iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52367

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Image Forgery Detection Using Deep Learning

Boda Nithin Kumar[1], Mukkerla Manovikas[2], Daggula Syanthan[3], Miryala RamaKrishna[4]
[1, 2, 3]*B.Tech Scholars, Dept. of Computer Science and Engineering Hyderabad-501301, India*
[4]*Assistant Professor, Dept. of Computer Science and Engineering, SNIST, Hyderabad-501301, India*

Abstract: ***In recent years, with the prevalence of cameras, taking pictures has become more and more popular. Images are essential to our daily life as they contain a wealth of information and often need to be enhanced to obtain additional information. Various tools are available to improve image quality. Nevertheless, they are also commonly used for fake images, leading to the spread of misinformation. This has increased the severity and frequency of image forgery, a major concern today. Many traditional techniques have been developed over time to detect fake images. Convolutional Neural Networks (CNNs) have gained a lot of attention in recent years, and CNNs are also influencing the field of image forgery detection. However, most image forgery techniques that exist in the CNN-based literature are limited to detecting specific types of forgery (image splicing or copy-transfer). Therefore, there is a need for techniques that can efficiently and accurately detect the presence of invisible counterfeits in images. In this article, we present a robust deep learning-based system (CNN) that uses mantra-net to identify image fakes. ManTraNet is end-to-end convolutional neural network consisting of two sub-networks. One for extracting features associated with tamper evidence and the other for detecting local anomalies between features. A graphical user interface (GUI) was created for detecting digitally processed images. The method has an accuracy of 96.4% and has been proven to be efficient and practical.***

I. INTRODUCTION

Advances in image editing software and the prevalence of edited images on the Internet have made algorithms for detecting tampered photos increasingly important. Manipulating images today is easy and can have serious consequences. Initially, image forgery was detected primarily through manual methods targeting specific traces left by image signal processing pipelines. Recently, the advent of deep learning has introduced convolutional neural networks (CNNs) into image forensics. It can be trained on the original image to recognize if two patches are from the same image or treated in a different way that indicates a forgery. Several networks have been introduced to improve the analysis of specific points be demosicing Artifacts. ManTraNet, considered here, is the pioneer of his third category of methods that directly train on fake images to identify fake regions. The ability of methods like ManTraNet to deliver excellent results on benchmark datasets has already been demonstrated. However, on such a dataset, similar to the evaluation set, neural networks can be trained on images and tampering. One might wonder whether such a feat would hold up in the wild, where the images are diverse and so different from the controlled environment of the training dataset. Furthermore, the interpretability of the results may be questioned. Such results often appear opaque because the reason for the detection is not immediately apparent. After a brief introduction to ManTraNet, we analyze the results on different images to question its performance in uncontrolled scenarios.

II. RELEATED WORK

In this article, we present a new method for detecting fake images based on a deep learning technique that uses convolutional neural networks (CNNs) to automatically learn a hierarchical representation from input RGB colors picture. The proposed CNN is specifically designed for image splicing and copy motion detection applications. Than that In contrast to the random strategy, the weights in the first layer of the network are initialized with a basic high pass filter set. It is used in Spatial Rich Model (SRM) to compute residual maps and acts as a regularizer for efficient suppression. Capture the impact of image content and subtle artifacts introduced by manipulation processes. Experimental Results from several public datasets show that the proposed CNN-based model outperforms some prior art methods

III. PROPOSED WORK

A. ManTraNet

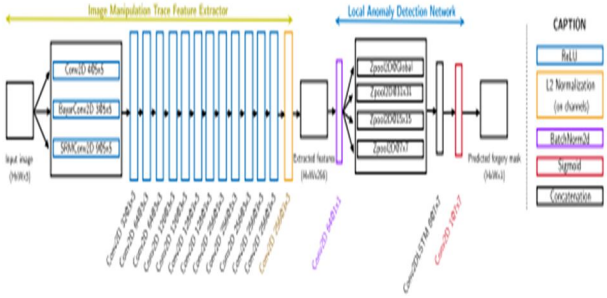
A unified deep neural architecture called ManTraNet to combat real-world image forgery, which typically involves various kinds and combined operations. Unlike many existing solutions, ManTra-Net is an end-to-end network, performing both detection and

©IJRASET: All Rights are Reserved

localization without additional pre- and post-processing. ManTra-Net is a fully convolutional network that handles images of any size and many known types of forgery such as splicing, copy-moving, deleting, enhancing, and even unknown types. This paper has three excellent contributions of his. We design a simple but effective self-supervised learning task to learn robust image manipulation traces from a classification of 385 image manipulation types. Furthermore, we formulate the fake localization problem as a local anomaly detection problem, design a z-score function that captures local anomalies, and propose a new long-short-term memory solution for evaluating local anomalies. Finally, we carefully perform ablation experiments to systematically optimize the proposed network design. Our extensive experimental results demonstrate the generalizability, robustness and superiority of ManTra-Net not only in individual types of manipulation/counterfeiting but also in complex combinations of them.

B. Network Architecture

ManTraNet is end-to-end CNN and its architecture is shown in Figure 1. input is color photograph. The output is a single-channel heatmap with floating (or integer) values between 0 and 1. between 0 and 255), representing the confidence of each position after saving the result as an image .Belongs to the forging region. Values close to 1 (or 255) correspond to areas where ManTraNet resides.Values close to 0 correspond to areas considered pristine, but very confidently forged.



The network itself consists of two sub-networks. The first subnetwork aims to extract manipulation traces from images and follows the VGG [36] architecture. takes an image as input,outputs 256 trait maps of the same size representing traits associated with different types of operations. The first layer consists of 16 5×5 convolutions for extracting initial features from the image. Four of these folds are conventional folds and nine are style-based realignment modules (SRMs).The remaining three are Bayar constrained convolutions. 16 functions linked A 3 × 3 convolutional layer follows. 32 functional channels on 1 level, 64 on 2 in order channels, 4 for 128 channels, 6 for 256 channels. The output of the last layer is used as Extracted features. All folds are followed by ReLU activations, except for the last layer. processed with L2 normalization. The second subnetwork takes the feature map as input and outputs a single channel map representing the confidence of each forged location. First put together 256 feature cards It was then fitted to 64 maps using a pointwise convolutional layer followed by stack normalization. For each feature map, ManTraNet computes the deviation of each pixel from the main feature. This map. If F is a feature map, the globally dominant feature μ−1 is thaverage of all values of F.

C. Training

Here we describe the training of the network in the original work. We focus on analyzing the results Please do not reproduce the training yourself as no training details were provided this paper is still in progress. The first subnet is trained in the Dresden Image Database [16] from the original images. out of all 80% of the images are used for training, 10% for validation and the remaining 10% for testing. Picture 256 × 256 patches are divided into uniform patches below the intensity standard deviation. 32/255 were rejected. A total of 1.25 million patches are retained. Samples are generated by uniform random patches and manipulations, apply manipulations to images and crop random patches 128x128 output area. The network is fed with a trimmed operating area, It is trained to recognize which operations have been used. For additional training modules, please visit it is not included in the original paper. A second sub-network is trained on his four synthetic datasets: Dataset synthesized from [37], [38] We use OpenCV [9] to color the image of Dresden [16] and another data set taken locally. Apply random operations to the same image. Training is done on 256x256 patches. Both networks were trained using Adam [19] with a batch size of 64 and 1000 batches per epoch. Optimizer with initial learning rate 10−4 and no decay. The learning rate is halved if: Validation loss does not improve over 20 epochs. The epoch with the best validation loss is final model.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

D. Detection of Forgeries

We show the ManTraNet response to forged images from the Korus dataset [21, 22]. First of all, ManTraNet is very responsive to many fakes and helps them out. recognition. That said, his ManTraNet reaction to these fakes is the same as his. Convert to a pure image like Figure 2. It's difficult because you're only given the output of ManTraNet. To distinguish between real fakes and false positives, even for a trained eye. Worse, the checked images correspond to controlled forgeries from the dataset. In the real world, images often undergo a lot of post-processing and editing, which can compromise their impact. Fakes are different or more difficult to detect than closer benchmark datasets the person the method was trained on. In Figure 4, ManTraNet actually unable to detect most of the real fake cases tested.

IV. ALGORITHM

A. CNN Algorithm Steps

1) *Convolutional Layer:* The Convolutional Layer is her first ConvLayer responsible for low-level capture.Features such as edge, color, and gradient placement. As you add layers, the architecture adapts to higher-level functionality
2) *ReLu Layer:* That activation function is responsible for transforming the summed weighted input the node for this input or output activation node.
3) *Pooling Layer:* A pooling layer serves to reduce the spatial size of the convolutional function.
4) *Fully Connected Layer:* Adding a fully connected layer is (usually) a cheap way to learn nonlinear a combination of high-level features represented by the output of a convolutional layer. A Fully Connected layer probably learns a nonlinear function. Convolutional Neural Network (ConvNet/CNN) is a deep learning algorithm that can take input images and assign importance (learnable weights and prejudices about different aspects/objects of the photo) and how to distinguish them from each other. ConvNet requires much less preprocessing compared to other classification algorithms. while in filters using primitive methods are developed manually with extensive training, and ConvNets have the ability to learn these Filter/Properties .

V. ADVANTAGE

1) One of the main advantages of image**s** is the wide availability of powerful digital imaging tools.
2) The advantage of using these functions is that they are rotation invariant and simple**.** 3. Superior efficiency and precision**.**

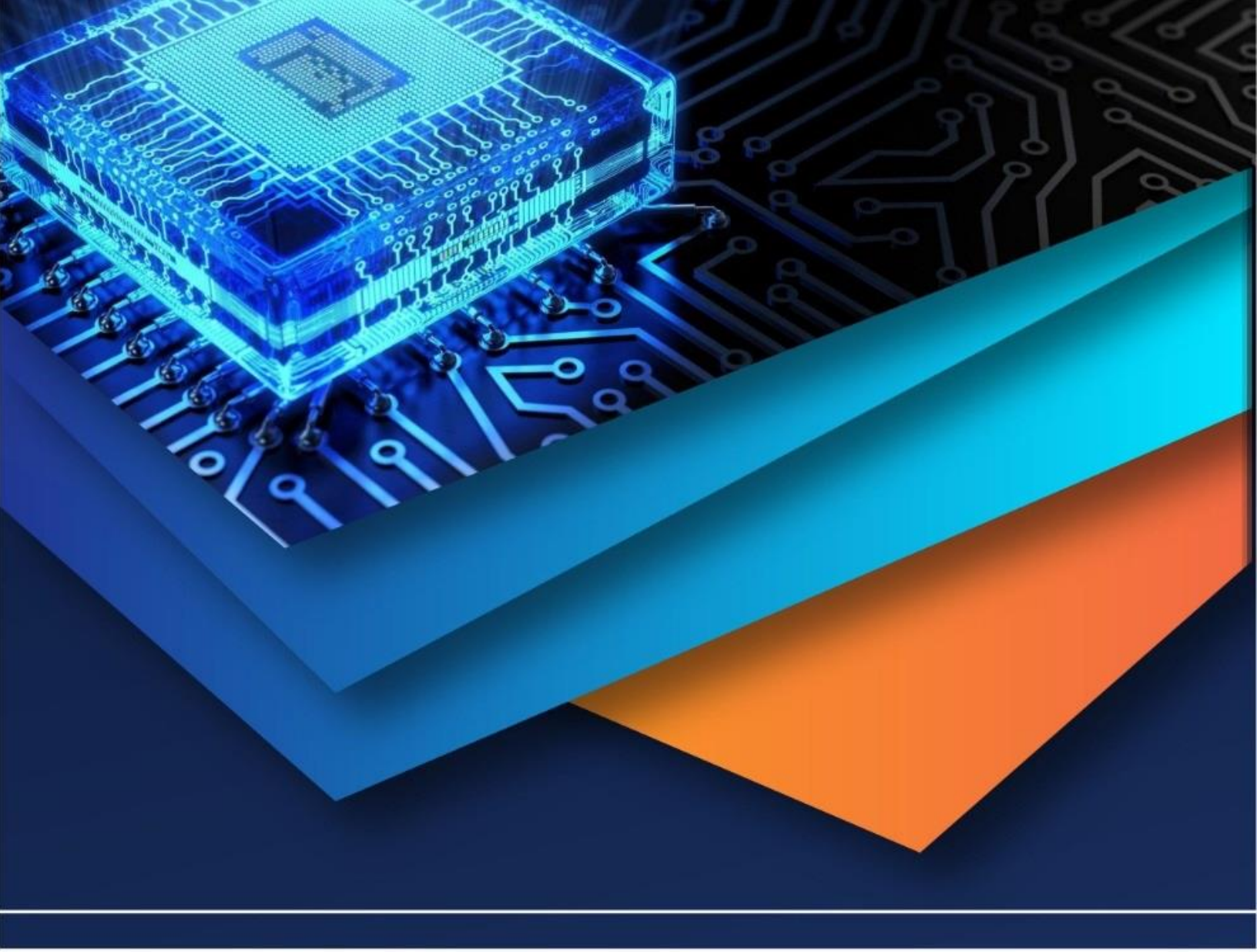
VI. CONCLUSION

In this paper, we analyzed the application of a CNN for image forgery detection as well as anomaly region identification. We introduce a end-to-end solution to image forgery localization called mantra-net. A total of 385 different types of image forgeries can be detected using this model, including forgeries of complex nature such as DNN aided image forgeries. Furthermore, we developed a web application interface for interacting with the model in an easy and effective manner.

REFERENCES

[1] NIST manipulation evaluation dataset, 2016, [online] available: https://www.Nist.Gov/itl/iad/mignimble-challenge-2017-evaluation CASIA tampered image detection evaluation dataset, 2012. Forensics.Idealtest.Org/casiav2.
[2] Nist manipulation evaluation dataset, 2016. Https://www.Nist.Gov/itl/iad/mig/ nimble-challenge-2017-evaluation.
[3] B. Bayar and M. C. Stamm, constrained convolutional neural networks: A new approach towards general purpose image manipulation detection, in: IEEE transactions on information forensics and security, vol. 13, no. 11, nov 2018, pages 2691-2706
[4] [19] p. Ferrara, T. Bianchi, A. De rosa and A. Piva, image forgery localization via fine-grained analysis of cfa artifacts (2012), in: IEEE transactions on information forensics and security, vol. 7, no. 5, pages 1566-1577

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)