International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 14, Number 5 (2021), pp. 419-423

A Review on Digital Image Forgery Detection

Jahnavi Ega
SRM University-AP, Andhra Pradesh, India

Deepak Sri Sai Krishna
SRM University-AP, Andhra Pradesh, India

V. M. Manikandan
SRM University-AP, Andhra Pradesh, India

Abstract:

In today's world, technological development in the digital world has led to a huge increase in the popularity of digital images in all our lives. Manipulation of digital images has become an easy task nowadays due to the wide availability of various image editing software such as Adobe Photoshop, GIMP, PaintShop, etc. The image forgery tasks can be carried out in different ways such as image retouching, copy-move forgery, and image splicing. The research on image forgery detection is mainly focused on two approaches: active methods and passive methods. In this paper, we give an overview of various image forgeries with interesting examples, the common way to detect the image forgery, and the key challenges during image forgery detection.

Keywords- Copy-move forgery, discrete cosine transform, image splicing, fake image, image forgery.

I. INTRODUCTION

The advancement in communication technology and the cheap availability of handheld devices such as tablets and mobile phones led to the sharing of a large amount of multimedia data. Images are one of the most commonly shared information by various means. There are lots of image editing software such as Adobe Photoshop, GIMP, etc. are available which help us to edit the images very easily. The images can be easily altered using the image editing software and the process of altering the meaning of an image by modifying the contents in the image is called image forgery [1, 2]. The image forgery can be classified into three:

1. Image retouching
2. Copy-move forgery (cloning)
3. Image splicing

Image retouching: This is treated as a less harmful image forgery in which some of the properties of the images to improve the quality. Generally, image retouching is used for editing the cover pages of magazines and for editing personal photos [1,2]. In general, the operations such as histogram equalization, brightness enhancement, etc. are performing as part of the image retouching operation. The kind of patchwork that we used to do on the old photos is also treated as image retouching. An example for image retouching is given in Fig. 1.

(a) Original image (b) After image retouching

Fig 1. Example for image retouching

Copy-move forgery: This is one of the most common types of image forgery in which some of the regions from an image will be copied and pasted in the same image to show the duplicated information or to hide some crucial information in the image [3-5]. A few examples of copy-move forgery are given in Fig. 2. Fig. 2(a) and Fig. 2(c) are the original images and Fig. 2(b) and Fig. 2(d) are generated through copy-move forgery.

(a) Original image (b) After copy-move forgery

(c) Original image (d) After copy-move forgery

Fig. 2. Examples for copy-move forgery

Another well-known example of copy-move image forgery detection is given in Fig. 3. This image is widely circulated and discussed in 2008 and it known as Iranian Missile case. The details of this image is available in the website [6]. Once this image is widely circulated The image given in Fig. 3 is basically a doctored image and the original image is given in Fig. 4.

Fig. 3. Doctored image

Fig. 4. Original image

Image splicing: Image splicing is a process of merging the features of two or more images to create a forged image with a different meaning [3-5]. One of the well-known examples of image splicing is given in Fig. 3 in which a shark is trying to attack the man on the ladder. This image was widely distributed in 2001 through email, but later it is identified as a forged image. The source images that are used to create a fake image is also given. It may be noted that the source images were captured by two different photographers.

(a) Original copter image

(b) Original shark image

(c) Forged image through image splicing

Fig. 5. Example for image splicing

Forged image creation and its wide distribution through various social media are very common nowadays to generate false evidence or to spoil the reputation of a person or company. The political parties are also started using the forged image to spoil the reputation of the opposition party or to create some fake reputation in the public. One of the recent spread images is given in Fig.4 in which the center of attraction is Russian President Vladimir Putin, but later it is declared as a fake image. Someone pasted Putin's image on an empty seat to create a fake image. The original image and fake image is given in Fig. 4.

(a) Fake image

(b) Original image

Fig. 6. Fake image example spread in social media

II. METHODS FOR FORGERY DETECTION

The whole discussion given in this section tells us the different ways the image forgery affects our social life. Digital image forgery detection is an active area of research in which we will try to identify whether a given image is forged or not. The next level of the image forgery is identifying the region that is forged. There are two approaches for image forgery detection:

- Active approach: In this, unique information called watermark will be embedded into the original image before uploading the image to some social networking sites [7-8]. Further, whenever the image owner wants to authenticate an image, the watermark can be extracted from the image for authentication purposes. If the embedded watermark is matching with the extracted watermark which indicates that there is no image forgery happened in the image.
- Passive approach: In a passive approach, we will not have any prior information about the image. Without any kind of prior information, we have to detect the image forgery. This is one of the most studied domains in the area of image forgery detection [9, 10].

In this research, we have focused on copy-move forgery detection using a passive approach. There are many algorithms are available in the literature which will take an image as the input and will detect the copy-moved region. The algorithms for copy-move forgery (under passive approach) can be classified into three categories:

1. Block-based approach
2. Keypoint-based approach
3. Hybrid approach

In this research, we have focused on copy-move forgery detection using a passive approach. There are many algorithms are available in the literature which will take an image as the input and will detect the copy-moved region. The algorithms for copy-move forgery (under passive approach) can be classified into three categories:

- Block-based approach: The input image will be divided into overlapping blocks of size BxB and all the pairs blocks will be compared by considering the pixel value as it or by extracting the features from the blocks. The block-based approach gives good detection accuracy if the copy-moved doesn't undergo any rotating or scaling operation [11-13].
- Keypoint-based approach: The keypoints and the corresponding feature vectors will be extracted from the image, and all the pairs of the keypoint feature vectors will be compared to find the matching regions. The keypoint-based approach can detect the copy-moved region even though if it has undergone some rotation or scaling. There are many keypoint detection techniques such as scale-invariant feature transform (SIFT), speeded-up robust features (SURF), etc. which will help extract the feature points for region matching [14-16].
- Hybrid approach: The hybrid approaches are introduced to make use of the advantages of both the block-based approach and keypoint-based copy-move forgery detection [17].

Block-based approaches are widely studied for many years and still, researchers are working in the area to design new copy-move forgery detection schemes. The basic steps in a copy-move forgery detection scheme are given below:

Step 1: : Divide the image into small overlapping blocks of size B×B pixels

Step 2 : Compute the features from all the overlapping blocks

Step 3 : Compare all the pair of feature vectors and whenever two blocks are matching mark it (binary matrix having the same size of the original image) as copy moved region.

Step 4 : Apply some morphological operations or filtering to remove the false-positive results (some small regions that are not copy-moved but detected as copy-moved),

Step 5 : Return the resultant binary matrix in which the copy-moved region will be marked with 1 and the remaining regions will be marked as 0.

A sample input image and expected output from a copy-move forgery detection system is given in Fig. 5.

Fig. 7. Overview of copy-move forgery detection scheme

The major challenges in a copy-move image forgery detection scheme using block-based approaches are listed below:

- If the image size is R×C and if we use a block size BB, then there will be (R-B+1) (C-B+1) number of blocks. While doing a brute force approach on all the blocks then it requires a very huge amount of computation. Let us assume that there N overlapping blocks in the image, then [N×(N-1)]/2 number of the block comparison is required. The complexity of these operations can be easily analyzed on an image of size 512×512 pixels. Let us assume that we have used a block size of 8x8 pixels. In such a case, there will be 255025 number of overlapping blocks in the image. If we consider all pairs blocks then 32,51,90,02,825 number of pairs should be get compared. This is a very huge computation overhead.
- As mentioned earlier, if the copy-moved region has undergone some rotation or scaling then the block-based detection technique may not find the forged regions.
- The size of the blocks that we suppose to use can not be predefined, it can be decided empirically. A small block-size may provide better results but it will increase the computational overhead.

The exhaustive comparison of all pairs of image blocks taking extensive time even for small images. To reduce the number of comparisons, the feature vectors extracted from the blocks can be sorted using lexicographic sorting techniques. Such sorting will bring similar features together and the computation of distance can be restricted to the blocks that are coming together. For example, the first feature vector need not be compared to all the remaining blocks, instead of that a set of feature vectors that are coming close to that can be compared. This approach is briefed given below:

Step 1: : Divide the image into small overlapping blocks of size B×B pixels

Step 2 : Compute the features from all the overlapping blocks

Step 3 Sort all the feature vectors (lexicographic)

Step 4 : Compare all the pair of feature vectors from a

group of feature vectors that are coming together. Whenever two blocks are matching mark it (binary matrix having the same size of the original image) as copy moved region.

Step 5 : Apply some morphological operations or filtering to remove the false-positive results (some small regions that are not copy-moved but detected as copy-moved),

Step 6 : Return the resultant binary matrix in which the copy-moved region will be marked with 1 and the remaining regions will be marked as 0.

There are a number of feature extraction techniques are utilized in the literature for copy-move forgery detection. A few of them are very briefly discussed in this section.

1. Discrete cosine transform (DCT)
2. Local binary pattern (LBP)
3. Histogram of gradients (HoG)
4. Histogram of orientated Gabor magnitude
5. Discrete wavelet transform (DWT)
6. Curvelet transform

The Euclidean distance is the most common distance metric used to compare the similarity S between two feature vectors. The Euclidean distance between two feature vectors A and B of size N is given below:

$$S = \sqrt{\sum_{K=1}^{N} (A_K - B_K)^2} \quad (1)$$

III. DATASET FOR THE STUDY

One of the well-known copy-move image forgery dataset is available [18]. The dataset consists of a copy-move forged image and a binary mask. As we discussed earlier from a copy-move image forgery detection scheme we will get a binary image. The result obtained from the copy-move forgery detection scheme should be compared with the binary mask available in the dataset to compute the following measures:

- Accuracy
- Precision
- Recall

The three parameters mentioned above is defined based on TP, TN, FP and FN are given below:

- TP: The number of forged pixels detected as forged pixels
- TN: The number of non-forged pixels detected as non-forged.
- FP: The number of non-forged pixels detected as forged pixels.
- FN: The number of forged pixels are detected as non-forged.

From TP, TN, FP, FN we can compute the efficiency parameters such as accuracy, precision and recall.

$$\text{Accuracy (A)} = \frac{(TP + TN)}{(TP + TN + FP + FN)} \times 100 \quad (1)$$

$$\text{Precision (P)} = \frac{TP}{(TP + FP)} \times 100 \quad (2)$$

$$\text{Recall (R)} = \frac{TP}{(TP + FN)} \times 100 \quad (3)$$

We are expecting 100% accuracy, precision and recall from an efficient algorithm.

A few images from copy-move image forgery dataset is given in Fig. .

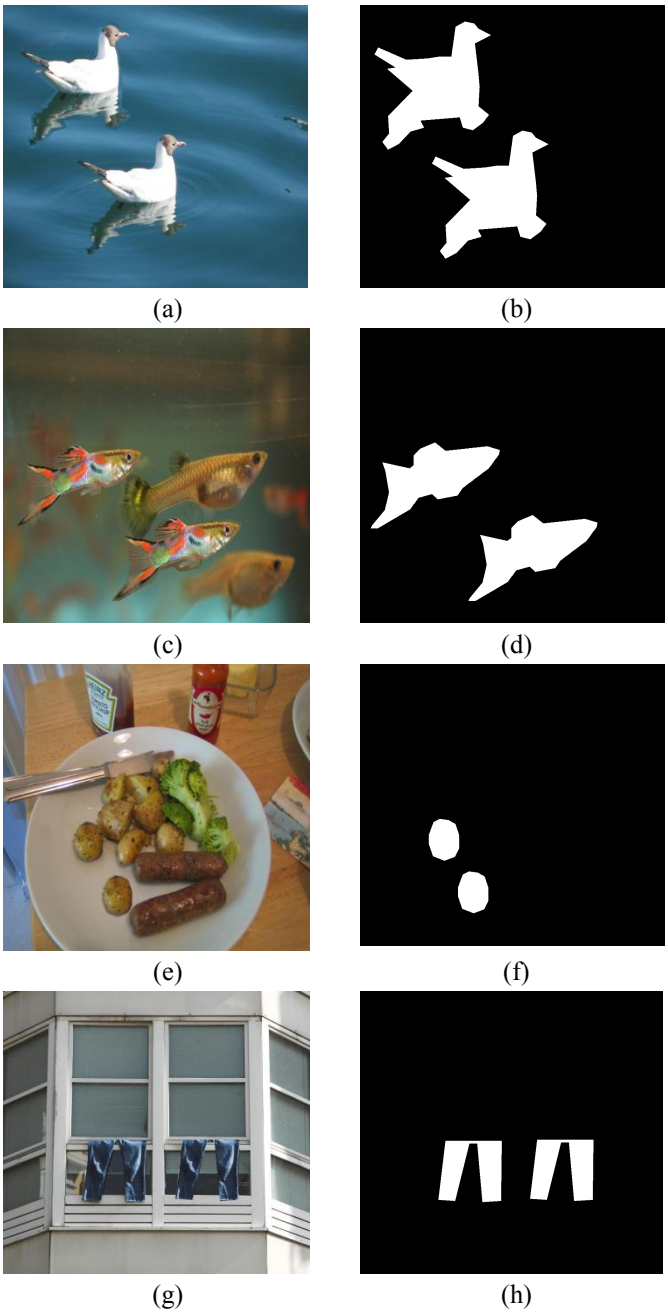

Fig. 8. Sample forged image and binary mask

VI. COCNLUSION

This paper reviews the basics of digital image forgery and various types of image forgeries are that are very common. The types of image forgeries are detailed in this paper with proper examples. Various approaches for forgery detection is discussed in this paper. A few common challenges in the existing schemes are also briefed so that the researchers can do further research in the areas discussed here. We have mainly discussed copy-move forgery detection in this paper and we have discussed the basic efficiency parameters that are used to evaluate a copy-move forgery detection scheme. The well-known copy-move forgery dataset is also introduced here which can be used while designing new copy-move forgery detection schemes.

REFERENCES

[1] Ansari, Mohd Dilshad, Satya Prakash Ghrera, and Vipin Tyagi. "Pixel-based image forgery detection: A review." IETE journal of education 55.1 (2014): 40-46.

[2] Qazi, Tanzeela, et al. "Survey on blind image forgery detection." IET Image Processing 7.7 (2013): 660-670.

[3] Abd Warif, Nor Bakiah, et al. "Copy-move forgery detection: survey, challenges and future directions." Journal of Network and Computer Applications 75 (2016): 259-278.

[4] Nathalie Diane, Wandji Nanda, Sun Xingming, and Fah Kue Moise. "A survey of partition-based techniques for copy-move forgery detection." The scientific world journal 2014 (2014).

[5] Soni, Badal, Pradip K. Das, and Dalton Meitei Thounaojam. "CMFD: a detailed review of block based and key feature based techniques in image copy-move forgery detection." IET Image Processing 12.2 (2017): 167-178.

[6] https://latimesblogs.latimes.com/babylonbeyond/2008/07/iran-doctored-m.html, accessed on 05-01-2020

[7] Hu, Wu-Chih, et al. "Effective image forgery detection of tampered foreground or background image based on image watermarking and alpha mattes." Multimedia Tools and Applications 75.6 (2016): 3495-3516.

[8] Benrhouma, Oussama, et al. "Chaotic watermark for blind forgery detection in images." Multimedia Tools and Applications 75.14 (2016): 8695-8718.

[9] Zhang, Zhi, Chengyou Wang, and Xiao Zhou. "A Survey on Passive Image Copy-Move Forgery Detection." Journal of Information Processing Systems 14.1 (2018).

[10] Sadeghi, Somayeh, et al. "State of the art in passive digital image forgery detection: copy-move image forgery." Pattern Analysis and Applications 21.2 (2018): 291-306.

[11] Al-Qershi, Osamah M., and Bee Ee Khoo. "Enhanced block-based copy-move forgery detection using k-means clustering." Multidimensional Systems and Signal Processing 30.4 (2019): 1671-1695.

[12] Parveen, Azra, Zishan Husain Khan, and Syed Naseem Ahmad. "Block-based copy–move image forgery detection using DCT." Iran Journal of Computer Science 2.2 (2019): 89-99.

[13] Sun, Yu, Rongrong Ni, and Yao Zhao. "Nonoverlapping blocks based copy-move forgery detection." Security and Communication Networks 2018 (2018).

[14] Wang, Xiang-Yang, et al. "A new keypoint-based copy-move forgery detection for small smooth regions." Multimedia Tools and Applications 76.22 (2017): 23353-23382.

[15] Wang, Xiang-Yang, et al. "A new keypoint-based copy-move forgery detection for color image." Applied Intelligence 48.10 (2018): 3630-3652.

[16] Sadeghi, Somayeh, et al. "Keypoint based authentication and localization of copy-move forgery in digital image." Malaysian Journal of Computer Science 30.2 (2017): 117-133.

[17] Rakesh, Saini, and Singh Sanjay. "Ameliorating the Performance of a Hybrid CMFD Technique." International Journal of Applied Engineering Research 13.22 (2018): 15511-15518.

[18] Copy-Move Forgery Dataset, http://www.diid.unipa.it/cvip/?page_id=48#CMFD, accessed on 05-01-2020.