Adversarial Learning Applied to Radio Frequency Data

Erik Blasch
Support from Air Force Office of Scientific Research

Collaborators: Uttam Majumder, Peter Zulch (AFRL)

Efficient and Robust Machine Learning – COE
https://madlab.ml.wisc.edu/

Outline

• Motivation
  – Sensor Fusion
  – Methods for Automatic Target Recognition (ATR)
  – RF Data (ATR and Communications)

• SAR Deep Learning Evaluation
  – Machine learning to Deep Neural Networks
  – Generative Adversarial Network Learning
  – Adversarial Response

• RF Emitter Learning
  – Deep Learning (GAN)
  – Information Fusion (ESCAPE data)

• Summary
Discussion (Methods)

• **Data-Driven**
  – Data Match (Template-Based)
  – Data modified (e.g., Genetic algorithms)
  – Data-Generated (Statistical Learning)

• **Model-Based**
  – Model-Assisted (data parameterized model)
  – Physics-Based Instances (synthetic, e.g. computer aided design)
  – First-Principle Models (holistic, Dynamic Data Driven Applications Systems)

• **Adversarial (Learning)**
  – Data-generated (sensor, environmental changes)
  – Attack instances (data, model poisoning)
  – Course of Action (what if responses to rare events)

• **Adaptation (Learning)**
  – Reinforcement Learning
  – Transfer Learning
  – Intelligent (responsive GAN)
Radio Frequency Data

(From: https://www.flickr.com/photos/usgao/5727623528)
## Synthetic Aperture Radar

### Radar Bands

<table>
<thead>
<tr>
<th>Freq Band</th>
<th>Freq Range (GHz)</th>
<th>Wavelength (cm)</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>HF</td>
<td>0.003-0.03</td>
<td></td>
<td>High Frequency (speed of ocean current)</td>
</tr>
<tr>
<td>VHF</td>
<td>0.03-0.3</td>
<td></td>
<td>Very High Frequency (over the horizon radar)</td>
</tr>
<tr>
<td>UHF</td>
<td>0.3-1</td>
<td></td>
<td>Ultra High Frequency (meteorology)</td>
</tr>
<tr>
<td>P</td>
<td>0.3-1</td>
<td>60-120</td>
<td>Foliage Penetration, Soil Moisture</td>
</tr>
<tr>
<td>L</td>
<td>1-2</td>
<td>15-30</td>
<td>Soil Moisture, Agriculture</td>
</tr>
<tr>
<td>C</td>
<td>4-8</td>
<td>4.0 – 8.0</td>
<td>Agriculture, Ocean (Polarimetric SAR)</td>
</tr>
<tr>
<td>X</td>
<td>8-12</td>
<td>2.4-4.0</td>
<td>Ocean High-range Resolution Radar</td>
</tr>
<tr>
<td>Ku</td>
<td>14-18</td>
<td>1.7-2.5</td>
<td>Snow cover</td>
</tr>
<tr>
<td>Ka</td>
<td>27-47</td>
<td>0.75-1.2</td>
<td>High Frequency radar</td>
</tr>
<tr>
<td>W</td>
<td>56-100</td>
<td></td>
<td>Remote Sensing, Communications</td>
</tr>
</tbody>
</table>

**Polarimetric SAR**

https://earth.esa.int/web/polsarpro/polarimetry-tutorial

**Moving and Stationary Target Acquisition Recognition (MSTAR) data set - 9.6 GHz X-band SAR** with a 1 foot range resolution × 1 foot cross-range resolution over 1° spacing of 360° articulations

AML for Radio Frequency Data

• MSTAR Papers (SAR)


-------------------------------------------------------------------------------------------------------------------------


This exciting resource identifies technical challenges, benefits, and directions of Deep Learning (DL) based object classification using radar data (i.e., Synthetic Aperture Radar / SAR and High range resolution Radar / HRR data). An overview of machine learning (ML) theory to include a history, background primer, and example and performance of ML algorithm (i.e., DL method) on video imagery is provided. Radar data with issues of collection, application, and examples for SAR/HRR data and communication signals analysis is also discussed. Practical considerations of deploying such techniques, including performance evaluation, hardware issues, and unresolved challenges.
Outline

• Motivation
  – Sensor Fusion
  – Methods for Automatic Target Recognition (ATR)
  – RF Data (ATR and Communications)

• SAR Deep Learning Evaluation
  – Machine learning to Deep Neural Networks
  – Generative Adversarial Network Learning
  – Adversarial Response

• RF Emitter Learning
  – Deep Learning (GAN)
  – Information Fusion (ESCAPE data)

• Summary
MSTAR – Moving and Stationary Target Acquisition and Recognition

Electro-optic Images of Objects

SAR Images of Objects

HRR/SAR signals of Objects


https://github.com/jpualoa/mstar
Radar Automatic Target Recognition

**ATR Operating Conditions**

- **Standard Operating Conditions**
- **Extended Operating Conditions 1, EOC-2**

<table>
<thead>
<tr>
<th>Number of Classes</th>
<th>Acquisition Geometry</th>
<th>Target State Variations</th>
<th>Target Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Depression, Squint, Rotation Angles</td>
<td>Articulation, configuration, intra-class modifications</td>
<td>Obscuration, camouflage, deception</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EOC-1</td>
<td>EOC-2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SOC</td>
<td></td>
</tr>
</tbody>
</table>


Standard Operating Conditions

Standard Operating Conditions

• Original Data Set


<table>
<thead>
<tr>
<th>Depr.</th>
<th>BMP2</th>
<th>BTR70</th>
<th>T72</th>
<th>BTR60</th>
<th>2S1</th>
<th>BRDM2</th>
<th>D7</th>
<th>T62</th>
<th>ZIL</th>
<th>ZSU234</th>
</tr>
</thead>
<tbody>
<tr>
<td>17°</td>
<td>233(SN9563)</td>
<td>233</td>
<td>232</td>
<td>256</td>
<td>299</td>
<td>298</td>
<td>299</td>
<td>299</td>
<td>299</td>
<td>299</td>
</tr>
</tbody>
</table>

3 Targets

10 Targets


Extended Operating Conditions


Geometry

Version
# Performance (MSTAR) - ML

<table>
<thead>
<tr>
<th>Method</th>
<th>Performance (%)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conditional False Alarm Rate (CFAR) [35 tgts]</td>
<td>89.0, 91, 85</td>
<td>Mossing, et al., 1998 [15]</td>
</tr>
<tr>
<td>Support Vector Machine (SVM) [3 tgts]</td>
<td>90.0, 81, 75</td>
<td>Zhao, et al., 2001 [16]</td>
</tr>
<tr>
<td>Conditional Gaussian [3 tgts]</td>
<td>92.0, 80, 79</td>
<td>O'Sullivan, et al., 2001 [17]</td>
</tr>
<tr>
<td>AdaBoost [3 tgts]</td>
<td>92.0, 82, 78</td>
<td>Sun, et al., 2007 [18]</td>
</tr>
<tr>
<td>Bayesian compressive sensing (BCS) [10 tgts]</td>
<td>92.0, - , -</td>
<td>Zhang, et al., 2013 [19]</td>
</tr>
<tr>
<td>Sparse Representation of Monogenic Signal</td>
<td>93.6, 88.4, -</td>
<td>Dong, et al. 2014 [20]</td>
</tr>
<tr>
<td>Iterative graph thickening (IGT)</td>
<td>95.0, 85, 80</td>
<td>Srinivas, et al., 2014 [21]</td>
</tr>
<tr>
<td>Modified Polar Mapping Classifier (M-PMC)</td>
<td>98.8, - , 97.3</td>
<td>Park, et al., 2014 [22]</td>
</tr>
<tr>
<td>Monogenic scale space (MSS)</td>
<td>96.6, 98.2, -</td>
<td>Dong, et al., 2015 [23]</td>
</tr>
</tbody>
</table>
# ATR Challenge Problems

<table>
<thead>
<tr>
<th>Challenge Problem</th>
<th>Challenge</th>
<th>Year</th>
<th>Ref</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recognition/detection/tracking/reconstruction</td>
<td>R D T R</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Standard SAR ATR evaluation experiments using the MSTAR public release dataset</strong></td>
<td>X X X</td>
<td>1998</td>
<td>[38]</td>
</tr>
<tr>
<td><strong>Data Dome: Full k-spacesampling for high frequency radar research</strong></td>
<td>X</td>
<td>2004</td>
<td>[39]</td>
</tr>
<tr>
<td><strong>A Challenge Problem for Detection of Target in Foliage</strong></td>
<td>X</td>
<td>2006</td>
<td>[40]</td>
</tr>
<tr>
<td><strong>Challenge Problem for 2D/3D Imaging of Targets from Volumetric Data Set in an Urban Environment</strong></td>
<td>X</td>
<td>2007</td>
<td>[41]</td>
</tr>
<tr>
<td><strong>A Challenge Problem for SAR-based GMTI in Urban Environments</strong></td>
<td>X X X</td>
<td>2009</td>
<td>[42]</td>
</tr>
<tr>
<td><strong>Civilian Vehicle Radar Data Domes</strong></td>
<td>X X</td>
<td>2010</td>
<td>[43]</td>
</tr>
<tr>
<td><strong>A Challenge Problem for SAR Change Detection and Data Compression</strong></td>
<td>X</td>
<td>2010</td>
<td>[44]</td>
</tr>
<tr>
<td><strong>Wide Angle SAR Data for Target Discrimination Research</strong></td>
<td>X</td>
<td>2012</td>
<td>[45]</td>
</tr>
</tbody>
</table>

MSTAR Publications

• Literature Review
Deep Learning

Deep Learning Algorithms

Generative Models
- Deep Belief Networks (DBN)
- Deep Boltzmann Machine
- Autoencoder

Hybrid Models
- Multi-Layer Perceptron
- Pulse-coupled NN (PCNN)
- Deep Neural Network (DNN)

Discriminative Models
- Deep stacking Nets (DSN)
- Convolutional NN (CNN)
- Recurrent NN (RNN)
Deep Learning Generative Methods

Maximum Likelihood

Explicit Density

Tractable Density

Belief Networks

CNN

Approximate Density

Variational

Autoencoder

Markov Chain

Boltzmann Machine

Implicit Density

Approximate Density

Markov Chain

Generative Stochastic Network

Direct

Generative Adversarial Network
Autoencoder
Generative Adversarial Networks

- **Trainig data** $(z)$
- **MSTAR Training Set**
- **G (Generator)**
- **D (Discriminator)**
- **Latent Space**
- **Noise Vector**
- **Noise** $(n)$
- **Generated Fake Samples**
- **Pre-trained**
- **Fine Tune Training**
- **Log(x)**
- **Predicted labels**
- **Is D Correct?**
- **Real or Fake**

Mathematical Formulas:

- \[ \min_{\theta_g} \sum_{i=1}^{m} \log \left( 1 - D \left( G \left( n^{(i)} \right) \right) \right) \]
- \[ \max_{\theta_d} \sum_{i=1}^{m} \log D \left( z^{(i)} \right) + \log \left( 1 - D \left( G \left( n^{(i)} \right) \right) \right) \]
## Performance (MSTAR) - DL

<table>
<thead>
<tr>
<th>Method</th>
<th>Performance (%)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SOC</td>
<td>EOC-1</td>
</tr>
<tr>
<td>A-ConvNets</td>
<td>99.1</td>
<td>96.1</td>
</tr>
<tr>
<td><strong>AFRLenNet</strong></td>
<td><strong>99.4</strong></td>
<td></td>
</tr>
<tr>
<td>CNN-SVM</td>
<td>99.5</td>
<td>95.75</td>
</tr>
<tr>
<td>VGG-S1</td>
<td>98.8</td>
<td>94.15</td>
</tr>
<tr>
<td>VGG-S, Feature Fusion, KNN</td>
<td>99.82</td>
<td>96.16</td>
</tr>
<tr>
<td>Joint Supervised Dictionary</td>
<td>97.65</td>
<td>98.39</td>
</tr>
<tr>
<td>GAN-CNN</td>
<td>97.53</td>
<td></td>
</tr>
<tr>
<td>MGAN-CNN</td>
<td>97.81</td>
<td></td>
</tr>
<tr>
<td>Triple GAN and Integrated GAN</td>
<td>99.9</td>
<td></td>
</tr>
</tbody>
</table>
MSTAR GAN - Adversarial Learning

Benefit 1 – higher accuracy

Achieve semi-supervised generation and recognition simultaneously. Supports scenarios when labeled samples are insufficient,

![Diagram of MSTAR GAN - Adversarial Learning](image)

Triple GAN and Integrated GAN \( \sim 99.9\% \) (with 600 labels)


* Difficult to detect imposter data
## MSTAR GAN - Adversarial Learning

Benefit 2 – results with fewer training samples

<table>
<thead>
<tr>
<th>Method</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>20 Samples</td>
</tr>
<tr>
<td>PCA-SVM</td>
<td>76.43</td>
</tr>
<tr>
<td>SRC</td>
<td>79.61</td>
</tr>
<tr>
<td>DNN</td>
<td>79.39</td>
</tr>
<tr>
<td>CNN</td>
<td>81.80</td>
</tr>
<tr>
<td>GAN-CNN</td>
<td>84.39</td>
</tr>
<tr>
<td>MGAN-CNN</td>
<td><strong>85.23</strong></td>
</tr>
</tbody>
</table>

**MSTAR GAN - Adversarial Learning**

**Benefit 3 – Synthetic Image Generation for Robustness**


<table>
<thead>
<tr>
<th>Experiment</th>
<th>Synth</th>
<th>Altered</th>
<th>Synth</th>
<th>Altered</th>
<th>Synth</th>
<th>Altered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: DualGAN, Baseline, Full</td>
<td><img src="image1" alt="Synth Image" /></td>
<td><img src="image2" alt="Altered Image" /></td>
<td><img src="image3" alt="Synth Image" /></td>
<td><img src="image4" alt="Altered Image" /></td>
<td><img src="image5" alt="Synth Image" /></td>
<td><img src="image6" alt="Altered Image" /></td>
</tr>
<tr>
<td>2: DualGAN, Baseline, Unmatched</td>
<td><img src="image7" alt="Synth Image" /></td>
<td><img src="image8" alt="Altered Image" /></td>
<td><img src="image9" alt="Synth Image" /></td>
<td><img src="image10" alt="Altered Image" /></td>
<td><img src="image11" alt="Synth Image" /></td>
<td><img src="image12" alt="Altered Image" /></td>
</tr>
<tr>
<td>3: DualGAN, N-NWL, Full</td>
<td><img src="image13" alt="Synth Image" /></td>
<td><img src="image14" alt="Altered Image" /></td>
<td><img src="image15" alt="Synth Image" /></td>
<td><img src="image16" alt="Altered Image" /></td>
<td><img src="image17" alt="Synth Image" /></td>
<td><img src="image18" alt="Altered Image" /></td>
</tr>
<tr>
<td>4: DualGAN, N-NWL, Unmatched</td>
<td><img src="image19" alt="Synth Image" /></td>
<td><img src="image20" alt="Altered Image" /></td>
<td><img src="image21" alt="Synth Image" /></td>
<td><img src="image22" alt="Altered Image" /></td>
<td><img src="image23" alt="Synth Image" /></td>
<td><img src="image24" alt="Altered Image" /></td>
</tr>
<tr>
<td>5: DualGAN, NWL, Full</td>
<td><img src="image25" alt="Synth Image" /></td>
<td><img src="image26" alt="Altered Image" /></td>
<td><img src="image27" alt="Synth Image" /></td>
<td><img src="image28" alt="Altered Image" /></td>
<td><img src="image29" alt="Synth Image" /></td>
<td><img src="image30" alt="Altered Image" /></td>
</tr>
<tr>
<td>6: DualGAN, NWL, Unmatched</td>
<td><img src="image31" alt="Synth Image" /></td>
<td><img src="image32" alt="Altered Image" /></td>
<td><img src="image33" alt="Synth Image" /></td>
<td><img src="image34" alt="Altered Image" /></td>
<td><img src="image35" alt="Synth Image" /></td>
<td><img src="image36" alt="Altered Image" /></td>
</tr>
</tbody>
</table>
MSTAR Adversarial Corruption

Robust 1 – Adversarial Corruption

• Corruption

MSTAR Adversarial Perturbation
Robust 2 – Model & Data Developed

SAR Image Formation

DNN models for the different SAR image formation methods *phase history* (PH), *range-Doppler* (RD), *polar format* (PF) and back-projection (BP, baseline) algorithm

MSTAR Adversarial Perturbation
Robust 3 – Adversarial attack mitigation

• Types of Attacks, Corruption

Simple models, such as aconv and convb, suffer the most when significant attacks happen whereas ResNet18 stays competitive.

CV Data Dome Adversarial Perturbation

Robust 4 – Adversarial Scenario Prediction

DNN models for the different SAR image formation methods *phase history* (PH), *range-Doppler* (RD), *polar format* (PF) and *back-projection* (BP, baseline) algorithm.

Outline

• Motivation
  – Sensor Fusion
  – Methods for Automatic Target Recognition (ATR)
  – RF Data (ATR and Communications)

• SAR Deep Learning Evaluation
  – Machine learning to Deep Neural Networks
  – Generative Adversarial Network Learning
  – Adversarial Response

• RF Emitter Learning
  – Deep Learning (GAN)
  – Information Fusion (ESCAPE data)

• Summary
Radio Frequency Adversarial Learning


• RF Transmitter Detection with GAN

• Objectives:
  • GAN to distinguish adversarial transmitters from trusted ones.
  • CNN with 2D convolutions to exploit the correlation in collected signal data of the trusted transmitters for trusted transmitter identification.
  • DNN to classify the trusted transmitters.
  • RNN with both LSTM and GRU cells to improve the accuracy of trusted transmitter classification by exploiting the temporal aspect of the signal data.

**Quadrature Phase Shift Keying**
- Bit modulation to tx more information
- Each device has unique signature based on electronics conducting the A/D operations

**Signals Classification and motivation to support “adversarial” environments**
Radio Frequency Adversarial Learning


- RF Transmitter Detection with GAN
  - Detection model - GAN
  - Classification Model Types
    - DNN, CNN
    - LSTM (RNN, GRU)

8 universal software radio peripheral (USRP) - 5 experiments

Real world testing on RF devices
ESCAPE Data Collection


Objective: Collection campaign to collect multi-source data on ground and SUAS targets. Supports multi-int fusion research. First of its kind collection

Sensors: Combined EO/IR/SIGINT on SUAS, tower SIGINT, tower radar, tower cameras, ground seismic & acoustic

Scenarios:
- Ground – Disparate moving emitting vehicles, various patterns, differing noise profiles
- Airborne – SUAS (2) targets, various flight profiles, ground idle to hovering to flight, multiples

Collection Statistics
- # Scenarios: 8 ground, 4 airborne
- # Ground runs: 47 of 63 planned
- # SUAS runs: 37 of 144 planned
- 84 of 207 planned runs (rain delays, equip. delays)
- 3 of 5 planned days for collection
- 13+ TB of data
  - EO cameras are the bulk of this

Other Test Specifics
- Lead Test Org.: AFRL/RIGC (P. Zulch)
- Support Contractors:
  - Michigan Tech. Research Institute (MTRI)
  - AIS
  - North Point Defense
- Multi-Int Payload: EO/IR/Passive RF
- 2 flown on SUAS (DJI M600)
- 1 Tower Mounted
## Sensor Baseline


- Multi-source data correlated on single targets

### Sensor Baseline Table

<table>
<thead>
<tr>
<th>Modality</th>
<th>Sensor Model</th>
<th>Ownership</th>
<th>Resolution (H X V)</th>
<th>Weight</th>
<th>Deployment (Height (m))</th>
<th>Near Ground Range (m)</th>
<th>Far Ground Range (m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EO</td>
<td>Basler Ace acA3800 FMV</td>
<td>MTRI (Deliverable)</td>
<td>(3840 X 2748)</td>
<td>133 g</td>
<td>SUAS (50)</td>
<td>0</td>
<td>250</td>
</tr>
<tr>
<td>IR</td>
<td>Flir Vu Pro R 640 FMV</td>
<td>MTRI (Deliverable)</td>
<td>(640 X 512)</td>
<td>114 g</td>
<td>SUAS (50)</td>
<td>5</td>
<td>140</td>
</tr>
<tr>
<td>Passive-RF</td>
<td>USRP B200</td>
<td>MTRI (Deliverable)</td>
<td>12 MHz BW 1245 MHz</td>
<td>350 g</td>
<td>SUAS (50)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Seismic</td>
<td>Raspberry Pi Shake</td>
<td>AFRL/RIGC</td>
<td>-</td>
<td>65 g</td>
<td>Ground (0)</td>
<td>0</td>
<td>250</td>
</tr>
<tr>
<td>Acoustic</td>
<td>Brue &amp; Kjaer 4952</td>
<td>AFRL/RIGC</td>
<td>-</td>
<td>114 g</td>
<td>Ground (0)</td>
<td>0</td>
<td>250</td>
</tr>
<tr>
<td>RADAR (UHF)</td>
<td>Akela Tapered Horns</td>
<td>MTRI</td>
<td>-</td>
<td>8 kg</td>
<td>Tower (33.54)</td>
<td>5</td>
<td>400</td>
</tr>
<tr>
<td>EO</td>
<td>Allied Vision Prosilica GX3300C</td>
<td>AFRL/RIGC</td>
<td>(3296 X 2472)</td>
<td>365 g</td>
<td>Tower (27.44)</td>
<td>30</td>
<td>250</td>
</tr>
<tr>
<td>Passive RF</td>
<td>Ettus N210 SDR</td>
<td>MTRI</td>
<td>-</td>
<td>1.2 kg</td>
<td>Tower (27.44)</td>
<td>0</td>
<td>Source Dependent</td>
</tr>
</tbody>
</table>

* Multimodal EO/RF DL & GAN submitted for review
Machine learning (ML) approach for target recognition requires huge amount of training data for better classification accuracy. However, obtaining measured data (particularly radio frequency) is difficult and expensive. Measured data for non-cooperative target are not readily available. Hence, generation of synthetic radar data using electromagnetic prediction code will play a vital role. Our first research task will be investigating transfer learning (TL) and generative adversarial networks (GAN) techniques. Our primary goal will be augmenting measured data by using high fidelity radio frequency data generated by XPatch or other electromagnetic prediction code that will resemble targets and operating environments. Our second research task will be development of an integrated processing and exploitation technique for multi-int data. As radar/EO/IR sensor data are collected, detection and identification of important objects are important. This process will allow us prioritization of mission essential surveilled data for real-time forensic analysis. After initial scan/processing of the data, ML will allow separating mission critical object data for further analysis/decision making. We will investigate machine learning based multi-int fusion technique.
Summary

• Motivation
  – Sensor Fusion, RF Data (ATR and Communications)

• SAR Deep Learning Evaluation
  – Machine Learning to Deep Learning
  – Need to combine data generation (signatures) with recognition (DL)

• RF Emitter Learning
  – Signature Generation
  – Work with communications operating conditions

• Information Fusion
  – Information Fusion (ESCAPE data)
  – Other non-traditional data sets