Digital Watermarking - Final Project
Code Documentation

Directories

We organize our code in different directories to ease access.

- copy_attack
- doc
- images
- sandbox
- secure_against_copy_attack
- starting_files
- testing_robustness

Directories which are particular of interest would be **copy_attack**, **secure_against_copy_attack** and **testing_robustness.** The other directories are for documentation, test and initial files.

Running a script

There are two ways to run the script. In terminal;

octave <script-name>

Or inside Octave interactive shell;

run <script-name>

If the system is complaining that a package is missing, install the package by using the following commands inside the Octave interactive shell:

```
pkg install image-2.4.1.tar.gz
pkg load all
```

copy_attack

We put the implementation of a copy_attack in this folder. The images are also located inside this folder. The script involved is **copy_attack.m.** Recovered string, is shown in standard out.

testing_robustness

In order to test whether, the watermarking system is robust against normal transformations, we have prepared several different scripts:

- text2png_averaging_filter.m
- text2png_cropping.m
- text2png_jpg_compression.m
- text2png_noise.m

Each script should be run separately and each script will create new output images.

secure_against_copy_attack

This is the implementation of our secure watermarking. A lot of the functions are separated in different files. To run the embedding in its entirety, run the script **secure_against_copy_attack.m.** The results would be shown in the standard out.