Lab 1
Rules and Virtual Env

Andrea Montibeller

UNIVERSITY
OF TRENTO

Profile Presentation

Andrea Montibeller, PhD
andrea.montibeller@unitn.it

Research Interests

1. Camera Source Attribution
   (Detect the device used to capture an image or a video)
2. Image DeepFake Detection
   (Is this image real or generated by an AI?)
3. Video DeepFake Detection and Localization
   (Is this video real or generated by an AI? If fake, the whole video was generated or just a specific region of it?)
4. Adversarial Multimedia Forensics
   (Study methods able to “break” algorithms of point 1, 2, and 3)

Guidelines and Suggestions

1. If you have any questions, please ask them during class. ALL questions are valuable and you are all here to learn.
2. If something is not working, DO NOT wait a few days before the challenge to ask for help.
3. Chatting in class with other students during class, if you are not whispering, is not allowed.
4. When you send mails with questions, be exhaustive
5. If you have questions on the challenge rules, ask them in class so anyone can listen.
6. If your teammates are not working, report them.

Lab 1
Capture the Mark Rules

Andrea Montibeller

UNIVERSITY
OF TRENTO

Capture the Mark Rules

A Few Notes:

1. Rules are here to be followed
2. Not following the rules means being penalized
3. Grey areas in rules are possible, but you can exploit them at your own risk.

Read and Learn the Rules Here

Rules Summary

- **Groups of 3/4 people**
- **Embedding code features**: invisibility and robustness
- **Embedding code CAN'T** print, open pop-up windows.
- **Embedding code inputs** are: full path to the image, full path to the watermark. The **ONLY output** is the watermarked image
- **Detection code features:** NO PRINT, NO POP-UP WINDOWS, MUST RUN in 5 seconds MAX
- **Detection code inputs/outputs**. **INPUTS** path to original image, path to watermarked image and path to attacked watermarked image. **OUTPUTS** decision on watermark detection (1/0), WPSNR
- **DETECTION CODE CANNOT FIND THE WATERMARK IN A NON-WATERMARKED IMAGE OR DESTROYED IMAGES (WPSNR<25) (CHECK!)**

Rules Summary

- **Code to implement the ATTACKs GOAL: REMOVE the watermark and PRESERVE image quality**
- **Code for ATTACKS:** can use only the attacks seen during the laboratory (you are free to combine them and localize them to specific image regions)
- **Code to implement the ATTACKs CANNOT** use the original image (e.g. the non-watermarked image)
- **Threshold** to be set using the Receiver Operating Curve (**ROC**) code of the laboratories.
- **MAX 3 PCs per-group** the day of the challenge.
- **NO SERVER ARE ALLOWED TO BE USED.**
- **MUST USE THE Virtual ENV given in class**

Lab 1
Virtual Env

Andrea Montibeller

UNIVERSITY
OF TRENTO

Overview

- During all our laboratories we will use Python
- As the server we are using for the challenge uses python ~~3.8,~~ 3.10 you are required to install that version of python on your computer.
- At least one PC per group must run Python ~~3.8~~ 3.10 as the code to detect the watermark must be encrypted the day of the challenge.
- Versions of python different than ~~3.8~~ 3.10 will not be able to run the encrypted detection script.
- <u>You can use CoLab but it is your responsibility being sure that everything runs as it should.</u>