Image Tampering Detection

Fahad Wahid - fwahid@hawk.iit.edu
Shan Shazad - sshazad@hawk.iit.edu
IIT School of Applied Technology

Introduction

- The purpose behind this project is to accurately determine whether a digital image has been tampered.
- Image processing programs, such as PhotoShop, making it more easy to create image forgeries from one or more images.
- In order to deal with forgeries of different nature
  - **Cloning, Splicing, Resampling**
- We use techniques based on Photo Response Non Uniformity (PRNU) noise, which deal uniformly with all these attacks.

Scope

- *The **main objective** of this project is to find a Digital Image Forgery Detection tool, and develop it further on how it should detect image tampering.*

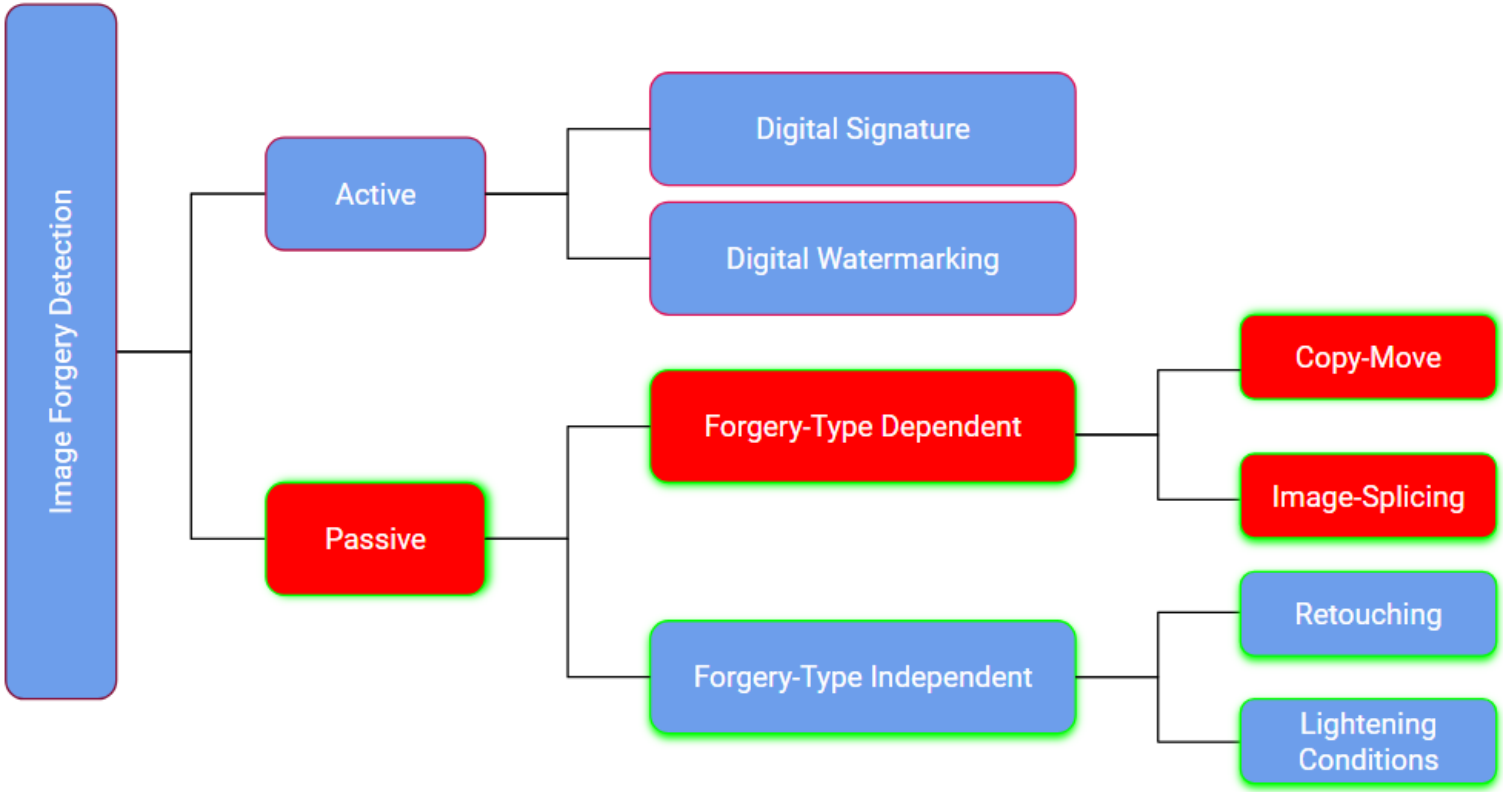
- *Determine whether a digital image has been tampered using passive forensic techniques (**blind**).*

Starter Project Reference

- *GRIP is a Image Processing Research Group of the University Federico of Naples.*
- *Main focus concerns image segmentation, denoising, image coding, and digital forensics*

www.grip.unina.it

Passive vs Active Image Tampering



What is PRNU?

*(**Photo-response non uniformity**) uses areas that looks imperfect and helps to form imaging sensor. Physical differences give a unique sensor pattern.*

Most common forms of image forgery, like copy-move or splicing, delete the original camera PRNU from the target region

- Unlike with most other approaches, the detection of tampering is based on the absence of the fingerprint, hence does not depend on the specific type of forgery.

- PRNU pattern is fairly robust to several common forms of image processing, such as JPEG compression, filtering, or gamma correction

Bayesian Example

fig.1

fig.2

1. Pristine image

2. The first mask, obtained for the genuine image, is used to compute the false alarm probability, as the ratio between the number of pixels declared forged (in red) and the image size.

fig.3

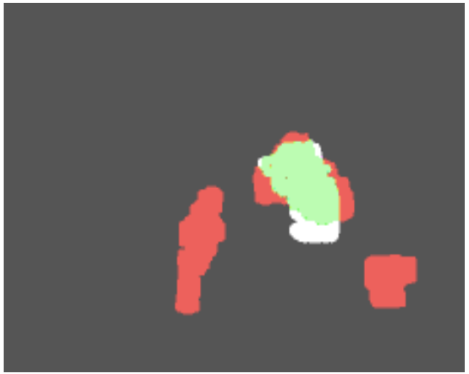
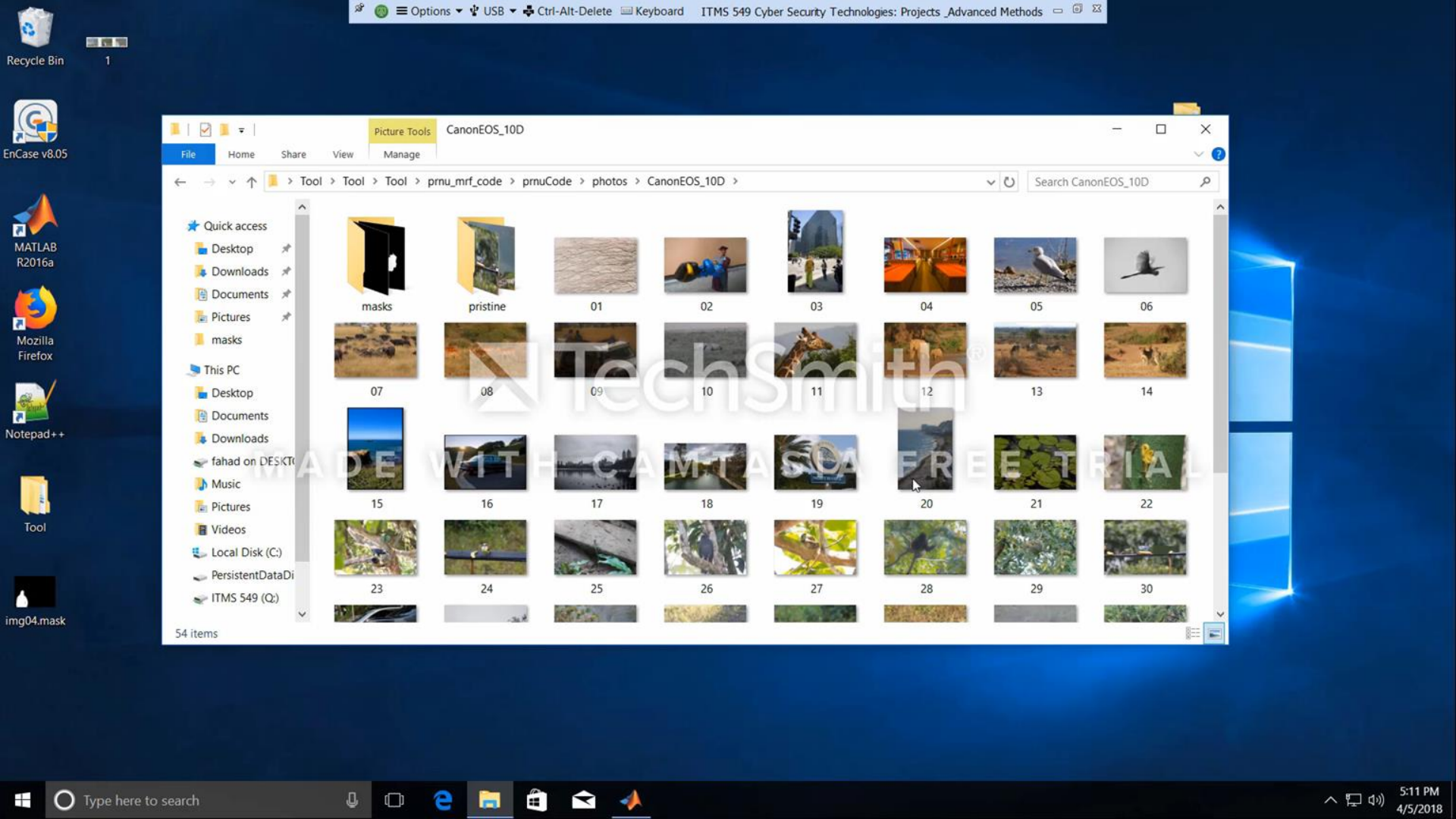


fig.4

***3.* Tampered image**

4. The second mask, obtained for the forged image, is used to compute the detection probability, as the ratio between the number of correctly identified forged pixels (in green) and the forgery size (white + green).


Options
USB
Ctrl-Alt-Delete
Keyboard
ITMS 549 Cyber Security Technologies: Projects _Advanced Methods
Recycle Bin
1
EnCase v8.05
MATLAB R2016a
Mozilla Firefox
Notepad++
Tool
img04.mask
Picture Tools
CanonEOS_10D
File
Home
Share
View
Manage
Tool › Tool › Tool › prnu_mrf_code › prnuCode › photos › CanonEOS_10D ›
Search CanonEOS_10D
Quick access
Desktop
Downloads
Documents
Pictures
masks
This PC
Desktop
Documents
Downloads
fahad on DESKTO
Music
Pictures
Videos
Local Disk (C:)
PersistentDataDi
ITMS 549 (Q:)
masks
pristine
01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
54 items
TechSmith
MADE WITH CAMTASIA FREE TRIAL
Type here to search
5:11 PM
4/5/2018

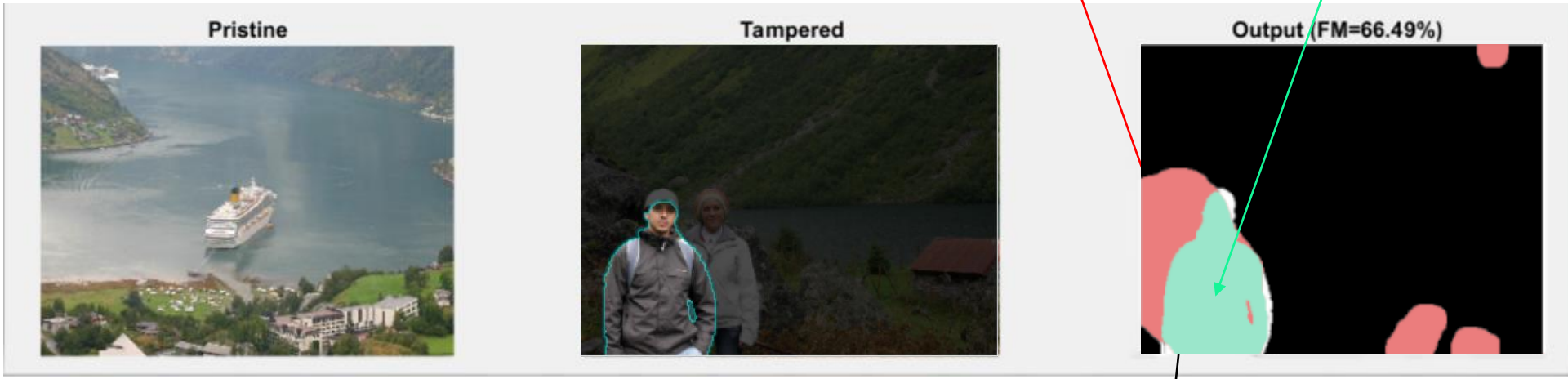
Approach

- *Collect the clean Images and tampered images on splicing and copy-move techniques.*
- *Use Bayesian MRF (Markov Random Fields) approach for PRNU based image forgery detection.*
  - *Compare Original and Tampered image.*
  - *Predict correlation index field with noise.*
  - *Again predict correlation index using BM3D (Block-matching and 3D filtering) denoising algorithm.*
  - *Color coded detection mask provided by Bayes-BM3D.*

Output

Predict correlation index field with noise.

Bayes-BM3D

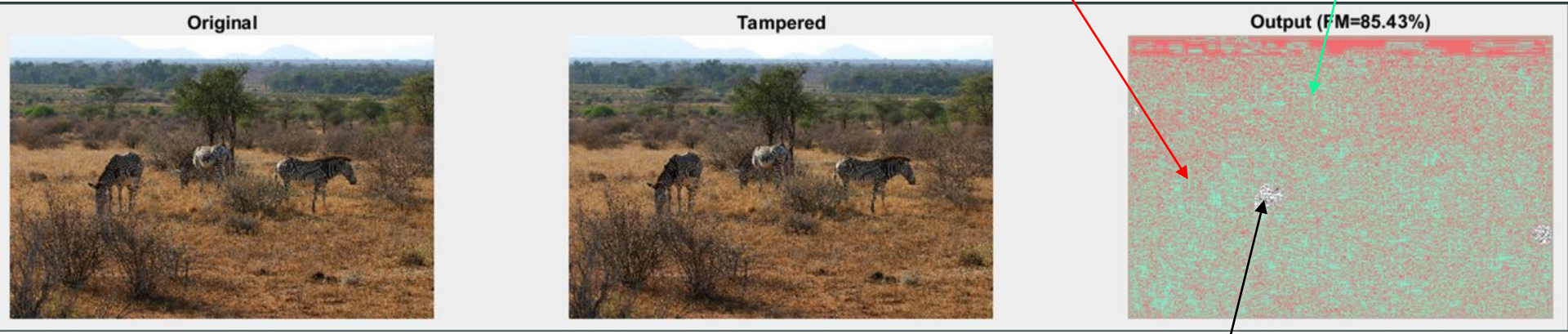


The white color indicates that this part of the image has been tampered/modified (mask)

Output

Red color shows genuine pixel declared tampered (false positive)

Green color indicates tampered pixels declared tampered



The white color indicates that this part of the image has been tampered/modified.

$$FM = \frac{2\,TP}{2\,TP + FN + FP}$$

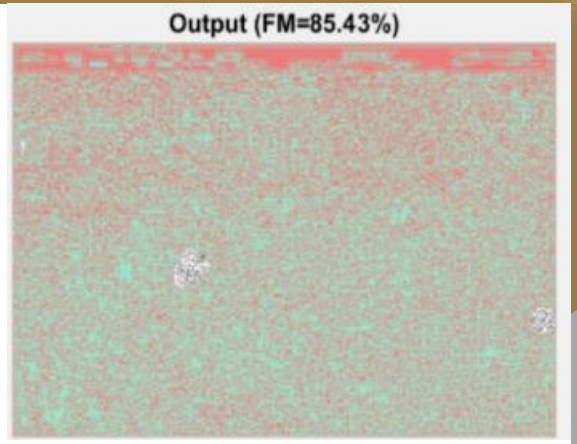
Where:

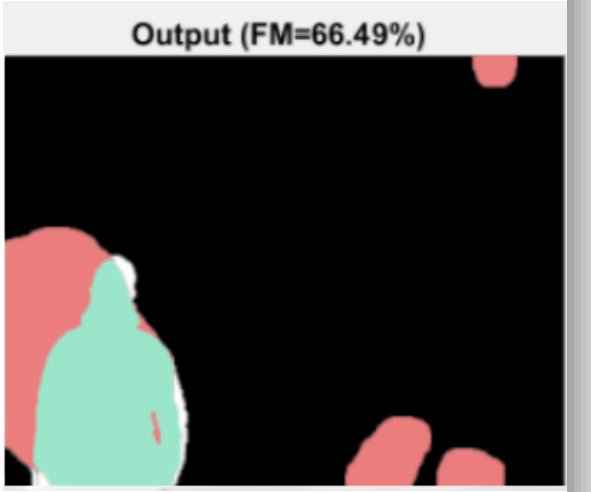
FM means F-measure

TP means the number detected forged pixels (**true positive**)

FN undetected forged pixels (**false negative**)

FP wrongly detected genuine pixels (**false positive**)





How is the mask generated?

- **The created mask uses a 3x3 block size which is the best size for capturing the trends in an image without introducing too much pixel variation.**

$$\begin{bmatrix} -1 & -2 & -1 \\ -2 & 12 & -2 \\ -1 & -2 & -1 \end{bmatrix}$$

- **The weight of 12 is placed on the center pixel along with all other neighbors' weights summing to -12.**
  - **Filters out all areas in an image that are similar and magnifies those that vary greatly.**

Experiment of Test Images

- All test images have the same size of 768 × 1024 pixels, and are cropped from the same region of the original images output by the camera.
- For each test image we consider both the genuine version, used to look for false positives, and a forged version, used to look for correct detections.
- Test of images were conducted on a CanonEOS_10D

Results

CLONING

43.87%

- 67 IMAGES
- PHOTOSHOP USED TO TAMPER

SPLICING

68.25%

- 67 IMAGES
- PHOTOSHOP USED TO TAMPER

RESAMPLING

90.65%

- 67 IMAGES
- PHOTOSHOP USED TO TAMPER

Conclusion

- **The tool needed original tampered image in order for the tool to detect any tampering**
- Modified the script to run the detection algorithm without having to need the original image
- Implemented script to generate mask
- Tested over 200 images that were pristine and tampered them using the passive forensic technique
- F-measure : Cloning < Splicing < Resampling

Thank you

Any Questions?