DESIGN AND DEVELOPMENT OF SOME APPROACHES FOR DIGITAL IMAGE FORGERY DETECTION AND LOCALIZATION

जाली डिजिटल तस्वीर का पता लगाने और उनके स्थानीकरण लिए कुछ पद्धतियों की रचना और विकास

Thesis submitted in partial fulfillment

for the award of degree

DOCTOR OF PHILOSOPHY

By

ANKIT KUMAR JAISWAL

अंकित कुमार जायसवाल

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY

(BANARAS HINDU UNIVERSITY)

VARANASI – 221 005

Roll No: 17071013

July 14, 2021

forged document detection. This dataset contains different types of forgery in documents and eight different types of operations performed on forged regions. This shows the diverse nature of the dataset. The major motivation behind developing a model for forged document detection is the importance of digital documents in the era of the digital transaction (i.e. digital documents are used almost everywhere) and the pressing need for a digital forgery detection model based on scanned digital documents. With regards to the challenges present in existing forgery detection models for images the developed model consists of an Inception block in the absence of dimensionality reduction, with scanned documents as an input. The experiments performed and demonstrated some interesting results. It opens up several directions for academic scholars to explore in the field of scanned documents forensics. The proposed model is analyzed on a publicly available dataset with constructed FD3 dataset and compared with the state-of-the-art methods. In this depth analysis first, image-level classification of forged and authentic documents was done. Then the pixel-level analysis of both types of forgeries was done in the forged documents. This analysis was figured out on all types of operations and transformations. The compared result shows that the performance of the proposed method is better than state-of-the-art

CHAPTER 6
CONCLUSION AND FUTURE DIRECTIONS

This chapter concludes the proposed works given in previous chapters of the thesis with the major contributions and findings. This chapter also gives future research directions for researchers by explaining open research issues in the field of digital image forgery.

6.1 Conclusion

Due to the advancement of smart handheld devices, low cost and higher bandwidth internet facilities, the use of image editing applications is increasing day by day. Using these applications, one can easily manipulate/tamper or synthesize images without any clue. So, the integrity and authentication of the image may be no longer preserved. Active and passive, two forensics schemes are widely used for the forgery detection in an image. The tampered region can be extracted using a pre-embedded watermark or digital signature in active schemes [129]. However, source files must be there to embed the watermark first for this scheme. On the other hand, the passive scheme finds some intrinsic fingerprint clues of images to detect manipulated areas. Passive attacks are imperially used when prior knowledge about the image is unavailable. Therefore, the development of image investigation schemes to verify authenticity and integrity is very important nowadays. A lot of passive techniques are already reported in the literature by researchers in the past two decades. But these techniques suffer from many challenges.

The contribution made in the thesis tried to overcome the challenges faced by previously reported forgery detection techniques. Chapter 1 of the thesis gives an introduction to digital image forgery, its type and forgery detection techniques. Further,

this chapter also defines the motivation behind the work. This chapter also lists the objectives of the thesis and contributions to the thesis.

Chapter 2 gives the literature review of digital image forgery detection techniques with its theoretical background. Digital image forgery is categorized into two classes. One is a copy-move forgery, and another is a spliced image. So reported approaches for digital image forgery detection are divided accordingly and given into its sections. A detailed description of these approaches is given in this chapter with their identified research issues. State-of-the-art techniques of CMFD are categorized into three classes based on their detection technique i.e. block-based, key-point based and data-driven based. Similarly, spliced image detection techniques are divided into two classes i.e. statistical and data-driven based. Block-based approaches for CMFD suffer from the challenges of geometrical transforms of the forged region and key-point-based approaches have limitations with small, duplicated regions. Data-driven approaches for spliced detection techniques are limited to the classification of forged or non-forged images only and don't work for the localization of spliced regions. Estimation of noise-pattern in the spliced image works better than other traces in statistical-based spliced image detection and localization techniques. But the most important challenge with these techniques is to estimate qualified noise patterns. Except for these findings, publicly available datasets and evaluation metrics used in the proposed approaches are also given in this chapter.

In chapter 3, some methods are proposed for CMFD considering the limitations of state-of-the-art techniques. The first proposed CMFD technique relies on DCT and ORB feature extraction and a distance-based clustering approach. Extracted DCT features are matched based on Euclidean distance. Extracted key points using ORB are matched using the k-NN procedure based on Hamming distances. To improve accuracy, false matches are removed with the help of a distance-based clustering technique. The proposed

technique is tested on a CoMoFoD small dataset. Experimental results show that the technique is not only efficient in detecting copy-move forged regions but also robust towards brightness and contrast change, noise addition, geometric transformations like scaling and rotation and multiple copy-move forgeries. Literature reported for CMFD has limitations of robustness with different geometric transformations and computation costs. So, in the second presented approach, a deep learning CNN model is developed using multi-scale input with multiple stages of convolutional layers. These layers are divided into two blocks i.e. encoder and decoder. In the encoder block, extracted feature maps from convolutional layers of multiple stages are combined and downsampled. Similarly, in the decoder block extracted feature maps are combined and upsampled. A sigmoid activation function is used to classify pixels into forged or non-forged using the final feature map. To validate the model two different publicly available datasets are used. The performance of the proposed model is compared with state-of-the-art methods which show that the presented data-driven approach is better.

In chapter 4, we have discussed the images which are being forged using the Image splicing technique, in which the region of an original image is cropped and pasted onto the other original image. This chapter also presents some methods and models for spliced image detection. So, to tackle this delinquent act, one must develop such a system that can instantly discriminate between the original and altered image. One of the best technologies that can tackle the problem and help to develop such a scheme is Machine learning. In the first proposed work, a machine learning classification technique logistic regression has been used to classify images into two classes, spliced and non-spliced images. For this, a combination of four handcrafted features has been extracted from images for the feature vector. Then these feature vectors are trained using a logistic regression classification model. A 10-fold cross-validation test evaluation procedure has

been used to evaluate the result. Articles based on statistical traces have been reported, one of the key ingredients for such a tool is noise inconsistency. The spliced region contains the non-homogeneous distribution of noise which acts as a feature to localize it. State-of-the-art techniques based on inconsistent noise are suffering from challenges like the requirement of prior knowledge about the image, localization of spliced region and estimation of inconsistent non-gaussian noise. In this proposed work, a blind local noise estimation technique has been introduced using a fourth-order central moment to localize the spliced region. This work tries to overcome the challenges of state-of-the-art techniques. Experimental analysis has been done on images of three publicly available datasets. Results are evaluated on pixel-level using a confusion matrix and some other performance measures.

The proposed methods for CMFD and spliced image detection depend on the assumptions of traces left during the forgery of the image. What if there is no clue about the type of forgery in an image? Other than that, what if the forged image is different from natural scenes captured by a digital camera i.e., medical images, scanned documents, or computer-generated images? For the detection of such forged images, two different data-driven approaches are given in the fifth chapter. Deep learning is surpassing technology for prediction or classification tasks in images. Challenges in this technology are a variety of datasets to train the model and specific architecture for a specific application. In the first work, a deep learning model is extended for the localization of tampered regions in a forged image. This is an extension of the well-known U-Net segmentation model. In the proposed model, batch normalization layers and identity blocks are placed at suitable places of the U-Net model to overcome the challenges such as overfitting and loss of information during max-pooling. To overcome the challenge of the dataset five different publicly available datasets are taken to train, validate and test

the model. The trained model is also tested on four created forged images (not belonging to the dataset) whose acquisition sources may be different i.e. medical image, identity document, natural image, and scanned report. The result of this proposed model is compared with state-of-the-art techniques which show that the method works better than others. Another proposed method is to detect forged digital scanned documents. To the best of our knowledge, there are none of the data-driven approaches for the detection of tampered scanned documents. To tackle this emerging obstacle, a deep learning convolutional neural network (CNN) is used in this work. Limitations of the small object have been taken care of with the small kernel size of the Inception block. This extracts local information while the large kernel size extracts global information from the input document. The advantage of the u-net model is leveraged here for training the model with the small size of the dataset. To train, validate and test the model a forged scanned document dataset is constructed which contains 6656 documents and their ground truth. The collection of different types of forgery and operations performed over the tampered region in documents has made the dataset diverse. The trained model is also tested on a publicly available dataset. The in-depth experiments are performed on the publicly available dataset as well as a constructed dataset with image-level and pixel-level analysis.

6.2 Future Research Directions

With the advancement of handheld devices, network and image editing applications challenges and issues with image authentication are also increasing day by day. Therefore, research works also need to be channelized which needs fresh innovative contributions for digital image authentication. We are currently in an era in which technology advances day by day. Improvement in digital camera design, use of digital images in healthcare, transportation system and other domain generates many open

research challenges for image authentication that need to be addressed. This section of the chapter delineates open research areas and future directions in this regard.

Light field cameras allow much more versatile post-capture customization including changing the depth of field, which leads to potentially significant variations in the image content. The functionally different image acquisition pipeline will render many existing forensic traces useless. New techniques will be required for the forensic analysis of such images.

Multi-sensor and multi-lens cameras rely on the former acquisition pipeline. However, the pipeline instance for each lens-sensor pair and final photograph is obtained via image fusion. In this case, it may be expected that existing techniques may work with only minor modifications. However further work in this direction is required. A lot of multi-sensor setups are there that invalidate existing forensic traces such as an L16 camera which is based on 16 sensor setups with varying focal lengths. The variability of sensor activation will invalidate even the most mature approach to sensor noise verification.

Decision fusion in digital image forensics is an emerging research direction. Decision fusion is the combination of results to achieve better performance in pattern recognition problems. Results from different methods, algorithms, sources or classifiers, can often be combined (fused) to give estimates of better quality than could be obtained from any of the individual sources alone. Analyzing an image requires evaluating the results of many techniques to conclude. It is shown that this is a complex task, not only to the varied nature but also the quality, of outputs. With the ever-growing amount of forensics techniques, it is important to understand how to combine them, and the implications of this in real-case scenarios.

Extensive use of the digital image in multiple domains also draws attention to research for the authenticity of the image. As we have already seen that acquisition