International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 12 | Dec - 2021 ISSN: 2582-3930

Image Forgery Detection Using MD5 Hashing

Jayant Yadav
Maharaja Agrasen Institute of Technology

Abstract— With the rise in social media and internet users there is a raise in the images data around the globe. Many images are edited and are represented in a different meaning for own benefits of a user, this is called as Image Forgery. The detection of such images is important as it can create fake news or false information. This paper intends to propose the solutions for the former problem through hashing method.

Keywords— Image Forgery, Image Hashing, Copy Move, Image Splicing

I. INTRODUCTION

Image Forgery is a method where an image is taken and edited and presented in such a way that the information or the meaning is changed. This method is widely used in create false information or misleading news and can be spread through digital media. The changes introduced in an image in this method are done in such a way that a normal user cannot be able to understand if the image is manipulated or is an original image. But with the use of hashing on a block of pixel values it can be decided that if the image is being manipulated or not.

This paper offers method to implement the use of hashing algorithm on top of an image and compare the hash values for the pixel blocks to decide if the image is forged. Hash functions always generate a unique value for a distinct data, and this can be beneficial when it comes to images as there are many pixel combinations. So, this problem can be covered through hashing functions.

The hashing is better compared to a machine learning method as hashing does not require additional data gathering and training. Also compared to a conventional machine learning there are less compute power required to run and deploy the method.

II. RELATED WORK

Almost every technology revolves around images in a certain way, and to detect image tampering and forgery is an important part for an organization. There are many relevant articles available on the same. Perpetual Hashing was used in [1] for detecting Copy-Move. This method processes the image in a greyscale pixel to extract features from the image and uses DCT matrix for a tile of image and this provide the authentication of the image, if the vectors of DCT matrix are different then it can be stated that the image has been tampered. Davarzani et al. [2] proposed to use two different categories for feature extraction for hashing. To extract local and global features gradient-based and LBP-based algorithms were adapted. Also, the feature is incorporated with a secret key to provide additional security to the detection algorithm. In [3] the image is hashed with respect to the Fast Fourier Transform method and feature vectors are generated based on the hashed values. These vectors are then compared to the targeted imaged to detect forgery in image.

III. PROPOSED WORK

Image forgery can be detected by applying a hashing function on this image. In order to detect the region of image which is tampered image can be divided into a fixed number of tiles and then hashing function can be applied individually. Later by comparing hash values, tampered regions of the image can easily detect.

The process of detecting forgery is segregated into 5 processes.

1. Image preparation
2. Image tiling
3. MD5 hashing
4. Calculation Tiles Hash values
5. Compare and highlight results

A. *Image Preparation:*

Both original image and tampered image are compressed, and the length and height are reduced as per equation:

C = (B / W)

height = (H* C)

So, the dimension of the adjusted image will be (B x height).

B. *Image tiling:*

The adjusted image is taken and divided into 25 sub images called as tiles.

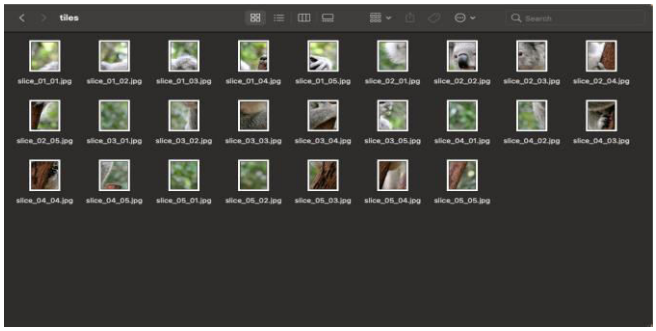

Figure 1: Image Tiles

C. MD5 Algorithm

For this method the MD5 algorithm is selected as I provide check sum for data integrity. MD5 will take a series of integers in our scenario it will be a series of pixels values and will generate a hexcode as a hash value of a particular image block.

The hash function will take one input an Image I to generate hash value h=H(I).

D. Calculate Image hash value of each tile.

Each tile will have a Hash value generated using MD5 algorithm. As shown in below image the hash value of each 25 tiles is calculated.

```
f2bc56e1d1d14d9216eef29eeee4553d
c8d095f626001bbadd2e1359f7033316
e4e42f1f339199e65623d6ed7ec10255
f2bc56e1d1d14d9216eef29eeee4553d
f2bc56e1d1d14d9216eef29eeee4553d
f2bc56e1d1d14d9216eef29eeee4553d
f2bc56e1d1d14d9216eef29eeee4553d
f2bc56e1d1d14d9216eef29eeee4553d
2755f793ab08e3bcde9c697048be4142
2e4111d1aedcb47e9bad5e18a5c2f067
f2bc56e1d1d14d9216eef29eeee4553d
ac4c3cef95aa26002da9c6ee7da5ac31
bf205ff0184930708590826fdbe60036
8d15b812b3945326d1bc301ac83962bb
f2bc56e1d1d14d9216eef29eeee4553d
f2bc56e1d1d14d9216eef29eeee4553d
a279a9d31a2a70a27c5caafc726a57eb
e3472c734dfb4513c6181142b50d0a88
421fdf67c008c99dd6b2b99f805f99fc
f2bc56e1d1d14d9216eef29eeee4553d
2c22407f6642c8c9c925363b3a55efdc
f2bc56e1d1d14d9216eef29eeee4553d
f2bc56e1d1d14d9216eef29eeee4553d
ee2c35c13d4673caee233a8f9961d5b5
2e4111d1aedcb47e9bad5e18a5c2f067
```

Image 2: Tiles Hash Values

E. Compare image and highlight tampered image tile.

If the hash value of a tile is not equal to the respected original tile hash value than that tile is taken, and a border is made in order to highlight the image. As shown in blow image.

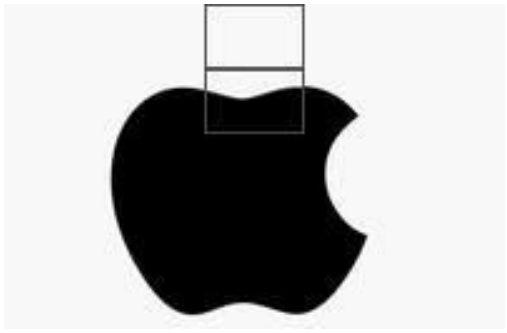

Figure-3 Processed Result Image

Proposed Algorithm

Step1: Adjust the images and compress the pixels of the image.

Step2: Divide both original and forged compressed image into 25 parts.

Step3: Calculate the Hash value of every tile for both the images.

Step4: Compare the Hash value with the respected tile.

Step5: Draw borders in the tile if the Hash value is different.

Step6: Merge the image with highlighted forgery edits in the image.

III. EXPERIMNETAL RESULTS

Image Forgery can be classified into a categories like copy move, splicing and rotation.

Attacks and its handling are demonstrated below.

*A. **Copy Move:***

This attack includes of a duplication of an object from insides of an image or from an external image. In below figures it can be shown that in tempered figures there are more coins than of the original image.

Original

Tampered

Figure 3: Copy Move Example Image

Figure 4: Copy Move Processed Image

B. Splicing Move:

This attack contains a part of image which is taken from another image and included in the images. In the below figure you can see that the part of the images is being copied and edited in the images as per the tampered image.

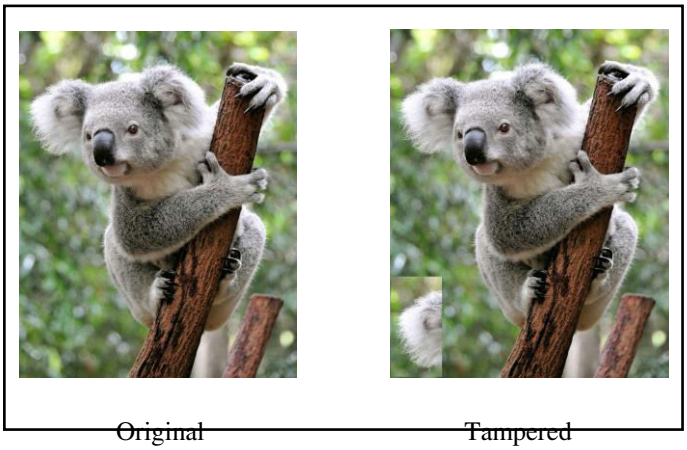

FIGURE 5: Splicing Move Example Image

Figure 6: Splicing Move Processed Image

C. Rotation:

In this attack the image presented is rotated around any of its axis(horizontally or vertically) as shown in below image.

Figure 7: Rotation Move Example Image

Figure 8: Rotation Move Processed Image

CONCLUSION

Number of research and study have been made to address this problem and many of the methods have proposed robust solution and generates accurate results. Each methods have a different approach and have different benefits when it comes to use cases. Here the MD5 Hashing is a reliable solution as it takes lesser computation and provides accurate results as well. The proposed algorithm has be tested with different categories of image and has proved to be effective in detection of image forgery.

REFERENCES

[1] Wang, Huan, and Hongxia Wang. "Perceptual Hashing-Based Image Copy-Move Forgery Detection". *Security And Communication Networks*, vol 2018, 2018, pp. 1-11. *Hindawi Limited*, doi:10.1155/2018/6853696. Accessed 14 Dec 2021.

[2] Davarzani, R., Mozaffari, S., Yaghmaie, K. (2015). 'Image authentication using LBP-based perceptual image hashing', *Journal of AI and Data Mining*, 3(1), pp. 21-30. doi: 10.5829/idosi.JAIDM.2015.03.01.03

[3] H. B. Kekre, D. Mishra, P. N. Halarnkar, P. Shende and S. Gupta, "Digital image forgery detection using Image hashing," 2013 International Conference on Advances in Technology and Engineering (ICATE), 2013, pp. 1-6, doi: 10.1109/ICAdTE.2013.6524736.