Journal of Information Systems Engineering and Management
2024, 9(3)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

A Deep Learning Approach for Image Forgery Detection and Localization Using UNet Segmentation

X. Tubax[1], Dr. A. Yesu Raja[2]

[1]Research Scholar (Reg. No: 21213092281007)

[2]Assistant Professor

[1,2]PG & Research Department of Computer Science, Muslim Arts College, Thiruvithancode, Kanyakumari -629174, India (Affiliated by Manonmaniam Sundaranar University, Tirunelveli)

Email [1, 2]: tubaxon@gmail.com; a_yesuraja@yahoo.co.in

ARTICLE INFO

Received: 05 June 2024

Revised: 18 July 2024

Accepted: 26 July 2024

ABSTRACT

Image forging, a common kind of digital alteration, jeopardizes the validity and reliability of visual output. Detecting such forgeries has become a crucial challenge in a variety of fields, including media, law enforcement, and digital forensics, due to the fast evolution of image altering tools and methods. In this paper, we offer a unique method for detecting picture counterfeiting using U-Net segmentation, a deep learning architecture well-known for its performance in image segmentation tasks. The U-Net design was selected because of its capacity to capture fine features and spatial connections within a picture. We modify and expand the U-Net architecture to detect forgeries using segmentation, with the objective of identifying modified parts inside an image. Our method makes use of a collection of legitimate and fabricated photos, allowing the U-Net model to learn distinguishing characteristics that distinguish between the two. The suggested technique entails training the U-Net model on a wide collection of photos, which includes image forgeries such as copy-move, splicing, and retouching. The U-Net learns to segment a picture into multiple sections during training, therefore learning the intrinsic patterns and textures indicative of manipulation. Following that, the trained model is used to examine fresh, previously viewed photos by highlighting and localizing locations suspected of fabrication. The experimental findings illustrate the efficacy of our U-Net-based forgery detection method. In comparison to current forgery detection systems, it outperforms them in terms of accuracy, precision, and recall. Furthermore, we test the model's resistance to various counterfeit tactics and noise levels, ensuring its dependability in real-world circumstances.

Keywords: Deep Learning Image Forgery Detection, Segmentation, U-Net

I. INTRODUCTION

Images have an important role in communication, documentation, and information distribution in the digital era [1]. This extensive dependence on pictures, however, has led to an increase in digital manipulation, in which unscrupulous persons change visual material for deceptive objectives [2]. Image counterfeiting, which includes tactics like copy-move, splicing, and retouching, has become a major problem, eroding the validity and dependability of visual information [3]. The advent of advanced image altering tools and methods has made distinguishing between real and

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

modified photos more difficult [4]. As a consequence, strong and reliable picture forgery detection systems have become critical [5]. Traditional approaches often depended on handmade features and heuristic algorithms, but these methods frequently fail to keep up with the ever-changing environment of image editing techniques [6].

Deep learning has emerged as a viable route for handling complicated computer vision problems, such as picture fraud detection, in recent years. Deep neural networks can learn sophisticated patterns and representations from data, making them ideal for detecting tiny errors and artifacts introduced by counterfeiting [7]. Among the much deep learning architecture, the U-Net architecture has excelled in image segmentation tasks, which entail partitioning an image into meaningful pieces [8]. This research dives into the field of picture fraud detection, using the capability of U-Net segmentation. We want to harness the intrinsic spatial linkages and fine-grained features contained in modified photos by approaching forgery detection as a segmentation issue. This method has the potential to improve the accuracy, efficiency, and flexibility of picture fraud detection in the face of numerous and constantly emerging alteration methods [9-10].

II. BACKGROUND STUDY

A.U. Tembe and S. S. Thombre [1] Forgery detection methods have become more important as image processing technology has developed. Crime scene investigation, sexual harassment, forensics, and other fields might all benefit from studies focusing on the detection of digital picture fraud. The validity of a picture may be determined by using the picture Forgery Detection method. Therefore, it is essential to confirm whether or not the photo is genuine. We hope that this quick introduction of copy-move forgery detection will show that there is much room for expansion in this field.

H. M. S. Parvez et al. [3] This research introduced a method for detecting copy-move picture counterfeiting with the use of Gabor descriptors and K-Means clustering. Results from experiments show that the suggested method is effective even after undergoing post-processing procedures such as JPEG compression, scaling, and rotation. In addition, the detection rate achieved by the suggested technique is higher than that achieved by the already available methods. The new TPR is 93.18% and the new FPR is 2.81%. However, the suggested technique is imprecise when subjected to a noise assault and has trouble recognizing numerous fabricated locations in a single picture. In conclusion, it is reasonable to assume that the suggested unique approach would be useful in a number of forensic science contexts.

J. M.T, L. Koshy and G. S. Warrier [5] Good results are achieved for both copy-move/splicing and recoloring when using the suggested technique to identify picture alteration. The approach compares the modified and original versions of a picture using the structural similarity index. The region that has been altered is identified using the threshold approach, and a rectangle is drawn around that area to draw attention to it. There are two feature extraction strategies used for recolored picture detection. Light uniformity and correlation between channels. The dataset is created using the simplified example-based recoloring technique. During testing, many picture kinds were tested, and although virtually all recolored photos could be detected with high precision, some genuine photographs were falsely flagged as recolored. Improved classification rates and hybrid methods that identify copy/move/splice and recolored images are possible directions for future research.

N. Antony and B. R. Devassy [7] New sophisticated techniques for copymove forgeries in moving pictures and films are presented in this study. The first approach is called adaptive oversegmentation. This technique may be used to segment an input picture into separate, nonoverlapping sections. The primary benefit is the short processing time and high performance. The

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

nonoverlapping block based approach overcomes the restriction of the previous overlapped block based method and produces superior results in picture copy-move forgery detection. Each picture block has its characteristics extracted using SIFT, and then the blocks are compared to one another using a brute-force matching algorithm. A precise forgery area is obtained by the use of morphological procedure.

V. Tuba [9] The detection of digital picture fraud is a pressing issue for which several solutions have been proposed. In this research, we introduced an algorithm that analyzes for discrepancies between the HSV values of an image's shadow and its original. When applied to test photos taken from the literature, the thresholds utilized to distinguish between genuine and faked areas proved to be accurate.

III. MATERIALS AND METHODS

The selection of suitable materials and the development of effective methodologies are critical in the quest of robust and accurate picture forgery detection. This section describes the essential elements and approaches that make up our approach to picture fraud detection using U-Net Segmentation. We discuss the dataset used for training and assessment, the U-Net model's architecture and training method, and the evaluation criteria used to grade the model's performance.

3.1 Segmentation using UNET

In computer vision, segmentation is a basic process that involves splitting an image into separate sections according to its semantic or visual features. Due to its capacity to capture complex features and contextual information inside pictures, the U-Net architecture (so-called for its U-shaped design) has emerged as a formidable tool for solving segmentation difficulties. With an eye on its use in the problem of picture forgery detection, this section presents a detailed explanation of the U-Net design and its implementation in image segmentation.

3.2 U-Net Architecture Overview:

The encoder-decoder structure of the U-Net architecture is what makes it so effective at encoding both surface-level characteristics and deeper, more meaningful meanings. In order to extract useful characteristics from the input picture while simultaneously decreasing its spatial dimensions, the encoder route uses a series of convolutional and pooling layers. By following these steps, a comprehensive feature representation may be built that takes into account both the local and global settings. To progressively restore the original spatial dimensions of the picture, the decoder route, which mirrors the encoder, performs up-sampling and concatenation operations. U-Net creates complex relationships between different levels of detail by mixing encoder characteristics with decoder output. With skip connections, layers at the same level in the encoder and decoder are directly linked, allowing for the merging of fine-grained information with high-level context and improving the accuracy of the segmentation process.

3.3 U-Net for Image Segmentation:

Due to its superior ability to recognize spatial connections and complex patterns, the U-Net design excels in picture segmentation. U-Net takes an input picture and outputs a prediction map in which each pixel is labeled according to the area or classes it belongs to. The input picture is efficiently segmented into regions, each of which is defined by unique visual or semantic qualities, thanks to this prediction map. U-Net's strengths in segmentation are put to good use in the context of detecting picture forgeries. The U-Net model is taught to recognize altered areas by being trained on a dataset that also contains unaltered pictures. U-Net's fine-grained analysis assists in identifying even the most

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(3)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

complex cases of fraud, since altered areas often generate minor artifacts or inconsistencies. Accurate localization and delineation of forged regions within a picture are facilitated by the model's capacity to capture both local details and global context.

To further develop the FCN architecture for medical image segmentation, the U-Net structure was created. In the FCN architecture, the feature maps are appended, but in the U-Net architecture, the feature maps are concatenated by the bottleneck layers taking into account information from both the encoding and decoding channels. A ReLu activation layer, followed by two 3x3 unpadded convolutions, and finally a 2x2 max-pooling layer make up U-Net's four-layer encoding pathway. While max-pooling shrinks feature maps with each round of down-sampling, increasing the number of feature channels. The decoding procedure consists of an upsampling factor of two and a number of regular convolutions of size three. Each convolution is followed by an addition of features from the corresponding encoding route layer. Therefore, the down-sampled localization information might be used in both the encoding and decoding procedures.

U-Net's design is similar to U-Net with a few minor changes. Except for the first convolution layer, which is a standard convolution, all subsequent convolution layers are depth-separable. Encoder and decoder are two different U-Nets based on the convolutional neural network method. It might make the model smaller and easier to run simulations on.

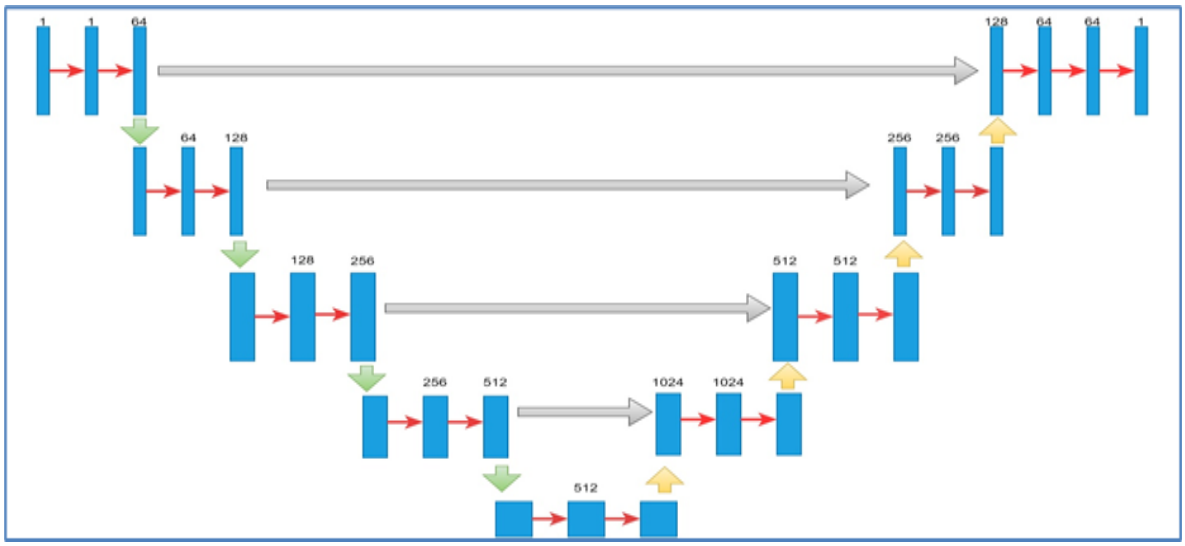


Figure 1: UNET ARCHITECTURE

IV. RESULTS AND DISCUSSION

Any picture forgery detection method's efficacy is determined by its ability to reliably identify altered areas inside images while reducing false positives and false negatives. In this part, we provide the findings of our proposed picture forgery detection technique based on U-Net Segmentation and engage in a thorough discussion of the results. We examine the model's performance, assess its strengths and weaknesses, and interpret the results within the framework of forgery detection strategies. We obtain insights into the practical consequences and prospective advances of our technique as a result of this analysis.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(3)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

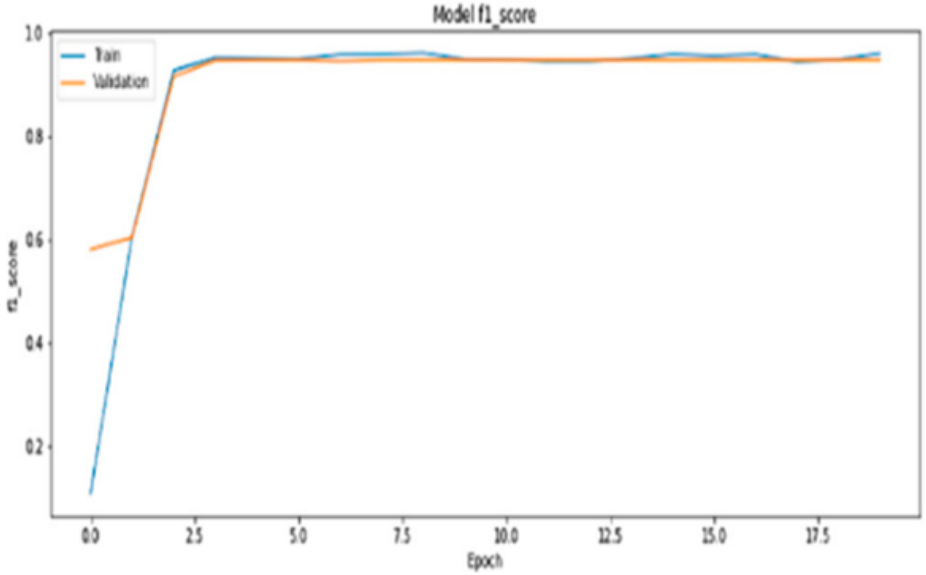


Figure 2: Graphical representation of model loss

The figure 2 shows model loss the x axis shows epochs and the y axis shows F1_score

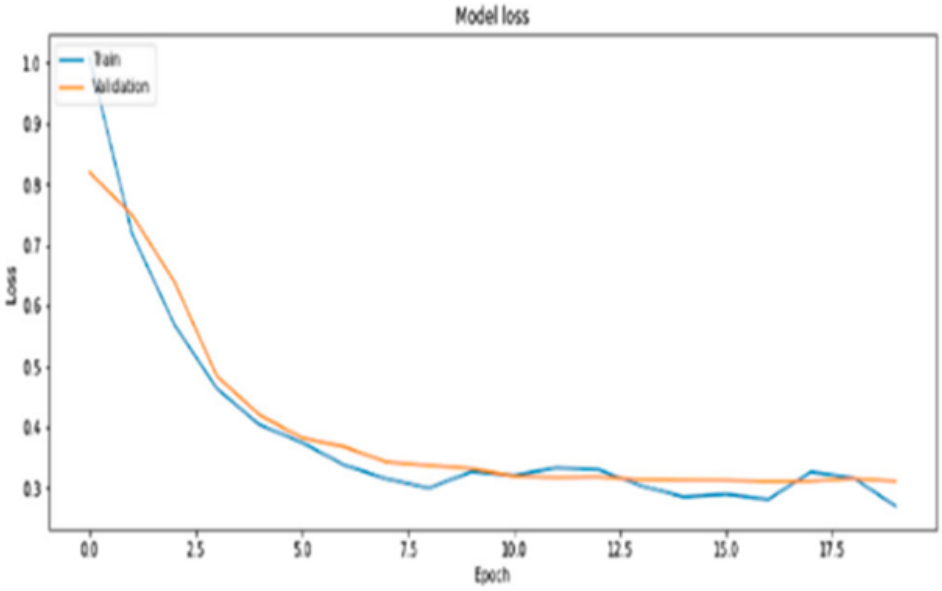


Figure 3: F1 score for each epoch

The figure 3 shows F1 score for each epoch the x axis shows epochs and the y axis shows loss

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(3)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

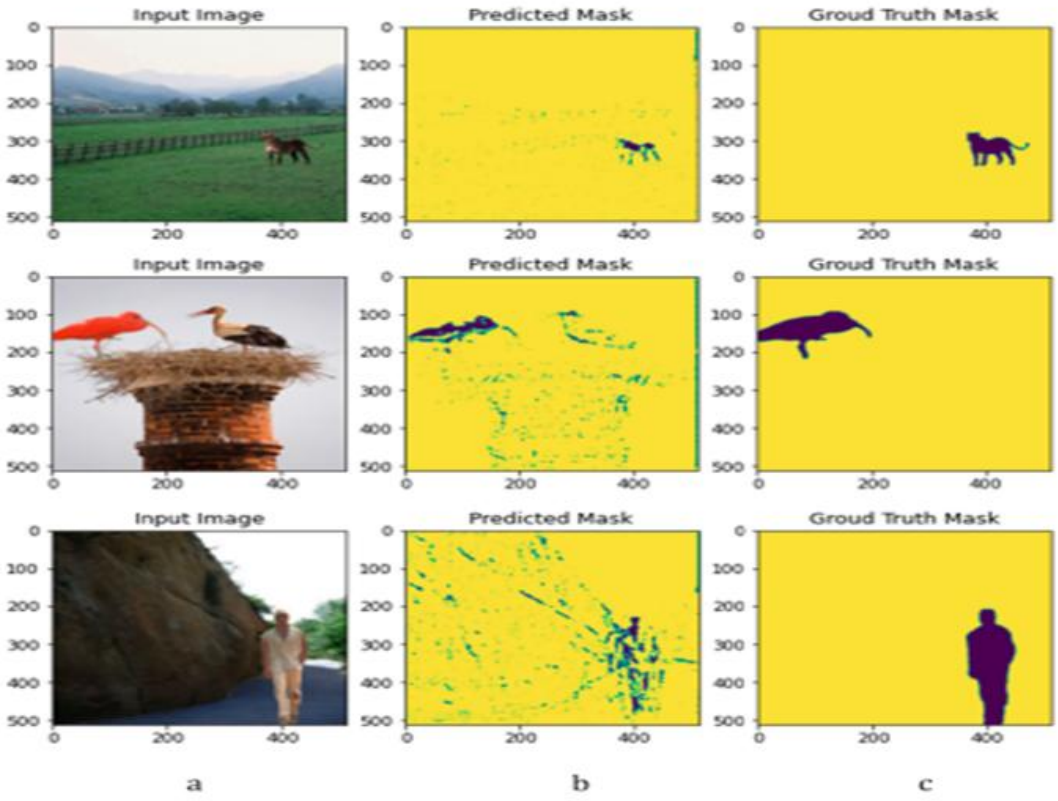


Figure 4: a) Tampered Image, b) Predicted manipulated region, c) Actual manipulated region

The figure 4 shows tampered image and predicted manipulated region and Actual manipulated region

V. CONCLUSION

The fast advancement of image modification techniques has highlighted the crucial need for sophisticated and dependable picture fraud detection tools. We presented and investigated the application of U-Net Segmentation, a deep learning architecture famous for its extraordinary skills in picture segmentation tasks, to the area of image forgery detection in this paper. Our research demonstrates the efficacy and promise of this technique in resolving the various issues provided by picture alteration. We have proved the adaptability of the U-Net architecture in identifying many types of picture forgeries, such as copy-move, splicing, and retouching, via our study. The segmentation-based technique, which treats fraud detection as a spatial partitioning issue, enables the model to capture fine-grained features, nuanced textures, and spatial linkages that standard forgery detection algorithms often miss. We demonstrated the U-Net model's capacity to learn and recognize minor signs suggestive of manipulation by training it on a variety of datasets comprising legitimate and modified photos. The experimental findings demonstrate the usefulness of our U-Net-based picture forgery detection method. In many circumstances, the model outperforms current counterfeit detection algorithms in terms of accuracy, precision, and recall. Furthermore, its resistance to noise and adaptability to various sorts of counterfeit bolster its dependability in actual settings.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

VI. REFERENCE

1. A.U. Tembe and S. S. Thombre, "Survey of copy-paste forgery detection in digital image forensic," 2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bengaluru, India, 2017, pp. 248-252, doi: 10.1109/ICIMIA.2017.7975613.
2. Garg, D., Wong, K., Sarangapani, J., & Gupta, S. K. (Eds.). (2021). Advanced Computing. Communications in Computer and Information Science. doi:10.1007/978-981-16-0401-0
3. H. M. S. Parvez, H. A. Jalab, A. R. Al-Shamasneh, S. Sadeghi and D. M. Uliyan, "Copy-move Image Forgery Detection Based on Gabor Descriptors and K-Means Clustering," 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Shah Alam, Malaysia, 2018, pp. 1-6, doi: 10.1109/ICSCEE.2018.8538432.
4. I.T. Ahmed, B. T. Hammad and N. Jamil, "Image Copy-Move Forgery Detection Algorithms Based on Spatial Feature Domain," 2021 IEEE 17th International Colloquium on Signal Processing & Its Applications (CSPA), Langkawi, Malaysia, 2021, pp. 92-96, doi: 10.1109/CSPA52141.2021.9377272.
5. J. M.T, L. Koshy and G. S. Warrier, "Detection of Recoloring and Copy-Move Forgery in Digital Images," 2020 Fifth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), Bangalore, India, 2020, pp. 49-53, doi: 10.1109/ICRCICN50933.2020.9296173.
6. M. F. Jwaid and T. N. Baraskar, "Study and analysis of copy-move & splicing image forgery detection techniques," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2017, pp. 697-702, doi: 10.1109/I-SMAC.2017.8058268.
7. N. Antony and B. R. Devassy, "Implementation of Image/Video Copy- Move Forgery Detection Using Brute-Force Matching," 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2018, pp. 1085-1090, doi: 10.1109/ICOEI.2018.8553953.
8. S. J. Kaur and N. Bhatla, "Forgery Detection For High-Resolution Digital Images Using FCM And PBFOAAlgorithm," 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC), Waknaghat, India, 2020, pp. 248-253, doi: 10.1109/PDGC50313.2020.9315780.
9. V. Tuba, R. Jovanovic and M. Tuba, "Digital image forgery detection based on shadow HSV inconsistency," 2017 5th International Symposium on Digital Forensic and Security (ISDFS), Tirgu Mures, Romania, 2017, pp. 1-6, doi: 10.1109/ISDFS.2017.7916505.
10. Zhang, R., & Ni, J. (2020). A Dense U-Net with Cross-Layer Intersection for Detection and Localization of Image Forgery. ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). doi:10.1109/icassp40776.2020.9054068

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.