of algorithm works at coarse-grain (image) level. For algorithms to locate the forged region, images need to be labeled with groundtruth mask, indicating the position of changed pixels. This type of algorithm works at fine-grain (pixel) level and outputs predicted mask. To measure the performance of the algorithm (localization of tampered region), the predicted mask of a test image is compared with ground truth mask.

TABLE II. PUBLICALLY AVAILABLE IMAGE FORGERY DATASETS

Dataset	Release Year	#Authentic /Tampered Images	Image Size	Format	Mask	Post Process
Columbia Gray	2004	933/ 912	128 * 128	BMP	No	No
Columbia Color	2006	183/ 180	757*568/ 1152* 768	TIFF	Yes	No
CAS1A v1.0	2009	800/ 921	384*256	JPEG	No	No
CASIA v2.0	2009	7491/ 5123	240*160/ 900*600	TIFF/ JPEG	No	Yes
MICC-F220	2011	110/ 110	722*480/ 800*600	JPEG	No	No
MICC-F2000	2011	1300/ 700	2048*1536	JPEG	No	No
IMD	2012	48/48	3000*2300	JPEG/ PNG	Yes	Optional
MICC-F600	2013	440/ 160	800*533/ 3888*2592	JPEG/ PNG	Yes	Yes
CoMo-FoD	2013	5200/ 5200	512*512	JPEG/ PNG	Yes	Yes
Carvalho	2013	100/ 100	2048*1536	PNG	Yes	Yes

The first online available dataset is Columbia Gray which was published in 2004. The images in this dataset are grayscale blocks extracted from 322 photos. To overcome this limitation, Columbia team published a new dataset in 2006 having color images but it contains the images with unsatisfying tampering effect. By considering increasing demand of larger dataset, the CASIA team published two tampering datasets. The Columbia datasets contains spliced images only whereas the CASIA datasets contains copy-move and spliced images.

Like the Columbia datasets, the MICC datasets contain the images with visually perceptible tampering effect. Tampered region in the images are randomly selected regions from the same images. Instead of selecting any random rectangular region, meaningful regions called "snippets" are selected by human experts in IMD dataset. COVERAGE dataset is released recently, in which the images contain similar-but-genuine objects (SGO) [27].

VI. Conclusions

We presented a comparative analysis of different deep learning techniques used for tampering detection, available image forgery datasets, different issues requiring attention in detection of image tampering, and performance measures used for evaluating accuracy of tampering detection. Tampering detection task can be viewed as (i) Detection-only task or (ii) Localization task. In Detection-only task, the detection is performed at image level so the result will be either the image is tampered or authentic. In Localization task, the detection is performed at pixel level so it marks off the tampered area in the forged image.

From this survey, we found that there are two approaches for tampering detection: (i) Traditional and (ii) Deep Learning. The traditional methods use hand-crafted features for tampering detection. From the survey, we conclude that the traditional methods do not work reliably across various tampering methods. Instead, the Deep Learning based methods have shown to be able to learn abstract and complex features, required for identification of tampered regions, automatically.

References

[1] W. Wang, J. Dong, and T. Tan, "A survey of passive image tampering detection," in International Workshop on Digital Watermarking, pp. 308–322, Springer, 2009.

[2] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," *IEEE Transactions on information forensics and security*, vol. 7, no. 6, pp. 1841–1854, 2012.

[3] M. Zampoglou, S. Papadopoulos, and Y. Kompatsiaris, "Large-scale evaluation of splicing localization algorithms for web images," *Multimedia Tools and Applications*, vol. 76, no. 4, pp. 4801–4834, 2017.

[4] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in *in Proceedings of Digital Forensic Research Workshop*, Citeseer, 2003.

[5] W. Chen, Y. Q. Shi, and W. Su, "Image splicing detection using 2d phase congruency and statistical moments of characteristic function," in *Security, Steganography, and Watermarking of Multimedia Contents IX*, vol. 6505, p. 65050R, International Society for Optics and Photonics, 2007.

[6] M. K. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," in *Proceedings of the 7th workshop on Multimedia and security*, pp. 1–10, ACM, 2005.

[7] M. K. Johnson and H. Farid, "Exposing digital forgeries in complex lighting environments," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 450–461, 2007.

[8] A. C. Popescu and H. Farid, "Statistical tools for digital forensics," in *international workshop on information hiding*, pp. 128–147, Springer, 2004.

[9] A. Myna, M. Venkateshmurthy, and C. Patil, "Detection of region duplication forgery in digital images using wavelets and log-polar mapping," in *International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007)*, vol. 3, pp. 371–377, IEEE, 2007.

[10] M. Bashar, K. Noda, N. Ohnishi, and K. Mori, "Exploring duplicated regions in natural images," *IEEE Transactions on Image Processing*, 2010.

[11] M. E. Wall, A. Rechtsteiner, and L. M. Rocha, "Singular value decomposition and principal component analysis," in *A practical approach to microarray data analysis*, pp. 91–109, Springer, 2003.

[12] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using sift algorithm," in *2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, vol. 2, pp. 272–276, IEEE, 2008.

[13] X. Pan and S. Lyu, "Detecting image region duplication using sift features," in *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 1706–1709, IEEE, 2010.

[14] L. Juan and L. Gwon, "A comparison of sift, pca-sift and surf," *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 8, no. 3, pp. 169–176, 2007.

[15] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy-move forgery detection based on surf," in *2010 International Conference on Multimedia Information Networking and Security*, pp. 889–892, IEEE, 2010.

[16] Y. Zhang, J. Goh, L. L. Win, and V. L. Thing, "Image region forgery detection: A deep learning approach.," in *SG-CRC*, pp. 1–11, 2016.

[17] B. Bayar and M. C. Stamm, "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*, pp. 5–10, ACM, 2016.

[18] R. Salloum, Y. Ren, and C.-C. J. Kuo, "Image splicing localization using a multi-task fully convolutional network (mfcn)," *Journal of Visual Communication and Image Representation*, vol. 51, pp. 201–209, 2018.

[19] I. Amerini, T. Uricchio, L. Ballan, and R. Caldelli, "Localization of jpeg double compression through multi-domain convolutional neural networks," in *2017 IEEE Conference on computer vision and pattern recognition workshops (CVPRW)*, pp. 1865–1871, IEEE, 2017.

[20] J. Chen, X. Kang, Y. Liu, and Z. J. Wang, "Median filtering forensics based on convolutional neural networks," *IEEE Signal Processing Letters*, vol. 22, no. 11, pp. 1849–1853, 2015.

[21] L. Bondi, S. Lameri, D. Güera, P. Bestagini, E. J. Delp, and S. Tubaro, "Tampering detection and localization through clustering of camera-based cnn features," in *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pp. 1855–1864, IEEE, 2017.

[22] D. Cozzolino and L. Verdoliva, "Single-image splicing localization through autoencoder-based anomaly detection," in *2016 IEEE International Workshop on Information Forensics and Security (WIFS)*, pp. 1–6, IEEE, 2016.

[23] Y. Rao and J. Ni, "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)*, pp. 1–6, IEEE, 2016.

[24] Y. Wu, W. Abd-Almageed, and P. Natarajan, "Busternet: Detecting copy-move image forgery with source/target localization," in *Proceedings of the European Conference on Computer Vision (ECCV)*, pp. 168–184, 2018.

[25] X. Bi, Y. Wei, B. Xiao, and W. Li, "Rru-net: The ringed residual u-net for image splicing forgery detection," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pp. 0–0, 2019.

[26] X. Wang, H. Wang, S. Niu, and J. Zhang, "Detection and localization of image forgeries using improved mask regional convolutional neural network," 2019.

[27] B. Wen, Y. Zhu, R. Subramanian, T.-T. Ng, X. Shen, and S. Winkler, "Coverageâ€"a novel database for copy-move forgery detection," in *2016 IEEE International Conference on Image Processing (ICIP)*, pp. 161–165, IEEE, 2016.