RESEARCH ARTICLE OPEN ACCESS

An Approach for Digital Image Forgery Detection

Pooja Bhole[1], Yash Pandey[2], Vikash Gautam[3], Vrushabh Mowade[4], Sanika Telang[5], Sujal Bhagat[6]

[1]Assistant Professor, Department of Artificial Intelligence, G H Raisoni Institute of Engineering and Technology, Nagpur, India
[2,3,4,5,6] UG Students, Department of Artificial Intelligence, G H Raisoni Institute of Engineering and Technology, Nagpur, India

Abstract
Image forgery detection is an important area of research in digital forensics, as it helps to ensure the authenticity and integrity of digital images. With the increment of digital image manipulation, it has become increasingly important to develop methods and techniques for detecting image forgery. Researchers have developed a range of approaches, including analyzing image metadata, detecting inconsistencies in image content, and using machine learning algorithms to recognize patterns of manipulation. Image forgery detection is used in various fields such as social media monitoring journalism, law enforcement, and forensic investigation. This paper provides an overview of the importance of image forgery detection and the various methods used to detect it.

Keywords: *forgery, splicing, copy-move, retouching, dependent, independent approach.*

Date of Submission: 02-04-2024 Date of acceptance: 13-04-2024

I. INTRODUCTION

Image forgery detection is the process of recognizing whether an image has been altered or manipulated in some way to create a false representation of reality. With the rise of digital media and advanced editing tools, it has become easier to create realistic forgeries that can receive even the most discerning viewers.

In the advancement of communication technology and availability of cell phones and desktops, it has resulted in sharing of large amounts of multimedia, data, images, videos, etc. Some of the most commonly shared media is Images and hence comes the risk of altering images. As nowadays it's cheap to access image editing softwares like Photoshop, PicsArt, Canvas, etc. The images can be altered using some softwares and the process of altering information and meaning of an image is called Image Forgery. Image forgery can be further classified into three types:

1. Copy-Move forgery / cloning
2. Image Splicing
3. Image retouching

Copy-Move forgery: One of the most common types of forgery is copy-move forgery often referred to as CMFD(Copy-Move forgery Detection). In simple words, In this type of forgery a part of an image is duplicated and pasted into some regions of the same image. CMFD helps in hiding information into an image. Therefore, the main objective of CMFD is to detect image areas that are the same or extremely similar.

Image Splicing: A frequently used technique of image forgery is Image splicing. Image splicing refers to the combination of two or more separate images to produce a merged image which highly differs from the original images. Image splicing is commonly followed by post processing such as compression or resizing images. Image splicing is much more harmful than other types of forgery. This type of forgery can alter the meaning of an image. Further resulting in many more issues.

Image retouching: Image retouching is a basic type of image forgery which is less harmful as compared to image splicing. In image retouching, images are enhanced or improved by enhancing their brightness, contrast, hue, etc. It is usually used for designing Thumbnails, Editing cover pages, etc.

DIGITAL IMAGE FORGERY DETECTION METHODS:

As with the growing technology and scientific development, image forgery has been catched in the eyes of multiple people, scientific researches, etc. From the research, researchers have figured out two methods for detection of forgery in an Image. The two approaches for forgery detection are:

1. Active approach
2. Passive approach

Active Approach: Active approach is the simplest way of preventing forgery in an image. There are two major approaches that are digital signatures and digital watermarking.

A. Digital signatures: Digital signatures are one of most common ways of preventing image forgery. A digital signature is used to represent the validity of a digital document using mathematical structures. Here, this digital signature can be only altered by the admin or the owner of the image. Hence, if any portion of the image is altered it will be noticed by the owner. Thus preventing forgery in an image.

Qualities of digital signatures:

1. Signature cannot be falsified by unauthenticated users.
2. Here, only the sender can sign the original image and the recipient can only confirm that signature.

B. Digital Watermark: Digital watermarking is a process of embedding a digital code via. Into an Image, audio or video. This is a security essence meant to discourage and detect piracy in multimedia. Digital watermarker are also used in forensics such as in fingerprint files. One of the main features of digital watermarker is tamper detection i.e. it is a veritable tool for detecting when a multimedia has been tampered.

Passive Approach: Passive Approach does not require any prior information about digital image. So here without any given data or prior data we have to figure out the forgery in the media. Here, this is one of the most widely used approaches in the domain of image forgery detection. As of now there are two approaches used in passive approach they are:

1. Dependent
2. Independent

Dependent Passive Approach: Dependent approach is a technique of passive forgery detection which mainly consists of detecting image splicing and copy-move forgery detection. Image splicing is a major issue of image forgery which is particularized by this approach. Copy-move detection consist of three approaches they are:

A. Block-based approach
B. Keypoint-based approach
C. Hybrid approach

These are the types of copy-move detection approaches which are further discussed in below paragraphs. These approaches detect copy-move forgery in an image. Here the algorithms take the image as an input and apply the approaches which further classify the image as whether it is forged or not. Let us discuss them below:

Block-Based Approach: As the input image is divided into block size of BxB and these blocks are overlapped the approach works as it compares the pixel value or extract the features from the block i.e. by SIFT(Scale variant feature transformation) algorithm. The block-based algorithm gives us good accuracy detection if the image has not been rotated or has been through scaling operations.

Keypoint-Based Approach: Keypoint based approach is another type of approach for copy-move detection. In this approach, the keypoints and features will be extracted from the image and then all the key points will be matched to find the matching regions. This algorithm can detect forgery even if the image has been through rotation or scaling operations. The keypoint extraction of image features can be done through methods like speeded-up robust features(SURF), etc. which will help to find the local features of the image.

Hybrid Approach: As the name suggests, Hybrid means mixture of two i.e. this approach will contain both features of block-based and keypoint-based approach and will also overcome the disadvantages of both approaches.

Independent Approach: Independent approach is another type of passive approach which deals with the forgery of resampling and image compression. Forgeries dealed by independent approach are:

A. Image Resampling
B. Image compression

Image Resampling: Image resampling refers to changing the pixels of an image. Here changing the pixels can downgrade the image quality. Image resampling is the technique of modifying a digital image and transforming it into another form. There are various reasons for manipulation of image some of them can be - change of resolution, change of orientation, etc. There are multiple methods used to detect image resampling i.e. K-nearest neighbor(KNN), bilinear interpolation, etc.

Image Compression: Image compression is a process of compressing the size of an image. This either works by removing bytes of images or by rewriting the image file in a certain way it takes less storage in simple terms modification of image directly by changing its rewriting the image. Sometimes image compression can lead to loss of information or robustness in an image because of the changing of quality of an image.

Objectives of image compression:

1. To reduce irrelevance and duplication of image data.
2. To be able to store or transfer data in an efficient form.

II. Literature Review:

The paper provides an understanding survey of passive image forgery detection techniques, including statistical analysis, JPEG compression, artifacts analysis, and noise analysis[1] This Paper provides an introduction to digital image forensics, including image manipulation approaches and the different techniques used for image forgery detection.[2]

The paper proposed a technique to detect copy-move forgery using color moments. First they divided the image into circle blocks. Then, they extracted feature vectors from the blocks using three-color moments. Later, the feature vector matrix has to be sorted lexicographically. To create a dataset, they used images from Google image search, then they created fake images by duplicating some regions in the image and putting it within the same image. They found that the proposed method had high accuracy and false positive ratio with 0.9981 and 0.0205 respectively [3]

The paper presented an algorithm to detect copy-move forgery. In their methodology they started with a pre-processing step: first they convert the image into grayscale, then to find out the intensity direction, they measure the gradient of the image and then they apply the Gaussian filter. Afterwards, they passed to the feature extraction phase: In this step they divide the image into overlapping blocks of fixed size. After the image is divided into blocks, the Histogram of Oriented Gradient (HOG) is calculated for each block of find descriptor features. Then, a matching step is performed to check the forged regions. The author used the Euclidean distance with a threshold value to get the decision. For the dataset, they used a public dataset called COMOFOD. They tested their approach on three different experiments using three different dataset sizes. They obtained best result false acceptance rate of 0.82 and false rejection rate of 0.17 in the case of taking 70 original images and 70 forged images.[4]

The author proposed a method where their aim was to detect tampered regions using a direct modification without any post-processing. Their method was based on the idea that the background of the forged image would not be coherent and consistent and the counterfeit region would appear different from the other instant neighboring regions. They used in their experiments a handmade dataset of 200 documents, each of which contains at least one forgery operation. Thus, collected 481 forgery instances with different types of forgery (such as copy-move, imitation and region cuts). They used SVM as a classifier for their experiments with a cross-validation. For the results, they showed that they were able to detect the forged regions with 7.38% and with 0.05% of false positive ratio.[5]

The paper proposed a technique that detects text lines that were manipulated or added to a numeric document. It is based on measuring the rotation and the alignment of the text to detect such errors in these text-line features. They performed the following steps: extracting text lines, calculating the alignment lines, calculating distances between these lines, and finally based on the distance, the lines are classified into usual alignment or unusual.[6]

This proposed a new method using convolutional neural networks to detect copy-move forgery. Using a small sample of training data, they slightly modify the network architecture taken from an existing database of trained models such as ImageNet. To accomplish their work. First, they built their handcraft dataset that contained about 10000 images, also they used both the OXFORD and the UCID datasets. Subsequently, the convolutional neural network CNN network was initialized while fine-tuning some of the parameters. Eventually, they can attain results by inputting test images into the obtained trained model. For the results, achieved good performance on both the OXFORD and the UCID datasets with 2.32% and 2.43% test error respectively. However, they got very poor performance for the handcraft database with 42% test error due to the random tampering operation.[7]

The paper has proposed a copy move forgery detection method in which they introduce a technique that optimizes SIFT and fuzzy C- means (FCM) clustering. The technology is based on the SIFT algorithm for feature extraction. Fuzzy C-mean clustering method is used to reduce the time complexity of the SIFT algorithm. First, the key points are used to extract the feature descriptor. Afterwards, they passed to a matching stage followed by a clustering algorithm to cluster the key points. For the experimental step, they used 573 pictures. They used the MICC-220 as a dataset plus their own data. They evaluated their method by measuring TPR, FPR and time complexity. To obtain the best results, three main parameters are used in the FCM algorithm which are: the number of clusters to create and the minimum amount of improvement. Their results depend on the datasets that are used, they observed that the TPR of the MICC-220 is preferred to the one obtained from their dataset, also the former exhibits a lower time complexity. Perhaps, that is due to the professional forged images used and the high number of images with high resolution in their dataset as compared to the MICC-220 dataset. [8]

Most of the methods have been proposed to detect splicing or CM forgery, however, The paper proposed a method that aimed to detect both splicing and CM forgery using the same dataset. This method merged block discrete cosine transform (DCT) and Zernike moments, using a process combining two main steps: finding image forgery using SVM classifier and classification of the output to either of the forgery types.

The proposed method extracted the features of a color image based on the developed threshold method. First they used DCT to transform non-overlapping blocks of an image into matrices from which the discriminative features for forgery detection are extracted using an enhanced threshold method. Before that, to minimize the effect caused by the diversity of the image content, they deployed a pre-processing step.

For copy-move forgery detection they used a feature extraction technique. Afterwards, they used the Patch Match Algorithm implementing three steps: initialization, propagation and random search. After the feature matching process they used a post-processing step to increase the possibility of detecting forgery in a proper manner without being exposed to a false alarm of Copy-move forgery detection.[9]

The paper suggested a technique that prevents digital documents from falsification. The aim of this work was proposing a new approach that is motivated by existing techniques that display security weaknesses. Using different techniques, such as the use of wavelet transform, for the purpose of developing a secret message for digital documents encryption.[10]

The paper presented a method that contains cellular automata (CA) for the system implementation in image forgery detection, where they present two methods. The first method is about using cellular automata and Lower Upper Decomposition and the second scenario using CA and Singular Value Decomposition. Their aim of presenting this method was to preserve digital image tampering by including an encrypted and unpredictable key into the image. [11]

It ensures the authenticity and integrity of digital images.It aims to comprehensively analyze image forgery detection methods using convection and advanced deep learning apps[12,13].

III. CONCLUSION

This paper has suggested the basics of digital image forgery and various types of image forgeries that are very common. The types of image forgeries are detailed in this paper with proper examples. Various approaches for forgery detection are discussed in this paper. A few common challenges in the existing schemes are also 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.

REFERENCES

[1]. "A Survey of Image Forgery Detection using Passive Techniques" by D. M. Mathai and S. S. Shankar.

[2]. “Digital image forensics a booklet for beginners” by M. Brain, F. C. Bartolome, V. Capelins, and A. Pica (1=1,2=2)

[3]. B. Ustubıoglu, V. Nabıyev, G. Ulutas, and M. Ulutas, “Image forgery detection using color moments”, in 2015 38th International Conference on Telecommunications and Signal Processing (TSP). IEEE

[4]. M. V. Hilal, P. Yannawar, and A. T. Gaikwad, “Image Inconsistency Detection using Histogram of Oriented Gradient (hog),” in 2017 1st International Conference on Intelligent Systems and Information Management (ICISIM). IEEE, 2017, pp. 22–25.

[5]. F. Cruz, N. Sidere, M. Coustaty, V. P. D’Andecy, and J.-M. Ogier, “Local Binary Patterns for Document Forgery Detection,” in 2017 14th IAPR International Conference on Document Analysis and Recognition (ICDAR), vol. 1. IEEE, 2017, pp. 1223–1228.

[6]. J. Van Beusekom, F. Shafait, and T. M. Breuel, “Text-line Examination for Document Forgery Detection,” International Journal on Document Analysis and Recognition (IJDAR), vol. 16, no. 2, pp. 189–207, 2013.

[7]. J. Ouyang, Y. Liu, and M. Liao, “Copy-Move Forgery Detection based on Deep Learning,” in 2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISPBMEI).

[8]. H. A. Alberry, A. A. Hegazy and G. I. Salama, “A fast SIFT based Method for Copy Move Forgery Detection”, Future Computing and Informatics Journal, Elsevier, 2018, 3, pp. 159-165.

[9]. C. S. Prakash, A. Kumar, S. Maheshkar, and V. Maheshkar, "An Integrated method of Copy-move and Splicing for Image Forgery Detection," Multimedia Tools and Applications, vol. 77, no. 20, pp. 26 939–26 963, 2018

[10]. A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "A Secure and Improved self-embedding Algorithm to Combat Digital Document Forgery," Signal Processing, vol. 89, no. 12, pp. 2324–2332, 2009.

[11]. A. P. Tafti and H. Hassannia, "Active Image Forgery Detection using Cellular Automata," in Cellular Automata in Image Processing and Geometry. Springer, 2014, pp. 127–145.

[12]. Dr.K.Prasanthi Jasmine, SK.Fhareedh, M.Navyan, K.Abhishek," Image Forgery Detection" Volume 11, 2023 ISSN: 2320-2882.

[13]. Preeti Sharma, Manoj Kumar & Hitesh Sharma "Comprehensive analyses of image forgery detection", 2022 Volume 82,pages 18117-18150.

[14]. Tanush Shekharappa, Gouda, M. Ravishankar, Dinesha H A," Image forgery Detection Using ML Algorithms", Volume 10, Issue 5(ISSN-2349-5162).