Panamerican Mathematical Journal
ISSN: 1064-9735
Vol 34 No. 3 (2024)

Detection of Cloning in Digital Images

Vaishali Ramdas Khandave[1], Dr. Shyamrao Gumaste[2]
[1,2] Research Scholar, *MET's Institute of Engineering*, Nashik, India, Savitribai Phule Pune University, Pune
[1]vaishali7187@gmail.com, [2]svgumaste@gmail.com

Article History:

Received: *05-06-2024*

Revised: *05-07-2024*

Accepted: *21-08-2024*

Abstract:

Digital image manipulation has grown common place among individuals and professionals in recent years. As a result, in domains where digital photographs are used, establishing the authenticity of photos has become crucial. Separating the genuine camera outputs from their altered or fabricated counterparts is necessary for image authentication. One common method of altering images is digital picture cloning. In this paper, author has used the SURF and SIFT algorithm to identify the clone image.

Keywords: Tampering, Digital Image, Cloning, SURF, SIFT

1. Introduction

Photographs were acknowledged as proof of evidence in various disciplines, including crime detection, forensic investigations, scientific research and publications, insurance claim investigations, and legal processes, among others. They were regarded as the most potent and reliable form of expression. However, the accessibility of inexpensive, user-friendly picture editing software led to the widespread use of photo modifications. The reliability and standing of photographs as proof have completely disappeared in all fields since it is now nearly impossible to distinguish between an authentic camera output and one that has been manipulated. Because of this, research on digital picture tamper detection has become crucial in order to distinguish manipulated digital photos from their original sources and validate the legitimacy of this widely used medium. There are several reasons why images are altered, and not all of these adjustments fall under the category of tampering or forging. As to the Oxford Dictionary, "tampering" in literature refers to tampering with anything in order to cause unlawful changes or damages to it. Thus, the term "tampering" refers to the act of manipulating photographs to create the appearance of a fact and deceive the viewer into believing otherwise by removing or adding essential details; this is distinct from basic adjustments such as adjusting brightness, contrast, or color.[1]

Detecting image forgeries is a very difficult task. It has become increasingly challenging to determine whether an image is real or false these days. One kind of passive technology is picture forgery detection, which use blind algorithms to identify manipulation in the suspected image without using any previous knowledge. They thus separated passive approaches into two categories: splicing and copy-move. [2]

The term "copy-move" refers to the process of copying a portion of an image and pasting it somewhere else inside the same image, usually to conceal undesirable areas. Image splicing, on the other hand, is the technique of copying a section of one image and putting it into another. As a result, the process of

identifying tampered sections involves looking for extremely similar regions in copy-move images and unusual parts in spliced photos.

2. Types of Tampering

The two main categories of manipulation techniques are tampering and steganography, depending on whether the manipulation is done on the image's apparent surface or its invisible planes. Again, tampering can be divided into two categories: context-based tampering and content-based tampering. The former occurs when modifications are made to the context of the scene pieces, while the latter does not.

In the second scenario, the image itself is not changed, but the recipient is tricked into thinking that the things in it are something else than they actually are.

The most common method used to commit copy-move forgeries, sometimes referred to as context-based photo tampering, is inserting scene fragments from one image into another or into the original. Cloning is the term for image manipulation that involves copying and pasting a portion of an image to itself in order to hide an object or replicate many instances of the objects in the scene. Splicing, on the other hand, is the procedure used to generate a forged image by copying and pasting a portion of one image into another.

2.1 Image Splicing

A portion of an image is copied and pasted into another image during image splicing, and no post-processing smoothing is done. When we talk about image tampering, we usually mean splicing and post-processing techniques to make the change undetectable to the human eye.

Example

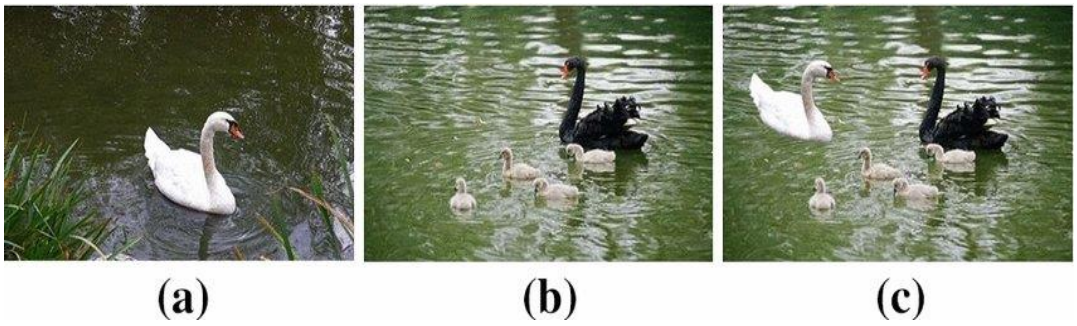


Figure 1 [3]

In the above image, figure 1 (a) is the Authenticate image, Figure 1 (b) is the Authenticate image, and Figure 1 (c) is the forged image generated by compositing images 1 and 2, after the required rescaling of the copied object.

2.2 Cloning

Copying or cloning Forgery is a form of image manipulation in which a portion of the image is copied and pasted onto another portion of the same image. This is typically done to conceal certain things from view or to reproduce a few more instances of a particular object in an image. It's among the methods for manipulating images that are most frequently utilized.

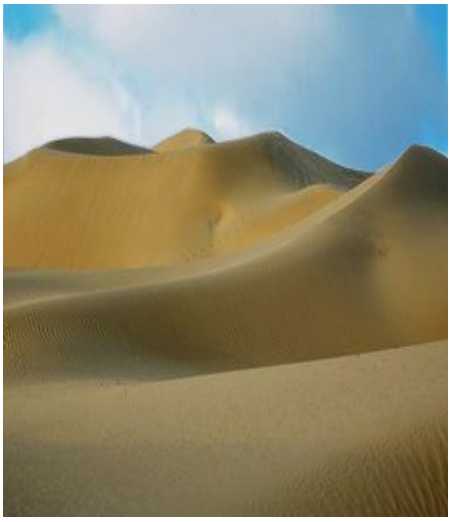


Figure 2 (a)

Figure 2 (b)

The image in Figure.2 (a) is a clone of the image Figure.2 (b). A portion of the sand is copied, pasted, and blended expertly to conceal the bird in the scene.

Figure 3 (a)

Figure 3 (b)

The image given in Figure.3 (a) is a clone of Figure.3 (b) where a portion of the original image is copied and pasted to recreate another instance of the gate [1].

When carried out carefully, it practically becomes impossible to see the clone and the cloned section can be anywhere in the image and have any shape or size, hence it is not computationally feasible to perform a comprehensive search of all sizes to all potential image locations. As a result, image authentication's clone detection challenge continues to be difficult.

In this work, the author detects the percentage of clone parts in an image. For this purpose, Speeded Up Robust Feature (SURF) algorithm is used. The following steps are written for clone detection from the photos.

3. Algorithm:

1. Load the two images. (the image should be loaded as a colour image)
2. Detection of key points of the first image using the SURF.
3. Compute the descriptors using the SURF algorithm for the key points detected in the first image.
4. Drawing the detected key points on the first image.
5. Detection of keypoints of the second image using the SURF.
6. Compute the descriptors using the SURF algorithm for the key points detected in the second image.
7. Drawing the detected key points on the second image.
8. Declaring a list to store the key point matches between the descriptors of first and second image.
9. FLANNBASED (Fast Library for Approximate Nearest Neighbors) algorithm is used which is responsible for matching feature descriptors between images.
10. The knnMatch(k nearest neighbors) method is used to find the k nearest neighbors for each descriptors in the first and second image descriptors (value of k=2) and it stores the matches in the list. This matching process is used to identify correspondences or similarities between the features extracted from the first and second image.
11. Then creating a new list that will store the “good” matches. This list represents a match between two key point descriptors.
12. Declaring a variable nndrRatio with value 0.7f (nearest neighbor distance ratio) and is used as a threshold to determine if a match is considered "good" based on the distances between the two closest matches.
13. Applying the loop over the matches list, which contains the matches between the first and second image key points. Each iteration processes a pair of matches.
14. Extracting a first and second matches and checking if the distance of the first match is less than or equal to the distance of the second match multiplied by the nndrRatio. If this condition is true, it means that the distance of the first match is sufficiently close to the distance of the second match, indicating a good match. In this case, the first match is added to the good Matches List. The loop continues until all matches have been processed. Overall, this loop iterates over the matches between the first and second keypoints, compares the distances of the matches using a ratio test, and adds the "good" matches to the good Matches List based on the specified nndrRatio.
15. if the number of good matches is greater than or equal to 7, indicating that an object has been found.
16. Creating an two empty linked list to store the corresponding key point position in the first and second image. Then it then extracts the positions of the keypoints from these lists and stores them separately in created linked list respectively. The resulting `LinkedList` objects hold the corresponding keypoint positions between the first and second images, which can be further used for geometric calculations or transformations in applications like image registration or object tracking.

4. Experimentation

The dataset that is downloaded from https://github.com/namtpham/casia2groundtruth is used for experimentation.

Dataset folder name is: CASIA2.0_revised.zip

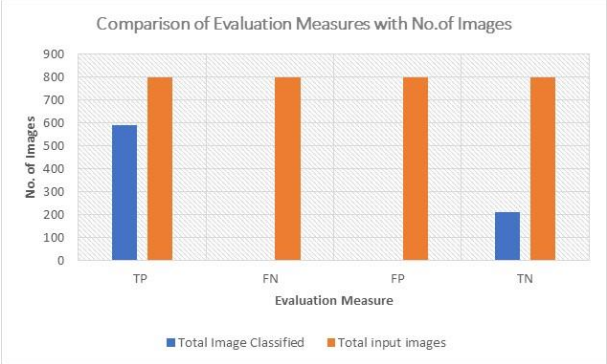
It contains 7491 authentic images and 5123 tampered images. From these images, author taken the 1600 clone images and obtained the results.

The following outcomes are achieved by feeding the system with every image in the dataset. Author finds the matching percentage between two images. The author classifies findings with a matching percentage of 50% or more as TP and those with a percentage of less than 50% as TN. First, a calculation is made using the evaluation measure findings.

Table 1: Result on Evaluation Measure

	True Positive (TP)	**False Negative (FN)**	**False Positive (FP)**	**True Negative (TN)**
Total Image Classified	589	0	0	211
Total Input Images	800	800	800	800
Percentage	74%	0%	0%	26%

The evaluation measure findings are displayed graphically as follows.



Graph 1: The Result on Evaluation Measures

The performance parameter's findings are derived as follows from the values of the evaluation measure mentioned above:

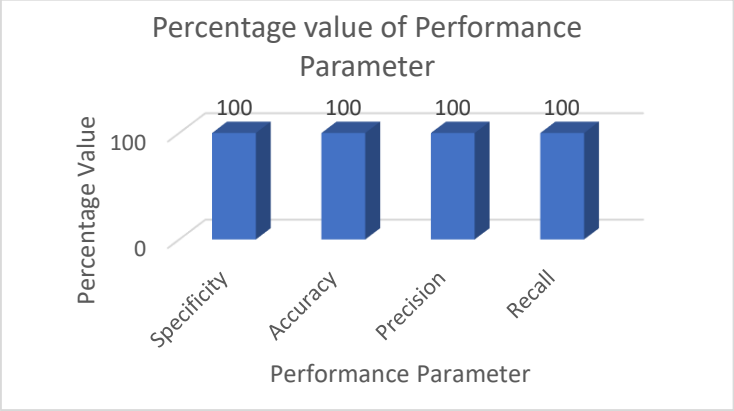
Specificity $= \frac{TN}{TN+FP}$ = 100%

Accuracy $= \frac{TP+TN}{TP+TN+FP+FN}$ = 100%

Precision $= \frac{TP}{TP+FP}$ = 100%

Recall $= \frac{TP}{TP+FN}$ = 100%

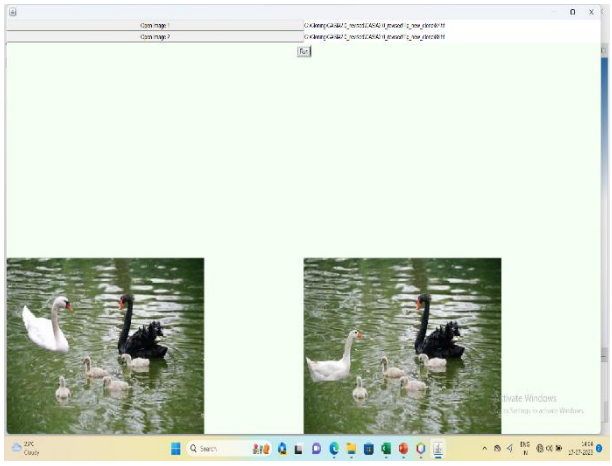
Below is a graph that displays the performance parameter's outcomes.



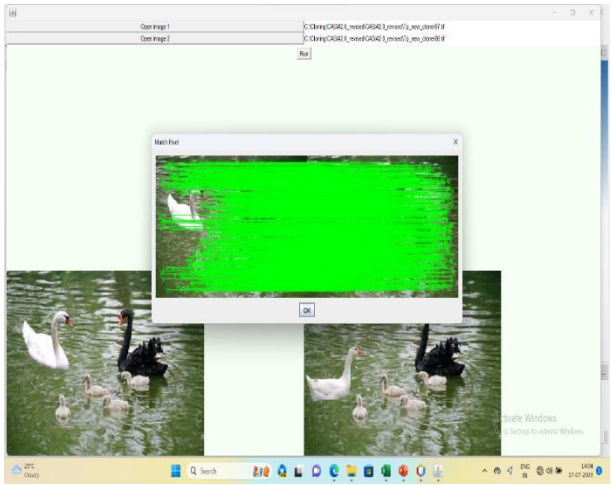
Graph 2: Performance Parameter

Images obtained from the result:

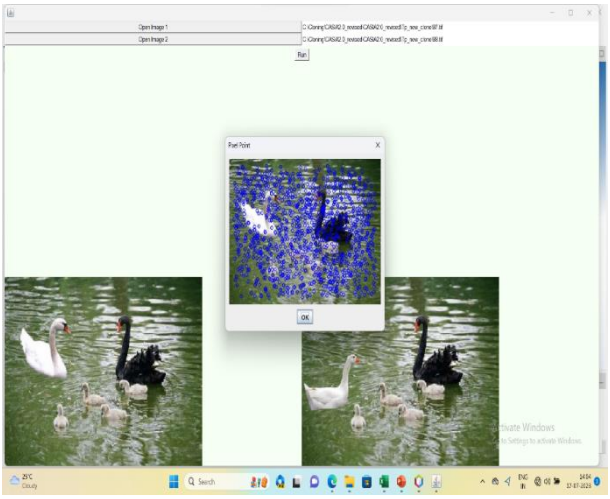
- Firstly, two images are taken as an input



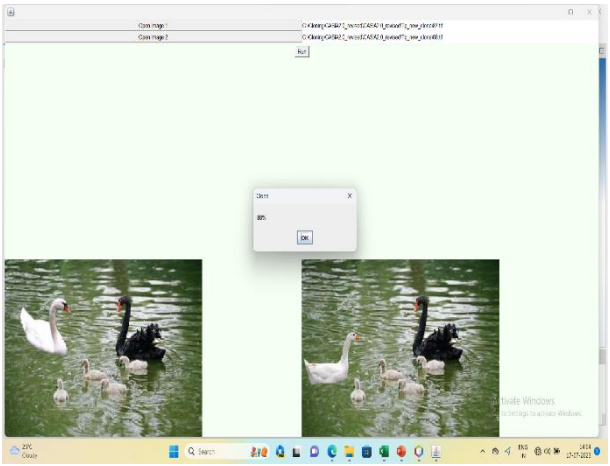
- Then matching two input images



- Plotting the key point pixel on the first image



- Finally displaying the result of the percentage of clone.



So it is observed that the given input images are 88% same.

The author classifies findings with a matching percentage of 80% or more as TP and those with a percentage of less than 80% as TN. The Author received the following findings.

Total input images are 800

Total image classified as TP = 455, FN = 0, FP = 0, TN = 345

Also, the author classifies findings with a matching percentage of 90% or more as TP and those with a percentage of less than 90% as TN. The Author received the following findings.

Total input images are 800

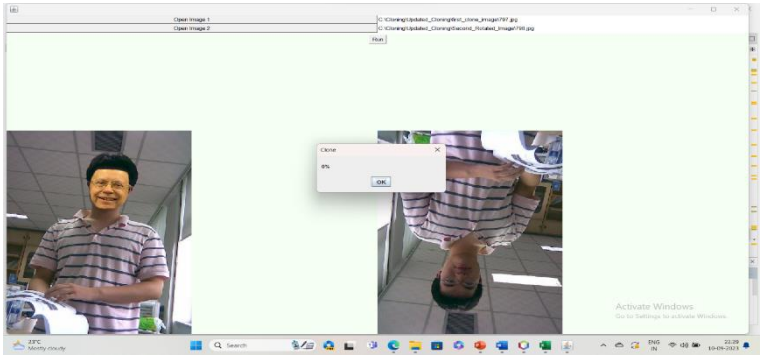
Total image classified as TP = 318, FN = 0, FP = 0, TN = 482.

The above work does not work for rotated images properly. So as a contribution, the author modified the algorithm which gives better results for rotating images.

The size of the two images should be the same as in the previous work. The author matches the keypoint pixel row-wise and column-wise (RGB format) in the work.

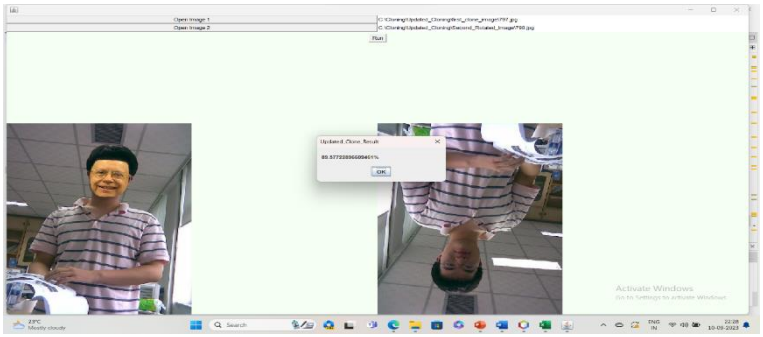
In the updated work, the author can take two images of different sizes. In this work, key points are stored and then matched.

Authors' previous work results for the rotated image



It is observed that previous work doesn't provide the percentage of matching between images if one image is rotated.

Author's modified work for the rotated image



It is observed that updated work gives 89% similarity of the given two images even though one image is rotated.

Conclusion:

Cloning, sometimes known as copy-move forgery, is a popular technique for manipulating images. In this paper the author detects the percentage of clone parts in an image. The results show that the author's work provides 100% accuracy. The author also worked on the rotated clone images and found better results for it. This work detects tampering in all type of images. This work can be used in digital authentication like social media.

References:

[1] Minati Mishra & MC Adhikary, "Detection of Clones in Digital Images", International Journal of Computer Science and Business Informatics (ISSN: 1694-2108), Vol. 2, No. 1, Pp. 1-12, January 2014.
[2] Youssef William, Sherine Safwat, Mohammed A.-M. Salem, 'Robust Image Forgery
[3] Detection Using Point Feature Analysis' Proceedings of the Federated Conference
[4] On Computer Science and Information Systems pp. 373–380, ISSN 2300-5963 ACSIS, Vol. 18
[5] Souradip Nath, uchira Naskar, "Automated image splicing detection using deep CNN-learned features and ANN-based classifier", Signal, Image and Video Processing (2021) 15:1601–1608. https://doi.org/10.1007/s11760-021-01895-5

[6] Zhongqian Jiang, Xun Gong, Haojie Fe, “Color-luminance adjustment for image cloning based on mean-value coordinates”, 2017 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC), 978-1-5386-3016-7/17/$31.00 ©2017 IEEE

[7] Binson V A, Neetha Mary Thomas, Sania Thoams, Abhijith Augustine, Sivakumar K S, “An Advance to Cloning Detection in Digital Forensics Investigations”, 2016 International Conference on Emerging Technological Trends [ICETT], 978-1-5090-3751-3/16/$31.00 ©2016 IEEE

[8] Yehu Shen, Lei Wei, Qiming Xu, and Zhenyun Peng, “A Simple and Fast Image Cloning Algorithm”, 2016 12th World Congress on Intelligent Control and Automation (WCICA), June 12-15, 2016, Guilin, China, 978-1-4673-8414-8/16/$31.00 ©2016 IEEE

[9] Taranjit Kaur, Akshay Girdhar, Geetika Gupta, “A Robust Algorithm For The Detection of Cloning Forgery”, International Conference On Computational Intelligence and Computing Research, 978-1-5386-1508-9/18/$31.00 ©2018 IEEE

[10] Yehu Shen, Lei Wei, Qiming Xu, Zhenyun Peng, “A Simple Real-time Image Cloning Algorithm Based on Modified Mean-Value Coordinates”, International Conference on Control, Automation and Information Sciences (ICCAIS), October 29-31, 2015, Changshu, China

[11] Uppuretla Pavan Kumar, T.S.R Krishna Prasad, “Improved Seamless Cloning based Image In painting”, OSR Journal of VLSI and Signal Processing (IOSR-JVSP), Volume 4, Issue 5, Ver. I (Sep-Oct. 2014), PP 38-45, e-ISSN: 2319 – 4200, p-ISSN No.: 2319 – 4197

[12] Roqaya Hamad Jaafar, Zahraa. H. Rasool, Abbas H. Hassin Alasadi, “New Copy-Move Forgery Detection Algorithm”, International Russian Automation Conference (RusAutoCon), 978-1-7281-0265-8/19/$31.00 ©2019 IEEE

[13] Umair A. Khan, Mumtaz A. Kaloi, Zuhaib A. Shaikh, Adnan A. Arain, “A Hybrid Technique for Copy-Move Image Forgery Detection”, 3rd International Conference on Computer and Communication Systems, 978-1-5386-6350-9/18/$31.00 ©2018 IEEE

[14] Chavi Rana, Gyanendra Kumar Singh, “A Survey on Digital Image Forgery Techniques and its Detection”, International Journal of Science, Engineering and Technology, 2021, 9:3, ISSN (Online): 2348-4098, ISSN (Print): 2395-4752

[15] Deepali Pal, Prof. Amit Shrivastav, “Detection of Digital Forgery Image using Discrete Wavelet Transform and SIFT Features Extraction”, International Journal of Scientific Research & Engineering Trends, Volume 7, Issue 4, July-Aug-2021, ISSN (Online): 2395-566X

[16] P. Garg, R. K. Yadav, D. V. C, D. Nirmala, N. P. Sable and K. Murari, "Estimation Analysis of Edge and Line Detection Methods in Digital Image Processing," *2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*, Bangalore, India, 2023, pp. 1-6, doi: 10.1109/SMARTGENCON60755.2023.10442722.

[17] Patel, S. K., Nair, R., & Kumar, A. (2019). Improving Power Efficiency in Embedded Systems Through Dynamic Voltage Scaling Techniques. International Journal on Advanced Electrical and Computer Engineering, 7(1), 98-105.

[18] Rao, N. J., Joshi, S., & Desai, P. R. (2020). A Study on the Integration of AI and IoT in Smart Home Systems. International Journal of Advanced Computer Engineering and Communication Technology, 8(4), 32-39.

[19] Verma, D. R., Singh, H., & Kale, M. P. (2021). Optimized Load Balancing in Cloud Computing Environments Using Metaheuristic Algorithms. International Journal Of Recent Advances in Engineering & Technology, 9(5), 115-121.

[20] Sharma, V., Gupta, R., & Dutta, K. S. (2022). Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey and Performance Analysis. International Journal on Advanced Electrical and Computer Engineering, 10(2), 78-85.

[21] Jyoti L. Bangare, E. al. (2024). Federated Texture Classification: Implementing Colorectal Histology Image Analysis using Federated Learning. Journal of Electrical Systems, 19(2), 131–147. https://doi.org/10.52783/jes.698