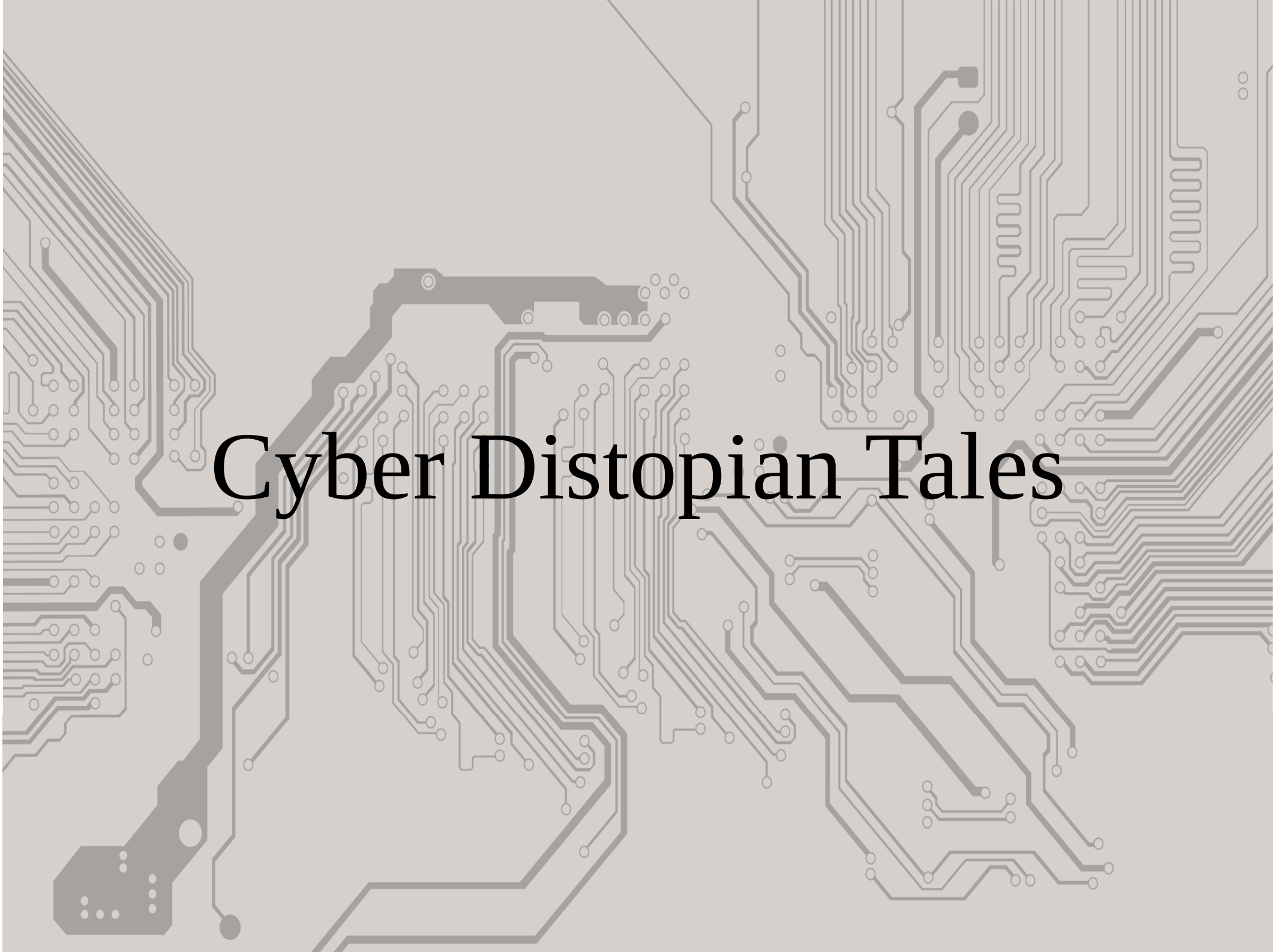

Cyber Distopian Tales

Miguel Mota Veiga

- Senior Security Consultant @ Fortconsult (part of NCC Group)
  - Penetration Testing, Physical Security, Social Engineering + Incident Response, Forensic and Malware Analysis
  - mve@fortconsult.net
- Traveler, Backpacker and Geocacher
- Crypto-Anarchist by default
- Dystopian Novels & Beer lover

Cyber Dystopia

- Carnivore, implemented by FBI around 1997
  - Packet Sniffer installed in the Americans ISP. It main objective was to capture email messages
- DCSNet, FBI point and click system
  - Used to instant wiretap US cellphones/landlines
- ECHELON, beginning of the 70's (US DoD)
  - Used to capture satellite, microwave communications (SIGINT)
- PRISM, NSA surveillance program
  - XKEYSCORE, FoxAcid, QUANTUM, TAO

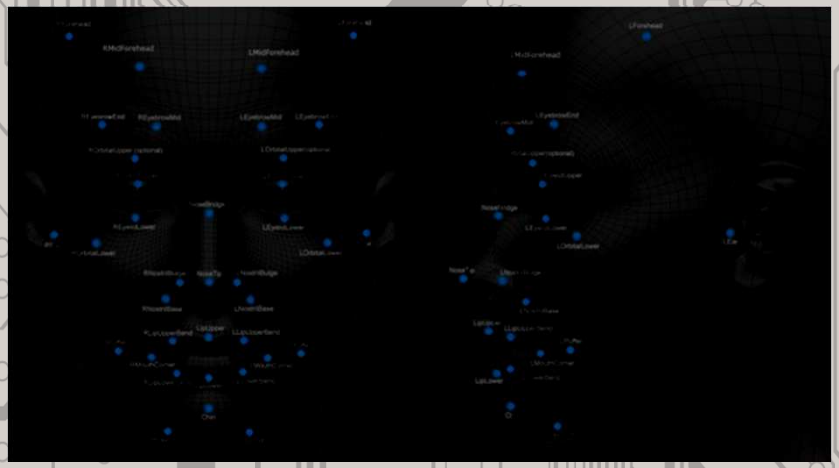
Cyber Dystopia

More info at:

–Cryptome.org

–Wikileaks.org

Facial Recognition



- What is it?
- How it works?
  - Face Detection
  - Face Tracking
  - Face Recognition
- Building systems;
- How can we defend against it?

What is it?

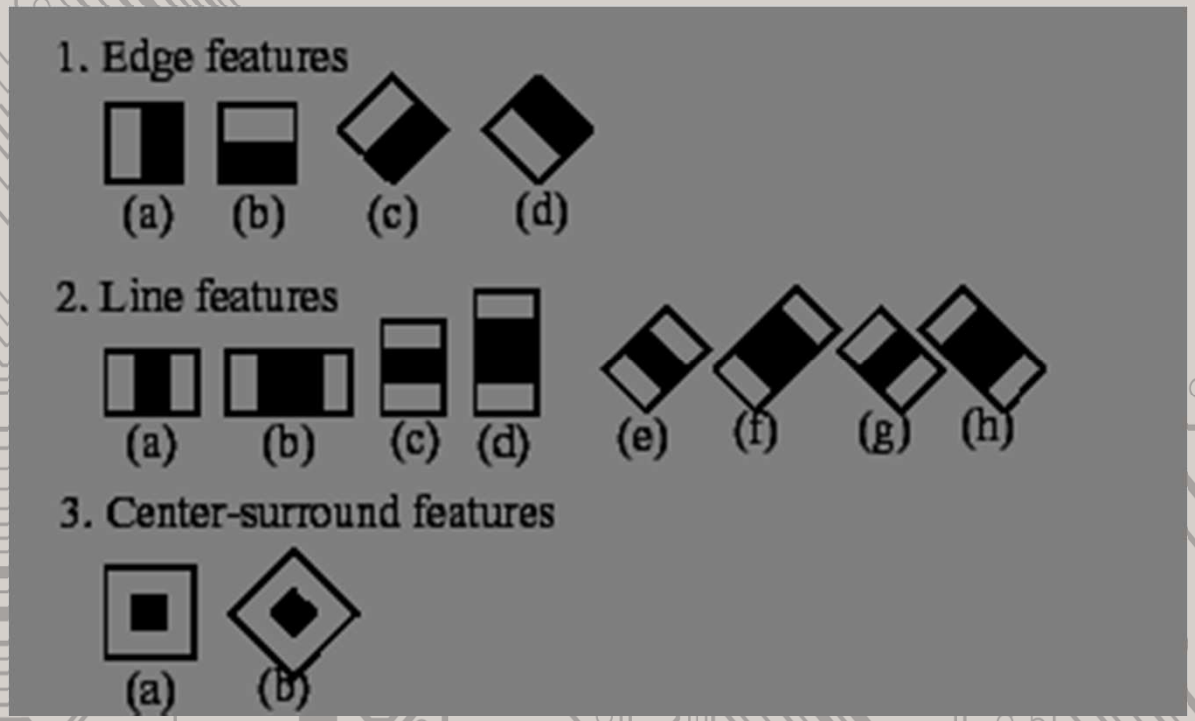
“A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database.

It is typically used in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems.” - Wikipedia

Haar Cascades – Adam Harvey

How it works?

Haar Cascade

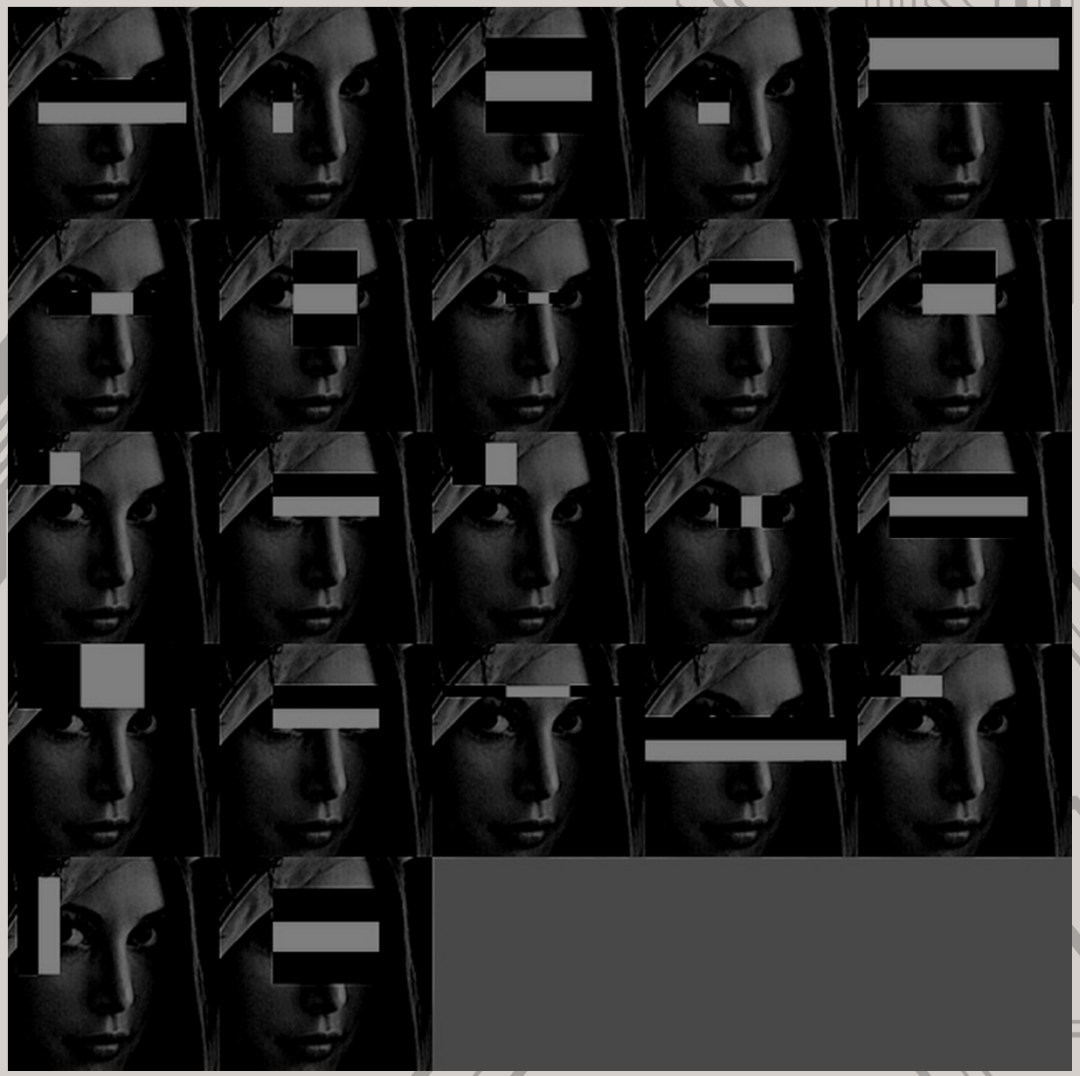


- What is it?

–A “cascade” is a series of Haar like features that combined, form a classifier

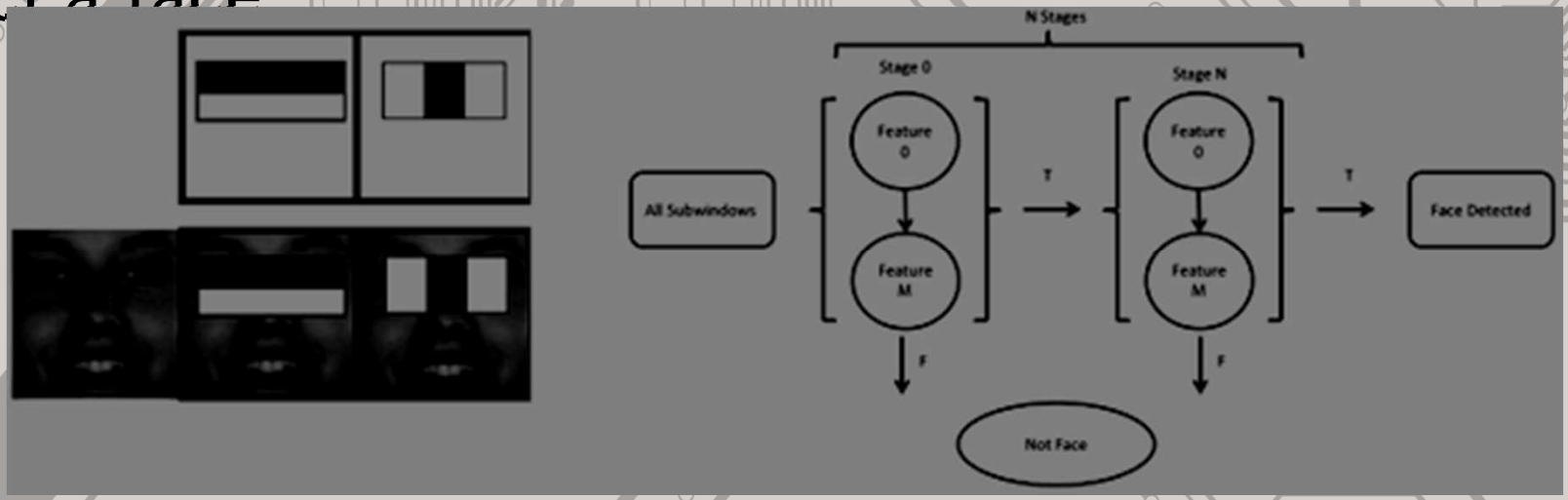
- What is a Haar like feature then?

Haar Cascade



Haar Cascade

- A single identifier is not enough
  - They are called “weak identifiers”
  - Haar cascade consist of a series of weak classifiers
  - They need to pass a series of classifiers in order to detect a face

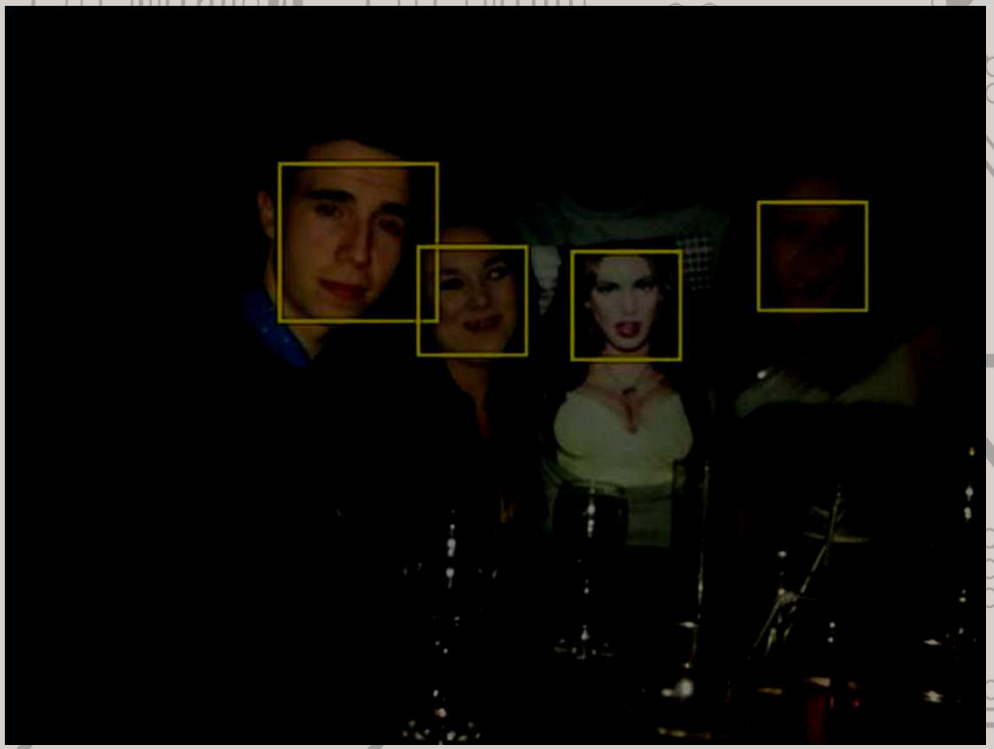


Advantages

- Extremely fast
- Scalable
- Can be used to detect any objects

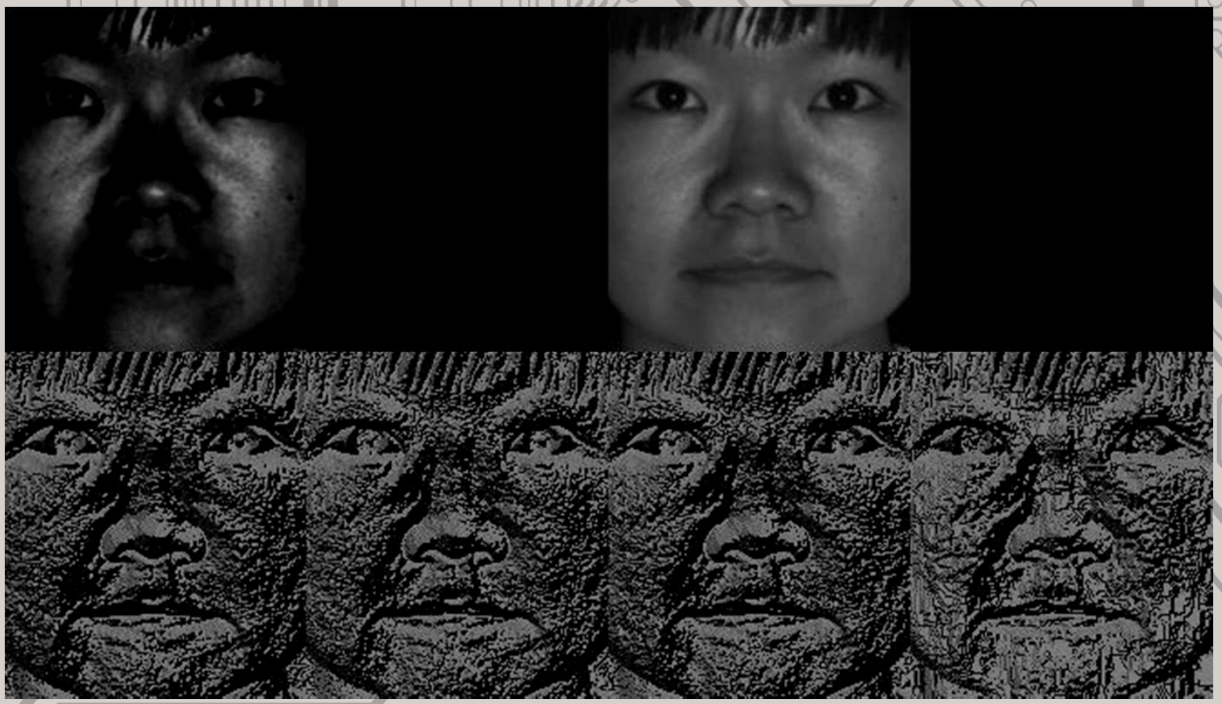
Disadvantages

- Mostly effective on frontal images/faces
- Not color friendly
- Work better in plain background areas



Local Binary Patterns

- Divide the image in blocks (16x16 pixels)
- Search in the neighborhood the value of each pixel
- We have our patterns



Facial Recognition for the Masses

Public Data

–Social Networks

Private Data

–ID cards

–Passports

–Driver licence

Facial Recognition for the Masses

Public Data

- (Semi-)Legal
- Low quality of photos
- Public Data
- Fairly easy to acquire
- http://graph.facebook.com/$i/picture?type=large

Private Data

- Illegal to acquire
- High quality of photos + Name
- Well, is private...
- How to aquire it? Grab in from the private network of Casa da Moeda? (Out of the question)

Facial Recognition for the Masses

- We are going to mass scan Facebook
- The more “legal” option
- Large database of photos and names
- Easy how to automatize the task
- Use TOR ;)

Facial Recognition for the Masses

```
Use LWP::Simple;
for ($i=1; $i < 99999999999999999; $i++){
    if (is_success (getstore
"http://graph.facebook.com/$i/picture?type=large", count)){
        print "[+] User ID $i FOUND\n";
        system ("wget -q
http://graph.facebook.com/$i/picture?type=large -O $i.jpg -q");
        }
    }
```

(Yes, I am using system(). I like to live on the edge)

DEMO

http://bit.ly/1JqIwEq

How to protect

- Mask, Hoodie, sunglasses and hats or other basic face covering
  - Masks are illegal
- Fooling cameras
  - Dracula teeth, fake nose, facial paint on points of interest
- Starting on Meth? :)

TODO List

- Port python scripts to Android / iOS
- Joining it with:
  - Voice detection / recognition
  - Video Analytics
  - License Plates
  - Devices that leak ESSID;


GRACIAS!
Questions?