International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Survey on Digital Image Tamper Detection Using Deep Learning Algorithms

*V.Aravind[a],V.Durga Prasad[a],S.Swathi[a],Y.V.S Kalyan[a],U.Sandhya[a],R. Cristin[a]**

[a]*Department of Computer Science and Engineering, GMR Instituut of Technology, Rajam,Andhra Pradesh, India.*

ABSTRACT

Images may be used as prison evidence in forensics and plenty of other fields. . Image forgery refers to digital image manipulation to hide certain important and useful image information. Image tampering is a special kind of photo forgery that alters an element or more than one parts of graphic context of given image. There are many methods to tamper the image like copy-move photo forgery because of this copying part of an image and pasting the copied components into identical image .Detection of image tampering is very essential, but it is a very difficult task for humans with their naked eye. We can detect image forgery with the help of machines by feeding them with large amounts of data and applying deep learning techniques. By giving the image, we can detect whether the image is original or tampered. In deep learning, the Convolutional Neural Network is popular neural network model to extract complicated visual features in digital images. VGG16 is a simple and widely used Convolutional Neural Network architecture used for image processing. This project mainly for implementing VGG-16 network model in image dataset and detecting whether the image is pristine or tampered and performance is measured using accuracy of the model.

Keywords:Image tampering, convolutional neural network, copy-move forgery, deep learning, VGG-16.

1. Introduction

Photography should be used as part of the documentation of all serious crime scenes, including site visitor conflicts, burglaries, murders, and any other serious crimes against people or property. Images, however, can be misleading and difficult for viewers. Nowadays, there are a lot of technologies available like Adobe graphics store etc. which can easily edit or easily manipulate digital images. Photo manipulation refers to digital image modification to hide certain important or useful image information. There are situations when it is very difficult to identify a fixed location in a unique image. Fraudulent image detection is pushed with the help of need for originality and maintaining the image integrity. Interfering with image is unique type of image manipulation that changes part or most of the content of a given image.

* *Corresponding author.* Tel.:+91 9095051375
E-mail address: cristin.r@gmrit.edu.in

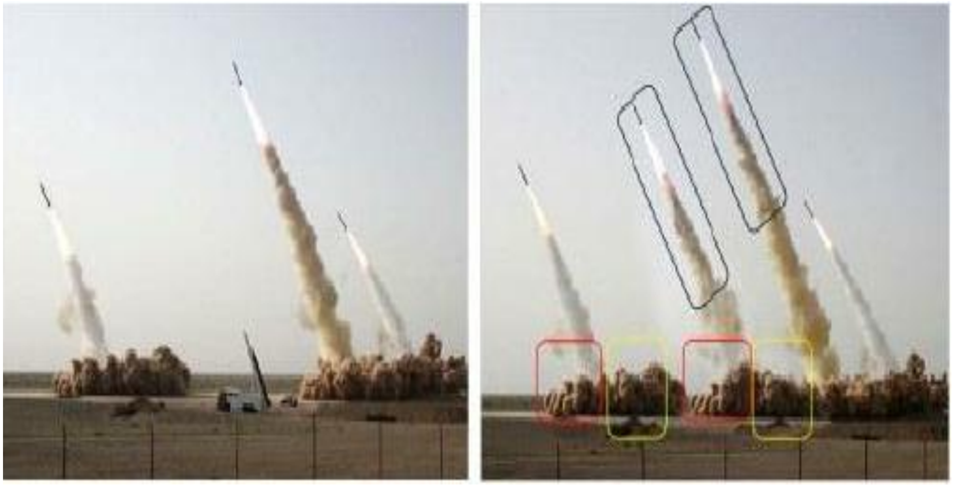

Figure1: Original Image and Fake Image

There are many methods such as cheating image-moving and pasting images etc. Copy image copying involves a single image i.e. part of the image is copied and pasted into the same image and image classification involves multiple images. The content of some images is copied and pasted into a single fake image. These lies can be misleading and must be accurately discovered .This deception in the image emerges as a realistic image but with the use of in-depth image processing techniques, we can distinguish real and fake pictures. Convolutional Neural Network is a type of in-depth learning strategy that can handle image data processing effectively. There are many models on CNN such as VGG-16, ResNet50, AlexNet that are very efficient and well-trained in advance with larger databases in a more precise way. This project deals with the acquisition of forged photocopying images using the VGG-16 algorithm and using the CASIA v2.0 data set. Model performance is measured using precision and accuracy. The various authors proposed a various image forgery detection techniques [6-11] in the research field

2. Related Work

Ali, S.S et al [1] proposed a robust deep learning method for image forgery detection in context of double image re-compression. CASIA v2.0 dataset is used for implementation of algorithm and proposed method which consists of 7491 pristine and 5123 tampered images. Images are recompressed using JPEG compression by applying Discrete Cosine Transform (DCT) followed by quantization. A light-weight CNN architecture is used inclusive of three convolutional layers followed by dense fully connected layer .Proposed technique obtained 92.23% accuracy with 98% quality.Marra, F et al.[2] This paper proposed the discovery of a fraudulent image based on CNN that makes decisions based on full image editing. Use multiple data sets: Vision, Dresden, NC2017, MFC2018, MFC2019 to get acquainted. In this structure, the images are not resized but processed intelligently and the results are linked online for a global decision. The framework consists of three blocks that make up the patch-level feature, combining features and global resolution. Advanced models have a fully illustrated frame and a complete CNN training solution for all types of counterfeit image detection. The model generates an ROC score of 0.83 points on all acquisitions and methods.

Kuznetsov, A. et al [3] introduced an algorithm for finding one of the most widely used forms of digital image deception namely Splicing. To solve the integration problem, they use CNN methods and divide images into two classes: real and distorted content. It is proposing a separation strategy based on image servants (episodes) which also eliminates the problem of data shortages. This model is a VNG-like architecture of CNN that accepts fixed size 40x40x3 leaflets as input signals and contains two convolutional blocks and two fully connected. They achieved 97.8% accuracy with a well-tuned model and 67.1% accuracy with compressed images.Rodriguez-Ortega.et al [4] proposed a common method of image detection that focuses on copy-move forgery using deep learning. To avoid the problem of bias and discrimination, authorize the model to be standardized by using 8 data sets that incorporate different types of images. The author has proposed two CMFD-based models for in-depth reading, one for custom design and one for transfer learning. By custom design the author has experimented with 5 different layouts with different layers. In transfer learning, the author considered a pre-trained VGG-16 model.The custom design model achieved 68% accuracy during the 1.8 second training period but the transfer learning model achieved 78% accuracy with the 2.8 training period.

Ouyang.et al [5] proposed a method of detection of novel fraud primarily based on the convolutional neural community. Authors simulated copy-move work using a rectangular block using computer production. The CNN architecture they use to implement CNN parameters based on the CaffeNet model, which is trained by ImageNet, and transferred to the launched CNN. Some parameters are adjusted such as reading rate, bulk size etc. Image data sets UCID and OXFORD were also used to mimic copy-pasting performance. The proposed model performed well on 97.6% of the generated data but did not perform well on animated photocopies and produced 58% accuracy.Rao Y.et al [6] introduces a new way of finding fake images that use 10 layers of CNN to automatically read hierarchical presentations on embedded images. Weights in the first layer of the network are started with a basic high throughput filter applied to the rich area model (SRM) and serve as a pre-processing module. Perform tests on CASIA v1.0 data sets, CASIA v2.0 and Columbia gray DVMM. First train CNN supervisors to learn disruptive activities with labeled pamphlets on training images and apply a single layer of FC at the end. Their proposed mode was given 98.04%, 97.83% and 96.38% accuracy in the specified databases, respectively.

Kalyani Dhananjay.et al[12] Mask R-CNN with MobileNet V1 is used. The mobile net is used because it is a model of light weight to be found compared to another and MobileNet V1 detects image splicing and copy move forgeries.To mark Mark R-CNN via MobileNet V1 seven different data sets are used such as Coverage, Casia 1.0, Casia 2.0, Columbia, MICC F220, MICC F600, MICC F2000.The R-CNN mask and Sobel filter are used for detection and retrieval of an object and for drawing a boundary around it to compile image and copy motion errors. Mask produced on solid images taken as two images, the character area may be white (True) and the background may be black (False).MobileNet's overall configuration was much better computer-based compared to ResNet-101. Matthew C.et al [13] specializes in a wide-ranging strategy for committing fraud and obtaining forged images using in deep learning. The proposed CNN architecture is for fraud detection covering eight layers. In this experiment the images are collected on 12 different camera models and devices without any previous interference or processing. Cut all the different images in half and split them into separate blocks. Most likely each block is associated with teens with their own distorted posters. All CNNs are used by Caffe's in-depth reading framework. The proposed model method can usually detect a few image illusions with median accuracy of 99.10%.

Sudiatmika .et al [14] detection of a forged image is done using an analysis of error level and in-depth reading strategies. The authors used the CASIA v2,0 database containing 7291 and 5123 corrupted images. The data set size has been changed to 224x224 pixels i.e. image orientation. In the next step, perform an analysis of the pressure errors. It is one way to identify images that have been deceived by keeping images in good quality and then calculating the difference from the compression phase. Authors have used VGG-16 structures to conduct training and analysis of error rate analysis. The model achieved 92.2% training accuracy and 88.46% validation using 100 times.Doegar .et al [15] proposes a CNNet-based model trained by CNN for various types of geometric distortions and forgery images. The AlexNet Architecture used in this paper, contains a number of layers and readable parameters and contains a total of 25 layers. The main layers are convolutional, pooling, ReLU, fully connected layers. The author has considered the MICC-F220 data set containing 220 images of which 110 are pure and 110 are forged. Images are resized to 227x227 according to the main version of the version. The features are extracted from a fully integrated layer and the SVM separator is used for resolution. The model finally achieved 93.94% accuracy with 100% accuracy and 89.19% accuracy.

Zhou J .et al [16] a neural block-based neural network is proposed to obtain forged images .The data sets considered were CASIA v1.0, CASIA v2.0 and the Columbia data set. The proposed method divides the larger image into smaller blocks of size 128x128 and these blocks are used to train the rich convolutional neural network and features are extracted from convolutional layer 8. They also do two-way integration which also proves that the model is very strong even in JPEG congestion. The proposed model uses the SVM separator and gained 97.62%, 97.87% and 96.38% accuracy respectively.Hebbar .et al [12] proposed a new framework for the detection of image impairment using Error Level Analysis and the Convolutional Neural Network with the proposed transmission method. Images are pre-evaluated for the use of ELA to illuminate the damaged area and are used for fine tuning the entire model. In buildings, instead of tearing down all work maps, use a GAP layer to obtain a standard operating vector that allows for reduced parameters, time and overlay. The model is best configured with a complete network training system with pre-processed snapshots of the CASIA2.0 database. Total performance if the version is correct with 97.58% accuracy with Residual Network 50 (ResNet50).

Yang .et al [17] proposed three Copy Move Forgery Detection (CMFD) algorithms namely key-based algorithms, block-based algorithms and in-depth reading algorithms. Key point-based algorithms are usually faster and more precisely run against geometric invasive operations and block-based algorithms can split image input into blocks and execute tasks in these blocks. The CMFD algorithm based on the proposed key points has four stages namely key output feature, matching, dual stage filter and image measurement. In this paper, a deceptive data set (IMD), a CoMoFoD data set, and a copy-move data (CMHD) database are used to evaluate the performance of the proposed algorithm and various well-represented various algorithms. The HFPM algorithm has obtained 92% accuracy in the CHMD database.NathS.et al [18-19] convolutional neural networks (CNN) are specifically used for features and a vector support device (SVM) as a detector that detects image manipulation primarily based on a feature vector. This test is done based on CASIA v2.0 database. This database is a collection of 12,614 colorful photographs, of which 7,491 are original and 5,123 are paired. ResNet-50 Architecture considers your included images of both length and width as 32 repetitions, and 3 as channel width. This structure consists of five separate sections and the two basic components of ResNet-50 are convolutional blocks and identity blocks. Based on experimental tests they found 97.33% accuracy in the CASIA v2.0 database.

Abdalla.et al [20-21] mainly aimed at building a convolutional neural network (CNN) to facilitate the discovery of counterfeit copy. Use a data set containing 166 and 1626 virtual images. Fake discovery may be subject to the power of a duplicate copy-motion image and the illusion of a copy. In this paper the detection of a fake image and local practice is used based on scale variation convolutional neural networks (SVCNNs). The element domain is targeted based on 3 specific phases of activity, polar cosine transforms (PCT), Zernike times (ZM), and Fourier-Mellin transform (FMT). Each hidden layer will enhance the strength of CNN's learning feature to increase its acquisition accuracy. This test achieved 90% accuracy.

VGG-16 Algorithm

The convolutional neural network is also known as ConvNet, which is a type of artificial neural network. The convolutional neural network has an insertion layer, an output layer, and a variety of hidden layers. VGG16 is a version of CNN (Convolutional Neural Network) which is regarded as one of the best computer-assisted visual models to date. in the configuration of the earlier art. They push the depth into 16-19 weight layers making it almost -138 trainees trained. VGG16 is an object detection and detection algorithm capable of distinguishing 1000 images of 1000 different categories with 92.7% accuracy. It is one of the most popular image classification algorithms and is easy to use with transfer learning.16 in VGG16 refers to 16 weighted components.

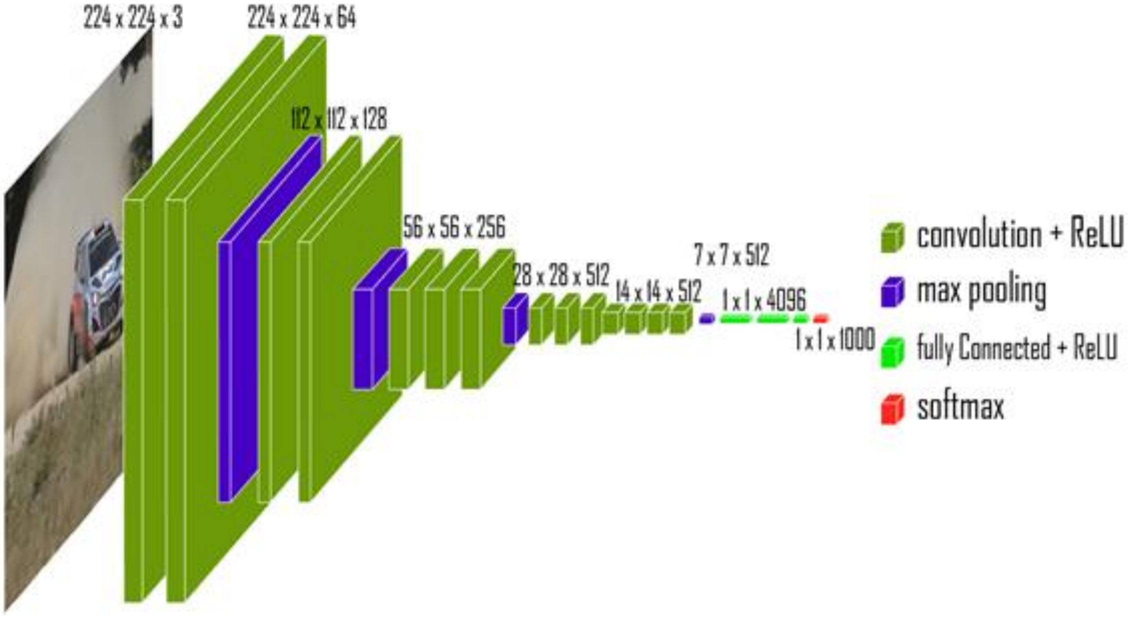

Figure 2: Architecture of VGG-16

In VGG16 there are thirteen conversion layers, five Max Pooling layers, and three dense layers comprising 21 layers but with only sixteen layers of weight i.e., a layer of readable parameters. The great thing about VGG16 is that instead of having a large number of hyper parameters they focus on having conviction layers of 3x3 filter with stride 1 and always use the same padding and maxpool layer 2x2 filter 2. Convolution and max pool. the layers are consistently arranged throughout the architecture. Conv-1 Layer has 64 filters, Conv-2 has 128 filters, Conv-3 has 256 filters, Conv-4 and Conv-5 has 512 filters. The Three Fully Combined Layers (FC) follow a number of flexible layers: the first two have 4096 channels each, the third makes the ILSVRC division which is 1000 channels and thus contains 1000 channels (one per class). The final layer is a soft-max layer. Training is very slow (the original VGG model was trained on the Nvidia Titan GPU for 2 weeks). The size of the VGG-16 trained imageNet weights is 528 MB. Therefore, it takes up a lot of disk space and bandwidth which makes it inefficient.

4. Conclusion

In this paper, we have proposed the VGG-16 neural network model for distinguishing real images from disturbed images. We have developed a combination system for learning neural network machine learning in advance and error analysis. Compared to the neural network conviction model vvg 16 gets high accuracy.in convolution neural network accuracy is 85.45% and VGG-16 is given over 86.24% accuracy.VGG-16 is a popular neural network model for extracting complex visual features in digital images. In short, we have divided the database into two types of damaged images and real images, and then determined the structures to be trained with a small database. The study results of this test show that we get the best training accuracy of 88.36% and certification is 86.13% over 100 epoch.

References

1. Ali, S.S.; Ganapathi, I.I.; Vu, N.-S.; Ali, S.D.; Saxena, N.; Werghi, N. Image Forgery Detection Using Deep Learning by Recompressing Images. Electronics 2022, 11, 403. https:// doi.org/10.3390/electronics11030403
2. Marra, F., Gragnaniello, D., Verdoliva, L., &Poggi, G. (2020). A full-image full-resolution end-to-end-trainable CNN framework for image forgery detection. IEEE Access, 8, 133488-133502.
3. Kuznetsov, A. (2019, November). Digital image forgery detection using deep learning approach. In Journal of Physics: Conference Series (Vol. 1368, No. 3, p. 032028). IOP Publishing.
4. Rodriguez-Ortega, Y., Ballesteros, D. M., &Renza, D. (2021). Copy-move forgery detection (CMFD) using deep learning for image and video forensics. Journal of Imaging, 7(3), 59.
5. Ouyang, J., Liu, Y., & Liao, M. (2017, October). Copy-move forgery detection based on deep learning. In 2017 10th international congress on image and signal processing, biomedical engineering and informatics (CISP-BMEI) (pp. 1-5). IEEE.
6. R. Cristin, N.R. Gladiss Merlin, T. Daniya" Geometrical Based Technique For Reflection Based Image Forgery Detection In Digital Images" International Journal of Scientific & Technology Research, Vol.No. 9, Issue No. 1, pp: 2654-2659.
7. B. Santhosh Kumar, S. Karthi, K. Karthika, and Rajan Cristin, "A Systematic Study of Image Forgery Detection", Journal of Computational and Theoretical Nanoscience (Scopus Indexed), Vol. 15,No.8 ,2018, Pages 1-4
8. Cristin R and Cyril Raj V, "Consistency features and fuzzy based segmentation for shadow and reflection detection in digital image forgery",science china information sciences, springer link, vol 65, no 1, pp 43-66, 2017
9. T. Daniya, N.R Gladiss Merlin, R.Cristin "Study on Digital Image Forgery Detection", International Journal of Advanced Science and Technology 29 (3),6851-6856
10. R. Cristin, N.R. Gladiss Merlin, T. Daniya" Geometrical Based Technique For Reflection Based Image Forgery Detection In Digital Images" International Journal of Scientific & Technology Research, Vol. No. 9, Issue No. 1, pp: 2654-2659.
11. B. Santhosh Kumar, R.Cristin, K.Karthick, T.Daniya "Study of Shadow and Reflection based Image Forgery Detection", IEEE International Conference on Computer Communication and Informatics(ICCCI -2019).
12. Rao, Y., & Ni, J. (2016, December). 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.
13. KalyaniDhananjayKadam , Swati Ahirrao , and KetanKotecha , Efficient Approach towards Detection and Identification of Copy Move and Image Splicing Forgeries Using Mask R-CNN with Mobile Net V1, , Computational Intelligence and Neuroscience ,Published 5 January 2022.
14. Matthew C. Stamm, Belhassen Bayar ,A Deep Learning Approach To Universal Image Manipulation Detection Using A New Convolutional Layer, IH&MMSec 2016, June 20-23, 2016.
15. Sudiatmika, I. B. K., & Rahman, F. (2019). Image forgery detection using error level analysis and deep learning. Telkomnika, 17(2), 653-659.
16. Doegar, A., Dutta, M., & Gaurav, K. (2019). CNN based image forgery detection using pre-trained AlexNet model. International Journal of Computational Intelligence & IoT, 2(1).
17. Zhou, J., Ni, J., & Rao, Y. (2017, August). Block-based convolutional neural network for image forgery detection. In International Workshop on Digital Watermarking (pp. 65-76). Springer, Cham
18. Hebbar, N. K., &Kunte, A. S. (2021). Transfer Learning Approach for Splicing and Copy-Move Image Tampering Detection. ICTACT Journal on Image and Video Processing, 11(4), 2447-2452.

19. Yang, J., Liang, Z., Gan, Y., &Zhong, J. (2021). A novel copy-move forgery detection algorithm via two-stage filtering. Digital Signal Processing, 113, 103032
20. Nath, S., &Naskar, R. (2021). Automated image splicing detection using deep CNN-learned features and ANN-based classifier. Signal, Image and Video Processing, 15(7), 1601-1608.
21. Abdalla, Y., Iqbal, M. T., &Shehata, M. (2019). Convolutional neural network for copy-move forgery detection. Symmetry, 11(10), 1280.
22. Geetha M, Pooja RC, Swetha J, Nivedha N, Daniya T (2020) Implementation of text recognition and text extraction on formatted bills using deep learning. Int J Contrl Automat 13(2):646–665
23. Santhosh Kumar B, Daniya T, Ajayan J (2020) Breast cancer prediction using machine learning algorithms. Int J AdvSciTechnol 29(3).