Adversarial Learning Applied to Radio Frequency Data

Erik Blasch

Support from Air Force Office of Scientific Research

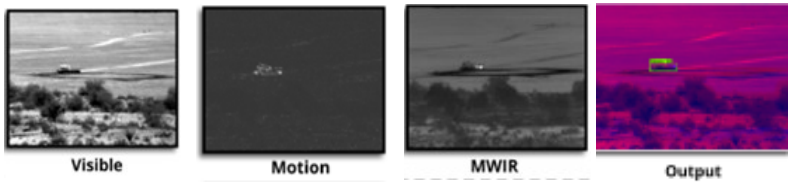
Collaborators: Uttam Majumder, Peter Zulch (AFRL)

Efficient and Robust Machine Learning – COE

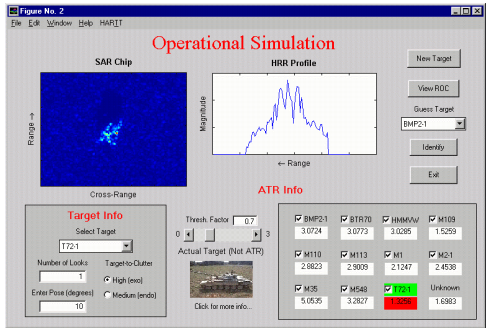
https://madlab.ml.wisc.edu/

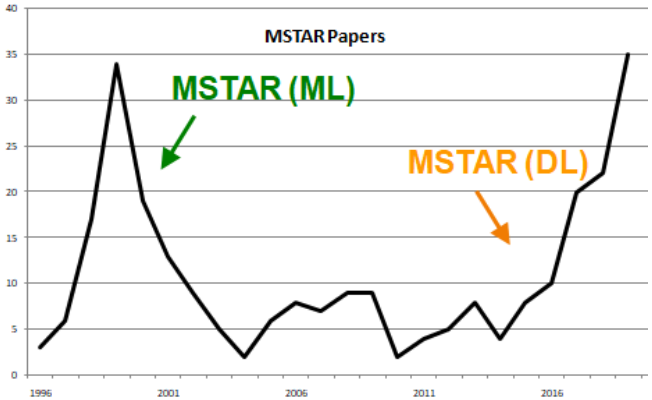
Dist A: 88ABW-2020-1776, 88ABW-2020-1777, 88ABW-2020-1778, 88ABW-2018-5339

Outline



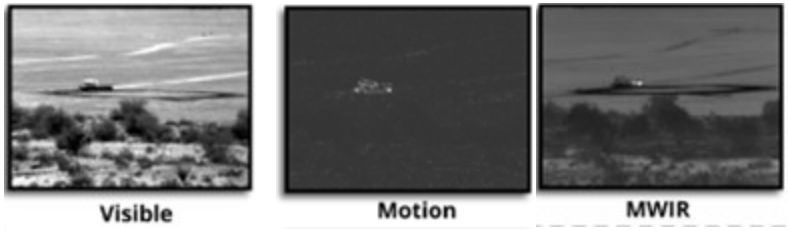
- **Motivation**
  - Sensor Fusion
  - Methods for Automatic Target Recognition (ATR)
  - RF Data (ATR and Communications)
- **SAR Deep Learning Evaluation**
  - Machine learning to Deep Neural Networks
  - Generative Adversarial Network Learning
  - Adversarial Response
- **RF Emitter Learning**
  - Deep Learning (GAN)
  - Information Fusion (ESCAPE data)
- **Summary**



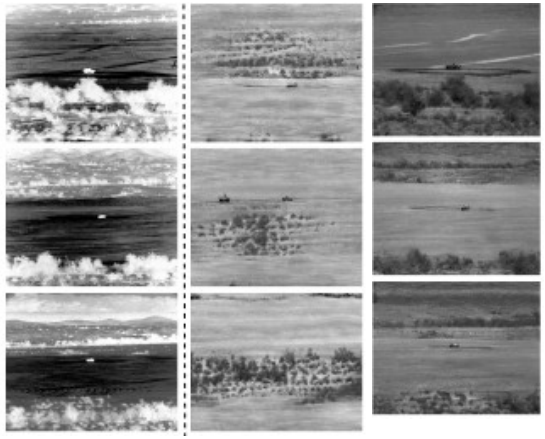


Discussion (Methods)

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

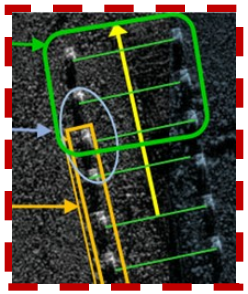


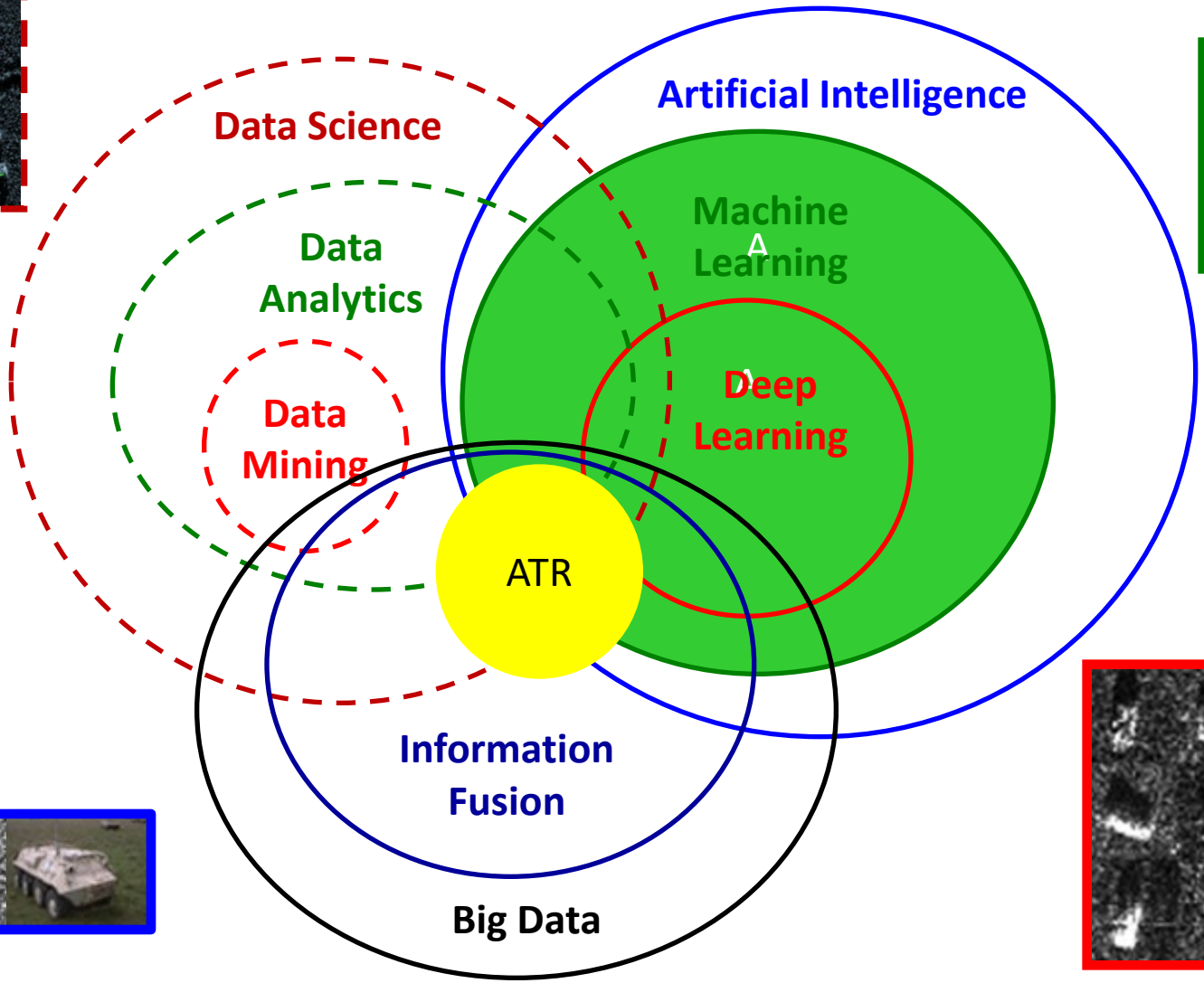
- **Model-Based**
  - Model-Assisted (data parameterized model)
  - Physics-Based Instances (synthetic, e.g. computer aided design)
  - First-Principle Models (holistic, Dynamic Data Driven Applications Systems)
- **Adversarial (Learning)**
  - Data-generated (sensor, environmental changes)
  - Attack instances (data, model poisoning)
  - Course of Action (what if responses to rare events)

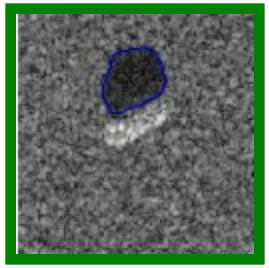


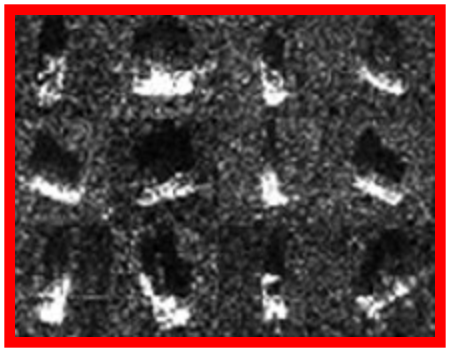
- **Adaptation (Learning)**
  - Reinforcement Learning
  - Transfer Learning
  - Intelligent (responsive GAN)

ATR Advances

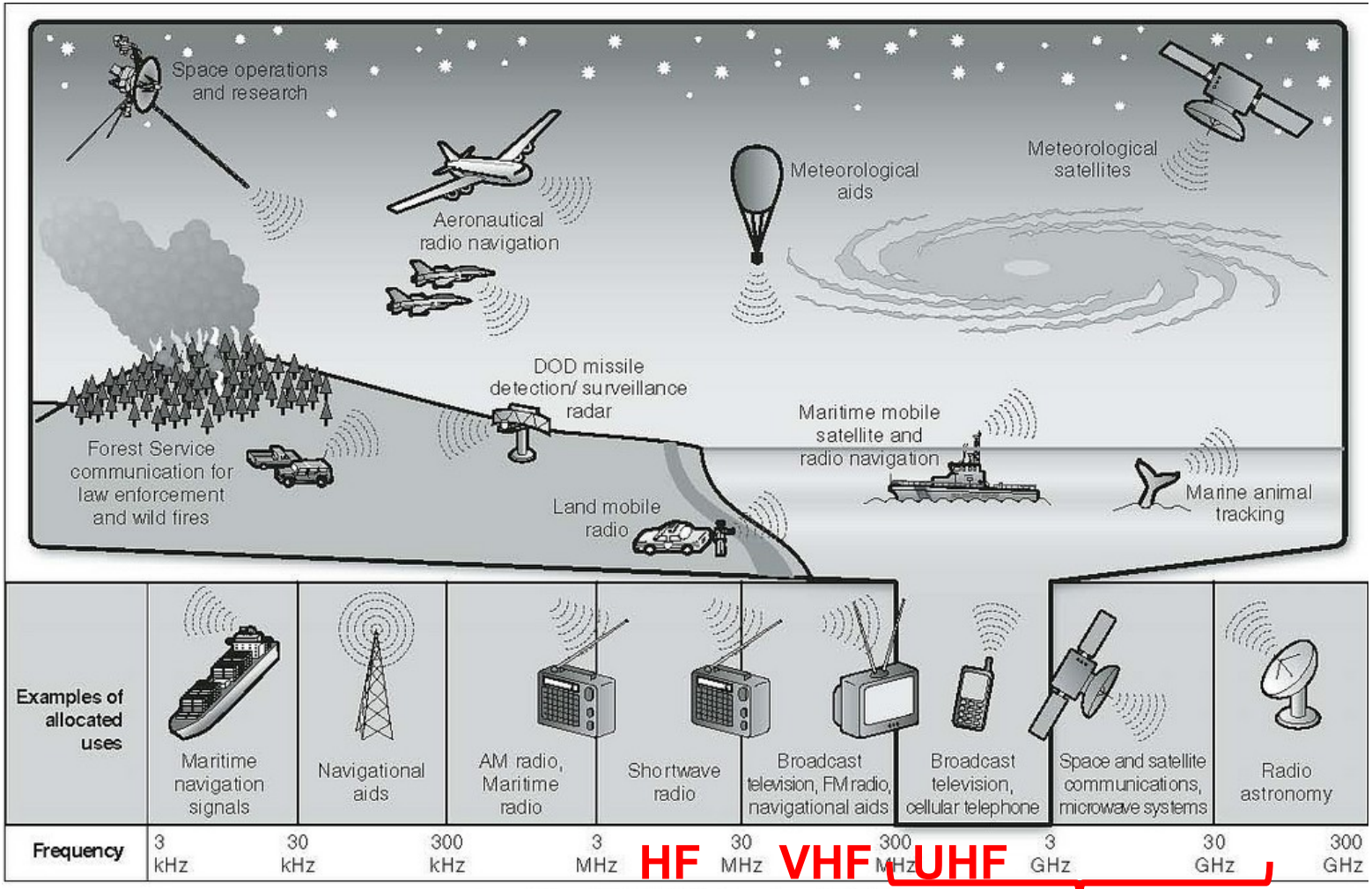








Radio Frequency Data



Source: GAO analysis of NTIA, federal agencies, and industry information.

(From : https://www.flickr.com/photos/usgao/5727623528)

Synthetic Aperture Radar

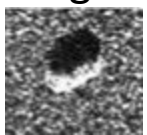
- **Radar Bands**

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

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



https://www.sdms.afrl.af.mil/index.php?collection=mstar

AML for Radio Frequency Data

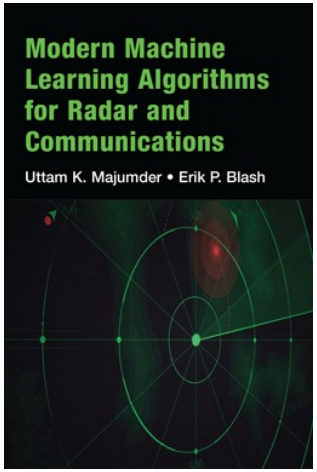
• MSTAR Papers (SAR)

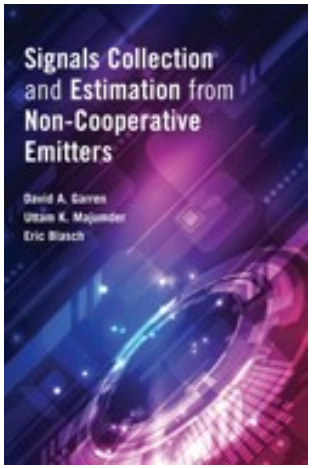
- **Lewis, B. (AFRL), Liu, J., Wong, A., "Generative adversarial networks for SAR image realism," *Proc. SPIE. 10647*, (2018).**
- Liu, W., Zhao, Y., Liu, M., *et al*., "Generating simulated SAR images using Generative Adversarial Network," *Proc. SPIE 10752*, (2018).
- Song, Q.., Xu, F., Jin, Y-Q., "SAR Image Representation Learning With Adversarial Autoencoder Networks," IEEE International Geoscience and Remote Sensing Symposium, IGARSS 2019.
- Zheng, C., Jiang, X., Liu, X., "Multi-Discriminator Generative Adversarial Network for Semi-Supervised SAR Target Recognition, *Conference (RadarConf),* (2019).
- Zheng, C., Jiang, X., Liu,, X., "Semi-Supervised SAR ATR via Multi-Discriminator Generative Adversarial Network," *IEEE Sensors Journal*, Volume: 19, Issue: 17, (2019).
- **Gao, F., Liu, Q., Sun, J., *et al*., "Integrated GANs: Semi-Supervised SAR Target Recognition," *IEEE Access 7*: 113999 – 114013, (2019).**

- **Roy, D., Mukherjee, T., Chatterjee, M., *et al*., "RFAL: Adversarial Learning for RF Transmitter Identification and Classification," *IEEE Tr. on Cognitive Comm. and Networking*, (2019).**
- **Majumder, U., Blasch, E., Garren, D., [*Deep Learning for Radar and Communications Automatic Target Recognition*], Artech House, (2020).**

Deep Learning For Radio Frequency ATR

- 1 – Introduction
- 2 – Mathematics review
- 3 – Machine Learning for ATR
- 4 – Deep Learning for ATR
- 5 – RF Data
- 6 – Single Target Recognition
- 7 – Multiple target Recognition
- 8 – Signals analysis
- 9 – Performance Evaluation
- 10 – Recent trends

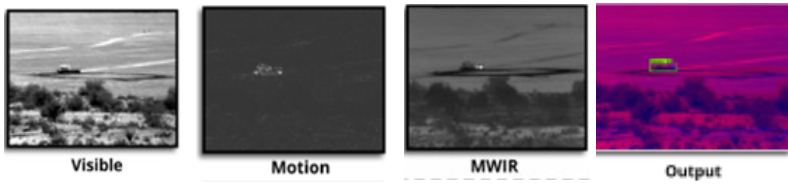




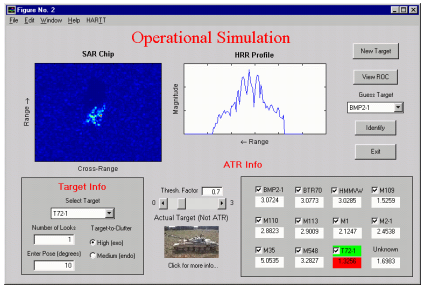
This exciting resource identifies technical challenges, benefits, and directions of Deep Learning (DL) based object classification using radar data (i.e., Synthetic Aperture Radar / SAR and High range resolution Radar / HRR data). An overview of machine learning (ML) theory to include a history, background 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

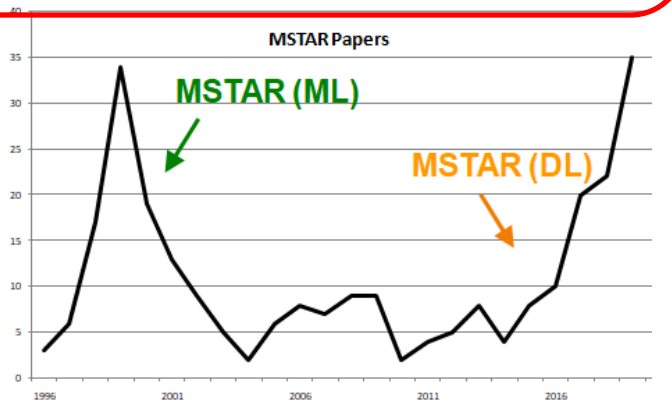
- **Motivation**
  - Sensor Fusion
  - Methods for Automatic Target Recognition (ATR)
  - RF Data (ATR and Communications)



- **SAR Deep Learning Evaluation**
  - Machine learning to Deep Neural Networks
  - Generative Adversarial Network Learning
  - Adversarial Response



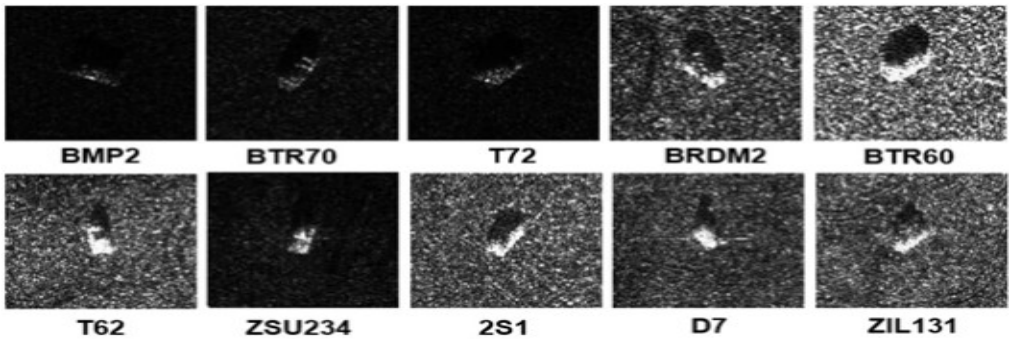
- **RF Emitter Learning**
  - Deep Learning (GAN)
  - Information Fusion (ESCAPE data)



- **Summary**

MSTAR – Moving and Stationary Target Acquisition and Recognition

Electro-optic Images of Objects



SAR Images of Objects

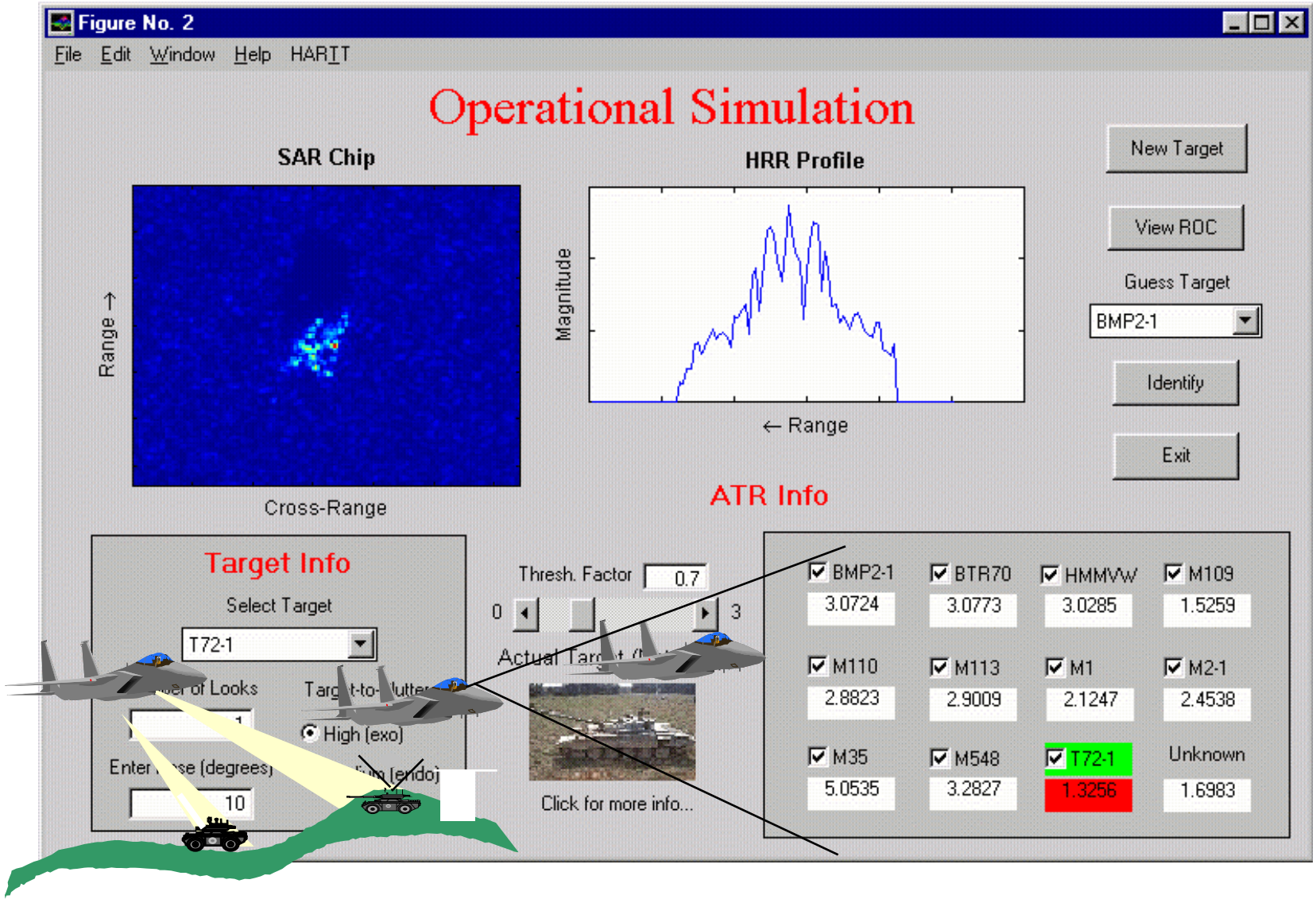
HRR/SAR signals of Objects

DARPA Data Collections, 1995/1996 (https://www.sdms.afrl.af.mil/index.php?collection=mstar)
E. Blasch, "*Derivation of a Belief Filter for Simultaneous High Range Resolution Radar Tracking and Identification,*" Ph.D. Thesis, Wright State University, 1999.

https://github.com/jpualoa/mstar

Radar Automatic Target Recognition

E. P. Blasch "Assembling a distributed fused Information-based Human-Computer Cognitive Decision Making Tool," *IEEE Aerospace and Electronic Systems Magazine,* Vol. 15, No. 5, pp. 11-17, May 2000.



ATR Operating Conditions

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

Number of Classes		
Acquisition Geometry	Depression, Squint, Rotation Angles	SOC
Target State Variations	Articulation, configuration, intra-class modifications	EOC-1
Target Deployment	Obscuration, camouflage, deception	EOC-2

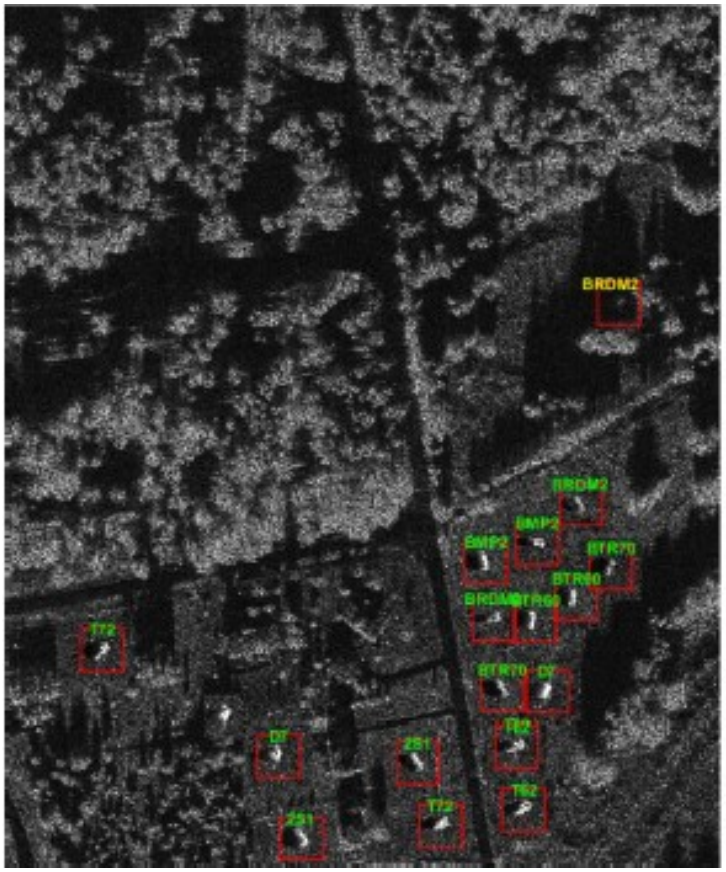
Eric R. Keydel, Shung Wu Lee, John T. Moore, "**MSTAR extended operating conditions**: a tutorial," Proc. SPIE 2757, Algorithms for Synthetic Aperture Radar Imagery III, 1996.

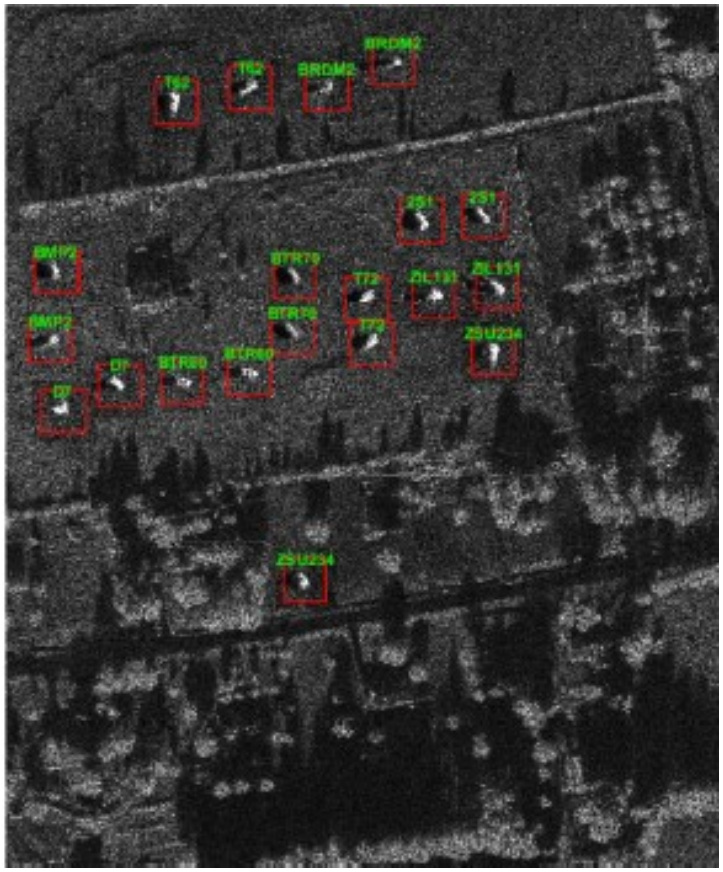
John C. Mossing, Timothy D. Ross, "Evaluation of SAR ATR algorithm performance sensitivity to MSTAR extended operating conditions," Proc. SPIE 3370, Algorithms for Synthetic Aperture Radar Imagery V, 1998.

E. P. Blasch and M. Bryant "Information Assessment of SAR Data For ATR," *Proceedings of IEEE National Aerospace and Electronics Conference*. Dayton, OH, pp. 414 – 419, 1998

Standard Operating Conditions

- S. Chen, et al., “Target Classification Using the Deep Convolutional Networks for SAR Images,” IEEE Tr. ON Geo. & Remote Sensing, 54(8):4806-4817, Aug. 2016





Standard Operating Conditions

- **Original Data Set**

E. P. Blasch and M. Bryant "Information Assessment of SAR Data For ATR," *Proceedings of IEEE National Aerospace and Electronics Conference*. Dayton, OH, pp. 414 – 419, July 1998

Michael Lee Bryant, Frederick D. Garber, "SVM classifier applied to the MSTAR public data set," Proc. SPIE 3721, 1999.

3 Targets **10 Targets**

Depr.	BMP2	BTR70	T72	BTR60	2S1	BRDM2	D7	T62	ZIL	ZSU234
17°	233(SN9563)	233	232	256	299	298	299	299	299	299
15°	195(SN9563) 196(SN9566) 196(SNC21)	196	231(SN812) 195(SN812) 191(SNS7)	195	274	274	274	273	274	274

- S. Chen, et al., "Target Classification Using the Deep Convolutional Networks for SAR Images," IEEE Tr. ON Geo. & Remote Sensing, 54(8):4806-4817, Aug. 2016
- H Ren, et al. "Joint Supervised Dictionary and Classifier Learning for Multi-View SAR Image Classification," *IEEE Access 7*: 165127 – 165142, 2019.

Extended Operating Conditions

S. Chen, et al., "Target Classification Using the Deep Convolutional Networks for SAR Images," IEEE Tr. ON Geo. &. Remote Sensing, 54(8):4806-4817, Aug. 2016

TEST EXAMPLES FOR EOC-1 (LARGE DEPRESSION VARIATION)

Class	Serial No.	Depression	No. Images
2S1	b01	30°	288
BRDM-2	E-71	30°	287
T-72	A64	30°	288
ZSU-234	d08	30°	288

Geometry

TEST EXAMPLES FOR EOC-2 (VERSION VARIANTS)

Class	Serial No.	Depression	No. Images
BMP-2	9566	15°, 17°	428
	c21	15°, 17°	429
T-72	812	15°, 17°	426
	A04	15°, 17°	573
	A05	15°, 17°	573
	A07	15°, 17°	573
	A10	15°, 17°	567

Version

TEST EXAMPLES FOR EOC-2 (CONFIGURATION VARIANTS)

Class	Serial No.	Depression	No. Images
T-72	S7	15°, 17°	419
	A32	15°, 17°	572
	A62	15°, 17°	573
	A63	15°, 17°	573
	A64	15°, 17°	573

Performance (MSTAR) - ML

Method	Performance (%)			Reference	
	SOC	EOC-1	EOC-2		
Pulse Couple Neural Network (PCNN) [35 tgts]	87.0	75	67	Blasch, 1998	[11]
Conditional False Alarm Rate (CFAR) [35 tgts]	89.0	91	85	Mossing, *et al.*, 1998	[**15**]
Support Vector Machine (SVM) [3 tgts]	90.0	81	75	Zhao, *et al.*, 2001	[**16**]
Conditional Gaussian [3 tgts]	92.0	80	79	O'Sullivan, *et al.*, 2001	[**17**]
AdaBoost [3 tgts]	92.0	82	78	Sun, *et al.*, 2007	[**18**]
Bayesian compressive sensing (BCS) [10 tgts]	92.0	-	-	Zhang, *et al.*, 2013	[**19**]
Sparse Representation of Monogenic Signal	93.6	88.4	-	Dong, *et al.* 2014	[**20**]
Iterative graph thickening (IGT)	95.0	85	80	Srinivas, *et al.*, 2014	[**21**]
Modified Polar Mapping Classifier (M-PMC)	98.8	-	97.3	Park, *et al.*, 2014	[**22**]
Monogenic scale space (MSS)	96.6	98.2	-	Dong, *et al.*, 2015	[**23**]

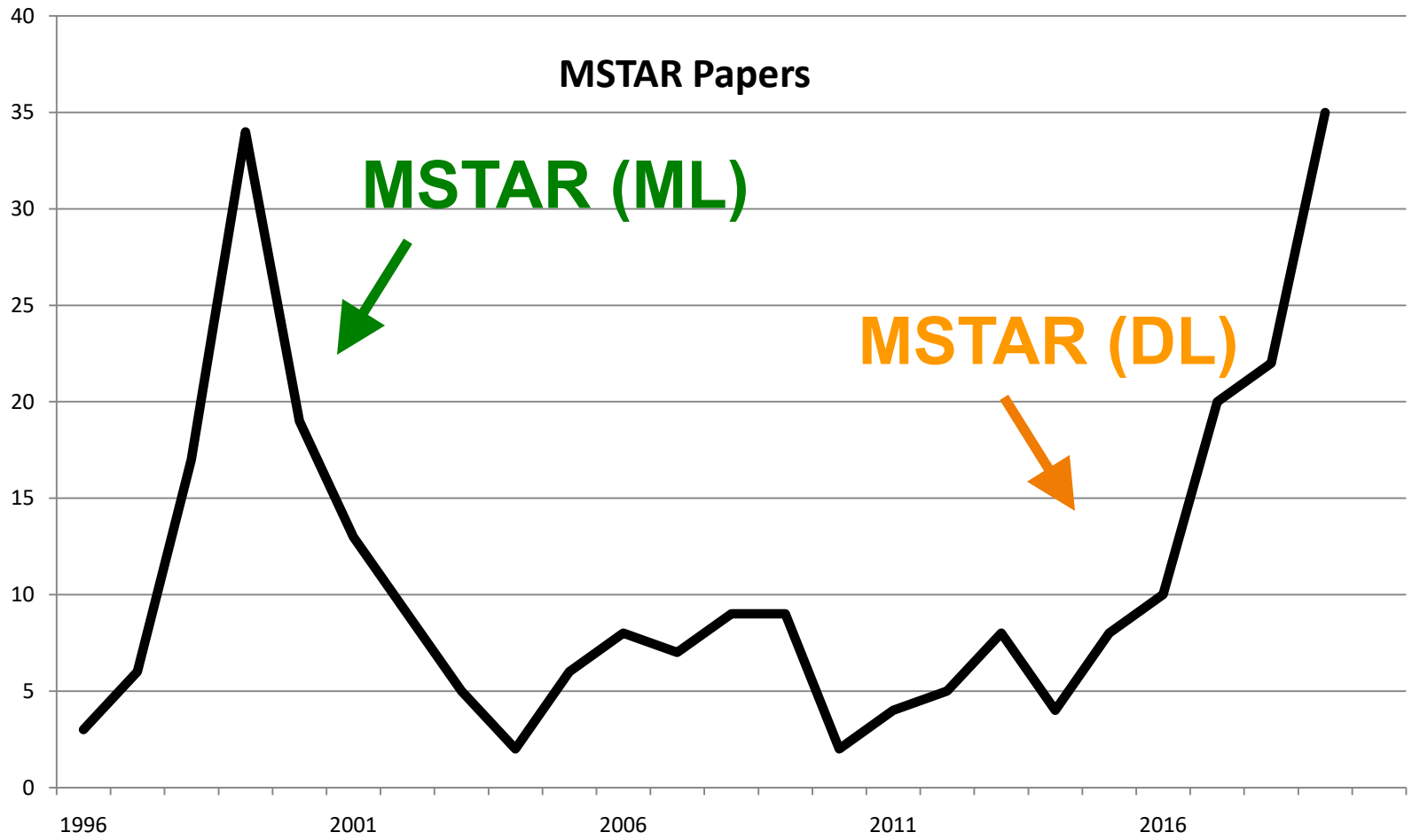
ATR Challenge Problems

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

Gorham, B. D., E. G. Zelnio, L. A. Gorham, *et al.*, "A synopsis of challenge problems," Proc. SPIE 8394, Algorithms for Synthetic Aperture Radar Imagery XIX, 2012.

MSTAR Publications

- **Literature Review**



Deep Learning

Deep Learning Algorithms

Generative Models

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

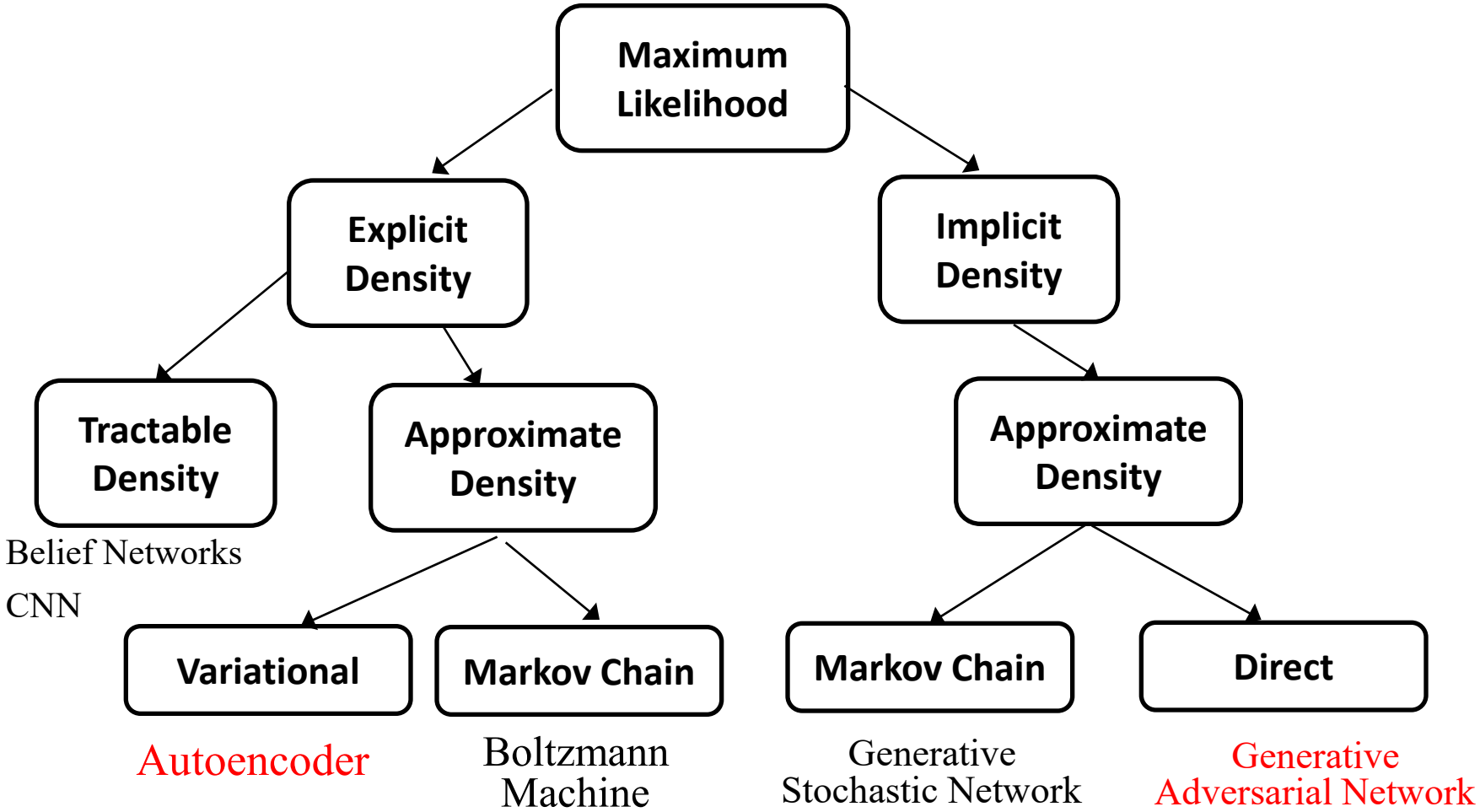
Discriminative Models

- Deep stacking Nets (DSN)
- Convolutional NN (CNN)
- Recurrent NN (RNN)

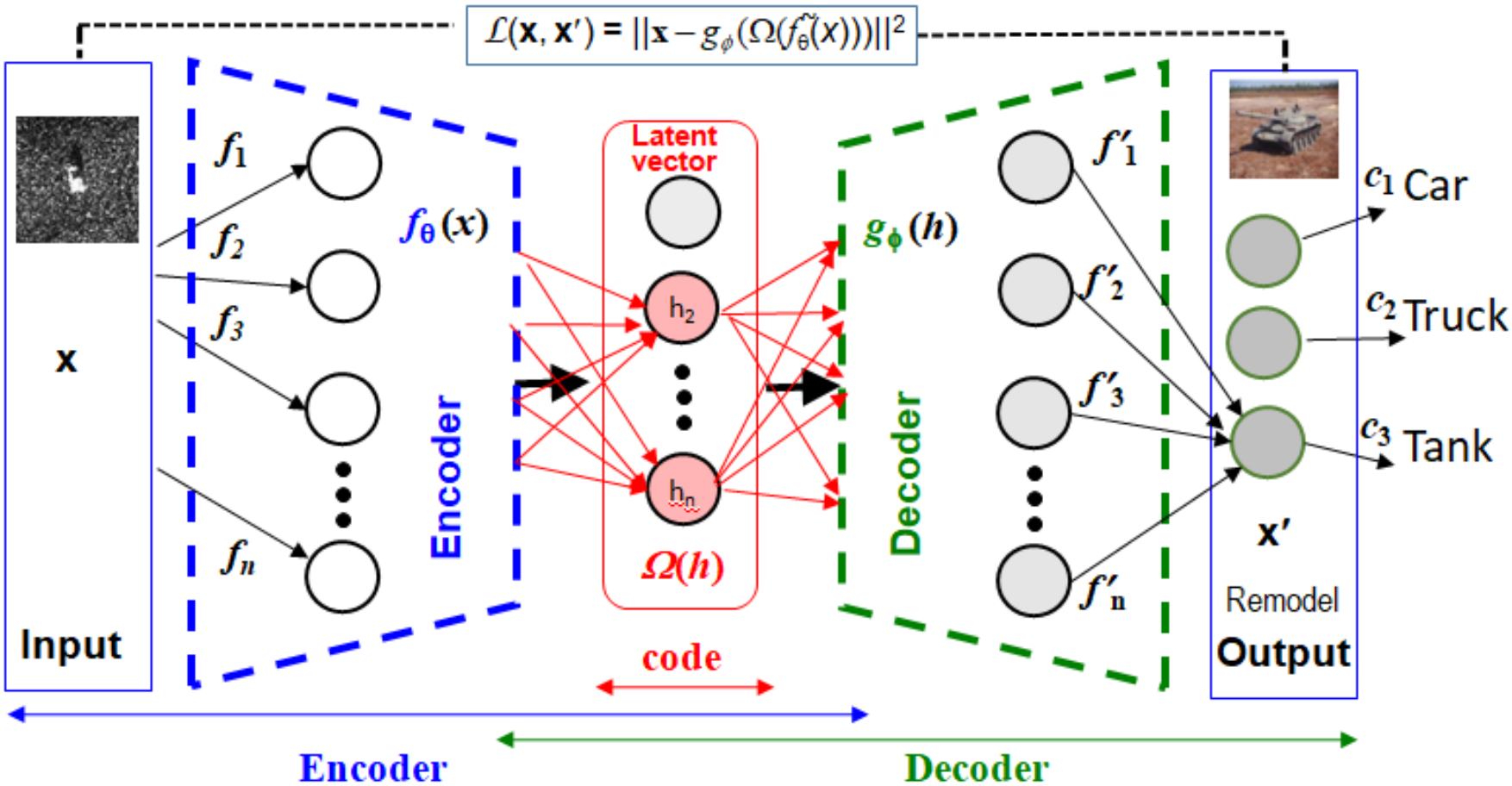
Hybrid Models

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

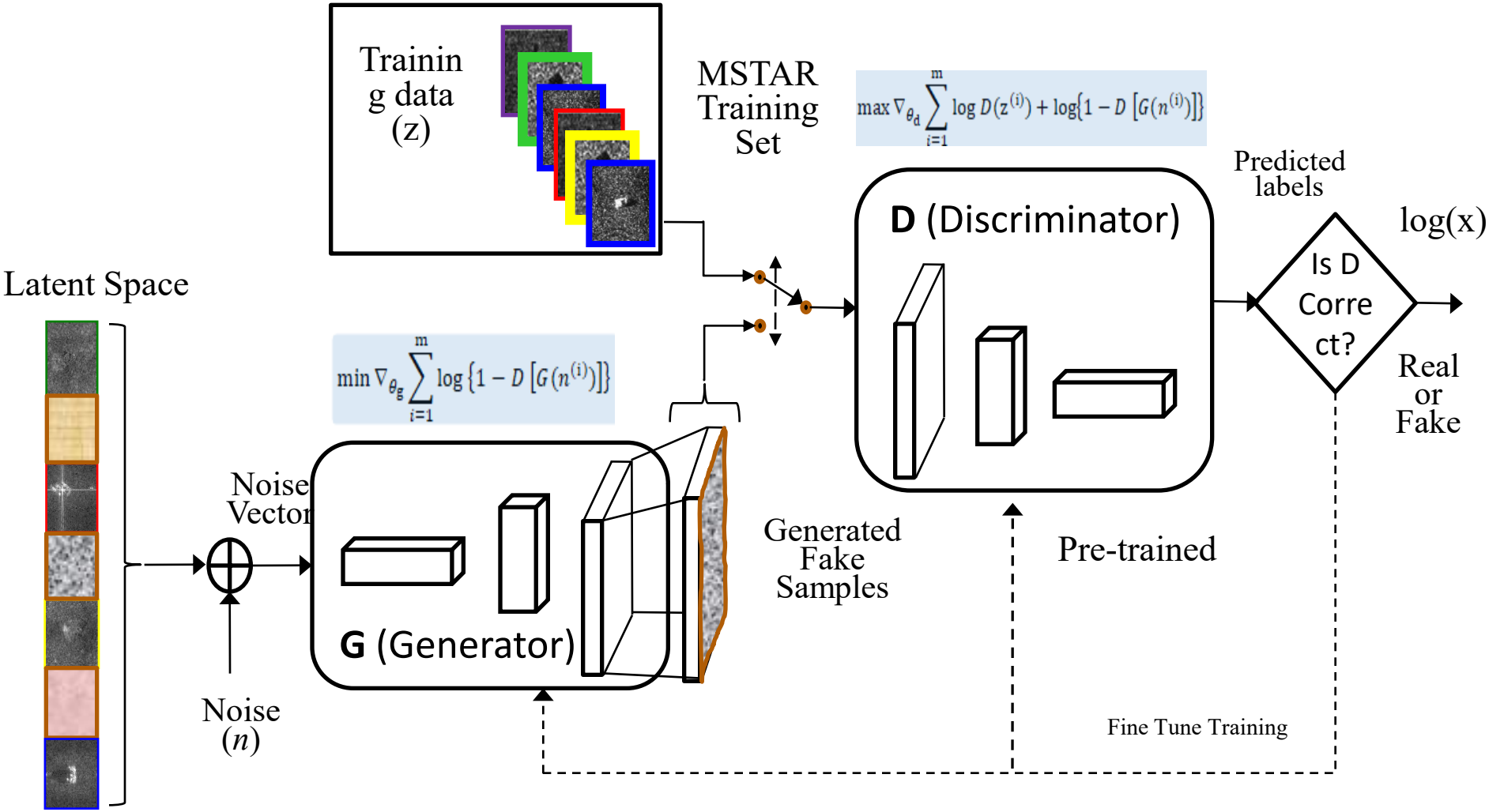
Deep Learning Generative Methods



Autoencoder



Generative Adversarial Networks



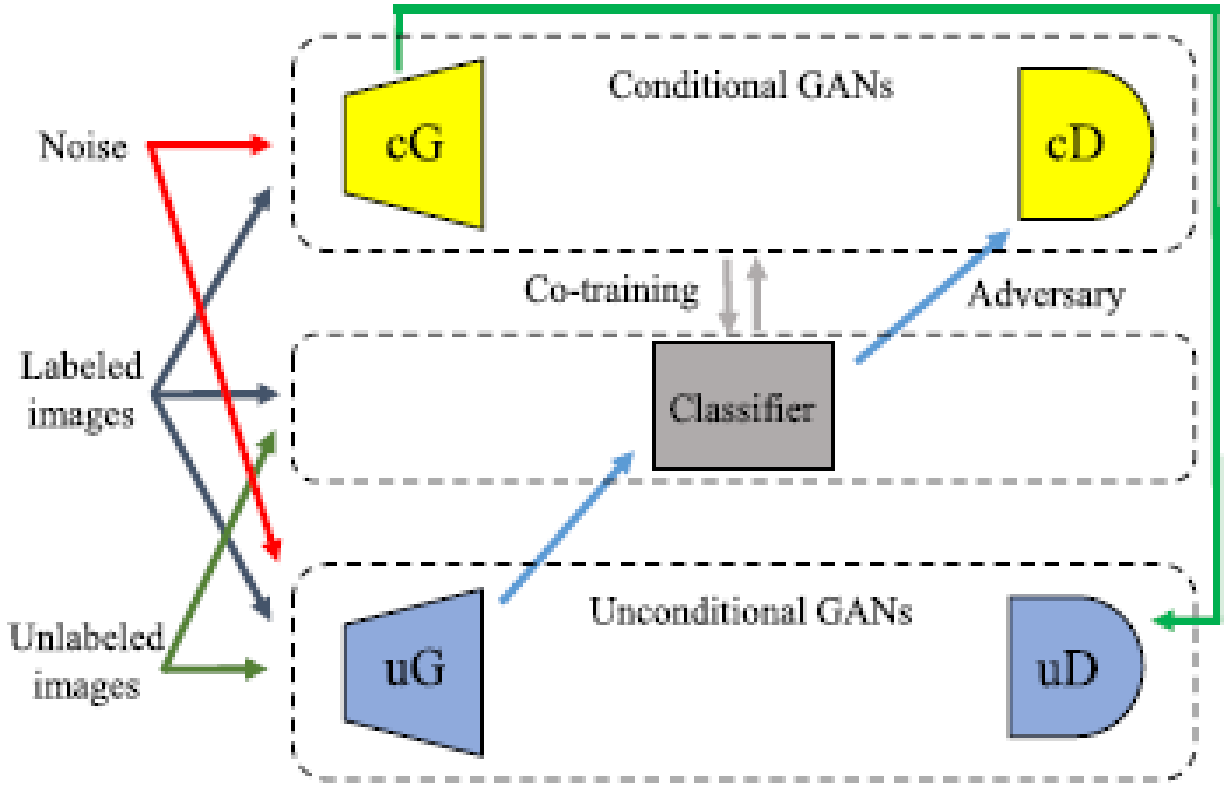
Performance (MSTAR) - DL

Method	Performance (%)			Reference	
	SOC	EOC-1	EOC-2		
A-ConvNets	99.1	96.1	98.9	Chen, *et al*., 2016	[24]
AFRLeNet	**99.4**			**Profeta *et al*., 2016**	[25]
CNN-SVM	99.5	95.75		Amrani, *et al*., 2017	[33]
VGG-S1	98.8	94.15		Amrani, *et al*., 2017	
VGG-S, Feature Fusion, KNN	99.82	96.16		Amrani, *et al*., 2017	
Multi-aspect aware bidirectional LSTM RNN	99.90	-	99.59	Zhang, *et al*. 2017	
Joint Supervised Dictionary	97.65	98.39			
GAN-CNN	97.53			Zheng, C et al, 2019	
MGAN-CNN	97.81			Zheng, C et al, 2019	
Triple GAN and Integrated GAN	99.9			Gao, F. Et al 2019	

MSTAR GAN - Adversarial Learning

Benefit 1 – higher accuracy

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



Triple GAN and Integrated GAN ~ 99.9% (with 600 labels)

Gao, F. et al, "Integrated GANs: Semi-Supervised SAR Target Recognition," IEEE Access, Vol 7, 2019.

*** Difficult to detect imposter data**

MSTAR GAN - Adversarial Learning

Benefit 2 – results with fewer training samples

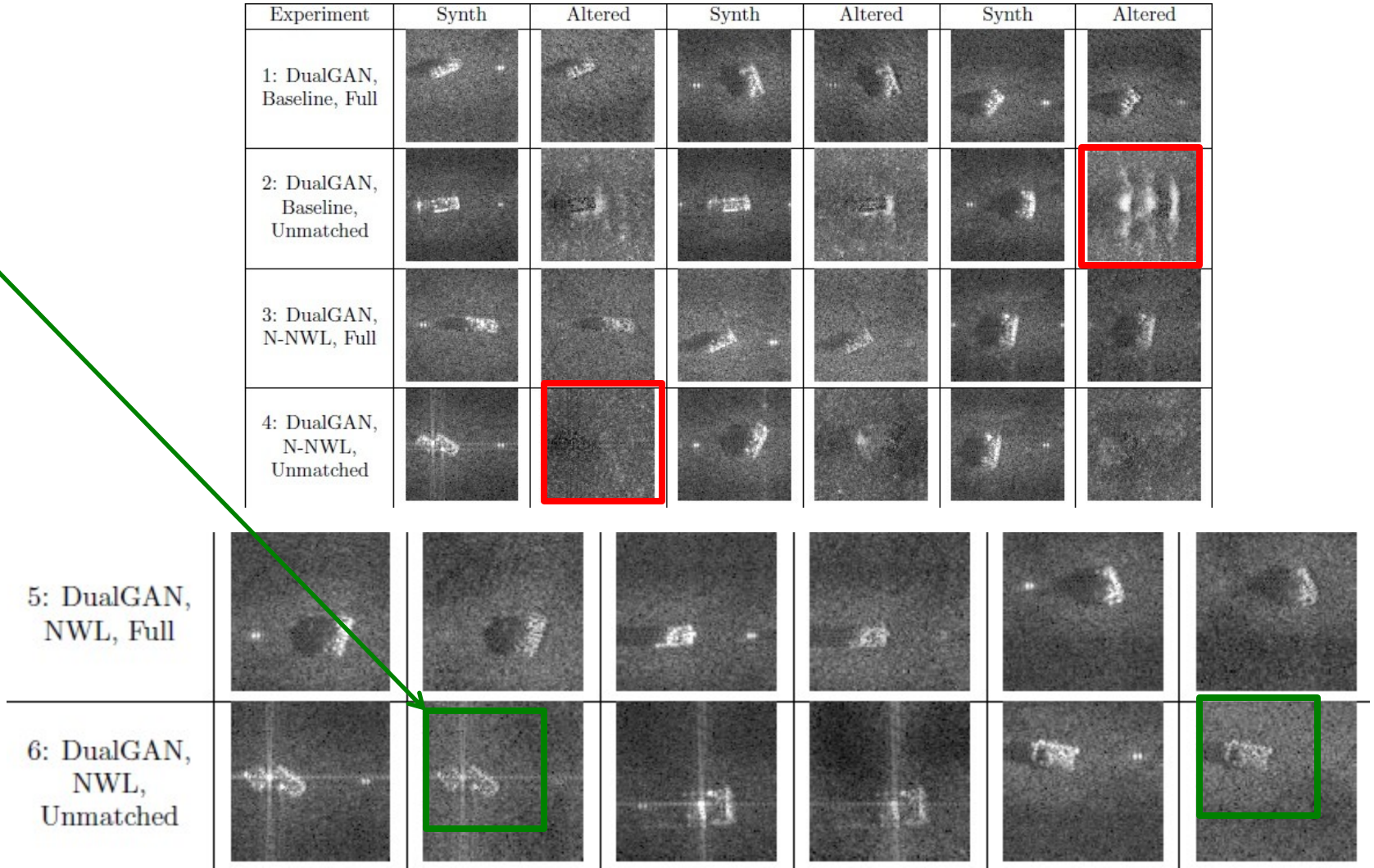
Method	**Accuracy**			
	20 Samples	40 Samples	80 Samples	All Samples
PCA-SVM	76.43	87.95	92.48	94.32
SRC	79.61	88.07	93.16	95.04
DNN	79.39	87.73	93.76	96.50
CNN	81.80	88.35	93.88	97.03
GAN-CNN	84.39	90.13	94.29	**97.53**
MGAN-CNN	**85.23**	90.82	94.91	**97.81**

Zheng, C., X. Jiang, X. Liu,, "Semi-Supervised SAR ATR via Multi-Discriminator Generative Adversarial Network," *IEEE Sensors Journal*, Volume: 19, Issue: 17, 2019.

MSTAR GAN - Adversarial Learning

Benefit 3 – Synthetic Image Generation for Robustness

- Lewis, B.(AFRL), Liu, J.(ASU), Wong, A.(Cornell), "Generative adversarial networks for SAR image realism," *Proc. SPIE. 10647*, (2018).



MSTAR Adversarial Corruption

Robust 1 – Adversarial Corruption

- **Corruption**

Original Test Chip | Target + Noise | Target + Corruption

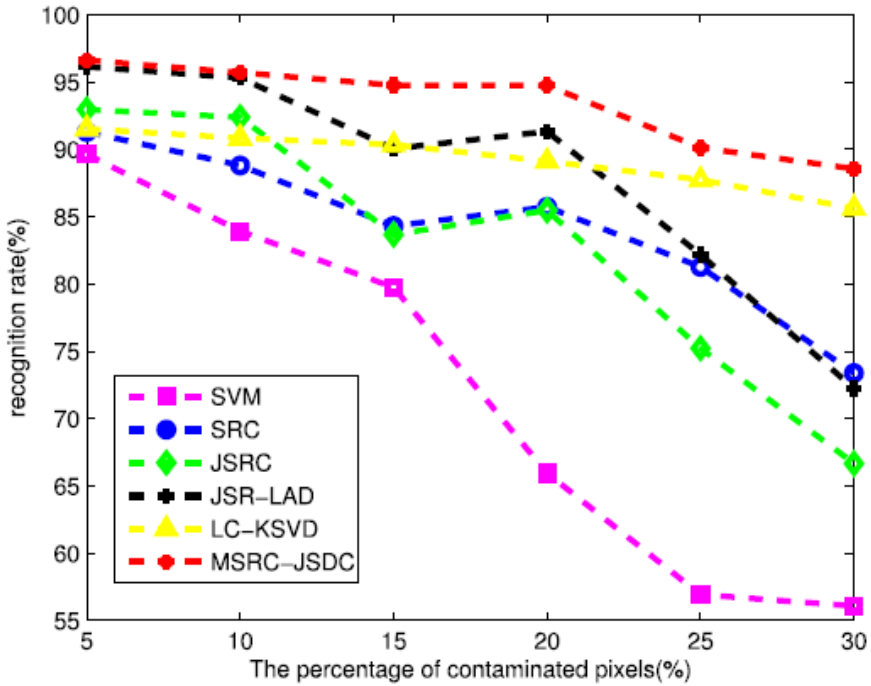


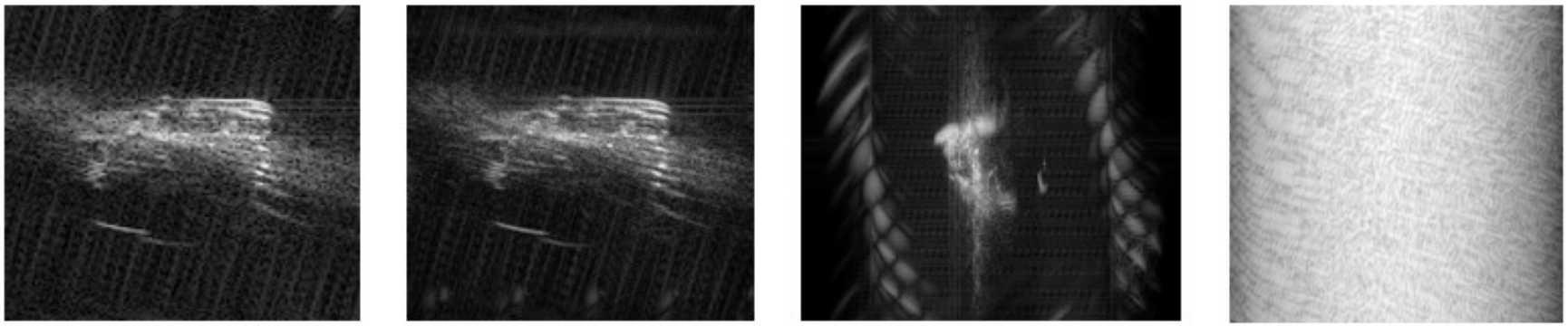
FIGURE 14. Recognition rates of different methods at different corruption levels.

Ren, H. et al, "Joint Supervised Dictionary and Classifier Learning for Multi-View SAR Image Classification," IEEE Access, Vol . 7, 2019.

MSTAR Adversarial Perturbation

Robust 2 – Model & Data Developed

SAR Image Formation



Backprojection (BP) | Polar Format (PF) | Range Doppler (RD) | Phase History (PH)

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

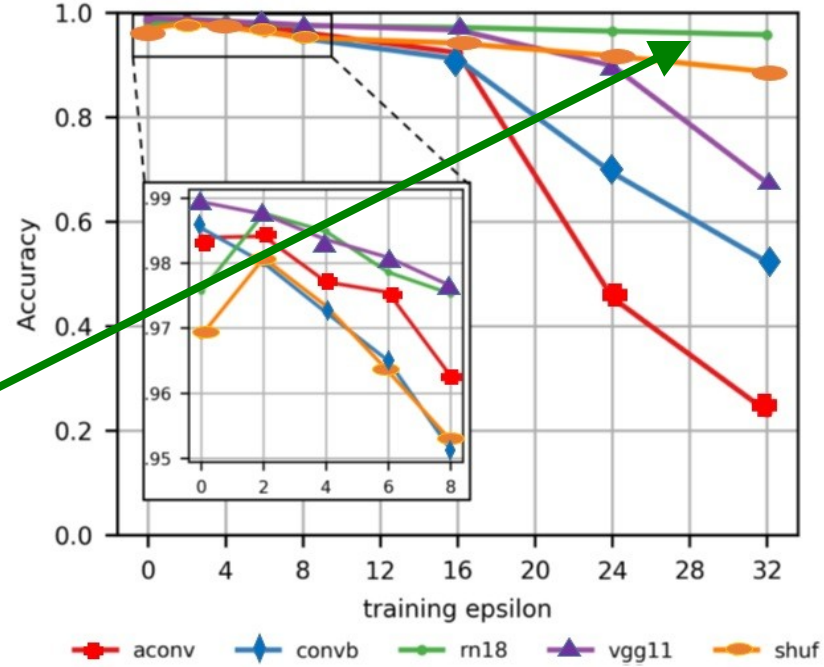
Inkawhich, N., E. Davis, U. Majumder, *et al*., "Advanced Techniques for Robust SAR ATR: Mitigating Noise and Phase Errors," *IEEE International Radar Conf*. 2020.

MSTAR Adversarial Perturbation

Robust 3 – Adversarial attack mitigation

- **Types of Attacks, Corruption**

Original Test Chip | Target + Noise | Target + Corruption

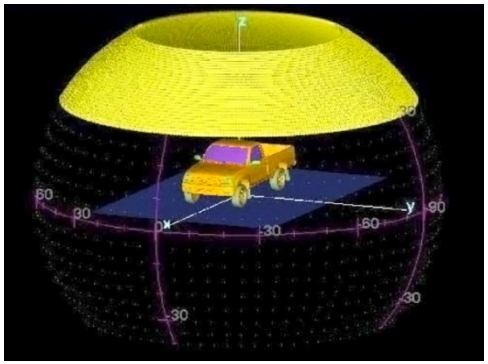


Simple models, such as aconv and convb, suffer the most **when significant attacks happen whereas ResNet18 stays competitive**

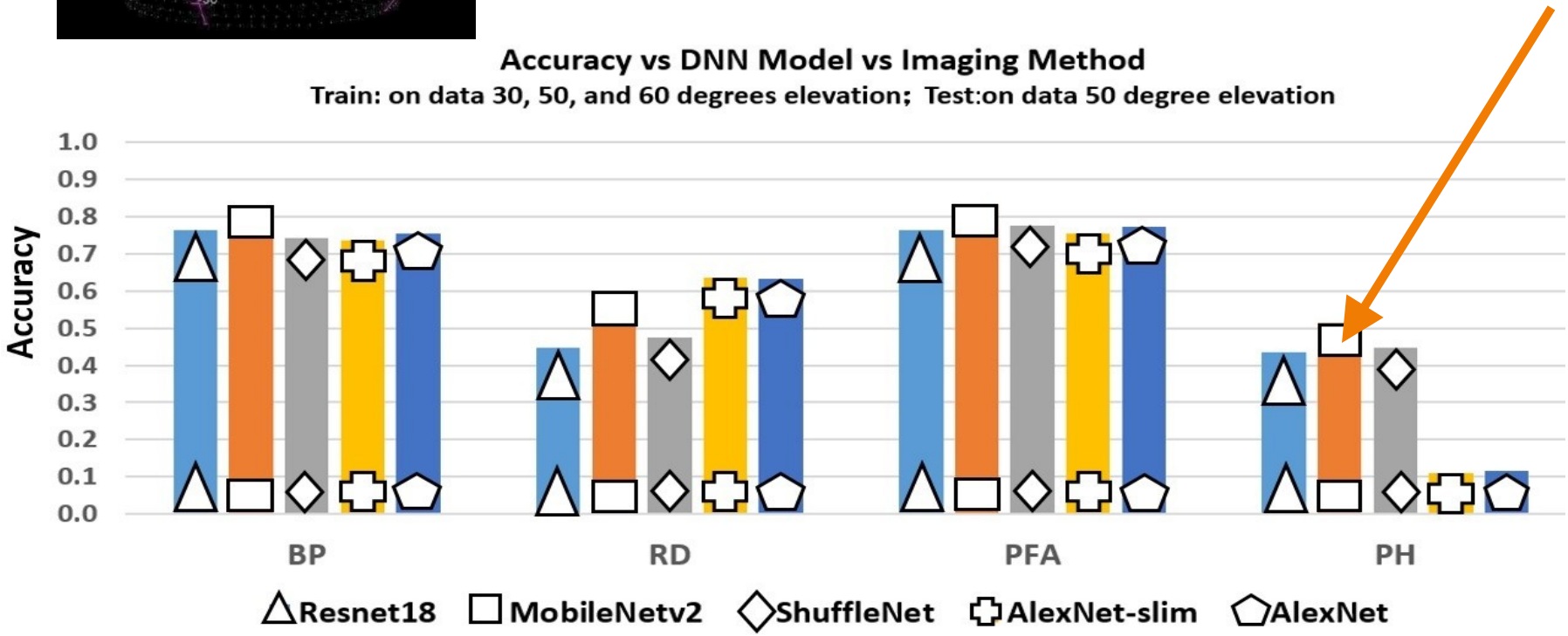
Inkawhich, N., E. Davis, U. Majumder, *et al.*, "Advanced Techniques for Robust SAR ATR: Mitigating Noise and Phase Errors," *IEEE International Radar Conf*. 2020.

CV Data Dome Adversarial Perturbation

Robust 4 – Adversarial Scenario Prediction



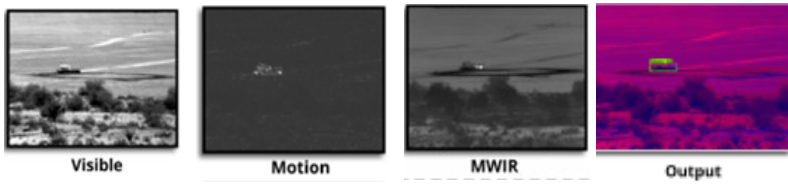
DNN models for the different SAR image formation methods *phase history* (PH), *range-Doppler* (RD), *polar format* (PF) and back-projection (BP, baseline) algorithm



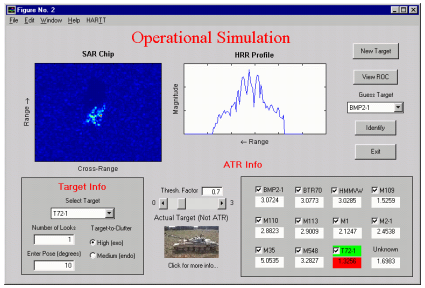
Inkawhich, N., E. Davis, U. Majumder, *et al.*, "Advanced Techniques for Robust SAR ATR: Mitigating Noise and Phase Errors," *IEEE International Radar Conf*. 2020.

Outline

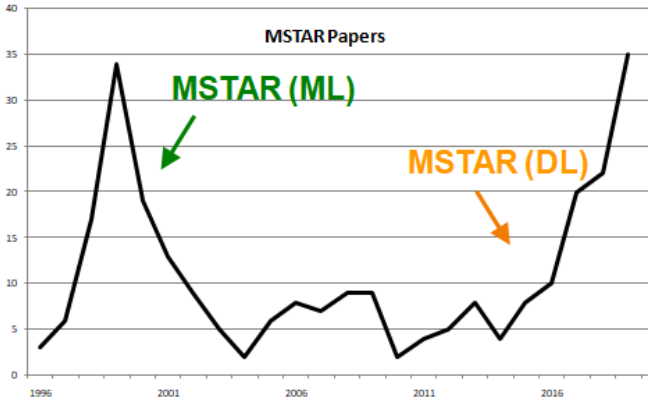
- **Motivation**
  - Sensor Fusion
  - Methods for Automatic Target Recognition (ATR)
  - RF Data (ATR and Communications)



- **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

Roy, D., Mukherjee, T., Chatterjee, M., *et al*., "RFAL: Adversarial Learning for RF Transmitter Identification and Classification," *IEEE Tr. on Cognitive Comm. and Networking*, (2019).

- **RF Transmitter Detection with GAN**

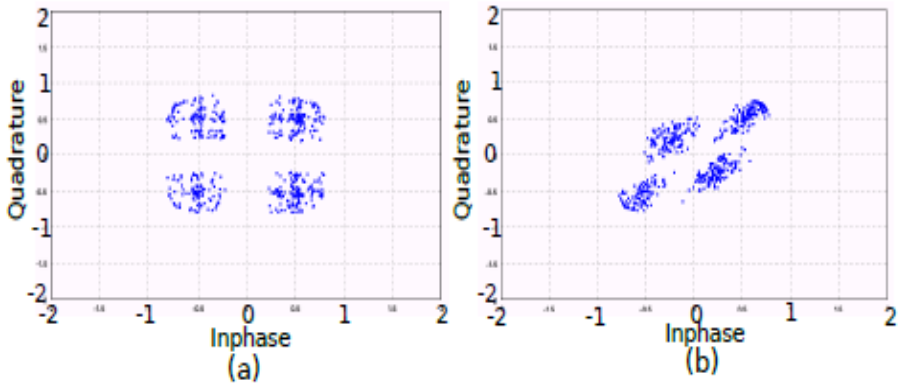
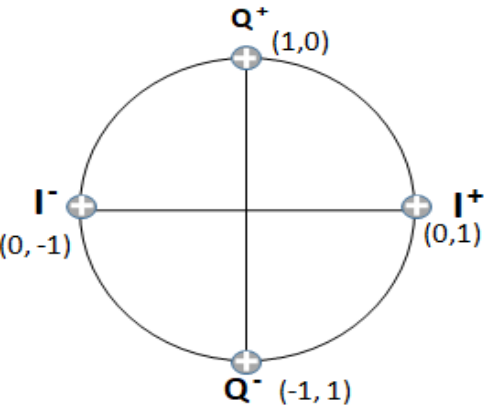
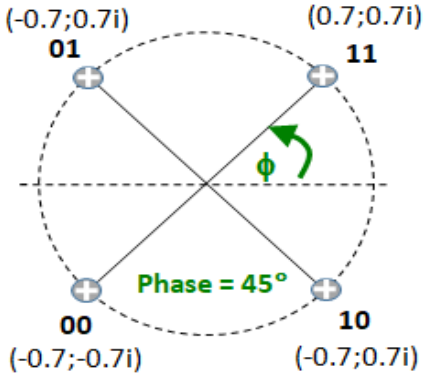


Fig. 1. I/Q Imbalance for QPSK: (a) Before (b) After 45° Phase Imbalance

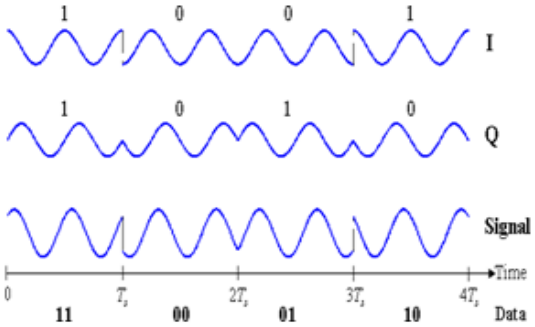
- **Objectives:**
- GAN to distinguish adversarial transmitters from trusted ones.
- CNN with 2D convolutions to exploit the correlation in collected signal data of the trusted transmitters for trusted transmitter identification.
- DNN to classify the trusted transmitters.
- RNN with both LSTM and GRU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



4-PSK



4-QPSK, (also, 4-QAM)



Quadrature Phase Shift Keying

-Bit modulation to tx more information

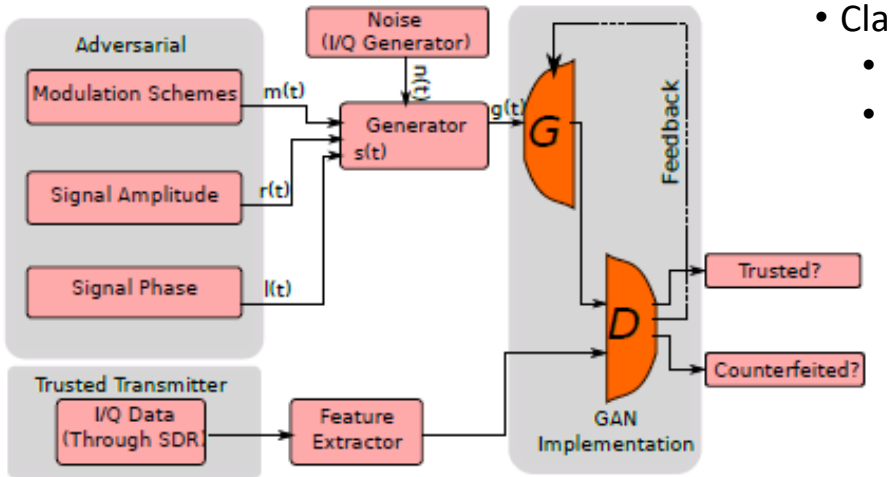
- each device has unique signature based on electronics conducting the A/D operations

Signals Classification and motivation to support "adversarial" environments

Radio Frequency Adversarial Learning

Roy, D., Mukherjee, T., Chatterjee, M., *et al.*, "RFAL: Adversarial Learning for RF Transmitter Identification and Classification," *IEEE Tr. on Cognitive Comm. and Networking*, (2019).

- RF Transmitter Detection with GAN

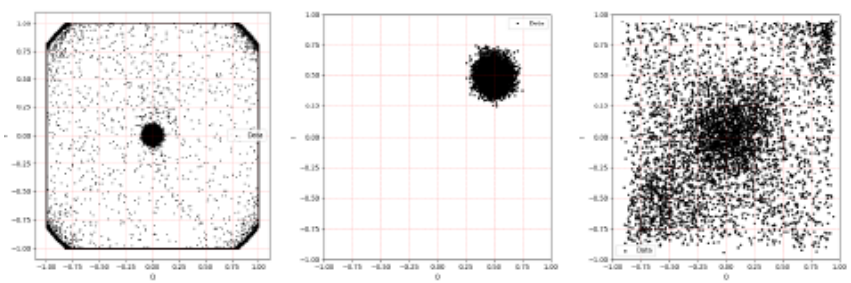


- Detection model - GAN
- Classification Model Types
  - DNN, CNN
  - LSTM (RNN, GRU)

8 universal software radio peripheral (USRP)
- 5 experiments

#Trans	Models	#Parameters	Acc (%)	Time (min)
4	CNN	38 Million	89.07	~25
4	DNN	6.8 Million	96.49	~12
4	RNN - LSTM	14.2 Million	97.40	~12
4	RNN - GRU	10.7 Million	97.85	~12
8	CNN	38 Million	81.59	~30
8	DNN	6.8 Million	94.60	~15
8	RNN - LSTM	14.2 Million	95.78	~16
8	RNN - GRU	10.7 Million	97.06	~16

TABLE III
COMPARISON OF THE VARIOUS IMPLEMENTATIONS



(a) Real Data (b) Generated Data before GAN Training (c) Generated Data after GAN Training

Models	#Layers	Learning Rate	Batch Size	Epochs	Optimizer
CNN	7	10^{-4}	128	45-50	*Adam* [53]
DNN	5	10^{-3}	128	35-40	*Adam* [53]
RNN-LSTM	6	10^{-3}	128	30-35	*SGD* [18]
RNN-GRU	6	10^{-3}	128	30-35	*SGD* [18]

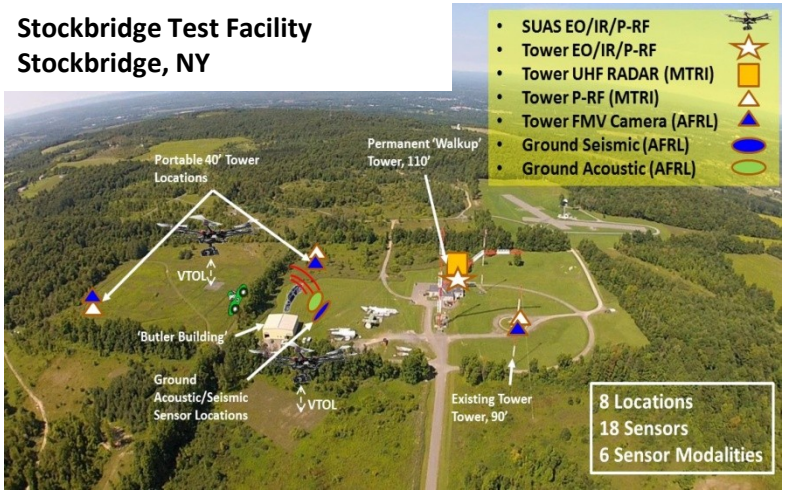
TABLE IV
COMPARISON OF CONFIGURATION SETTINGS FOR DIFFERENT MODELS

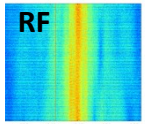
Real world testing on RF devices

ESCAPE Data Collection

Zluch, et al, ESCAPE Data Collection for Multi-Modal Data Fusion Research ," IEEE Aerospace, 2019

Stockbridge Test Facility
Stockbridge, NY





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

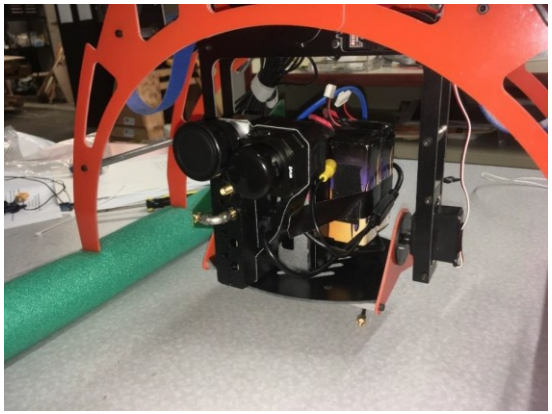
Airborne – SUAS (2) targets, various flight profiles, ground idle to hovering to flight, multiples

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

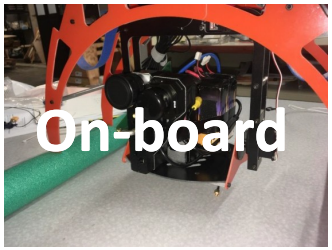


- Multi-Int Payload: EO/IR/Passive RF
- 2 flown on SUAS (DJI M600)
- 1 Tower Mounted

Sensor Baseline

P. Zulch, M. Distasio, T. Cushman, et al, " ESCAPE Data Collection for Multi-Modal Data Fusion Research," *IEEE Aerospace*, March 2019.

- **Multi-source data correlated on single targets**



Modality	Sensor	Ownership	Resolution (H X V)	Weight	Deployment (Height (m))	Near Ground Range (m)	Far Ground Range (m)
EO	**Basler Ace acA3800 FMV**	MTRI (Deliverable)	**(3840 X 2748)**	133 g	**SUAS (50)**	**0**	**250**
IR	**Flir Vu Pro-R 640 FMV**	MTRI (Deliverable)	**(640 X 512)**	114 g	**SUAS (50)**	**5**	**140**
Passive-RF	**USRP B200**	MTRI (Deliverable)	12 MHz BW 1245 MHz	350 g	**SUAS (50)**	**-**	**-**

Modality	Camera Model	Ownership	Pixel Resolution (H X V)	Weight	Expected Deployment (Height (m))	Near Ground Range (m)	Far Ground Range (m)
Seismic	**Raspberry Pi Shake**	AFRL/RIGC	**-**	65 g	**Ground (0)**	**0**	**250**
Acoustic	**Bruel & Kjaer 4952**	AFRL/RIGC	**-**	114 g	**Ground (0)**	**0**	**250**
RADAR (UHF)	**Akela Tapered Horns**	MTRI	-	8 kg	**Tower (33.54)**	**5**	**400**
EO	**Allied Vision Prosilica GX3300C**	AFRL/RIGC	**(3296 X 2472)**	365 g	**Tower (27.44)**	**30**	**250**
Passive RF	**Ettus N210 SDR**	MTRI	**-**	1.2 kg	**Tower (27.44)**	**0**	**Source Dependent**

*** Multimodal EO/RF DL & GAN submitted for review**

Opportunity

- **http://nrc58.nas.edu/RAPLab10/Opportunity/Opportunity.aspx?LabCode=13&ROPCD=132005&RONum=C0135**

RO#	Location
13.20.05.C0135	Rome, NY 134414514

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