

Image Forgery Detection

Author: Zhengqi Yang

Date: 12/04/2019

Contents

1. Introduction
2. Methodology
3. Results
4. Reference

Introduction

A Color Filter Array (CFA) demosaicing based tamper detection approach was applied in this project. This approach is based on the fact that an image tampering operation changes CFA demosaicing artifacts in a measurable way so that the lack of CFA might indicate the presence of tampering. This is achieved with two methods (CFA pattern number estimation and CFA based noise analysis) [1]. Besides this, Error-level analysis (ELA) was also applied on a few test images, which CFA did not show expected results. This method is based on the fact that if a section of the image is at significantly different error level, then it likely indicates a digital modification.[2]

Methodology

CFA Pattern Number Estimation:

Block size: 16

Mean Square Error(MSE) between the original image and re-interpolated images

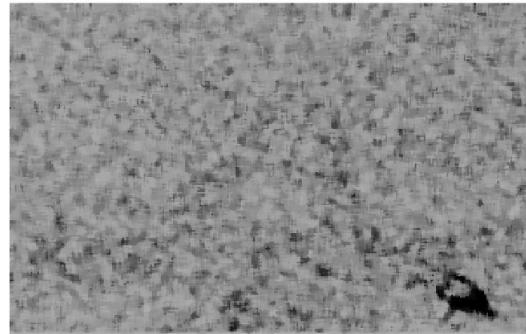
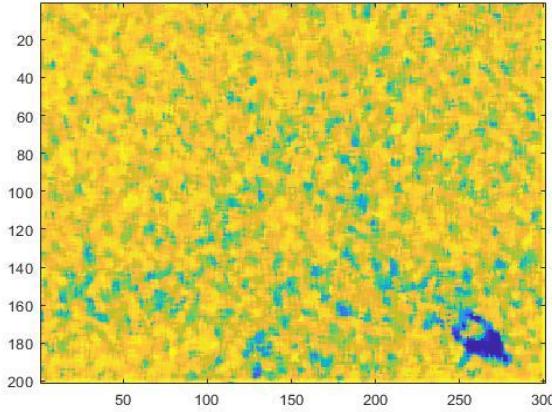
Tamper Detection: None MSE significantly smaller than the others

ELA: Quality 90 Multiplier 15

OutputMap=(abs(double(lmIn)-double(lmJPG))*Multiplier);

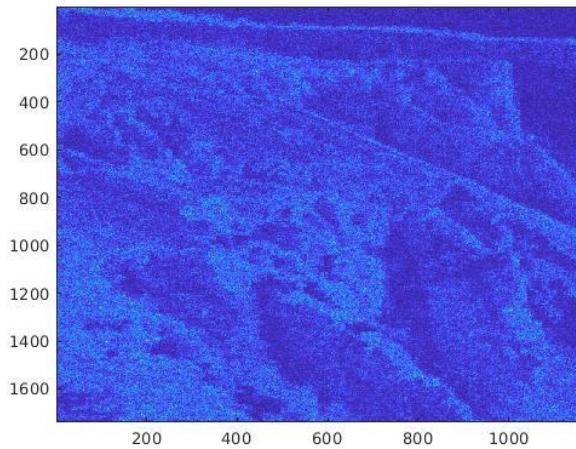
Results

Test Image 1 via CFA:



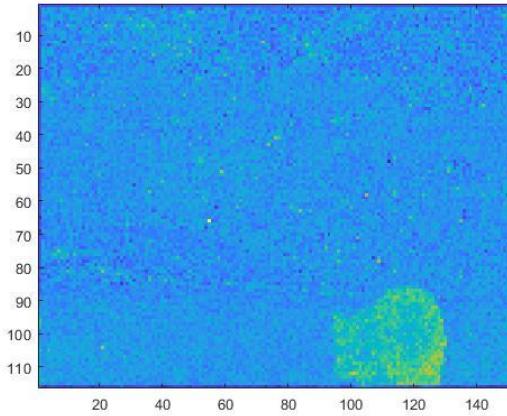
Results

Test Image 2 via ELA



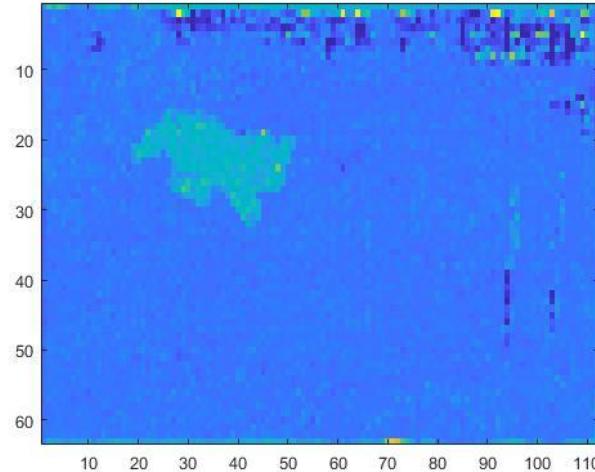
Results

Test Image 3 via CFA



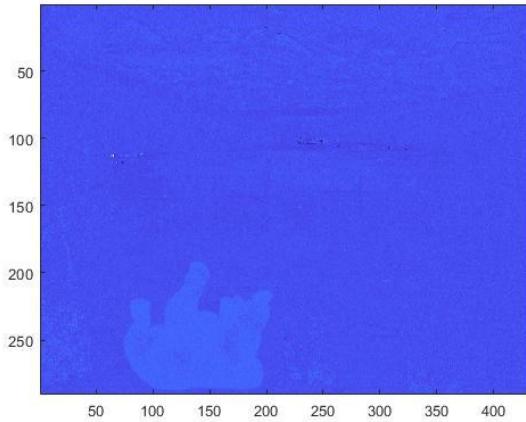
Results

Test Image 4 via CFA



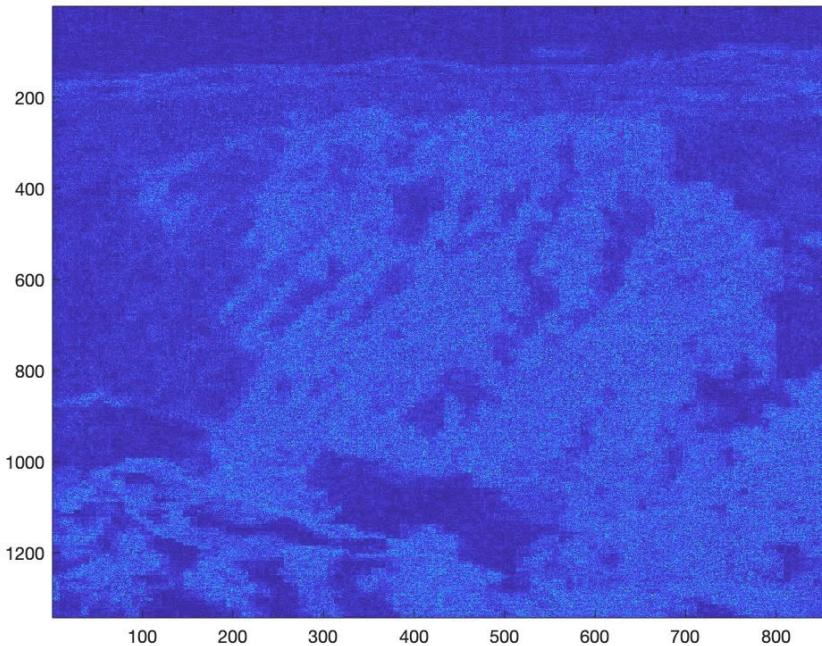
Results

Test Image 5 via CFA



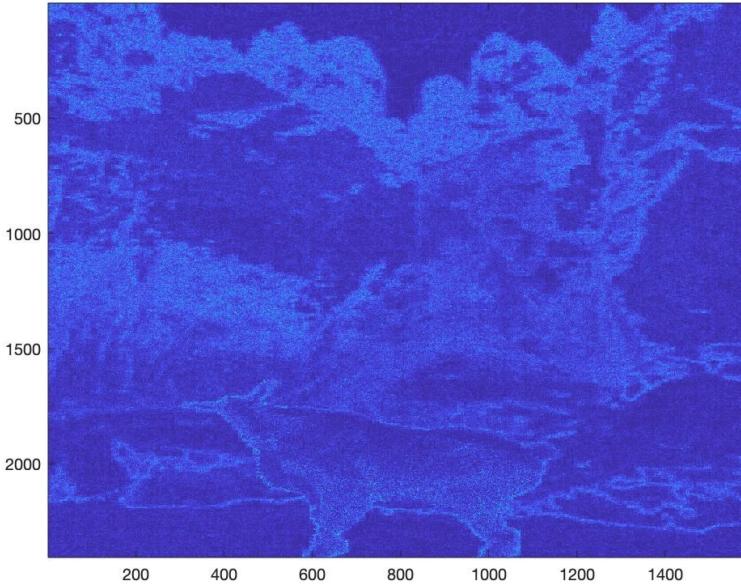
Results

Test Image 6 via ELA



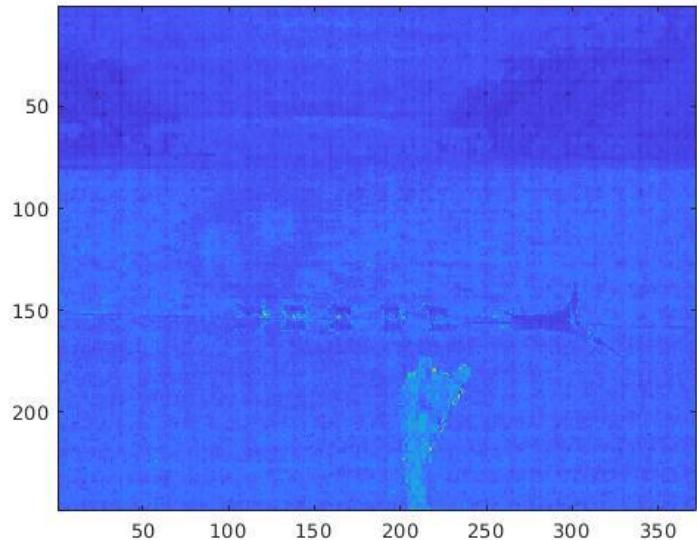
Results

Test Image 7 via ELA



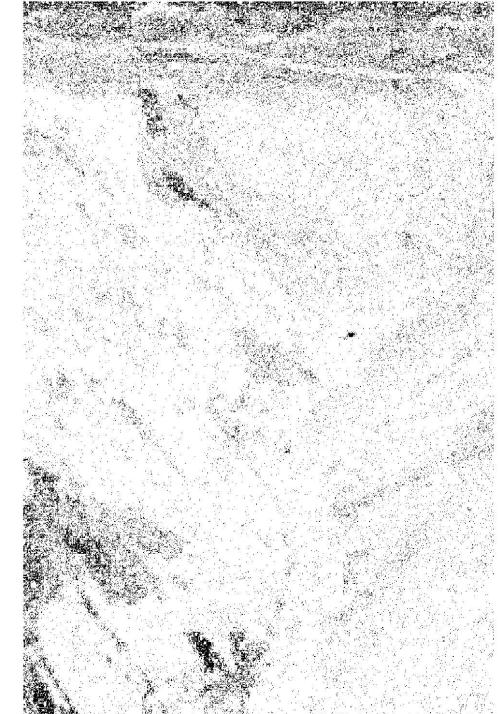
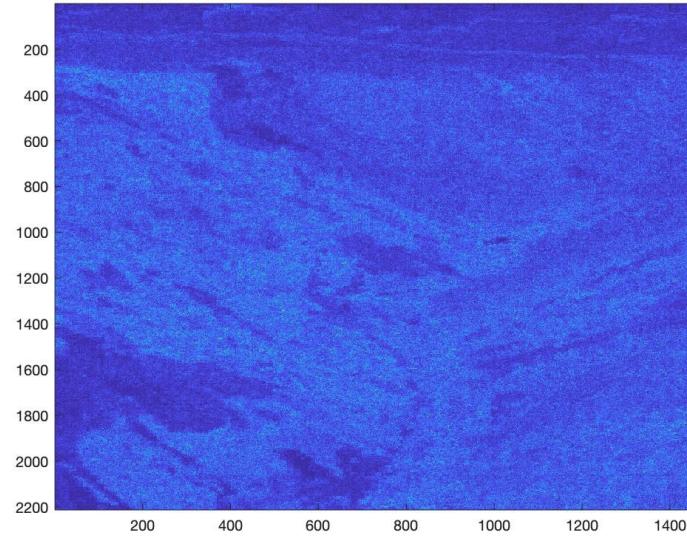
Results

Test Image 8 via CFA



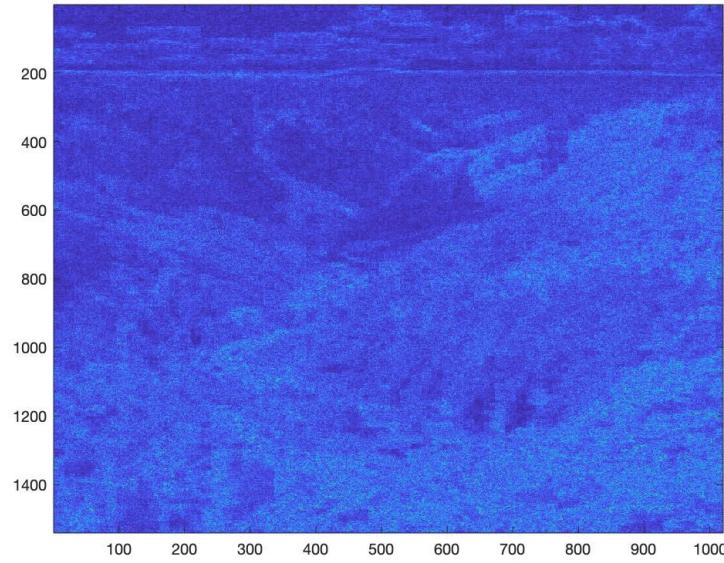
Results

Test Image 9 via ELA



Results

Test Image 10 via ELA



Reference

- [1] A. Dirik and N. Memon, *Image Tamper Detection based Demosaicing Artifacts*, 2009 16th IEEE
- [2] <http://fotoforensics.com/>