Synopsis of

Application of image blobs and illumination component in image tamper detection techniques

Thesis submitted for degree of

Doctor of Philosophy

In

Computer science

By

Niyishaka Patrick

Reg.No. 14MCPC21

Under the supervision of

Prof. Chakravarthy Bhagvati

School of Computer and Information Sciences

University of Hyderabad

P.O. Central University

Hyderabad – 500046, India

December - 2020

Contents

1 Introduction

Image tampering is a malicious act of adding, removing, or changing, some major areas of a digital image. The main purpose of image tampering is to mislead the viewers or public opinion and history shows that the earliest known surviving photograph made in a camera, was taken by Joseph Nicéphore Niépce in 1826 [5, 7], but around 1860 photographs were already being manipulated[7]. Since then, with the digital era, the manipulation of photographs has been made simpler and very much easier by computer tools. Since engineer Steven Sasson [8] invented the first self-contained (portable) digital camera back in 1975, the digital revolution has basically changed the way how images are created, consumed and perceived. In 1987 the photo editing computer program for personal computers known as Adobe Photoshop was released. Today, it is so popular that the term "photoshop" refers to digital image editing and manipulation. According to[9], around 95 million photos are uploaded daily on the social media platform "Instagram", and since its creation in 2010, more than 40 billion photos have been shared. Around 350 million photos per day are uploaded to the social media platform "Facebook" [6]. Now, with the gigantic amount of photographs on social media, the questions arise like in [16], how many of the photographs can we trust on social media? How to tell the authentic from the tampered? The field of *Digital Image Forensics* has emerged to help restore some trust to digital images. the *Digital Image Forensics* aims at validating the authenticity of images by identifying the imaging device that captured the image or detecting the traces of forgeries[21].

Generally, the *Digital Image Forensics* categorizes the digital image tampering detection algorithms into two categories: *active detection algorithm* which embeds digital watermark or digital signature in the image, and *passive or blind detection algorithm* which does not consider any prior information to be embedded beforehand.[21]. The passive detection approach has attracted more attention since most of todays digital images on social media, internet, and other fields do not have digital watermarking or signature embedded. The two common types of digital image tampering include **copy-move forgery or Cloning**, in which a part of an image is copied and pasted to another part of the same image[20], and **image splicing or image composition** which involves the composition of two or more regions/images from different sources in a single image [14].

2 Problem Statement, Aim and Objectives

2.1 Problem Statement

Today's computer technology has made the process to create the *copy-move forgery* and the *image splicing forgery* very effortless. Various image tamper detection techniques have been proposed to encounter the above-mentioned forgeries. However, they exhibit numerous limitations that need to be addressed and sophisticated image tamper detection tools that are robust, effective, and efficient, need to be developed.

2.2 Aim

To provide digital image tamper detection techniques using blind image forensics that tackle the limitations of the existing copy-move forgery detection techniques and the image splicing forgery detection techniques.

2.3 Objectives

1. Identify the limitations of the existing copy-move forgery detection techniques and the image splicing forgery detection techniques.

2. Study of different image characteristics and efficient features that can be used to reveal the clues of image tampering.

3. Develop detection methods for each of the above-identified limitations.

4. Testing of the behavior and performance of the developed methods on standard benchmark datasets.

3 Literature Survey

3.1 Copy-move forgery detection

A large number of copy-move forgery detection (*CMFD*) methods have been proposed to deal with various forms of image copy-move forgeries *(CMF)*. Mostly all of them are generally divided into the following major categories: *Block-based*, *Keypoint-based*, and *Segments-based* approaches.

In the block-based approach, image is divided into small overlapping or non- overlapping blocks, the blocks or block features are matched against each other to determine blocks or features that are very similar [22].

In the keypoint-based approach, keypoints are detected in the regions with high entropy in the image without any image subdivision. Then, each keypoint is described by a feature vector of a certain size. Finally, the feature vectors are compared against each other to determine which feature vectors are very similar [10].

Some recent techniques have adopted image segments as alternatives to image blocks in CMFD [11]. Image is divided into non-overlapping regions called segments or superpixels [12], features are extracted in each segment, and features from different segments are matched to find out which ones are very similar.

3.2 Image splicing forgery detection

Most recent techniques to encounter the image splicing forgery are based on machine learning [17, 23]. They consider the image splicing problem as a binary classification task. They consider two phases for the splicing tamper detection task:

1. Phase 1: classify images as authentic or tampered(forged).
2. Phase 2: detect and localize areas of forgery in forged images.

3.3 limitations of existing techniques

- Copy-move forgery detection
  - The main limitations of block-based CMFD techniques include the difficulty of finding the appropriate size of the block. Small blocks increase the computational cost of matching and also do not give robust features. Large blocks cannot be used to detect small forged areas, and uniform areas such as background regions can be detected as duplicates.
  - The main limitations of keypoints-based CMFD techniques include the large number of keypoints to match and the need for filtering techniques such as Random Sample Consensus (RANSAC) to remove or reduce the false positives.

  - Often, segments-based CMFD techniques split a single CMF region into two or more regions (oversegmentation). Uniform areas such as background regions can be detected as duplicates.

- image splicing tamper detection

  - The existing methods with high detection accuracy are very computationally expensive.
  - The existing methods with high detection accuracy are complex models. Most of them rely on the complex deep learning models which are very expensive to train, run on expensive GPUs, and require a very large amount of data to perform better.
  - It is a challenge to determine effective and efficient features or image characteristics that can be used to reveal traces of splicing forgery for the classification task.
  - There is no known standard mechanism to localize the spliced forged regions.

4 Proposed Contents of the Thesis

This thesis consists of 7 chapters. Chapter 1 includes an introduction to image forgery and digital image forensics. It also provides the motivation and necessary background for the work reported in this thesis. It concludes by providing the scope of the thesis. Chapter 2 discusses the literature survey in the area of image tampering detection. Chapter 3, 4, 5, and 6, cover our contributions and published works in the field. Finally, Chapter 7 draws conclusions and direction for future work.

The content of each of these chapters are summarized below:

4.1 Chapter 1: Introduction

This chapter introduces the field of digital image forensics, copy-move forgery, and image splicing forgery. It also provides motivation and describes the scope of the thesis.

4.2 Chapter 2: Related Work

Chapter 2 describes an overview of the state-of-the-art methods in copy-move forgery and image splicing detection methods. The limitations and drawbacks of existing techniques are discussed.

4.3 Chapter 3: Copy-move forgery detection using DoG and ORB

The utilization of image blobs to tackle the limitations of existing CMFD methods is presented. Image blobs are regions detected in scale-space, they present more advantages over image blocks and image segments in copy-move forgery detection. This chapter discusses the use of DoG (Difference of Gaussian) blob detector [19] to detect regions in image, with rotation invariant and resistant to noise feature detection technique called ORB (Oriented Fast and Rotated Brief)[13] to expose copy-move regions.

4.4 Chapter 4: Copy-move forgery detection using image blobs and BRISK feature

This chapter discusses an alternative CMFD approach using image blobs and BRISK (Binary Robust Invariant Scalable Keypoints) [18] features to overcome some of the limitations of Block-based, Keypoints-based, and Segments-based CMFD techniques. We show that that Blobs and BRISK approach reduces the number of keypoints to match by almost 50%, and also reduces the false matches without requiring a filter algorithm.

4.5 Chapter 5: Geometric transformation parameters estimation from copy-move forgery using image blobs and features:AKAZE, BRISK, ORB, SIFT, and SURF

This chapter presents a method that can detect the copy-move forgery and estimates the geometric transformations parameters between the authentic region and its duplicate using image blobs and scale-invariant features. A blob post-process operation followed by a 2D affine transformations are used to estimate the geometric transformations parameters.

4.6 Chapter 6: Image splicing detection technique based on illumination component and LBP

The chapter presents the use of the illumination and chrominance features to expose the image splicing forgery. While creating a spliced image it is difficult to achieve proper illuminant conditions for the entire image because images are taken from different cameras with different lighting conditions; this introduces Illumination inconsistencies that can be used to reveal tampering artifacts. The authors in[15] showed that the traces of tampering that can not be detected by naked eyes are hidden in the chrominance channel since human vision is sensible to luminance changes than chrominance changes. LBP (Local Binary Patterns) is a powerful feature for texture classification [15] . Therefore, for image splicing tamper detection task, we used the illumination component, chrominance features, and LBP.

4.7 Chapter 7: Conclusion and Future Work

We summarize the work reported in the thesis and outlines future directions. The following research directions are suggested for future:

- To be able to recover the original image from the copy-move forged image; Study needs to be done to determine which is the authentic region and which is the tampered region.
- Study needs to be carried out with illumination component and deep learning models like shallow convolution neural network to enable the model to automatically learn low-level features (e.g., edges and boundaries) to increase the detection performance.

List of Publications

[1] Niyishaka Patrick and Chakravarthy Bhagvati. **Digital Image Forensics Technique for Copy-Move Forgery Detection Using DoG and ORB.** ICCVG 2018, Warsaw, Poland, September 17-19, 2018, Proceedings. $10.1007/978-3-030-00692-1\_41$.

[2] Niyishaka Patrick and Chakravarthy Bhagvati. **Copy-Move forgery detection using image blobs and BRISK feature**. *Multimedia Tools and Applications (MTAP)*, https://doi.org/10.1007/s11042-020-09225-6.

[3] Niyishaka Patrick and Chakravarthy Bhagvati. **Geometric transformation estimation from copy-move forgery using image blobs features and keypoints**. *Multimedia Tools and Applications (MTAP)*, Communicated.

[4] Niyishaka Patrick and Chakravarthy Bhagvati. **Image splicing detection technique based on illumination component and LBP**. *Multimedia Tools and Applications (MTAP)*, https://doi.org/10.1007/s11042-020-09707-7.

Key References

[5] **16 Famous First Photographs in History: From the Oldest Photo Ever to the Worlds First Instagram**. https://mymodernmet.com/first-photograph-photography-history/. Accessed: 2019-07-12.

[6] **Facebook-Statistics**. https://www.brandwatch.com/blog/facebook-statistics/. Accessed: 2019-07-11.

[7] **First Photograph**. https://www.hrc.utexas.edu/exhibitions/permanent/. Accessed: 2019-07-12.

[8] **The inventor of the first self-contained (portable) digital camera**. https://en.wikipedia.org/wiki/Steven_Sasson. Accessed: 2020-01-10.

[9] **Social-Media-Statistics**. https://dustinstout.com/social-media-statistics/. Accessed: 2019-07-11.

[10] Irene Amerini, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, and Giuseppe Serra. **A SIFT-Based Forensic Method for CopyMove Attack Detection and Transformation Recovery**. *Information Forensics and Security, IEEE Transactions on*, **6**:1099–1110, 10 2011.

[11] Anuradha, Singh Baljinder, and Sood Ritika. **A Hybrid Algorithm For Image Forgery Detection**. *International Journal of Computer Science and Mobile Computing*, **7**:122–128, 03 2018.

[12] Zhihua Ban, Jianguo Liu, and Li Cao. **A novel Gaussian mixture model for superpixel segmentation**. *CoRR*, **abs/1612.08792**, 2016.

[13] G. Bradski, K. Konolige, V. Rabaud, and E. Rublee. **ORB: An efficient alternative to SIFT or SURF**. In *2011 IEEE International Conference on Computer Vision (ICCV 2011)(ICCV)*, **00**, pages 2564–2571, 11 2011.

[14] Sekhar Chandra and T N Sankar. **Review of Image Splicing Forgery Detection Techniques**. *Journal of Emerging Technologies and Innovative Research*, **3**, 2016.

[15] Hakimi Fahime, Hariri Mahdi, and GharehBaghi Farhad. **Image splicing forgery detection using local binary pattern and discrete wavelet transform**. *2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), Tehran*, pages 1074–107, 2015.

[16] Hany Farid. **Digital doctoring: how to tell the real from the fake**. 2006.

[17] Bappy Jawadul H., Roy-Chowdhury Amit K., Bunk Jason, Nataraj Lakshmanan, and Manjunath B.S. **Exploiting Spatial Structure for Localizing Manipulated Image Regions**. In *2017 IEEE International Conference on Computer Vision (ICCV)*, pages 4980–4989, 2017.

[18] Stefan Leutenegger, Margarita Chli, and Roland Y. Siegwart. **BRISK: Binary Robust Invariant Scalable Keypoints**. In *Proceedings of the 2011 International Conference on Computer Vision*, ICCV '11, pages 2548–2555, Washington, DC, USA, 2011. IEEE Computer Society.

[19] David G. Lowe. **Distinctive Image Features from Scale-Invariant Keypoints**. *International Journal of Computer Vision*, **60**(2):91–110, Nov 2004.

[20] Joseph Ojeniyi, Bolaji O Adedayo, Ismaila Idris, and Shafii Abdulhamid. **Hybridized Technique for Copy-Move Forgery Detection Using Discrete Cosine Transform and Speeded-Up Robust Feature Techniques**. *International Journal of Image, Graphics and Signal Processing*, **10**:22–30, 04 2018.

[21] Judith A Redi, Wiem Taktak, and Jean-Luc Dugelay. **Digital image forensics: a booklet for beginners**. *Multimedia Tools and Applications*, **51**(1):133–162, Jan 2011.

[22] Xiang Yang Wang, Li Xian Jiao, Xue Bing Wang, Hong Ying Yang, and Pan Pan Niu. **A new keypoint-based copy-move forgery detection for color image**. *Applied Intelligence*, **48**(10):3630–3652, Oct 2018.

[23] Zhongping Zhang, Yixuan Zhang, Zheng Zhou, and Jiebo Luo. **Boundary-based Image Forgery Detection by Fast Shallow CNN**. pages 2658–2663, 08 2018.