

# Near Sensor Image Denoising with Deep Learning: Review, Perspectives, and Application to Information System Security

Florian LEMARCHAND<sup>†</sup>, Erwan NOGUES<sup>†‡</sup> and Maxime PELCAT<sup>†§</sup>

<sup>†</sup> IETR/INSA, Rennes, France

<sup>‡</sup> DGA-MI, Bruz, France

<sup>§</sup> Institut Pascal, Clermont-Ferrand, France

## Summary:

- Introduction
- Compromising Emanations Detection
- Statistical Image Denoising
- Near Sensor Platforms for Statistical Denoising
- Perspectives for ToxicIA

RESSI – May 16<sup>th</sup> 2019

## Context:

- PhD Title : Recognition of Images and Intercepted Signals using Embedded Artificial Intelligence
- Pôle d'Excellence Cyber (PEC) PhD Grant
- Partnership between DGA-MI and IETR VAADER
- DGA-MI and DGA-IA developed ToxicIA --> Proof Of Concept (POC) on using machine learning to enhance the interpretation of compromising emanations
- POC has ended and is transferred to VAADER team for perspective further enhancement
- This PhD has ToxicIA as a case study

## Context:

- PhD Title : Recognition of Images and Intercepted Signals using Embedded Artificial Intelligence
- Pôle d'Excellence Cyber (PEC) PhD Grant
- Partnership between DGA-MI and IETR VAADER
- DGA-MI and DGA-IA developed ToxicIA --> Proof Of Concept (POC) on using machine learning to enhance the interpretation of compromising emanations
- POC has ended and is transferred to VAADER team for perspective further enhancement
- This PhD has ToxicIA as a case study

## Context:

- PhD Title : Recognition of Images and Intercepted Signals using Embedded Artificial Intelligence
- Pôle d'Excellence Cyber (PEC) PhD Grant
- Partnership between DGA-MI and IETR VAADER
- DGA-MI and DGA-IA developed ToxicIA --> Proof Of Concept (POC) on using machine learning to enhance the interpretation of compromising emanations
- POC has ended and is transferred to VAADER team for perspective further enhancement
- This PhD has ToxicIA as a case study

## Context:

- PhD Title : Recognition of Images and Intercepted Signals using Embedded Artificial Intelligence
- Pôle d'Excellence Cyber (PEC) PhD Grant
- Partnership between DGA-MI and IETR VAADER
- DGA-MI and DGA-IA developed ToxicIA --> Proof Of Concept (POC) on using machine learning to enhance the interpretation of compromising emanations
- POC has ended and is transferred to VAADER team for perspective further enhancement
- This PhD has ToxicIA as a case study

## Context:

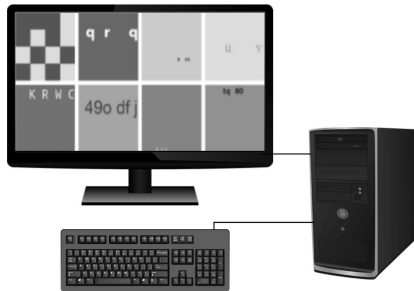
- PhD Title : Recognition of Images and Intercepted Signals using Embedded Artificial Intelligence
- Pôle d'Excellence Cyber (PEC) PhD Grant
- Partnership between DGA-MI and IETR VAADER
- DGA-MI and DGA-IA developed ToxicIA --> Proof Of Concept (POC) on using machine learning to enhance the interpretation of compromising emanations
- POC has ended and is transferred to VAADER team for perspective further enhancement
- This PhD has ToxicIA as a case study

## Context:

- PhD Title : Recognition of Images and Intercepted Signals using Embedded Artificial Intelligence
- Pôle d'Excellence Cyber (PEC) PhD Grant
- Partnership between DGA-MI and IETR VAADER
- DGA-MI and DGA-IA developed ToxicIA --> Proof Of Concept (POC) on using machine learning to enhance the interpretation of compromising emanations
- POC has ended and is transferred to VAADER team for perspective further enhancement
- This PhD has ToxicIA as a case study

## Target System With Video Display

Display signal can be digital (e.g. DVI, DP, HDMI) or analog (e.g. VGA).

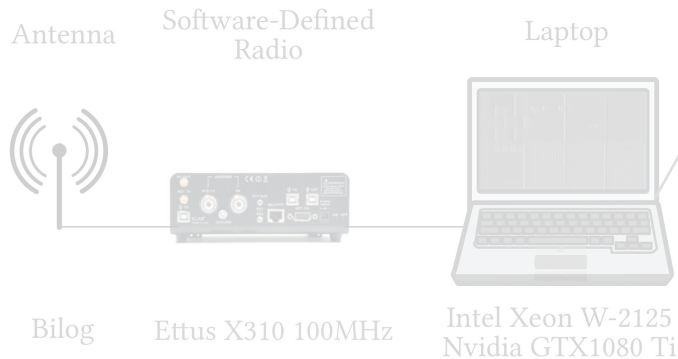


Compromising  
Emanations

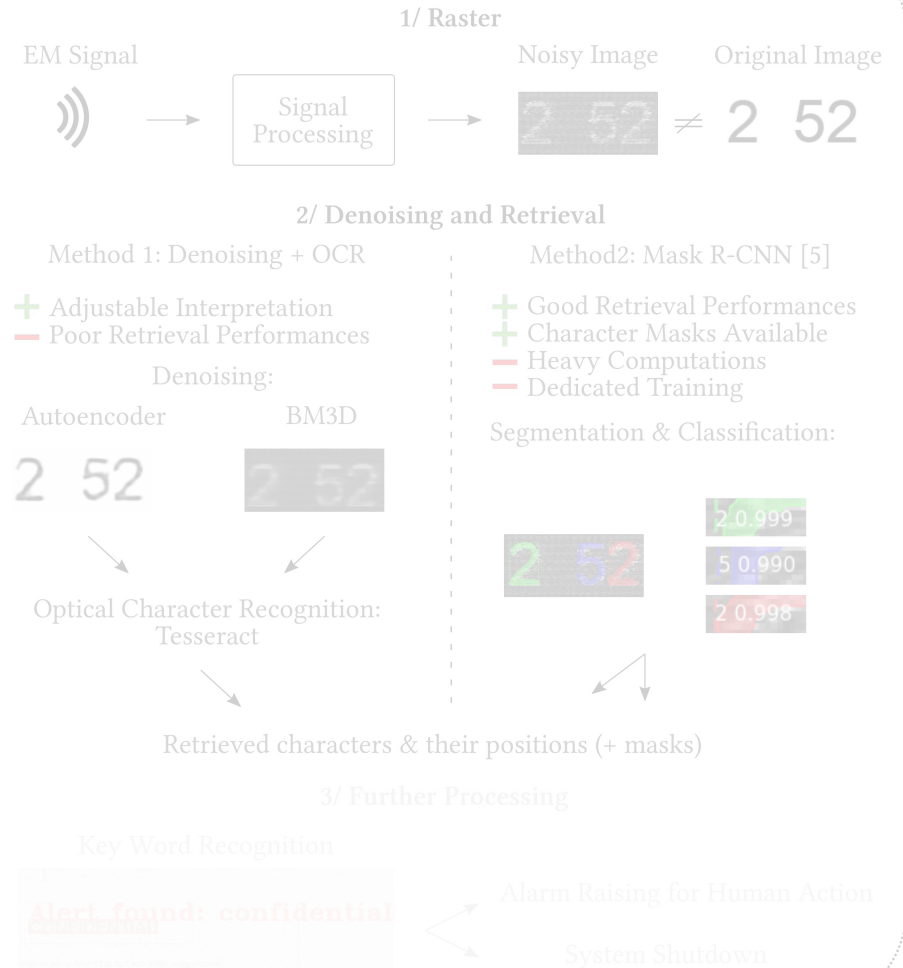
≈ 10 m



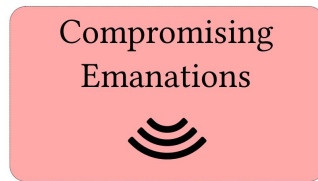
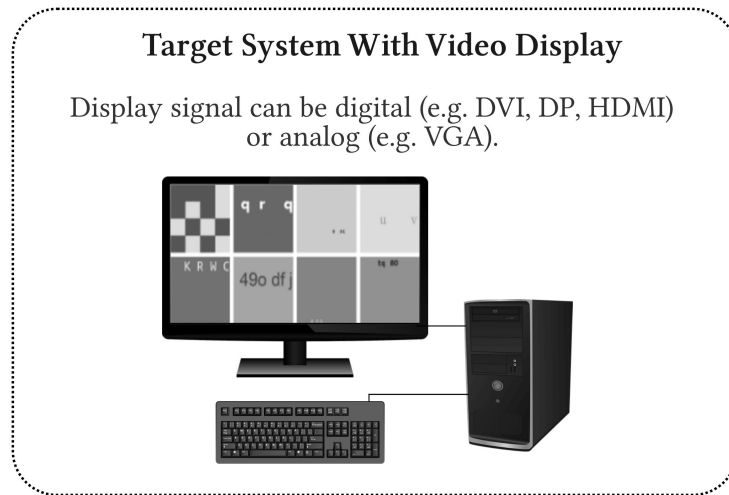
## Current Interception System to be Embedded



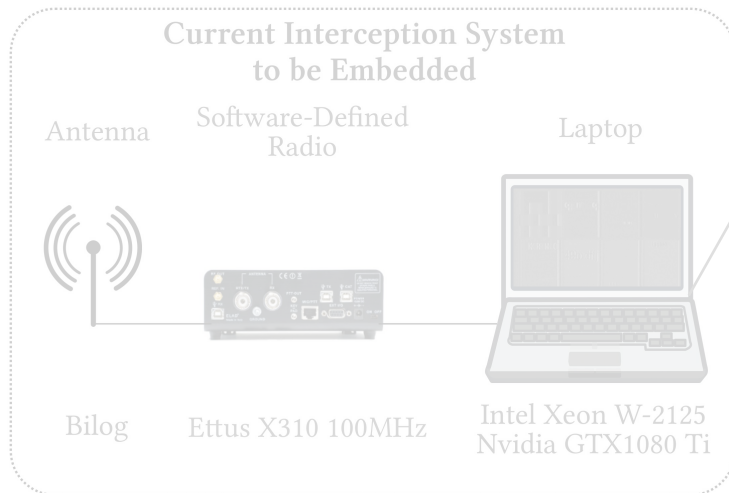
## Interpretation Pipeline: Case Study of Character Retrieval

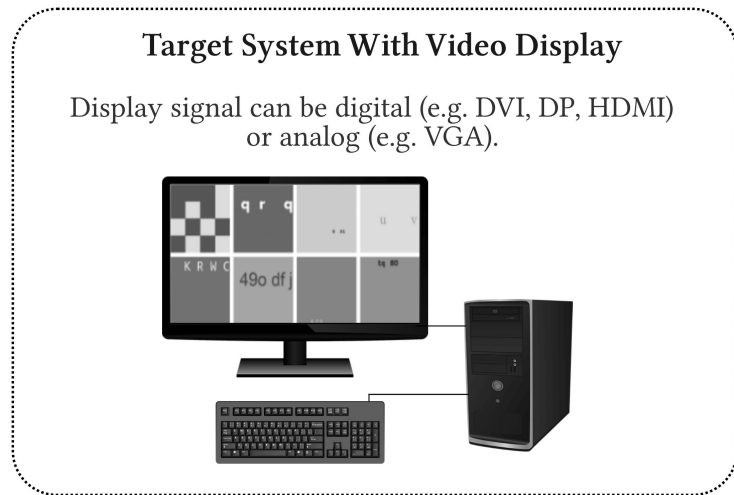




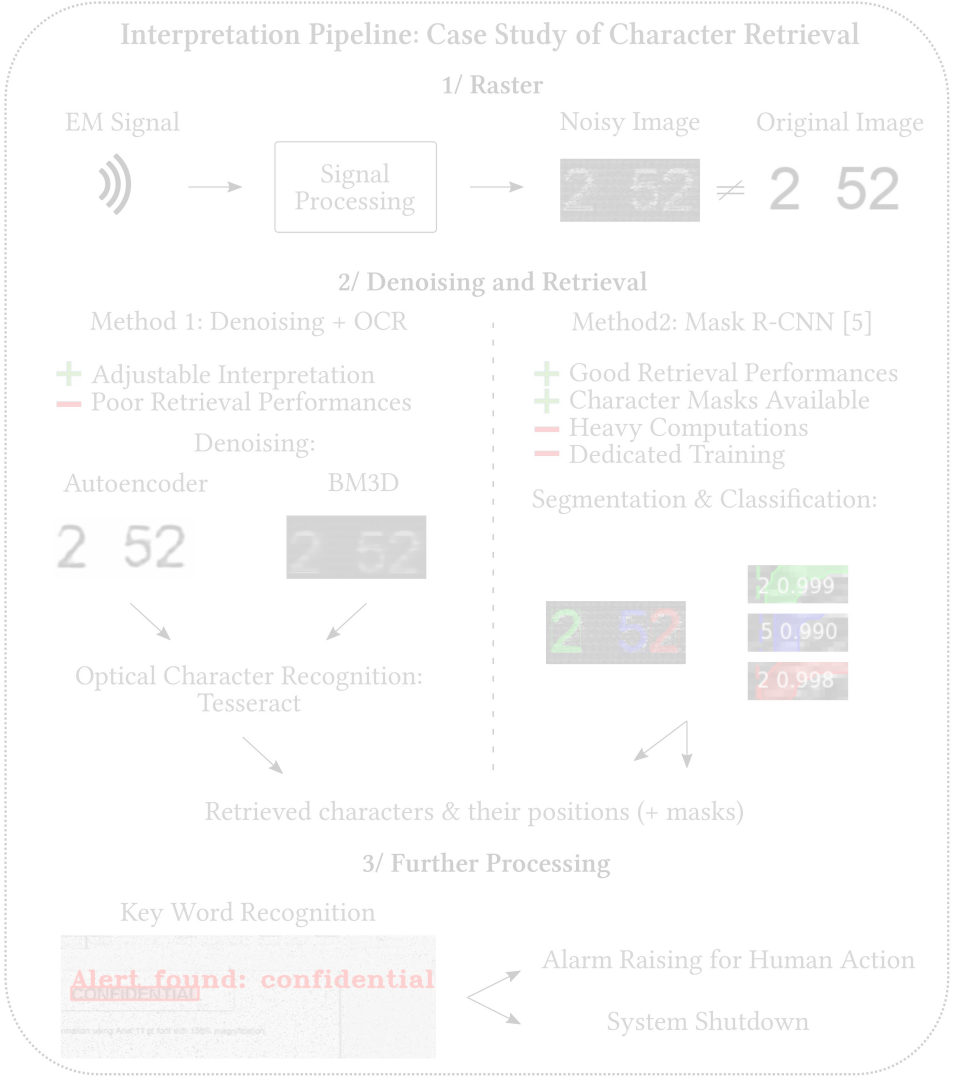
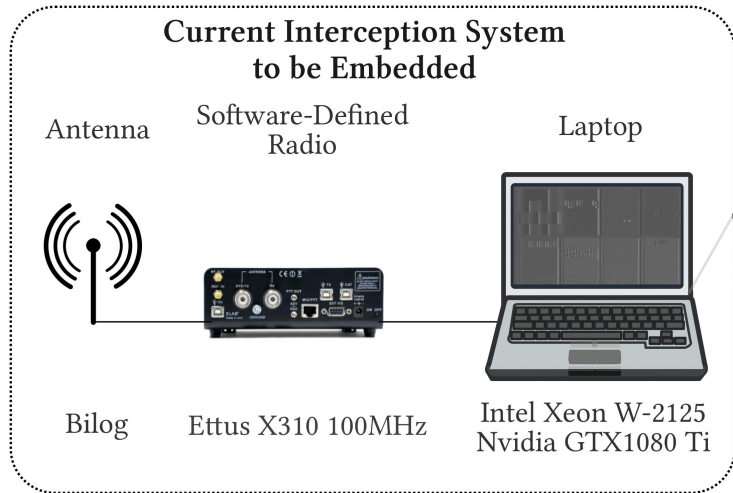
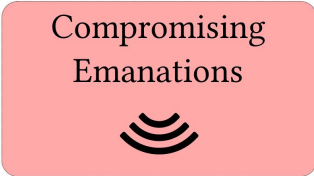


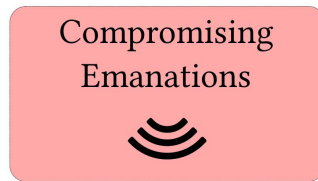
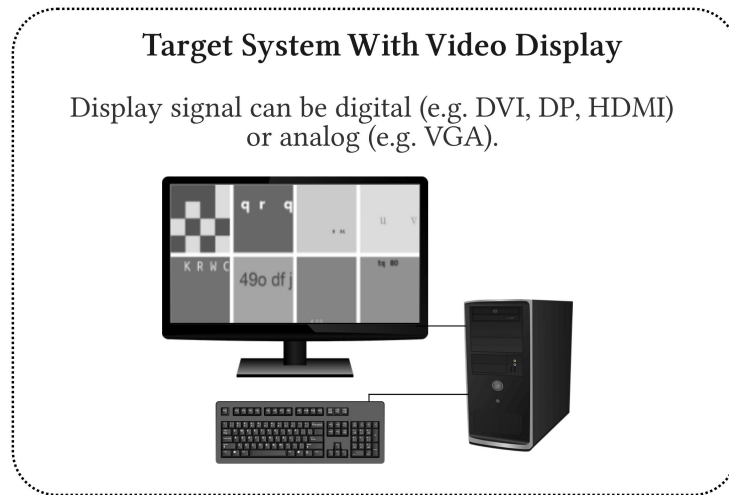
≈ 10 m



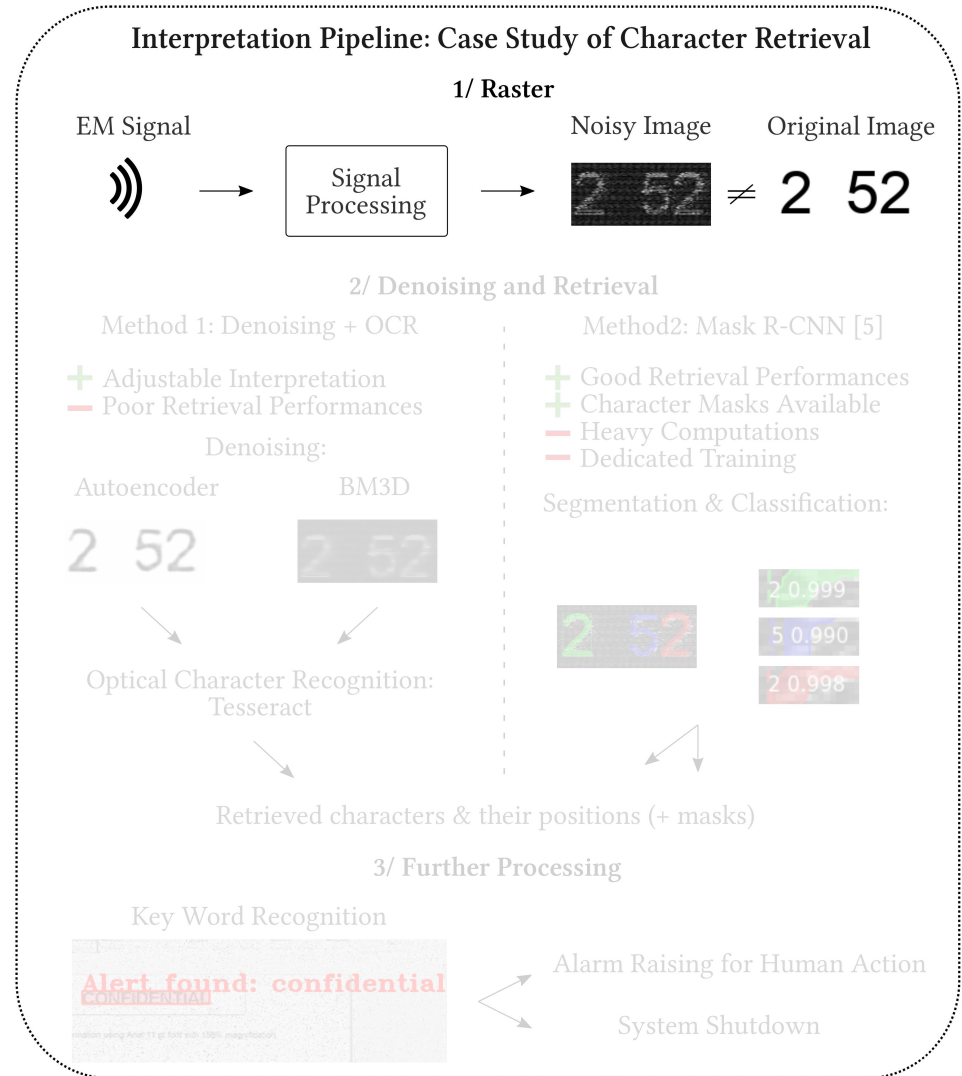
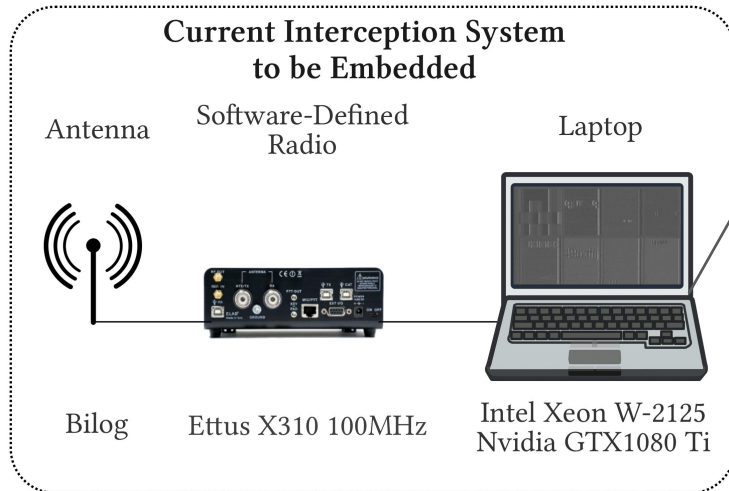


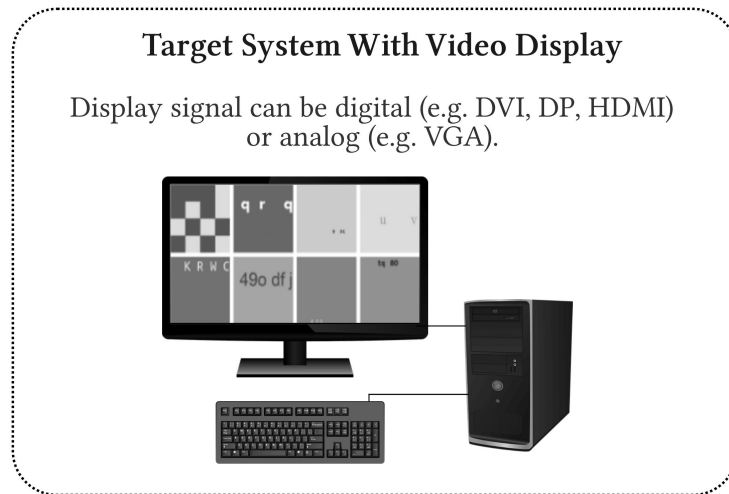
≈ 10 m



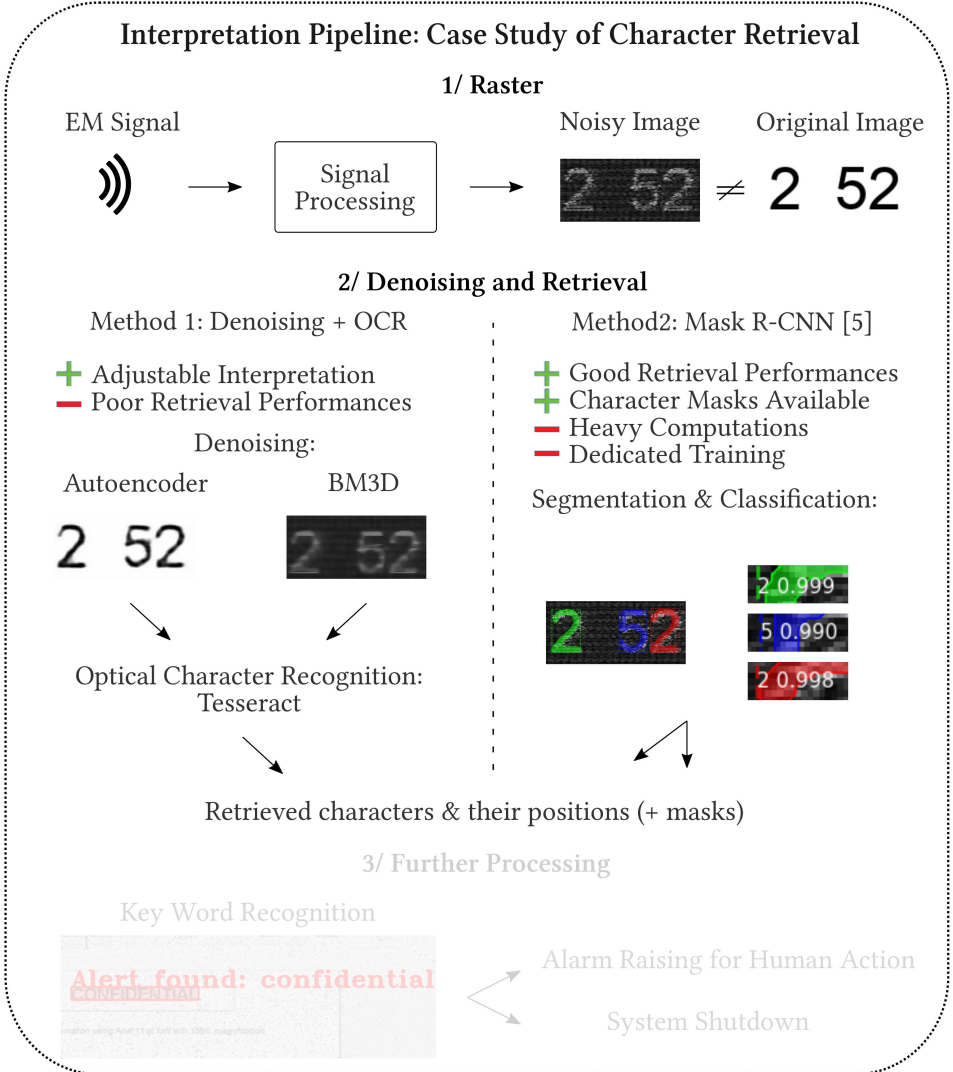
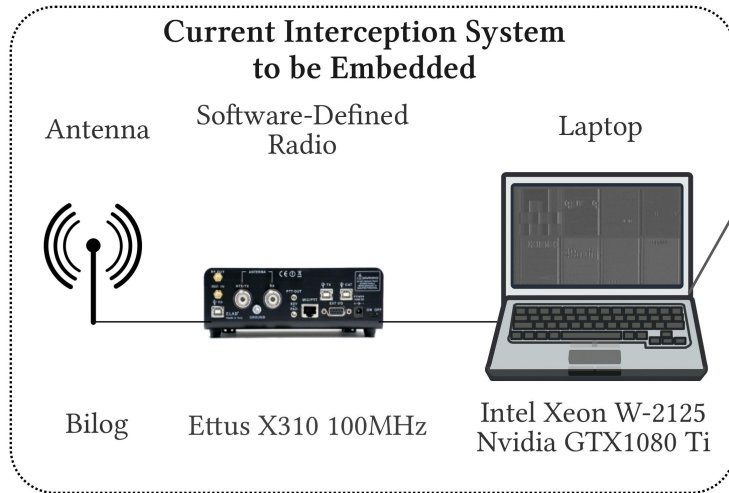


≈ 10 m



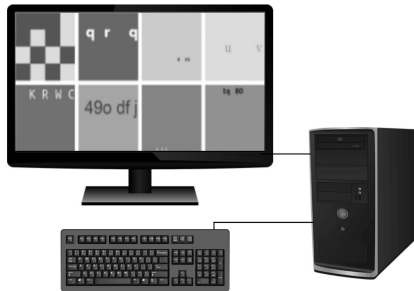


≈ 10 m



## Target System With Video Display

Display signal can be digital (e.g. DVI, DP, HDMI) or analog (e.g. VGA).

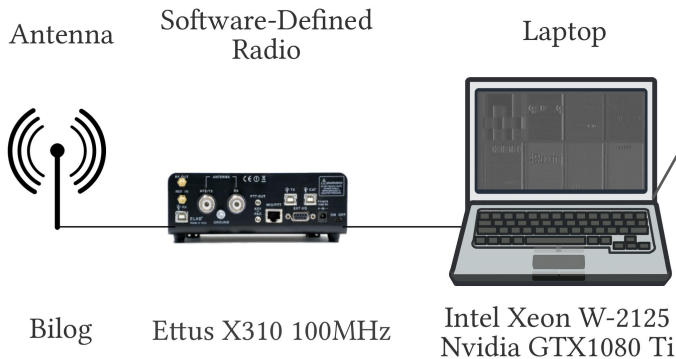


Compromising  
Emanations

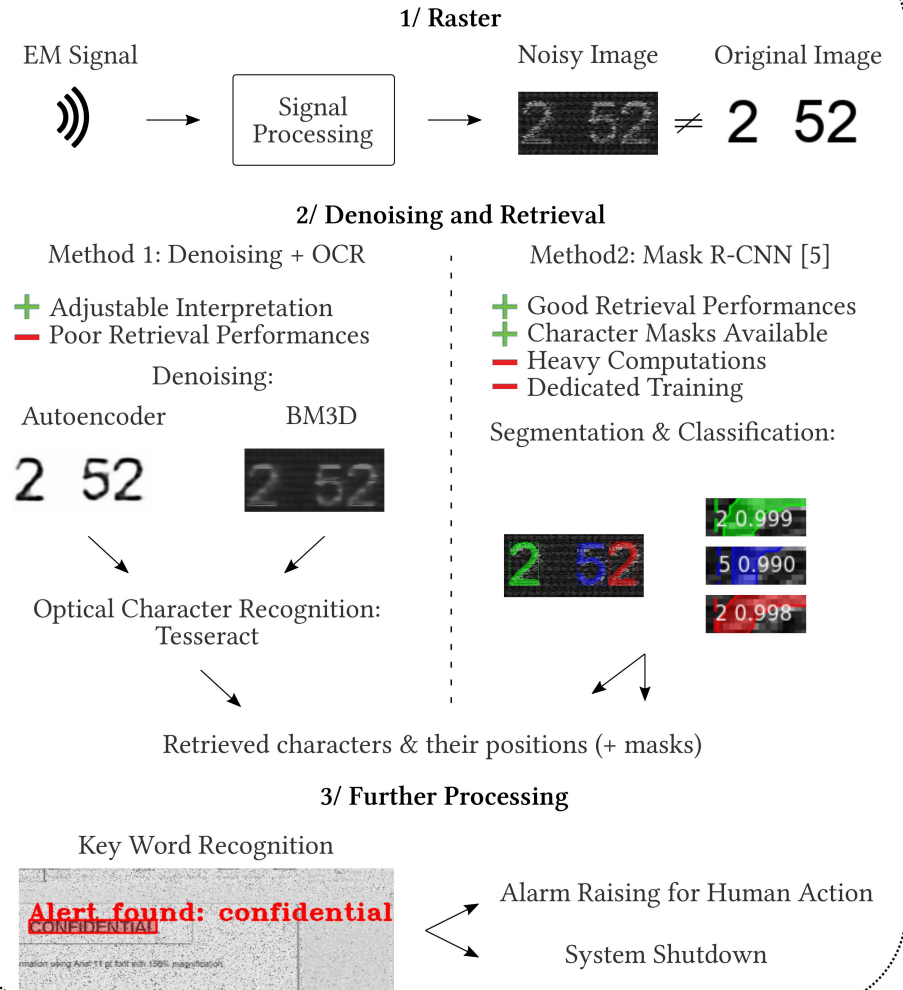
≈ 10 m



## Current Interception System to be Embedded

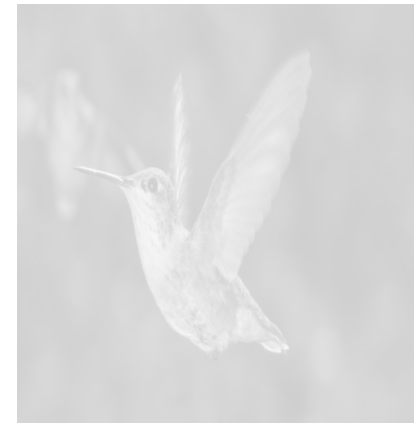


## Interpretation Pipeline: Case Study of Character Retrieval





Noisy Sample



Denoised Sample

Denoising Methods

## Non-Statistical

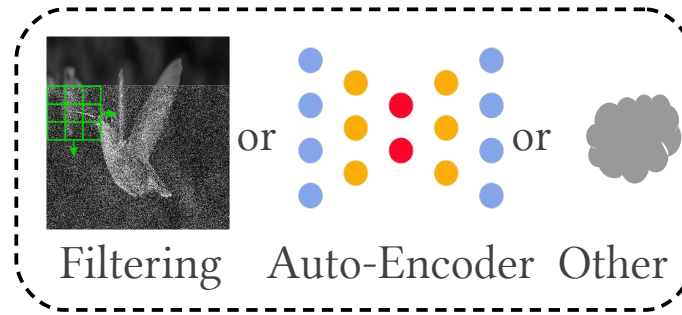
- + Low Computation
  - + No need for training dataset
  - Dedicated to a noise model
- e.g. :  
Filters (Median, Mean, ...)  
Block-Matching 3D (BM3D)  
Transform Domain (FFT)

## Statistical

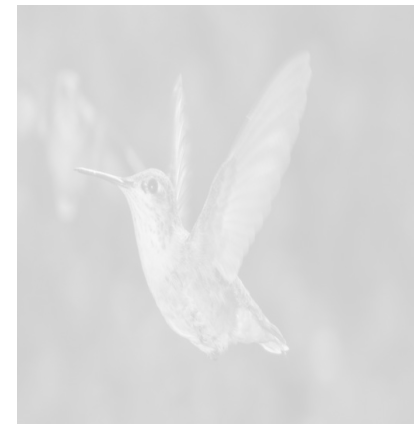
- + Support several noise models
  - + High SNR improvements
  - Heavy computations
- e.g. :  
Stacked/Sparse Auto-Encoders  
Generative Adversarial Networks  
Fine-tuned Deep Neural Networks



Noisy Sample



Denoising Methods



Denoised Sample



## Non-Statistical

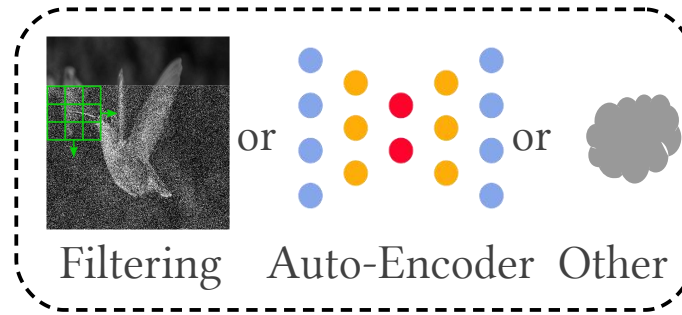
- + Low Computation
  - + No need for training dataset
  - Dedicated to a noise model
- e.g. :  
Filters (Median, Mean, ...)  
Block-Matching 3D (BM3D)  
Transform Domain (FFT)

## Statistical

- + Support several noise models
  - + High SNR improvements
  - Heavy computations
- e.g. :  
Stacked/Sparse Auto-Encoders  
Generative Adversarial Networks  
Fine-tuned Deep Neural Networks



Noisy Sample



Denoising Methods



Denoised Sample



## Non-Statistical

- + Low Computation
  - + No need for training dataset
  - Dedicated to a noise model
- e.g. :  
Filters (Median, Mean, ...)  
Block-Matching 3D (BM3D)  
Transform Domain (FFT)

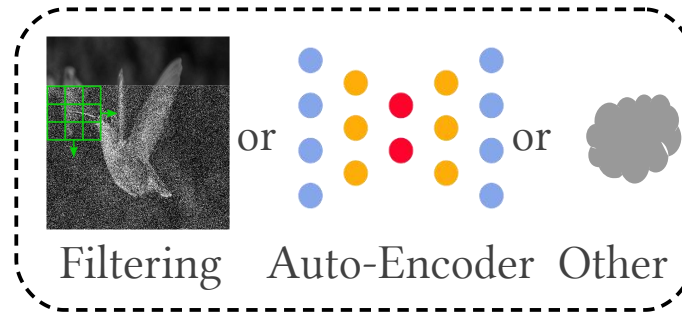
## Statistical

- + Support several noise models
  - + High SNR improvements
  - Heavy computations
- e.g. :  
Stacked/Sparse Auto-Encoders  
Generative Adversarial Networks  
Fine-tuned Deep Neural Networks





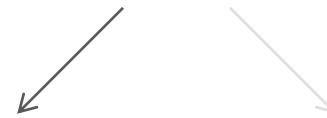
Noisy Sample



Denoising Methods



Denoised Sample



## Non-Statistical

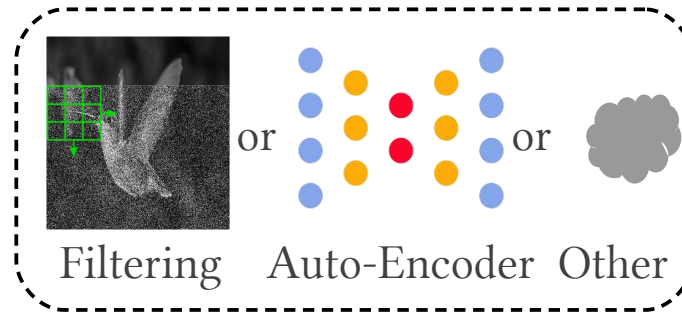
- + Low Computation
  - + No need for training dataset
  - Dedicated to a noise model
- e.g. :
- Filters (Median, Mean, ...)
  - Block-Matching 3D (BM3D)
  - Transform Domain (FFT)

## Statistical

- + Support several noise models
  - + High SNR improvements
  - Heavy computations
- e.g. :
- Stacked/Sparse Auto-Encoders
  - Generative Adversarial Networks
  - Fine-tuned Deep Neural Networks



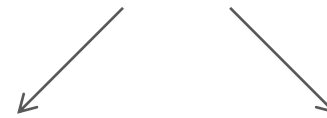
Noisy Sample



Denoising Methods



Denoised Sample



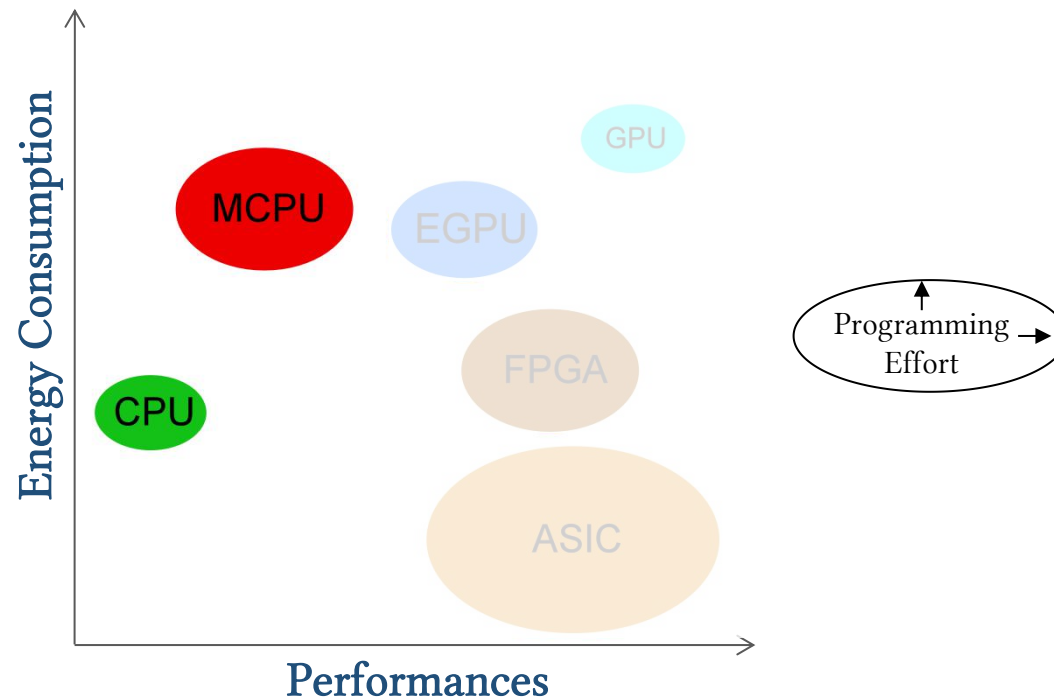
## Non-Statistical

- + Low Computation
  - + No need for training dataset
  - Dedicated to a noise model
- e.g. :  
Filters (Median, Mean, ...)  
Block-Matching 3D (BM3D)  
Transform Domain (FFT)

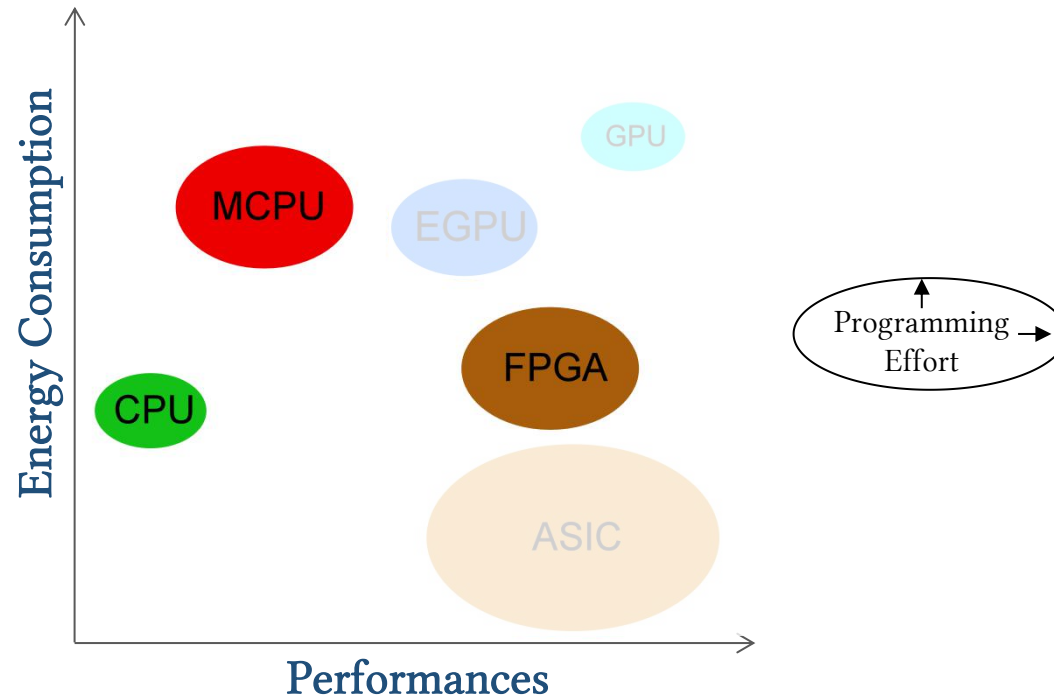
## Statistical

- + Support several noise models
  - + High SNR improvements
  - Heavy computations
- e.g. :  
Stacked/Sparse Auto-Encoders  
Generative Adversarial Networks  
Fine-tuned Deep Neural Networks

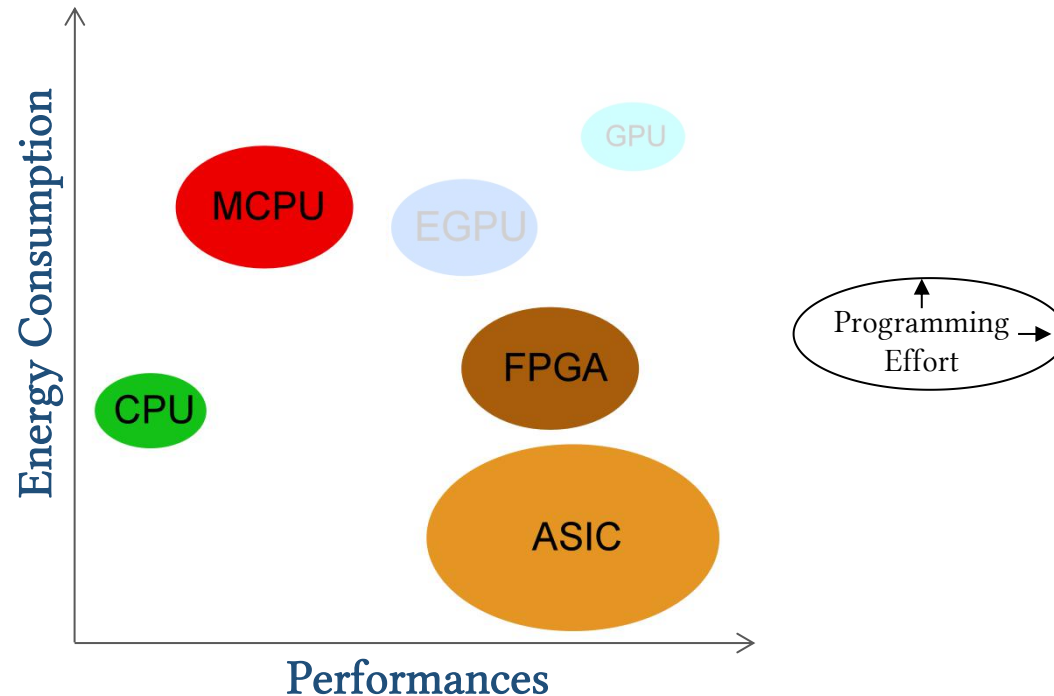
- **Single, Multi, Many-core CPUs** : New instructions set made especially for Deep Neural Networks (DNN) → Intel, ARM, Kalray
- **FPGAs** : High parallelism and good energy efficiency → Intel (ex-Altera), Xilinx
- **ASICs** : Application specific hardware highly efficient
- **Embedded GPUs** : Low power consumption and good performances → Nvidia, Coral, Intel



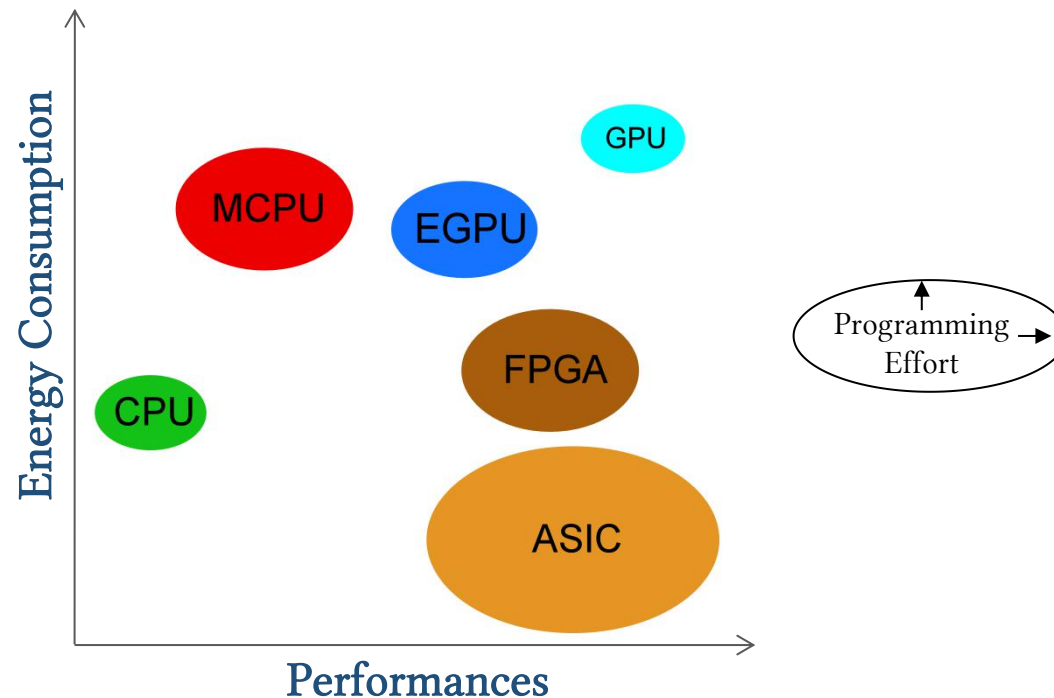
- **Single, Multi, Many-core CPUs** : New instructions set made especially for Deep Neural Networks (DNN) → Intel, ARM, Kalray
- **FPGAs** : High parallelism and good energy efficiency → Intel (ex-Altera), Xilinx
- **ASICs** : Application specific hardware highly efficient
- **Embedded GPUs** : Low power consumption and good performances → Nvidia, Coral, Intel



- **Single, Multi, Many-core CPUs** : New instructions set made especially for Deep Neural Networks (DNN) → Intel, ARM, Kalray
- **FPGAs** : High parallelism and good energy efficiency → Intel (ex-Altera), Xilinx
- **ASICs** : Application specific hardware highly efficient
- **Embedded GPUs** : Low power consumption and good performances → Nvidia, Coral, Intel



- **Single, Multi, Many-core CPUs** : New instructions set made especially for Deep Neural Networks (DNN) → Intel, ARM, Kalray
- **FPGAs** : High parallelism and good energy efficiency → Intel (ex-Altera), Xilinx
- **ASICs** : Application specific hardware highly efficient
- **Embedded GPUs** : Low power consumption and good performances → Nvidia, Coral, Intel



## Network Reduction

- Connection pruning
- Weight quantization/sharing
- Huffman coding

## New Networks


- Smaller networks by design (e.g. : MobileNets)
- Approximate computing, fault tolerance


## Training Phase Enhancement

- Better choice of training samples
- Data Augmentation
- Artificial sample generation

**Image Denoising with Embedded Deep Learning:  
Review, Perspectives and Application to Information System Security**

Florian Lemarchand - Erwan Nogues - Maxime Pelcat





### Image Denoising

Facts

- Noise is inherent to every sensor being analog or digital.
- There are plenty of noise models : Gaussian, Impulsive, Quantization, Speckle, Structured, ...

Denoising Methods

Non-Statistical

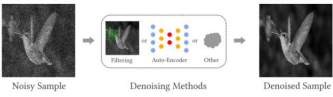
- + Low Computation
- + No need for training dataset
- Dedicated to a noise model

e.g. : Filters (Median, Mean, ...) Block-Matching 3D (BM3D) Transform Domain (FFT)

Statistical

- + Support several noise models
- + High SNR improvements
- Heavy computations

e.g. : Stacked/Sparse Auto-Encoders Generative Adversarial Networks Fine-tuned Deep Neural Networks



Noisy Sample      Denoising Methods      Denoised Sample

Strategies for Embedding Statistical Methods

Network Reduction [1]

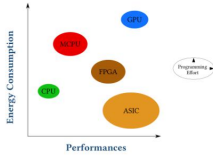
- Connection pruning
- Weight quantization/sharing
- Huffman coding

New Networks

- Smaller networks by design (e.g. : MobileNets) [2]
- Approximate computing, fault tolerance

### Platforms for Near Sensor Denoising

- **Single, Multi, Many-core CPUs** : General purpose processor executing DNN with a parallelism depending on the number of cores. New instructions set made especially for Deep Neural Networks (DNN) → Intel, ARM, Kalray
- **Embedded GPUs** : Fast evolving systems designed especially to embedded DNN with reasonable effort, low power consumption and good performances → Nvidia, Coral, Intel
- **FPGAs** : Complex to program but High-Level Synthesis (HLS) tools progressing [3]. High parallelism and good energy efficiency → Intel (ex-Altera), Xilinx
- **ASICs** : Application specific hardware defined circuits highly efficient but complex and expensive to design.



Energy Consumption


Performances

### Application to Information System Security

Detection of compromising Electro-Magnetic (EM) emanations [4] using a learned Optical Character Recognition (OCR)

Target System With Video Display

Display signal can be digital (e.g. DVI, DP, HDMI) or analog (e.g. VGA).



Compromising Emanations

~ 10 m

Current Interception System to be Embedded

Antenna    Software-Defined Radio    Laptop

Bilog    Ettus X310 100MHz    Intel Xeon W-2125    Nvidia GTX1080 Ti

Interpretation Pipeline: Case Study of Character Retrieval

1/ Raster

EM Signal → Signal Processing → Noisy Image → Original Image

2/ Denoising and Retrieval

Method 1: Denoising + OCR      Method 2: Mask R-CNN [5]

- + Adjustable Interpretation
- Poor Retrieval Performances

Denoising: Autoencoder      BM3D

Segmentation & Classification:

Optical Character Recognition: Tesseract

Retrieved characters & their positions (+ masks)

3/ Further Processing

Key Word Recognition      Alarm Raising for Human Action

System Shutdown

### References


[1]S. Han et al., « Deep Compression: Compressing Deep Neural Networks with Pruning, Trained Quantization and Huffman Coding », 2015.


[2]A. G. Howard et al., « MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications », 2017.


[3]K. Abdelnabi et al., « Towards Efficient CNN Graphs on Embedded FPGAs », IEEE Embedded Systems Letters, 2017.

[4]M. G. Kuhn et R. J. Anderson, « Soft Transient: Hidden Data Transmission Using Electromagnetic Emanations », 1998.

[5]K. He et al., « Mask R-CNN », in 2017 IEEE International Conference on Computer Vision (ICCV), 2017.







Thank you for your attention!  
For questions --> Poster Session at 18:15 p.m.

Contact :  
florian.lemarchand@insa-rennes.fr