Detection of fake images and camera attribution using PRNU

Master Thesis Dissertation

Jose C. Mendoza-Jimenez

20 agosto 2023

Abstract

MSc Dissertation project WIP

Contents

1. Introduction

Digital image forensics plays a pivotal role in detecting image manipulations and forgeries. This project centers around the development of an advanced technique leveraging Photo Response Non-Uniformity (PRNU) patterns. The goal is to create a robust method for identifying potential image tampering and ensuring the integrity of digital visual content. This report presents the methodology, experimental results, and analysis of our PRNU-based approach.

2. Literature Review and Related Work

The study of image forensics has led to various methods for detecting image manipulations. Notably, PRNU-based techniques have gained attention for their effectiveness in identifying tampered images. PRNU patterns, which capture unique sensor-specific noise in images, offer valuable insights for image authenticity verification. This project builds upon these concepts and explores novel approaches to PRNU-based forgery detection.

3. Description of the Task and Dataset

The primary objective of this project is to develop an accurate PRNU-based forgery detection algorithm. To evaluate our approach, we utilize a diverse dataset comprising real-world images, each containing varying degrees of manipulation. This dataset covers different forms of tampering, allowing us to thoroughly evaluate the performance of our PRNU-based method.

4. Methodology

Our approach employs PRNU patterns to detect potential image manipulations. The input image is processed using convolutional neural networks (CNNs) to extract and analyze PRNU features. PRNU patterns are captured from the reference images and processed using convolutional layers with ReLU non-linearities. The final output, the anonymized image, is obtained through an element-wise sum of the input image and the processed PRNU patterns.

5. Experimental Setting

To evaluate the effectiveness of our PRNU-based approach, we conducted comprehensive experiments using the benchmark dataset. Training parameters, data augmentation techniques, and evaluation metrics are defined in this section. We outline the training strategies and discuss how our method performs across various manipulation scenarios.

6. Results

Our experimental results demonstrate the efficacy of our PRNU-based approach in detecting manipulated images. We provide a detailed analysis of detection accuracy for different types of manipulations, showcasing the strengths and limitations of our method. The results highlight the potential of PRNU-based techniques to contribute significantly to the field of image forensics.

7. Analysis

In this section, we delve into a thorough analysis of the experimental results. We discuss the performance of our approach across different manipulation scenarios and provide insights into the factors influencing its accuracy. Additionally, we compare our method with existing techniques, emphasizing its advantages in terms of detection rates and computational efficiency.

8. Conclusion and Future Work

The project concludes by summarizing the contributions and outcomes of our work. We discuss the significance of our PRNU-based approach in the context of image forensics and its potential to ensure the authenticity and integrity of digital images. As future work, we propose investigating advanced architectures, exploring adversarial training, and extending the method to video forensics.

By harnessing the power of PRNU patterns, this project advances the field of image manipulation detection and enhances our ability to detect tampered images. Our approach holds promise for a range of applications that require the verification and authentication of digital visual content.

Appendix 1

Additional visualizations from exploratory data analysis

Citations