CyberPhysical systems for Security and Services

UNIVERSITÀ DI SIENA 1240

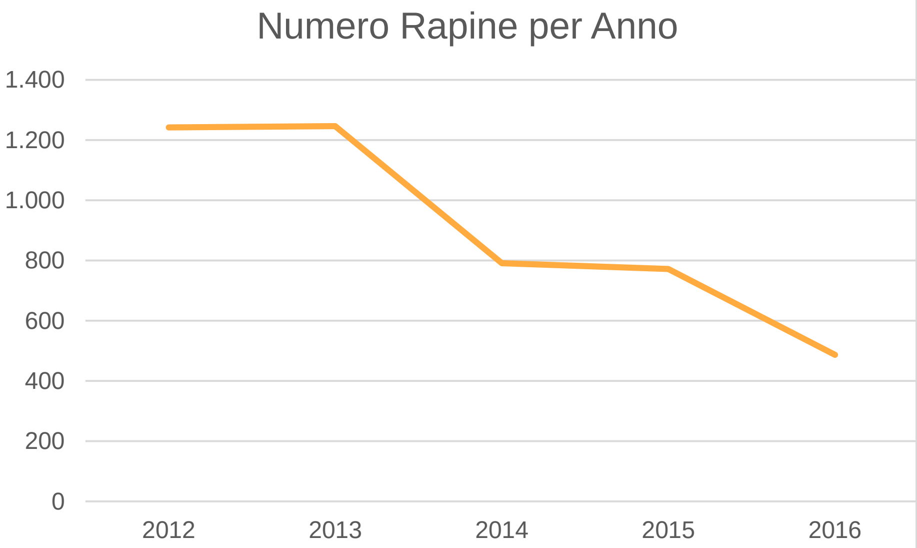
MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

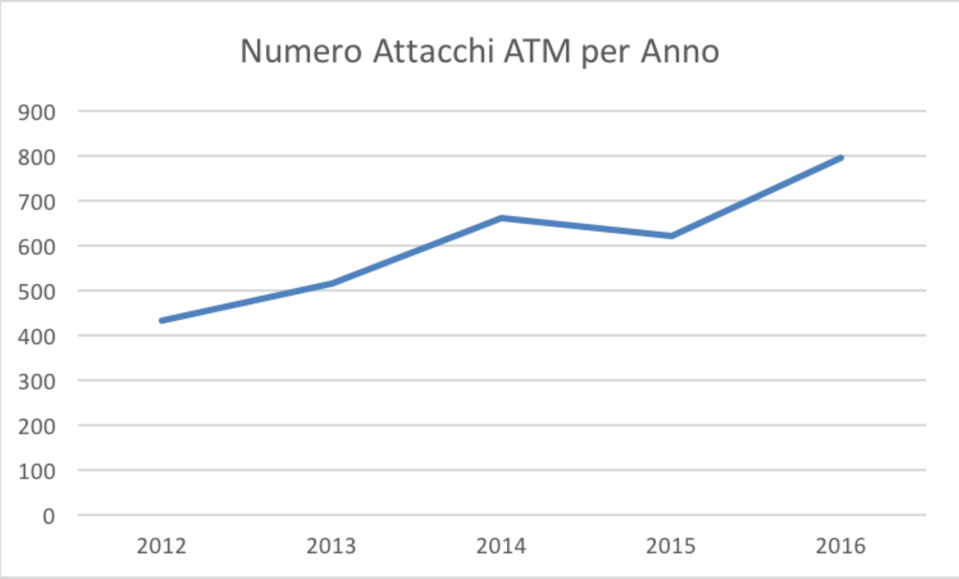
Antonio Rizzo,
Alessandro Rossi,
Francesco Montefoschi,
Giovanni Burresi
Carlo Festucci,
Maurizio Caporali

Siena, 14 Sett 2018

Case of study: ATM-Sense

TREND Rapine vs Attacchi ATM - Fonte ABI 2017





The evolution of **ATM Fraud**

1967

Introduction of the ATM

The cash dispenser is born.

1973

Lloyds Bank

(U.K.) deploys several networked devices.

1991

Five criminals

conduct a series of ATM robberies that involve intentionally causing a machine malfunction and physically attacking the technicians who attended the machine.

Late 1990s

Criminal groups

operating out of Japan improve ram-raiding by using a truck carrying heavy machinery to completely demolish/uproot ATM machines in order to physically steal cash.

2008

10,302 skimming incidents

are reported in Europe.

2009-2010

An unknown gang

of fraudsters make charges of 20 cents to $10 from over a million bank accounts throughout a period of several years.

2013

A group of international

thieves break into an Indian debit card system, lift customers' personal information and use it to steal $45M”

2014

Malware is installed

in a number of aging, European ATM machines.

2015

FICO reports a 546% increase

in ATM fraud cases in US since 2014

2016

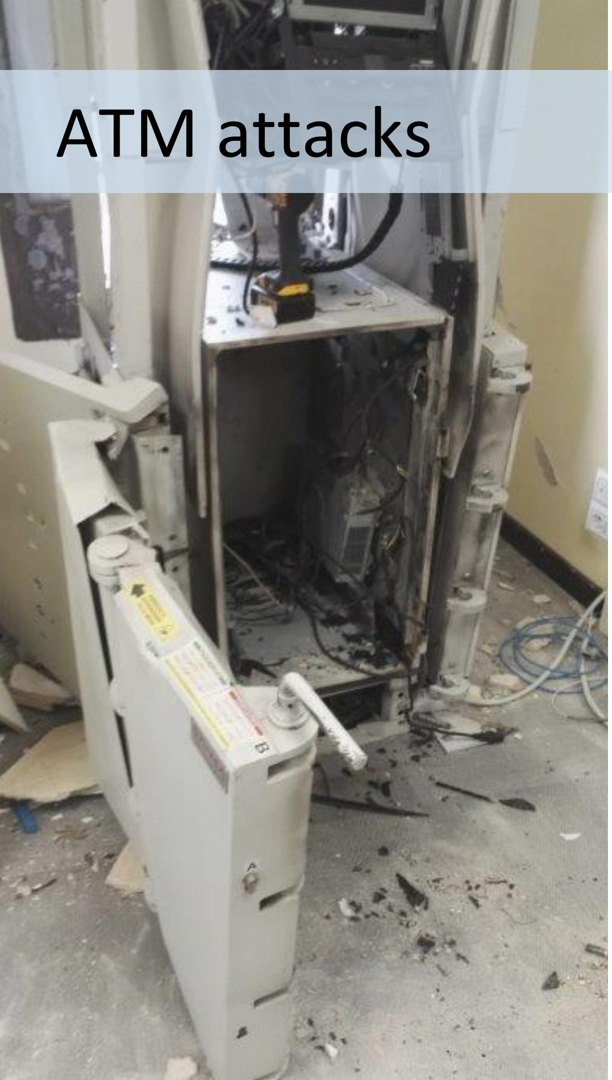
New age of ATM fraud

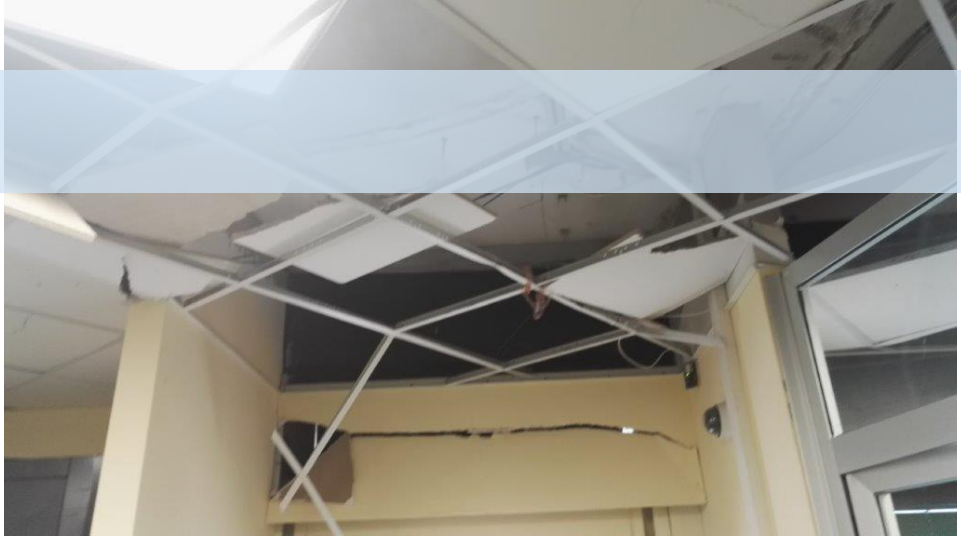
JUNE $13 million is stolen from South Africa's Standard Bank through 14,000 transactions.

JULY ATM machines in Taiwan are suspended after more than $2 million is stolen from 34 First Bank machines at 20 branches.

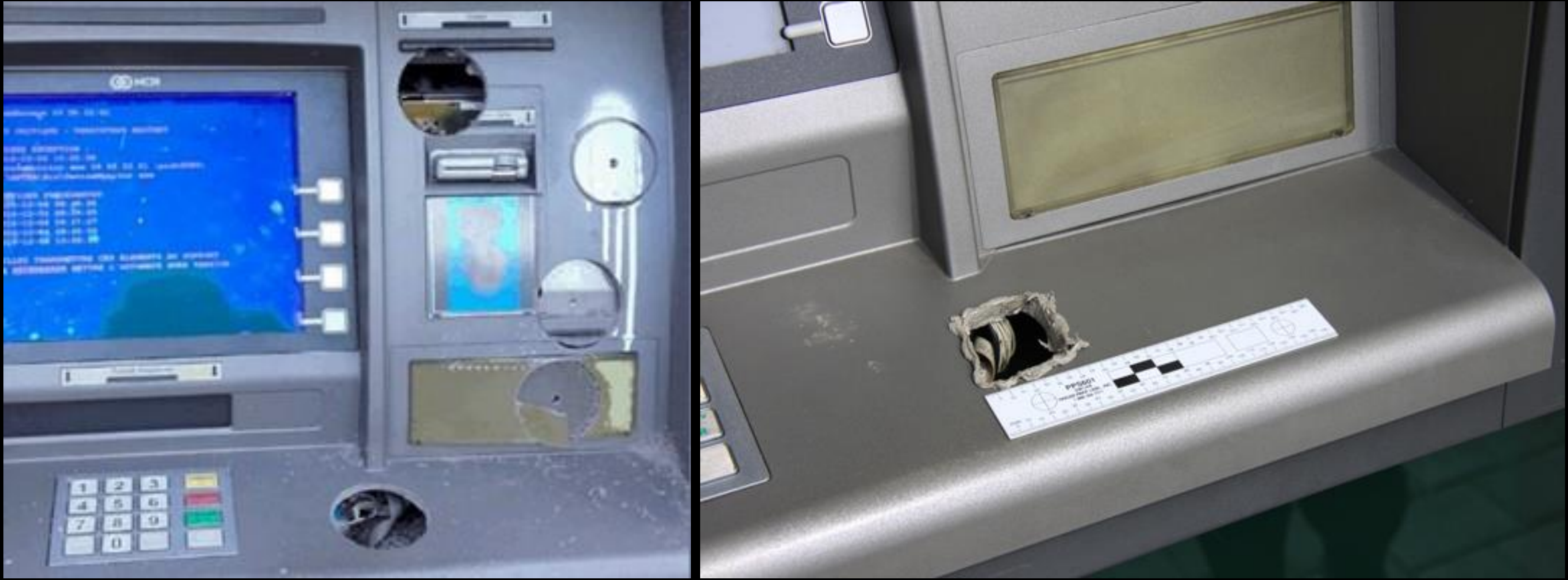
THETARAY

ATM attacks





New Attacks



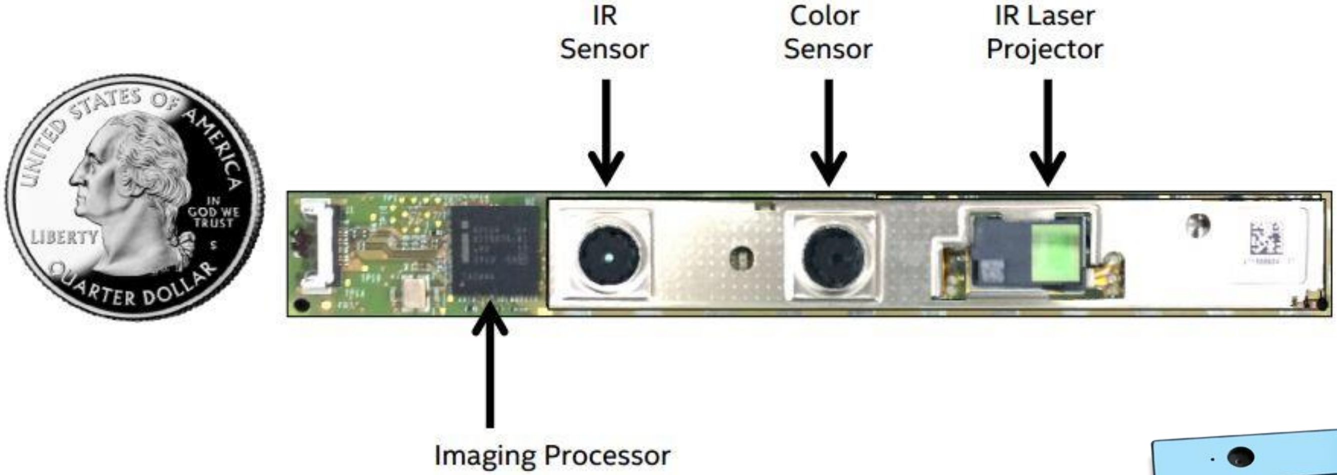
https://www.europol.europa.eu/newsroom/news/27-arrested-in-successful-hit-against-atm-black-box-attacks

Video Surveillance Approach

Intel RealSense Depth Cameras

- **Powerful Open Souce SDK**
- **Easily Embeddable**

intel REALSENSE TECHNOLOGY

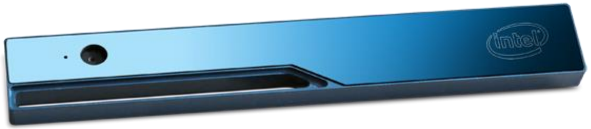


IR Sensor

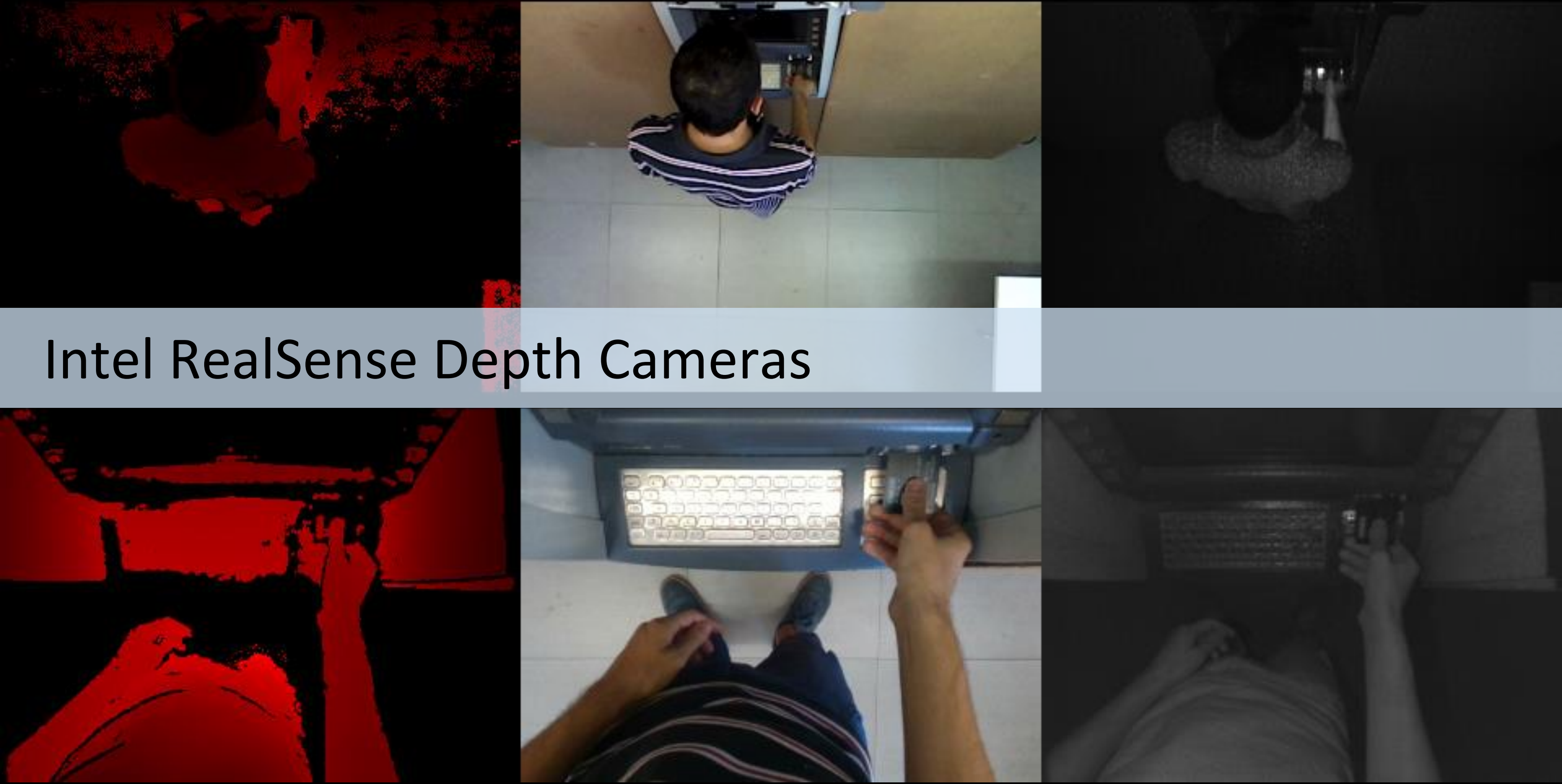
Color Sensor

IR Laser Projector

Imaging Processor



Intel RealSense Depth Cameras



Convolutional Neural Networks

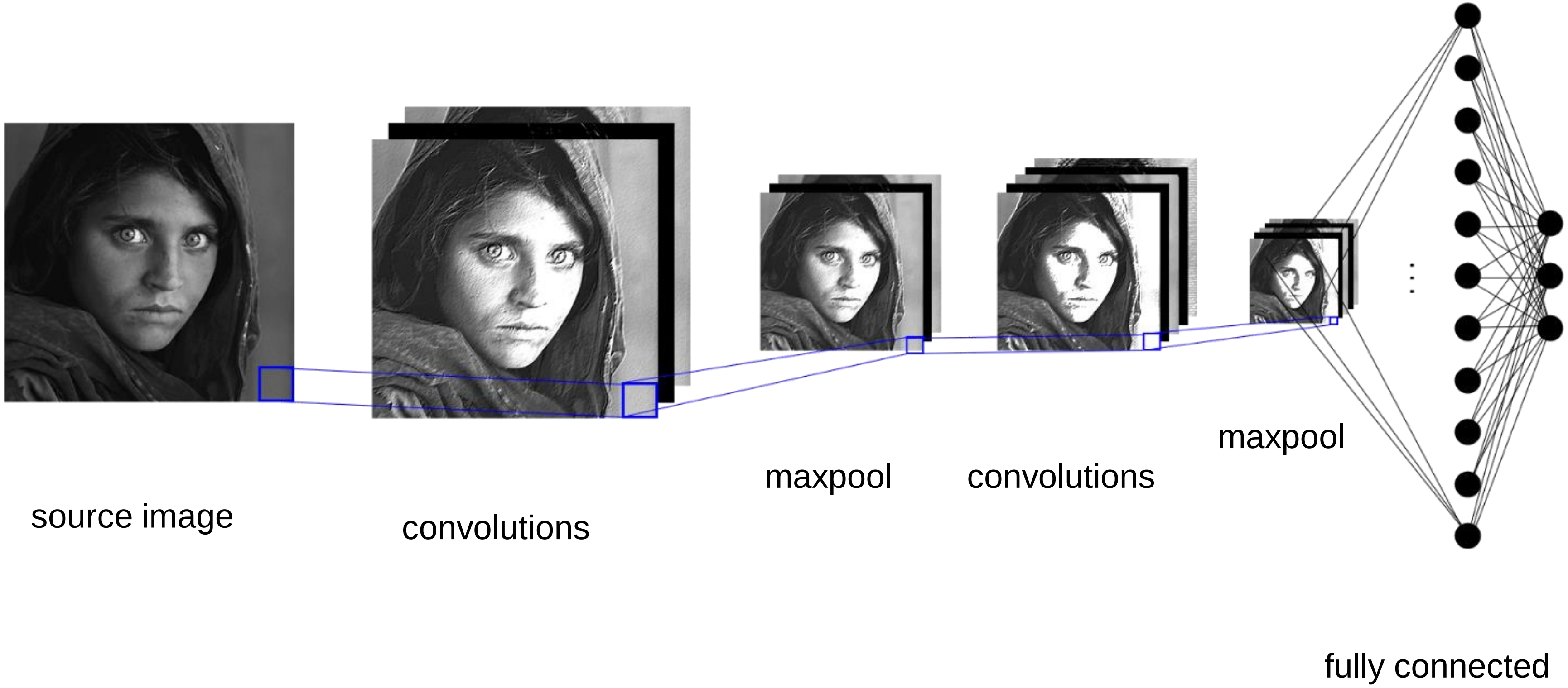


Image Convolutions

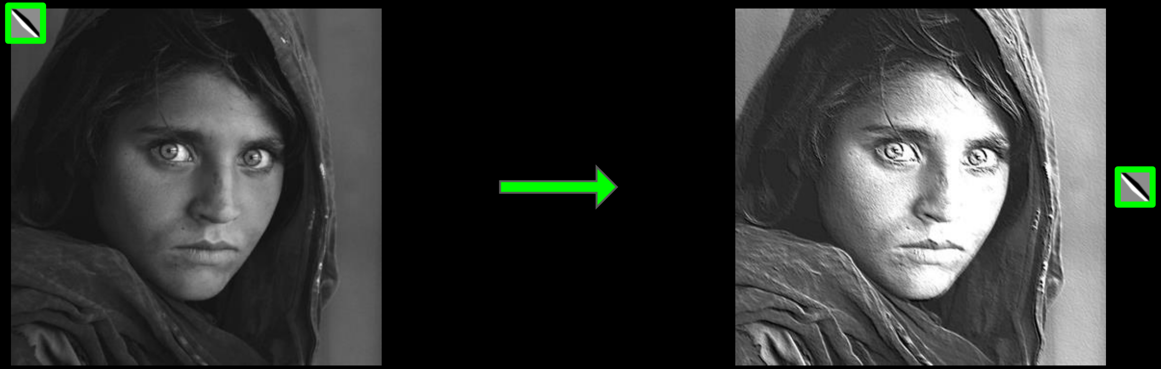


Image Convolutions

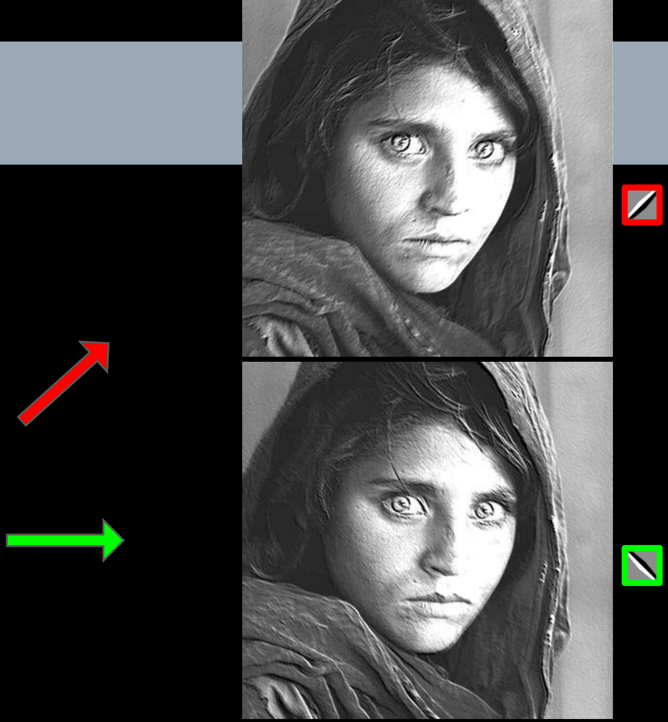
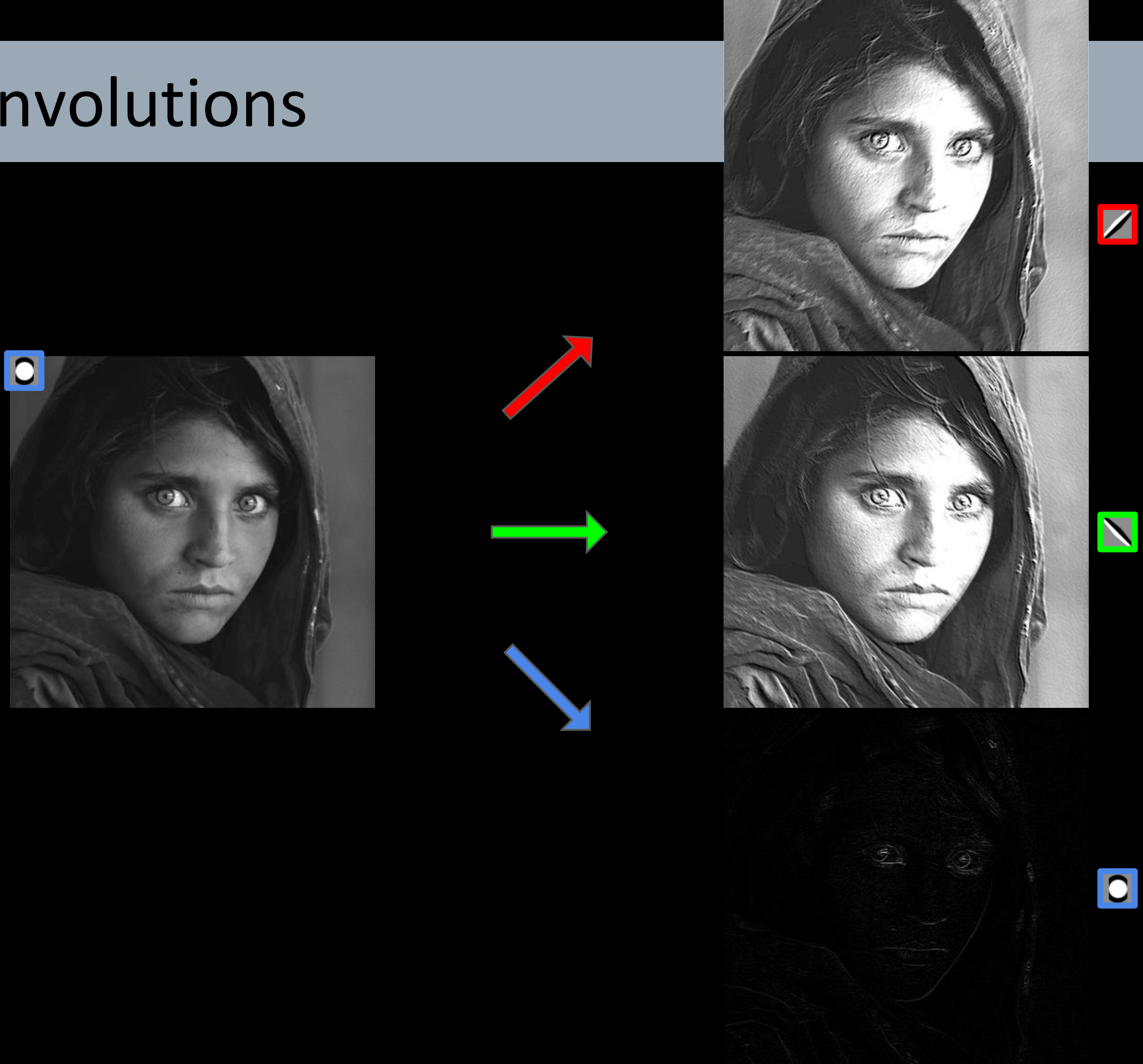
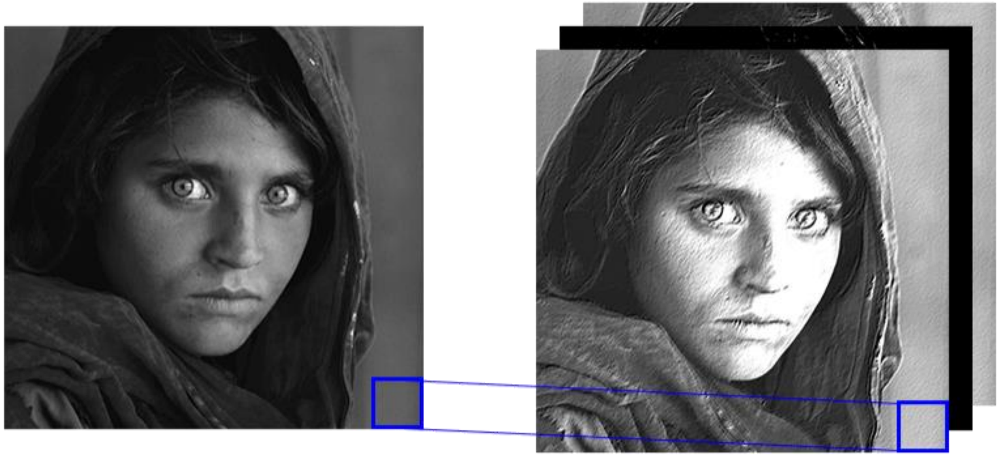


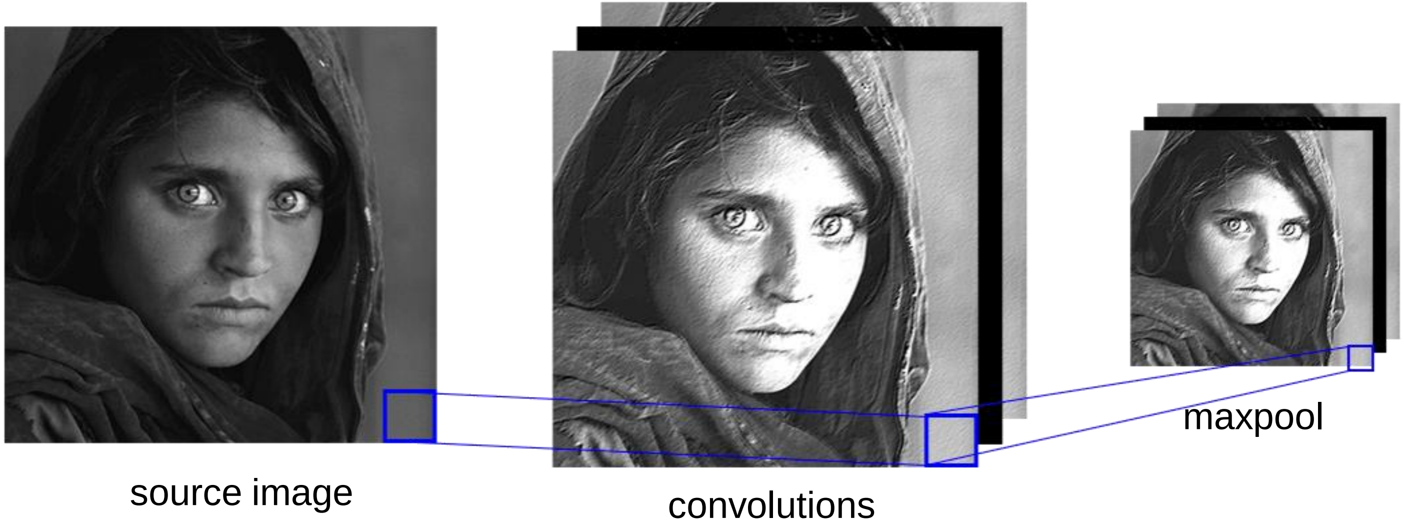
Image Convolutions



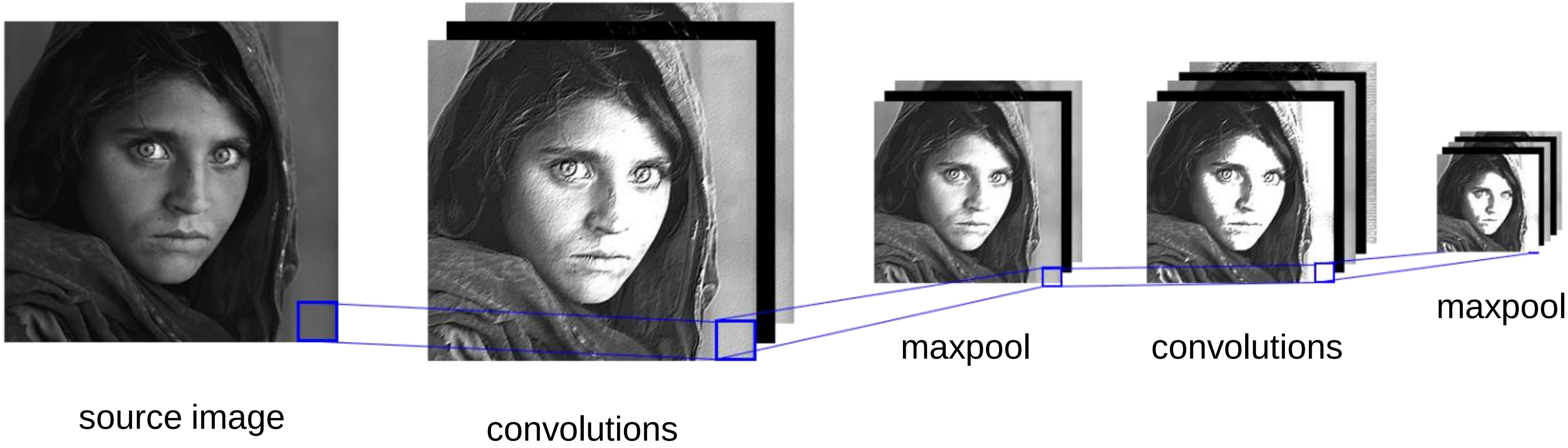
Convolutions



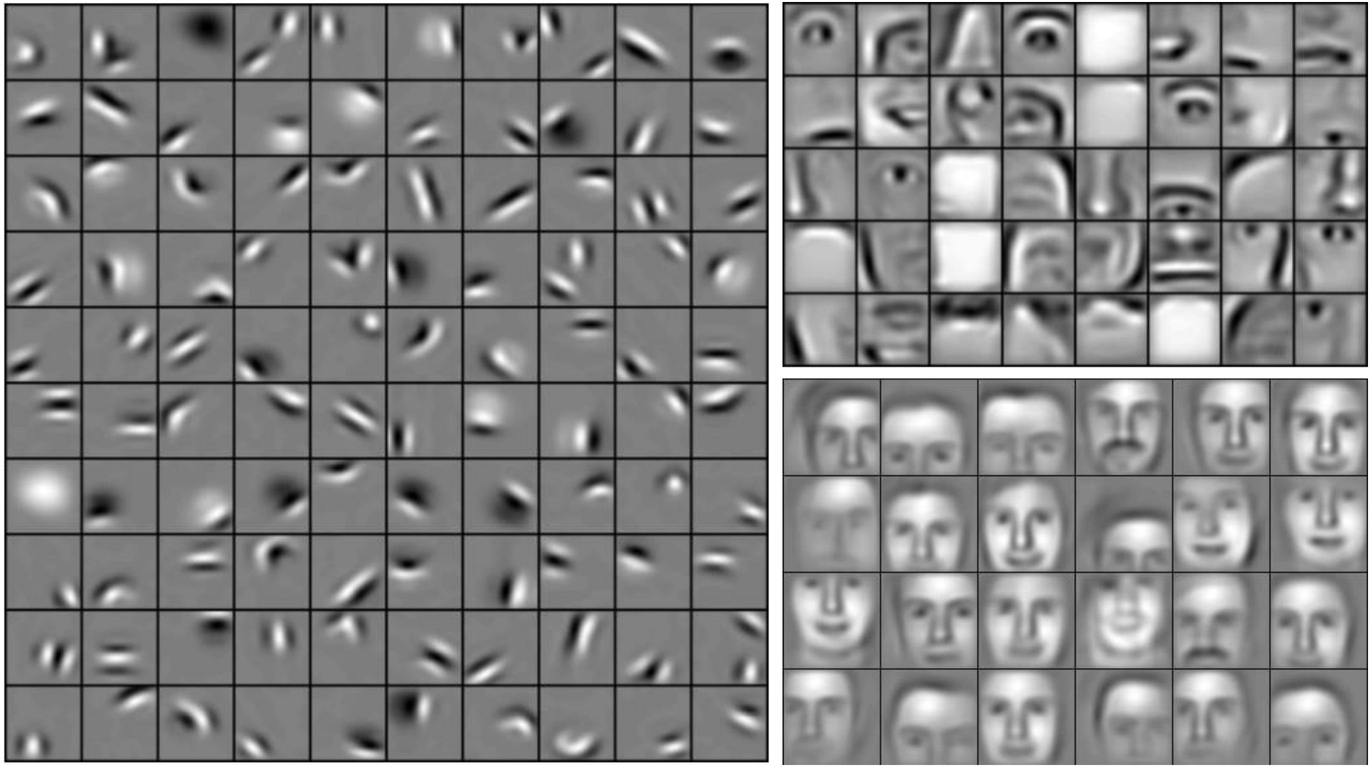
Max Pooling



More layers...



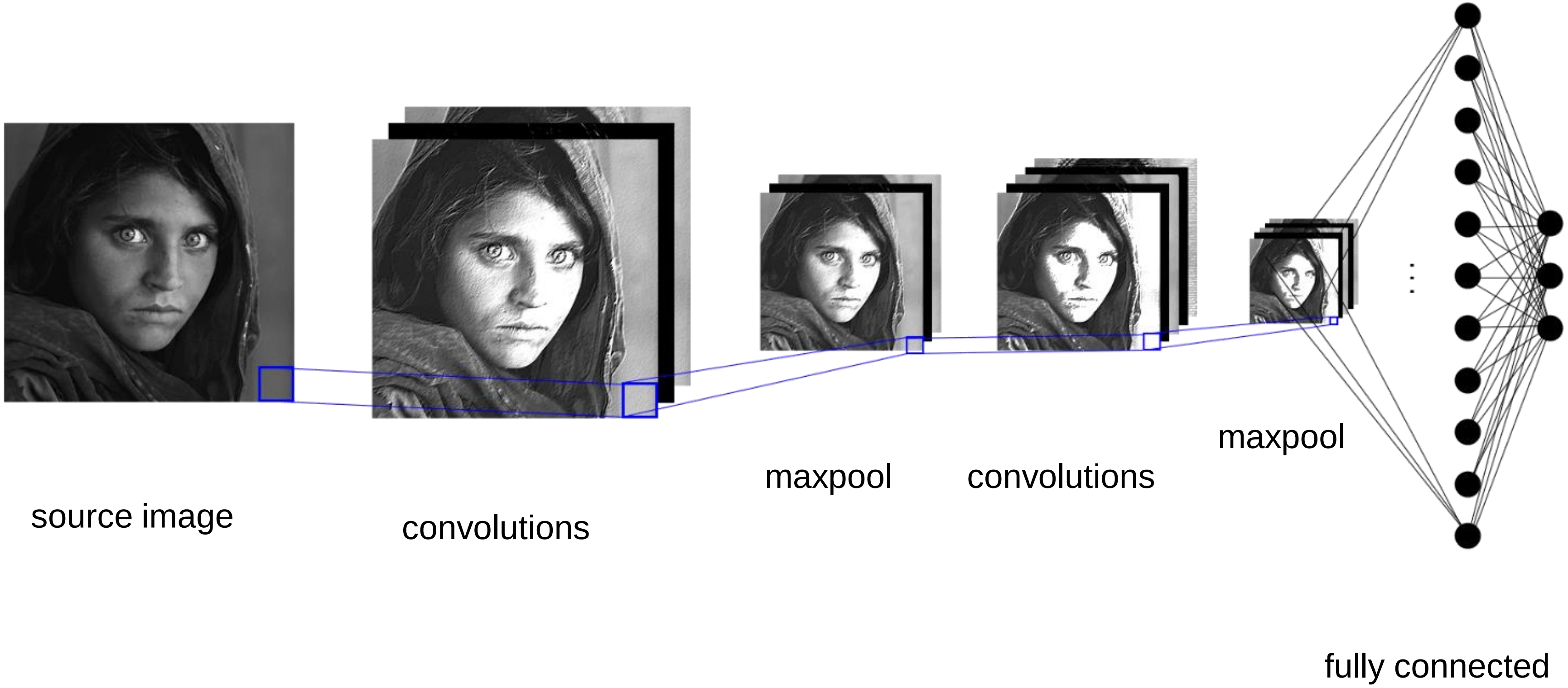
Visualizing Convolutional Layers



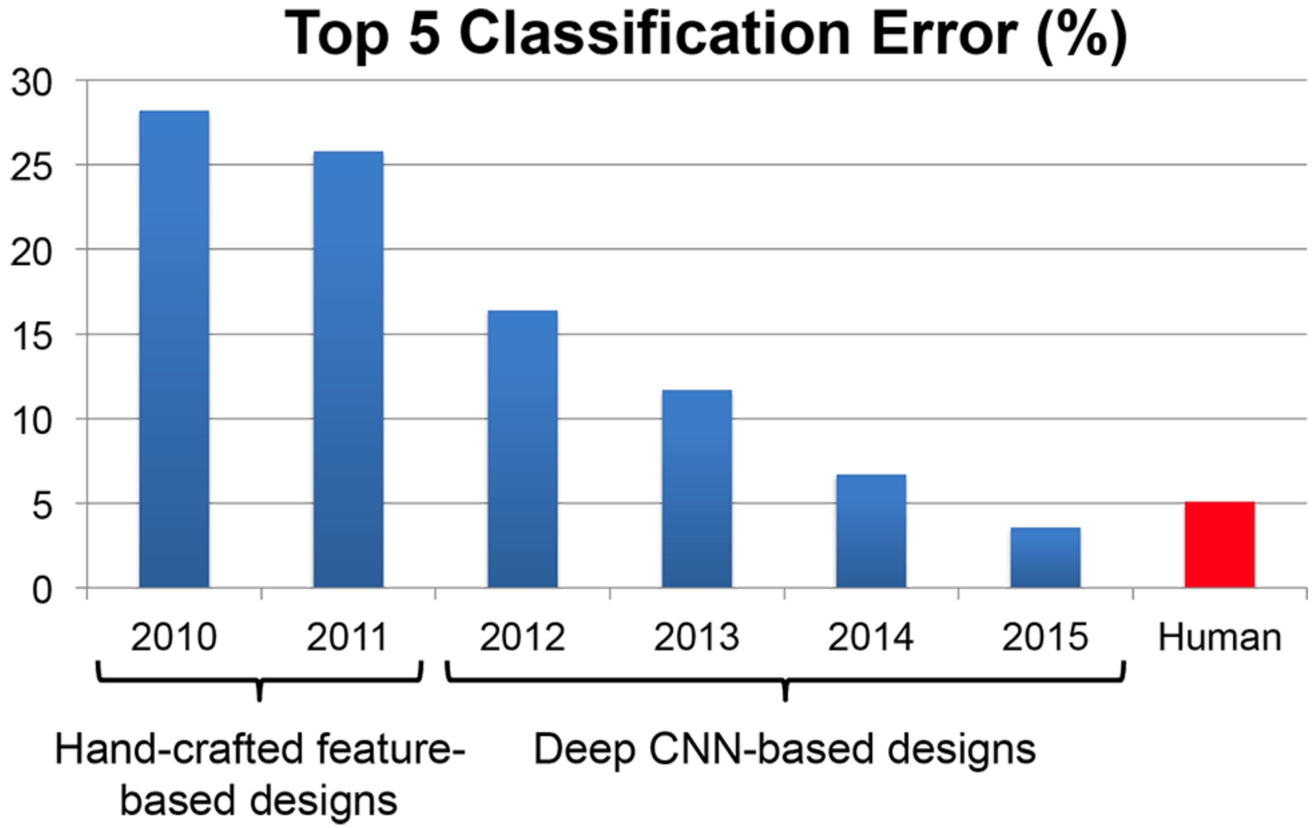
References:

- Lee, H., Grosse, R., Ranganath, R., & Ng, A. Y. (2009, June). Convolutional deep belief networks for scalable unsupervised learning of hierarchical representations. In Proceedings of the 26th annual international conference on machine learning (pp. 609-616). ACM.

Convolutional Neural Networks



CNN: ImageNet Classification Error



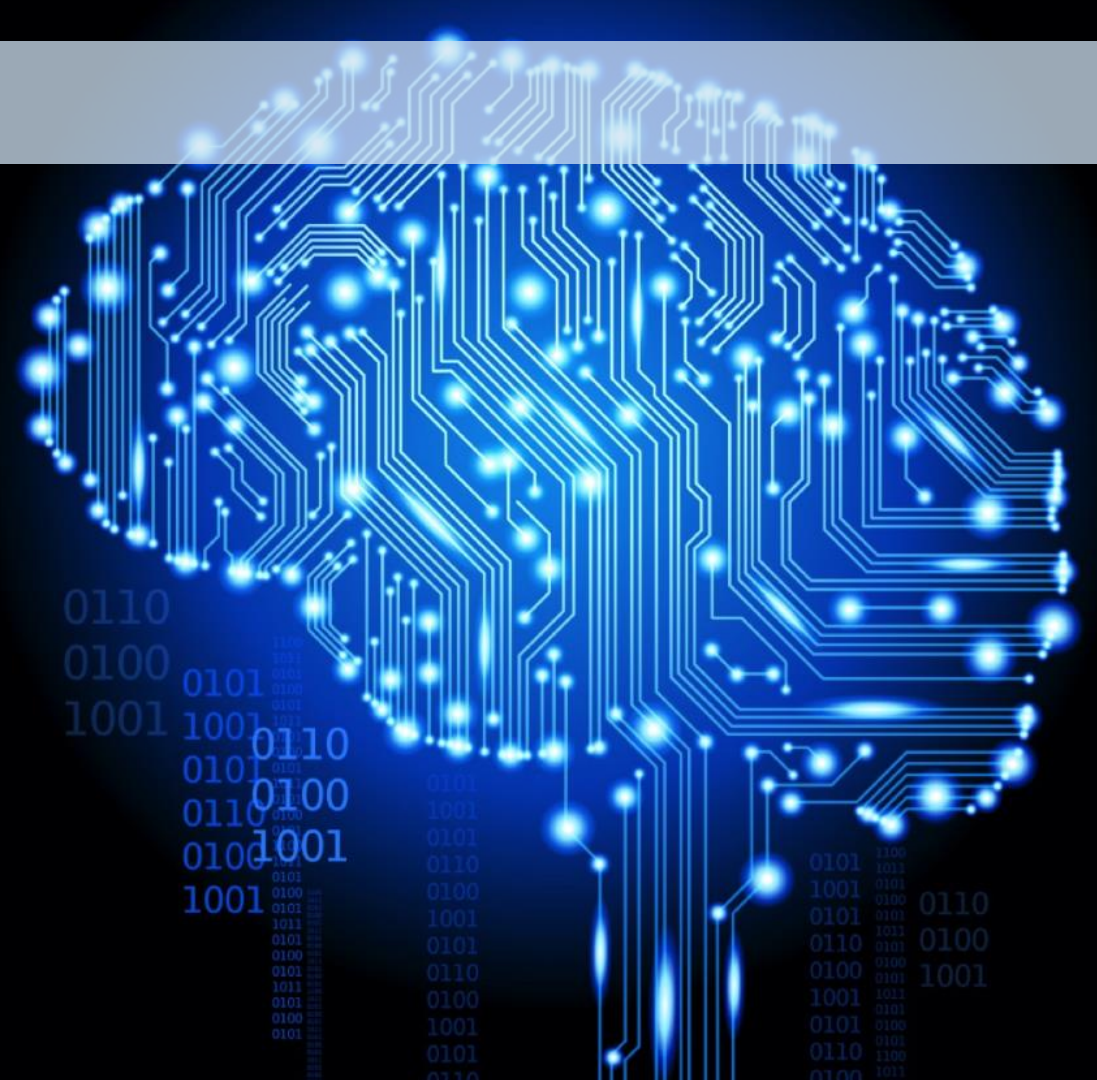
References:

- Russakovsky, Olga, et al. "Imagenet large scale visual recognition challenge." International Journal of Computer Vision 115.3 (2015): 211-252

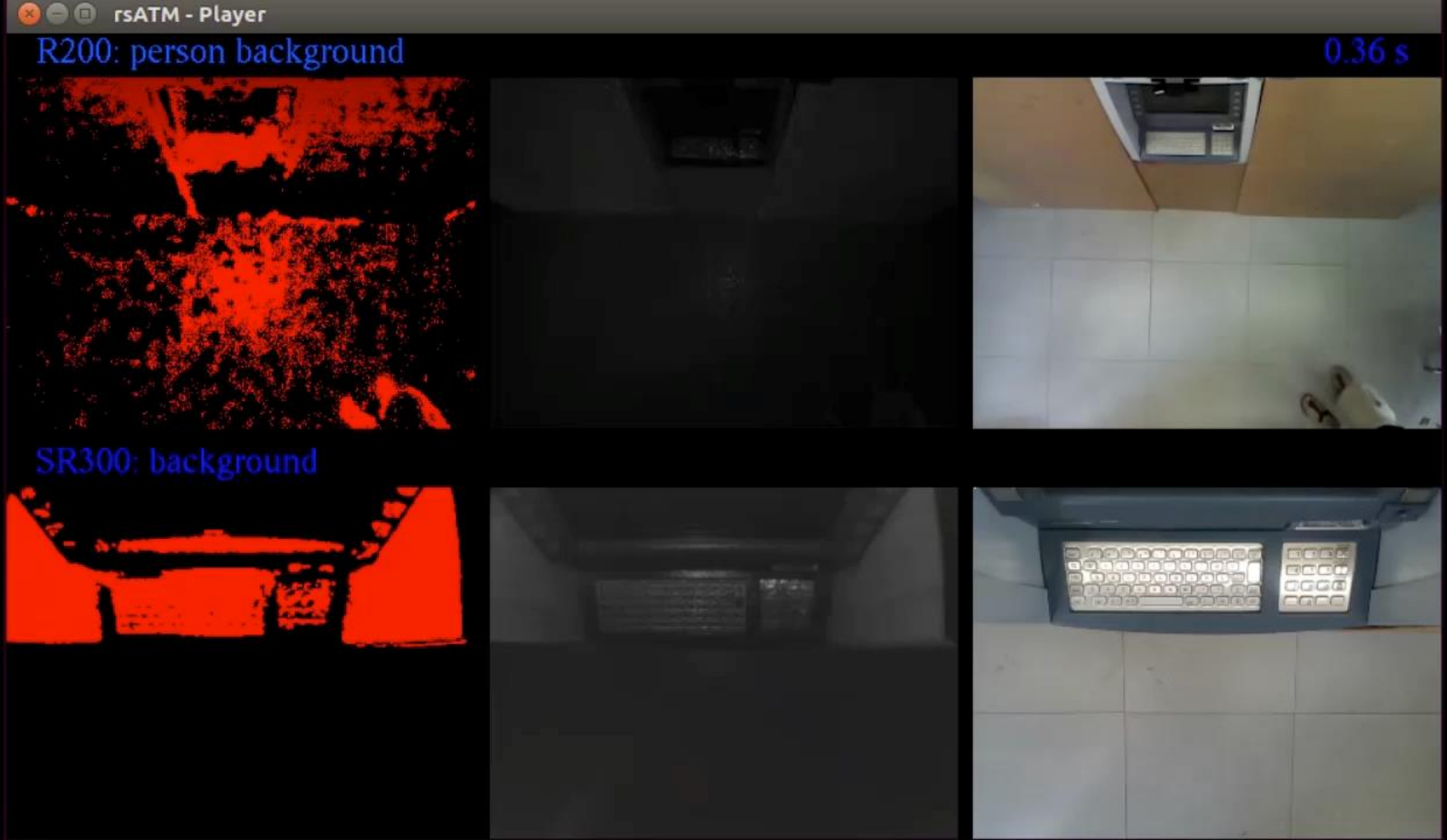
- Hardware Architectures for Deep Neural Networks, ISCA Tutorial, MIT

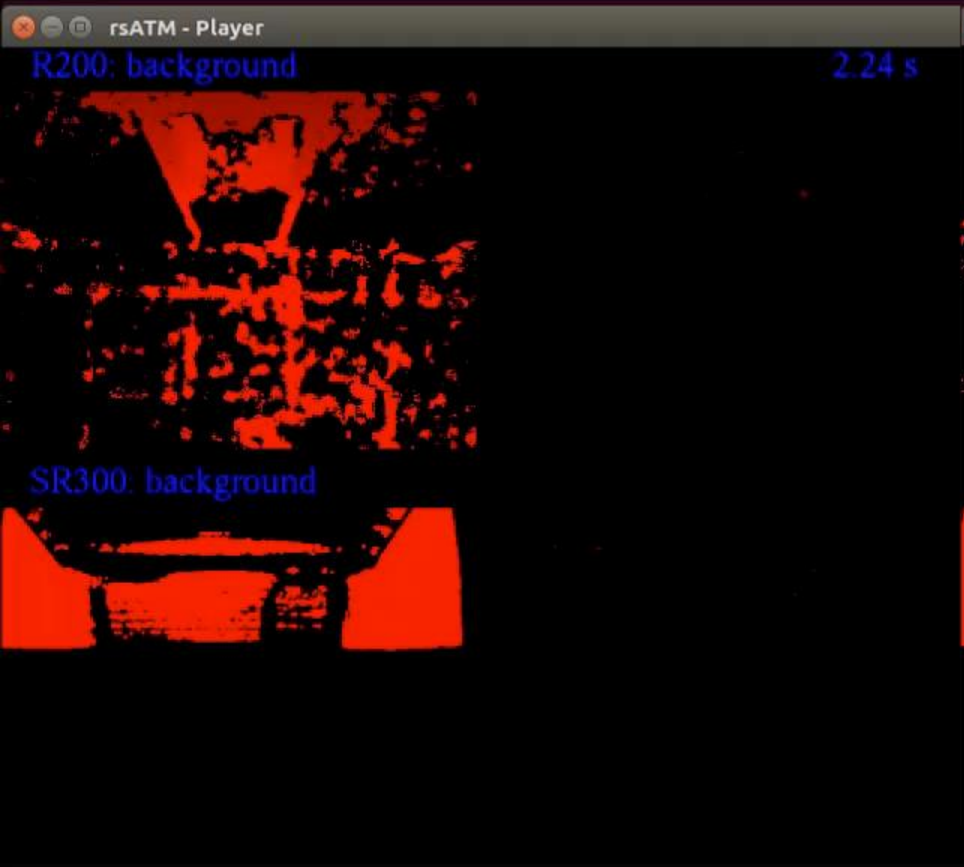
Machine Learning Process

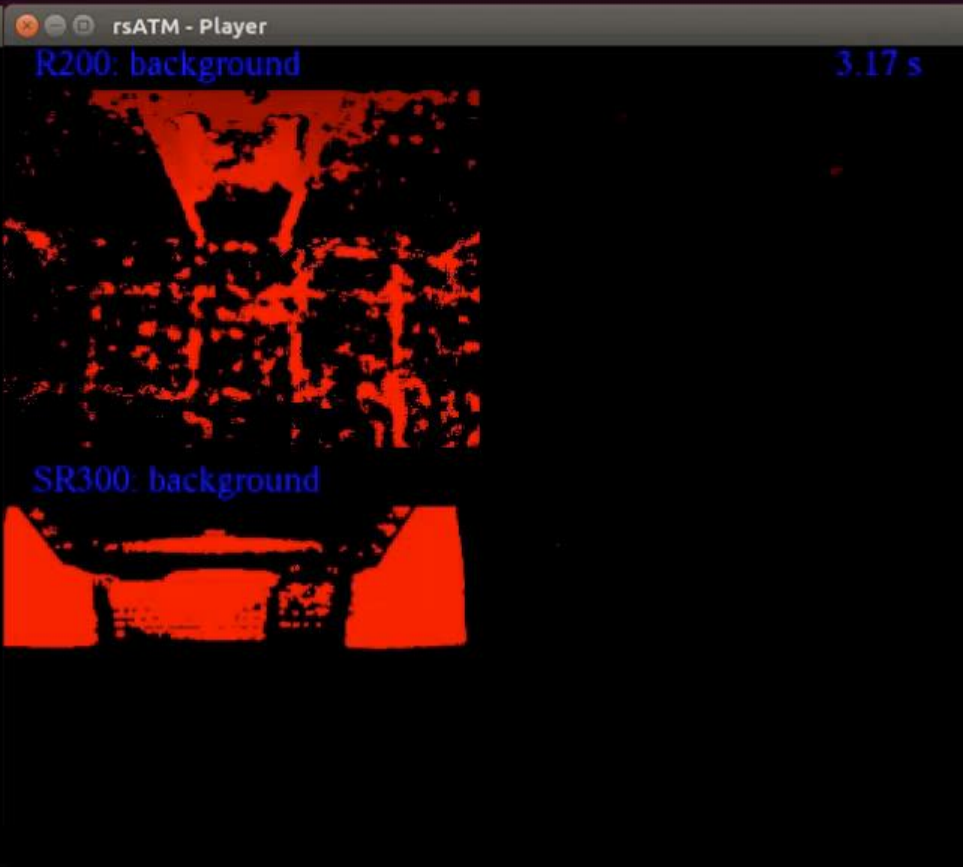
1. Get a dataset
2. Define the network architecture
3. Train and Test the model



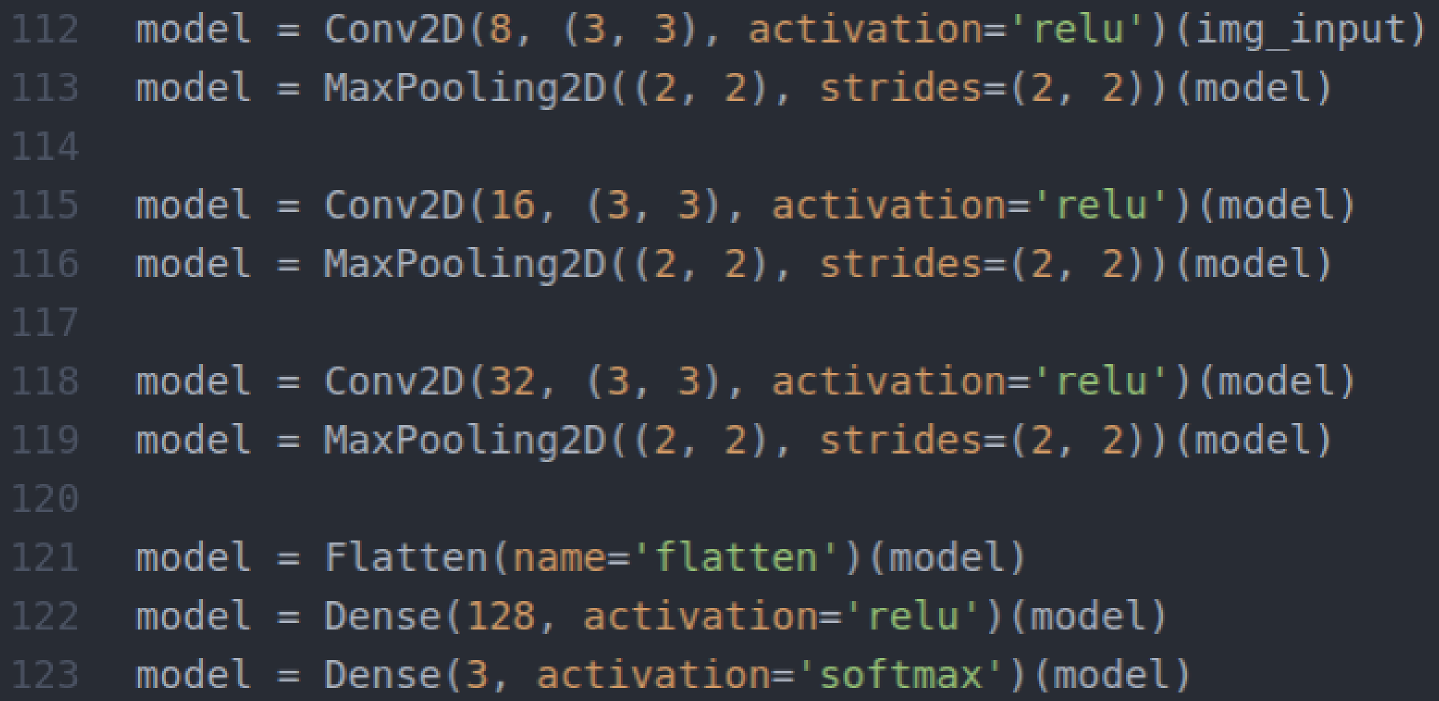
1. Get a Dataset


rsATM - Player
R200: person background
0.36 s
SR300: background


rsATM - Player
R200: background
2.24 s
SR300: background


rsATM - Player
R200: background
3.17 s
SR300: background

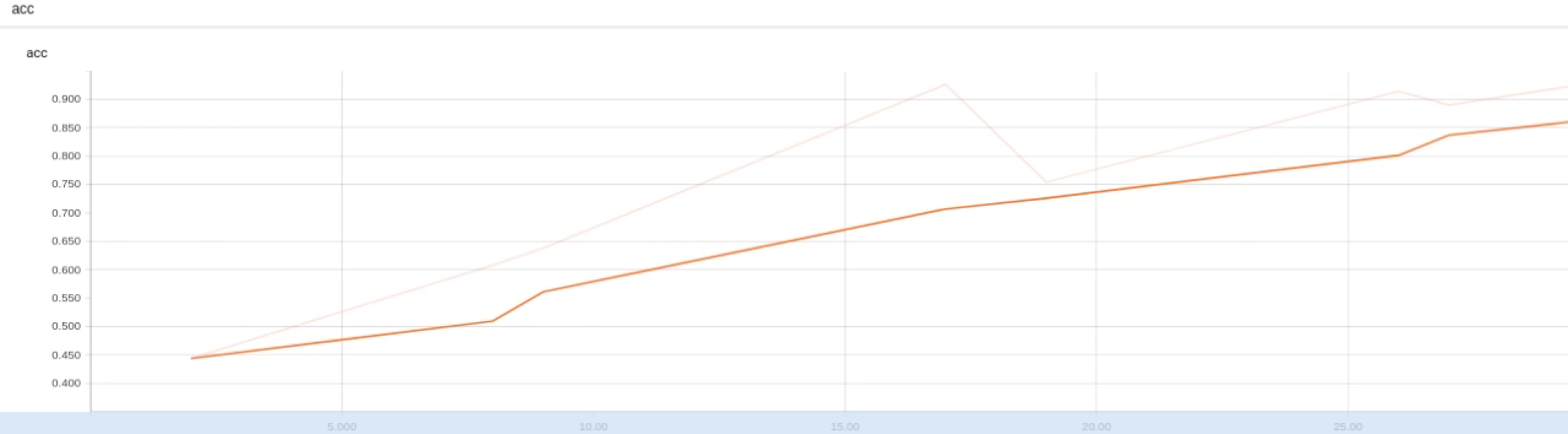
2. Define the Network Architecture

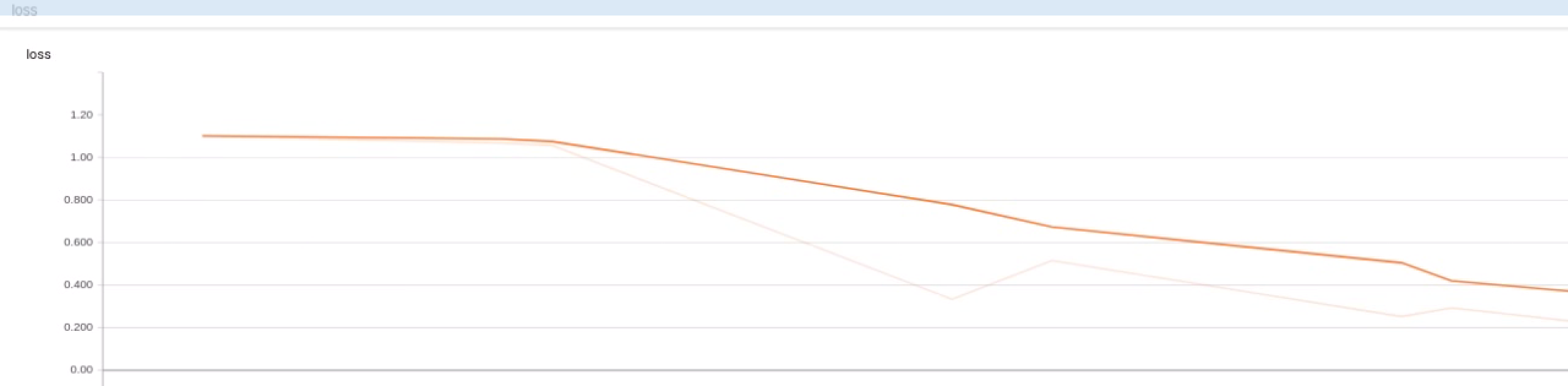


```
model = Conv2D(8, (3, 3), activation='relu')(img_input)
model = MaxPooling2D((2, 2), strides=(2, 2))(model)

model = Conv2D(16, (3, 3), activation='relu')(model)
model = MaxPooling2D((2, 2), strides=(2, 2))(model)

model = Conv2D(32, (3, 3), activation='relu')(model)
model = MaxPooling2D((2, 2), strides=(2, 2))(model)

model = Flatten(name='flatten')(model)
model = Dense(128, activation='relu')(model)
model = Dense(3, activation='softmax')(model)
```

BSC
Barcelona
Supercomputing
Center

3. Train and Test the Model





Results

Single Frame analysis:

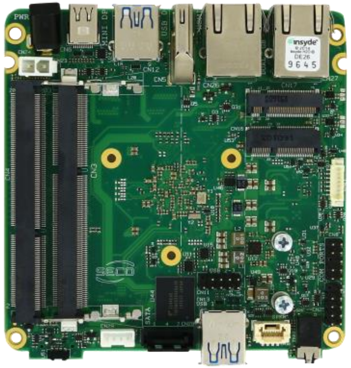
Test Dataset Classification Accuracy	
Background	98.19%
Withdrawal	97.05%
Attack	98.32%
Average	97.85%

- mean: 0.5 sec

Model Running on SECO SBC–A80 with Intel Braswell CPU

Five Frames analysis:

- No false alarms
- No undetected attacks
- Attack detection time:
  - mean: 2.4 sec
  - max: 3.3 sec



Predicting Security

Thank You