PAPER • OPEN ACCESS

A Deep Learning based Method for Image Splicing Detection

To cite this article: Kunj Bihari Meena and Vipin Tyagi 2021 J. Phys.: Conf. Ser. 1714 012038

View the <u>article online</u> for updates and enhancements.

You may also like

 The influence of axial offset of fusion splicing on a large mode area fiber based oscillator

Hanwei Zhang, Baolai Yang, Peng Wang et al.

- 2-cut splicing and 4-cut splicing on DNA molecule

molecule I Aisah, P R E Jayanti and A K Supriatna

 Photo splicing detection using error level analysis and laplacian-edge detection plugin on GIMP

E Ramadhani



1714 (2021) 012038 doi:10.1088/1742-6596/1714/1/012038

A Deep Learning based Method for Image Splicing Detection

Kunj Bihari Meena and Vipin Tyagi Jaypee University of Engineering and Technology Raghogarh, Guna – MP, INDIA

corr. author : dr.vipin.tyagi@gmail.com

Abstract. Image manipulation has become an easy task due to the availability of user-friendly multimedia tools. The images can be manipulated in several ways. Image splicing is one of such image manipulation methods in which two or more images are merged to obtain a single composite image. These manipulated images can be misused to cheat others. This paper proposes a deep learning-based method to detect image splicing in the images. First, the input image is preprocessed using a technique called 'Noiseprint' to get the noise residual by suppressing the image content. Second, the popular ResNet-50 network is used as a feature extractor. Finally, the obtained features are classified as spliced or authentic using the SVM classifier. The experiments performed on the CUISDE dataset show that the proposed method outperforms other existing methods. The proposed method achieves an average classification accuracy of 97.24%.

1. Introduction

The digital images are ubiquitously available around us at every moment. Digital images play a vital role in various important fields such as magazines, newspapers, education, insurance, medical, entertainment industry, matrimonial websites, etc. The image editing tools have become so advanced and user friendly that anyone can manipulate the images. There are various ways to manipulate or forge digital images. Image splicing and copy-move forgery are the two most common ways to tamper with the images. In image splicing forgery, two or more images (or part of the images) are combined to get a single spliced or composite image. An example of image splicing is shown in figure 1. However, in the copy-move forgery, the part of the image is replicated within the same image at different locations. In the past few years, the number of image forgery cases has increased by leaps and bound. Now-a-days, social media campaigning has also become a new trend in elections around the globe. On a positive note, digital images are widely used to create awareness about the election. At the same time, it has been also observed that the forged images or images with false information are also being circulated on social media to influence the public. In a study [1], it was concluded that during the recent Brazilian presidential elections around 13.1% of Whatsapp posts were fake. Most recently, various fake images went viral on social media platforms comprising false information about the COVID-19 pandemic [2]. Therefore, in order to revive the trustworthiness of the digital images, it becomes important to devise some methods that can authenticate the images.

In the last few years, many authors have suggested various methods to authenticate the images. These methods can be grouped as active forgery detection and passive forgery detection [3–7]. The active forgery detection methods rely on some prior information about the input images. Whereas the passive forgery detection methods do not need any prior information about the input image, rather these methods reveal the forgery by extracting some clues based on the change in the intrinsic properties of the image. Unfortunately, in most situations, the forged images are obtained from different social media platforms. For such forged images, it becomes almost impossible to find their

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.

1714 (2021) 012038 doi:10.1088/1742-6596/1714/1/012038

origin. Hence, active forgery detection methods are less useful in the current time. In other words, passive forgery detection methods are more relevant to detect a forgery in digital images.



Figure 1. Example of the image splicing forgery [4].

The common workflow of image splicing detection is shown in figure 2. The first step in this workflow is preprocessing, which is an optional step. Various image preprocessing operations used in past include RGB to YCbCr conversion [8], [9], RGB to HSV conversion [10], and RGB to Grayscale conversion [11]. The main purpose of the preprocessing step is to focus on the features related to a specific channel. The feature extraction step in figure 2 is the most important step where useful features are extracted from the input image. In the early days of image forgery detection, the methods mainly relied on the traditional feature extraction techniques used in computer vision. Sometimes these feature extractors are known as hand-crafted feature extraction techniques as these features are primarily designed to focus on some specific characteristics of the image and created manually by some experts. Some of the popular hand-crafted feature extractors that were used in image splicing detection are, discrete wavelet transform (DWT) [12], contourlet transform [14], Hilbert-Huang transform [15], local binary pattern (LBP) [13], discrete cosine transform (DCT) [13]. Mostly handcrafted feature-based image splicing detectors use a support vector machine (SVM) as a classifier [12], [13]. As opposed to hand-crafted feature-based image splicing detection methods the recent developments ([16], [17], [18], [19], [20]) have focused on deep learning-based image splicing detection. In general, the deep learning-based methods can learn more generalized features from the input images. Hence, deep learning-based image splicing detection methods have become much popular in the last few years. In this way, all the existing image splicing detection methods can be classified as hand-crafted feature-based and deep learning-based methods.

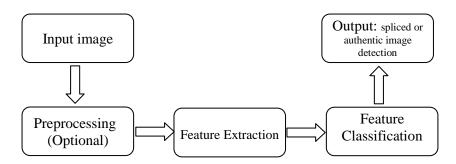


Figure 2. The common workflow of image splicing detection.

The deep learning-based methods have observed unprecedented success in various fields like image processing, digital image forensics [21,22], fraud detection, self-driving cars, virtual assistance and face recognition systems, etc. Various convolutional neural networks were proposed to detect the

CONSILIO 2020 IOP Publishing

Journal of Physics: Conference Series

1714 (2021) 012038 doi:10.1088/1742-6596/1714/1/012038

objects in digital images in the last decade. Motivated by the success of deep learning, this paper proposes a new image splicing detection method based on deep learning.

The main contributions of this paper are, firstly, the input image is preprocessed using the newly developed deep learning-based technique called Noiseprint to obtain the noise residual map. Generally, different camera images are considered for the splicing process. Hence the noise properties of the source images remain different and can be easily identified from the noise residual map. Secondly, the features from noise residual maps are extracted using the pre-trained ResNet-50 network. In this way, the weights of the ResNet-50 network are transferred to learn the important distinguishing features of spliced and authentic images. Extensive experiments were performed on the CUISDE dataset to evaluate the performance of the proposed method.

The rest of the paper is arranged as follows: Section 2 presents a detailed survey of the existing image splicing detection methods. Introduction to the Noiseprint model is provided in section 3. Section 4 discusses the proposed deep learning-based method. Section 5 demonstrates the experimental results and also provides details about evaluation parameters and image datasets. Section 5 also presents result comparisons with the existing image splicing detection methods. Finally, section 6 provides the conclusion of the work.

2. Related works

This section presents the related research work in this area. Many researchers have proposed methods to detect image splicing forgery. As mentioned earlier the existing image splicing detection methods can be classified into two broad categories namely hand-crafted features-based and deep learning-based methods. Some of the popular methods in each of the categories are reviewed in the subsequent sections.

2.1 Hand-crafted feature-based image splicing detection methods

Ng. and Chang [23] investigated a method to detect image splicing based on the bicoherence magnitude of the 2D signal in the digital image. In this study, the authors have suggested that the values of bicoherence magnitude and phase features are generally increased due to the image splicing operation. After that, an SVM classifier was employed to classify the images as authentic or spliced. Zhang et al. [24] introduced a method based on homography constraint and graph cut. The authors have also proposed an online feature selection framework to further boost the detection accuracy. Li et al. [15], have proposed a method to detect image splicing in digital images by extracting the features from the image using the Hilbert-Huang transform. The local binary pattern (LBP) was used as a feature extractor in the two different image splicing detection methods proposed in [25], [26]. Zhao et al [27] developed an approach to detect the image splicing based on 2-D Noncausal Markov Model. This method also uses an SVM classifier for classifying the images as authentic or spliced. Wang et al. [28] put forward a method using Markov of quaternion component separation in the quaternion discrete cosine transform domain and QWT domain. In this method, the authors have calculated intrablock and inter-block Markov features in the luminance (Y) channel of the YCbCr color model.

Recently, Kanwal et al. [9] designed a method to reveal the image splicing in the digital images based on the local ternary count. In this method, RGB to YCbCr conversion is used as a preprocessing step. Jaiswal et al. [11] have demonstrated a hybrid method by combining four features HoG, LTE, DWT, and LBP. In this method, first, the RGB image is converted into a greyscale image. After that logistic regression classifier was used to predict the decision about the authenticity of the image. Meanwhile, Wang et al. [29] proposed a method based on the quaternion discrete cosine transform (QDCT) and Markov features. In this method, the feature dimension per image was 2916. The method uses an SVM as a classifier. Most recently, Wang et al. [30] introduced a method to detect and locate the image splicing based on a coarse-to-fine grained technique. The local noise is extracted using the Laplace operator and then the regions are clustered based on connected region expansion/corrosion.

CONSILIO 2020

IOP Publishing

Journal of Physics: Conference Series

1714 (2021) 012038

doi:10.1088/1742-6596/1714/1/012038

Rao et al. [16] proposed a method to detect image splicing based on deep learning. This method utilizes a convolutional neural network (CNN) to automatically learn hierarchical features from the input images. This method first applied the high-pass filters to get the noise residual. Moreover, the method uses an SVM classifier. Bunk et al. [31] developed a method based on Radon transform and deep learning. In this method, the input image is divided into small patches, and then from each patch, the Radon resampling features are calculated. To locate the forgery Random Walker segmentation approach was used. Liu et al. [32] designed a deep learning model to detect image splicing forgery. This method also uses a conditional random field to adaptively combine the results from the CNNs. The authors have concluded that their method outperformed the other existing methods. Meanwhile, Salloum et al. [33] proposed a method to detect image splicing using two fully convolutional networks (FCN). The first network is a single-task network that mainly learns the surface label features. Whereas the second network is a multi-task network which is a dual-path network. This dual-path network mainly learns the edge or boundary of the spliced region.

Pomari et al. [10] proposed a method based on illumination inconsistencies and deep learning to unveil the image splicing. Chen et al. [34] improved the performance of [32] and proposed a new method to detect the image splicing. In this method, instead of using a single fully convolutional network (FCN) the authors use three FCNs with different upsampling layers. Moreover, the pretrained weights of the VGG-16 network were used to initialize all three FCNs. Xiao et al. [35] investigated an approach to detect image splicing based on a coarse-to-refined convolutional neural network (C2RNet) and diluted adaptive clustering. In this approach, the features at different scales are calculated using course-CNN and refined-CNN, from the small patches of the input image. Rao et al. [36] put forward a technique to detect image splicing in images based on a two-branch CNN. In this method, high-pass filters are applied to suppress the effect of image content. And then CNN is used as a local descriptor. The features are classified as forged or authentic using an SVM.

Recently, Wang et al. [19] developed a deep learning-based image splicing method where the authors have used a convolutional neural network with a weight combination strategy. This method used three different features that include YCbCr features, edge features, and PRNU features. All the three features merged together using the combination strategy. Ahmed et al. [17] introduced a method based on deep neural network ResNet-Conv. In this method, two variants of ResNet CNN namely ResNet-50 and ResNet-101 were used to obtain an initial feature map from RGB images. The authors further proposed the Mask-RCNN to localize the forgery. Hussien et al. [18] designed a method in which the features are extracted using a color filter array (CFA) based analysis. Then the authors have employed the principal component analysis (PCA) technique to reduce the feature dimension from 6672 to 784. Finally, a deep belief network is used as a feature classifier. This method was evaluated on the Columbia grayscale dataset. Some of the good review papers related to image splicing detection methods are [37], [38].

Based on the above discussion it can be concluded the image splicing detection is an active area of research and many researchers are paying attention to this area. Though a good number of attempts were made in the past to address the problem of image splicing detection these methods still have the following main limitations, first, the hand-crafted feature-based methods are not robust to deal with the challenging situation especially when the forged images are post-processed. This is because the hand-crafted features only focus on certain properties of the image. Second, the existing methods show low classification accuracy, hence there is a scope to improve the classification accuracy. To overcome these limitations, this paper proposes a deep learning-based method to detect the image splicing in digital images.

1714 (2021) 012038 doi:10.1

doi:10.1088/1742-6596/1714/1/012038

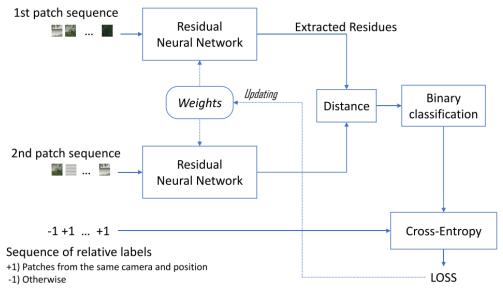


Figure 3. The architecture of the Noiseprint model [39].

3. Noiseprint model

One of the most successful methods to obtain noise residuals from the digital images is photo-response non-uniformity (PRNU). However this method has two main limitations [39], first, this method requires several images to evaluate the camera fingerprint, and second, its performance is mainly affected due to the low power of the signal of interest with respect to noise. To overcome these two limitations, Cozzolino et al. [39] have proposed a new method namely *Noiseprint* to obtain the noise residual from the images. This method aims to suppress the image content and to focus on camera specific noise-based fingerprints. To achieve this, the authors have proposed a siamese based model as shown in figure 3. This model has two identical convolutional neural networks namely residual neural network.

The Noiseprint model was trained by feeding the sequence of image patches in both the CNNs. The siamese network minimizes the error distance for positive samples (image patches from the same camera models) and maximizes the error distance for negative samples (image patches from the different camera models). The Noiseprint model was trained on a large number of image patches to demonstrate state-of-the-art performance. The authors have compared the Noiseprint model with exiting top-performing methods including PRNU based method and concluded that the performance of the Noiseprint model is superior to others. A sample spliced image with corresponding noise residual map obtained using the Noiseprint model is shown in figure 4. Note that the forged image mentioned in figure 4 was created by inserting the aircraft image (which is a part of the image that was taken using a different camera) in the original image. It is easy to see that the noise residual map highlights the spliced part (aircraft). Therefore, the residual map of a spliced image is likely to have some highlighted areas whereas no such artifacts are expected from the authentic image. These distinguishing features are learned in the proposed feature extraction scheme.

1714 (2021) 012038 doi:10.1088/1742-6596/1714/1/012038



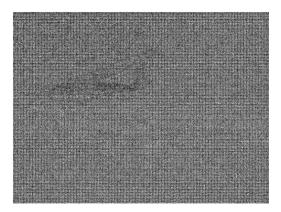


Figure 4. Spliced image (left) with the corresponding noise residual map (right) obtained using the Noiseprint model [39].

4. The proposed image splicing detection method

The complete architecture of the proposed method is shown in figure 5, which consists following three main steps:

4.1 Obtaining noise residual map using the Noiseprint

Generally, the spliced images are created from the images that are captured by different camera models. Each camera model introduces a unique fingerprint during the image acquisition process. Hence these camera-specific fingerprints can be extracted and used to reveal the image splicing forgery. There exist several methods that can be used to extract the camera-specific fingerprints. However the latest development is the Noiseprint model [39], the brief introduction about Noiseprint is provided in section 3. If the Noiseprint model is denoted by M, the noise residual map $\hat{I}(x,y)$ corresponding to the input image I(x,y) can be obtained using equation 1.

$$\hat{I}(x,y) = M(I(x,y)) \tag{1}$$

4.2 Extracting features using ResNet-50

Deep learning-based methods require large data to train the model. However, the image splicing datasets that are available in the public domain are not so large in terms of the number of images. Lack of availability of sufficient data to train a deep learning model has motivated the concept of transfer learning. Transfer learning allows us to solve a similar problem by transferring the knowledge of any existing well-trained deep learning model. In this way, instead of training the new deep learning model from the scratch, we can utilize the weights of pre-trained models. Therefore, to take the advantage of transfer learning and also avoid any overfitting problem, the weights of the pre-trained ResNet-50 network are used as a feature extractor. Note that the weights from the first 49 layers of ResNet-50 were used because the last layer is a simple softmax layer with 1000 neurons. Though any classic network such as InceptionNet, VGG-19, etc. can serve the purpose, we have selected ResNet-50 due to its simple and robust architecture. In this step, the features for all the training images that include authentic and spliced images are extracted and stored as feature vector V as follows (equation 2):

$$V = \begin{bmatrix} X_1, X_2, \dots, X_n spliced \\ X_1, X_2, \dots, X_n authentic \end{bmatrix}$$
 (2)

4.3 Feature classification using support vector machine

1714 (2021) 012038

doi:10.1088/1742-6596/1714/1/012038

Feature classification is also an important step in the image splicing detection process. There exist various feature classification techniques such as multilayer perceptron [22], linear discriminant analysis, support vector machine (SVM), etc. However, for image splicing detection an SVM classifier is mostly preferred over the other. Hence, the proposed method also utilized an SVM classifier with a radial basis function (RBF) kernel. The feature vector obtained in equation 2 along with the correct labels (1 for authentic and 0 for spliced image) is passed as the input to the SVM classifier and then the SVM determines the correct class of each image. It is worthy to note that the proposed method replaces the last softmax layer in the ResNet-50 network using the SVM classifier.

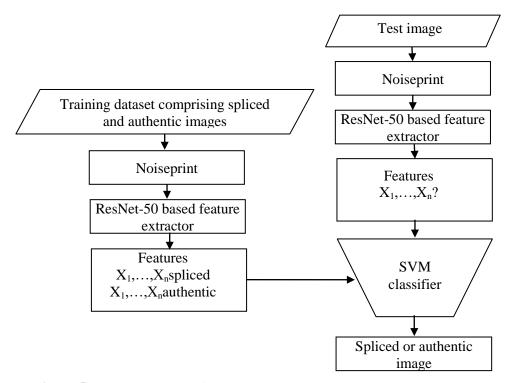


Figure 5. The architecture of the proposed image splicing detection method.

5. Implementation and performance evaluation

The proposed method is implemented in the python programming language. Some libraries such as Keras and Tensorflow were used to implement deep learning modules. The performance evaluation is done on a computer with Quadro RTX 4000 NVIDIA GPU with 16 GB RAM and Windows 10 operating system. The description of the image dataset used for experiments is given in the next section.

5.1 Dataset and evaluation parameters

The Columbia Uncompressed Image Splicing Detection Evaluation (CUISDE) dataset [40] was used to evaluate the performance of the proposed method. The dataset includes a total of 363 uncompressed images. There are a total of 180 spliced and 183 authentic images in the dataset stored in TIFF formats. The pixel resolution of the images is in the range from 757×568 to 1152×768. The images are captured using four different camera models namely 'canong3', 'nikond70', 'canonxt', and 'kodakdcs330'. The images include various objects and scenes such as the keyboard, books, tables, etc. Around 15% of images are captured in outdoor cloudy weather which makes outdoor illumination similar to indoor conditions. The spliced images were created using Adobe Photoshop software. Figure 6 shows a few example images from this dataset.

1714 (2021) 012038

doi:10.1088/1742-6596/1714/1/012038



Figure 6. Example images from CUISDE dataset, top row: authentic images; bottom row: spliced images.

In the literature, most of the authors have used detection accuracy metrics to evaluate their proposed image splicing detection methods. Hence, we have also used the detection accuracy metric to evaluate the proposed method. The detection accuracy is defined as (Eq.3) [41], [42], [26]:

Detection accuracy
$$=\frac{T_p+T_n}{T_p+T_n+F_p+F_n} \times 100$$
 (3)

Where T_p is the true positive and defined as the total number of images that are correctly detected as spliced. T_n is the true negative and defined as the total number of authentic images that are detected as authentic. F_p is the false positive and defined as the total number of authentic images that are erroneously detected as spliced. F_n is the false negative and defined as the total number of spliced images that have erroneously identified as authentic.

5.2 Experimental results

The k-fold cross-validation evaluation scheme is one of the popular evaluation schemes in the machine learning area. This evaluation scheme provides reliable results especially when the training dataset is small. In our case, we have selected k=10, hence, our evaluation scheme becomes 10-fold cross-validation. In this scheme, we first, shuffle all the images randomly. Second, the whole dataset is divided into 10 unique groups (folds). In the third step, we train the model on images in 9 groups and consider the remaining one group for testing purposes. In the fourth step, we discard the model and repeat the same steps for all remaining groups. Finally, the average accuracy from all ten evaluations is considered as the final detection accuracy of the proposed model. One of the benefits of k-fold cross-validation methods is that all the images in the dataset are considered for both training and validating purposes.

From the experiments, it was observed that proposed method can detect an average of 178 forged images correctly out of 180 forged images in the dataset (this indicates $T_p=178$). In other words, we can say that proposed method failed to detect only two images out of 180 forged images in the dataset (this indicates $F_n=2$). Further, it has also been observed that a total of 175 authentic images were detected as authentic out of 183 authentic images in the dataset (this indicates $T_n=175$). That means the proposed method classified eight authentic images as forged (this indicates $F_n=8$). The proposed method obtains an average detection accuracy of 97.24% on the CUISDE dataset.

1714 (2021) 012038

doi:10.1088/1742-6596/1714/1/012038

5.3 Result comparison with existing methods

This section compares the experimental results of the proposed method with the other existing state-of-the-art image splicing detection methods. A total of eight methods namely Zhao et al. [41], Muhammad et al. [42], Vidyadharan et al. [26], He et al. [12], Alahmadi et al. [43], Hakimi et al. [25], Manu et al. [44], and Zhang et al. [13] were used for the comparison purpose. The comparative results highlighted in Table 1 prove the superiority of the proposed deep learning-based method in terms of detection accuracy. From Table 1, it can be observed that the accuracy of the proposed method is 97.24% which is the highest among all referenced methods. It can also be noticed that the hand-crafted feature-based method [43] have shown the second-best detection accuracy of 96.60%. This concludes that the combination of LBP and DCT shows good robustness. At the same time, it can be noticed that the method of He et al. [12] is the worst performing method among all, from this it can be assumed that the feature combination of DCT and DWT performed poorly.

Table 1. Experimental results comparison

Method	Used Feature extractor	Classifier	Detection accuracy (%)
Zhao et al. [41]	Optimal chroma-like channel	SVM with Gaussian kernel	93.14
Muhammad et al. [42]	Steerable pyramid transform and LBP	SVM	96.39
Vidyadharan et al. [26]	LBP	Random forest	92.01
He et al. [12]	DCT and DWT	SVM	87.52
Alahmadi et al. [43]	DCT and LBP	SVM	96.60
Hakimi et al. [25]	LBP, wavelet transform, and PCA	SVM	95.13
Manu et al. [44]	DCT	SVM	95.98
Zhang et al. [13]	DCT and LBP	SVM	91.38
The proposed method	ResNet-50	SVM with RBF kernel	97.24

6. Conclusion

In this paper, a deep learning-based method to detect the image splicing forgery is proposed. The proposed method outperforms other existing methods on the CUISDE dataset and obtains an accuracy of 97.24%. The proposed method performs well due to two main reasons: first, the Noiseprint based residual noise map highlights the tapering artifacts in the spliced images in a more accurate manner. Second, the use of deep CNN ResNet-50 based feature extractor and transfer learning part of the method can learn the distinctive features between the authentic and spliced images. The proposed method classifies images as authenticated or spliced using the SVM classifier. In the future, the proposed method can be further enhanced to distinguish authentic videos (videos recorded using a single camera) from spliced videos (videos created by merging different videos). Moreover, this work can be extended to locate the exact spliced region in the forged image.

- [1] Machado C, Kira B and Howard P N 2019 A Study of Misinformation in WhatsApp groups with a focus on the Brazilian Presidential Elections *WWW '19: Companion Proceedings of The 2019 World Wide Web Conference* pp 1013–9
- [2] Jessica McDonald 2020 Social Media Posts Spread Bogus Coronavirus Conspiracy Theory
- [3] Tyagi V 2018 Understanding Digital Image Processing (CRC Press)
- [4] Ansari M D, Ghrera S P and Tyagi V 2014 Pixel-Based Image Forgery Detection: A Review *IETE J. Educ.* **55** 40–6
- [5] Meena K B and Tyagi V 2020 A hybrid copy-move image forgery detection technique based on Fourier-Mellin and scale invariant feature transforms *Multimed. Tools Appl.* **79** 8197–212. https://doi.org/10.1007/s11042-019-08343-0

1714 (2021) 012038 doi:10.1088/1742-6596/1714/1/012038

- [6] Meena K B and Tyagi V 2020 A copy-move image forgery detection technique based on tetrolet transform *J. Inf. Secur. Appl.* **52** 102481. https://doi.org/10.1016/j.jisa.2020.102481
- [7] Meena K B and Tyagi V 2019 A copy-move image forgery detection technique based on Gaussian-Hermite moments *Multimed. Tools Appl.* **78** 33505–33526. https://doi.org/10.1007/s11042-019-08082-2
- [8] Meena K B and Tyagi V 2019 A Novel Method to Distinguish Photorealistic Computer Generated Images from Photographic Images 2019 Fifth International Conference on Image Information Processing (ICIIP) (Shimla, India) pp 385–90. 10.1109/ICIIP47207.2019.8985711
- [9] Kanwal N, Girdhar A, Kaur L and Bhullar J S 2020 Digital image splicing detection technique using optimal threshold based local ternary pattern *Multimed. Tools Appl.* **79** 12829–12846
- [10] Pomari T, Ruppert G, Rezende E, Rocha A and Carvalho T 2018 Image Splicing Detection Through Illumination Inconsistencies and Deep Learning *Proc. Int. Conf. Image Process. ICIP* 3788–92
- [11] Jaiswal A K and Srivastava R 2020 A technique for image splicing detection using hybrid feature set *Multimed. Tools Appl.* **79** 11837–60
- [12] He Z, Lu W, Sun W and Huang J 2012 Digital image splicing detection based on Markov features in DCT and DWT domain *Pattern Recognit.* **45** 4292–9
- [13] Zhang Y, Zhao C, Pi Y, Li S and Wang S 2015 Image-splicing forgery detection based on local binary patterns of DCT coefficients *Secur. Commun. Networks* **8** 2386–95
- [14] Zhang Q and Lu W 2016 Joint Image Splicing Detection in DCT and Contourlet Transform Domain *J. Vis. Commun. Image Represent.* **40** 449–58
- [15] Li X, Jing T and Li X 2010 Image Splicing Detection Based on Moment Features and Hilbert-Huang Transform *IEEE Int. Conf. Inf. Theory Inf. Secur.* 1127–30
- [16] Rao Y and Ni J 2017 A deep learning approach to detection of splicing and copy-move forgeries in images 8th IEEE Int. Work. Inf. Forensics Secur. WIFS 2016 1–6
- [17] Ahmed B and Gulliver T A 2020 Image splicing detection using mask-RCNN *Signal, Image Video Process.* **14** 1035–1042
- [18] Hussien N Y, Mahmoud R O and Zayed H H 2020 Deep Learning on Digital Image Splicing Detection Using CFA Artifacts *Int. J. Sociotechnology Knowl. Dev.* **12** 31–44
- [19] Wang J, Ni Q, Liu G, Luo X and Kr S 2020 Image splicing detection based on convolutional neural network with weight combination strategy *J. Inf. Secur. Appl.* **54** 102523
- [20] Abd E I, Taha E A and Zayed H H 2020 A Passive Approach for Detecting Image Splicing Based on Deep Learning and Wavelet Transform *Arab. J. Sci. Eng.* **45** 3379–86
- [21] Meena K B and Tyagi V 2020 A Deep Learning Based Method to Discriminate Between Photorealistic Computer Generated vol 19 (Springer Singapore). https://doi.org/10.1007/978-981-15-6634-9_20
- [22] Meena K B and Tyagi V 2019 Methods to Distinguish Photorealistic Computer Generated Images from Photographic Images: A Review *Advances in Computing and Data Sciences*, vol. 1 (Springer Nature Singapore Pte Ltd.) pp 64–82. https://doi.org/10.1007/978-981-13-9939-8_7
- [23] Ng T, Chang S and Sun Q 2004 Blind detection of photomontage using higher order statistics *IEEE Int. Symp. Circuits Syst.* 7–10
- [24] Zhang W, Cao X, Qu Y, Hou Y, Zhao H and Zhang C 2010 Detecting and extracting the photo composites using planar homography and graph cut *IEEE Trans. Inf. Forensics Secur.* **5** 544–55
- [25] Hakimi F, Hariri M and Gharehbaghi F 2016 Image splicing forgery detection using local binary pattern and discrete wavelet transform *Conf. Proc. 2015 2nd Int. Conf. Knowledge-Based Eng. Innov. KBEI 2015* 1074–7
- [26] Vidyadharan D S and Thampi S M 2017 Digital image forgery detection using compact multitexture representation *J. Intell. Fuzzy Syst.* **32** 3177–3188
- [27] Zhao X, Wang S, Li S and Li J 2015 Passive Image-Splicing Detection by a 2-D Noncausal Markov Model *IEEE Trans. Circuits Syst. Video Technol.* **25** 185–99
- [28] Wang R, Science C, Lu W, Science C, Yat- S, Li J, Science C, Xiang S, Zhao X, Academy C and Wang J 2018 Digital Image Splicing Detection Based on Markov Features in QDCT and

1714 (2021) 012038

doi:10.1088/1742-6596/1714/1/012038

- QWT Domain Int. J. Digit. Crime Forensics 10
- [29] Wang J, Liu R, Wang H, Wu B and Shi Y 2020 Quaternion Markov Splicing Detection for Color Images Based on Quaternion Discrete Cosine Transform *KSII Trans. Internet Inf. Syst.* **14** 2981–96
- [30] Wang X, Zhang Q, Jiang C and Zhang Y 2020 Coarse-to-fine Grained Image Splicing Localization Method Based on Noise Level Inconsistency 2020 Int. Conf. Comput. Netw. Commun. 79–83
- [31] Bunk J, Bappy J H, Mohammed T M and Nataraj L 2017 Detection and Localization of Image Forgeries Using Resampling Features and Deep Learning *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops* pp 1881–9
- [32] Liu B and Pun C M 2018 Locating splicing forgery by fully convolutional networks and conditional random field *Signal Process. Image Commun.* **66** 103–12
- [33] Salloum R, Ren Y and Jay Kuo C C 2018 Image Splicing Localization using a Multi-task Fully Convolutional Network (MFCN) *J. Vis. Commun. Image Represent.* **51** 201–9
- [34] Chen B, Qi X, Wang Y, Zheng Y, Shim H J and Shi Y Q 2018 An Improved Splicing Localization Method by Fully Convolutional Networks *IEEE Access* **6** 69472–80
- [35] Xiao B, Wei Y, Bi X, Li W and Ma J 2019 Image Splicing Forgery Detection Combining Coarse to Refined Convolutional Neural Network and Adaptive Clustering *Inf. Sci.* (Ny). **511** 172–91
- [36] Rao Y, Ni J and Zhao H 2020 Deep Learning Local Descriptor for Image Splicing Detection and Localization *IEEE Access* 25611–25
- [37] Zampoglou M, Papadopoulos S and Kompatsiaris Y 2017 Large-scale evaluation of splicing localization algorithms for web images *Multimed. Tools Appl.* **76** 4801–34
- [38] Meena K B and Tyagi V 2019 Image Forgery Detection: Survey and Future directions *Data*, *Engineering and applications*, *vol.2* pp 163–95. https://doi.org/10.1007/978-981-13-6351-1 14
- [39] Cozzolino D and Verdoliva L 2019 Noiseprint: a CNN-based camera model fingerprint *IEEE Trans. Inf. Forensics Secur.* 1–13
- [40] Yu-Feng Hsu S-F C 2006 Detecting image splicing using geometry invariants and camera characteristics consistency *IEEE Int. Conf. Multimed. Expo* 549–52
- [41] Zhao X, Li S, Wang S, Li J and Yang K 2012 Optimal chroma-like channel design for passive color image splicing detection *EURASIP J. Adv. Signal Process.* **2012** 1–11
- [42] Muhammad G, Al-Hammadi M H, Hussain M and Bebis G 2014 Image forgery detection using steerable pyramid transform and local binary pattern *Mach. Vis. Appl.* **25** 985–95
- [43] Alahmadi A, Hussain M, Aboalsamh H, Muhammad G, Bebis G and Mathkour H 2016 Passive detection of image forgery using DCT and local binary pattern *Signal, Image Video Process.* 11 81–8
- [44] Manu V T and Mehtre B M 2019 Tamper detection of social media images using quality artifacts and texture features *Forensic Sci. Int.* **295** 100–12