Study on Deep Learning Based Techniques for Image Tamper Detection

Manjunath S[1], Saadhvi Hosmane[2], Punyashree M[3], Aditi Ladia[4] and Anirudha Malpani[5]
[1]*Associate Professor, Department of Information Science and Engineering, Global Academy of Technology, Bangalore*
[2,3,4,5]*Student, Department of Information Science and Engineering, Global Academy of Technology, Bangalore*

***Abstract* - Photographs are the foremost powerful and trustworthy media of expression. At present, digital images not only give forged information but also work as agents of secret communication. Users and editing professionals manipulate digital images with various objectives. Scientists and researchers manipulate images for his or her work to urge published; medical images are tampered to misrepresent the patients' diagnostics, journalists use the trick for creating and giving dramatic effect to their stories, politicians, lawyers, forensic investigators use tampered images to direct the opinion of people, court, or law to their favor then on. Hence, distinguishing the primary images from faked lots and establishing the authenticity of digital photographs has gained much importance in recent times. The objective of this study is to understand different techniques to detect image tampering usingDeep Learning.**

***Index Terms*– Block-based approach, Copy-Move, CNN, Deep Learning, Image Tampering.**

I. INTRODUCTION

In recent times, digital image tampering is easier due to easy access of commercial image editing software, free or paid. For example, these software's have made it easier to duplicate and manipulatethe image's content without (significantly) demeaning its quality or leaving any visible suggestions to an untrained eye(depending on the skills of the user, the software used, etc.).

Image manipulation, often known as image editing, is any type of action performed on digital images using any software. Image forgery is a technique for altering the content of an image to make it contradict a historical truth. Image tampering is a sort of image forgery in which new content is substitutedfor some of the original content in an image. It's termed copy-move tampering if the new content is copied from the same image, and it's called image splicing if the new content is copied from a different image. The statement of the intended alteration of facts restricted within the digital image to hide it or modifyit'll be known as attacks.

Traditional approaches for image manipulation detection usually use handcrafted structures. The major problem with these methods is the procedures can categorize a particular type of manipulation by recognizing a definite feature in that image. The most common alteration strategies found in image composition are copy-move, splicing, etc. In addition, the images that are extensively shared over the social media on the internet can be easily altered to misrepresent their meaning with malicious intention.Detecting traces of manipulation of the image is an instigative task and comparatively difficulty to declare images are trustworthy. Hence, the determination in enhanced image manipulation detection cannot be ignored.

II. LITERATURE REVIEW

In digital forensics, the detection of the presence of tampered images are important. The main take through of this literature is that majority of them identify certain features in images tampered by a specific tampering method (such as copy-move, splicing, etc). This implies that the tactic doesn't work reliably across various tampering methods. Additionally, in terms of tampered region localization, most of the work targets only JPEG images because of the exploitation of double compression artifacts left during the re-compression of the manipulated image. However, inreality digital forensics tools mustn't be specific to any image format and can even be ready to localize the region of the image thatwas modified.

In [1], the authors have proposed a two stage Deep learning approach to seek out featuresin order to detect tampered images in numerous image formats.For the first stage, they utilized a Stacked Autoencoder model to be told the complex feature for each individualpatch. In the second stage, they integrated the contextual information of eachpatch thus the detection was conducted more accurately. In their experiments, they were able to obtain an overall tampered region localization accuracy of about 91.09%over both TIFF and JPEG images from CASIA dataset, with a fall-out of 4.31% and a precision of 57.67% respectively. The accuracy over the JPEG tampered images was around 87.51%, which outperforms the 40.84% and 79.72% that were obtained from two state ofthe art tampering detection approaches. The authors in [2] proposed a Deep learning-based approach to detect object-based forgery within the advanced video. The presented deep learning approach uses aconvolutional neural network (CNN) to automatically extract high-dimension features from the inputimage patches. Different from the quality CNN models utilized in computer vision domain, they letvideo frames undergo three preprocessing layers before being fed into the CNN model. They includea frame absolute difference layer to cut down temporal redundancy between video frames, a maxpooling layer to reduce computational complexity of image convolution, and a high-pass filter layerto enhance the residual signal left by video forgery. Additionally, an asymmetric data augmentationstrategy has been established to urge a similar number of positive and negative image patches beforethe training. The experiments have demonstrated that the proposed CNN-based model with thepreprocessing layers has achieved excellent results. A customized convolutional neural network, named CGFace was proposed by the authors in [3]. It was specificallydesigned for the computer-generated face detection task by customizing the number of convolutionallayers, so it performs well in detecting computer-generated face images.Later on, an imbalancedframework (IF-CGFace) is formed by altering CGFace’s layer structure to manage to the imbalanceddata issue by extracting features from CGFace layers and use them to teach AdaBoost and eXtremeGradient Boosting (XGB). Further on, theyexplained about the tactic of generating an outsized computer-generateddataset supported the state-of-the-art PCGAN and commenced model. Followed by these various experiments were carried out to the means that the proposed model with augmented input yields the absolute best accuracy at98%. Finally, they provided comparative results by applying the proposed CNN architecture on imagesgenerated by another GAN research. In [4], the authors have proposed image forgery check system supported SURF features, it is most often a pixel basedtechnique where after preprocessing the photographs, relevant features are extracted and compared with an outlined estimated threshold value. According to the demonstrated results it's decided whether the image has been forged or notand if it’s, then the part where tampering has been done is displayed as a forged part. The proposed algorithm was tested using an open source CASIA image dataset. The presented result shows that SURF feature-based authentication provide forgery detection accuracy of 97%. The result was then compared with other techniques in similar domain to prove the novelty of the work. The author A Kuznetsov in [5] has presented an algorithm for detecting one of the foremost commonly used typesof digital image forgeries - splicing. The algorithm is based on the use of the VGG-16convolutional neural network. Here, image patches are taken as input and obtains results for each patch i.e., original or forgery. During the training stage the author selected patches from original image regions and on the borders of embedded splicing. The obtained results approximately has high classification accuracy such as 97.8% accuracy for fine-tuned model and around 96.4% accuracy for the zero-stage trained for a bunch of images containing artificial distortions in comparison with existing solutions and also the experimental research was conducted using the CASIAdataset.

The authors in [6] proposed an effective and efficient technique for detecting the copy-move forged imagesupported deep learning. They proposed an algorithm that initializes the tampered image because the input to the system to determine the tampered region. The system includes processes like segmentation, featureextraction, dense depth reconstruction, and eventually identifying the tampered areas. Theproposed Deep learning-based system can save on computational time and detect theduplicated regions with more accuracy. The understanding and extensive literature review of state-of-the-art techniques of deep learning within the detection of copy-move image forgery was presented by the authors of [7]. Because of this development of sophistication of tools and software like Adobe Photoshop,Pixir, and Affinity, digital images content is typically simplymanipulated, and thus forged images are produced. Thus, the process authenticating a digital image becomes difficultsuch as to differentiate between manipulated images and actualimages through the naked eyes.And also, the importance ofdigital image forensics has attracted many researchers who aredeeply involved during this area and has established manytechniques for forgery detection in image forensics. Lately, Deep learning approach features a high interest among researchersacross the sector and has shown good end in its application. Thus, forensic researchers plan to apply deep learningapproach as a way for detecting forgery image.[9] In this paper, the author proposed an innovative image forgery system that has been supported by Discrete Cosine Transformation (DCT) and native Binary Pattern (LBP) and a replacementfeature extraction method using the mean operator. First, images are divided into non-overlappingfixed size blocks and 2D block DCT is applied to capture changes because of image forgery.Also, LBP is applied to the magnitude of the DCT array to reinforce forgery artifacts. Finally, the mean of aparticular cell across all LBP blocks is computed, which yields a tough and fast number of features and presentsa more computationally efficient method. Using Support Vector Machine (SVM), the proposedmethod has been extensively tested on four documented publicly available gray scale and color imageforgery datasets, and additionally on an IoT based image forgery dataset that was built. Experimentalresults reveal the prevalence of the proposed method over recent state-of-the-art methods in terms ofwidely used performance metrics and computational time and demonstrate robustness against lowavailability of forged training samples.[10] Due to availability of many software's like Photoshop, GIMP, and Coral Draw, it is very hard to differentiate between original image andtampered image. Traditional methods for image forgerydetection often use handcrafted features.The matter with thetraditional approaches of detection of image tampering is thatmost of the methods can identify a selected sort of tampering byidentifying a particular feature in image. Currently Deep learning methods are used for image tampering detection. These methods reported better accuracy than traditional methods due totheir capability of extracting complex features from image. Inthis paper, the author presents an in depth survey of deep learning basedtechniques for image forgery detection, outcomes of survey inform of analysis and findings, and details of publicly availableimage forgery datasets.

GoogleNet deep learning model to extractthe image features and use Random Forest machine learning algorithm to detect whether the image is forged or not was implemented in [11].The proposed approach was implemented on the publicly available dataset MICC-F220 with k-fold cross validation approach to separate the dataset into training and testing dataset and compared with the state-of-the-art approaches. In [12] a mask regional convolutional neural network (Mask R-CNN) approachfor patch-based inpainting detection was proposed. [13] In recent years, many tampering operations were performed on the image and post-processingis done to erase the traces left behind by the tampering operation, making itmore difficult for the detector to detect the tampering. It was found that to detect image manipulation are often supported by Deep learning methods. In this paper, the authors had more focus on the study of various recent image manipulation detection techniques. Authors also examined various image forgeriesthat can be performed on the image and various image manipulation detectionand localization methods. In [14] a Deep learning-based method was proposed to detect image splicing within the images. At the start, the inputimage is preprocessed employing a technique called 'Noiseprint' to urge the noise residual bysuppressing the image content. Then he favored ResNet-50 network is employed as a featureextractor. Finally, the obtained features are classified as spliced or authentic using the SVMclassifier. The experiments performed on the CUISDE dataset show that the proposed methodoutperforms other existing methods. The proposed method achieves a mean classificationaccuracy of 97.24%. [15] In contrast with another recentsurvey, this paper covers significant developments in passiveimage forensic analysis methods adopting deep learningtechniques. Existing methodologies are studied concerningbenefit, limitation, the dataset used, and type ofattackconsidered. The paper further highlights future challenges andopen issues, and also provides the possible future solution inbuilding efficient tampering detection mechanism using deep learning technique. Experiment outcomes show goodperformance in reference to TPR, FPR, and F1-Score.

III.POSSIBLE SOLUTION FOR IMAGE TAMPER DETECTION

Recent image tampering work shows using deep learning techniques such as CNN aid in improving tampering detection accuracies. However, existing tampering detection methodologiespredominantly focused on identifying aparticular type of manipulations such as splicing, resampling, copy-move, etc. As a result, some method works well fordetecting one kind of attack; however, fails to detect another kind of hybrid attack such as introducing resampling attack ofcopy-move tampered segment. Along with that, it is practicallya difficult task to know the tampering type in advance. Then,segmenting only the tampering region is very difficult; especially when there exist multiple forgeries of similar patterns within an image. CNN in object segmentation have attained the very goodresult, CNN extracts hierarchical feature from the different level to segment meaningful shape ofrespective objects. Contrasting with meaningful segmentation, the tampered segment can be copied segment for anotherportion of an image, or it could be a removed object within an image. A well-crafted tampered image generally exhibits a good correlation between the authentic and tampered image. Thus, for detecting tampering and segmenting tampered region efficientlythe methodology explained in section IV.

IV.LITERATURE REVIEW SUMMARY

Article Number	AuthorNames	Year of Publication	Methodology	Pros	Cons
[1]	Ying Zhang,Jonathan Goh, LeiLeiWinandVrizlynn Thing	2016	Three-level, 2-D Daubechieswaveletdecompositionand StackedAutoencoders. CASIAv1.0,CASIAv2.0& Columbiadataset	Obtainedanaccuracyof91.09%.	CanworkwithonlyJPEGandTIFFimages. DeepBeliefNetworksnotexplored.
[2]	Ye Yao, YunqingShi, ShaoweiWeng andBoGuan.	2017	Stochastic Gradient DescentisusedtooptimizeCNN-based model.	Pristine Frame Accuracy:98.45±0.37%, ForgedFrame Accuracy:89.90±1.15%, Frame Accuracy:96.79± 0.11%	There is no mention of how tousethetrainedCNN-basedmodel to detect object forgeryinlowerbitrateorlowerresolutionvideosequences.
[3]	L. Minh Dang,Syed IbrahimHassan, SuhyeonIm, Jaecheol Lee,Sujin Lee andHyeonjoonMoon.	2018	CGFace model. PCGANdatasetandBEGANdataset.	CGFace Accuracy:98%AUC:81%	Themodelproposedinthispaper onlyextractsfeaturesfromadeep learningapproach,itwouldbeworthwhiletoinvestigateotherhiddenfeaturesfromcomputer-generated face images.

[4]	Payal Srivastava,Manoj Kumar,Vikas Deep andPurushottam Sharma	2019	SpeedUpRobustFeature(SURF)Method. CASIAdataset.	Accuracy:98%	Afteranalysingvariousimages of the dataset, it wasdiscovered that thecorresponding blocks fromboth images that have a pixeldifferenceofmorethan40000and areclassifiedasforged. But we don't know whichblocksaregenuineandwhich areforgeries.
[5]	AKuznetsov.	2019	The proposed model is likethe architecture of a VGG-like convolutional network.It takes patches with a fixedsize of 40x40x3 as inputsignals and is made up oftwo convolutional blocksand two fullyconnected blocks	Accuracy:97.8%	DetectsonlySplicing attacks.
[6]	Ritu Agarwal andOm PrakashVerma.	2019	The tampered image is usedasinput,andVGGNETis usedtoextractfeatures.After afewcomputations,theforgedareaisdetectedand displayedasoutput.	Accuracy:95%	The proposed method does notdetect images that have beenforged using the multi-clonedattack.Whilematchingmultipletamperedpatchesinan image, the patch matchingprocedureintheproposed approachgetsconfused.
[7]	Arfa Binti ZainalAbidin, AzurahBinti A Samah,Haslina BintiHashim andHairudin BinAbdulMajid.	2019	Copy-MoveForgeryDetection.Amedianfilteringdetectionmethodusingadeeplearningapproachbasedon Convolutional NeuralNetwork(CNN).	Many of the DeepLearning methods usedfor forgery detectionperformed better thanother forgery detectionmethods. Furthermore,they are reported to bemore efficient,particularlywhenGPU-based technology isused.	DeepLearningmethodsrequire a huge set of trainingandtestingdatafor thealgorithmtoworkefficiently.

[8]	Gul Muzaffer andGuzin Ulutas.	2019	Itconsistsofthreebasicsteps: •Deeplearning-basedfeatureextraction • Featurematching • Post-processing. PretrainedAlexNetconvolutionalneuralnetwork used.	Accuracy:93.94%	Detectsonlycopy-moveforgeries.Amorerobustmethod canbedeveloped.
[9]	MohammadManzurul Islam,Gour Karmakar,JoarderKamruzzamanand ManzurMurshed.	2020	Traditional machine learningtechnique(SVM)and hand-crafted features. FBDDFdataset.	Accuracy:95.84%	Professionally manipulatedimages contain various typesof attacks but the proposedmethod detects only splicingand copy-move attacks.
[10]	ZankhanaJ.Barad and Mukesh M.Goswami.	2020	Convolutional NeuralNetwork (CNN).	Deep-learning techniquesaremoreefficientthantraditionaltechniques.	DeepLearningmethodsrequire a huge set of trainingandtestingdataforthealgorithmtoworkefficiently.
[11]	Amit Doegar,Maitreyee Duttaand GauravKumar.	2020	RandomForestMachineLearning Algorithm, k-crossfoldapproach(k=5)and GoogleNetforfeatureextraction.	Accuracy:93.94%	MoreMachineLearningalgorithmscanbeexploredthatmayprovidebetterresults.
[12]	Xinyi Wang, HeWang andShaozhangNiu.	2020	Thebasisoftheproposedmethodologyis MaskR-CNNusing COCO dataset.	AccuracywithQF95%is96.7%.	Datasetsizecan beincreased.
[13]	Rahul Thakur andRajesh Rohilla.	2020	Variousrecentimagemanipulationdetection techniques.	Deeplearningbasedtechniquesautomatically learnthefeaturesandclassify.	Deep learning methods requirea larger dataset to be trainedwhen compared to traditionalmethods.

[14]	Kunj BihariMeena and VipinTyagi.	2021	Consistsofthreemainsteps: • Obtainingnoiseresidualmapusing the Noiseprint • Extracting features usingResNet-50 Feature classification using supportvectormachine	Accuracy:97.24%	Theexactsplicedregionisnotknown.
[15]	Manjunatha S andMaliniM Patil	2021	CNN in object segmentation haveattained very good results; CNNextracts hierarchical feature fromdifferentlevelstosegmentmeaningfulshapeofrespectiveobjects.	Recall/TPR:97.5% FPR:1.4% F1-Scoreperformance:97.7%	Considersafewassumptionsbefore putting the model towork.

IV. METHODOLOGY

The block-based approach splits an input digital image into blocks of square or circle for analysis during the pre-processing stage. These blocks can either overlap or not overlap with one another. These blocks can either overlap or not overlap with one another. Then, the features are extracted from these blocks and compared against one another to see the similarity between blocks within the image. Once the matched blocks are detected, these blocks represent the manipulation of forgery performed within the image as shown in the figure 1.

After a part of image where the forgery is detected, the sort of the forgery attack is detectedfurthermore. Generally, the feature extraction techniques for block-based are withinthe variety of frequency transform, texture and intensity, moments invariant, log polar transform,dimension reduction etc.From the literature, the matching techniques for block-based are often divided into sorting, hash, correlation, Euclidean distance, and others.

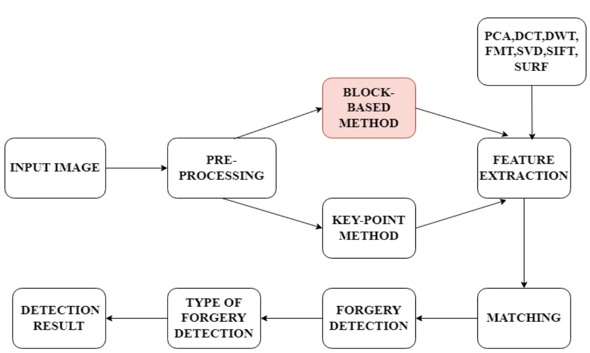

Figure 1:Methodology

V. CONCLUSION

In most of the research papers, researchers have clarified that image tampering detection may be a very complicated proceduredue to the vacuity of different software packages. All features are very sensitive to operations within the interference process. So, features in the image tampering process plays a pivotal part in the process of tamper discovery. All the prevailing methods don't achieve good accuracies for all kinds of forgery attacks like Splicing, Compression, Rotation, Resampling, Copy-move, and so on.

In computer vision, modern improvements in semantic tampering detection procedures are based on CNN and RNN. It is also found that it is important to design an efficient Deep Learning-based feature extraction mechanism that learns correlation among pixels more efficiently to get more accurate results. In the last decade, the utilization of convolutional neural networks (CNN) has spread within the image forensic community. These algorithms have focused on training the CNN to see the most effective features to classify camera models. One advantage of using CNN is that the features are extracted directly from the image dataset. The principal advantage of these CNN based approaches is that they are capable of learning classification features directly from image data. Itis also found that CNN-based tampering detection methodologies are highly efficient in detecting multiple tampering with high accuracies.

REFERENCES

[1] Ying Zhang, Jonathan Goh, Lei Lei Win & Vrizlynn Thing, “Image Region Forgery Detection: A Deep Learning Approach”, Proceedings of the Singapore Cyber-Security Conference (SG-CRC) 2016, doi:10.3233/978-1-61499-617-0-1.

[2] Ye Yao, Yunqing Shi, Shaowei Weng and Bo Guan, “Deep Learning for Detection of Object-Based Forgery in Advanced Video”, MDPI, Symmetry,26 December 2017, doi:10.3390/sym10010003.

[3] L. Minh Dang, Syed Ibrahim Hassan, SuhyeonIm, Jaecheol Lee, Sujin Lee and Hyeonjoon Moon, “Deep Learning Based Computer-Generated Face Identification using Convolutional Neural Network”, MDPI, Applied Sciences,13 December 2018, doi:10.3390/app8122610.

[4] Payal Srivastava, Manoj Kumar, Vikas Deep and Purushottam Sharma, “A Technique to Detect Copy-Move Forgery using Enhanced SURF”, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volum-8, Issue-6S August 2019, doi: 10.35940/ijeat. F1133.0886S19.

[5] A Kuznetsov, “Digital image forgery detection using deep learning approach”, Journal of Physics: Conference Series, ITNT 2019,doi:10.1088/1742-6596/1368/3/032028.

[6] Ritu Agarwal and Om Prakash Verma, “An efficient copy move forgery detection using deep learning feature extraction and matching algorithm”, Springer Science Business Media, LLC, part of Springer Nature 2019, 23 December 2019.

[7] Arfa Binti Zainal Abidin, Azurah Binti A Samah, Hairudin Bin Abdul Majid and Haslina Binti Hashim, “Copy-Move Image Forgery Detection Using Deep Learning Methods: A Review”, 978-1-7281-6726-8/19/$31.00 2019 IEEE.

[8] Gul Muzaffer and GuzinUlutas, “A new deep learning-based method to detection of copy-move forgery in digital images”, 978-1-7281-1013-4/19/$31.00 2019 IEEE.

[9] Mohammad Manzurul Islam, GourKarmakar, Joarder Kamruzzaman and Manzur Murshed, “A Robust Forgery Detection Method for Copy–Move and Splicing Attacks in Images”, MDPI, electronics,12 September 2020, doi:10.3390/electronics9091500.

[10] Zankhana J. Barad and Mukesh M. Goswami, “Image Forgery Detection using Deep Learning: A Survey”, 2020 6th International Conference on Advanced Computing & Communication Systems (ICACCS), 978-1-7281-5197-7/20/$31.00 2020 IEEE.

[11] Amit Doegar, Maitreyee Dutta and Gaurav Kumar, “Image Forgery Detection Using Google Net and Random Forest Machine Learning Algorithm”, Journal of University of Shanghai for Science and Technology, Volume 22, Issue 12, December – 2020, doi - 10.51201/12508.

[12] Xinyi Wang, He Wang and ShaozhangNiu, “An Intelligent Forensics Approach for Detecting Patch-Based Image Inpainting”, Hindawi, Mathematical Problems in Engineering, Volume 2020, Article ID 8892989, 10 pages, 28 October 2020, https://doi.org/10.1155/2020/8892989.

[13] Rahul Thakur and Rajesh Rohilla, “Recent Advances in Digital Image Manipulation Detection Techniques: A brief Review”, Forensic Science International, 24 April 2020,Published by Elsevier,https://doi.org/10.1016/j.forsciint.2020.110311.

[14] Kunj Bihari Meena and Vipin Tyagi, “A Deep Learning based Method for Image Splicing Detection”, Journal of Physics: Conference Series, CONSILIO 2020, IOP Publishing,doi:10.1088/1742-6596/1714/1/012038.

[15] Manjunatha S and Malini M Patil, “Deep learning-based Technique for Image Tamper Detection”, 2021 Third International Conference on Intelligent Communication Technologies & Virtual Mobile Networks (ICICV), 978-1-6654-1960-4/20, doi: 10.1109/ICICV50876.2021.9388471, 2021 IEEE.

[16] Marra, Francesco &Gragnaniello, Diego &Verdoliva, Luisa &Poggi,Giovanni. A Full-Image Full-Resolut ion End-to-End-Trainable CNNFramework for Image Forgery Detect ion, 2019.

[17] Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," 2016 Workshopon Information Forensics and Security (WIFS), Abu Dhabi, 2016, pp. 1-6,DOI: 10.1109/WIFS.2016.7823911.
[18] D. Cozzolino and L. Verdoliva. Single-image splicing localizationthrough autoencoder-based anomaly detection, 2016 IEEE InternationalWorkshop on Information Forensics and Security (WIFS), Abu Dhabi,2016, pp. 1-6, DOI: 10.1109/WIFS.2016.7823921.
[19] A. J. Fridrich, B. D. Soukal, and A. J. Luks, Detect ion of copy-move forgery in digital images, in Proceedings of Digital Forensic ResearchWorkshop, Citeseer 2003.
[20] R. Dixit, R. Naskar, and A. Sahoo. Copy-move forgery detectionexploiting statistical image features, 2017 InternationalConference onWireless Communications, Signal Processing, and Networking(WiSPNET), Chennai, 2017, pp. 2277-2281.
[21] IreneAmerinia, TiberioUricchioa, LambertoBallana, Roberto Caldellia.Localization of JPEG double compression through multi-domainconvolutional neural networks. IEEE Conference on Computer Visionand Pattern Recognition Workshops 2017. DOI10.1109/CVPRW.2017.233.
[22] Belhassen Bayar, Matthew C. Stamm. ADeep Learning Approach ToUniversal Image Manipulation Detection Using A New ConvolutionalLayer. ACM. ISBN 978-1-4503-4290-2/16/06.
[23] Henry Farid. Image Forgery Detection. IEEE Signal ProcessingMagazine, March 2007.