# Selected Topics

### 20 Feb 2020 (Digital Forensics)

#### Digital Forensics

Digital Forensics is regarding all the possible actions describing manipulation of multimedia digital objects. In the field, there are very very specific specializations.

#### Methodology can be Active or Passive

Active is considered requiring some sort of altering or manipulation of the digital media (i.e: cryptography, etc) and you require an entire cryptographic structure. Watermarking would fall under the active method, and can be thought of as fragile or robust, depending on whether compression affects the watermark)

Passive is considered not altering or manipulating the digital media, but instead, comparing the source identification, as well as the integrity of the media.

Therefore it is clear from the description that these two things solve slightly different problems or concerns within the field.

#### Digital Media has digital fingerprints

This concept is akin to the traditional modes of forensics, which thinks about how human beings leave behind traces, such as fingerprints that identify themselves in an act. This concept applies in a way to digital media through the concept of camera lenses as well as other factors. The digital fingerprint is broken down into three categories:

1. In-camera fingerprints (this would be your lens imperfections, etc)

2. Out-camera fingerprints (this would be your post-processing signature, etc)

3. Geometric (scene) fingerprints (this would be the physical environment, lighting, shadows, reflections, abberations, etc)

#### Image Acquisition can be broken down into eight parts

We can think about this image acquisition process, and identify how we can analyze it.

1. Light projection to some sensor

2. mapping values from sensors -> digital process

3. adjusting signals

4. filters to account for colors

5. interpolation/demosaiking

6. color correction/gamma correction

7. sharpening/post-processing

8 storage of images

#### Different sensors (cameras) have different unique properties

We can break these properties down by the noise level:

1. Fixed Pattern Noise (this would be due to micro-imperfection of the lenses, causing dead pixels etc... on a scale of a 100 megapixel camera, it is almost impossible to replicate the imperfections exactly.)

2. Photo-response non-uniformity (this is more like sensors not responding to the environment in exactly the same way, meaning that certain pixels may have slightly different representations between sensors. If you think about the pixels or sensors as buckets, uniform light should yield uniform buckets, but this is of course not the case)

#### We can detect manipulation through a concept of a “double compression”

In the photo world, there is a lot of JPEG images, and that involves some sort of compression. If we can detect double compression, that would mean that our images have been saved originally (compressed), and then manipulated and saved again (compressed again). This could be detected when there is a mismatch or desync of the blocks that we expect (8x8 in JPEG compression usually), and this could be used to detect copy and paste manipulation.