Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Enhanced Visual Media Transparency Through Advanced Image Forgery Detection Techniques

Rayaprolu Aswini[1], C Dastagiraiah[2]

[1]M.Tech, Department of CSE, Anurag University, Hyderabad, Telangana, India, aswini.rayaprolu123@gmail.com
[2]Assistant Professor, Department of CSE, Anurag University, Hyderabad, Telangana, India dastagiraiah.cse@anurag.edu.in

In recent years, a great deal of doctored and altered photos have been created and disseminated through the Internet and media because of the accessibility and simplicity of image manipulation. Several methods have been suggested for determining whether an image is genuine and, in certain instances, for identifying where the image has been manipulated or fabricated. This study provides a comprehensive overview of current image forgery detection systems that utilize Deep Learning (DL), focusing on techniques that may detect copy-move and splicing attacks. In the same vein as splicing, the image-targeting uses of DeepFake-generated content are also examined. This survey couldn't come at a better moment, as deep learning-powered techniques are currently dominating the market, delivering top-notch results across all benchmark datasets. The methods are described along with the datasets used for training and validation, and we go over their main features. Their performance is also examined and compared (to the best of our ability). Our discussion of potential avenues for further study in the areas of deep learning architecture and evaluation, as well as dataset construction for straightforward technique comparison, builds upon this work.

Keywords: Deep Learning, Image forgery detection, Digital images.

1. Introduction

Digital images are an integral aspect of many modern-day disciplines, including scientific study, medical imaging, diplomatic justice, and news reporting. The general public takes pictures with the expectation that these digital images will faithfully capture actual events as they unfold in the actual world. But as picture processing and multimedia technologies advance, processing digital photographs becomes easier. A major crisis of trust will ensue as a consequence of the hidden risks associated with image security, which will surely have detrimental impacts on society as a whole. The "bear riding image" was widely distributed online in 2018, and Russian President Vladimir Putin formally commented to it in an interview with NBC: If you look at Figure 1 on the left, you can see that Putin altered the real horse image on the right to make it look like he's riding a bear. The ability to alter images in order

to convey incorrect information has grown increasingly subtle and even fabricated as technology has progressed. For this reason, it is crucial that sectors where digital images are used extensively, such news media, forensics, security detection and others, improve their ability to determine if an image is real and promptly identify any signs of digital image manipulation.

Figure 1. Untrue and actual images of "Putin riding a bear"

According to [1] Following deep learning's success in computer vision, an increasing number of researchers have sought to apply the technique to picture forensics since 2016 [2-4]. But there are major differences when compared to the typical computer vision tasks: 1) The goal of identification is different; in image forensics, the model must be able to spot the reformed area of the image. 2) The statistical traits are distinct: when doing picture forensics, it is crucial to pay close attention to the minute alterations linked to the boundary of tampering. 3. Post-processing has different effects; specifically, post-processing image cleaning technology is awful at masking manipulation artifacts.

So far, forensic tools have been greatly improved by the abundance of deep learning-based picture forgery detection algorithms that have emerged.

There are primarily two tasks in digital picture forensics that rely on deep learning [5]: 1) Detecting methods of tampering: It is important to determine the methods used to manipulate image material, which can include splicing, copying and relocating, computer-generated, and multiple 2) Finding the manipulated area: Finding the manipulated area in the fake image is essential. You can export the material in two ways: either as a bounding box or as a binary mask.

While there are a few prior evaluations on digital forensics [6-8], our paper's classification viewpoint and emphasis are significantly different: 1) The study skips over a number of forensic techniques, such as picture traceability forensics and image tampering geolocation, in favor of concentrating on the issue of detecting tampered images. 2) Rather of putting a lot of effort into conventional tampering detection approaches, this research focuses on a deep learning-based approach. 3) This research is motivated by the need for tampering targets and aims to organize solutions for different tampering detection jobs rather than classifying deep network topologies.

2. Literature Review

A new approach to detecting picture forgeries was suggested in the paper [9]. This method does not involve the installation of digital watermarks in the photographs, nor does it involve the comparison of the images for the purposes of training and testing. It was claimed by the authors that the individual picture features that were extracted during the acquisition phase represent proof in and of themselves that the image is genuine. In many cases, these characteristics can be observed with the naked eye. In particular, it employs picture artifacts that are brought about by a variety of anomalies as markers in direction to ascertain the validity of the image. Also proposed a technique for detecting cases of picture alteration by means of a color filter array. It has the ability to compute a basic threshold-based classifier as well as a single feature. The researchers verified their methods using manipulated photos, CG graphics, and real images. The error rates were found to be low in the experimental examination.

Image forgery detection was the goal of a research survey in [10], which relied on deep learning approaches. The methods used to spot the reality of pictures on openly available databases were also analyzed.

In [11], the authors introduced a deep learning-based design for detecting copy or move image fraud using the end – to - end trainable technology BusterNet. The architecture that BusterNet employs is a two-branch architecture. The first subset aims to locate manipulable parts by analyzing visual artifacts, while the second subset uses visual similarities to locate copyable or movable parts. In order to train BusterNet efficiently, they recommended a step-by-step process and simple procedures for datasets unrelated to the study's subject. Their thorough research examination shown that compared to conventional copy/move algorithms, BusterNet performed far better. To evaluate the proposed architecture, the CASIA and CoMoFoD datasets were used.

The article [12] explored the significance of identifying instances of image manipulation by employing deep learning-based methods on datasets that are accessible to the general public, such as CASIA, UCID, MICC, and other similar datasets. They discussed the approach of passive picture forensic analysis and brought attention to the obstacles that lie ahead in the process of building a mechanism for the detection of images that have been altered.

In a different piece of research, [13] developed a novel IDF method that took a CNN as its foundation. One of the objectives of this method is to acquire an automatic understanding of how picture modification might be carried out. As input, the image-altering features that are formed after the contents of a picture are destroyed are utilized by the IDF technique that has been discussed. This approach disregards the visual and sensory aspects of the image in favor of studying the local operational linkage among pixels, as manipulation can alter some resident connections.

As a result, it is able to identify instances of forgeries inside an image.

For the purpose of identifying instances of digital image counterfeiting, a CNN-based architecture was proposed in a different research study [14]. It was proposed by them that the preprocessing stage is intimately connected with the primary layer of the CNN method. In this process, it looks for problems that arise as a result of manipulation. They used trial photos to

train the CNN model, while the support vector machine was employed to identify any alterations that were present.

An RRU-Net, which stands for ringed residual U-Net, was introduced in [15] for the purpose of detecting forgeries in picture slicing. They suggested an architecture that makes use of an end-to-end image segmentation link in order to detect instances of counterfeiting with increased accuracy. The RRU-Net study aimed to establish an approach that makes use of RRU-Nets and is capable of detecting manipulations without the need for pre- and post-processing. This was accomplished by utilizing human brain principles. Generally speaking, the human brain is responsible for systems that involve recollection and consolidation. As a result, the objective of this method is to maximize the capacity for learning of a CNN, which is modeled after the characteristics of the human brain. With their invention, which uses residual propagation to help a CNN remember its input feature information, they were able to overcome gradient deterioration. Because the response feature is combined with the remaining answer, it can distinguish between the actual and fake regions. In contrast to the traditional, state-of-the-art procedures, the experimental results showed that the suggested approach yielded better results. Another study used the steganalysis model to suggest a transfer learning-based methodology that benefits from prior knowledge. This study is referred to as [16]. When applied to the BOSSBase and BOW datasets, this approach yielded an average accuracy rate of 97.36 percent.

An approach that relies on transfer learning was introduced in [17]. This method utilizes the AlexNet methods pre-trained weights, which aids in training reduction. In this method, the support vector machine (SVM) serves as the classifier. The overall performance of the vehicle was satisfactory.

According to [18], a fully connected network with multitasking capabilities should be used. Given that the output of a standard single-task fully linked network is unpredictable, the suggested method outperformed it by a significant margin. In order to accomplish numerous jobs at once, the authors suggested a network with multiple output streams. In this case, the surface label will be acquired by one of these streams and the interface area's edge by the succeeding one.

The article [19] presented a novel method for the identification of picture splicing that makes use of an algorithm that is based on features. For the purpose of computing local features, this method makes use of the combination of images that occur together. Following that, the local features are utilized in order to retrieve the feature parameters. Combining the segmentation procedure with the expectation-maximization method allows for learning to take place. This is because there are ways in which spliced and host photos can look different.

3. Traditional Passive Forgery Detection Methods

A number passive, so-called "conventional" procedures for detecting image fraud have been proposed since the turn of the millennium, and we'll touch on them briefly here. This is by no means an all-inclusive or even thorough examination of these techniques; we acknowledge that. In order to conduct a more thorough evaluation. Commonly known as "classic" or

"traditional" methods, conventional passive ones draw on statistical, geometric, signal processing, and physics and statistics, among other disciplines. In reality, they date back to before the DL age in which we currently find ourselves, and as a result, they need very little data to carry out their training phase. Common examples of classic machine learning methods used by those that still need training data include clustering, SVMs, linear and logistic regression, random forests, and many more. We still classify those as standard methods in this case since they use models with a minimal number of parameters and don't necessitate a mountain of data for training. Both of these factors lead us to believe that a brief overview of some of the more conventional methods might be helpful:

1. The amount of data needed for training is usually minimal, if any at all, as indicated before. Naturally, this is helpful in cases when gathering a sufficient number of tagged photos to train a deep learning technique with a huge number of parameters is challenging or impossible. Most of these techniques also don't require as much processing power, making them ideal for use on commercially available, low-power devices like tablets and smartphones.

2. Deep learning models can also benefit from utilizing some of the fundamental ideas and principles upon which these approaches are based, either to hasten the training period or to improve performance. As an example, the output of a CNN is subjected to an SVM model as the last step of the classification process in reference [20]. This case uses a DCT transform and a YCbCr color space conversion as pre-processing steps prior to a CNN. A CNN takings the Laplacian filter residuals (LFR) that were calculated on the input images as input instead of the pictures themselves. is pixel-dependent.

These methods work on the premise that by producing anomalies, some alterations can alter the picture's statistical information right down to the pixel level.

These outliers can manifest in a variety of ways; some are spatial, some are frequency, and yet others are a mix of the two. It would be computationally difficult to investigate every potential combination of shape and size for copied portions because they can be of any size. But during copy-move attacks, it's communal to see a lot of overlap between the duplicated parts of the picture.

In [21], the Discrete Cosine Transform (DCT) is suggested by the writers as a possible approach. Specifically, a DCT was applied to each of the image's overlapping blocks. Each block was described using the DCT coefficients as a feature vector. After that, we grouped the most comparable DCT block coefficients and ordered them lexicographically to find duplicate regions. The second strategy suggested using a Principal Component Analysis (PCA) on the characteristics of picture blocks before comparing the blocks' representations in the resulting space with decreased dimensions. When little changes are made to the cloned regions, such as adding noise or using lossy compression, these methods remain stable. Geometric modifications, such as scaling or rotation, are typically beyond the capabilities of these approaches. Thus, let's think about a scenario where a geometric transformation is employed to bolster the credibility of a copy-move attack. Interpolation between nearby pixels is a typical component of geometric transformations; bilinear and cubic interpolation are the two most popular methods. A distinct correlation pattern is generated between these pixels by means of the selected approach. The next step is to use statistical approaches to identify these patterns,

which will help in locating areas that have been manipulated geometrically. In [22], we see an example of this method in action.

3.1 Format based

Digital camera photos are typically saved in JPEG format. In other words, the picture is subdivided into 8 × 8 pixel sections, which are subsequently subjected to DCT transformation and quantization. Therefore, near the boundary of adjacent blocks, certain artefacts are produced. Image modifications such as copy-move or splicing modify the JPEG artefact pattern. To approximation the JPEG quantization table, the authors of [23] suggested using a sample region (which is intended to be legitimate) of the target image. After that, we separated the picture into slabs and determined a "slab artefact" measure for each one. Manipulated blocks are identified when this metric's score considerably differs from the average value across the full image.

3.2 Camera based

All digital cameras produce images with their own unique "footprint" or "signature," and these techniques capitalize on this fact. This information might also be helpful when trying to identify the camera used to take a picture. The authors of [24] estimated the parameters of the previously stated PRNU using a series of images captured by a known camera. This term is camera specific and models the outcome of processing activities performed in-camera. The target image, which should have been captured using the same camera, is also used to extract these PRNU parameters, which are then compared with the ones that were calculated before. The basic premise is that the estimated parameters will be different if a merging operation using a diverse kind of camera has been performed.

3.3 Lighting based

It is usually difficult for an attacker to guarantee that the forgery's lighting is consistent with the surrounding image when they execute a copy-move or splicing operation. It can be challenging, even with expert software like Adobe Photoshop, to compensate for this effect. To prove authenticity, lighting (or physics) based methods first construct a worldwide lighting method using the mark image, and then look for local discrepancies.

3.4 Geometry based

The geometry-based approach takes advantage of the fact that when a 3D scene is copied or spliced, the resulting image often has some strange geometric qualities. The so-called main point is typically located close to the image's center, as noted by the authors of [25], who presented a method to estimate it by analyzing known planar objects. They also demonstrated that the principal point shifts when an item is translated in the picture plane, which can be used as proof of fraud.

In [26], an additional intriguing strategy was put out. The original concept was to use a perspective change to flatten down certain recognizable things, such license plates or billboard signage. Using a camera calibration, one can take measurements of the reference objects on a flat surface; these data can be used to determine whether or not the objects in the image are real.

4. Deep Learning Based Methods

In the last ten years, deep learning techniques have become increasingly popular and have found useful applications in solving a wide range of scientific challenges. Their exceptional performance in classification, regression, and segmentation issues is the main reason behind this. These algorithms can get better results than people on some jobs. Another important reason why deep learning techniques have become so popular is that, unlike traditional machine learning methods, they do not necessitate domain-specific expertise or the researcher to manually construct meaningful features to feed into the learning algorithm. Deep learning models such as Convolution Neural Networks (CNNs) can automatically extract descriptive features from the input data that capture qualities unique to a certain task.

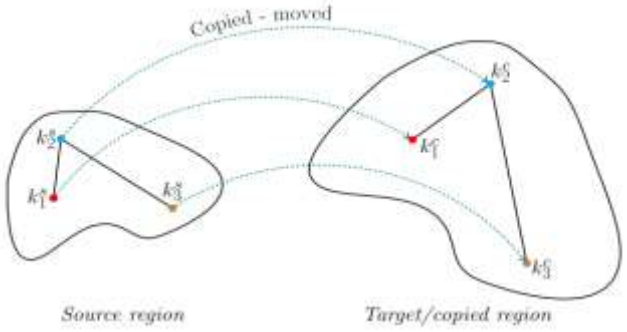

Figure 2. A matching technique based on classical features to identify copy-move manipulation.

Conventional, physics-based approaches to IFD problem solving were common prior to the broad use of DL in many domains. Discrete cosine transform (DCT) and discrete wavelet transform (DWT) [27] are examples of frequency domain conversion procedures that might be applied to the input images during preprocessing. Alternatively, YCbCr or another color space could be used. Using either block-based or keypoint-based approaches, a variety of picture characteristics were recovered. Producing identified heatmaps often involves the last steps of feature matching and filtering. Classical methods for copy-move picture recognition, as shown in Figure 2, involve feature matching by extracting SIFT keypoints from the source and target regions. Features generated by DL models outperform features created by humans in many computer vision tasks, especially when dealing with massive amounts of data [29]. To illustrate the current trend in this area of study, Figure 3 shows the history of prominent DL-based IFD methods along with their respective backbone networks.

Figure 3. The colourful circles represent the DL backbone networks that correlate to the DL-based IFD findings found in the literature.

A series of consecutive For splicing detection, CNN C2RNet was suggested in [30], which includes Coarse-CNN and Refined-CNN. The Coarse-CNN, which consists of 13-convolutional layers, 5-max pooling layers, and 2-fully connected layers, was trained with the input copy in order to identify potentially suspicious areas of coarse splicing by comparing the original and spliced versions of the image. To further improve the detected results, the Refined-CNN—which consists of 16-convolutional layers, 5-max pooling layers, and 3-fully connected layers—was fed the output feature map of the Coarse-CNN. In addition, the discovered splicing findings utilizing C2RNet were refined using post-processing operations such as morphological procedures, and convex-full filling. The convex-full filling approach may miss non-simply linked spliced regions, and the adaptive filter may not effectively eliminate falsely detected edges of real regions. In [31], the encoder-decoder network is built using SegNet. In this study, the latent representation was not derived from a single encoder-decoder but rather from the encoder's outputs in conjunction with the LSTM network that was taken from [32].

Long short-term memory, decoder-encoder, and skip connections are the 3-primary components of the image-splicing localization network suggested by [33]. This approach's LSTM component is comparable to what's found in [34] and [35]. This method's encoder-decoder differs from the one in [36] due to its inspiration from U-Net. A rectified linear unit (ReLU) served as the initiation function for the encoder component, which also had convolutional layers, max-pooling, and batch normalization. The encoder's residual blocks employed a combination of long and short skip connections to acquire The decoder received input from both the long short-term memory (LSTM), and the encoder, since this was a hybrid strategy.

5. Implementation

Visual media is essential for forming public opinion, spreading information, and influencing societal attitudes in the current digital era. However, the proliferation of sophisticated image editing tools and the rise of malicious image manipulation techniques pose significant challenges to the transparency and integrity of visual content. Image forgery, the act of varying images to deceive viewers or misrepresent reality, undermines the credibility of visual media and erodes public trust. To address these challenges, advancements in image forgery detection have become essential. This document presents an indication of the implementation of advancements in image forgery detection to enhance transparency in visual media. The implementation encompasses various stages, including data collection, preprocessing, analysis, augmentation, modelling, training, and evaluation. The implementation begins with data collection, where a diverse dataset comprising authentic and forged images is gathered. This dataset represents various types of manipulations and forgeries encountered in real-world scenarios. The collected data undergoes preprocessing, involving normalization, resizing, and noise reduction, to prepare it for analysis.

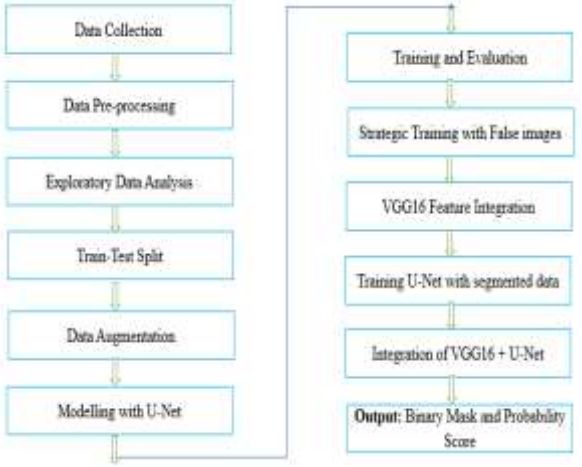

Figure 4. Flow of the System

5.1 Algorithm VGG-16

Input_image function VGG16: # Convolutional layers

Conv2D(activation='relu', padding='same', kernel_size=(3,3), filters=64)(image_input)

Conv2D(activation='relu', padding='same', kernel_size=(3,3), filters=64)

Pool_size=(2,2), strides=(2,2); MaxPooling2D

Conv2D(activation='relu', padding='same', kernel_size=(3,3), filters=128

Conv2D(activation='relu', padding='same', kernel_size=(3,3), filters=128

Pool_size=(2,2), strides=(2,2); MaxPooling2D

Conv2D(activation='relu', padding='same', kernel_size=(3,3), filters=256)

Conv2D(activation='relu', padding='same', kernel_size=(3,3), filters=256)

Conv2D(activation='relu', padding='same', kernel_size=(3,3), filters=256)

Pool_size=(2,2), strides=(2,2); MaxPooling2D

Conv2D(activation='relu', padding='same', kernel_size=(3,3), filters=512)

Conv2D(activation='relu', padding='same', kernel_size=(3,3), filters=512)

Conv2D(activation='relu', padding='same', kernel_size=(3,3), filters=512)

Pool_size=(2,2), strides=(2,2); MaxPooling2D

Conv2D(activation='relu', padding='same', kernel_size=(3,3), filters=512)

Conv2D(activation='relu', padding='same', kernel_size=(3,3), filters=512)

Conv2D(activation='relu', padding='same', kernel_size=(3,3), filters=512)

Pool_size=(2,2), strides=(2,2); MaxPooling2D

Flatten the layer and all of the linked layers.

Dense(units=4096, activation='relu') Flatten()

Dropout percentage (0.5)

Dense (activation='relu', units=4096)

Dropout percentage (0.5)

Dense(activation='softmax, units=num_classes)

revert output_logits

6. Results and Analysis

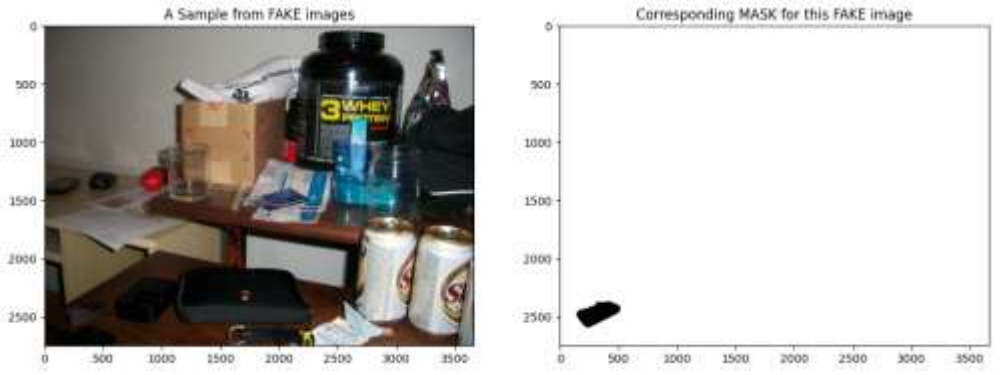

Figure 5. Random sample FAKE images and its corresponding MASK

After performing the process of exploratory data analysis, it displays the output in the form of MASK for the FAKE image which is shown in Figure 5.

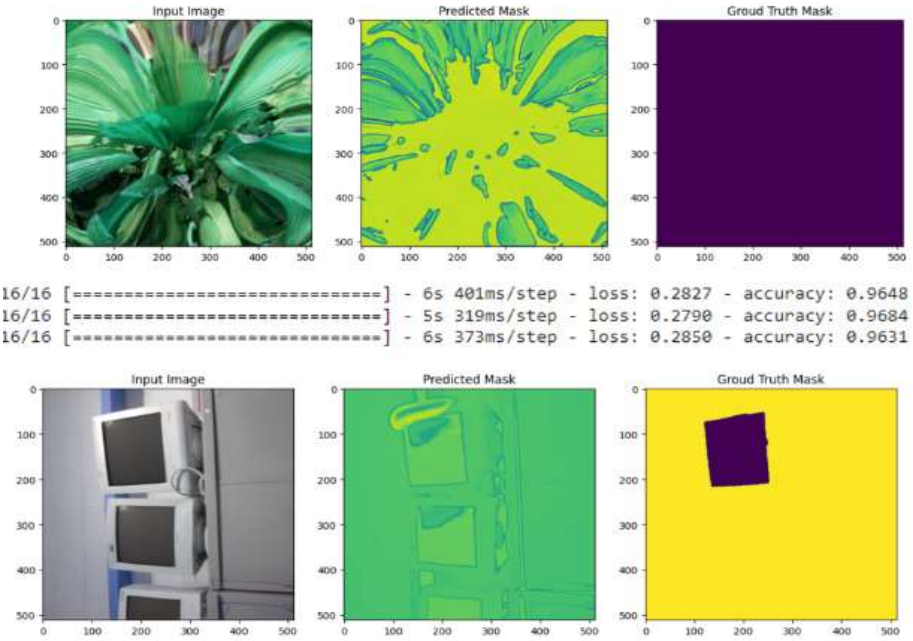

Figure 6. Input image, accuracy, its ground truth mask along with predicted mask

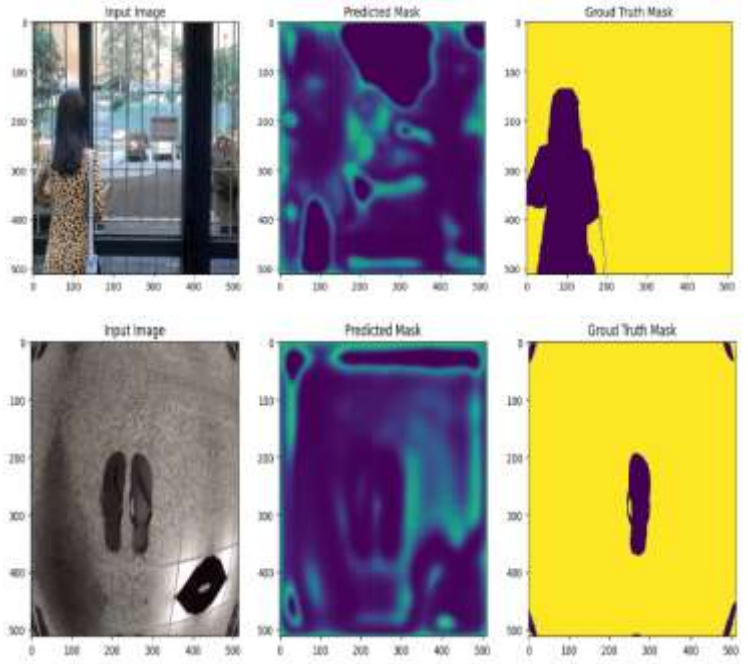

Figure 7: Input image, its ground truth mask along with predicted mask

Finally pass the corresponding MASK as input to Modelling and the Above Figure 6 and 7 prints the input image, its ground truth mask along with predicted mask as output after undergoing through the process of modelling, segmenting Train, Test and Validation splits with size = 128 using stride = 32.

7. Conclusion

This study delivers a concise overview of the deep learning-based approach to localizing picture forgeries. Our primary criterion for selecting these solutions is the network architecture they employ. There is a wide range of options for the creation of tamper location approaches for dissimilar specialized challenges due to the fact that dissimilar network topologies have their own features and advantages. The location of image forgeries is fraught with both possibilities and threats as deep learning technology continues to evolve. Along with addressing present concerns and potential future research areas, this article provides an overview of datasets and performance evaluation measures frequently utilized in picture forgery localization. Readers can better understand the current state of research regarding the location of picture forgeries because of this. In the future, we will keep researching ways to combat picture manipulation and forgery, and we will update our digital image forensics toolkit often to ensure the safety of multimedia files.

References

1. A. Krizhevsky, I. Sutskever and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," Commun. ACM, vol. 60, no. 6, pp. 84–90, 2017, (June 2017). https://doi.org/10.1145/3065386. [Google Scholar]
2. J. Bunk, "Detection and localization of image forgeries using resampling features and deep learning," in 2017 IEEE Conf. on Computer Vision and Pattern Recognition Workshops (CVPRW), pp. 1881–1889, 2017, https://doi.org/10.1109/CVPRW.2017.235. [Google Scholar]
3. N. Huang, J. He and N. Zhu, "A novel method for detecting image forgery based on convolutional neural network," in 2018 17th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications/12th IEEE Int. Conf. on Big Data Science and Engineering (TrustCom/BigDataSE), pp. 1702–1705, 2018, https://doi.org/10.1109/TrustCom/BigDataSE.2018.00255. [Google Scholar]
4. Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," in 2016 IEEE Int. Workshop on Information Forensics and Security (WIFS), pp. 1–6, 2016, https://doi.org/10.1109/WIFS.2016.7823911. [Google Scholar]
5. S. Walia and K. Kumar, "Digital image forgery detection: A systematic scrutiny," Australian Journal of Forensic Sciences, vol. 51, no. 5, pp. 488–526, 2019. [Google Scholar]
6. P. Korus, "Digital image integrity, A survey of protection, and verification techniques," Digital Signal Process Ing, vol. 71, pp. 126, 2017. [Google Scholar]
7. L. Verdoliva, "Media forensics and deep fakes: A no study on the influence of the temperature on the performance of the system," IEEE. Journal of Selected Topics in Signal. Processing, 2020, vol. 14, no. 5, pp. 910–932, 2020. [Google Scholar]
8. I. Castillo Camacho and K. Wang, "A comprehensive review of deep learning-based methods

for image forensics," Journal of Imaging, vol. 7, no. 4, pp. 69, 2021. [Google Scholar]
9. Varga, D. Multi-Pooled Inception Features for No-Reference Image Quality Assessment. Appl. Sci. 2020, 10, 2186.
10. Bai, X.; Yang, M.; Huang, T.; Dou, Z.; Yu, R.; Xu, Y. Deep-Person: Learning discriminative deep features for person Re-Identification. Pattern Recognit. 2020, 98, 107036
11. Manjunatha, S.; Patil, M.M. Deep learning-based Technique for Image Tamper Detection. In Proceedings of the 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 4–6 February 2021; pp. 1278–1285.
12. Corel Database. Available online: http://www.coreldraw.com/ (accessed on 4 August 2021).
13. Wang, X.; Wang, H.; Niu, S.; Zhang, J. Detection and localization of image forgeries using improved mask regional convolutional neural network. Math. Biosci. Eng. 2019, 16, 4581–4593
14. R. Y. Wang, B. L. Chu, Z. Yang, Zhou Linna, "A Review of Visual Depth Forgery Detection Technology," Chinese Journal of Image and Graphics, vol. 27, no. 1, pp. 43–62, 2022.
15. Z. J. Barad and M. M. Goswami, "Image forgery detection using deep learning: A survey," in 2020 6th Int. Conf. on Advanced Computing and Communication Systems (ICACCS), pp. 571–576, 2020, https://doi.org/10.1109/ICACCS48705.2020.9074408.
16. L. Haodong, Z. Peiyu and L. Bin, "A survey on deep learning based digital image tampering loculi," Journal of Signal Processing, vol. 5, no. 12, pp. 2278–2301, 2021, https://doi.org/10.16798/j.iSSN.10030530.2021
17. A. Novozámský, B. Mahdian and S. Saic, "IMD2020: A large-scale annotated dataset tailored for detecting manipulated images," in 2020 IEEE Winter Applications of Computer Vision Workshops (WACVW), pp. 71–80, 2020, https://doi.org/10.1109/WACVW50321.2020.9096940.
18. S. Agrawal, P. Kumar and S. Seth, "SISL: Self-supervised image signature learning for splicing detection and localization," arXiv preprint arXiv:2203.07824, 2022.
19. A. Kumar, A. Bhavsar and R. Verma, "Syn2real: Forgery classification via unsupervised domain adaptation," in 2020 IEEE Winter Applications of Computer Vision Workshops (WACVW), pp. 63–70, 2020, https://doi.org/10.1109/WACVW50321.2020.9096921.
20. Abdalla Y, Iqbal T, Shehata M (2019) Copy-move forgery detection and localization using a generative adversarial network and convolutional neural-network. Information 10(09):286. https://doi.org/10.3390/info10090286
21. Adobe Photoshop. https://www.adobe.com/it/products/photoshop.html. Accessed 16 Mar 2022
22. Agarwal R, Verma O (2020) An efficient copy move forgery detection using deep learning feature extraction and matching algorithm. Multimed Tools Appl 79. https://doi.org/10.1007/s11042-019-08495-z
23. Barni M, Phan QT, Tondi B (2021) Copy move source-target disambiguation through multi-branch cnns. IEEE Trans Inf Forensics Secur 16:1825–1840
24. Blog post on Elcomsoft, April 2011. https://blog.elcomsoft.com/2011/04/nikon-image-authentication-system-compromised/. Accessed 16 Mar 2022
25. Cao Z, Gao H, Mangalam K, Cai Q-Z, Vo M, Malik J (2020) Long-term human motion prediction with scene context. In: Vedaldi A, Bischof H, Brox T, Frahm J-M (eds) Computer vision - ECCV, pp 387–404
26. Chen J, Liao X, Qin Z (2021) Identifying tampering operations in image operator chains based on decision fusion. Sig Process Image Commun 95:116287. https://doi.org/10.1016/j.image.2021.116287
27. Y. Rao, J. Ni, and H. Zhao, ''Deep learning local descriptor for image splicing detection and

localization,'' IEEE Access, vol. 8, pp. 25611–25625, 2020
28. K. Asghar, X. Sun, P. L. Rosin, M. Saddique, M. Hussain, and Z. Habib, ''Edge–texture feature-based image forgery detection with cross-dataset evaluation,'' Mach. Vis. Appl., vol. 30, nos. 7–8, pp. 1243–1262, Oct. 2019.
29. N. T. Pham, J.-W. Lee, G.-R. Kwon, and C.-S. Park, ''Efficient image splicing detection algorithm based on Markov features,'' Multimedia Tools Appl., vol. 78, no. 9, pp. 12405–12419, Oct. 2018.
30. N. T. Pham, J.-W. Lee, and C.-S. Park, ''Structural correlation based method for image forgery classification and localization,'' Appl. Sci., vol. 10, no. 13, p. 4458, Jun. 2020.
31. M.-J. Kwon, I.-J. Yu, S.-H. Nam, and H.-K. Lee, ''CAT-Net: Compression artifact tracing network for detection and localization of image splicing,'' in Proc. IEEE Winter Conf. Appl. Comput. Vis. (WACV), Jan. 2021, pp. 375–384.
32. M.-J. Kwon, S.-H. Nam, I.-J. Yu, H.-K. Lee, and C. Kim, ''Learning JPEG compression artifacts for image manipulation detection and localization,'' Int. J. Comput. Vis., vol. 130, no. 8, pp. 1875–1895, Aug. 2022.
33. B. Xiao, Y. Wei, X. Bi, W. Li, and J. Ma, ''Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering,'' Inf. Sci., vol. 511, pp. 172–191, Feb. 2020.
34. J. Zhang, T. Fukuda, and N. Yabuki, ''Automatic object removal with obstructed Façades completion using semantic segmentation and generative adversarial inpainting,'' IEEE Access, vol. 9, pp. 117486–117495, 2021
35. Balaraju, J., and P. V. R. D. Prasada Rao. "Investigation and finding a DNA cryptography layer for securing data in Hadoop cluster." Int. J. Advance Soft Comput. Appl 12.3 (2020).