Skoltech

SkoltechSIM: GPS Spoofing Detection Artifact

Deep Learning Course 2024

Oleg Sautenkov
Yaroslav Solomentsev
Alexander Zolotarev
Joshua Udobang

27 May 2024

Skoltech

Problem at hand

GNSS - the best way to navigate the **outdoor** drones.
GNSS can be easily tricked.

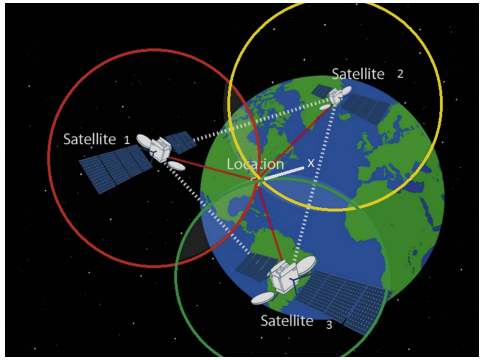


Figure 1. GNSS Triangulation Scheme

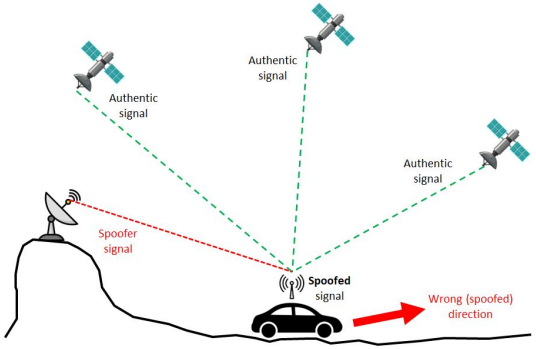


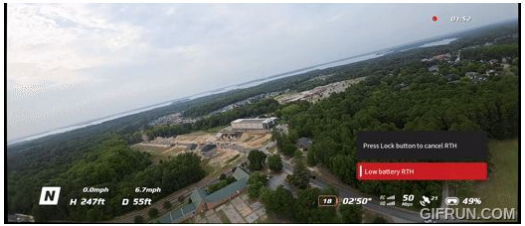
Figure 2. GNSS Spoofing Example

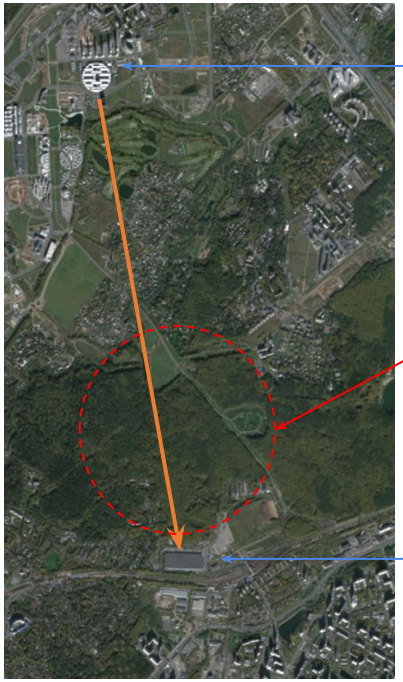
GNSS Jamming is overwhelming relatively weak GNSS signals.
GNSS Spoofing is more sophisticated, tricking the receiver into calculating a false position, which could send an aircraft off the desired course.

General problem: The operation of complex **UAV** cargo delivery and **UAV** transportation systems can **be violated**. **UAVs** can be **hijacked,** intentionally **crashed,** or sent to an **energetically important hub.**

Skoltech

Problem Statement





Flying

GPS spoofing

Result

Skoltech

Research Problem Statement

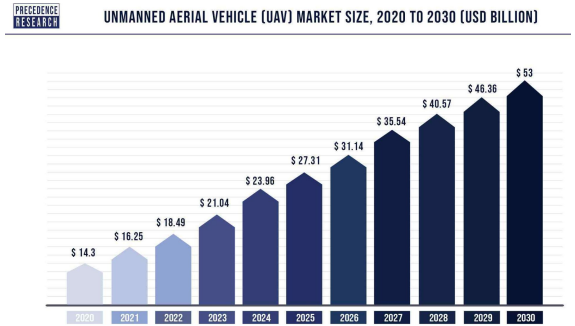


Figure 1. UAV Market Forecast in $ Millions 2020-2030 [1]

Figure 2. Shenzhen Delivery Drones [2]

Figure 3. Result [3]

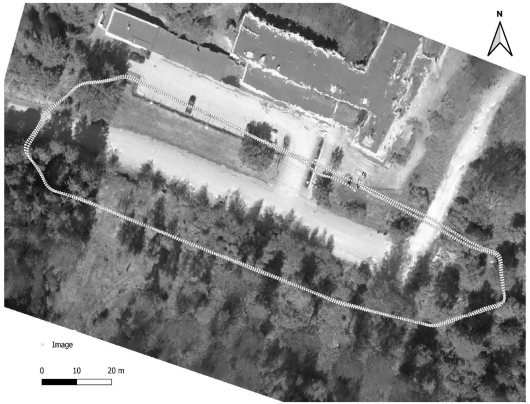
Research gap: There is no any cheap redundant method to detect **the drone spoofing.**

Hypothesis: The drones are able to **detect GPS spoofing with Neural Networks.**

Skoltech

[1] Source: Inkwood Research https://www.inkwoodresearch.com/
[2] Source: TechCrunch https://techcrunch.com/2021/12/29/meituan-food-drone-delivery-china/
[3] Source: The Times of Israel https://www.timesofisrael.com/in-apparent-world-first-idf-deployed-drone-swarms-in-gaza-fighting/

Paper



DeepSIM: GPS Spoofing Detection on UAVs using Satellite Imagery Matching

☑ Spoofing Artifact detector
☒ The same dataset

[1] Xue, Nian & Niu, Liang & Hong, Xianbin & li, zhen & Hoffaeller, Larissa & Poepper, Christina. (2020). DeepSIM: GPS Spoofing Detection on UAVs using Satellite Imagery Matching. 10.1145/3427228.3427254.

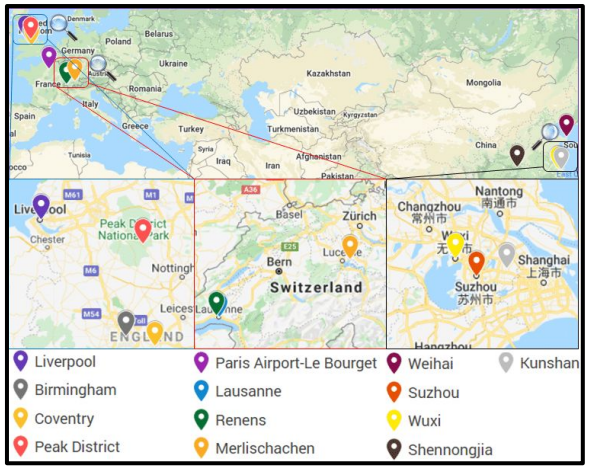
Skoltech

Tasks and problems:

1. The satellites images are significantly differing from the belly-mounted UAV camera.
2. The paper was published on quite old architecture.

Skoltech

Dataset description



Images in the dataset are part of **two** categories: **aerial** photography and **satellite** imagery. As of now, the total number of imagepairs in the dataset is 967 (appr. 12.08 Gigabyte).
In total, there are **967 aerial photos**. Among them are **605 realistic scene** photos with a light height of 120 m, that were captured using UAV; 343 of these photos were taken in Suzhou, China, and 20 photos were captured in Kunshan, China.

Skoltech

Dataset description

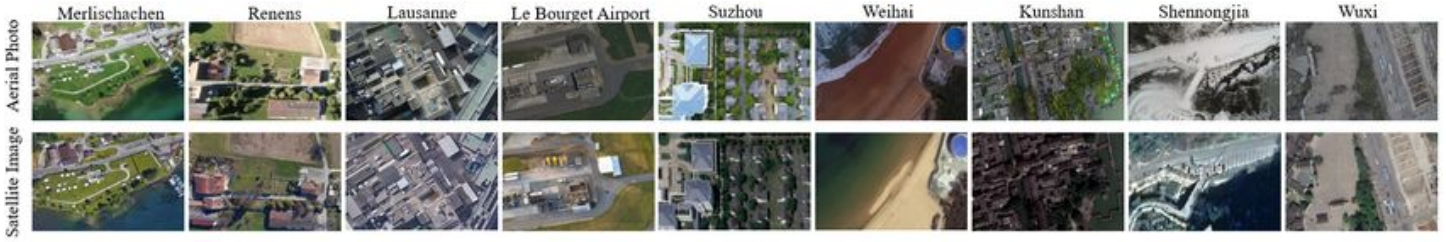
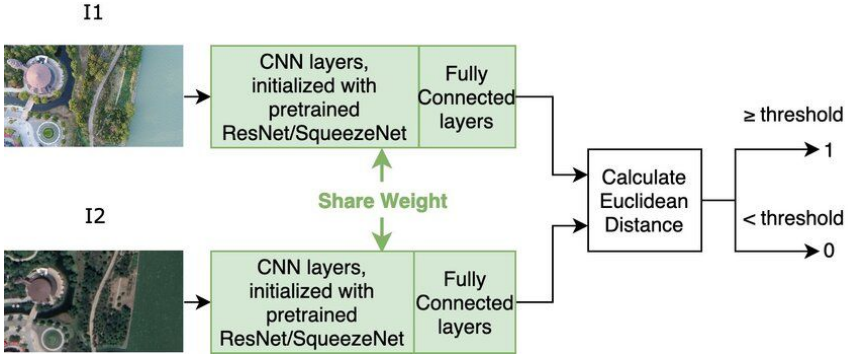


Table 1: Specification summary of aerial photography.

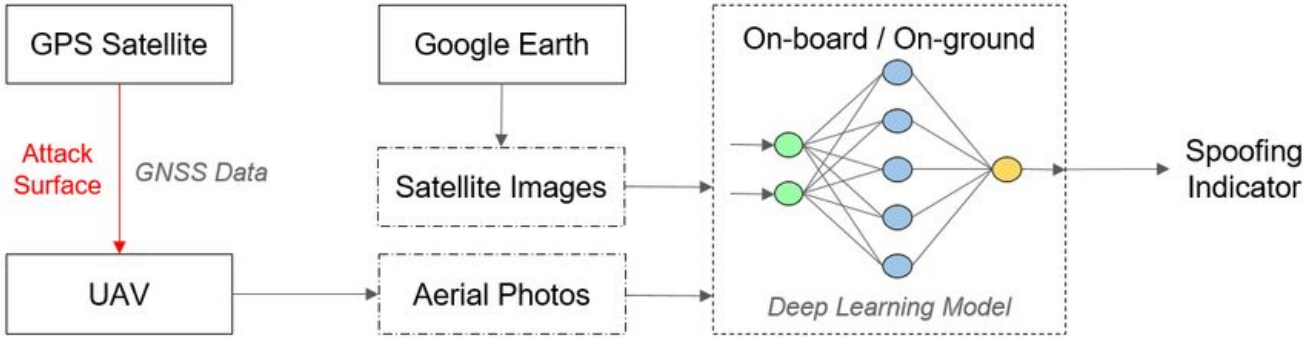
Place	Pixel resolution	Ratio	#Images	Flight height	Shooting time	Scenario features	Camera	Usage
Suzhou	5472×3078	16:9	343	120 m	9/2018–3/2019	lakeside city	DJI	training&test
Kunshan	5472×3078	16:9	20	120 m	10/2018	heritage town	DJI	training&test
Weihai	5472×3078	16:9	57	120 m	10–11/2018	coastal city	DJI	training&test
Shennongjia	5472×3078	16:9	9	120 m	12/2018	mountain forests	DJI	training&test
Wuxi	5472×3078	16:9	69	120 m	3/2019	downtown	DJI	training&test
Birmingham	5472×3078	16:9	37	120 m	4/2019	city park	DJI	test-only
Coventry	5472×3078	16:9	15	120 m	5/2019	university campus	DJI	test-only
Liverpool	5472×3078	16:9	41	120 m	4/2019	urban&park	DJI	test-only
Peak District	5472×3078	16:9	14	120 m	5/2019	national park	DJI	test-only
Merlischachen	4608×3456	4:3	160	162 m	4/2013	lakeside village	Canon IXUS	training&test
Renens	4608×3456	4:3	40	162 m	10/2016	cropland	Sequoia	training&test
Lausanne	5472×3648	3:2	113	100 m	1/2000	industrial zone	S.O.D.A.	training&test
Le Bourget Airport	4608×3456	4:3	49	120 m	6/2013	airport	Canon IXUS	training&test

Skoltech

Methodology

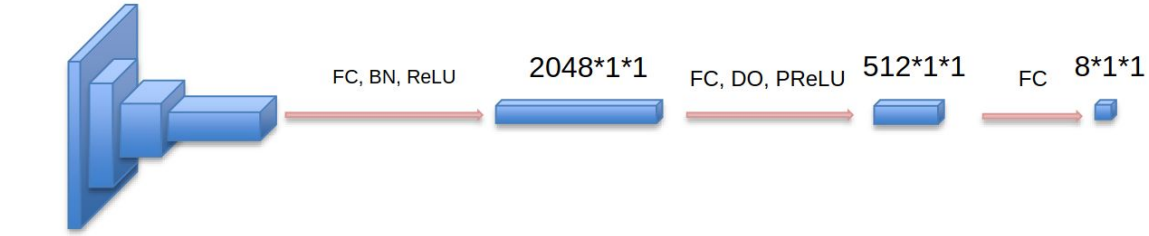


$$\mathcal{L} = \frac{1}{2}\{(1-y)\times d^2 + y \times max(margin - d, 0)^2\},$$

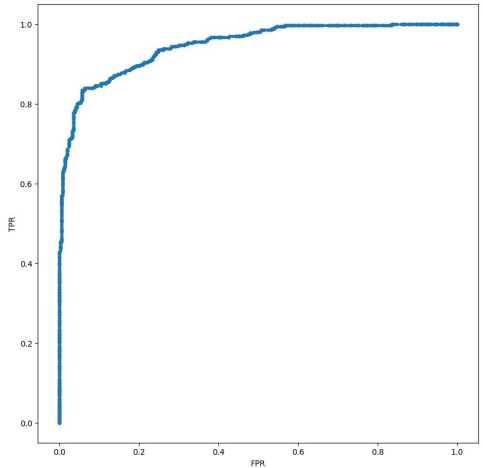


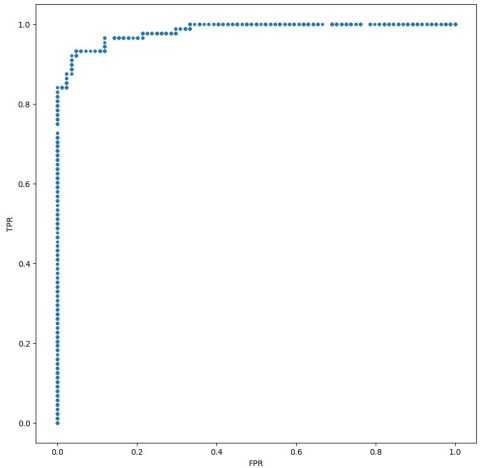
Skoltech

ResNet34 Backbone (original)



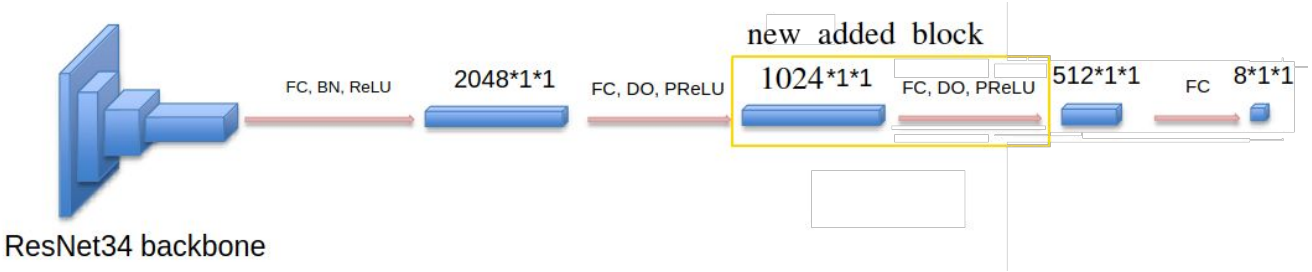
ResNet34 backbone

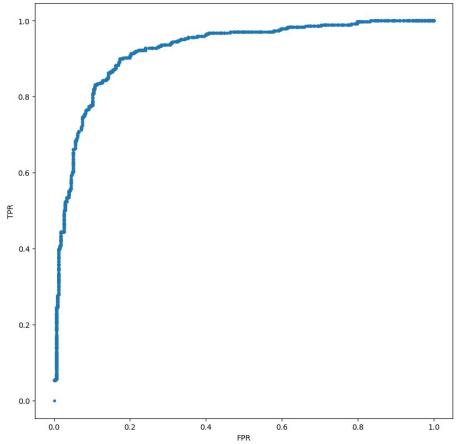


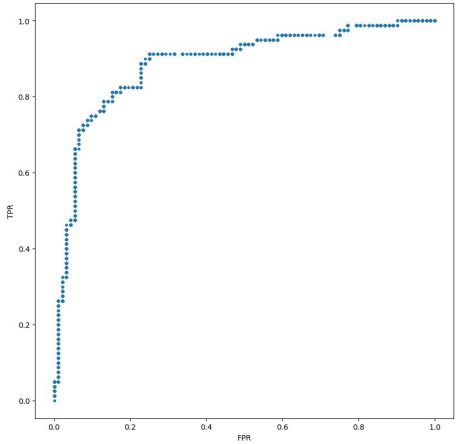


Skoltech

ResNet34 with added block

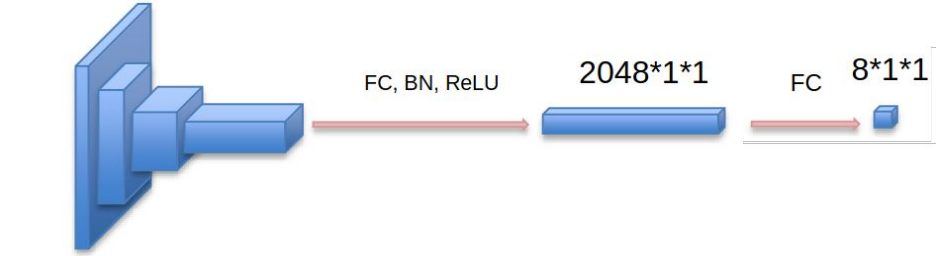


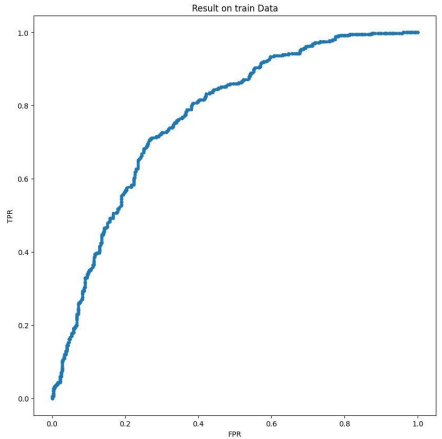


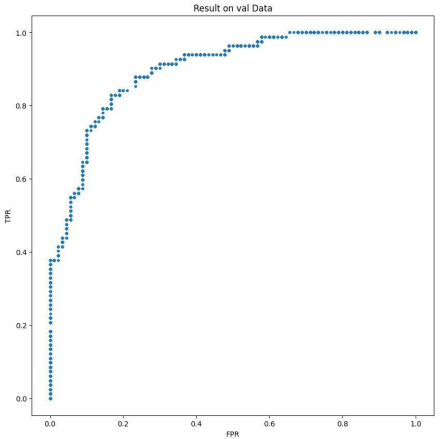


Skoltech

ResNet34 with removed block

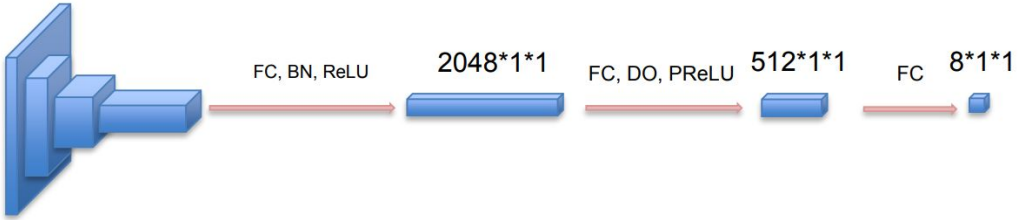




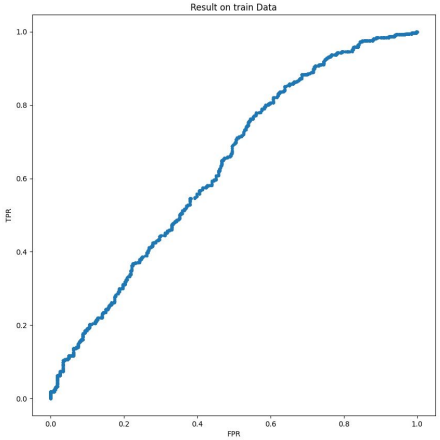


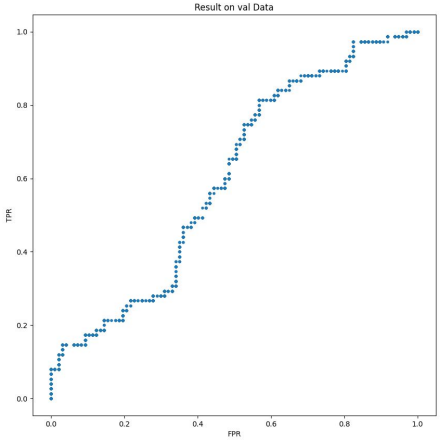
Skoltech

ResNeXt50 Backbone.
ROC-curves



ResNeXt50 backbone





Skoltech

Augmented data. Grayscaling

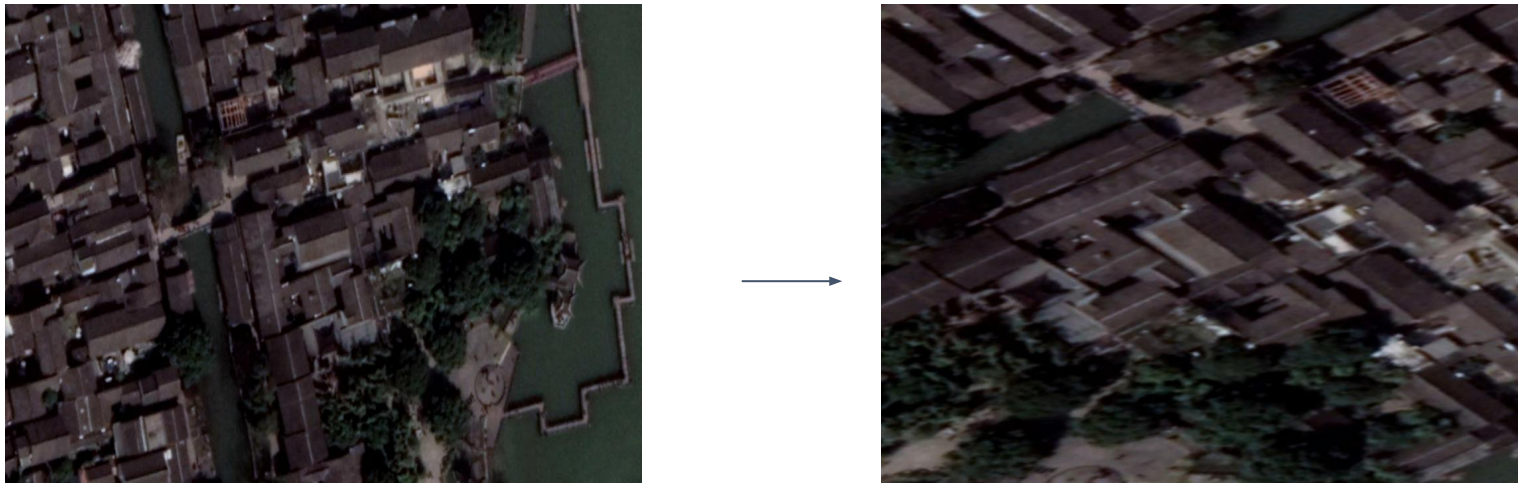
https://github.com/Lariiii/DeepSimDataAugmentation/blob/master/augmentation.py

Augmented data. Cropping

https://github.com/Lariiii/DeepSimDataAugmentation/blob/master/augmentation.py

Skoltech

Augmented data. Rotating and cropping



Skoltech

https://github.com/Lariiii/DeepSimDataAugmentation/blob/master/augmentation.py

Augmented data. Fog

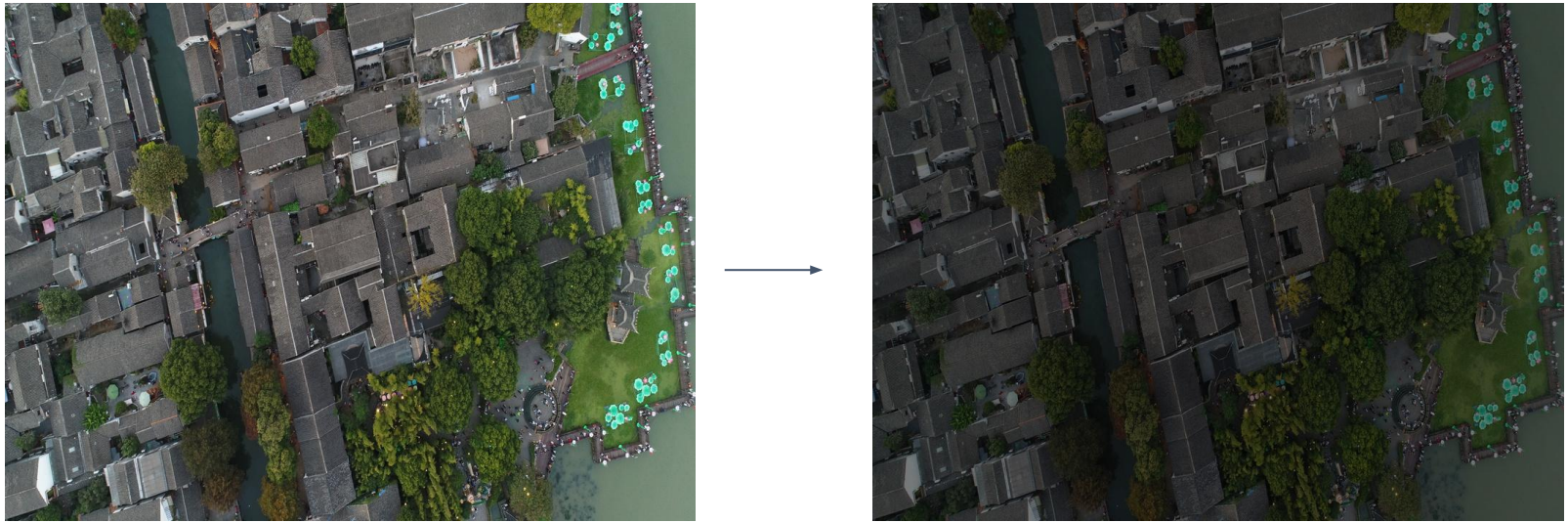
Skoltech

https://github.com/Lariiii/DeepSimDataAugmentation/blob/master/augmentation.py

Augmented data. Clouds

https://github.com/Lariiii/DeepSimDataAugmentation/blob/master/augmentation.py

Augmented data. Darkening



https://github.com/Lariiii/DeepSimDataAugmentation/blob/master/augmentation.py

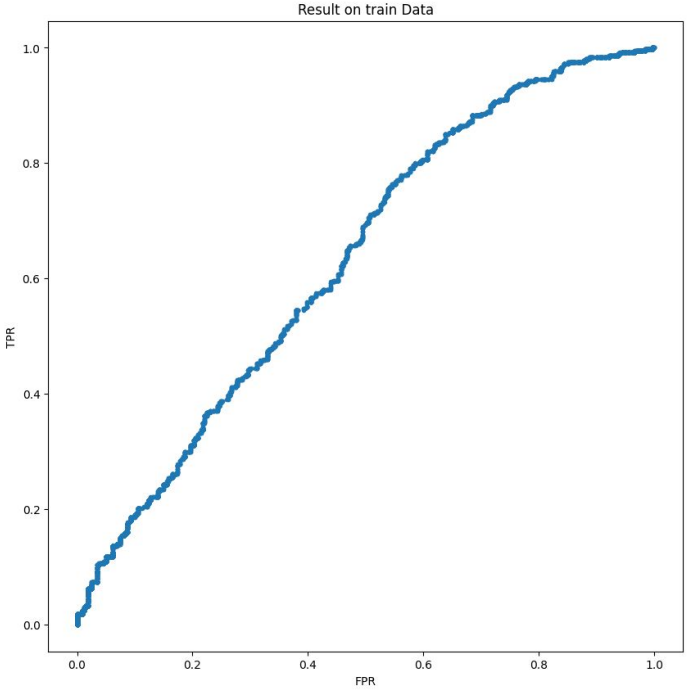
Skoltech

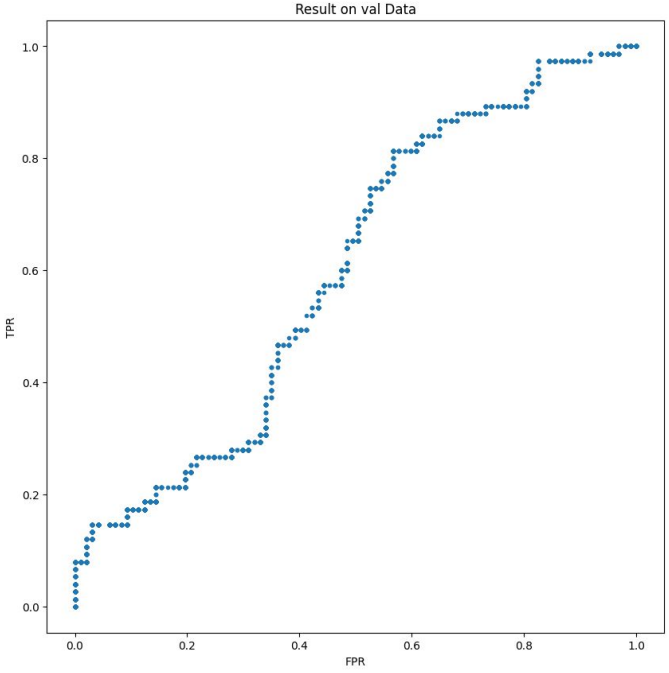
Augmented data. Brightening

https://github.com/Lariiii/DeepSimDataAugmentation/blob/master/augmentation.py

Skoltech

ResNet34 on augmented data. ROC-curves





Skoltech

Results

Table 1: Metrics of trained models on training sample

	TPR	FPR	Accuracy	Precision	Recall	F1-score
Original SiameseResNet34 proposed by authors	0.941	0.189	0.875	0.828	0.941	0.881
SiameseResNet34 with additional linear block	0.880	0.240	0.824	0.808	0.880	0.842
SiameseResNet34 without a linear block	0.722	0.297	0.712	0.701	0.722	0.711
SiameseResNeXt50	0.75	0.550	0.594	0.560	0.75	0.641
Original SiameseResNet34 on augmented data	0.776	0.561	0.619	0.613	0.776	0.685

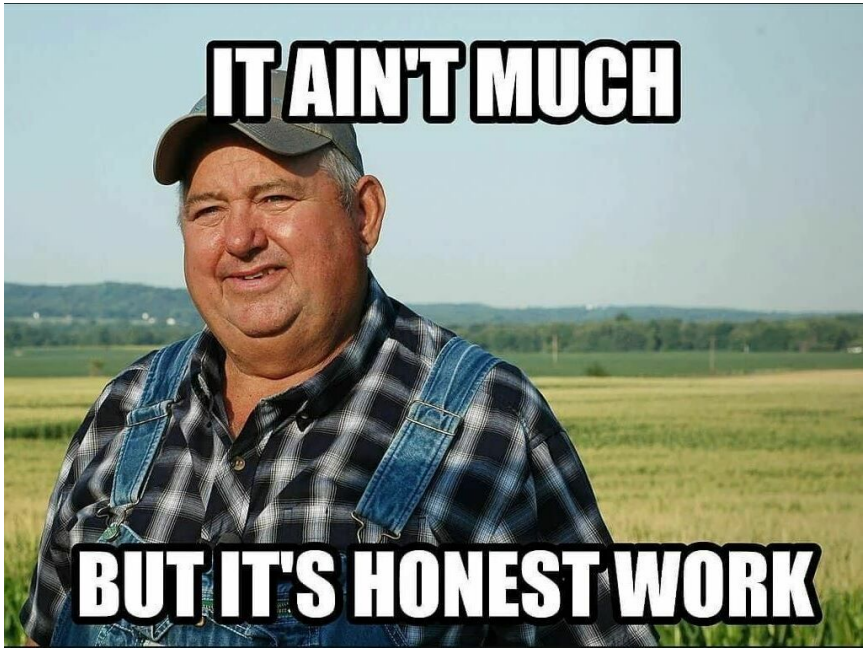
Table 2: Metrics of trained models on validation sample

	TPR	FPR	Accuracy	Precision	Recall	F1-score
Original SiameseResNet34 proposed by authors	0.967	0.183	0.895	0.853	0.967	0.906
SiameseResNet34 with additional linear block	0.893	0.340	0.773	0.714	0.893	0.794
SiameseResNet34 without a linear block	0.821	0.227	0.796	0.775	0.821	0.798
SiameseResNeXt50	0.840	0.551	0.663	0.648	0.840	0.731
Original SiameseResNet34 on augmented data	0.827	0.608	0.581	0.512	0.827	0.633

Conclusion

1. We researched the SatUAV dataset
2. We learned how to use the augmentations
3. We tried different architectures
4. We tried to apply modern architectures, but it was so time-consuming. We were not successful in outperforming the authors, however, the closest result was an old architecture with added linear block.
5. The augmentation of authors didn't provide any improvements on the model, so most probably the authors were not very honest with the augmentation pipeline and its results.

Thank you for your attention.



Skoltech