Naval Cybersecurity in the Age of AI: deceptive ISAR Images Generation with GANs

1st IEEE LCN Workshop on Maritime Communication and Security (MarCaS)

Giulio Meucci, Bertan Karahoda, Amir Hosein Oveis,
Francesco Mancuso, *Edmond Jajaga, Alessandro Cantelli-Forti*

Daytona Beach, FL, USA - 05 October 2023

Photo by Chris Pagan on Unsplash

Motivation

- **Supply chain attacks**

  - Compromising the radar system, altering or injecting false data to create misleading radar readings, which could misdirect defense resources

  - National interests in compromising a system sold to another country, to mislead or disable the operational capabilities of the buyer country and then create a tactical advantage
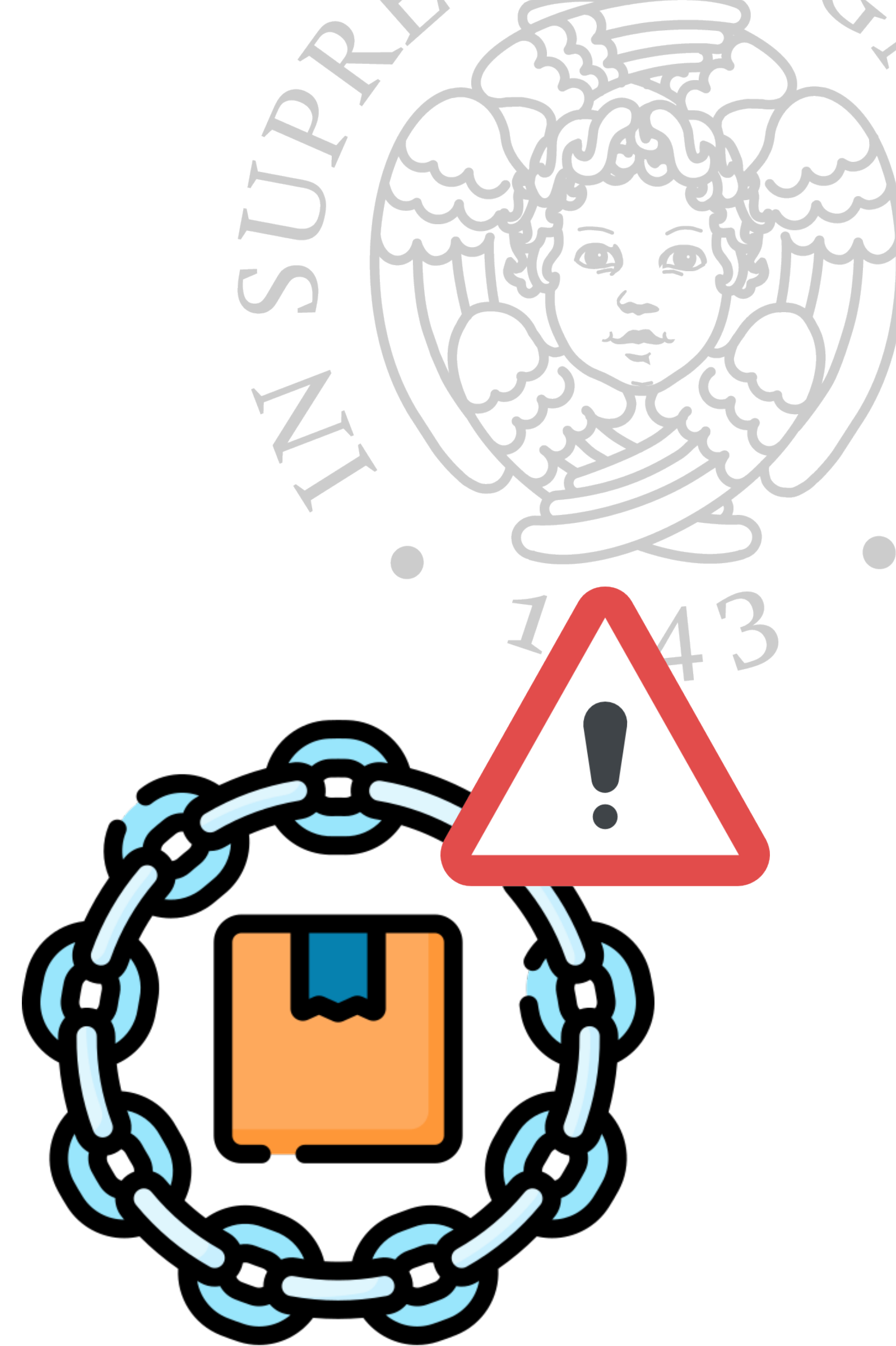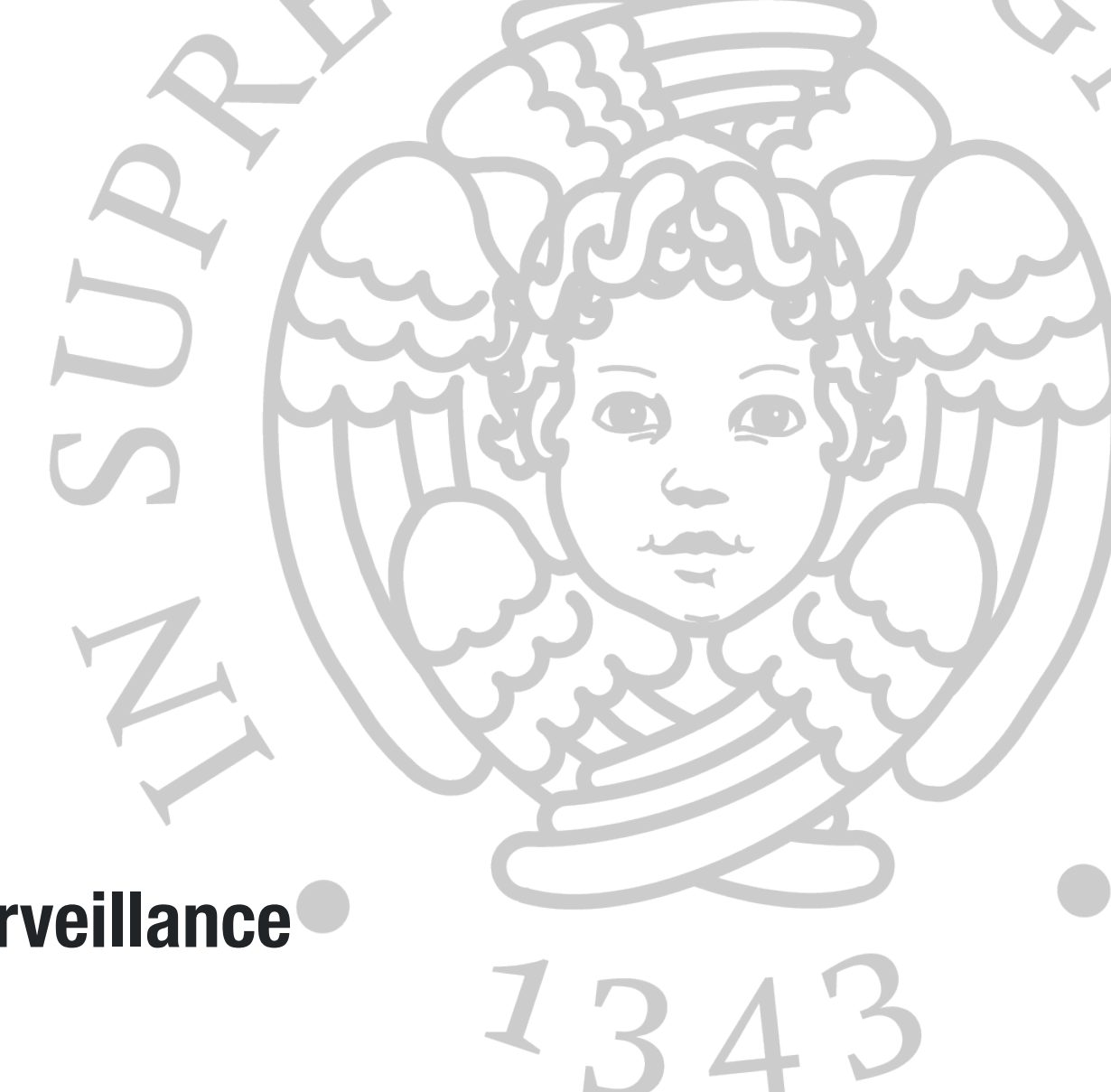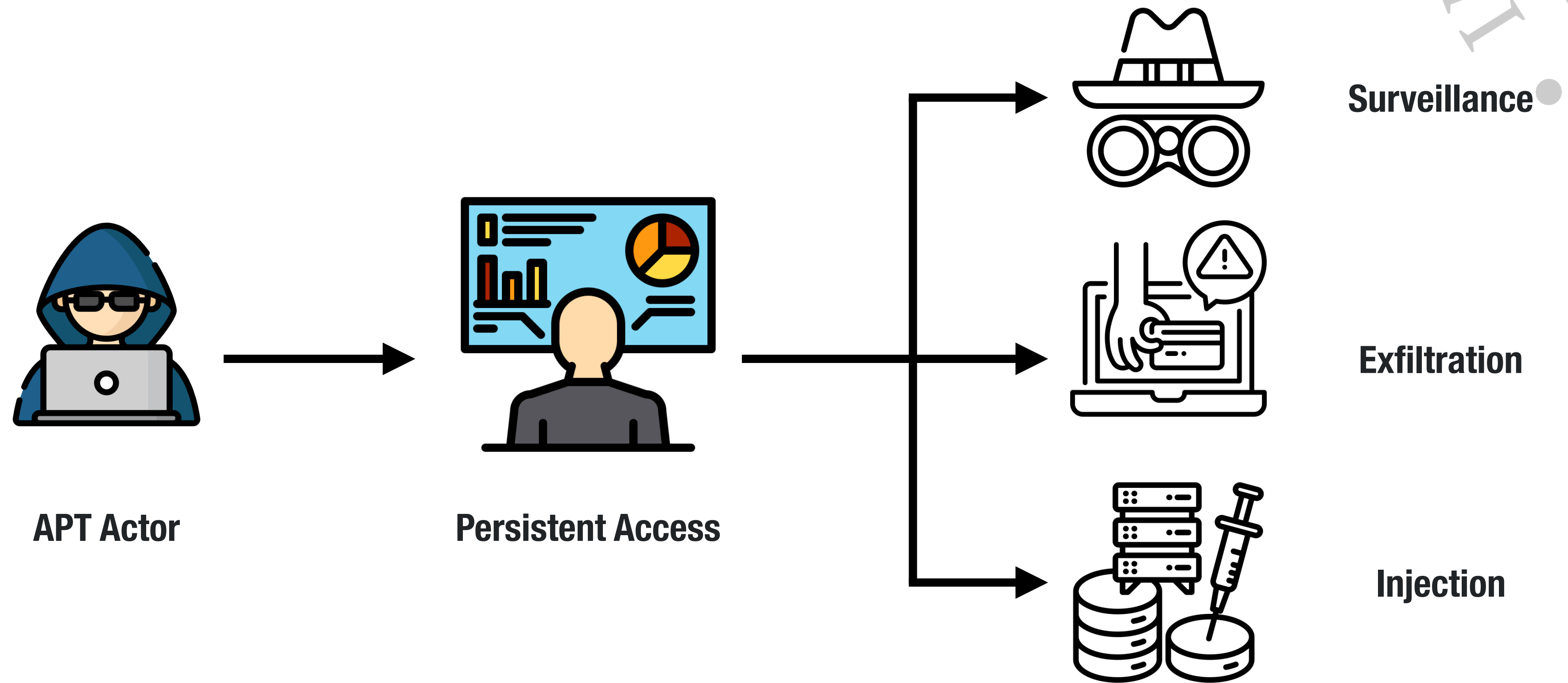
Presentation Outline
MarCaS 2023

- The Cyber Threat

- Inverse Synthetic Aperture Radar Imaging

- The proposed framework

- Experiment and results
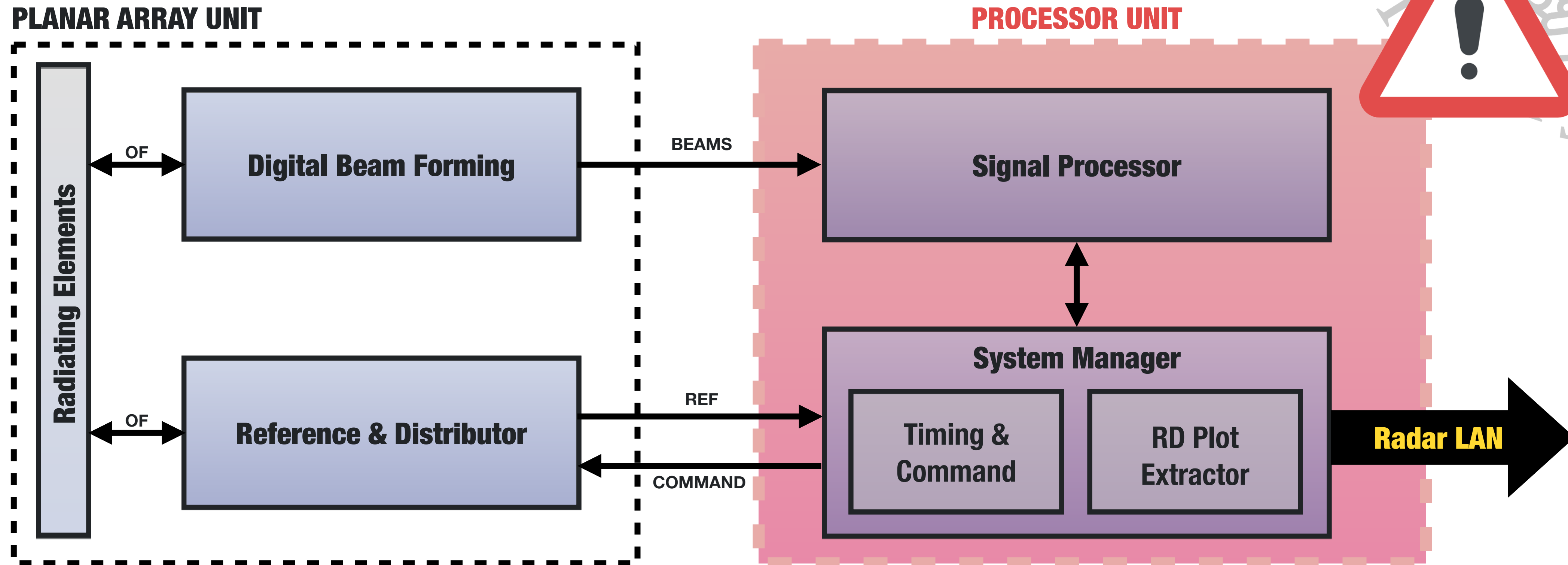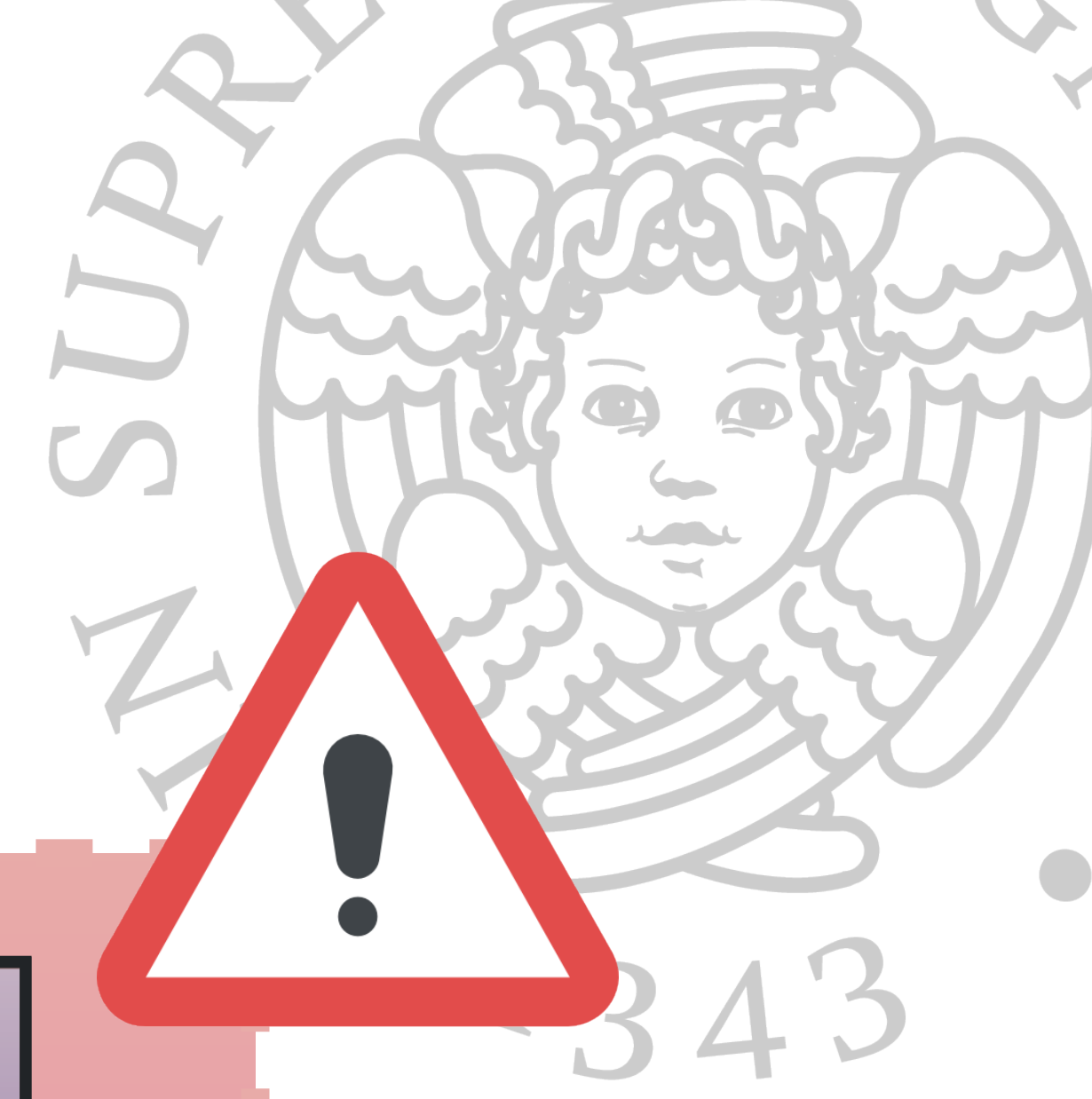
- Conclusion and future works
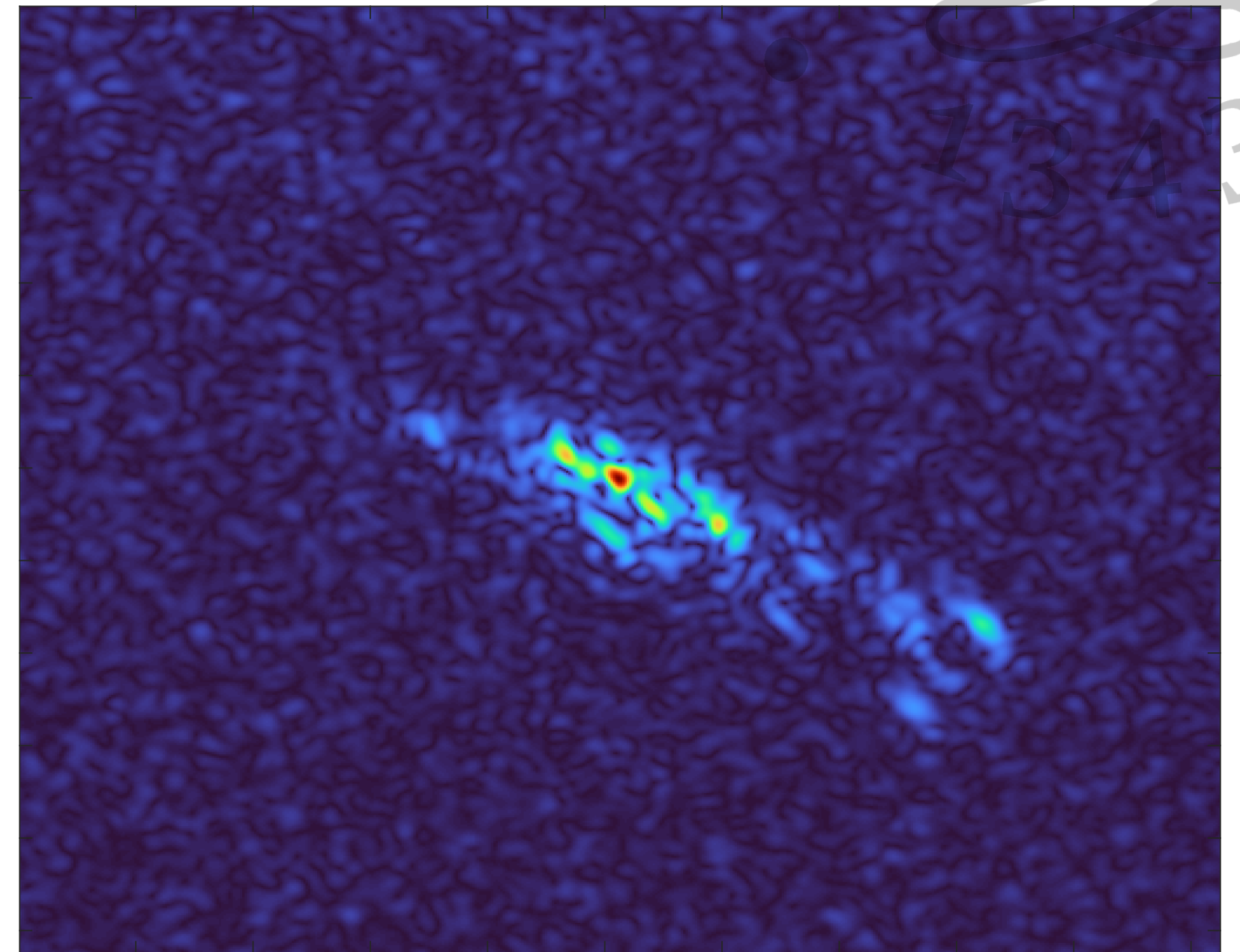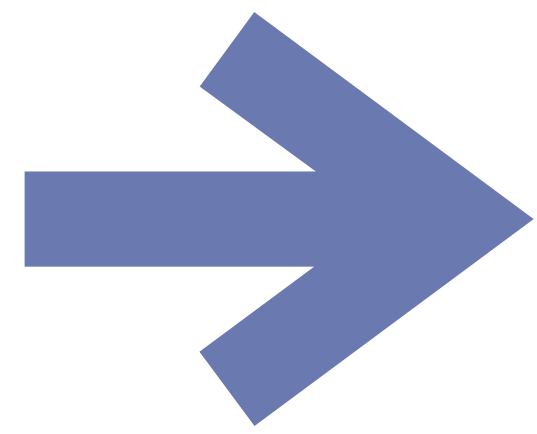
The Cyber Threat
Advanced Persistent Threat

APT Actor

Persistent Access

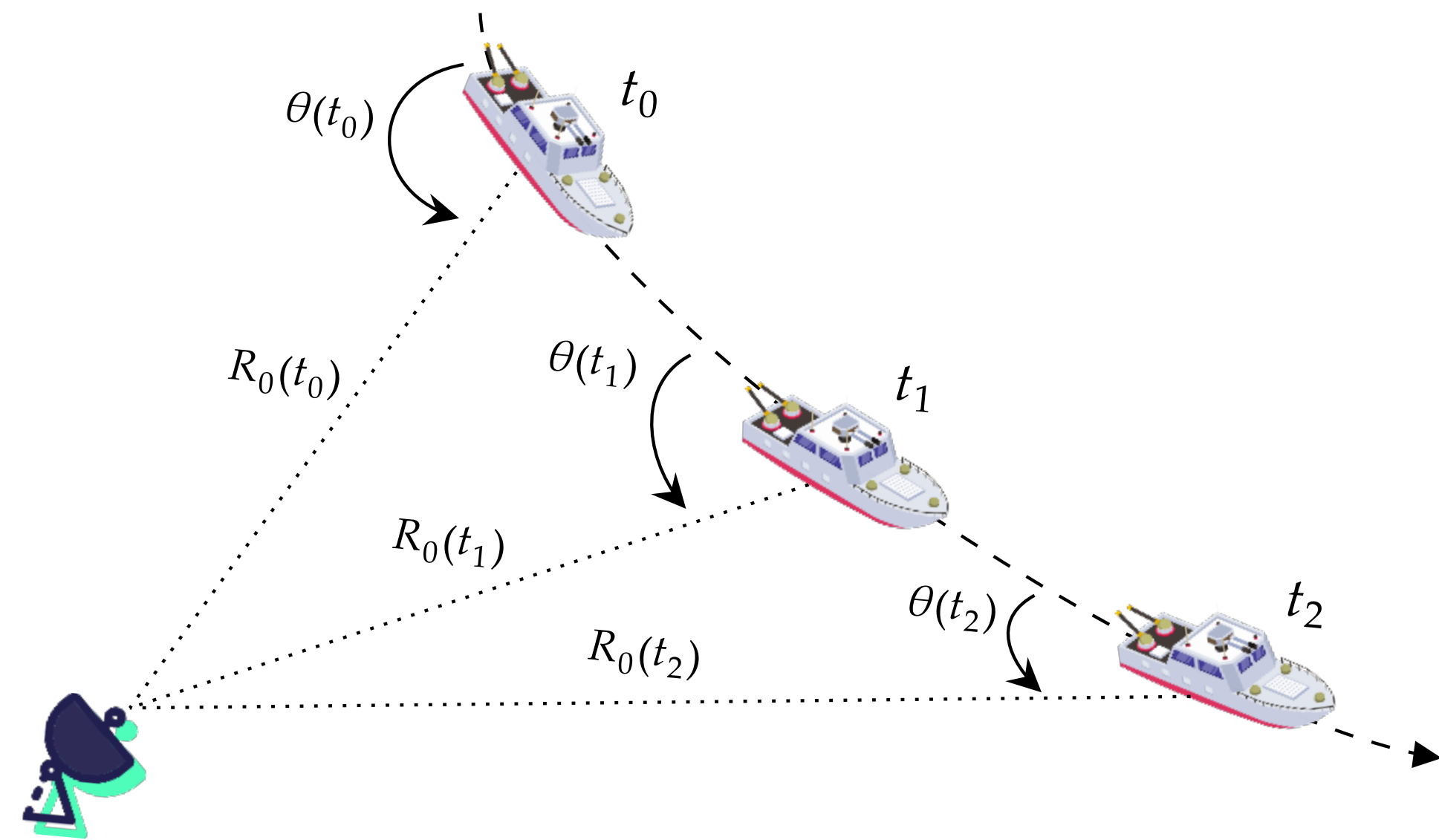Surveillance

Exfiltration

Injection

The Cyber Threat
Software Defined Radar System

ISAR Imaging
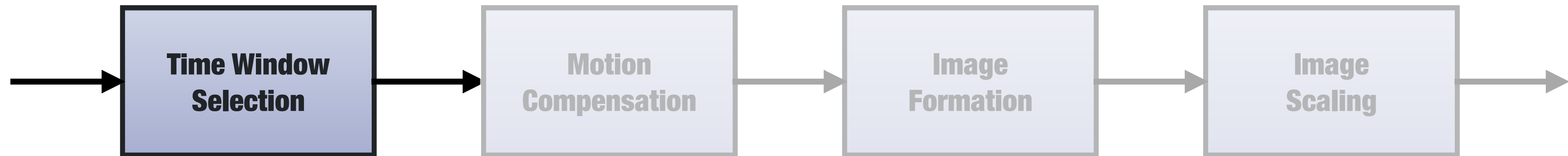## Inverse Synthetic Aperture Radar

ISAR Imaging
Image formation

$$S(f, n) = W(f, n) \iint_{x_1, x_2} f(x_1, x_2) \, e^{-j\frac{4\pi f}{c}[R_0(n) + x_2 \cos(\Omega n T_R) + x_1 \sin(\Omega n T_R)]} dx_1 dx_2$$

$$I(\tau, \nu) = 2D - FT \left[W(X_1, X_2) \iint_{x_1, x_2} f(x_1, x_2) \, e^{-j2\pi(x_1 X_1 + x_2 X_2)} dx_1 dx_2 \right] \quad \begin{cases} x_1 = \frac{c}{2 f_0 \Omega} \nu \\ x_2 = \frac{c}{2} \tau \end{cases}$$
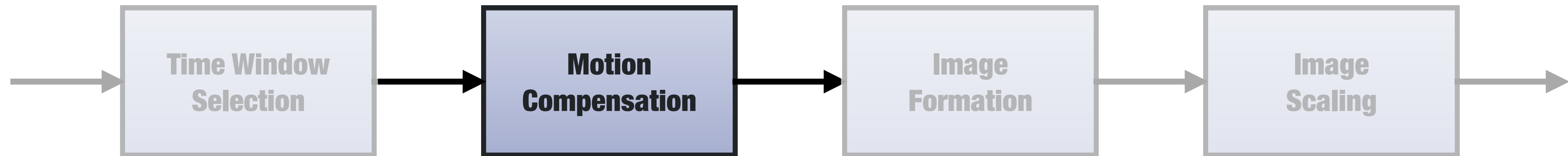
| Time Window Selection | → | Motion Compensation | → | Image Formation | → | Image Scaling |

ISAR Imaging
Image formation

$$S(f, n) = W(f, n) \iint_{x_1, x_2} f(x_1, x_2)\, e^{-j\frac{4\pi f}{c}[R(\ n) + x_2 \cos(\Omega n T_R) + x_1 \sin(\Omega n T_R)]}\, dx_1 dx_2$$

$$I(\tau, \nu) = 2D - FT\left[W(X_1, X_2) \iint_{x_1, x_2} f(x_1, x_2)\, e^{-j2\pi(x_1 X_1 + x_2 X_2)}\, dx_1 dx_2 \right] \qquad \begin{cases} x_1 = \frac{c}{2f_0 \Omega} \nu \\ x_2 = \frac{c}{2} \tau \end{cases}$$
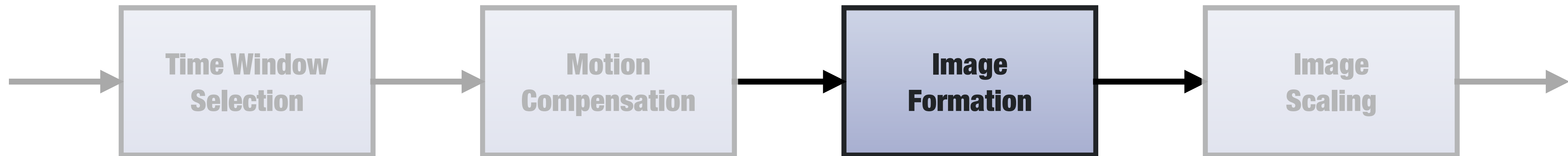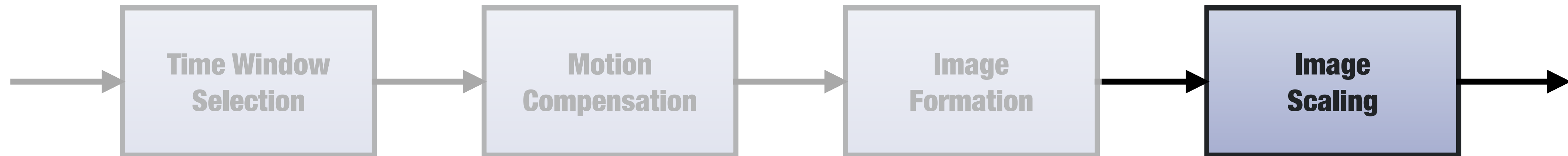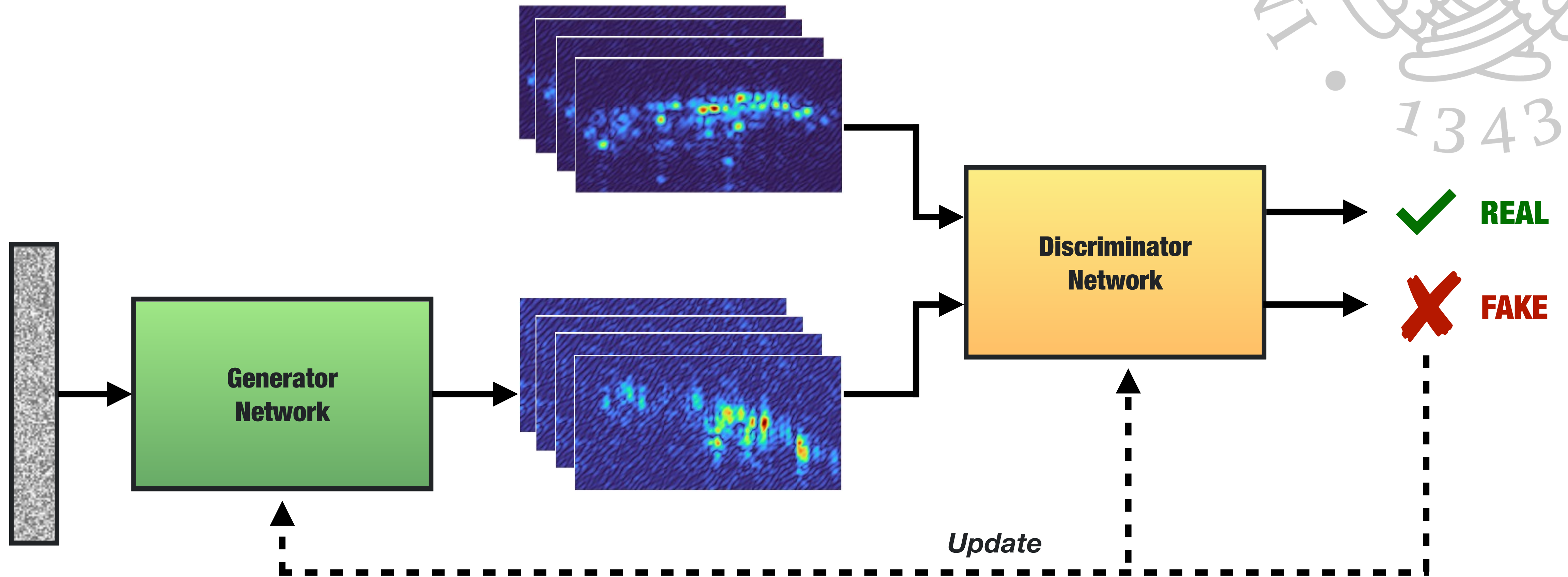
```
┌─────────────┐      ┌─────────────┐      ┌─────────────┐      ┌─────────────┐
│ Time Window │      │   Motion    │      │    Image    │      │    Image    │
│  Selection  │ ───► │Compensation │ ───► │  Formation  │ ───► │   Scaling   │
└─────────────┘      └─────────────┘      └─────────────┘      └─────────────┘
```

ISAR Imaging
Image formation

$$S(f,n) = W(f,n) \iint\limits_{x_1,x_2} f(x_1,x_2) \, e^{-j\frac{4\pi f}{c}[R_0(n)+x_2\cos(\Omega nT_R)+x_1\sin(\Omega nT_R)]} dx_1 dx_2$$

$$I(\tau,\nu) = 2D - FT\left[W(X_1,X_2) \iint\limits_{x_1,x_2} f(x_1,x_2) \, e^{-j2\pi(x_1 X_1 + x_2 X_2)} dx_1 dx_2\right]$$

$$\begin{cases} x_1 = \frac{c}{2f_0\Omega}\nu \\ x_2 = \frac{c}{2}\tau \end{cases}$$

```
┌──────────────┐     ┌──────────────┐     ┌──────────────┐     ┌──────────────┐
│ Time Window  │     │    Motion    │     │    Image     │     │    Image     │
│  Selection   │ ──▶ │ Compensation │ ──▶ │  Formation   │ ──▶ │   Scaling    │
└──────────────┘     └──────────────┘     └──────────────┘     └──────────────┘
```

ISAR Imaging
Image formation

$$S(f,n) = W(f,n) \iint\limits_{x_1,x_2} f(x_1,x_2)\, e^{-j\frac{4\pi f}{c}[R_0(n)+x_2\cos(\Omega nT_R)+x_1\sin(\Omega nT_R)]}\, dx_1 dx_2$$

$$I(\tau,\nu) = 2D-FT\left[W(X_1,X_2) \iint\limits_{x_1,x_2} f(x_1,x_2)\, e^{-j2\pi(x_1 X_1 + x_2 X_2)}\, dx_1 dx_2\right]$$

$$\begin{cases} x_1 = \frac{c}{2f_0\Omega}\nu \\ x_2 = \frac{c}{2}\tau \end{cases}$$

```
Time Window     →     Motion     →     Image     →     Image
Selection             Compensation     Formation       Scaling
```

The proposed framework
Generative Adversarial Network

The proposed framework
Data Encoding
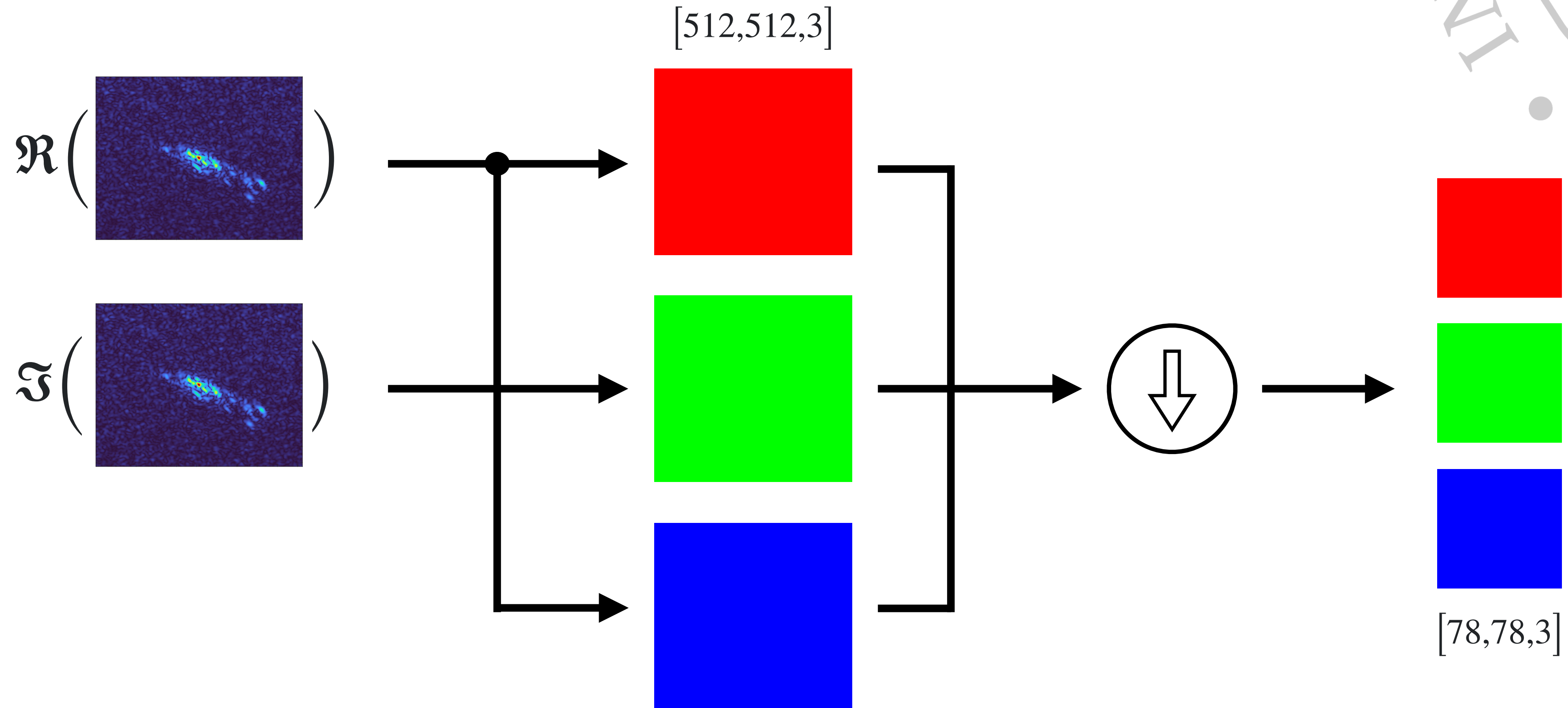
Experiment and results
Exploiting real data

Astice A5379
33.25 (L) x 6.47 (W) x 12 (H) [m]
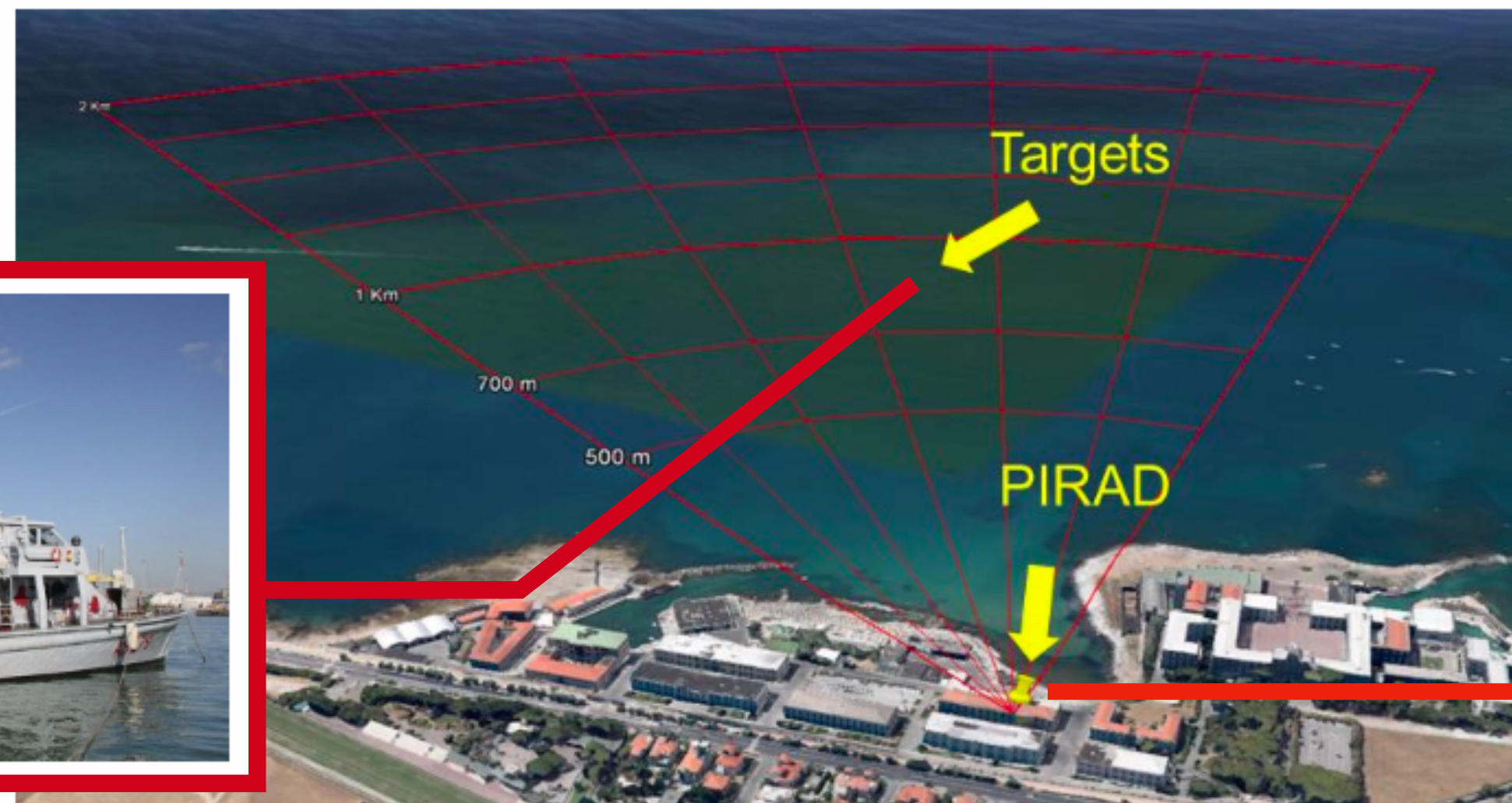
Istituto Vallauri, Livorno, Italy

Targets

PIRAD

Multi-channel X-Band Interferometric Radar

Training set: 720 ISAR images

Experiment and results
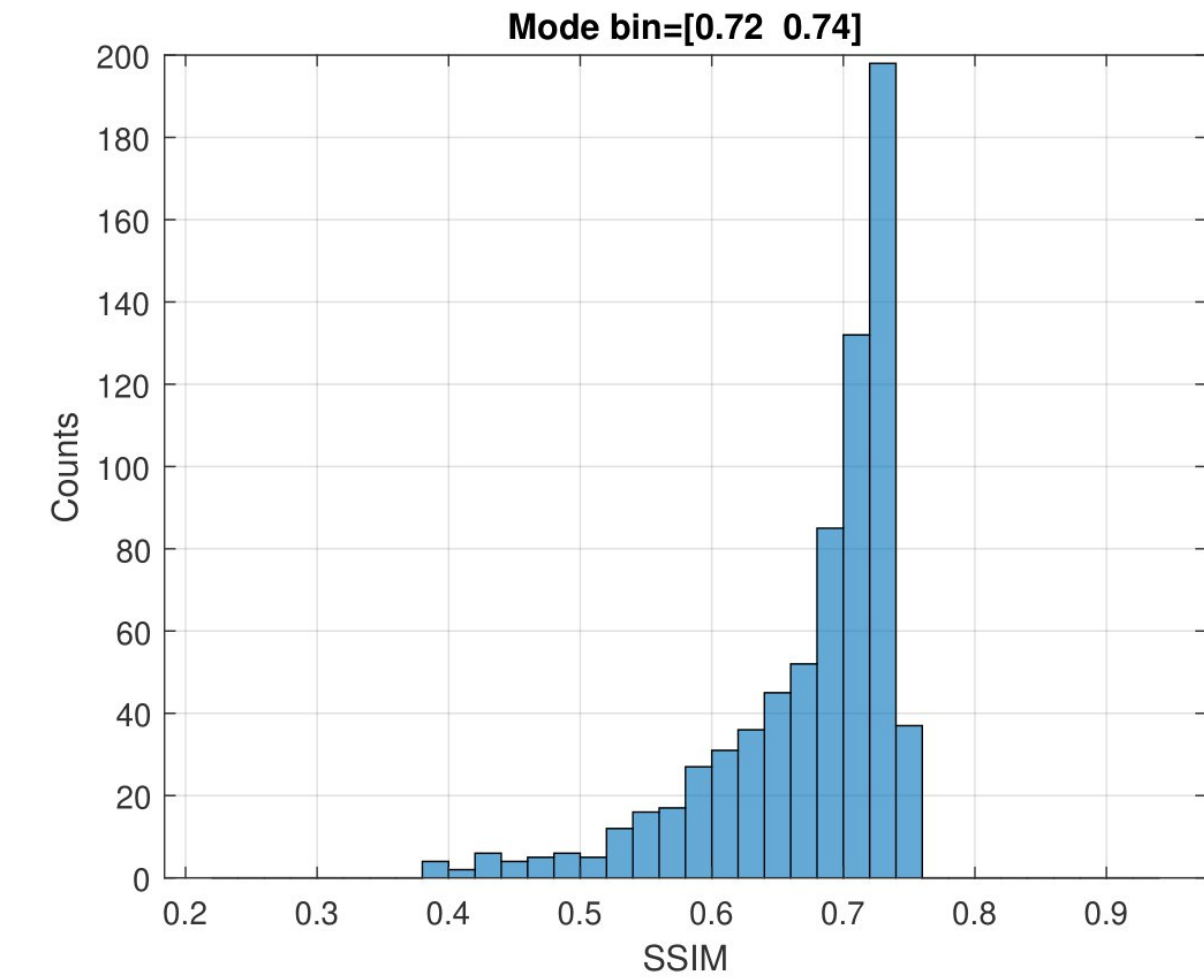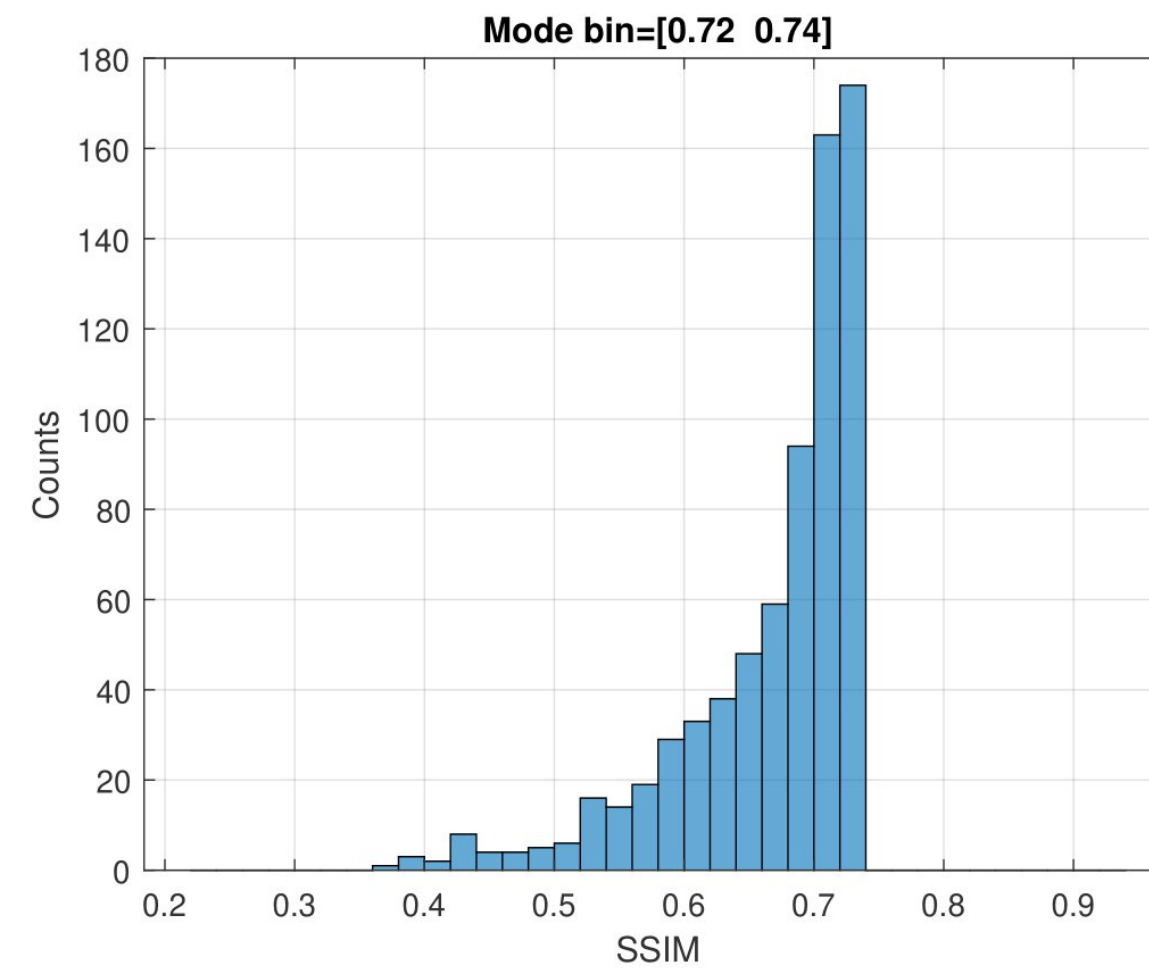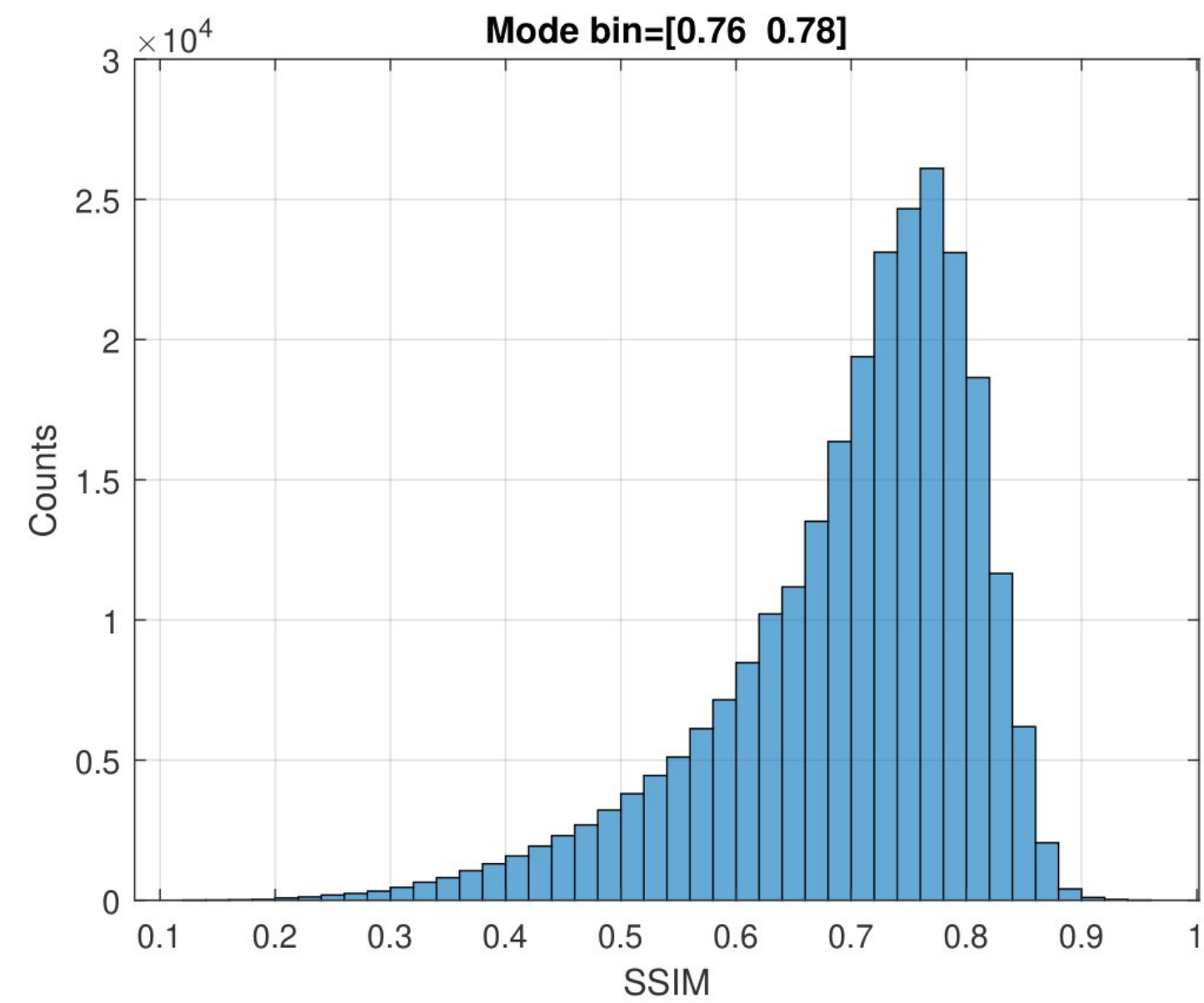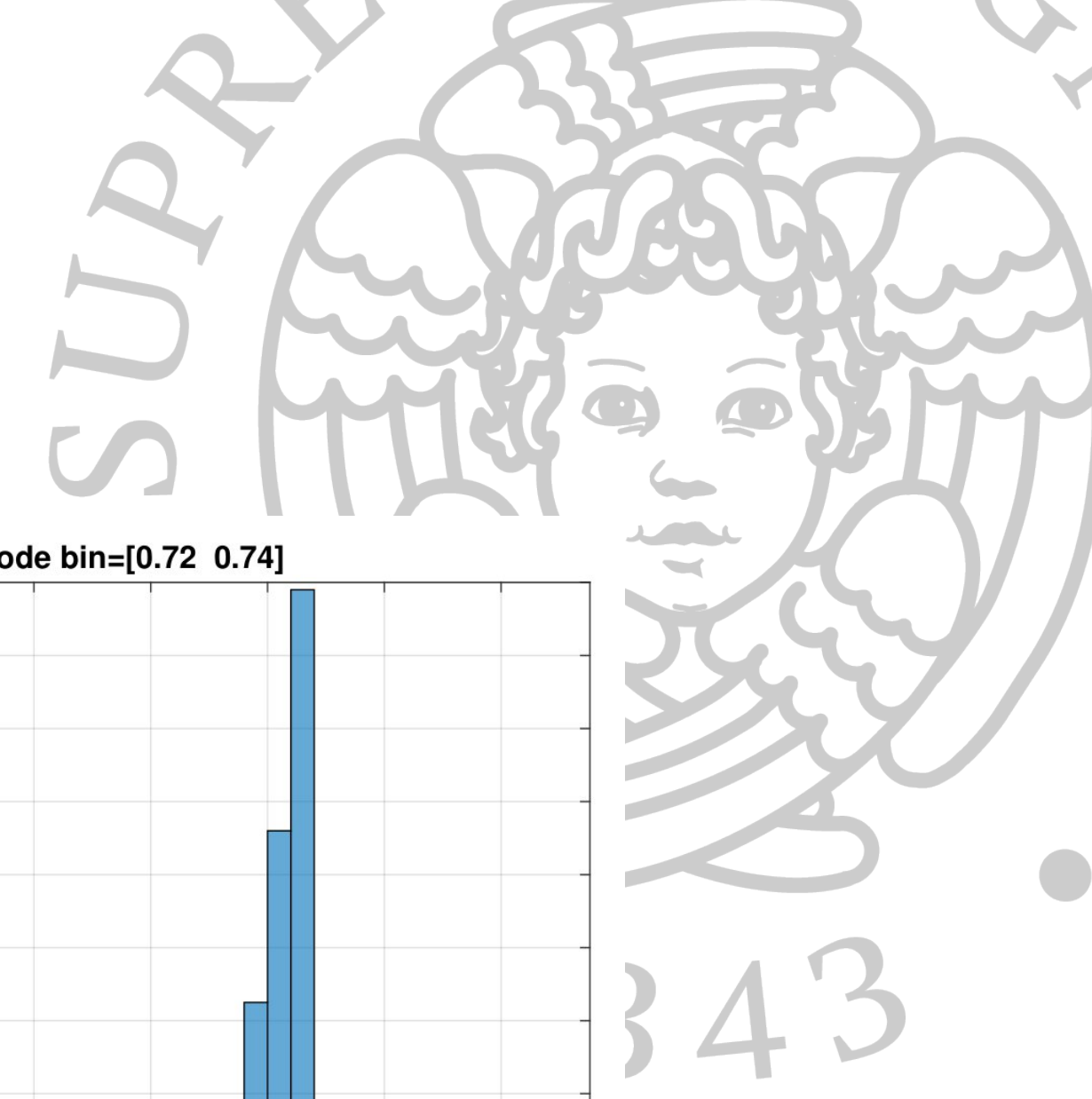## Exploiting real data
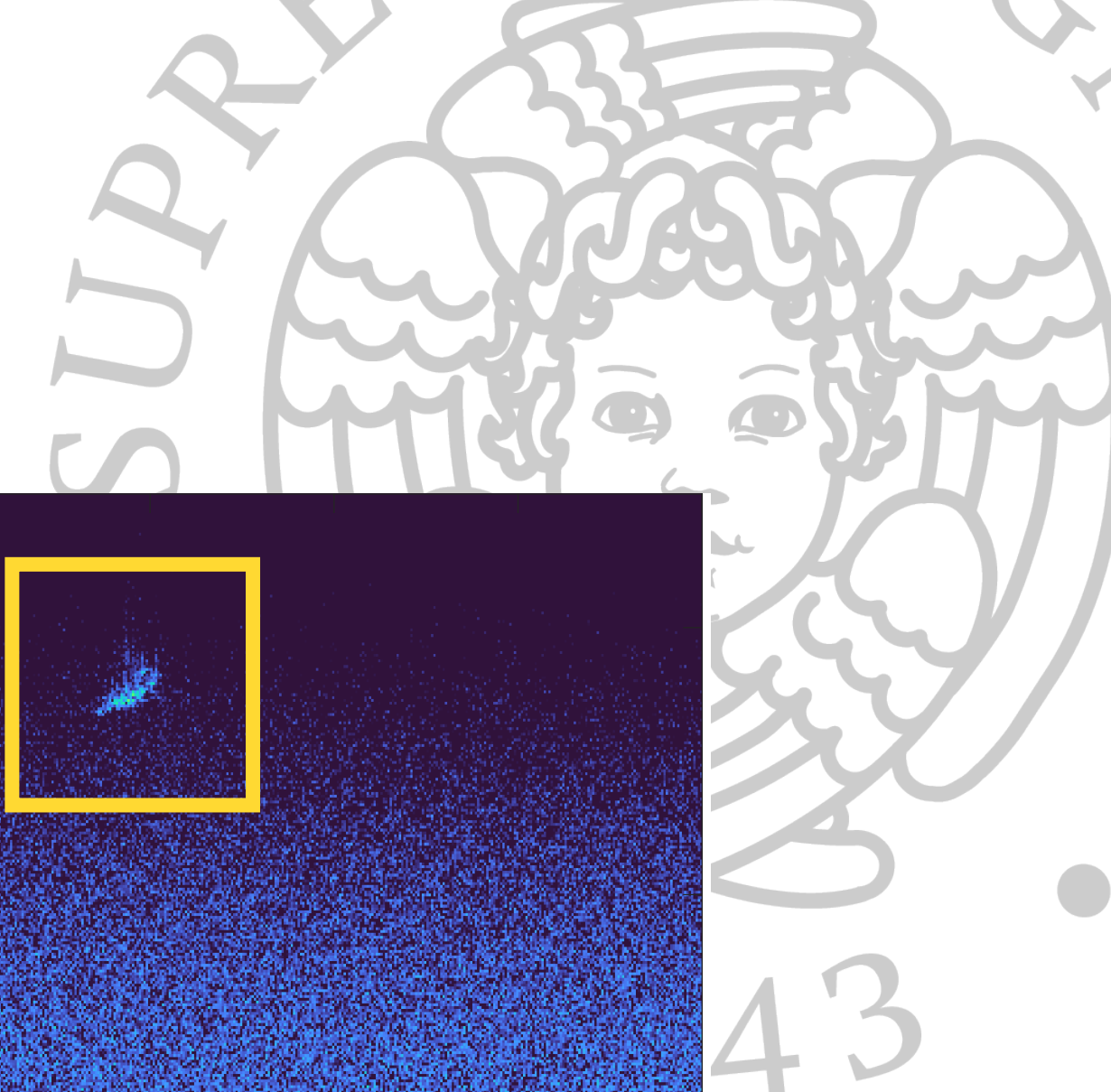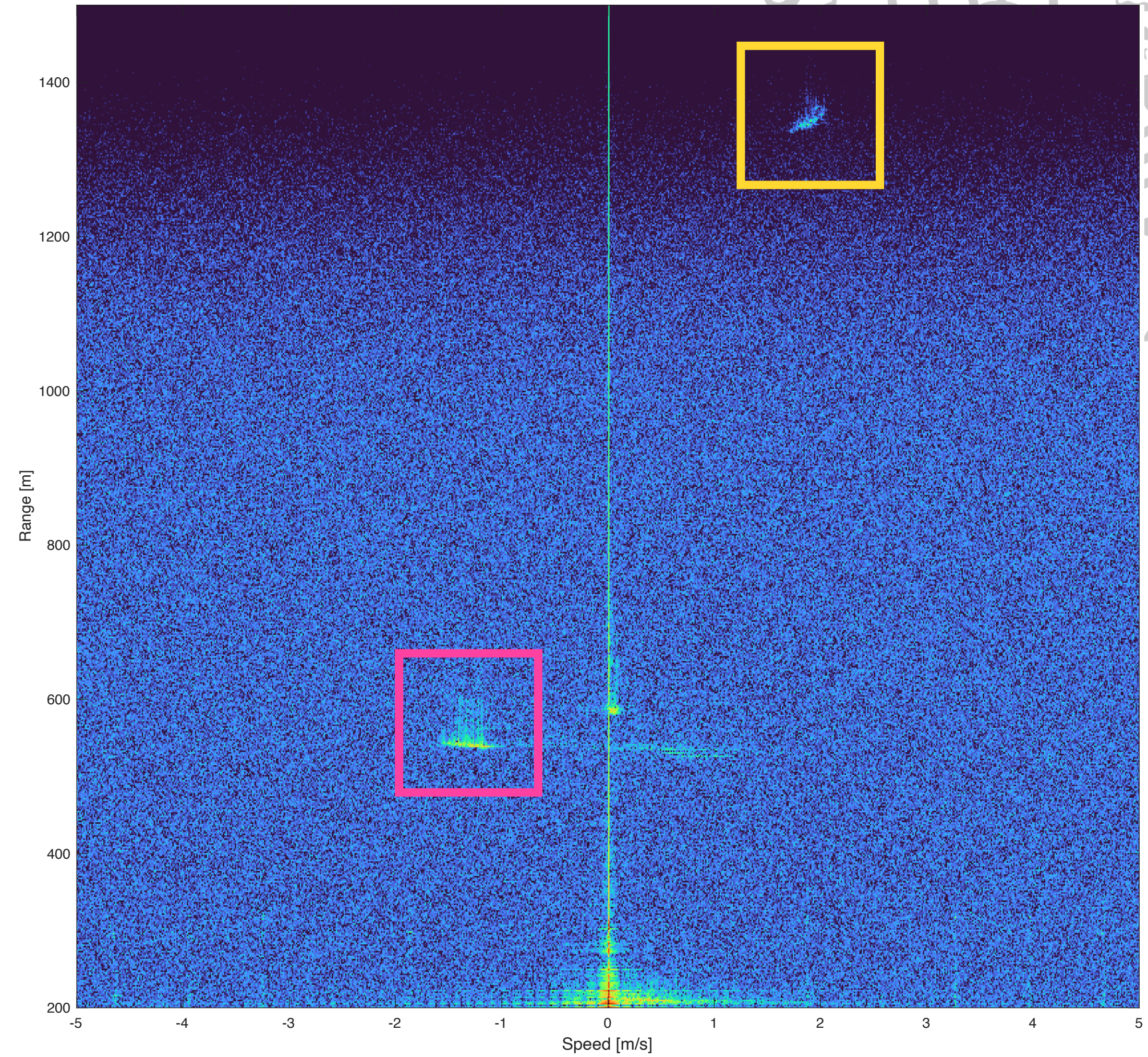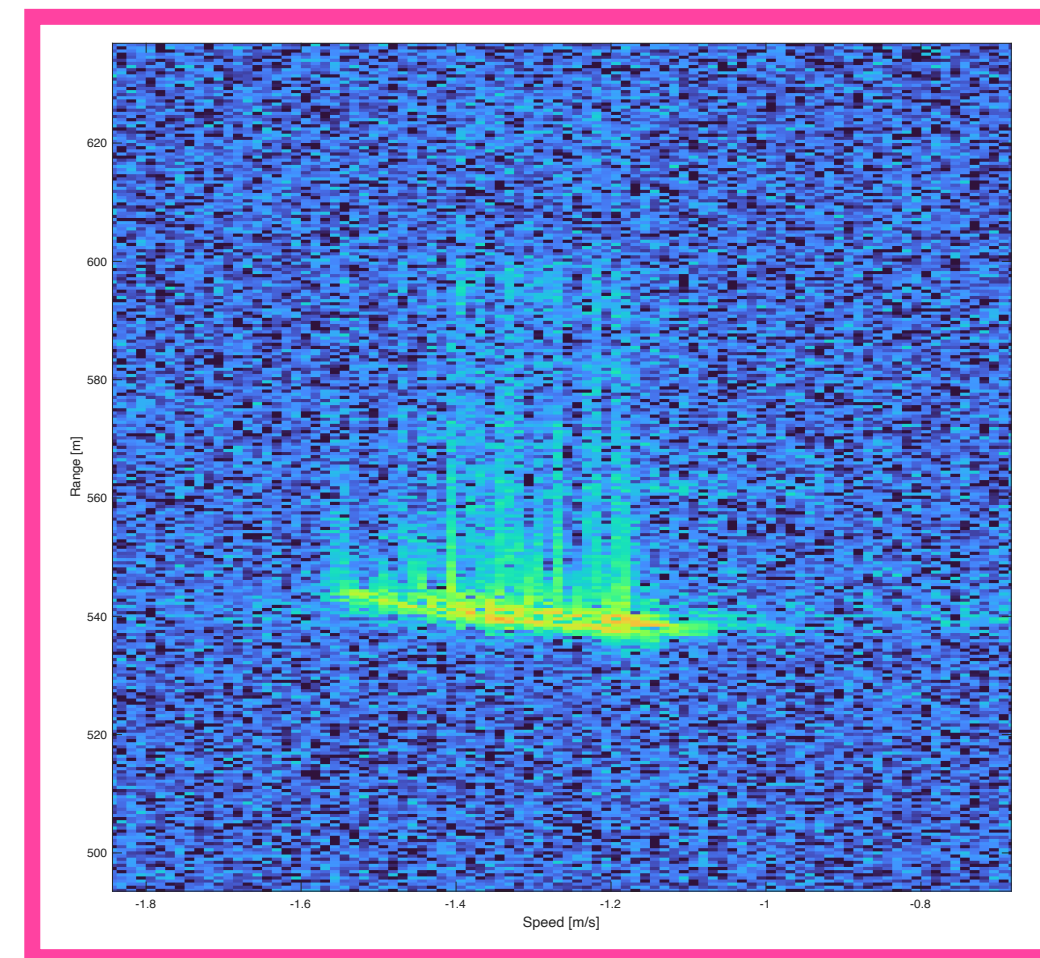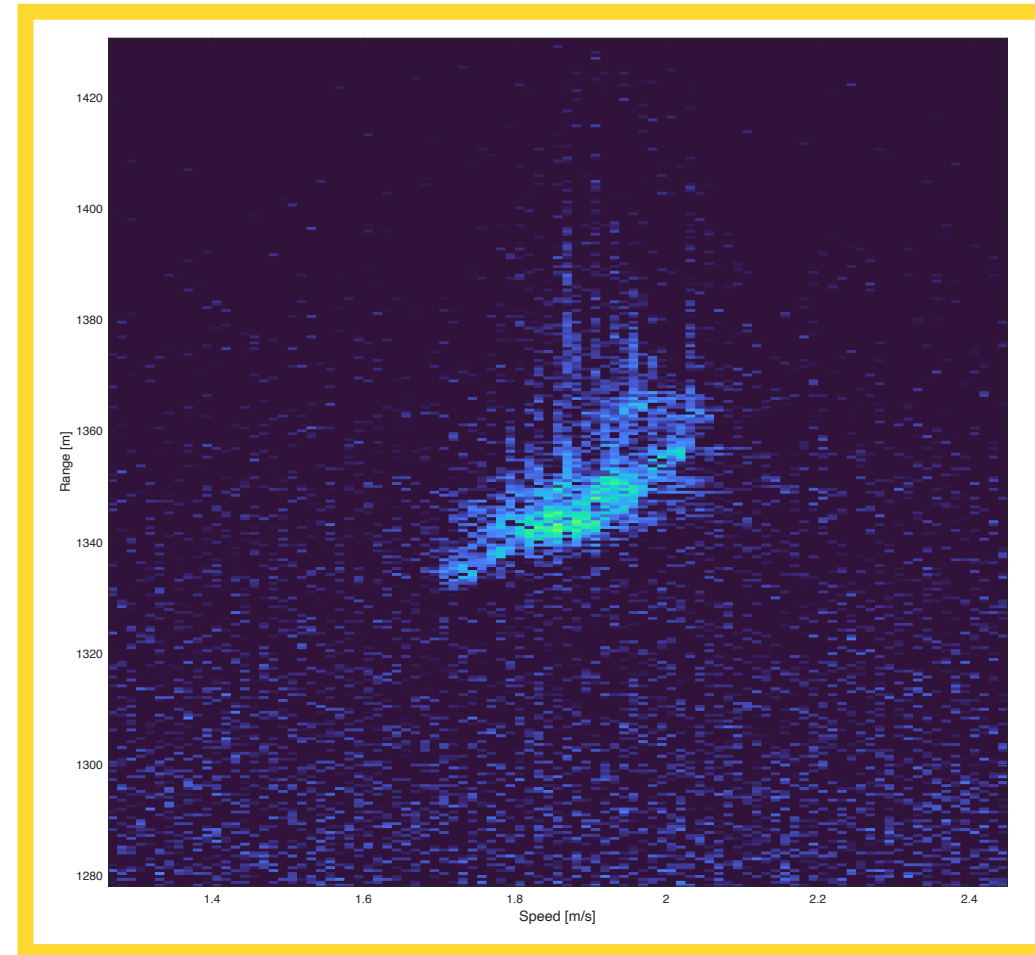
Experiment and results
Generated or real?
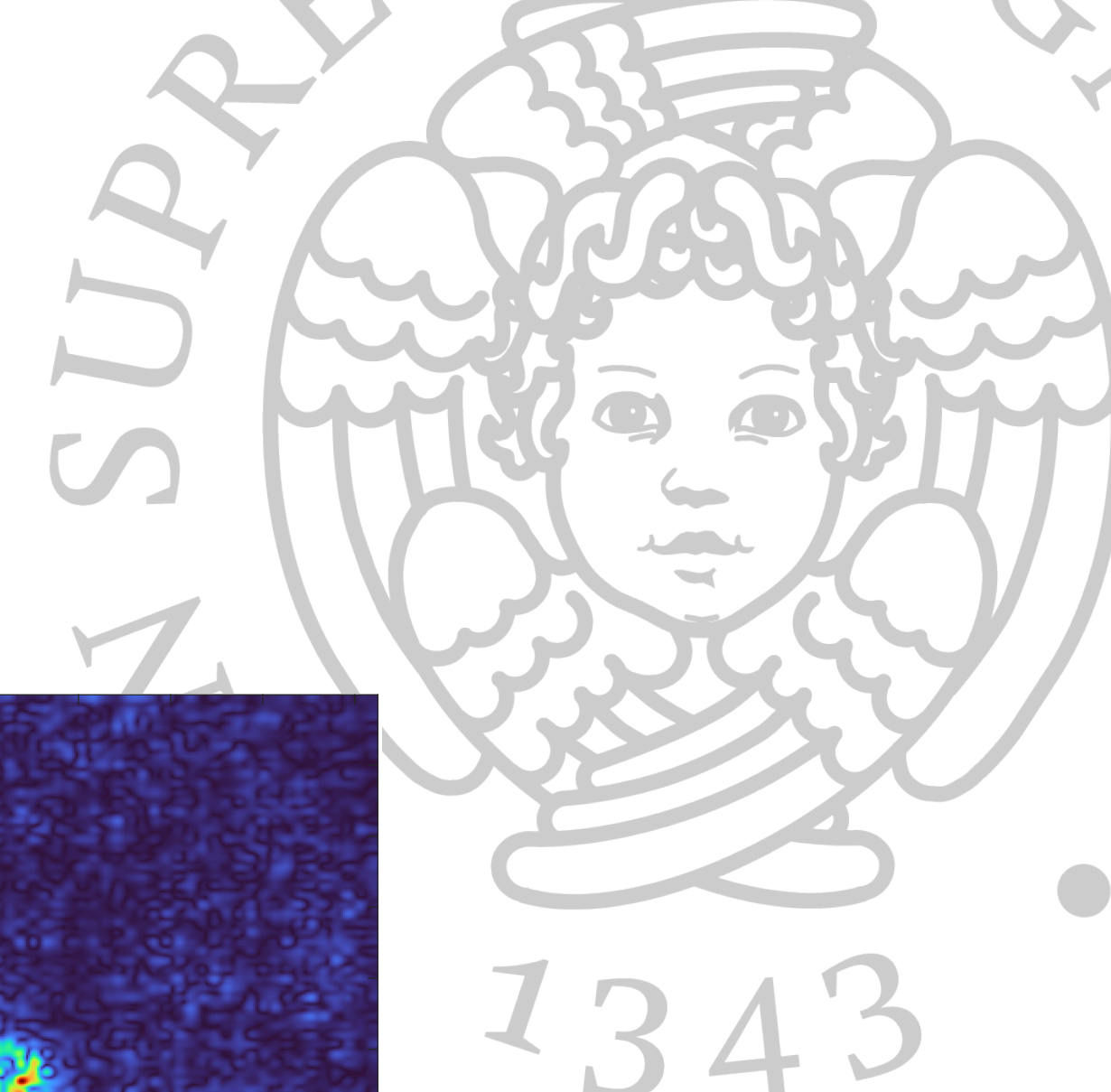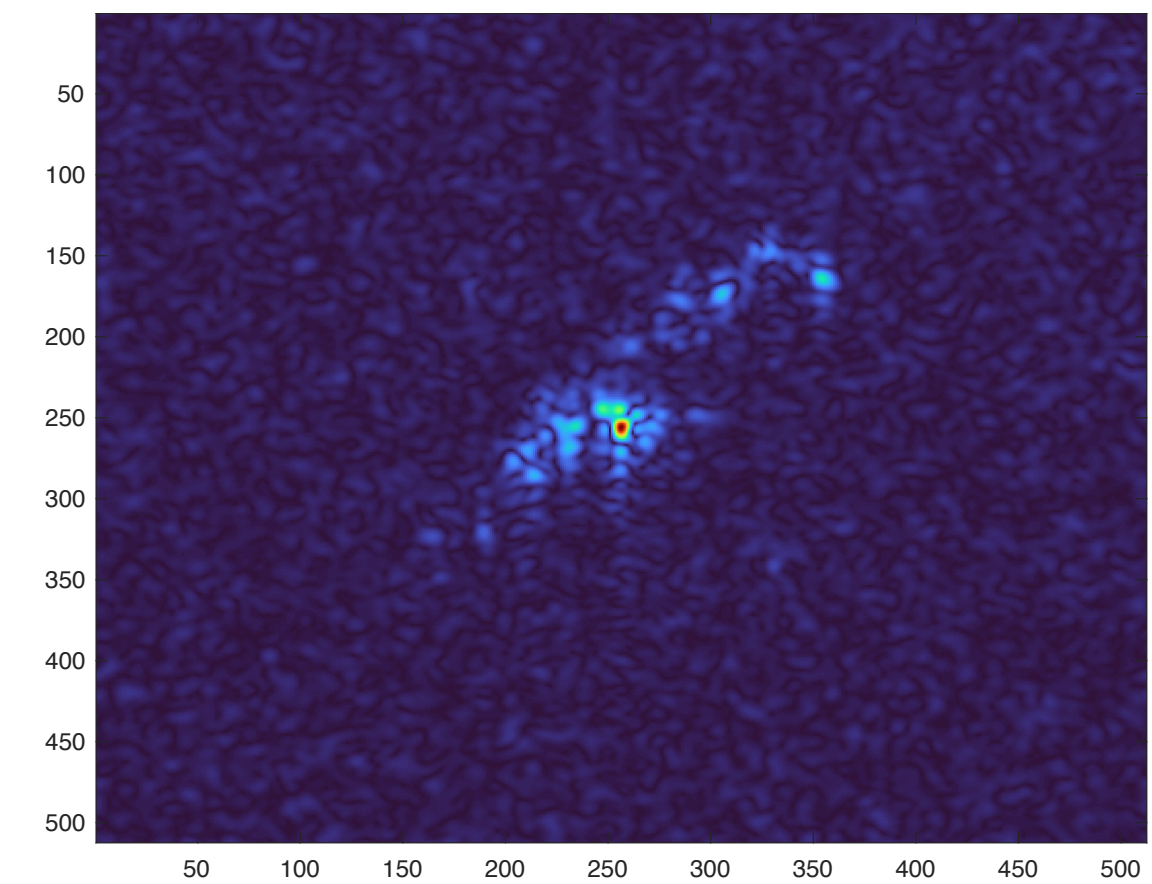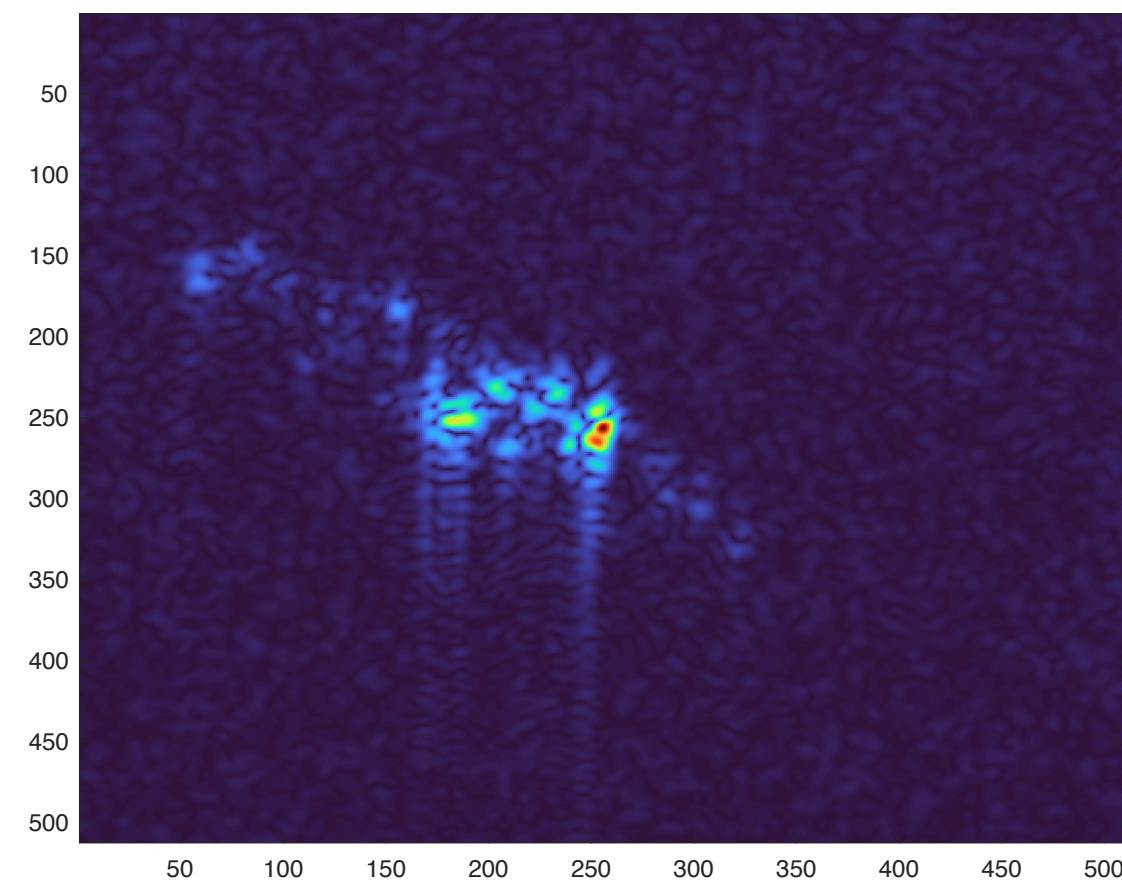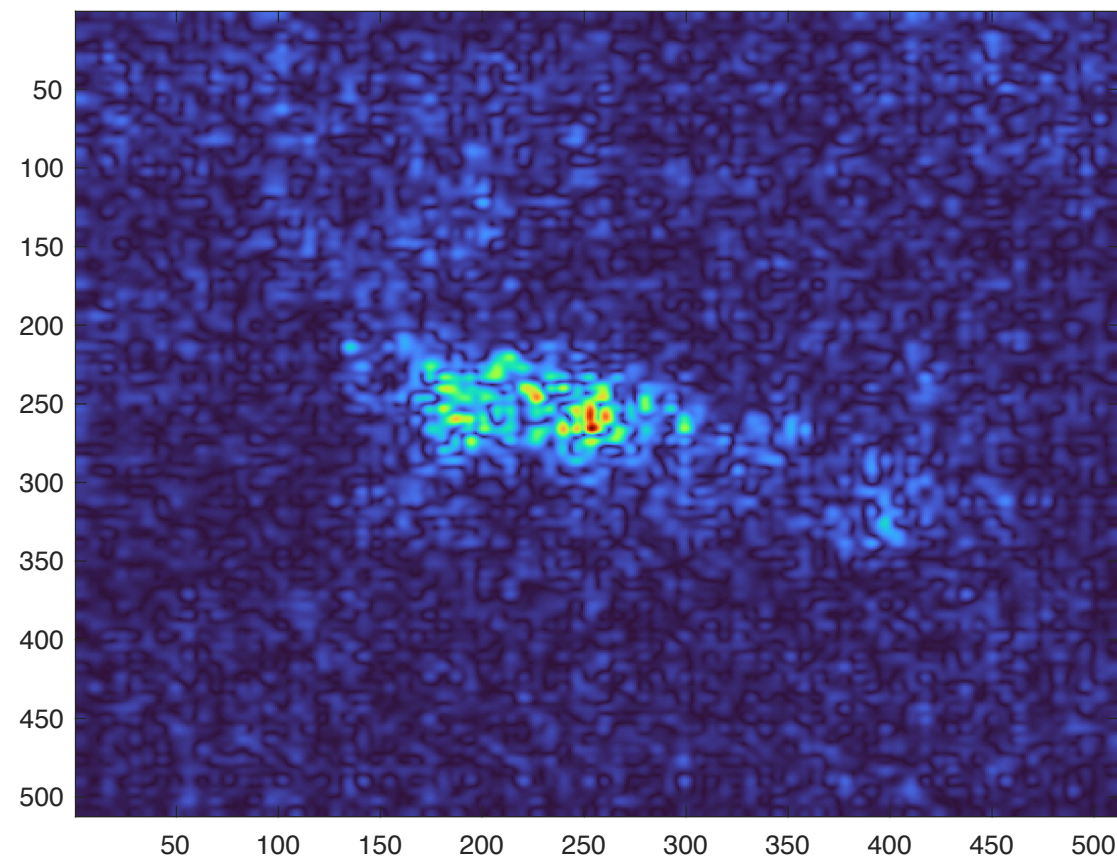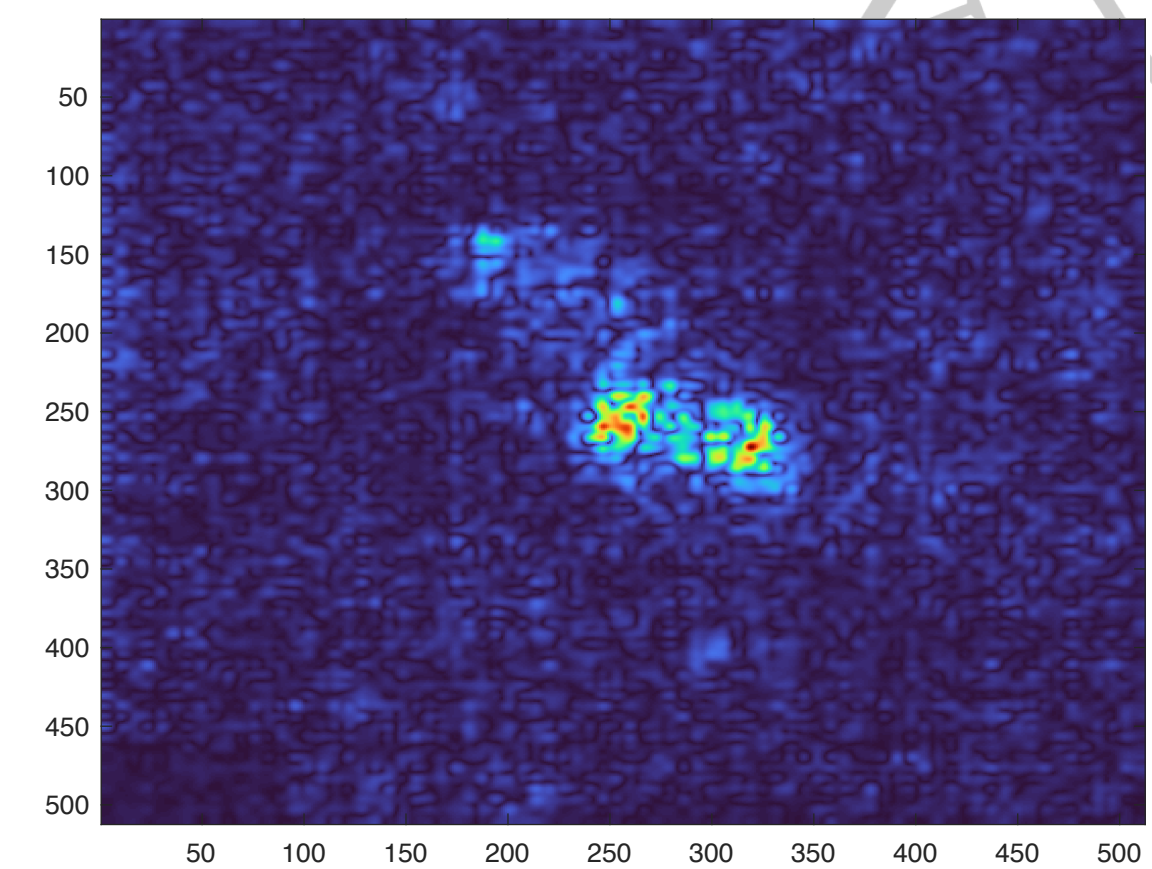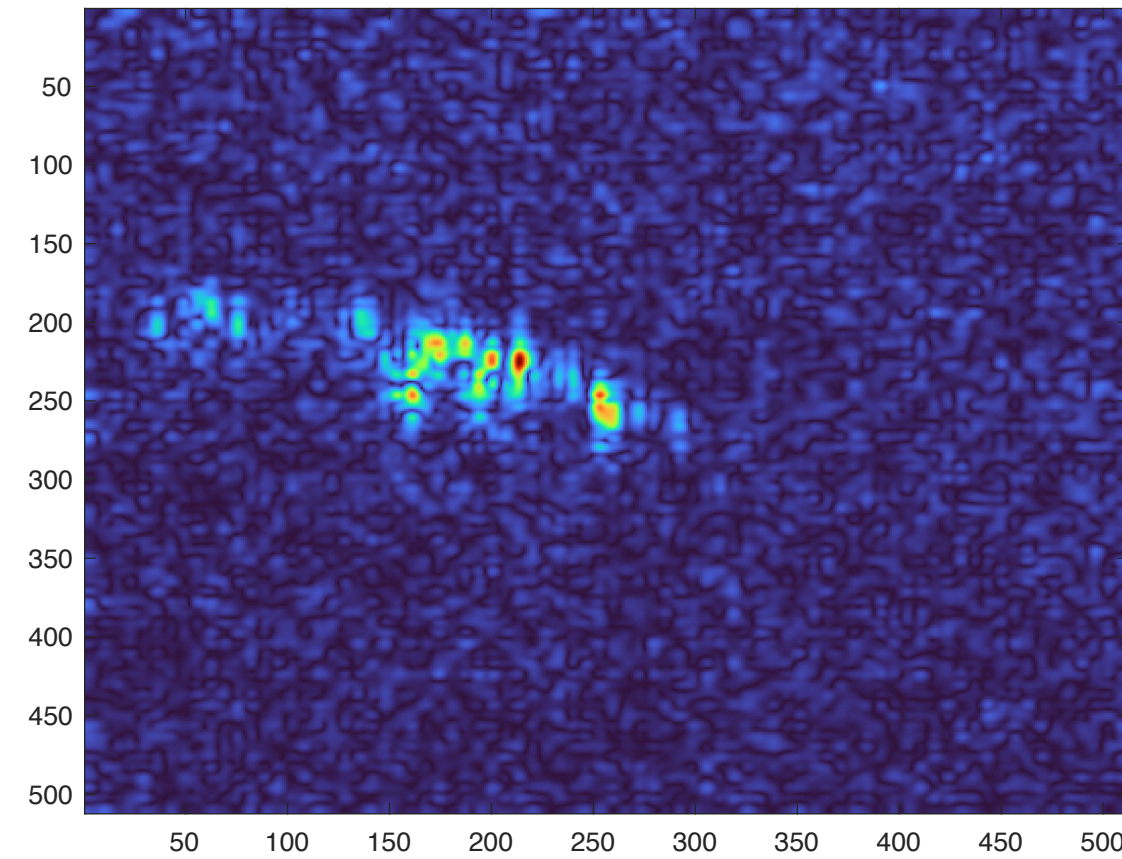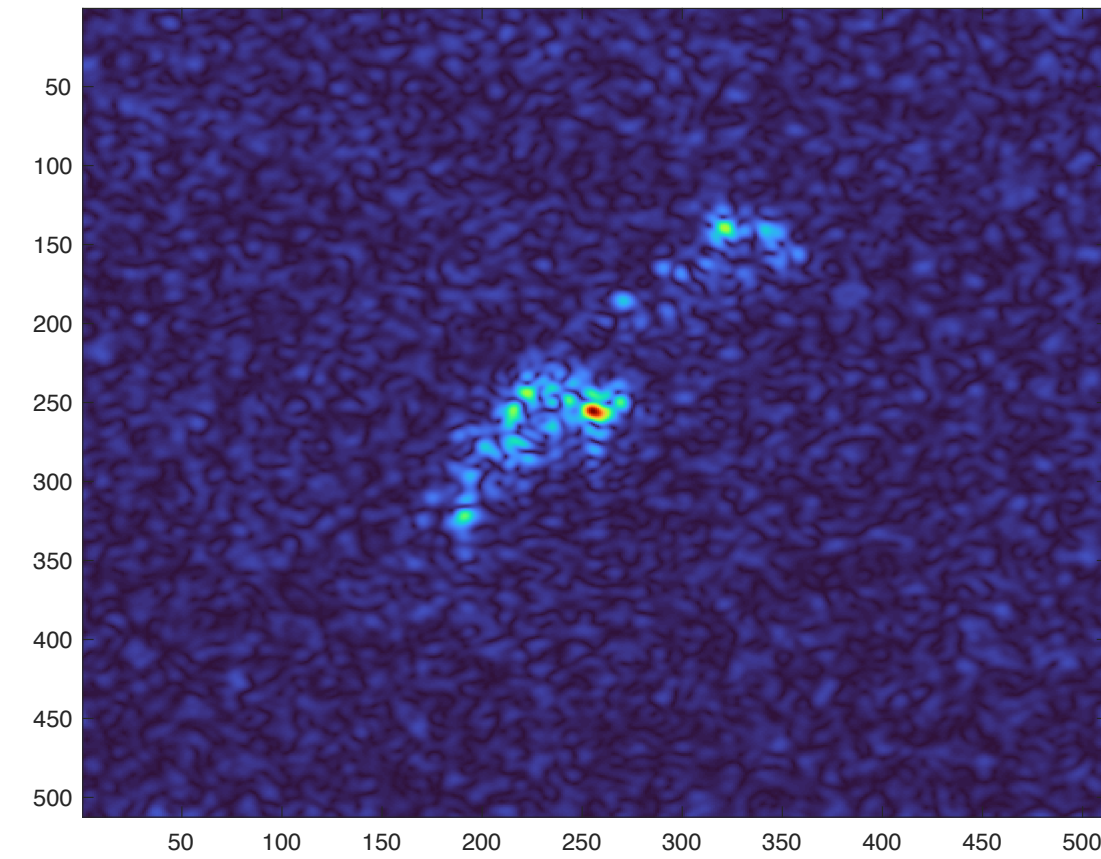
Experiment and results
Structure Similarity Index
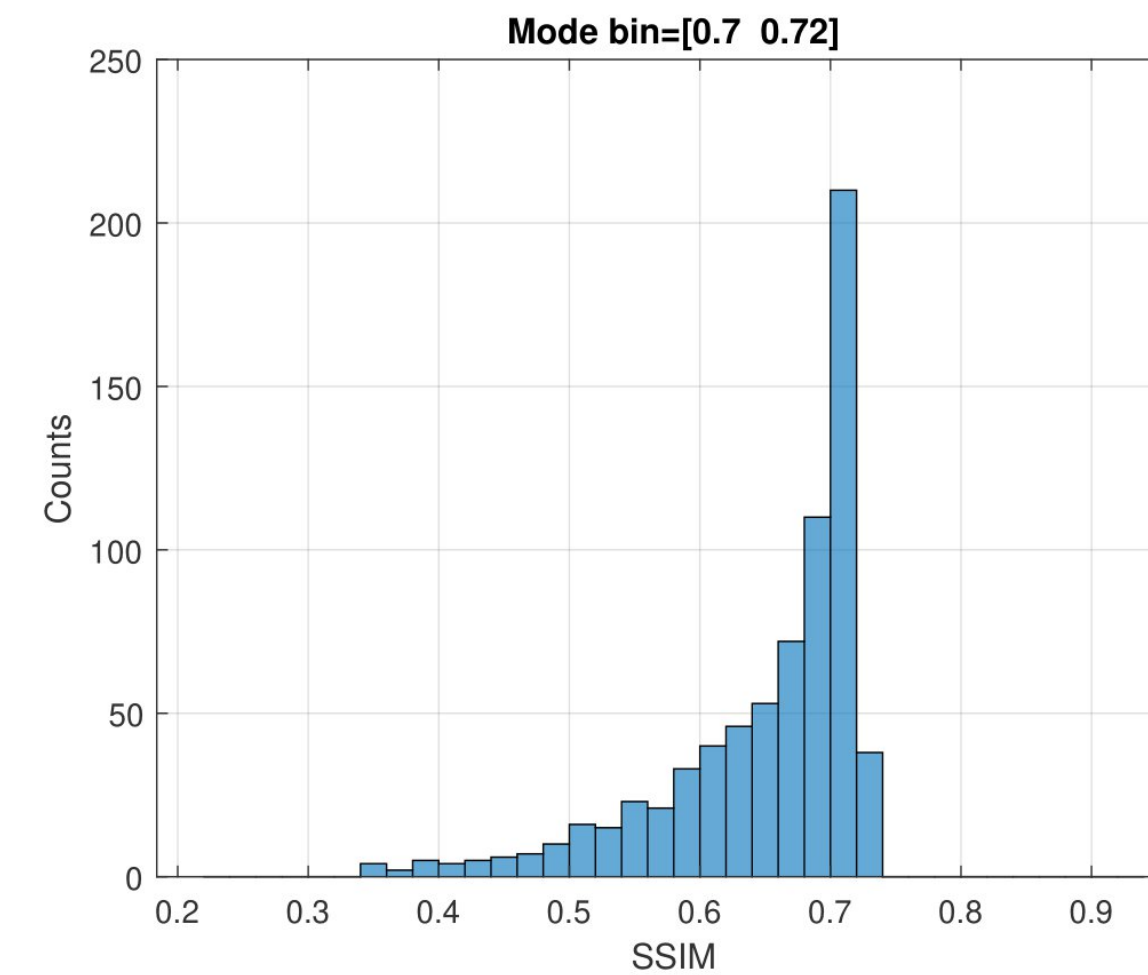
Conclusion
And future works

- We need more and diverse real data

- Meaningful phase information is important for radar systems

- Limitation due to the Image Projection Mechanism

- **Future goal:** develop techniques to recognise decoy images

Q&A
Thanks for your attention!

🏠 *http://labrass.cnit.it*

✉️ *francesco.mancuso@phd.unipi.it*