2022 International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS) | 978-1-6654-6883-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/IC3SIS54991.2022.9885600

A Comparative Analysis of Image Forgery Detection Techniques

Mohit Baviskar
Department of Computer Engineering
College of Engineering, Pune
Pune, India
mohitbaviskar360@gmail.com

Sheetal Rathod
Department of Computer Engineering
College of Engineering, Pune
Pune, India
rathod.sheetal24@gmail.com

Jay Lohokare
Department of Computer Science
State University of New York, Stony Brook
Stony Brook, USA
jlohokare@cs.stonybrook.edu

***Abstract*—An image is an essential medium for information sharing. Growth in technology led to the development of various applications like Adobe Photoshop, Snapseed, Gimp, and Prisma. These applications make it very easy for anyone to modify an image, giving rise to a new field of research called image forgery. Different pixel-level, block-based, camera-based, and mathematical algorithm-based techniques were developed to identify forged or modified images. Deep learning methods showed promising results as they considered more features than traditional methods. The study aims to conduct a comparative examination of image forgery methods. This paper also proposes an eight-layer CNN-based model with a relu activation function for the first seven layers and a sigmoid for the last one. Pretrained models VGG-16 and VGG-19 are used for comparison with the proposed model as they are the most widely used image classification models. In the proposed approach, the image dataset is first used to create a new dataset by applying the ELA (error level analysis) method to the original images. It is used for training the proposed model. The Casia dataset and MICC F2000 datasets were used for experimentation. This paper presents a comparative analysis of forgery methods based on the results. Results reveal that the proposed CNN model trained on ELA images outperforms other pre-trained models. All the models produced better results for MICC-F2000 than for the Casia dataset. The proposed model showed promising results on the small-sized image.**

***Index Terms*—image forgery, deep learning, image tampering, image classification, convolutional neural network, error level analysis**

I. Introduction

The term ”image forgery” means modifying or altering an original digital image for some unethical or illegal purposes. The development and improvement in the field of computer graphics have been tremendous. It led to the creation of softwares like Photoshop, Prisma, Snapseed, Gimp, and many more making image editing easy. Photo manipulation is frequently exploited on social media, the business world, and even for criminal purposes. The unlawful use of image tampering should be of great concern because it poses a significant threat to society, the government, and industry. Consequently, the legitimacy of photos found on the Internet needs to be checked. Maintaining the integrity of digital photos is essential. In such cases, it is possible to use forgery detection methods to assess the legitimacy of the images. Different approaches to detecting false images are discussed in the next paragraph.

In recent decades, several different approaches have been developed. Traditional techniques include methods based on key-points and blocks [16]. One of the first approaches was DCT (Direct Cosine Transformation) [15]. It works properly with copy-move forgery. Different pixel-based methods are also used with different combinations of steps like application of DWT (Discrete Wavelet Transform), dividing an image into pixel blocks, applying different filters, using radix sort and removal of noise [17]. Other methods of image forgery detection include median filters, high pass filters, deep learning methods, and more. Earlier studies focused on some traditional and deep learning approaches. One of their issues is the lack of utilisation of different types of data sets generated from various sources. They did not consider the comparison of image classification models. The research was carried out using the error level analysis method to detect false images [14]. Nevertheless, they were specifically made for a particular purpose.

This work focuses on three major deep learning models for identifying image forgery. The study presented is the first case study involving multiple deep learning models and error level analysis techniques. Two well-known datasets in image forgery are used for the research work. It covers several image formats like JPEG, TIFF, and PNG.

The study showed that the CNN model combined with the ELA method suits the problem statement. The combined approach has future applications in the field of image forensics. The proposed model presented in this paper is a lightweight CNN model. One of its advantages is that it contains no fully connected convolutional layer.

The remainder of the paper is organised in the following manner: Section II gives an overview of various types of image forgery. Imagenet models and error level analysis techniques are also explained in Section II. Section III presents related works. The proposed system is described in section IV, while the experimental setup and results are defined in section V. Conclusion remarks are given in section VI.

II. Types of Image Forgery, CNN models and ELA

A. Types of Image Forgery

Several approaches for image authentication have been developed [11]. There are two essential authentication methods:

Active authentication and Passive authentication.

1) Active authentication: Active authentication requires prior knowledge of the photograph for the authentication process. It is concerned with data concealment, in which some code is placed in the image during the generating process. Verifying this code validates the image's authenticity. Digital watermarking and digital signatures are the two forms of active authentication mechanisms. Digital watermarks are implanted into photos during the acquisition or processing step. In contrast, digital signatures insert some secondary information, generally taken from the image, into the image at the acquisition end. The fundamental disadvantage of these techniques is that the watermark or signature must be placed into photographs when recorded using specific equipment, requiring previous knowledge of the image.

2) Passive authentication: Passive authentication, often known as image forensics, is the method of authenticating photographs without prior information other than the image itself. Passive approaches are founded on the notion that, while tampering may not leave any visible evidence, it is likely to change the underlying statistics. These discrepancies are what are utilised to identify manipulation. Passive approaches are divided into forgery-dependent and independent forgery techniques.

Forgery-dependent detection methods detect only specific types of forgeries, such as copy-move and splicing, dependent on the type of forgery performed on the image. In contrast, independent forgery methods detect counterfeits independent of forgery type but based on artefact traces left during the resampling process and lighting inconsistencies. The primary goal of the passive detection approach is to determine if a picture is original or not. Most existing algorithms take features from images, then choose an appropriate classifier and categorise the features.

Copy-move Forgery:

One of the most popular image tampering techniques is copy-move; spotting this counterfeit is difficult since the cloned image takes part from the same image. A portion of a picture is copied and pasted into another portion of the same image in Copy-Move image forgery. It simply entails copying picture blocks into the same image and concealing vital information or objects from view.

Image splicing Forgery:

Image splicing is a picture compositing technique that involves joining image fragments from the same or separate images without further post-processing, such as smoothing the borders between the pieces. Image splicing forgery is the synthesis or merging of two or more photographs that drastically alters the source image to create a fabricated image. When photos with different backgrounds are blended, making the borders and limits indistinguishable becomes exceptionally challenging.

3) Image retouching: Image retouching is another image counterfeiting technique often employed for professional and entertainment reasons. Most retouching operations are performed to improve or diminish the image's attributes. Retouching is also used to make a believable composite of two photos, which may require rotating, resizing, or extending one of the images.

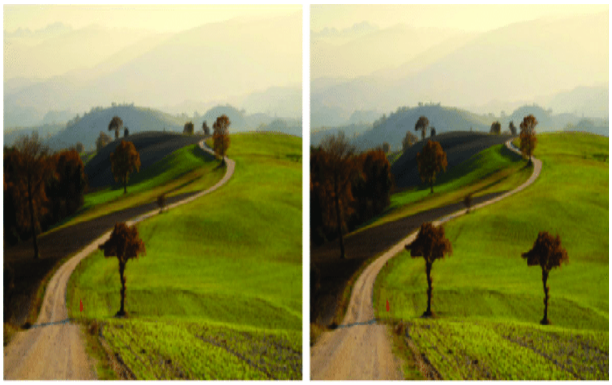

Fig. 1. copy-move forgery
[13]

(a) (b)

Fig. 2. image-splicing forgery
[18]

B. Deep Learning models and ELA

1) VGG models: VGG (Visual Geometry Group) is a multi-layered deep CNN (Convolutional Neural Network) architecture. The "deep" refers to the 16 and 19 layers in VGG-16 and VGG-19, respectively. The VGG architecture is the basis for cutting-edge object recognition models. It is used widely as image recognition framework. The VGG model, often known as VGGNet, is a convolutional neural network model introduced by A. Zisserman and K. Simonyan of the University of Oxford that supports 16 layers. The VGG16 model was trained using Nvidia Titan Black GPUs for several weeks. It substitutes AlexNet's large kernel-sized filters, resulting in considerable gains over AlexNet. The VGG19 model works on the same concepts as the VGG16 model, except it supports 19 layers.

2) Error level analysis: The investigation of compression artefacts in digital data with lossy compressions, such as JPEG, is known as error level analysis (ELA). It allows detecting parts of a picture with varying compression levels. The entire picture should be at the same level when using JPEG photos. A digital alteration suggests if a part of the image has

Fig. 3. normal image

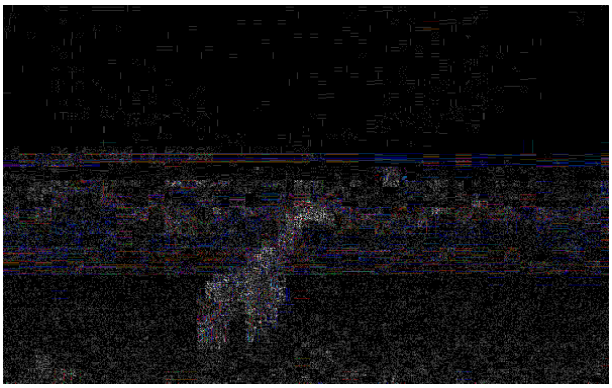

Fig. 4. image generated after applying ela

a noticeably different error level. ELA draws attention to discrepancies in JPEG compression rates. Equal edges in the ELA result should have similar brightness. All high-contrast edges should resemble one another, and all low-contrast edges should resemble one another. Low-contrast edges should be almost as bright as high-contrast edges in an original shot. Under ELA, comparable textures should have the same colour. Surface intricacy, such as a close-up of a basketball, will likely result in a greater ELA than a smooth surface. Under ELA, all flat surfaces should be about the same hue, regardless of their actual colour.

III. Related Works

The detection of copy-move and image splicing forgeries is the topic of this study. A lot of work has been done in this field in the last few decades. Pretrained models were used by Ouyang et al. in [1] for forgery classification. The models were adjusted and fine-tuned using small dataset samples to improve performance. Doegar et al. proposed the use of the Alexnet Model along with the SVM classifier [6], which employs the MICC F2000 dataset for training. In [3], Chen et al. used median filter residual to learn and obtain features from the image, which were further used to train the CNN model.A similar approach was used in [4]. They developed a novel convolutional layer of filters that would obscure the image's information while learning modified detecting characteristics. The first layer of the neural network was a pre-trained CNN that was used to extract dense features from test images. The final discriminative features for SVM classification were generated using a feature fusion strategy. Rao and Ni [2] created dense features using a high pass filter and a feature fusion approach. An analogous method was given in [10] by Wu et al. for blind forensics. A high-pass filter was used to reduce the detrimental impact of picture content on the tampering analysis process. Salloum et al. [5] advocated using a fully convolutional multi-task network. One branch was for learning the surface, while the other was for detecting the edges. An autoencoder-based method was suggested by Cozzolino and Verdoliva [7]. An autoencoder was given local features extracted from the image's noise residual, which produced an implicit model of the data. By iterating discriminative feature labelling and autoencoding, the implicit model eventually matches the new data, while the spliced area is flagged as anomalous. Zhang et al. [9] proposed a similar approach with stacked autoencoders. Based on CNN's feedback and propagation process, RRU-Net was used for forgery detection and localization by Bi et al. [8]. The proposed method showed promising results for the localization of the forged region.A combined approach of key-point and patch matching is proposed for copy-move forgery detection is presented in [13]. The ELA technique was used in [12] to increase the CNN model's efficiency. The proposed CNN model consisted of multiple dense layers.

IV. Proposed System

A. Image Preprocessing

Depending on the model, image preprocessing was slightly different. For the VGG models, the images were normalised. Further, they were resized to 224x224x3, the input size for standard VGG models. For the proposed model, a new dataset of images representing the difference in compression level over various regions in the image was generated. The ELA method was used for creating the above dataset from the original image dataset. The image was first saved in JPEG format before ELA; this applied a new compression level over the image. The difference between the first and newly stored images forms the ELA image. The images were later scaled and normalised. Finally, they were resized to a 125 x 125 x 3 input size for the proposed model.

B. Models

A modification was made to standard VGG models for the given problem statement. Only two classes were classified; therefore, the last classification layer was changed. The proposed CNN model consists of a total of eight layers. The first seven layers use the relu activation function. While the last layer, which is responsible for classification, uses the sigmoid function. The first seven layers all consist of 64 filters and have a kernel size of 5 x 5. After every two convolutional layers, a max-pooling layer of size 2 x 2 is applied.

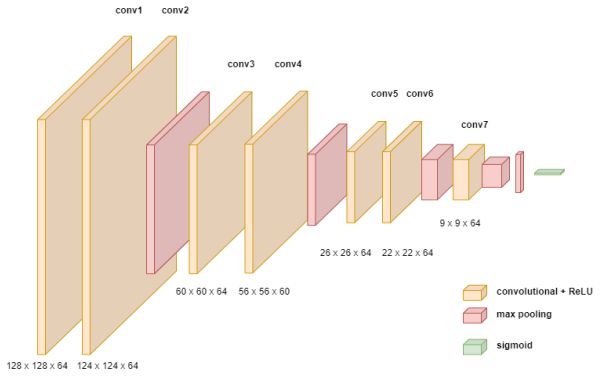

Fig. 5. Proposed Model

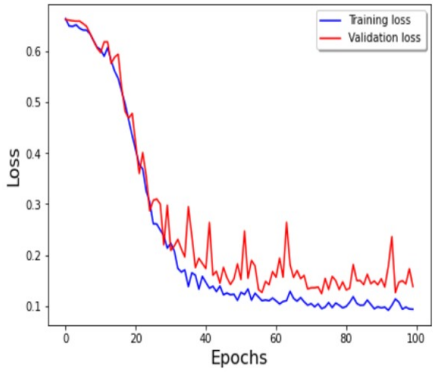

Fig. 6. ela-images trained CNN model loss for MICC F200 dataset

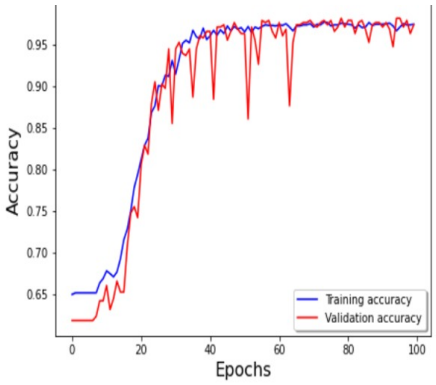

Fig. 7. ela-images trained CNN model accuracy for MICC F200 dataset

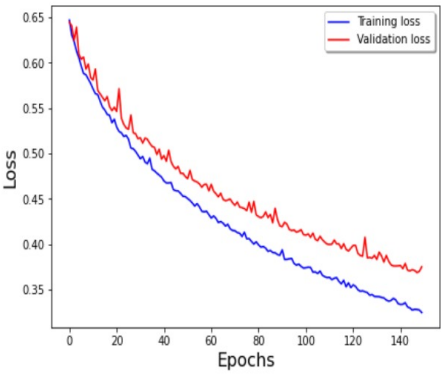

Fig. 8. VGG-19 model loss for MICC F200 dataset

C. Model training

All the models were trained for 50, 100, 150, and 200 epochs. It was observed that after 150 epochs, the model's performance did not improve. The models were trained for 150 epochs. The batch size was kept at 32. A ratio of 15:4:1 was used for splitting datasets into training, validation, and test datasets. A standard learning rate of 1e-4 was used. The Adam optimiser was used for training. The early stop callback method was utilised during training.

V. Experiments and Results

A. Experimental Setup

1) Hardware Setup: : The models were trained on 16GB GPU and 13GB RAM systems. The CPU used was Intel Xeon, and GPU used was Tesla P100.

B. Datasets

1) CASIA: (Chinese Academy of Sciences' Institute of Automation) The CASIA v2.0 dataset uses post-processing of tampered regions to create realistic and challenging false photos. It is a collection of 7491 authentic and 5123 altered colour images. CASIA v2.0 analyses uncompressed photos and JPEG images with various Q factors.

2) MICC F2000: (Media Integration and Communication Center, University of Florence) There are 1300 genuine photos and 700 manipulated photos in the collection. The images are up to 2048 x 1536 pixels in size. The manipulated region accounts for 1.12 per cent of the entire picture.

C. Results

The accuracy of the CNN model used with ELA gave training accuracy of around 0.92 and validation accuracy of 0.88 for the Casia dataset. It was better than the validation accuracies of VGG-16 and VGG-19, which were 0.63 and 0.62, respectively. Similarly, the accuracy for the MICC F2000 dataset was 0.93 for the CNN model. The VGG-16 and VGG-19 accuracy were 0.85 and 0.88, respectively. The testing accuracy for most of the models was the same as the validation accuracy.

TABLE I
CASIA V2 DATASET RESULTS

model	Accuracy	precision	recall	f1	error
VGG19	0.63	0.62	0.62	0.62	0.6452
VGG16	0.66	0.64	0.65	0.63	0.6
proposed model	0.92	0.88	0.88	0.88	0.22

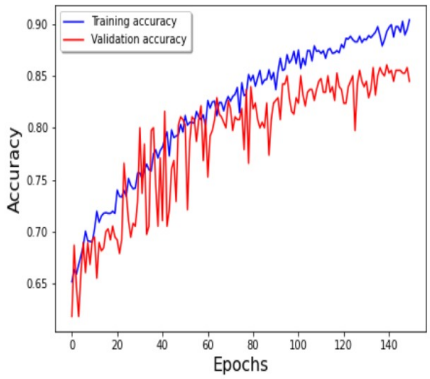

Fig. 9. VGG-19 model accuracy for MICC F200 dataset

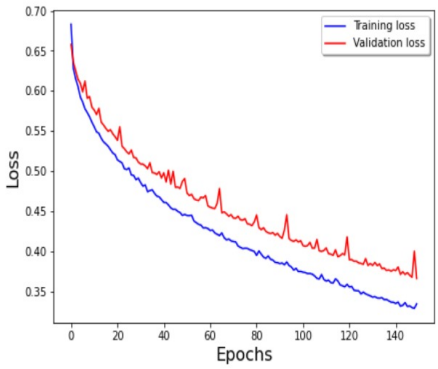

Fig. 10. VGG-16 model loss for MICC F200 dataset

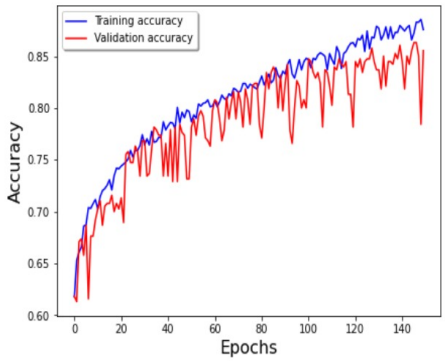

Fig. 11. VGG-16 model accuracy for MICC F200 dataset

TABLE II
MICCF2000 DATASET RESULTS

model	Accuracy	precision	recall	f1	error
VGG19	0.9	0.84	0.93	0.88	0.32
VGG16	0.88	0.85	0.85	0.85	0.33
proposed model	0.95	0.94	0.93	0.93	0.18

D. Discussion

The proposed model shows good accuracy as the images created through the ELA method focus on uniformity of compression in images. The model was able to classify images of sizes up to 1 MB correctly. However, there were some exceptions in testing where this model failed to classify correctly. The prime reason is that the image's compression level becomes almost the same after applying compression several times. Sometimes authentic images were classified as tampered ones due to unevenness in the colour space of images. The VGG-19 outperforms the VGG-16 for the MICC F2000 data set. However, the results are nearly identical for the CASIA data set, a much larger data set. So, there is a possibility of overfitting. However, validation and test accuracy contradict this.

VI. CONCLUSION

The paper presents a comparative study of various methods. The pre-trained VGG-16 and VGG-19, considered the best among the available models for image forgery detection, are compared with the CNN model trained on images preprocessed with the ELA method. The lightweight CNN model outperformed pre-trained models in terms of accuracy. The ELA method can be used for preprocessing pictures before they are tested for forgery. The presented study might be expanded to form a combined approach of ELA preprocessing and pre-trained models. This research can be further extended by considering more deep learning models and other techniques for preprocessing.

REFERENCES

[1] Ouyang, Y. Liu and M. Liao, "Copy-move forgery detection based on deep learning", 2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISPBMEI), Shanghai, 2017

[2] Rao, Y., and Ni, J. (2017). "A deep learning approach to detection of splicing and copy-move forgeries in images". 8th IEEE International Workshop on Information Forensics and Security, WIFS 2016

[3] Chen, J., Kang, X., Liu, Y., and Wang, Z. J. (2015)." Median Filtering Forensics Based on Convolutional Neural Networks". IEEE Signal Processing Letters, 22(11), 1849–1853.

[4] Belhassen Bayar and Mathew C. Stamm. "A Deep Learning Approach To Universal Image Manipulation Detection Using A New Convolutional Layer". ACM. ISBN 978-1-4503-4290-2/16/06.

[5] Ronald Salloum, Yuzhuo Ren, and Jay Kuo. "Image Splicing Localization Using A Multi-Task Fully Convolutional Network". arXiv:1709.02016v1-06/09/2017.

[6] Amit Doegar, Maitreyee Dutta and Gaurav Kumar. "CNN based Image Forgery Detection using pre-trained AlexNet Model". Proceedings of International Conference on Computational Intelligence and IoT (ICCI-IoT) 2018

[7] David Cozzolino and Luisa Verdoliva. "Single-image splicing localization through autoencoder-based anomaly detection". IEEE International Workshop on Information Forensics and Security (WIFS), Abu Dhabi, 2016, pp. 1-6, DOI: 10.1109/WIFS.2016.7823921.

[8] Xiuli Bi, Yang Wei, Bin Xiao and Weisheng Li. "The Ringed Residual U-Net for Image Splicng Forgery Detection". IEEE SIGNAL PROCESSING LETTERS, VOL. 22, NO. 11, NOVEMBER 2015

[9] Ying Zhang, Jonathan Goh, Lei Lei Win, and Vrizlynn Thing. "Image Region Forgery Detection: A Deep Learning Approach". Proceedings of the Singapore Cyber-Security Conference (SG-CRC) 2016; 1 – 11.

[10] Jian Wu , Xu Chang, Tongfeng Yang, Kai Feng. "Blind Forensic Method Based on Convolutional Neural Networks for Image Splicing Detection". 2019 IEEE 5 th International Conference on Computer and Communications.

[11] G. K. S. Gaharwar, Prof. V. V. Nath , R. D. Gaharwar. "COMPREHENSIVE STUDY OF DIFFERENT TYPES IMAGE FORGERIES".International Journal of Science Technology and Management. Vol. No.4 Special Issue No.1, August 2015

[12] C G Sri, S Bano, T Deepika, N Kola, Y L Pranathi."Deep Neural Networks Based Error Level Analysis for Lossless Image Compression Based Forgery Detection".2021 International Conference on Intelligent Technologies (CONIT) Karnataka, India. June 25-27, 2021
[13] Ke Liu, Wei Lu, Cong Lin, Xinchao Huang, Xianjin Liu, Yuileong Yeung, Yingjie Xue."Copy move forgery detection based on key-pointand patch match".Multimedia Tools and Applications, Springer Science+Business Media, LLC, part of Springer Nature 2019
[14] Qurat-ul-ain, Nudrat Nida, Aun Irtaza, Nouman Ilyas. "Forged Face Detection using ELA and Deep Learning Techniques".2021 International Bhurban Conference on Applied Sciences and Technologies (IBCAST) Inslamabad, Pakistan. 12-16 Jan. 2021
[15] Ahmet Boz, Hasan Şakir Bilge. "Copy-move image forgery detection based on LBP and DCT". 2016 24th Signal Processing and Communication Application Conference (SIU) Zonguldak, Turkey. 16-19 May 2016
[16] Henry Farid. "Image Forgery Detection". IEEE Signal Processing Magazine, March 2007
[17] Pradyumna Deshpande and Prashasti Kanikar. "Pixel Based Digital Image Forgery Detection Techniques". International Journal of Engineering Research and Applications, 2012
[18] Casia 2 Dataset, http://forensics.idealtest.org/
[19] MICC F2000 Dataset, micc dataset
[20] CoMoFoD, http://www.vcl.fer.hr/comofod
[21] Columbia DVMM Image Splicing Datasets, http://www.ee.columbia.edu/ln/ dvmm/newDownloads.htm