# Edited Image Detection to Prevent Forgery using CNN: a Review

Shuvra Smaran Das
shuvradas59@gmail.com
April 2021

## Motivation

We are in an era of advanced technologies surrounding us. We spend most of our time on technology like Facebook, Instagram, YouTube, and so on. For the recent epidemic, the use of this social media has increased so much. Now, we are uploading more pictures and videos than ever before. At the same time, when this data goes to the public news feed, anyone can manipulate these images with some advanced photo editing technology like Adobe Photoshop, GNU GIMP. These technologies do not require much effort to edit the user's original image as a duplicate. So, fake news has spread more than ever. Moreover, these image forgers are doing it intentionally or for fun. Recently, by using Artificial Intelligence (AI) called Deepfakes, clothes are stripped digitally from photographs [8] of users and shared on social media. Deepfakes are computer-generated images and videos, often convincing, based on an existing template. Victims are already afraid and worried about these things. Moreover, the images are so realistic that most users believe that these images are authentic. These things can happen to us too. However, we cannot stop using these social platforms because these platforms are the only way to communicate with others and continue our daily work online. These types of crimes should be strictly prevented and let users know which of the images are real and not. Thus, victims and users may be able to know and assure the truth about this fraud. Here, we will be analyzed image-related paperwork, including the original and the duplicate images, to inform users about image forgery. So, users will no longer believe in these fake images.

# Literature Review

## *INTRODUCTION*

Image forgery is manipulating a digital image to hide some of the image's important or valuable information. It can be challenging to distinguish the edited area from the original image in some cases. It has been recorded [16] in history dating back to the 1840s. Hippolyta Bayard is the first person to produce a false image in history. Forgers are doing it for blackmailing someone or for spreading false news about the victim to grow a negative reputation about them. Furthermore, people who are seeing these images are not concerned about their sources at all! Some of them are doing it for fun and share on social media without giving a thought because they do not have to be an expert to do it.

## *TYPES OF IMAGE FORGERY*

### *Image Retouching*

Image retouching is a process to give some alternative and enhancement to the presentations. Image retouching is considered less harmful than the other image forgeries. We can see every day and every magazine, posters, advertisement and so on. Every seller wants to make their products look as good as possible, like enhancing the shininess of the jewelry or balance the brightness, sharpness, and so on. Also, on the magazine's front page, they make the cover photo as glamorous as possible to attract clients. Though the actual image is not changing here, just some enhancement of the image is occurring. Nevertheless, this is not ethical at all.

Figure 1: Example of Image Retouching [15]

## *Image Splicing*

Image Splicing is a process of cutting a part of an image and adding that part to another image to look like a real one. The forger can completely change the actual subject of the image, and the thing that has not happened at all can be found in the picture. The forgers need two or more images to do it. They crop a particular position from an image and paste it to another image using Photo Editing tools. To make it more realistic, they use image retouching here. Otherwise, it is too simple nowadays, by using the photo editing software for a forger.

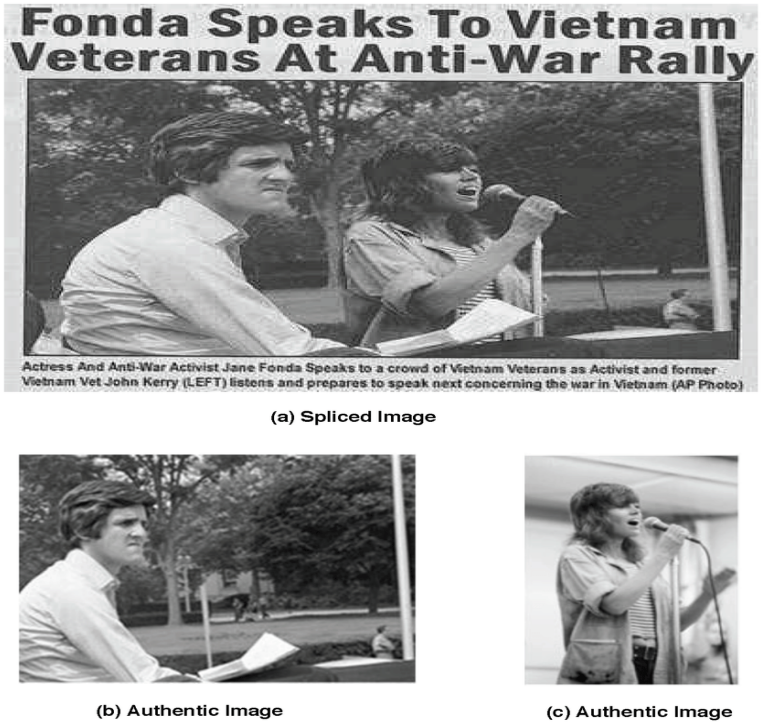


Figure 2: Picture-c has been cropped from that picture and add it into the picture-b. And the final outcome we can see picture-a as a newspaper headline [5].

## *Copy-Move Attack*

Copy-move attack is most commonly used in image forgery, and it is also challenging to detect. The resources need to do this manipulation are not like the image splicing technique. Here, the forger can manipulate the image by a single image. In the copy-move attack, the forger copies a part of an image and paste it

into another part of the same image. The forgers do it to try to hide something informative from this image or try to make it more violent than the original one.

Figure 3: In the first image, there are only three missiles. But the forgers used the same image but added another missile to it in another part to make it more violent and hide the truth. But the added missile is no different from the original one. So, the forger is just copied one of the three missiles from the original one and copy-paste it into the edited one.

## *IMAGE FORGERY DETECTION AND PREVENTION TECHNIQUES*

### *Inconsistencies in the Image*

Image forgery can be detected by finding out some inconsistency in that specific image. The lack of expertise of the forger or lack of proper attention when doing image forgery may turn into some image inconsistency. In paper [18], the image inconsistency can find out by reflection of the image to the reflector. When a picture is not accurate, and part of that image can be found several times to some reflector like glass. The angle of the actual image and edited image will vary. However, the barrier of that technique is if there is no reflector at all or the reflector is not in the direct position with the image. Paper [14] with a similar type of

solution but with shadow. If there is an image of something, there should be some shadows around it. So, the angles between the shadows of the accurate picture and the edited can be different. Here, researchers have used texture consistency of shadows and the light source's strength and differences. However, the barrier is if there are no shadows on cloudy days or nights. Paper [20] used the image angle rotation technique, which is another type of inconsistency because the original image rotation and copy-paste image rotation in an image will vary. However, nowadays, photo editing tools use perfect scaling and rotational measurements. In the paper, researchers have satisfactory accuracy, and researchers can also know the geometric history of that image. Furthermore, in paper [22], researchers have used some boundary measurements of an image. Here, researchers found out the specific boundary of the image and specify the forgery part in the image using the Fast SCNN method, which is 60% faster than the SWD method. For the dataset CASIA 2.0, the method observes an accuracy of 80%. Moreover, it also works for low-resolution images, and the method observes an accuracy of 85%. Furthermore, it also works for all formats of images. However, this model's limitation is that it can only work for simple images like from one image; it can detect only one forgery part. However, there can be multiple forgery parts in a single image which is considered a complex image. These type of complex images can't detect by that paper.

### *Median Filtering Detection*

The median filtering technique [2] is a non-linear optical filtering method for eliminating noise from images and signals. In some cases, forgers use the median filtering technique to make the image forgery more realistic. In the paper, [21] used MFF (median filtering forensics) feature set, which works for arbitrary images (like low resolution, raw images), and it can detect image forgery when a part of filtered image inserts into a non-filtered image or vice-versa. In this MFF approach, the detection accuracy varies from 78% to 90% (64*64 pixels), which was the first study on local media filtering in an image. So, accuracy is quite good as a very first work. In the paper [6], researchers have analyzed the statistics behind the median filtered images for original non-filtered images, median filtered images, and low filtered images. The use of GLF technique is effective for both

uncompressed and post-compressed images and also for high and low-resolution images too. The method observes an accuracy for GLF varies from 83% to 95% (64*64 pixels). Before the paper [13] model is needed camera model in the dataset by which the images have been captured. However, this paper removes that barrier. The auto-regressive model is used here to capture statical properties so that it can be well fitted, and the performance of AR is better than GLF and MFF for images less than (32 * 32) pixel size. The average accuracy is quite good, which is 82% to 94% for image size greater than 32*32 to 64*64. Overall, in the paper [7], got accuracy for 32*32 and 64*64 images. Previous AR and GLF methods have the possibility of data loss which this paper has prevented. The researchers used the modified Convolutional Neural Network, which is specific, and used Relu to train the large model faster. The accuracy of the method observes an accuracy for (64*64) image is 85% to 97% and for (32*32) images is 79% to 93% which best among above those. In the paper, [4] shows that the accuracy is near the perfect score with 99.10% on average with any image manipulation by adding just a layer in the Convolutional Neural Network approach.

### *Copy-Move Detection*

For Copy-Move and Slicing detection [1], [3], the paper [11] used BDCT and ZM polar and by using dataset CASIA v1.0 and v2.0, the method observes an accuracy of 99.03% and for the splicing images its accuracy is 99.11%.

## *OBJECTIVE*

The main objective of this study is to find out the best possible ability for detecting a forgery image. In this research, the specific object is to identify the best possible model for all possible types of forgery images. Also, let the user know about that forgery image and quickly realize the current scenarios to take the possible steps.

### *Sub-Objectives*

The first sub-objective is to determine the available image forgery techniques [17] are using most of the time and how they use those. This sub-objective will go to

the Descriptive Research. It will help understand and describe the technologies forgers use for image forgery and which one is more dangerous than the others.

The second sub-objective compares the accuracy and constraints of the current techniques to build a relationships among those. This sub-objective will go to the Correlation Research. Here, we have to find out if we could change one model's constraints because it will affect the other types of detection techniques to retrieve the better output. Moreover, we also have to try to determine the relationship (or differences) between forgery and forgery detection; both use the Median Filtering Model.

The third sub-objective is to determine the best models among all and why those are related to detecting the image forgery. After finding out the relationships among the detection techniques, we need to examine how we can build the best model to detect any image forgery. For that, we need to clarify how these models are related to each other.

### *Research Questions*

1. How to detect the different types of edited image?
2. What are the techniques available to detect image forgery?
3. Which technique is the best for any type of image forgery?

## Proposed Methodology

To tackle mentioned questions, we have to follow some methodologies. In the first research question, we have to figure out that how a model can detect an edited image as a human does by extracting features from an image and figure out if that image is edited or not. Here, we have to use process methodology to tackle this question. In the process methodology, we have to make sure that the model works as a human does. Before mentioned about three types of detection techniques; 1. Image Retouching, 2. Image Splicing, 3. Copy-Move attack.

From paper[19], we can detect image retouching forgery by an active and passive approach where the active approach uses the watermarking detection from an image. However, many images do not have any watermarks at all. So, in the passive approach, we can use statistical and image patterns with the original

differences.From the paper[12], we can detect the spliced and non-spliced images using logistic regression. In the paper[9], researchers used an efficient detection technique to detect copy-move image forgery.

In the second research question, I have already found out the related works about different detection techniques. I have already mentioned and analyzed some papers with their different detection techniques. So, the second research question can be tackled by using Experimental Methodology.

For the last question, we have to analyze the time complexity, accuracy, and so on. This question can be tackled by using Formal Methodology. In the formal methodology, we have determined the best algorithm or solution among the available techniques to solve the problem. In the experimental methodology, we have already experimented with many papers for different techniques and different types of image forgery. Moreover, I have also collected the best possible accuracy for each image forgery with multiple techniques. In the paper [10], also provided some state of art accuracy lists for different techniques. However, our main objective is to find out the best solution or model which will work for any image forgery, which is reasonably related to the last research question. Users will not concern about the type of image forgery. Instead, they want to clarify about the image is edited or not. It can be any image forgery. That is why we have to tackle any image forgery with the best accuracy and minimum time limit to detect the edited image. The selected approach to solve the selected problem is by using Convolutional Neural Networking. As I have mentioned earlier in the literature review section, in paper [4], we can detect any type of edited image by using Convolutional Neural Networking with an accuracy of 99.10%. The approach is quite familiar and well supported with good and quick feedback which very much necessary for the formal methodology.

The future work of this research can be that the system will be able to blur the edited image initially without notifying or seeing it by the users. Many techniques have to operate to tackle the question, and we have to build the system for the users from the ground. It can be tackled using the Build Methodology. We have to build a demo software to see it works or not and update the software from users' feedback or use a relevant model, which will solve the research question appropriately.

# References


[1] Abidin, Arfa Binti Z. ; Majid, Hairudin Bin A. ; Samah, Azurah Binti A. ; Hashim, Haslina B.: Copy-move image forgery detection using deep learning methods: A review. In: *2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS)* IEEE, 2019, S. 1–6

[2] Agarwal, R. ; Khudaniya, D. ; Gupta, A. ; Grover, K.: Image Forgery Detection and Deep Learning Techniques: A Review. (2020), S. 1096–1100. http://dx.doi.org/10.1109/ICICCS48265.2020.9121083. – DOI 10.1109/ICICCS48265.2020.9121083

[3] Amerini, I. ; Ballan, L. ; Caldelli, R. ; Del Bimbo, A. ; Serra, G.: A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery. In: *IEEE Transactions on Information Forensics and Security* 6 (2011), Nr. 3, S. 1099–1110. http://dx.doi.org/10.1109/TIFS.2011.2129512. – DOI 10.1109/TIFS.2011.2129512

[4] Bayar, Belhassen ; Stamm, Matthew C.: A Deep Learning Approach to Universal Image Manipulation Detection Using a New Convolutional Layer. In: *Association for Computing Machinery* (2016), 5–10. http://dx.doi.org/10.1145/2909827.2930786. – DOI 10.1145/2909827.2930786. ISBN 9781450342902

[5] BRENNEMAN, RICHARD: *Kerry Photo Altered, Used for Political Attack*. https://www.berkeleydailyplanet.com/issue/2004-02-17/article/18291, Tuesday, February 17, 2004

[6] Chen, Chenglong ; Ni, Jiangqun ; Huang, Rongbin ; Huang, Jiwu: Blind Median Filtering Detection Using Statistics in Difference Domain. In: *Springer Berlin Heidelberg* (2013), S. 1–15. http://dx.doi.org/10.1007/978-3-642-36373-3. – DOI 10.1007/978–3–642–36373–3

[7] Chen, J. ; Kang, X. ; Liu, Y. ; Wang, Z. J.: Median Filtering Forensics Based on Convolutional Neural Networks. In: *IEEE Signal Processing Letters* 22 (2015), Nr. 11, S. 1849–1853. http://dx.doi.org/10.1109/LSP.2015.2438008. – DOI 10.1109/LSP.2015.2438008

[8] Clahane, Patrick: *Fake naked photos of thousands of women shared online.* https://www.bbc.com/news/technology-54584127, 20 October 2020

[9] Fridrich, A J. ; Soukal, B D. ; Lukáš, A J.: Detection of copy-move forgery in digital images. In: *in Proceedings of Digital Forensic Research Workshop* Citeseer, 2003

[10] Gill, Navpreet K. ; Garg, Ruhi ; Doegar, Er A.: A review paper on digital image forgery detection techniques. In: *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* IEEE, 2017, S. 1–7

[11] Hema Rajini, NH: Image forgery identification using convolution neural network. In: *International Journal of Recent Technology and Engineering (IJRTE)* 8 (2019)

[12] Jaiswal, Ankit K. ; Srivastava, Rajeev: A technique for image splicing detection using hybrid feature set. In: *Multimedia Tools and Applications* (2020), S. 1–24

[13] Kang, X. ; Stamm, M. C. ; Peng, A. ; Liu, K. J. R.: Robust Median Filtering Forensics Using an Autoregressive Model. In: *IEEE Transactions on Information Forensics and Security* 8 (2013), Nr. 9, S. 1456–1468. http://dx.doi.org/10.1109/TIFS.2013.2273394. – DOI 10.1109/TIFS.2013.2273394

[14] Ke, Yongzhen ; Qin, Fan ; Min, Weidong ; Zhang, Guiling: Exposing image forgery by detecting consistency of shadow. In: *The Scientific World Journal* 2014 (2014)

[15] Li, Leida ; Zhou, Yu ; WU, Jinjian ; QIAN, Jiansheng ; CHEN, Beijing: Color-Enriched Gradient Similarity for Retouched Image Quality Evaluation. In: *IEICE Transactions on Information and Systems* E99.D (2016), 03, S. 773–776. http://dx.doi.org/10.1587/transinf.2015EDL8204. – DOI 10.1587/transinf.2015EDL8204

[16] Marshall, Colin: *The First Faked Photograph (1840).* https://www.openculture.com/2019/10/the-first-faked-photograph-1840.html, October 22nd, 2019

[17] Nirmalkar, Nitish ; Kamble, Shailesh ; Kakde, Sandeep: A review of image forgery techniques and their detection. In: *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)* IEEE, 2015, S. 1–5

[18] O'Brien, James F. ; Farid, Hany: Exposing Photo Manipulation with Inconsistent Reflections. In: *ACM Trans. Graph.* 31 (2012), Februar, Nr. 1. http://dx.doi.org/10.1145/2077341.2077345. – DOI 10.1145/2077341.2077345. – ISSN 0730–0301

[19] Sundaram.A, Meenakshi: IMAGE RETOUCHING AND IT'S DETECTION - A SURVEY. In: *International Journal of Research in Engineering and Technology* 04 (2015), S. 30–34

[20] Wei, W. ; Wang, S. ; Zhang, X. ; Tang, Z.: Estimation of Image Rotation Angle Using Interpolation-Related Spectral Signatures With Application to Blind Detection of Image Forgery. In: *IEEE Transactions on Information Forensics and Security* 5 (2010), Nr. 3, S. 507–517. http://dx.doi.org/10.1109/TIFS.2010.2051254. – DOI 10.1109/TIFS.2010.2051254

[21] Yuan, H.: Blind Forensics of Median Filtering in Digital Images. In: *IEEE Transactions on Information Forensics and Security* 6 (2011), Nr. 4, S. 1335–1345. http://dx.doi.org/10.1109/TIFS.2011.2161761. – DOI 10.1109/TIFS.2011.2161761

[22] Zhang, Z. ; Zhang, Y. ; Zhou, Z. ; Luo, J.: Boundary-based Image Forgery Detection by Fast Shallow CNN. (2018), S. 2658–2663. http://dx.doi.org/10.1109/ICPR.2018.8545074. – DOI 10.1109/ICPR.2018.8545074