VAADER
IETR research team

IETR

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES

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

Florian LEMARCHAND[†], Erwan NOGUES [†‡] and Maxime PELCAT[†§]

[†] **IETR/INSA, Rennes, France**

[‡] DGA-MI, Bruz, France

[§] Institut Pascal, Clermont-Ferrand, France

Summary:

RESSI – May 16th 2019

Introduction

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 transfered to VAADER team for perspective further enhancement
- This PhD has ToxicIA as a case study

Introduction

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 transfered to VAADER team for perspective further enhancement
- This PhD has ToxicIA as a case study

Introduction

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 transfered to VAADER team for perspective further enhancement
- This PhD has ToxicIA as a case study

Introduction

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 transfered to VAADER team for perspective further enhancement
- This PhD has ToxicIA as a case study

Introduction

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 transfered to VAADER team for perspective further enhancement
- This PhD has ToxicIA as a case study

Introduction

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 transfered to VAADER team for perspective further enhancement
- This PhD has ToxicIA as a case study

Compromising Emanations Detection

Target System With Video Display

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

≈ 10 m

Compromising Emanations

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

+ Adjustable Interpretation
− Poor Retrieval Performances

Denoising: Autoencoder, BM3D

Optical Character Recognition: Tesseract

Method2: Mask R-CNN [5]

+ Good Retrieval Performances
+ Character Masks Available
− Heavy Computations
− Dedicated Training

Segmentation & Classification:

Retrieved characters & their positions (+ masks)

3/ Further Processing

Key Word Recognition

Alert found: confidential

Alarm Raising for Human Action

System Shutdown

Compromising Emanations Detection

Target System With Video Display

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

≈ 10 m

Compromising Emanations

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

+ Adjustable Interpretation
− Poor Retrieval Performances

Denoising: Autoencoder, BM3D

Optical Character Recognition: Tesseract

Method2: Mask R-CNN [5]

+ Good Retrieval Performances
+ Character Masks Available
− Heavy Computations
− Dedicated Training

Segmentation & Classification:

Retrieved characters & their positions (+ masks)

3/ Further Processing

Key Word Recognition

Alert found: confidential

Alarm Raising for Human Action

System Shutdown

Compromising Emanations Detection

Target System With Video Display

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

≈ 10 m

Compromising Emanations

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

+ Adjustable Interpretation
− Poor Retrieval Performances

Denoising: Autoencoder, BM3D

Optical Character Recognition: Tesseract

Method2: Mask R-CNN [5]

+ Good Retrieval Performances
+ Character Masks Available
− Heavy Computations
− Dedicated Training

Segmentation & Classification:

Retrieved characters & their positions (+ masks)

3/ Further Processing

Key Word Recognition

Alert found: confidential

Alarm Raising for Human Action

System Shutdown

Compromising Emanations Detection

Target System With Video Display

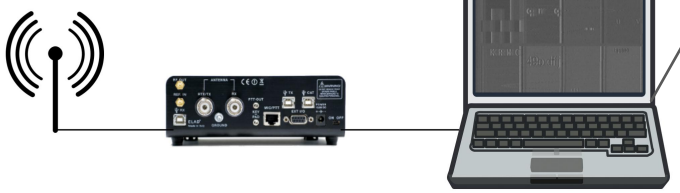
Display signal can be digital (e.g. DVI, DP, HDMI) or analog (e.g. VGA).

≈ 10 m

Compromising Emanations

Current Interception System to be Embedded

Antenna — Software-Defined Radio — Laptop

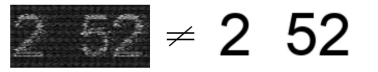


Bilog — Ettus X310 100MHz — Intel Xeon W-2125 Nvidia GTX1080 Ti

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

+ Adjustable Interpretation
− Poor Retrieval Performances

Denoising: Autoencoder, BM3D

Optical Character Recognition: Tesseract

Method2: Mask R-CNN [5]

+ Good Retrieval Performances
+ Character Masks Available
− Heavy Computations
− Dedicated Training

Segmentation & Classification:

Retrieved characters & their positions (+ masks)

3/ Further Processing

Key Word Recognition

Alarm Raising for Human Action

System Shutdown

Compromising Emanations Detection

Target System With Video Display

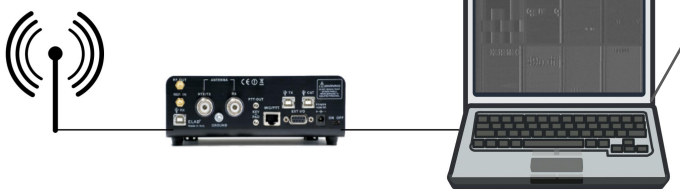
Display signal can be digital (e.g. DVI, DP, HDMI) or analog (e.g. VGA).

≈ 10 m

Compromising Emanations

Current Interception System to be Embedded

Antenna — Software-Defined Radio — Laptop

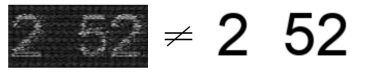


Bilog — Ettus X310 100MHz — Intel Xeon W-2125 Nvidia GTX1080 Ti

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

\+ Adjustable Interpretation
− Poor Retrieval Performances

Denoising: Autoencoder, BM3D

Optical Character Recognition: Tesseract

Method2: Mask R-CNN [5]

\+ Good Retrieval Performances
\+ Character Masks Available
− Heavy Computations
− Dedicated Training

Segmentation & Classification:

Retrieved characters & their positions (+ masks)

3/ Further Processing

Key Word Recognition

Alarm Raising for Human Action

System Shutdown

Compromising Emanations Detection

Target System With Video Display

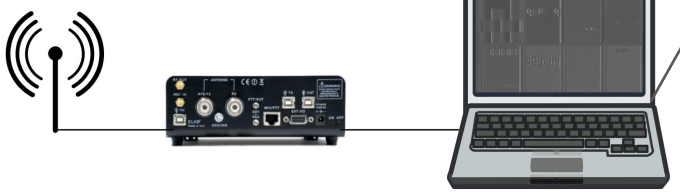
Display signal can be digital (e.g. DVI, DP, HDMI) or analog (e.g. VGA).

≈ 10 m

Compromising Emanations

Current Interception System to be Embedded

Antenna — Software-Defined Radio — Laptop

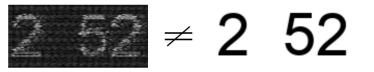


Bilog — Ettus X310 100MHz — Intel Xeon W-2125 Nvidia GTX1080 Ti

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

- \+ Adjustable Interpretation
- − Poor Retrieval Performances

Denoising: Autoencoder, BM3D

Optical Character Recognition: Tesseract

Method2: Mask R-CNN [5]

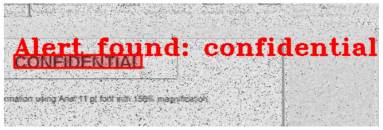
- \+ Good Retrieval Performances
- \+ Character Masks Available
- − Heavy Computations
- − Dedicated Training

Segmentation & Classification:

Retrieved characters & their positions (+ masks)

3/ Further Processing

Key Word Recognition



→ Alarm Raising for Human Action

→ System Shutdown

Statistical Image Denoising

Noisy Sample

Denoising Methods

Denoised Sample

Non-Statistical

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

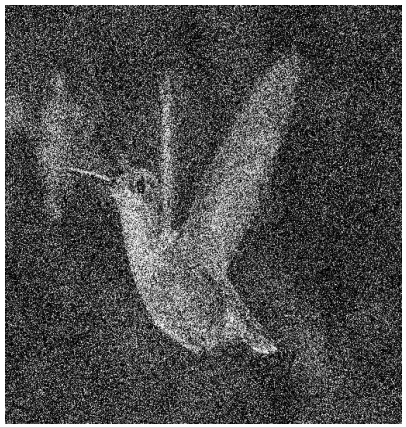
e.g. : Filters (Median, Mean, ...)
Block-Matching 3D (BM3D)
Transform Domain (FFT)

Statistical

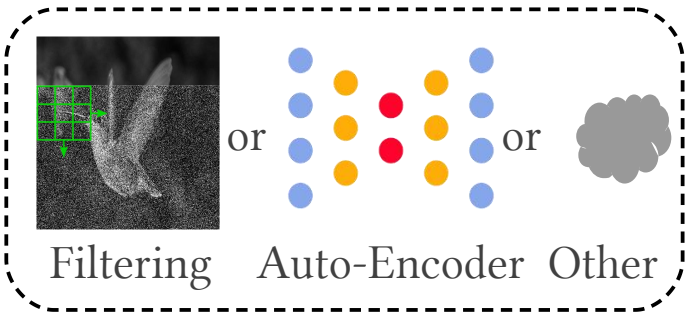
\+ Support several noise models
\+ High SNR improvements
− Heavy computations

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

Statistical Image Denoising



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)

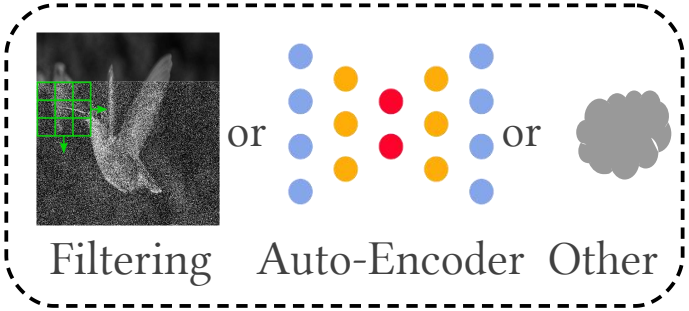
Statistical

\+ Support several noise models
\+ High SNR improvements
− Heavy computations

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

Statistical Image Denoising

Noisy Sample



Denoising Methods

Denoised Sample

Non-Statistical

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

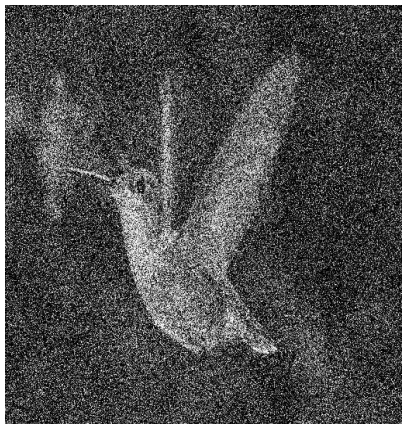
e.g. : Filters (Median, Mean, ...)
Block-Matching 3D (BM3D)
Transform Domain (FFT)

Statistical

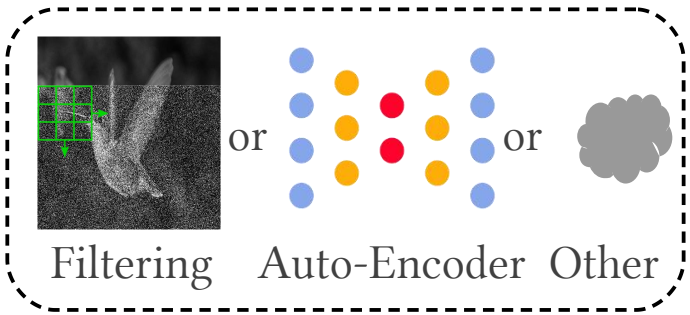
\+ Support several noise models
\+ High SNR improvements
\- Heavy computations

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

Statistical Image Denoising



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)

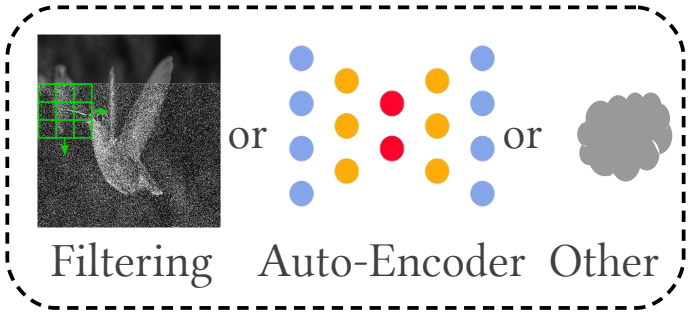
Statistical

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

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

Statistical Image Denoising

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)

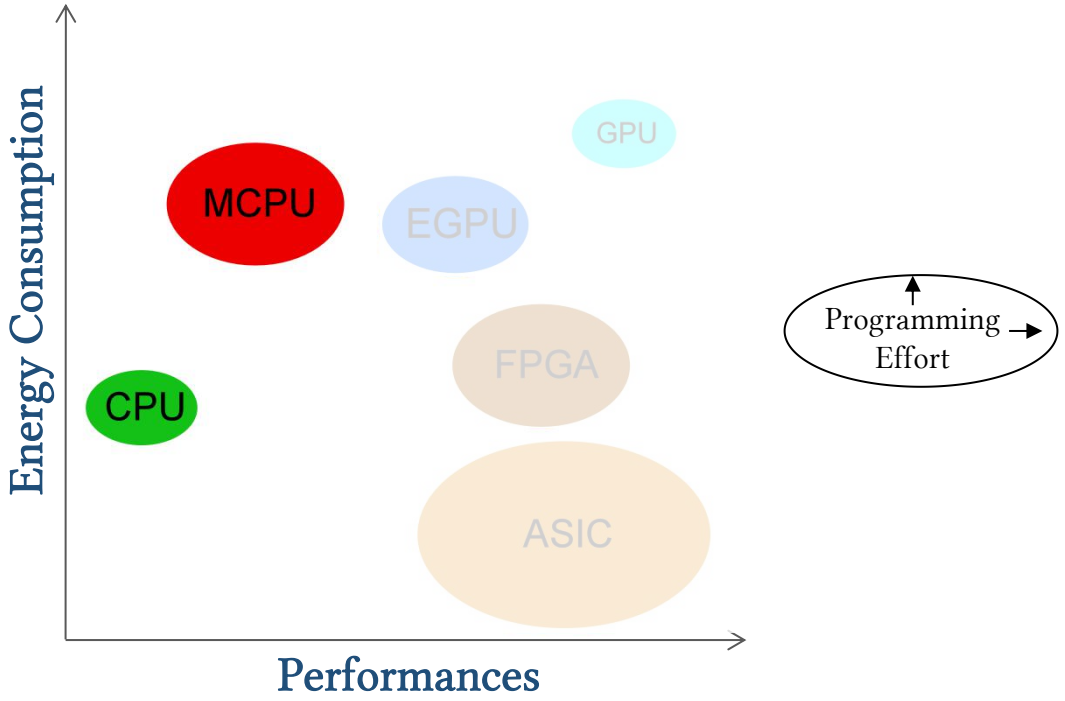
Statistical

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

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

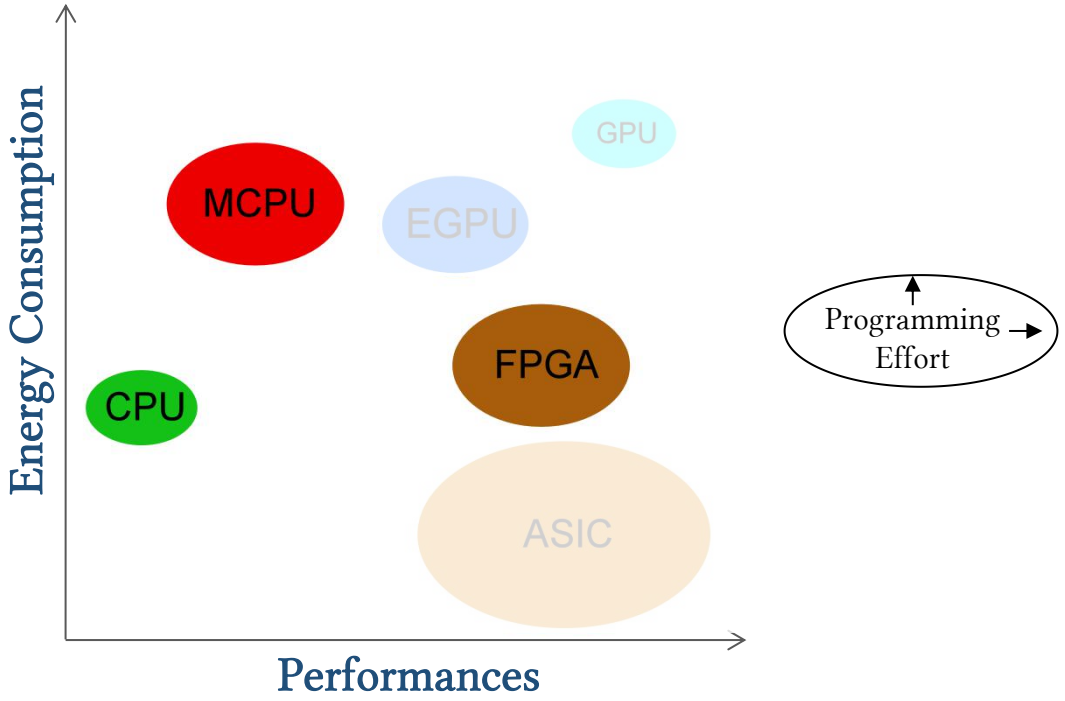
Near Sensor Platforms for Statistical Denoising

- **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



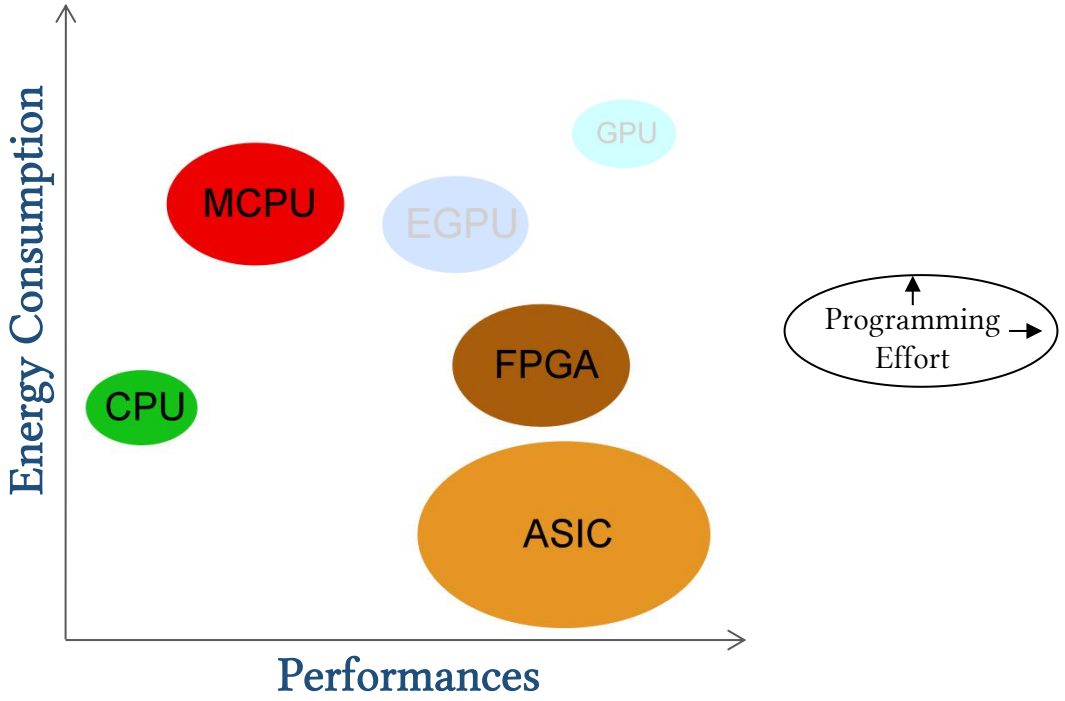
Near Sensor Platforms for Statistical Denoising

- **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



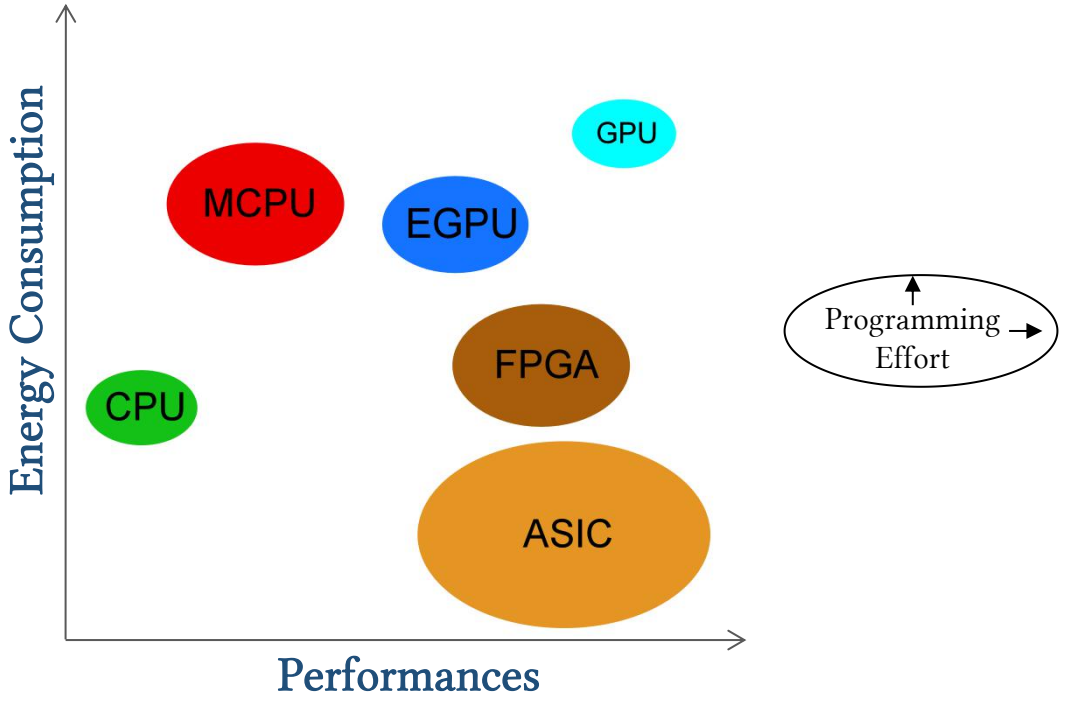
Near Sensor Platforms for Statistical Denoising

- **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



Near Sensor Platforms for Statistical Denoising

- **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



Perspectives for ToxicIA

Network Reduction

- Connection pruning
- Weight quantization/sharing
- Huffman coding

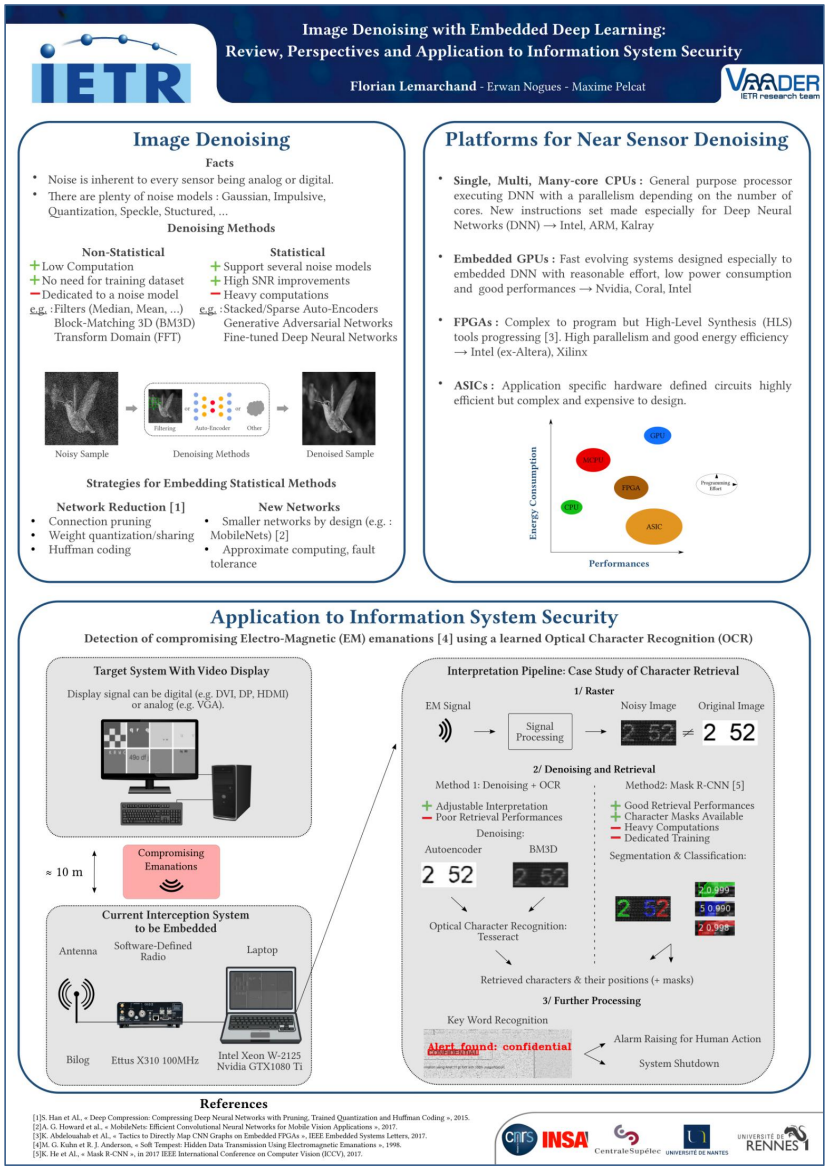
New Networks

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

Training Phase Enhancement

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

Questions & Discussions



Thank you for your attention!

For questions --> Poster Session at 18:15 p.m.

Contact :

florian.lemarchand@insa-rennes.fr