Centre for Frontier AI Research

CFAR

Robust VisIntel:

A Road towards Robustness of Visual Intelligence

GUO Qing, Scientist, CFAR

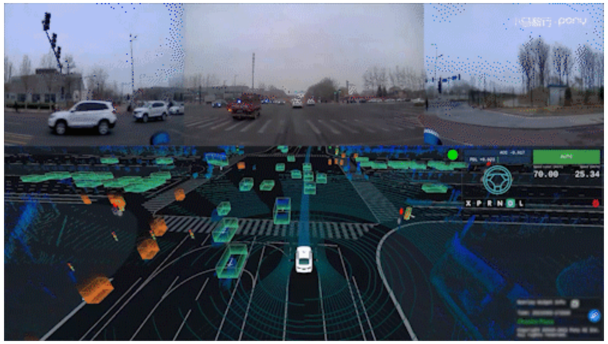
tsingqguo@ieee.org

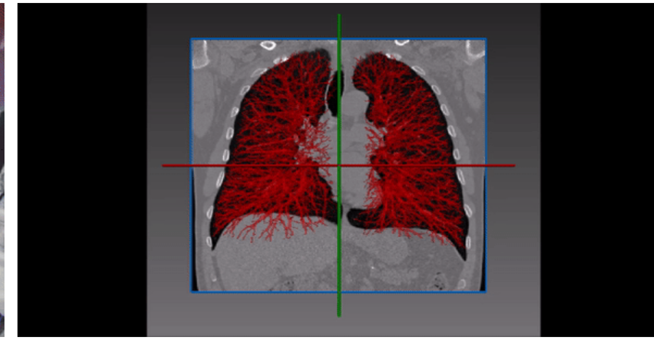
https://tsingqguo.github.io/

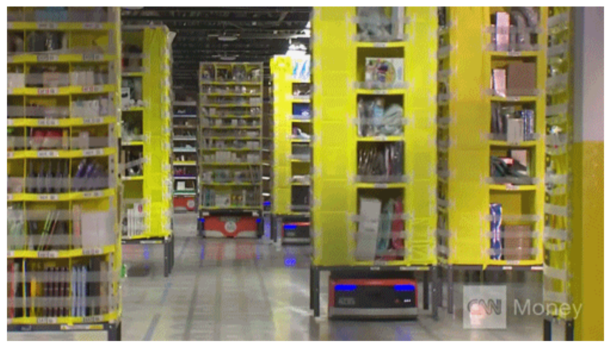
CREATING GROWTH, ENHANCING LIVES

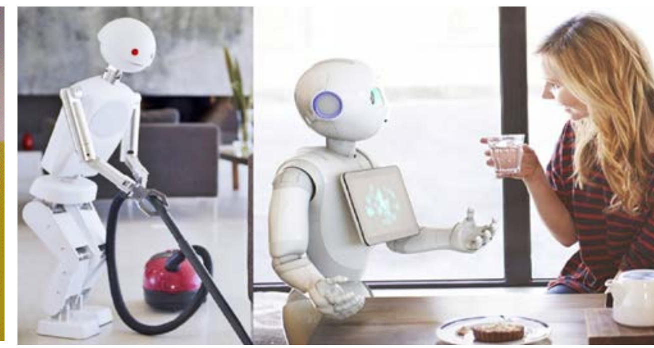
Visual Intelligence Everywhere

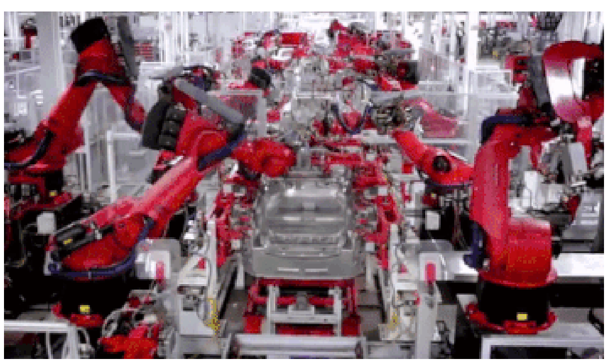
Centre for Frontier AI Research
CFAR



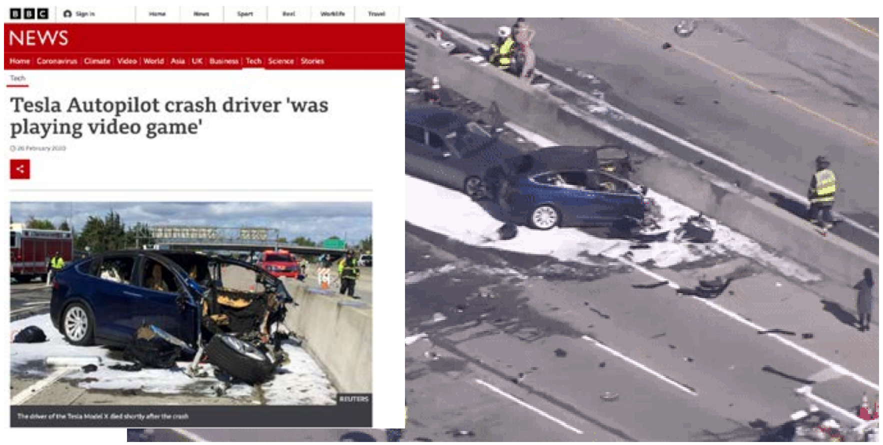


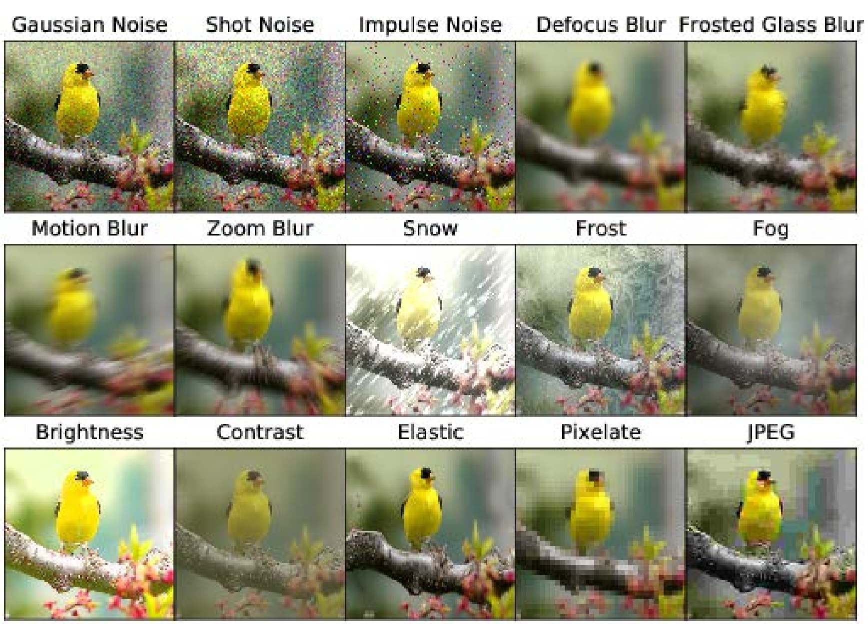






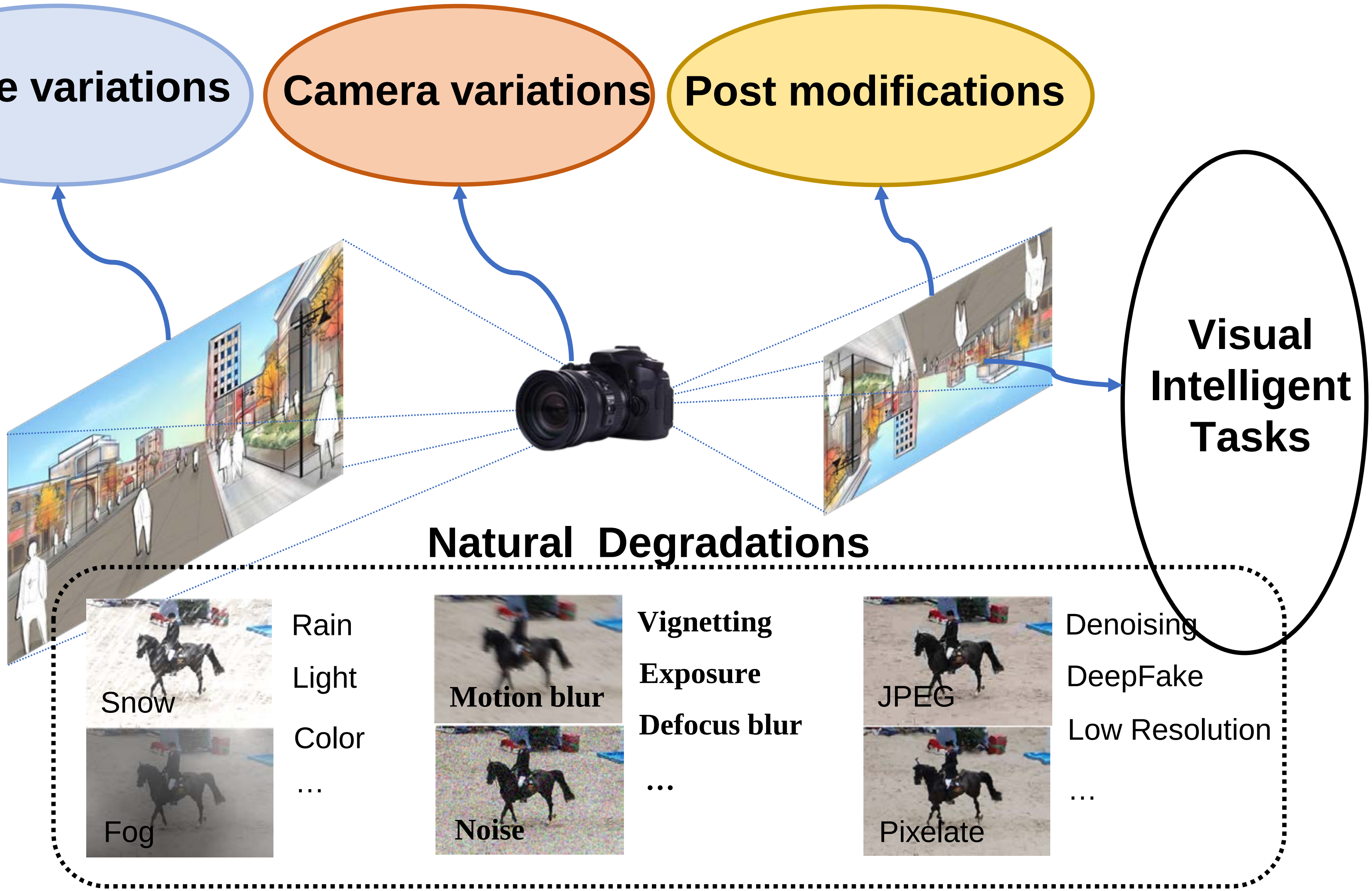
Robustness Issues





Hendrycks D, Dietterich T. Benchmarking neural network robustness to common corruptions and perturbations, In ICLR, 2019.

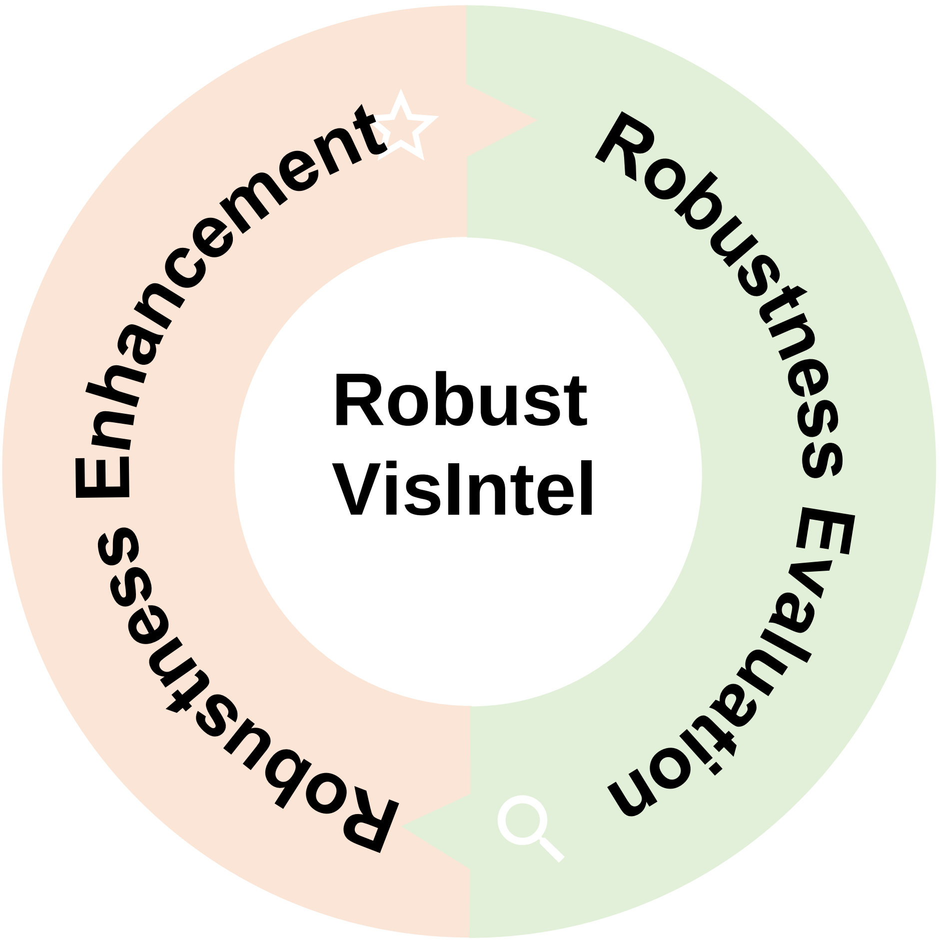
Complex Real-world Scenarios



Research Goals

Centre for Frontier AI Research
CFAR

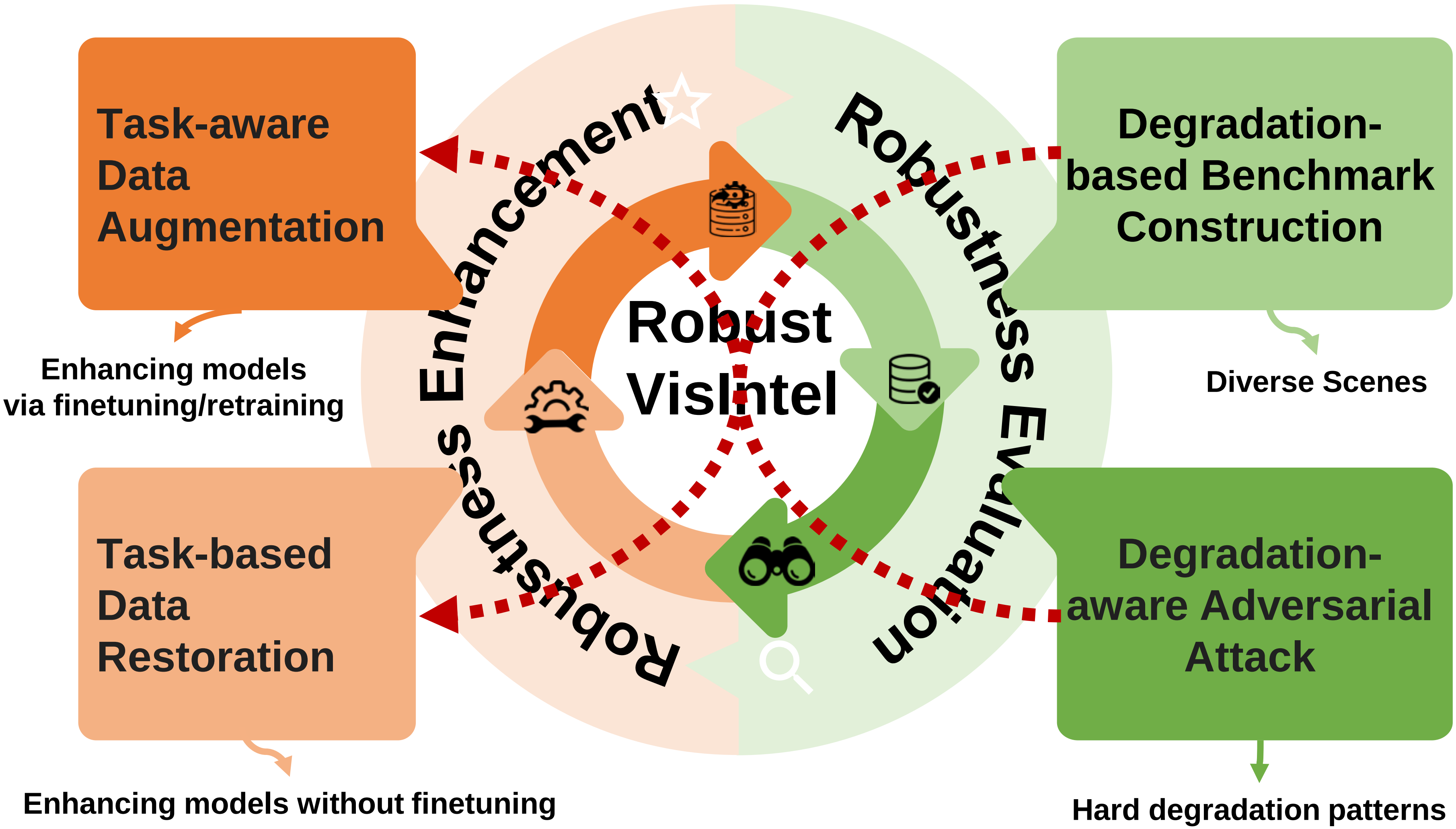
Goal: *Robustness <u>Evaluation</u> and <u>Enhancement</u> of Visual Intelligence to <u>Real-world Degradations:</u>*



Research Goals

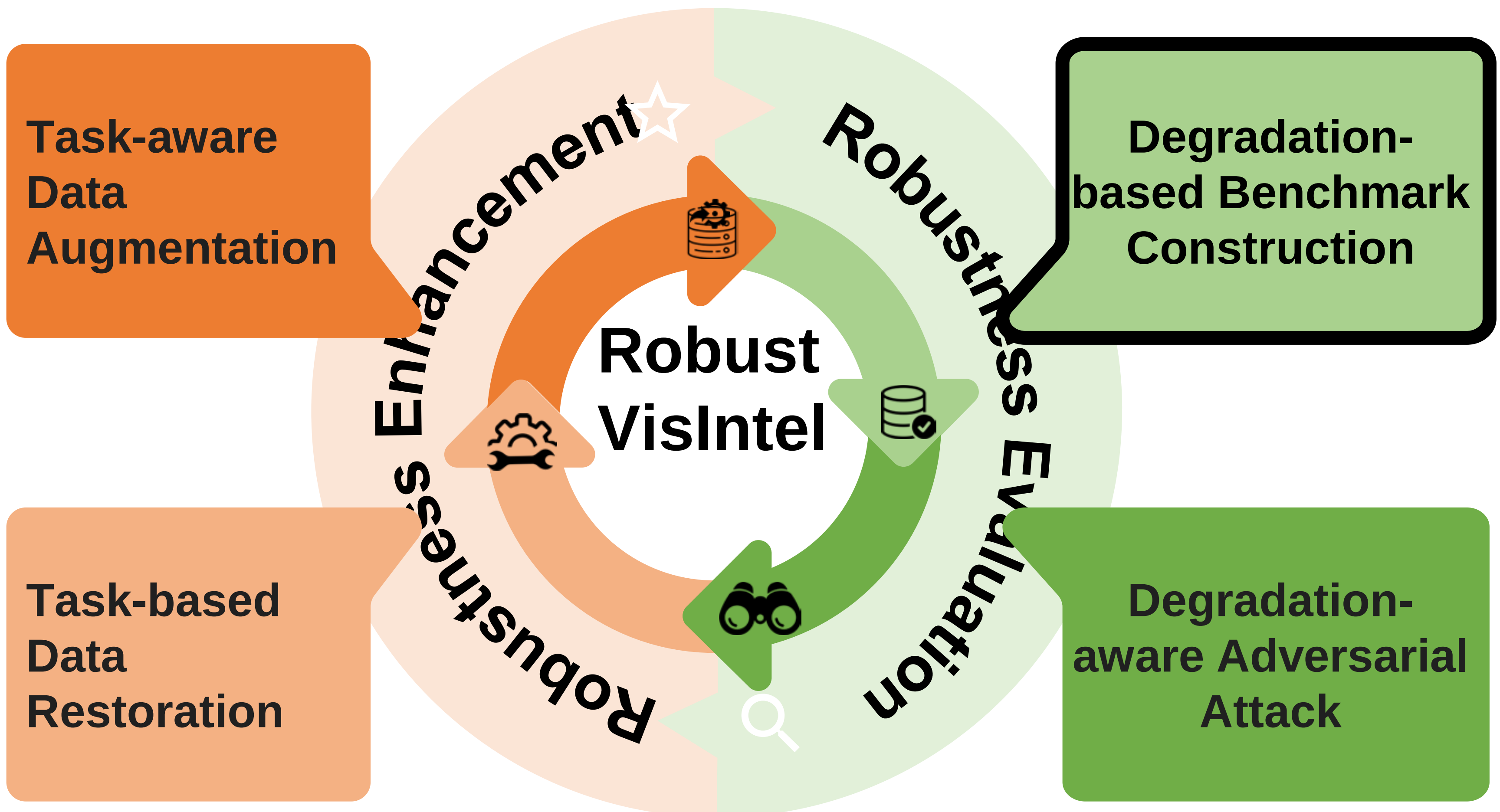
Centre for Frontier AI Research
CFAR

Goal: *Robustness Evaluation and Enhancement of Visual Intelligence to Real-world Degradations:*



Research Goals

Goal: *Robustness <u>Evaluation</u> and <u>Enhancement</u> of Visual Intelligence to <u>Real-world Degradations:</u>*



Robustness Evaluation

Blurred Video Benchmark – An Example (TIP' 21)

➢ Motivation

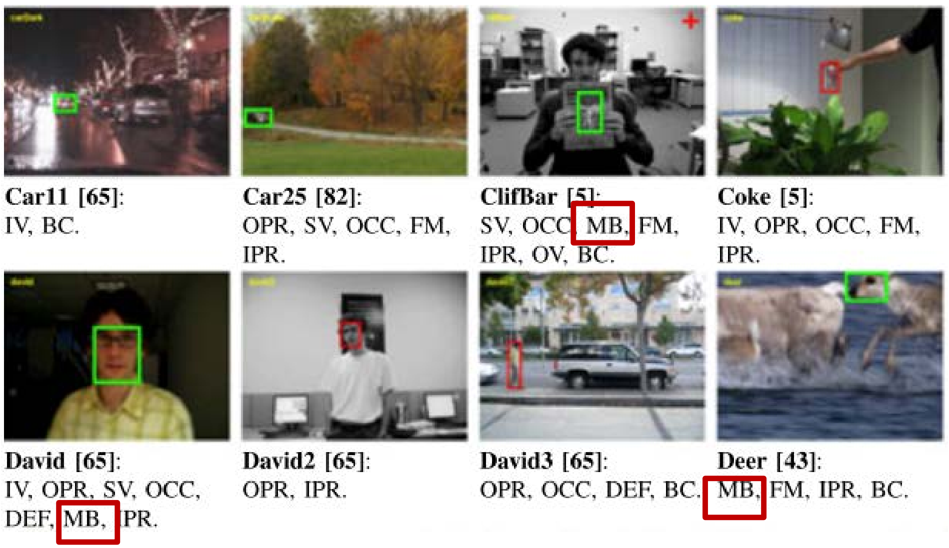
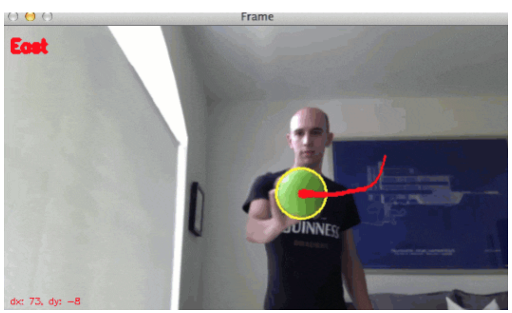


TABLE 2
Annotated Sequence Attributes with the Threshold Values in the Performance Evaluation

Attr	Description
IV	Illumination Variation—The illumination in the target region is significantly changed.
SV	Scale Variation—The ratio of the bounding boxes of the first frame and the current frame is out of range. $[1/t_s, t_s]$, $t_s > 1$ ($t_s = 2$).
OCC	Occlusion—The target is partially or fully occluded.
DEF	Deformation—Non-rigid object deformation.
MB	Motion Blur—The target region is blurred due to the motion of the target or the camera.
FM	Fast Motion—The motion of the ground truth is larger than t_m pixels ($t_m = 20$).
IPR	In-Plane Rotation—The target rotates in the image plane.
OPR	Out-of-Plane Rotation—The target rotates out of the image plane.
OV	Out-of-View—Some portion of the target leaves the view.
BC	Background Clutters—The background near the target has similar color or texture as the target.
LR	Low Resolution—The number of pixels inside the ground-truth bounding box is less than t_r ($t_r = 400$).



- ✗ **Cannot exclude other factors during evaluation**
- ✗ **Cannot evaluate the effects of different blur levels**

Y. Wu, J. Lim, and Ming-Hsuan Yang. Object Tracking Benchmark. In IEEE TPAMI, 2015.
H. Fan, L. Lin, F. Yang, et al. LaSOT: A High-quality Benchmark for Large-scale Single Object Tracking. In CVPR, 2019.
Q. Guo, W. Feng, R. Gao, Y. Liu, and S. Wang. Exploring the Effects of Blur and Deblurring to Visual Object Tracking. In IEEE TIP, 2021

Robustness Evaluation

Blurred Video Benchmark – An Example (TIP' 21)

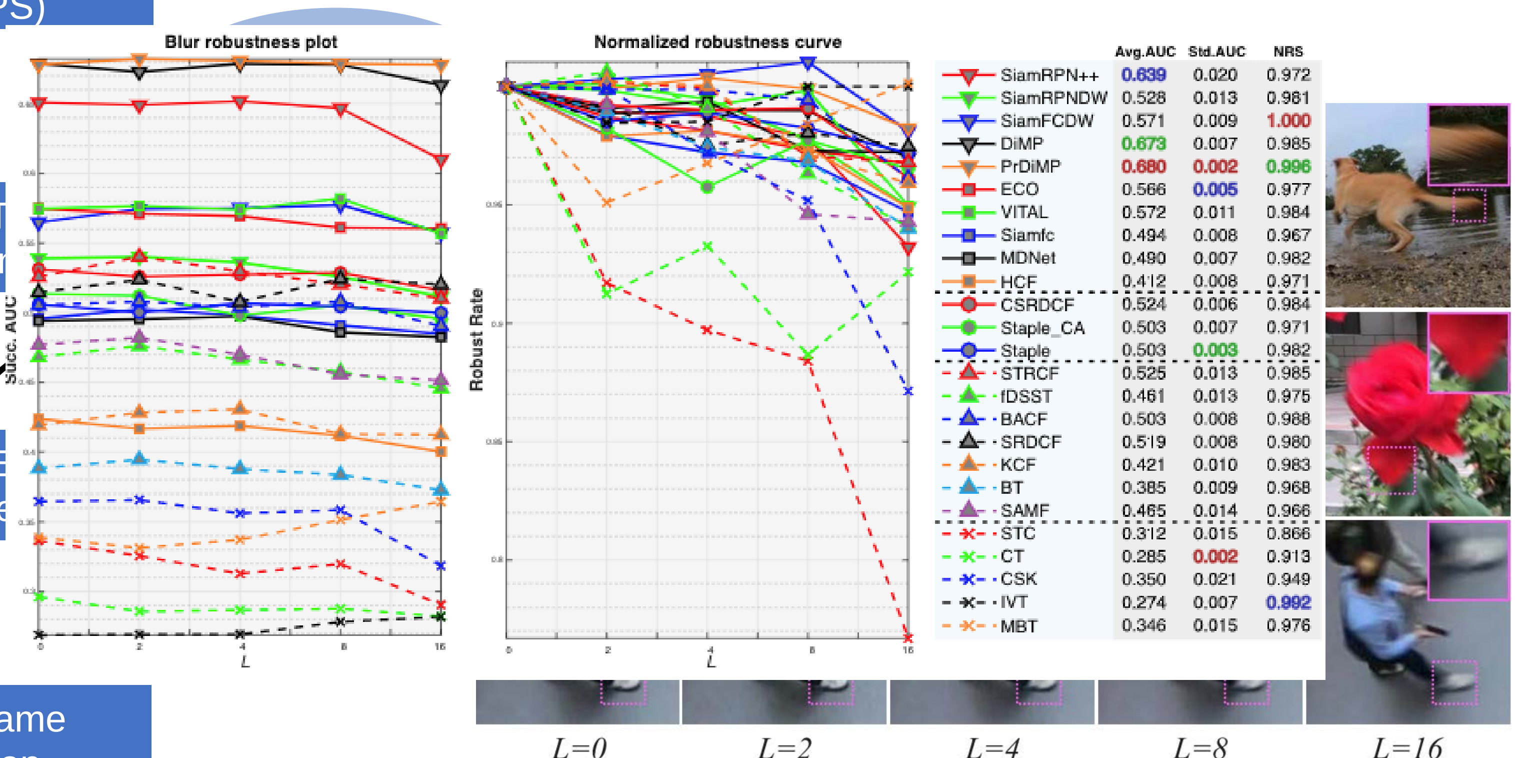
- **Construction strategies**

High frame-rate video collection (240FPS)

Ground T... Labelli...

Multi-level B... Video Gene...

Initial Frame Selection



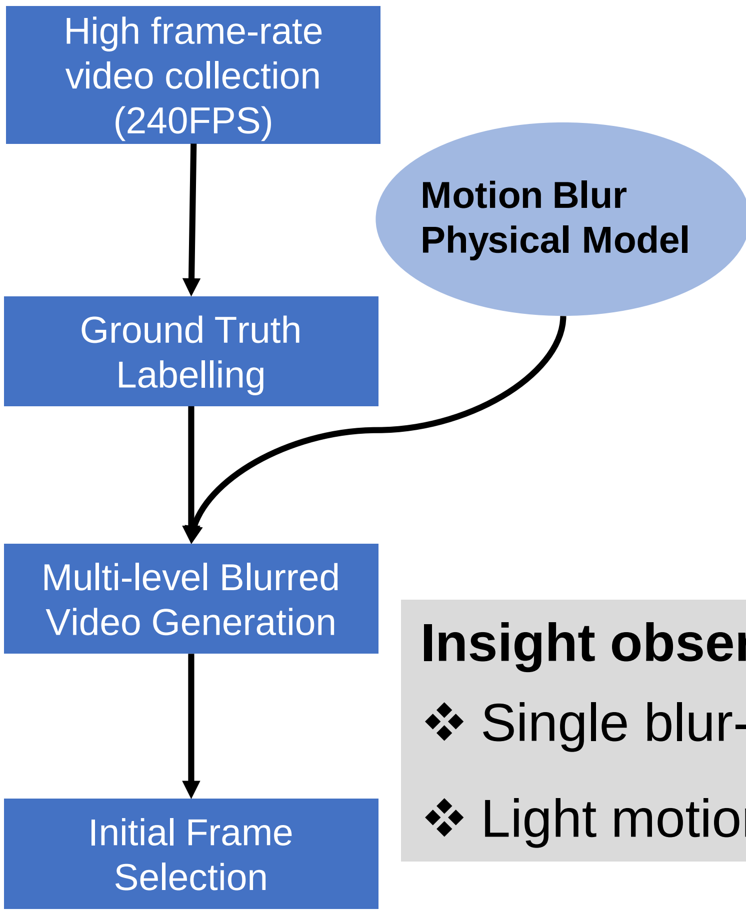
	Avg.AUC	Std.AUC	NRS
SiamRPN++	0.639	0.020	0.972
SiamRPNDW	0.528	0.013	0.981
SiamFCDW	0.571	0.009	1.000
DiMP	0.673	0.007	0.985
PrDiMP	0.680	0.002	0.996
ECO	0.566	0.005	0.977
VITAL	0.572	0.011	0.984
Siamfc	0.494	0.008	0.967
MDNet	0.490	0.007	0.982
HCF	0.412	0.008	0.971
CSRDCF	0.524	0.006	0.984
Staple_CA	0.503	0.007	0.971
Staple	0.503	0.003	0.982
STRCF	0.525	0.013	0.985
fDSST	0.461	0.013	0.975
BACF	0.503	0.008	0.988
SRDCF	0.519	0.008	0.980
KCF	0.421	0.010	0.983
BT	0.385	0.009	0.968
SAMF	0.465	0.014	0.966
STC	0.312	0.015	0.866
CT	0.285	0.002	0.913
CSK	0.350	0.021	0.949
IVT	0.274	0.007	0.992
MBT	0.346	0.015	0.976

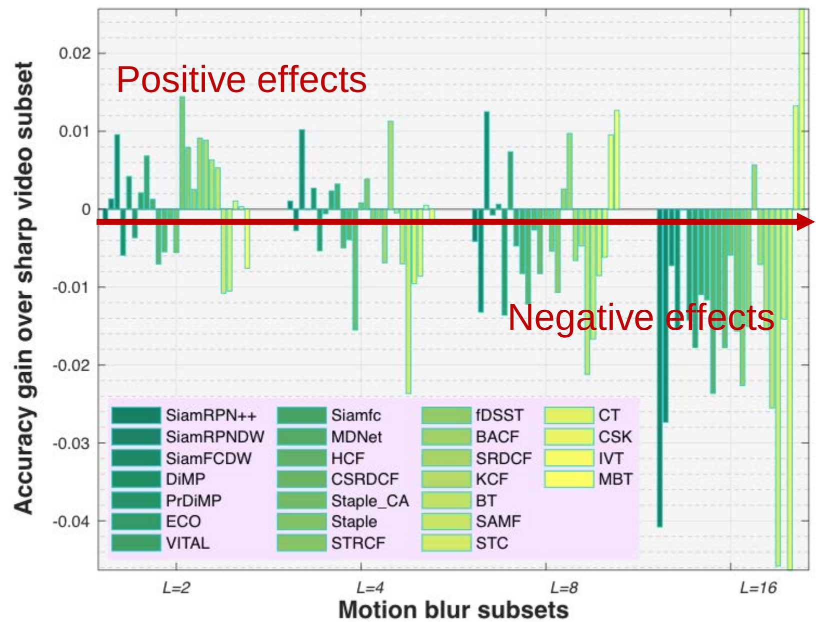
Q. Guo, W. Feng, R. Gao, Y. Liu, and S. Wang. Exploring the Effects of Blur and Deblurring to Visual Object Tracking. In IEEE TIP, 2021

Robustness Evaluation

Blurred Video Benchmark – An Example (TIP' 21)

➢ **Some insight observations**





Insight observations:

❖ Single blur-level videos are not enough.

❖ Light motion blur is helpful but heavy blur is harmful.

Q. Guo, W. Feng, R. Gao, Y. Liu, and S. Wang. Exploring the Effects of Blur and Deblurring to Visual Object Tracking. In IEEE TIP, 2021

Robustness Evaluation

Blurred Video Benchmark – An Example (TIP' 21)

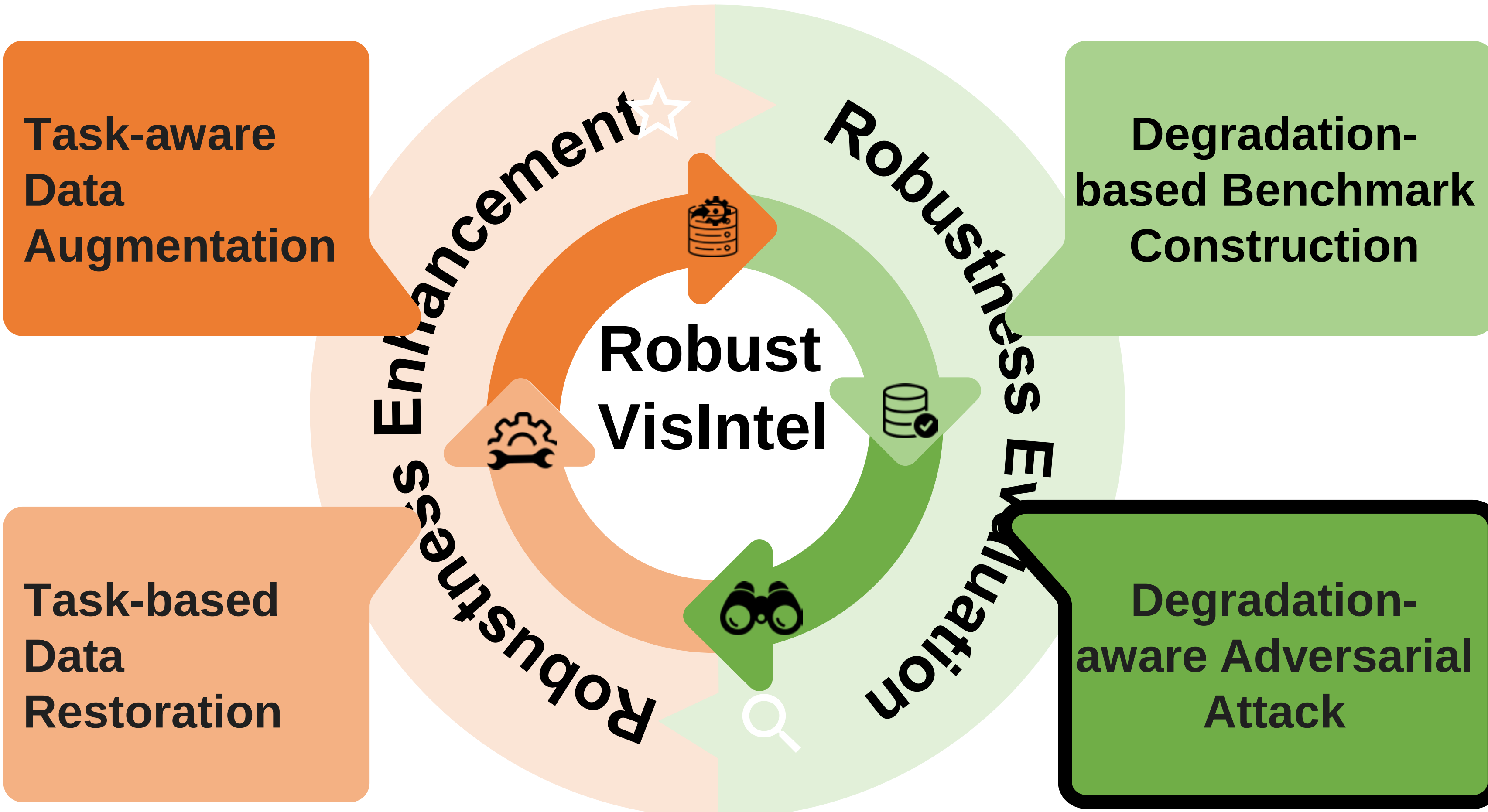
➢ **Limitations**

✗ **Cannot cover the diverse and hard blur patterns.**

Q. Guo, W. Feng, R. Gao, Y. Liu, and S. Wang. Exploring the Effects of Blur and Deblurring to Visual Object Tracking. In IEEE TIP, 2021
Y. Wu, J. Lim, and Ming-Hsuan Yang. Object Tracking Benchmark. In IEEE TPAMI, 2015.
H. Fan, L. Lin, F. Yang, et al. LaSOT: A High-quality Benchmark for Large-scale Single Object Tracking. In CVPR, 2019.

Robustness Evaluation

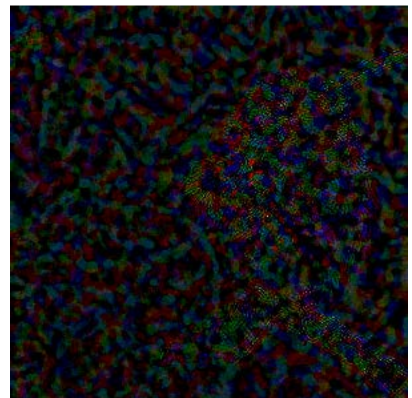
Goal: *Robustness Evaluation and Enhancement of Visual Intelligence to Real-world Degradations:*



Robustness Evaluation

Centre for Frontier AI Research
CFAR

Additive-Perturbation Adversarial Attack

$\mathbf{X}^{\mathrm{real}}$  + δ  = 

Incv3: Bird

Incv3: Dog

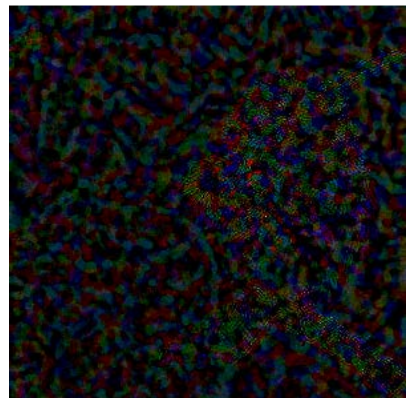
$$\arg\max_{\delta} J(\mathbf{X}^{\mathrm{real}} + \delta, y) \;\; \text{subject to} \;\; \|\delta\|_{\mathrm{p}} \leq \epsilon$$

✓ **Noise-like adversarial perturbation cannot represent diverse natural degradations in the real world.**

.Ian J Goodfellow, Jonathon Shlens, and Christian Szegedy. Explaining and harnessing adversarial examples. In ICLR, 2015.
Alexey Kurakin, Ian J Goodfellow, and Samy Bengio. Adversarial examples in the physical world. In ICLRW, 2017.
Y. Dong, T. Pang, H. Su, and J. Zhu. Evading defenses to transferable adversarial examples by translation-invariant attacks. In CVPR, 2019.
Q. Guo, X. Xie, F. Juefei-Xu, L. Ma, Z. Li, W. Xue, W. Feng, and Y. Liu. Spark: Spatial-aware online incremental attack against visual tracking. In ECCV, 2020

Robustness Evaluation

General Adversarial Attack

$O($  $\mathbf{X}^{\mathrm{real}}$ $, +$  δ $) =$ 

Incv3: Bird

Incv3: Dog

$$\arg\max_{\delta} J(O(\mathbf{X}^{\mathrm{real}}, \delta), y) \text{ subject to } \mathrm{regular}(\delta)$$

$$\arg\max_{\delta} J(\mathbf{X}^{\mathrm{real}} + \delta, y) \text{ subject to } \|\delta\|_p \leq \epsilon$$

✓ **Turning the additive operation to nature degradation-based operations.**

Robustness Evaluation

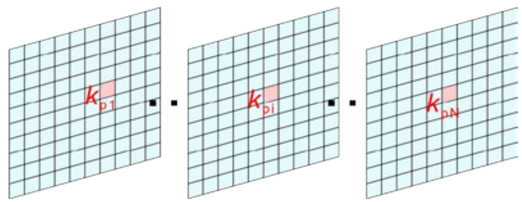
Adversarial Blur Attack（NeurIPS’ 20）

Blur(

$\mathbf{X}^{\text{real}}$

Incv3: Bird

,



Pixel-wise blur kernels

) =

Incv3: Car

$$\mathcal{K} = \{\mathbf{k}_p | \forall p \text{ in } \mathbf{X}^{\text{real}}\}$$

$$\arg\max_{\mathcal{K}} J(\{\sum_{q \in \mathcal{N}(p)} \mathbf{X}_q^{\text{real}} k_{pq}\}, y)$$

$$\text{subject to } \forall p, \|\mathbf{k}_p\|_0 \leq \epsilon,$$

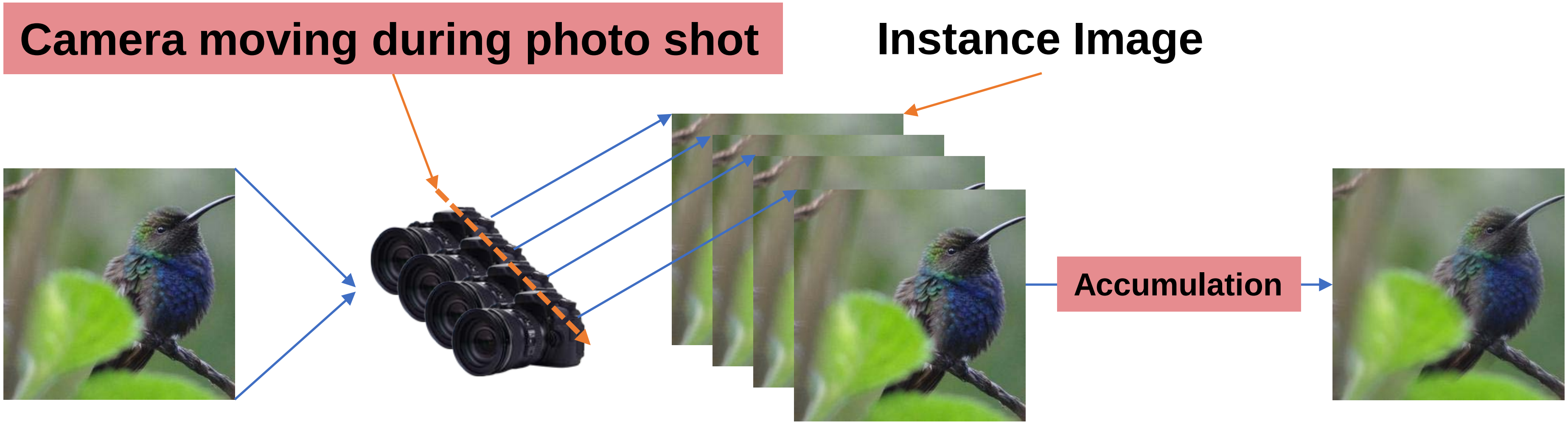
$$\max(\mathbf{k}_p) = k_{pp}, \sum_{q \in \mathcal{N}(p)} k_{pq} = 1,$$

Robustness Evaluation

Centre for Frontier AI Research
CFAR

Adversarial Blur Attack（NeurIPS’ 20）

➢ **Physical model of motion blur**

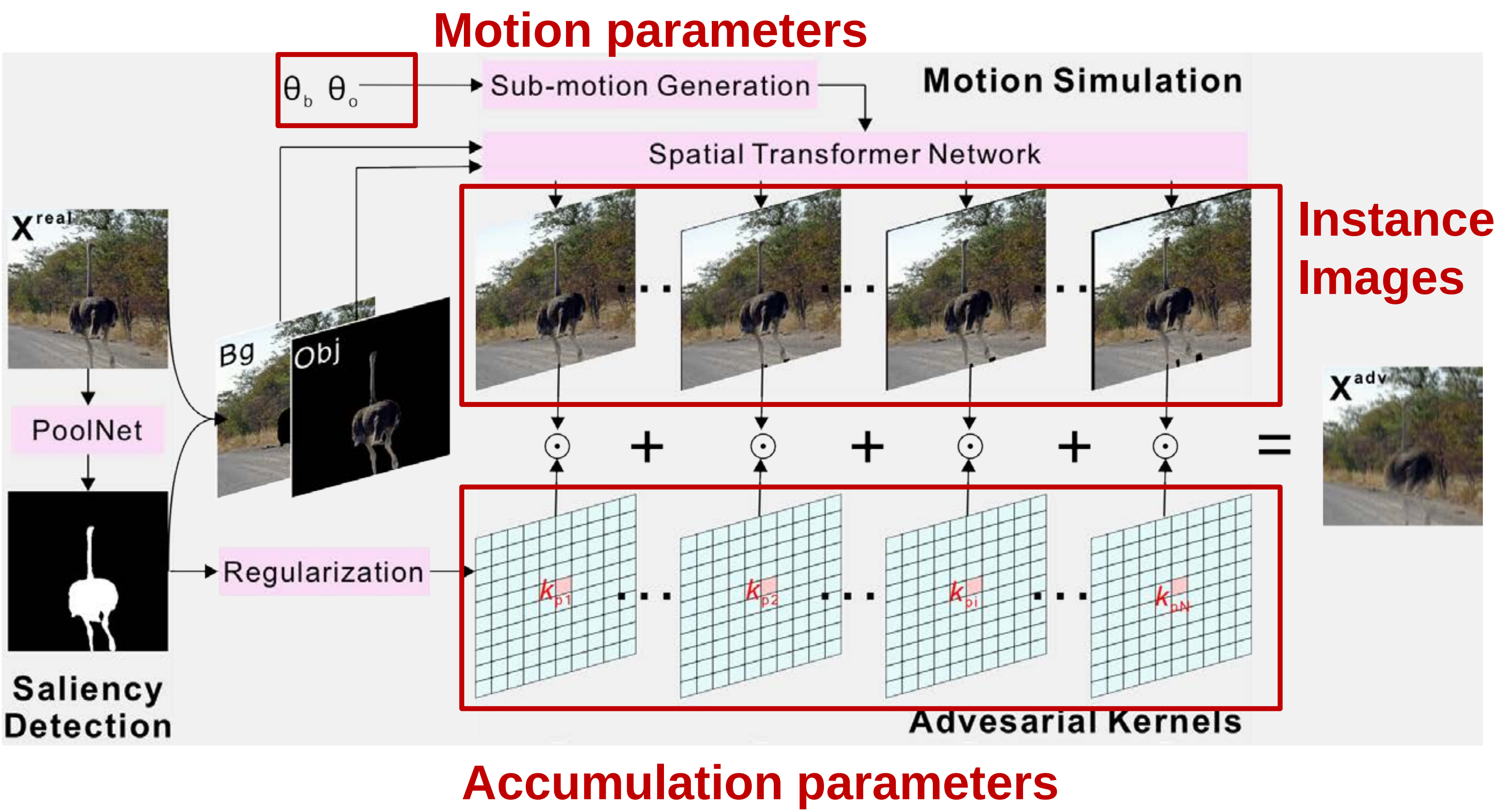


✓ **Pattern of motion blur is mainly decided by the motion of the camera/object and the accumulation process.**

Robustness Evaluation

Adversarial Blur Attack（NeurIPS’ 20）

➢ **Digital Simulation of motion blur**

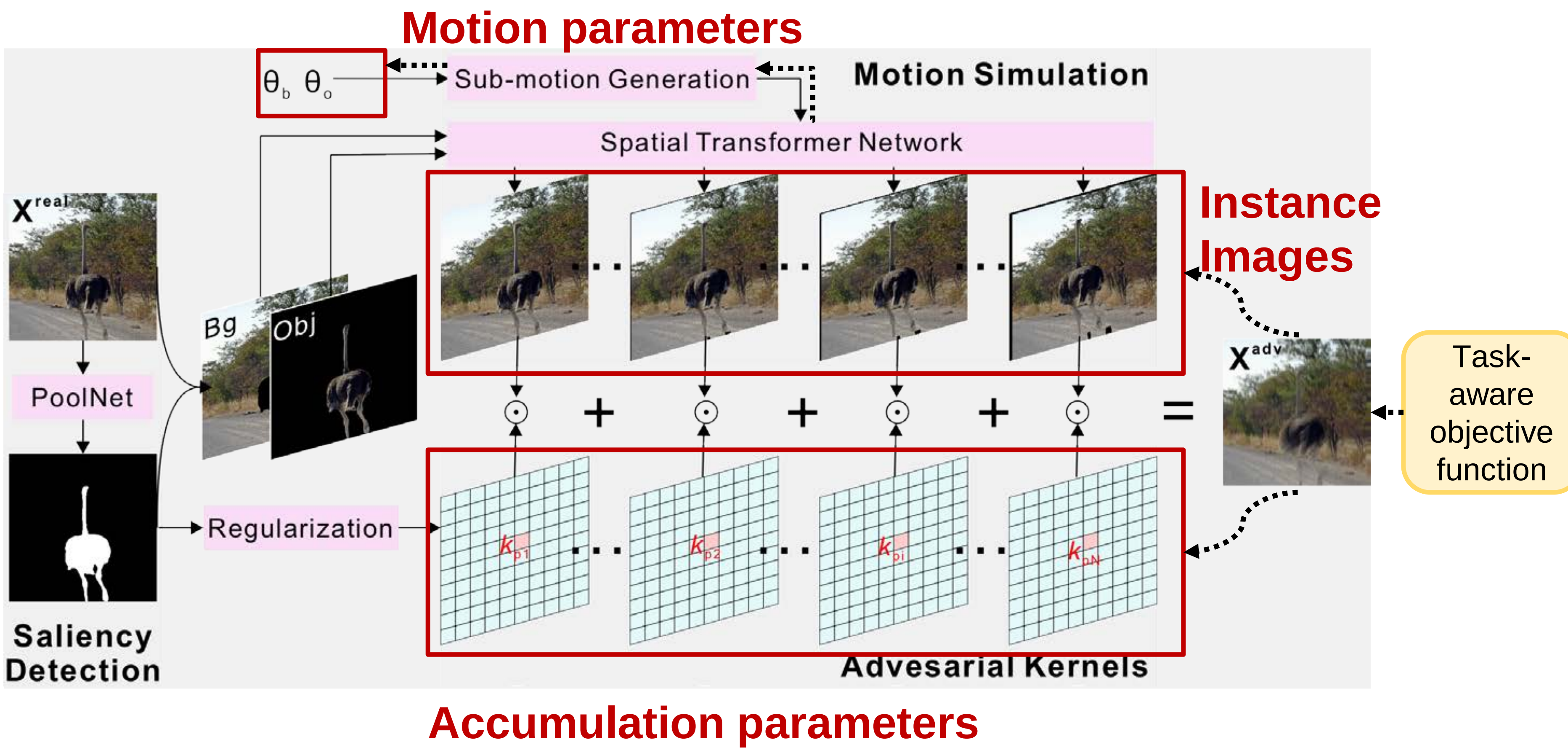


Q. Guo, F. Juefei-Xu, X. Xie, et. al. **Watch out! Motion is Blurring the Vision of Your Deep Neural Networks. NeurIPS 2020.**

Robustness Evaluation

Adversarial Blur Attack（NeurIPS' 20）

➢ **Adversarial motion blur**

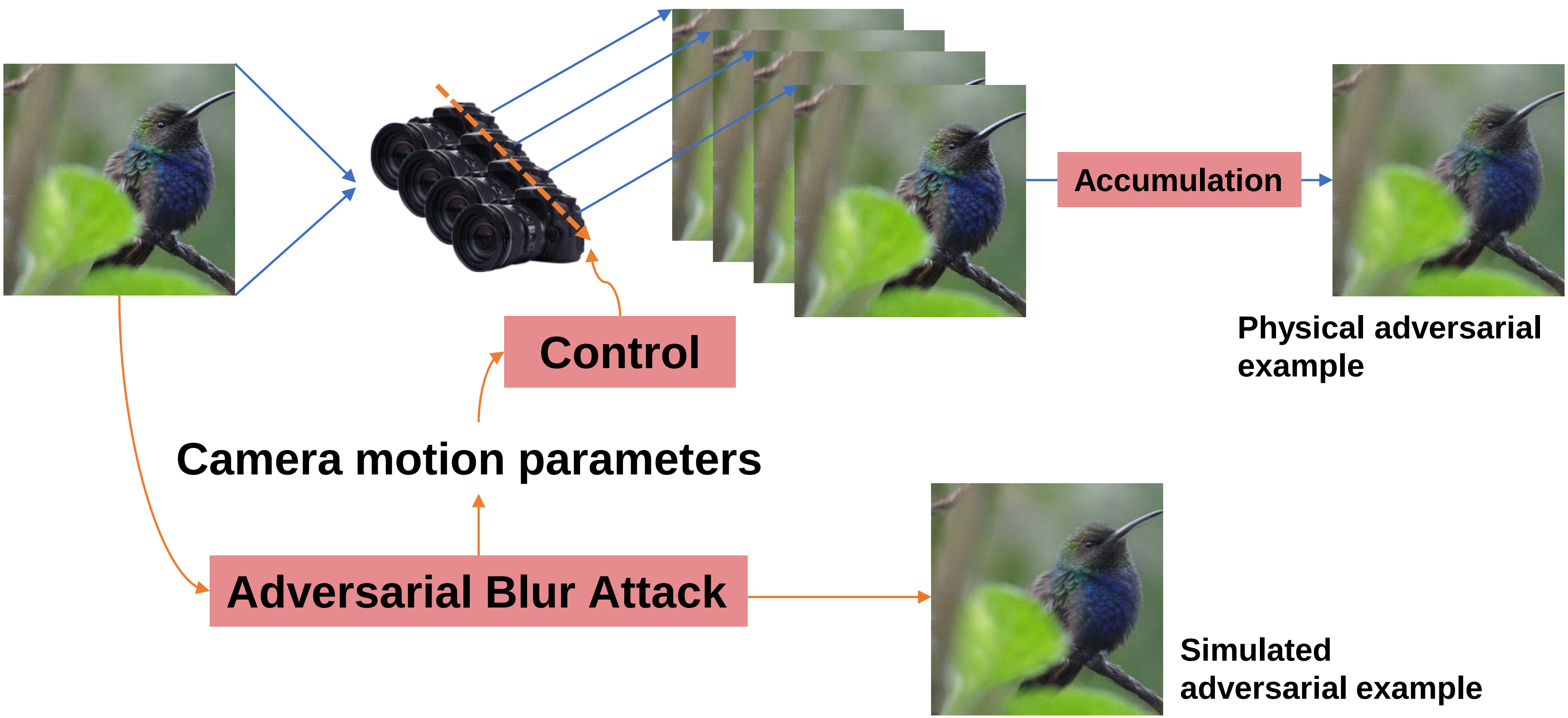


Q. Guo, F. Juefei-Xu, X. Xie, et. al. **Watch out! Motion is Blurring the Vision of Your Deep Neural Networks. NeurIPS 2020.**

Robustness Evaluation

Adversarial Blur Attack（NeurIPS’ 20）

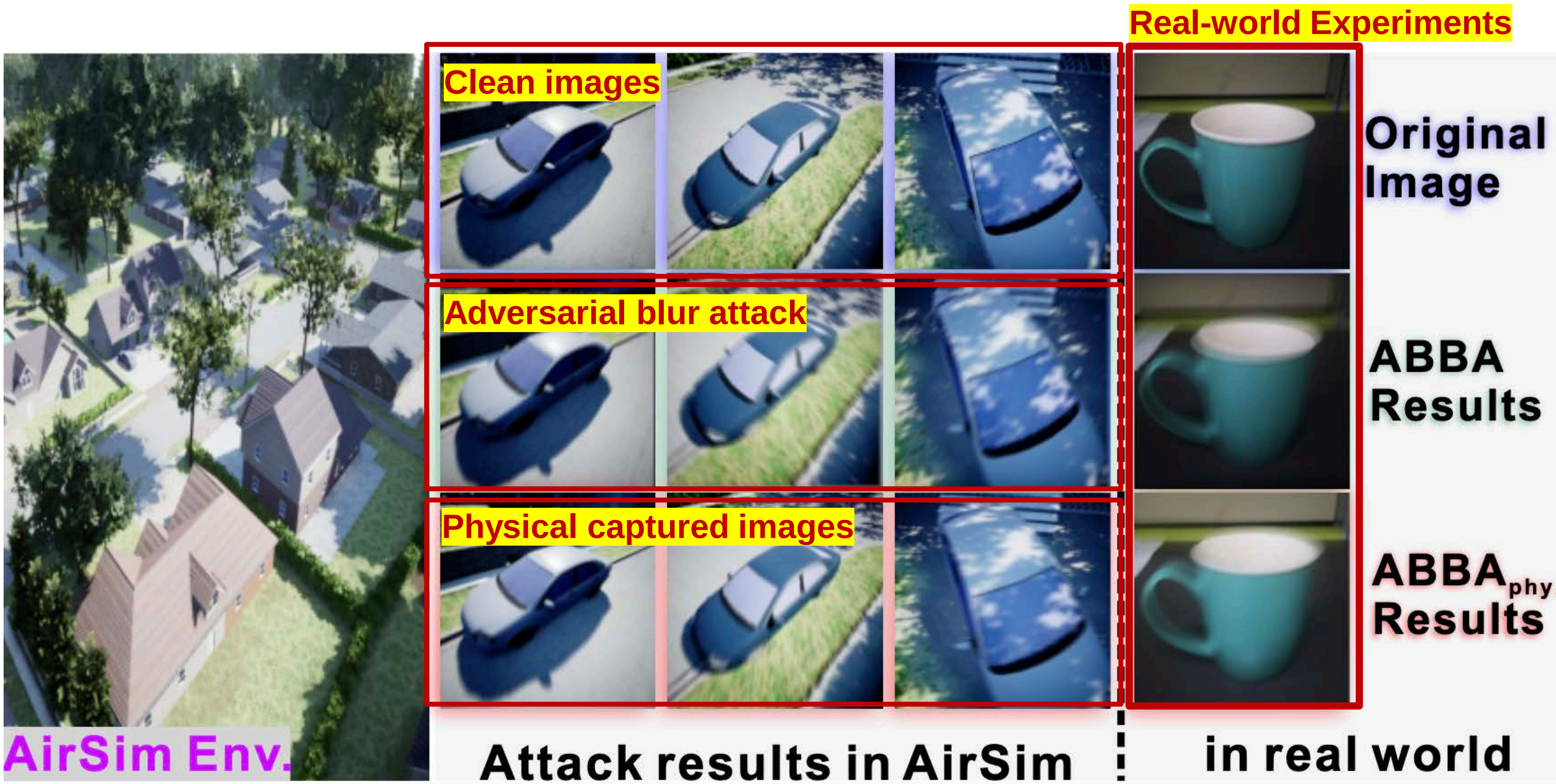
➢ **Physical Adversarial Blur Attack**



Robustness Evaluation

Adversarial Blur Attack（NeurIPS' 20）

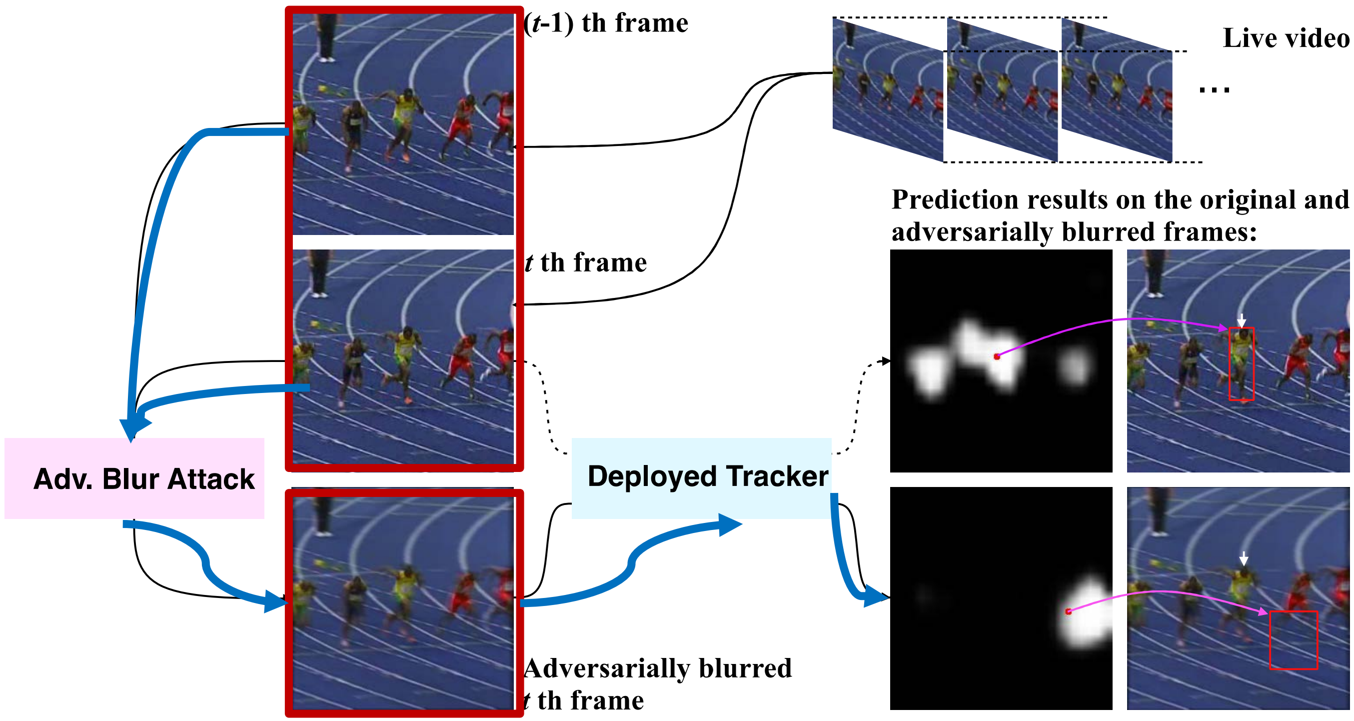
- Physical Adversarial Blur Attack



Q. Guo, F. Juefei-Xu, X. Xie, et. al. **Watch out! Motion is Blurring the Vision of Your Deep Neural Networks. NeurIPS 2020.**

Robustness Evaluation

Adversarial Blur Attack against Tracking（ICCV’ 21）

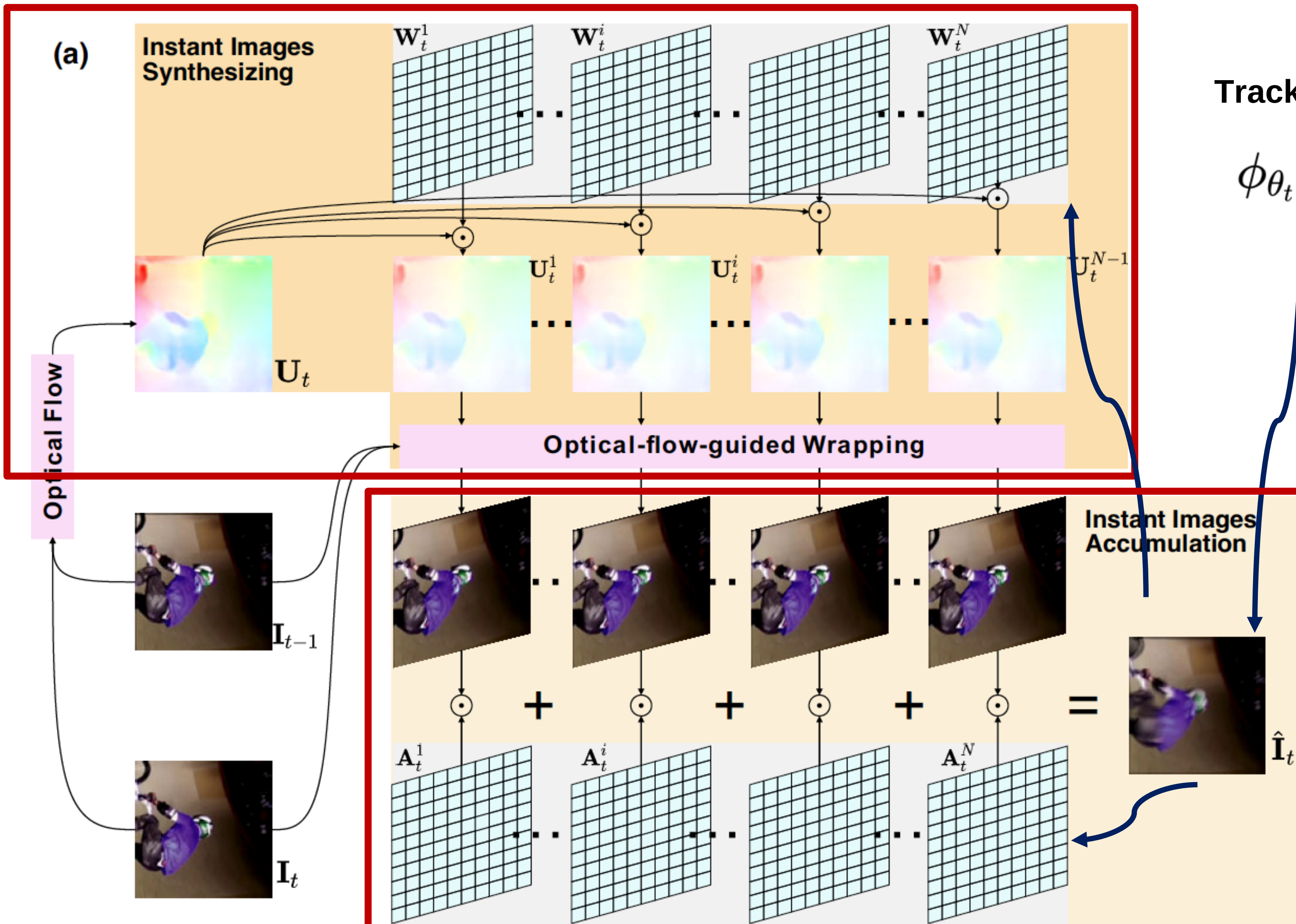


- ✓ **How to make tuned motion blur keep realistic blur appearance?**
- ✓ **How to realize efficient adversarial blur attack to adapt the real-time trackers?**

Q. Guo, Z. Chen, F. Juefei-Xu, et. al. Learning to Adversarially Blur Visual Object Tracking. in **ICCV 2021.**

Robustness Evaluation

Adversarial Blur Attack against Tracking（ICCV’ 21）



Q. Guo, Z. Chen, F. Juefei-Xu, et. al. Learning to Adversarially Blur Visual Object Tracking. in **ICCV 2021.**

Robustness Evaluation

Adversarial Blur Attack against Tracking（ICCV’ 21）

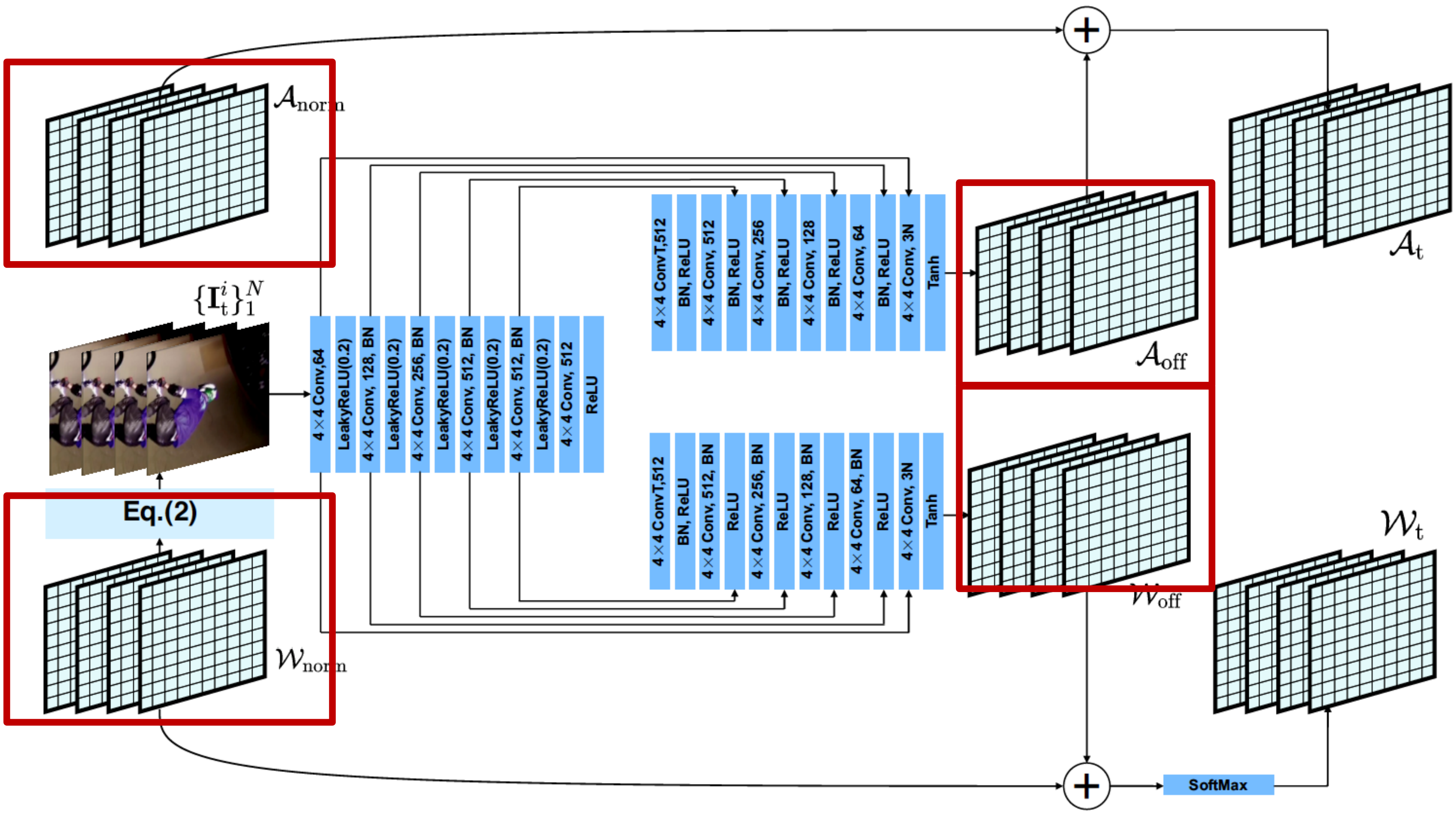


Figure 3: Architecture of JAMANet.

Q. Guo, Z. Chen, F. Juefei-Xu, et. al. Learning to Adversarially Blur Visual Object Tracking. in **ICCV 2021.**

Robustness Evaluation

Adversarial Blur Attack against Tracking（ICCV’ 21）

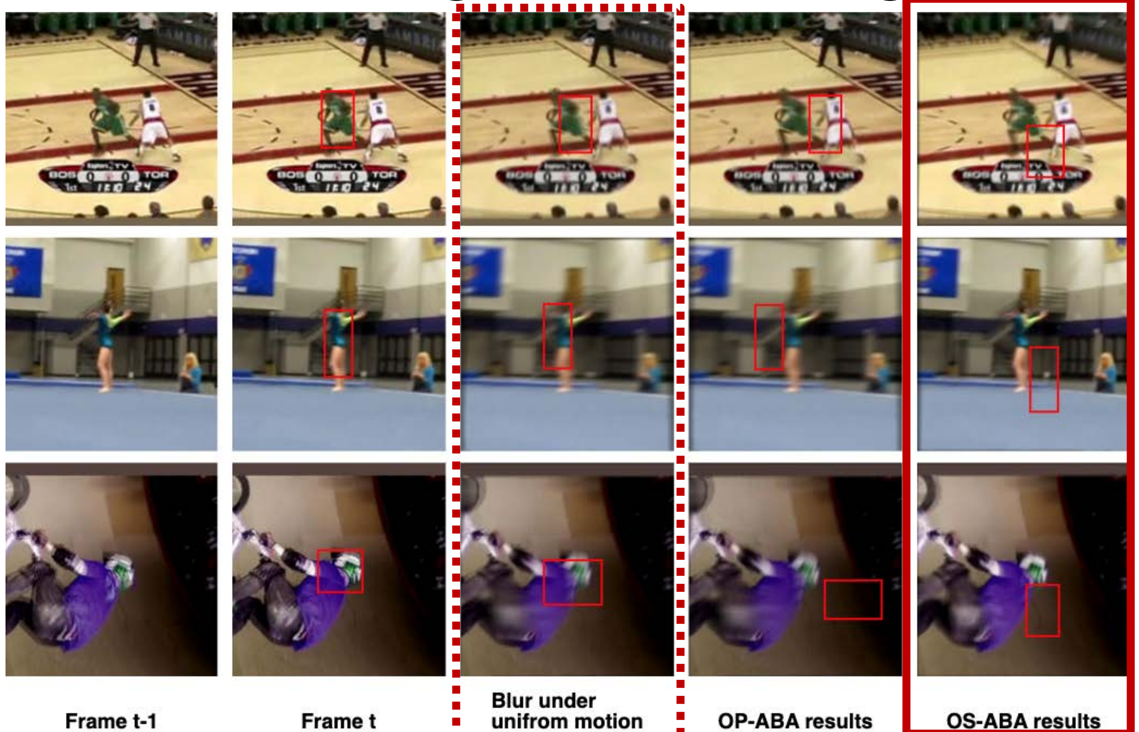


Table 4: Effects of $\mathcal{W}_t$ and $\mathcal{A}_t$ to OP-ABA and OS-ABA by attacking SiamRPN++(ResNet50) on OTB100. The best results are highlighted by red color.

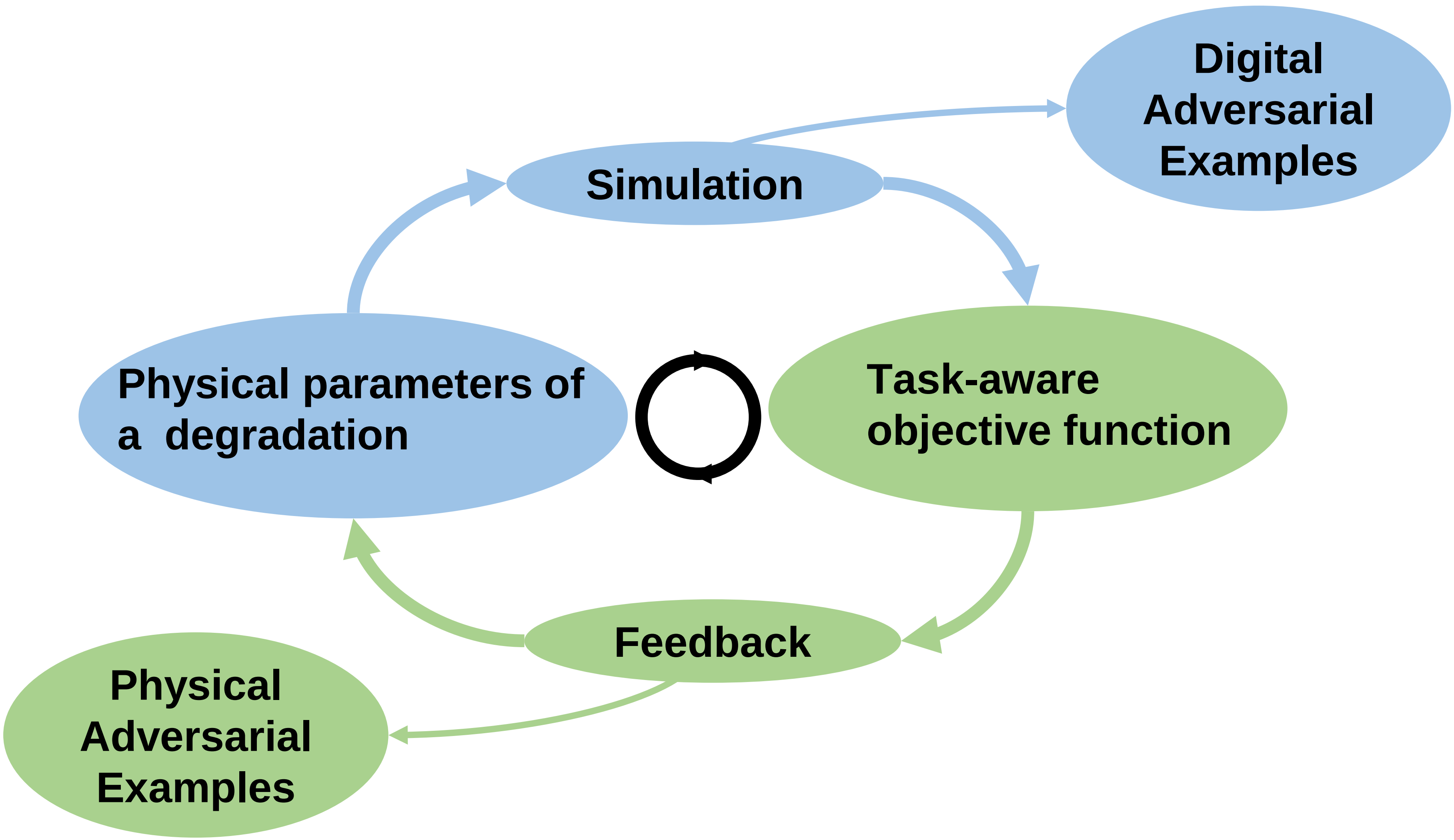
Attackers	Succ. Rate	Succ. Drop ↑	Prec.	Prec. Drop ↑
Original	66.5	0.0	87.8	0.0
Norm-Blur	65.3	1.2	86.2	1.6
OP-ABA w/o $\mathcal{A}_t$	51.5	15.0	67.6	20.2
OP-ABA w/o $\mathcal{W}_t$	40.9	25.6	53.4	34.4
OP-ABA	35,3	**31.2**	46.1	**41.7**
OS-ABA w/o $\mathcal{A}_t$	61.0	5.5	80.8	7.0
OS-ABA w/o $\mathcal{W}_t$	41.6	24.9	58.3	29.5
OS-ABA	38.4	**28.1**	55.3	**32.5**

Q. Guo, Z. Chen, F. Juefei-Xu, et. al. Learning to Adversarially Blur Visual Object Tracking. in **ICCV 2021.**

Robustness Evaluation

Degradation-aware Adversarial Attack

- Generalizing adversarial blur attack to other degradations



Robustness Evaluation

Centre for Frontier AI Research
CFAR

Solution1: Degradation-aware Adversarial Attack

Adversarial **Deformation/Rain/Fog/Relighting** Attack (ACMMM'20, IEEE TIFS & TMM)

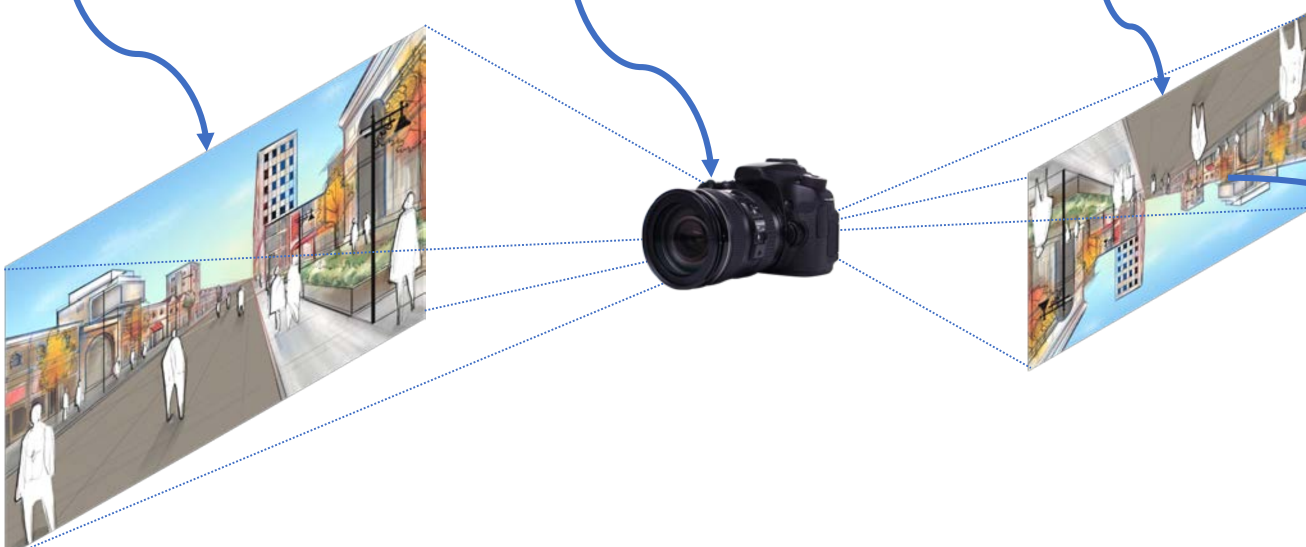
Adversarial **Noise/Vignetting/Exposure** Attack (ECCV'20, IJCAI'21, CVPR'22)

Adversarial **Denoising/DeID** Attack (TMM' 21)

Scene variations

Camera variations

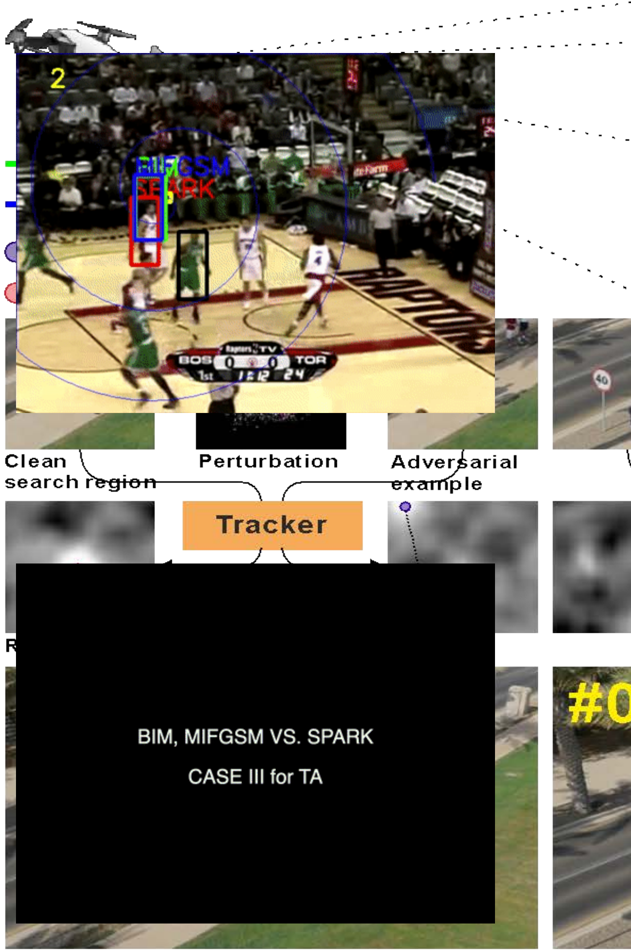
Post modifications

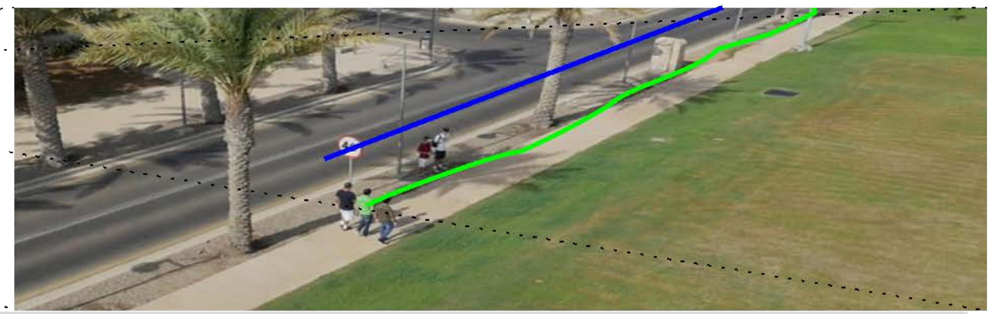


Visual Intelligent Tasks

Robustness Evaluation

SPARK - Effects of noise to tracking (ECCV’20)





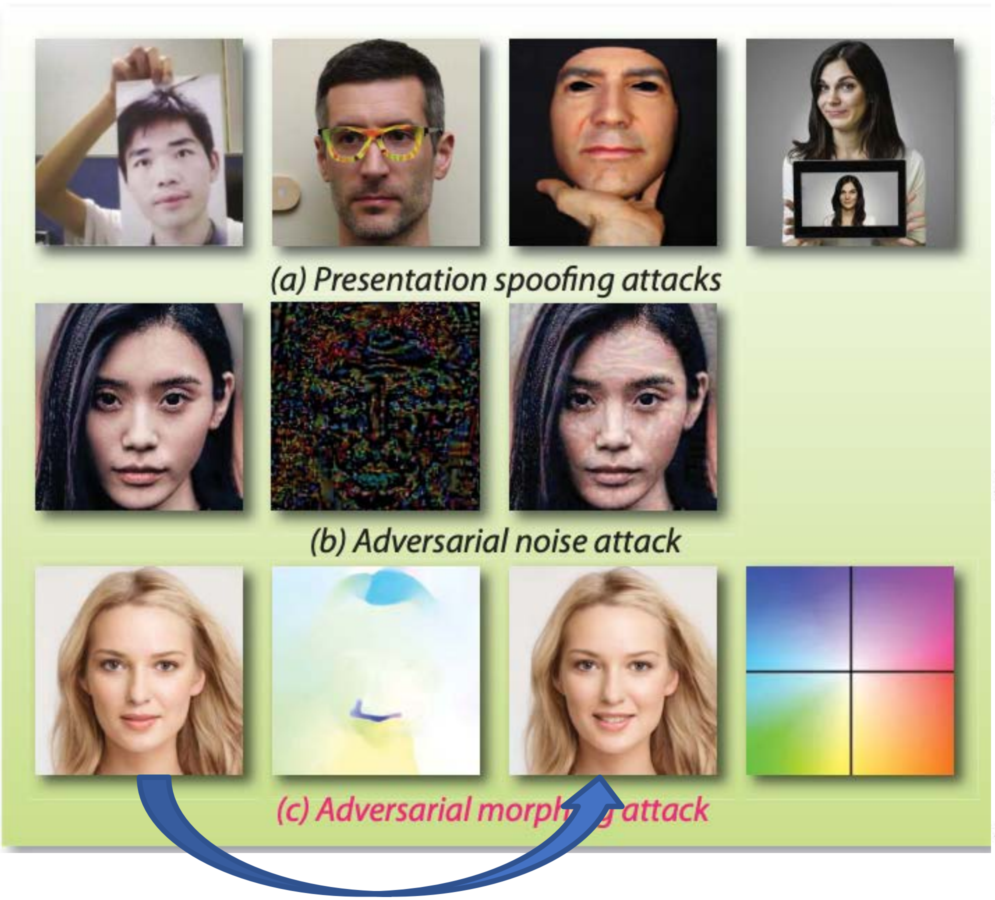
Main Challenges:

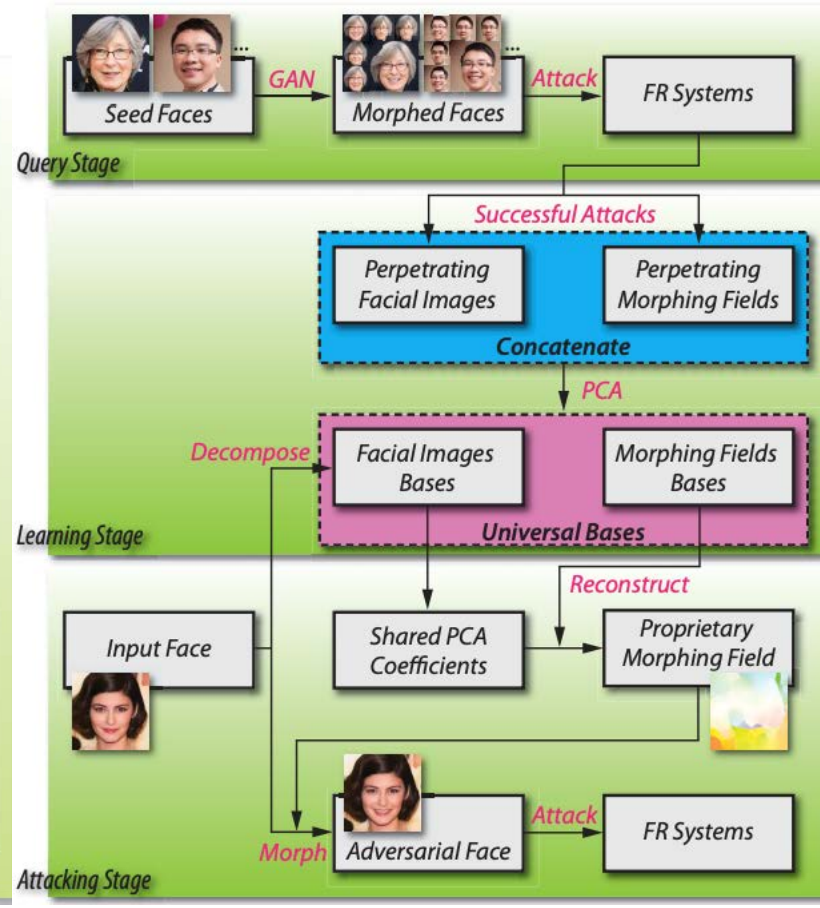
- ✓ Tracking focuses on the object trajectory instead of category.
- ✓ Tracking requires the attacking to be enough efficient.

Q. Guo, X. Xie, F. Juefei-Xu, et. al. **SPARK: Spatial-aware Online Incremental Attack Against Visual Tracking. ECCV 2020.**

Robustness Evaluation

Amora- Effects of deformation to FR (ACM-MM’20)





Run Wang, Felix Juefei-Xu, **Qing Guo*,** Yihao Huang, Xiaofei Xie, Lei Ma, and Yang Liu. **Amora: Black-box Adversarial Morphing Attack.** ACM-MM,

Robustness Evaluation

AVA - Effects of vignetting to recognition (IJCAI'21)

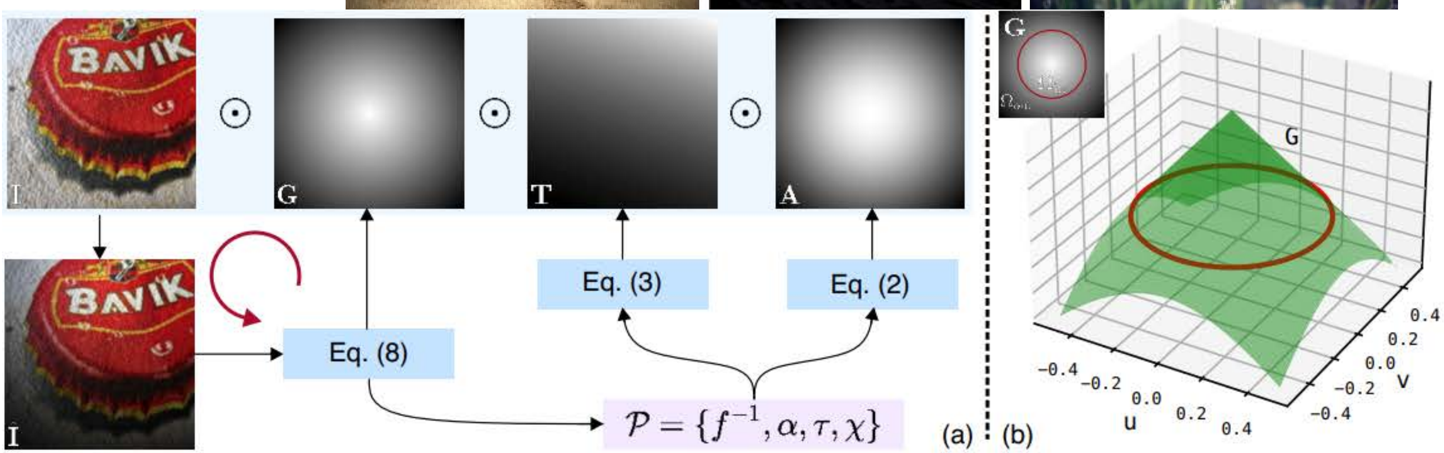
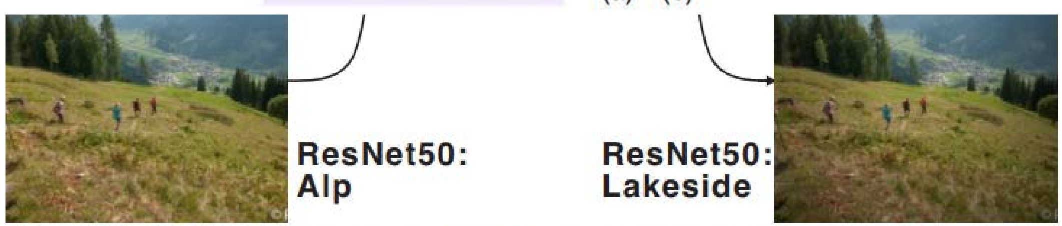


Figure 2: (a) shows the whole process of RA-AVA. (b) shows the 3D surface of the initialized **G**. The red line is the curve splitting the image to 2 parts, *i.e.*, Ω_{in} and Ω_{out}.



(b) Adversarial Vignetting Examples

Binyu Tian, Felix Juefei-Xu, **Qing Guo***, et. al. **AVA: Adversarial Vignetting Attack against Visual Recognition**. **IJCAI 2021.**

Robustness Evaluation

Effects of exposure and noise to CoSOD (CVPR'22)

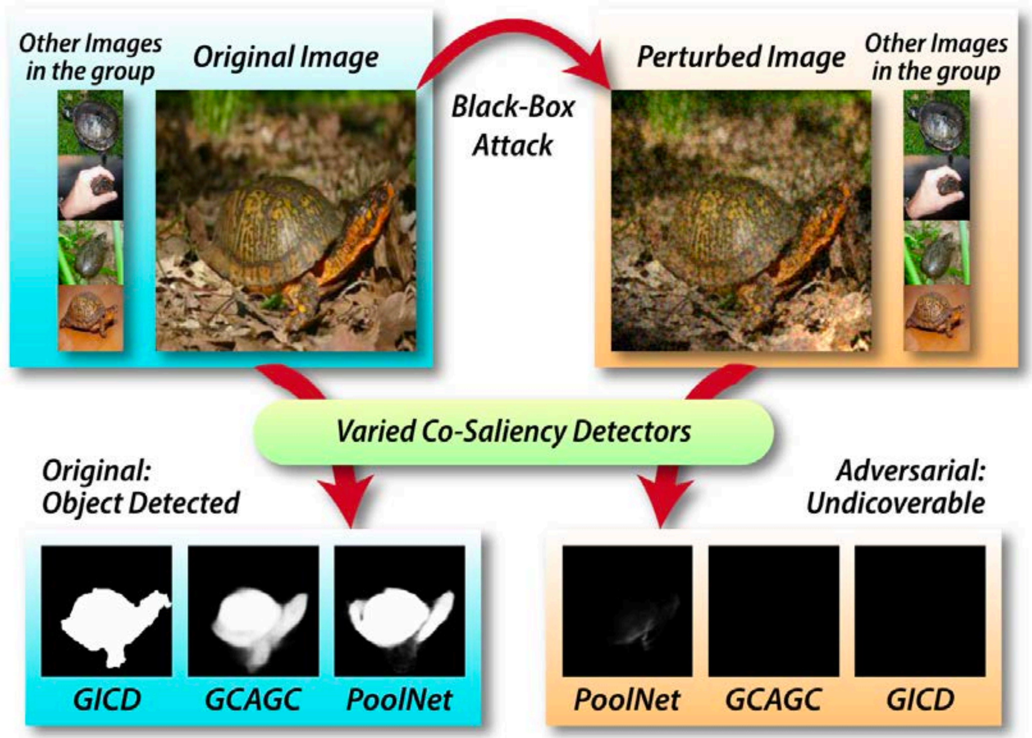


Figure 1: Overall of the novel problem and our solution. We expect the perturbed image to be undiscoverable in an even dynamically growing group of images across multiple CoSOD methods, which is much more challenging and practical in real-world scenarios. Note that our attack is black-box and can be performed without references provided in the group.

Ruijun Gao, **Qing Guo*** , Felix Juefei-Xu, Hongkai Yu, Xuhong Ren, Wei Feng, and Song Wang. Making Images Undiscoverable from Co-Salient Object Detection. In CVPR 2022 .

Robustness Evaluation

Centre for Frontier AI Research
CFAR

Effects of rain to recog. & detection

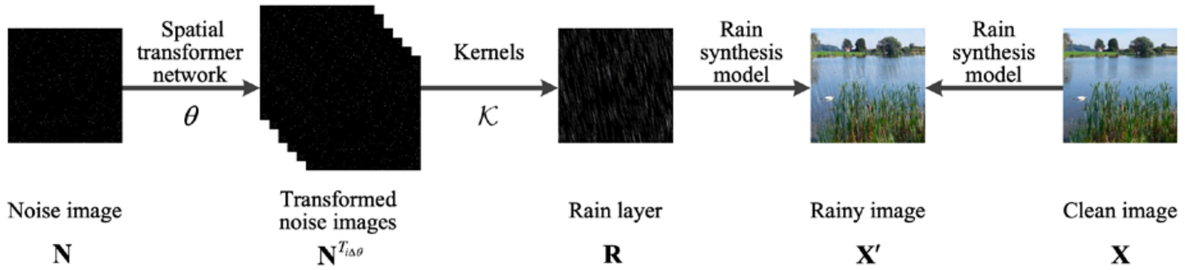
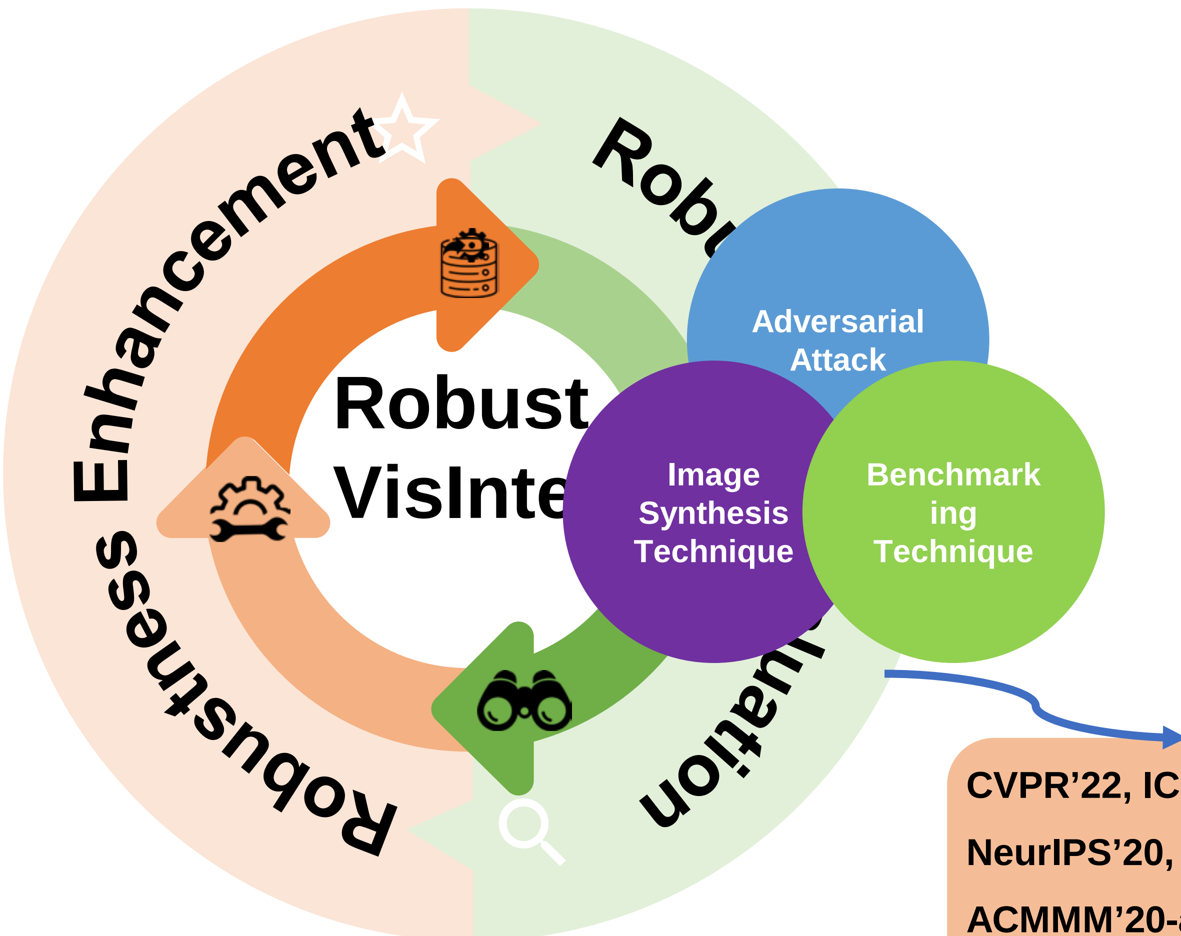


Figure 4: Comparison of our adversarial rainy images on three datasets (a-c) and other synthesized rainy images from Rain100H (Yang et al. 2017), Rain800 (Zhang, Sindagi, and Patel 2019), Rain1200 (Zhang and Patel 2018), Rain1400 (Fu et al. 2017) and Physics-based Rain Rendering (Halder, Lalonde, and Charette 2019) (d-h).

Liming Zhai, Felix Juefei-Xu, **Qing Guo***, Xiaofei Xie, Lei Ma, Wei Feng, Shengchao Qin, and Yang Liu. **It's Raining Cats or Dogs? Adversarial Rain Attack on DNN Perception.** in https://arxiv.org/abs/2009.09205.

Robustness Evaluation

Goal: *Robustness <u>Evaluation</u> and <u>Enhancement</u> of Visual Intelligence to <u>Real-world Degradation:</u>*



CVPR'22, ICCV'21,

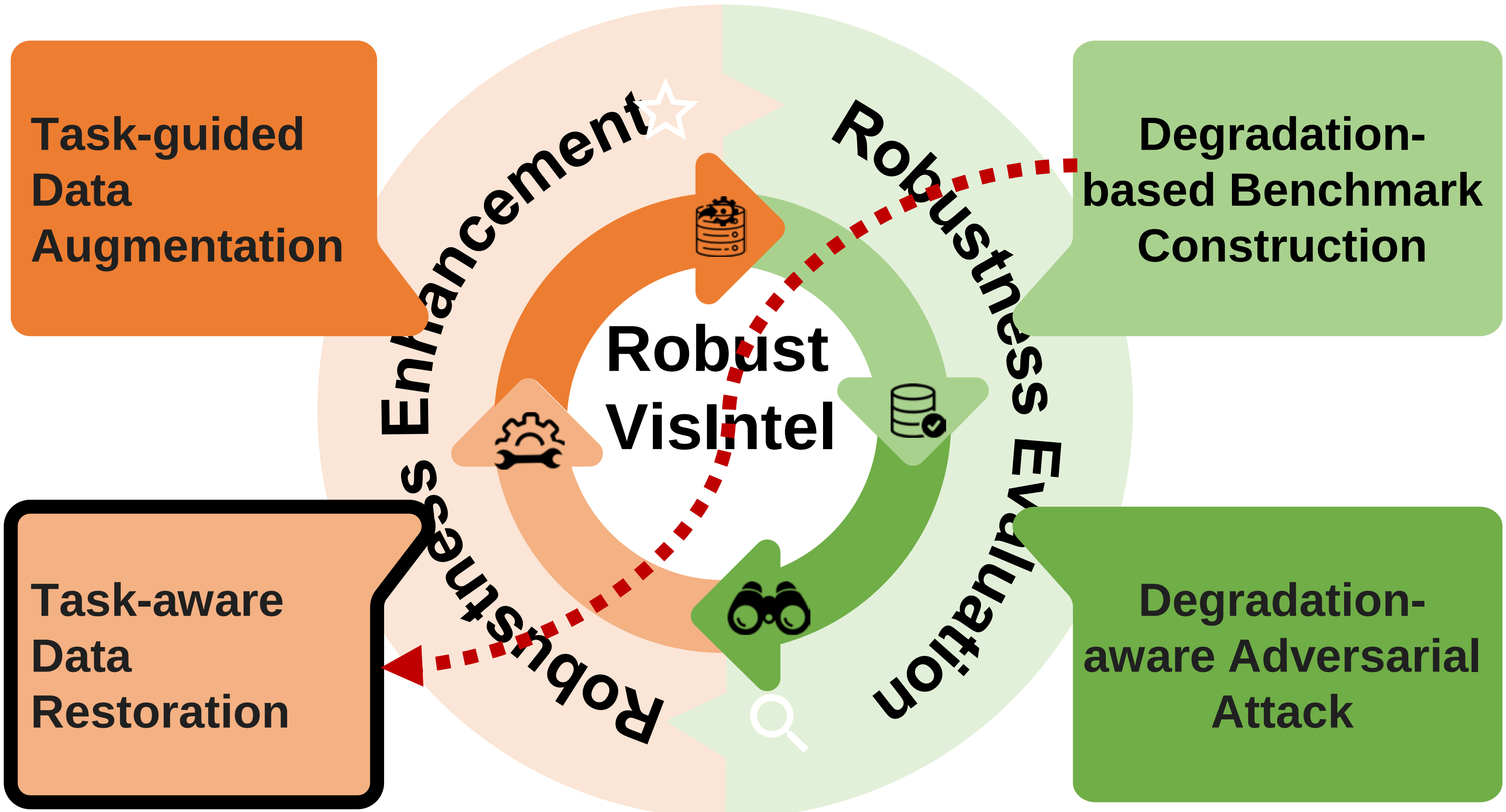
NeurIPS'20, ECCV'20,

ACMMM'20-a, IJCAI'21,

ICME'21,TIP'21, TMM' 21

Robustness Enhancement

Goal: *Robustness Evaluation and Enhancement of Visual Intelligence to Real-world Degradation:*



Robustness Enhancement

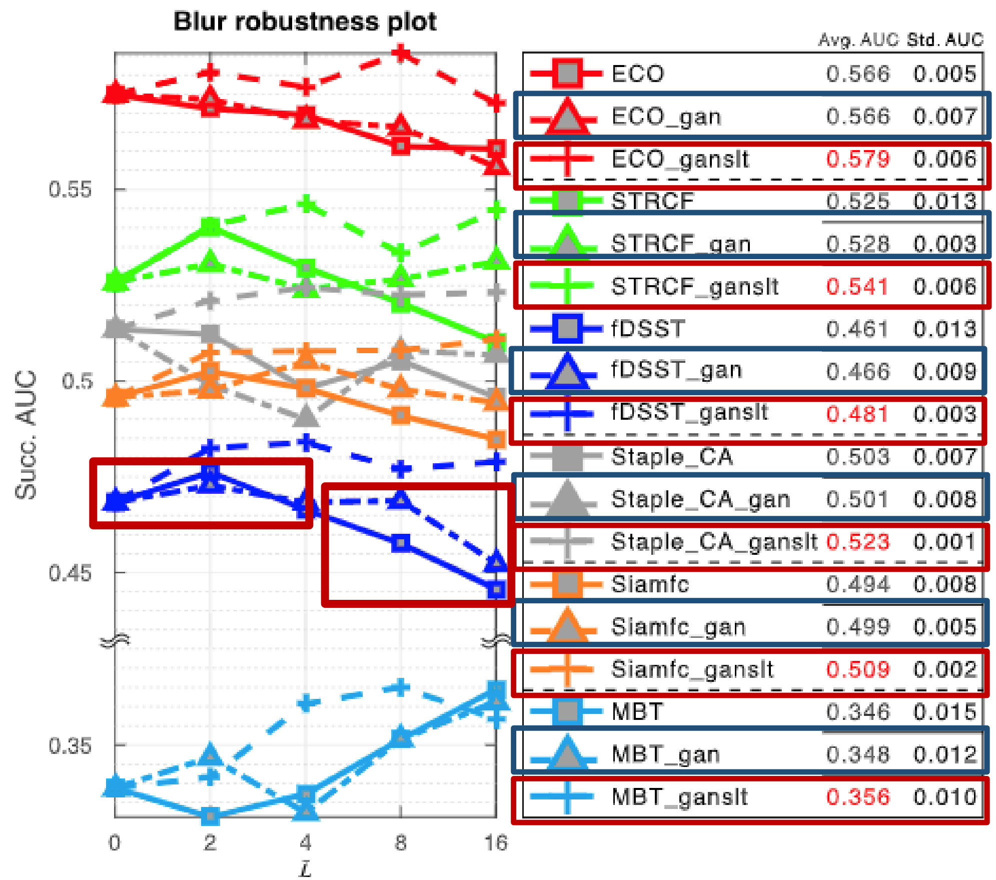
Centre for Frontier AI Research
CFAR

Selective Deblurring for Blur Robust Tracking (TIP’ 21)

➢ **Motivation**

❖ Blurred Video Benchmark: **Effects of deblurring to different blur levels are different.**

❖ Blurred Video Benchmark: **Selective deblurring improves tracking accuracy significantly**



_gan: deblurring all frames **_ganslt: selective deblurring w.r.t GT**

Q. Guo, W. Feng, R. Gao, Y. Liu, and S. Wang. Exploring the Effects of Blur and Deblurring to Visual Object Tracking. In IEEE TIP, 2021

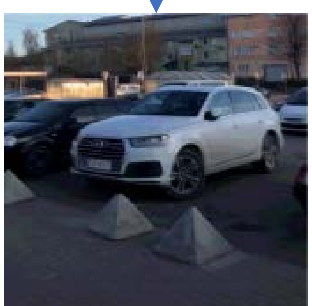
Robustness Enhancement

Centre for Frontier AI Research
CFAR

Selective Deblurring for Blur Robust Tracking (TIP' 21)

➢ **DeblurGAN-D as Blur Assessor**

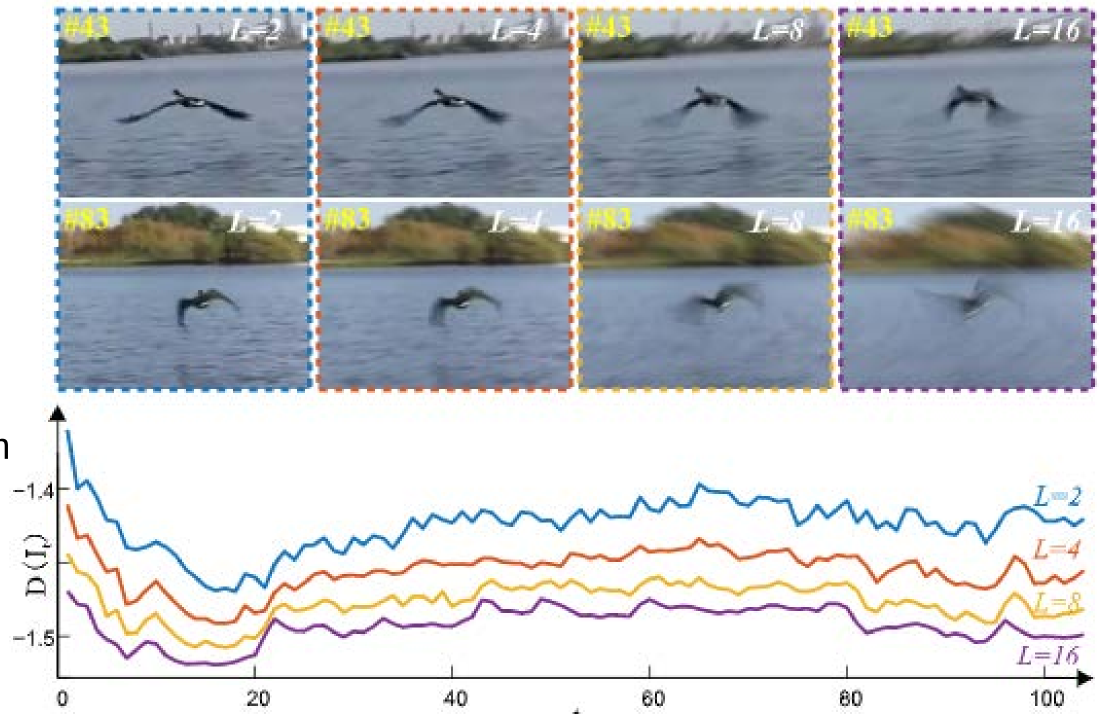
Generator



Discriminator

Blur level from heavy to light during training

Deblurred



Q. Guo, W. Feng, R. Gao, Y. Liu, and S. Wang. Exploring the Effects of Blur and Deblurring to Visual Object Tracking. In IEEE TIP, 2021

Robustness Enhancement

Selective Deblurring for Blur Robust Tracking (TIP' 21)

➢ **Pipeline**

Selective deblurring via DeblurGAN-D

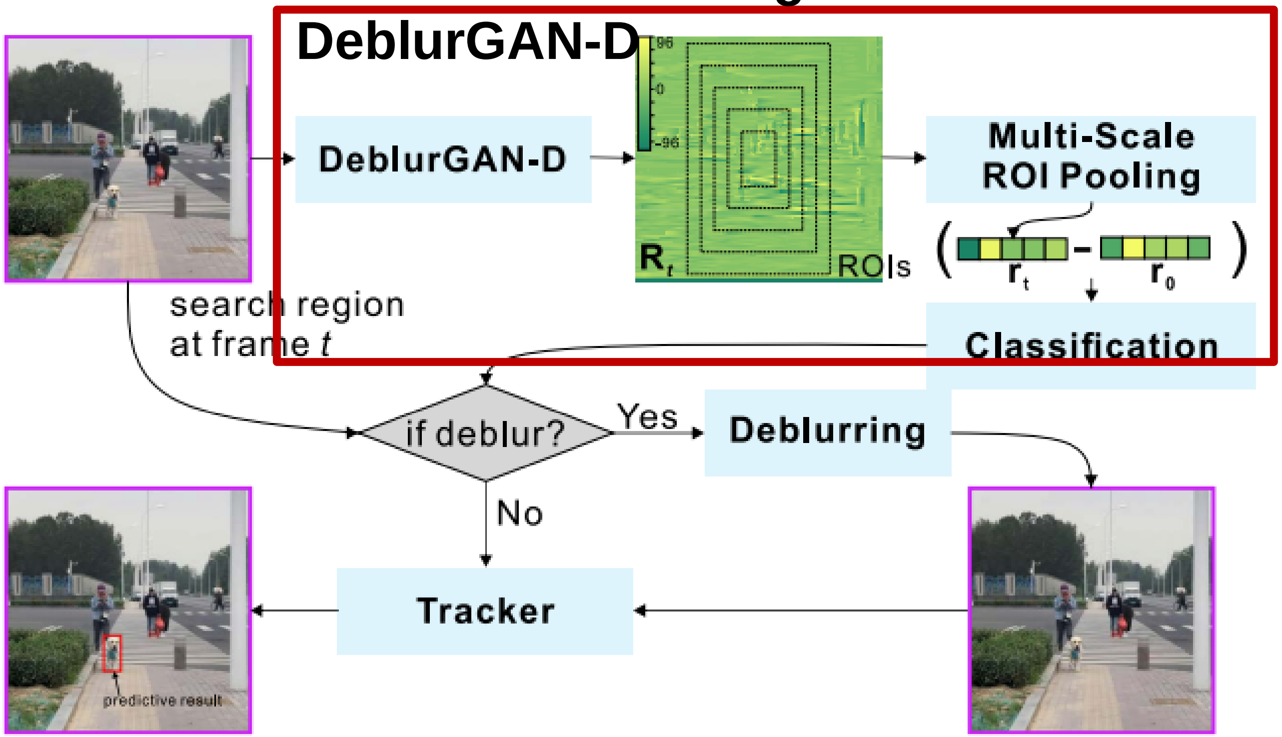


Fig. 10. The pipeline of our selective deblurring-based tracking. We can use existing deblurring methods, *e.g.*, DeblurGAN-G [14] for 'deblurring', and the classification is set as an offline trained SVM that indicates when we should deblurring a coming frame *t*.

Q. Guo, W. Feng, R. Gao, Y. Liu, and S. Wang. Exploring the Effects of Blur and Deblurring to Visual Object Tracking. In IEEE TIP, 2021

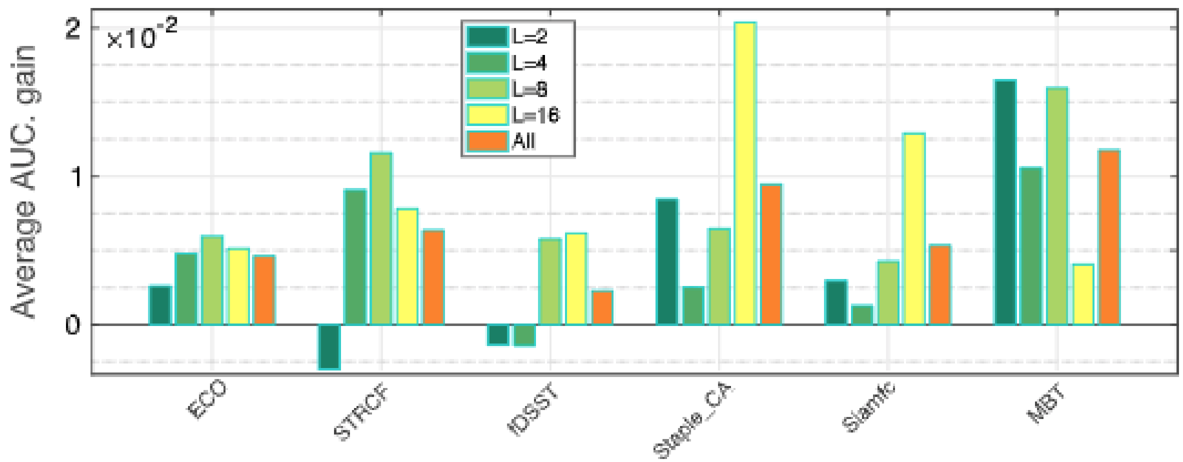
Robustness Enhancement

Selective Deblurring for Blur Robust Tracking (TIP' 21)

➢ **Results**

TABLE I
COMPARISON RESULTS ON THE MOTION BLUR SUBSET OF OTB.

Trackers	raw (AUC)	blur-robust tracking (AUC)
fDSST	0.512	**0.530**
Staple_CA	0.551	**0.561**
Siamfc	0.343	**0.353**
MBT	0.233	**0.242**
ECO	0.677	**0.679**
STRCF	0.633	**0.637**

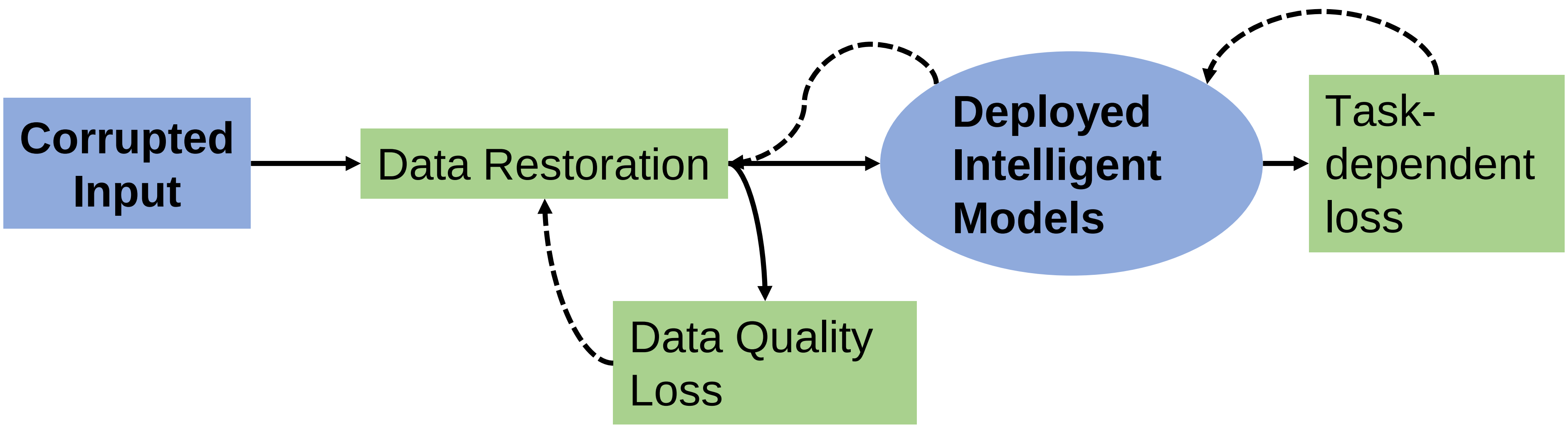


Q. Guo, W. Feng, R. Gao, Y. Liu, and S. Wang. Exploring the Effects of Blur and Deblurring to Visual Object Tracking. In IEEE TIP, 2021

Robustness Enhancement

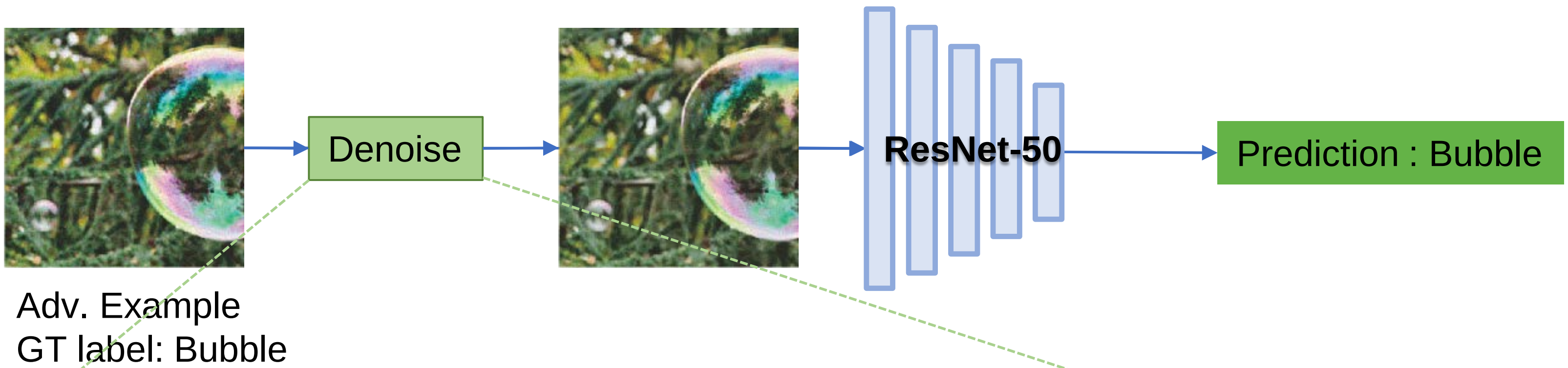
Task-aware Data Restoration

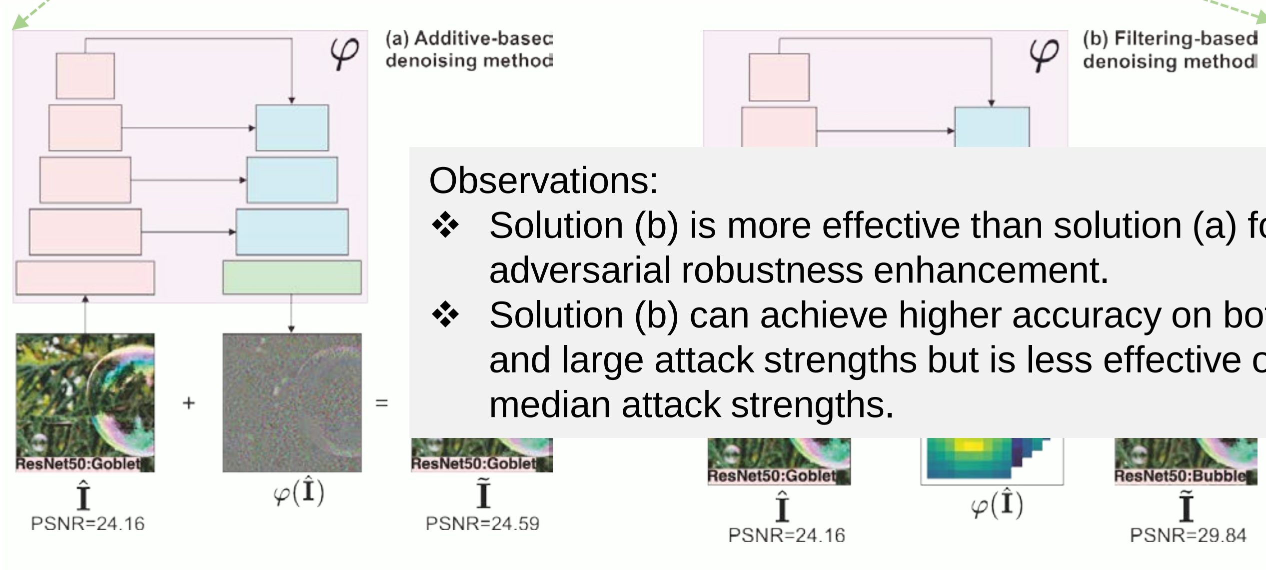
- ➢ **Generalizing deblurring to other degradation restorations**



Robustness Enhancement

Task-aware Data Restoration – Denoising (MM'21)





Observations:

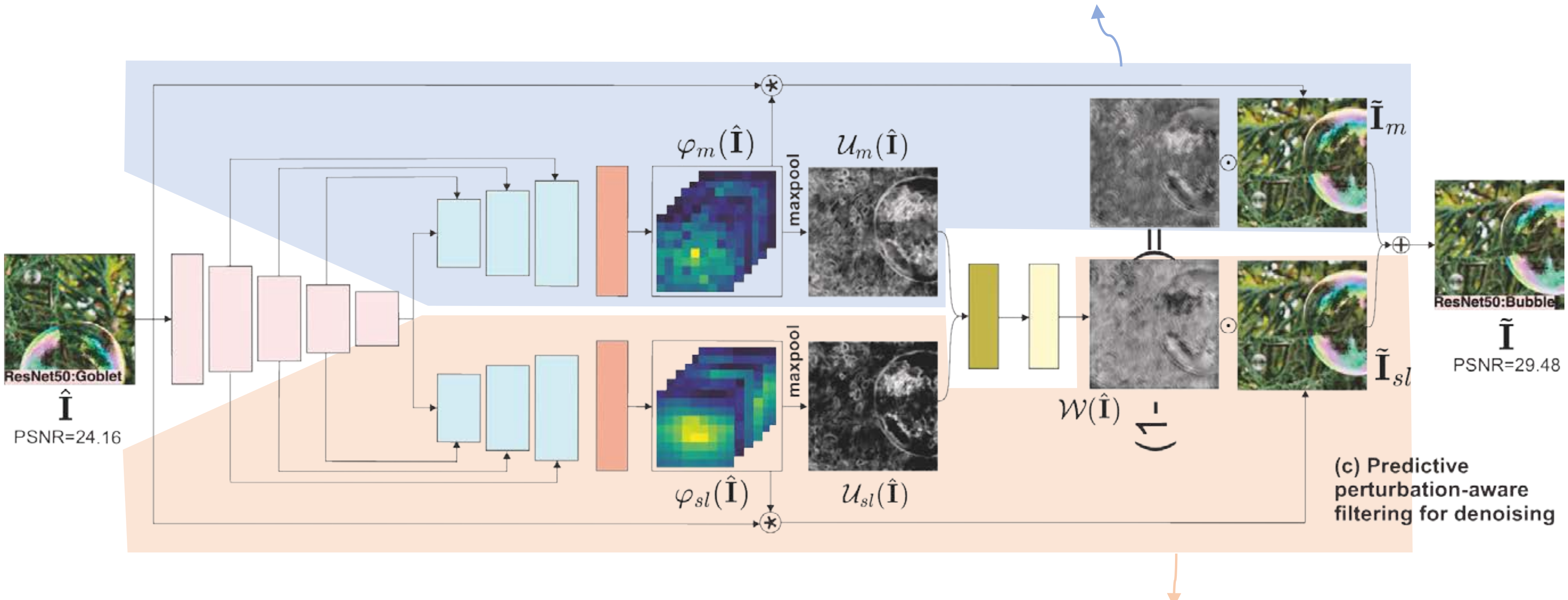
- ❖ Solution (b) is more effective than solution (a) for adversarial robustness enhancement.
- ❖ Solution (b) can achieve higher accuracy on both small and large attack strengths but is less effective on the median attack strengths.

Y. Huang, **Q. Guo***, F. Juefei-Xu, et. al. AdvFilter: Predictive Perturbation-aware Filtering against Adversarial Attack via Multi-domain Learning. in ACM-MM, 2021.

Robustness Enhancement

Task-aware Data Restoration – Denoising (MM’21)

1st predictive filtering for median attack strength

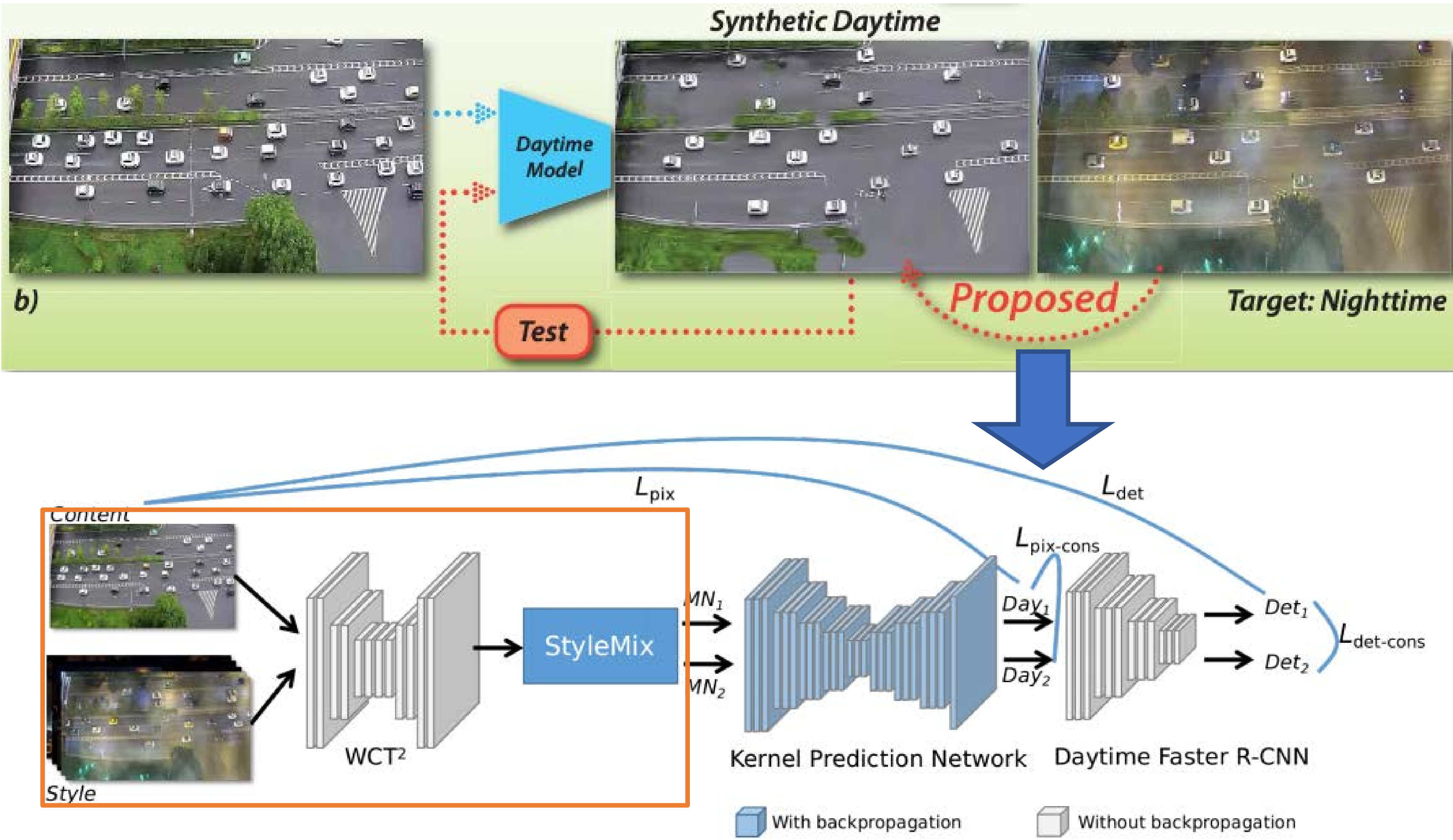


2nd predictive filtering for small&large attack strengthes

Y. Huang, **Q. Guo***, F. Juefei-Xu, et. al. **AdvFilter: Predictive Perturbation-aware Filtering against Adversarial Attack via Multi-domain Learning**. in ACM-MM, 2021.

Robustness Enhancement

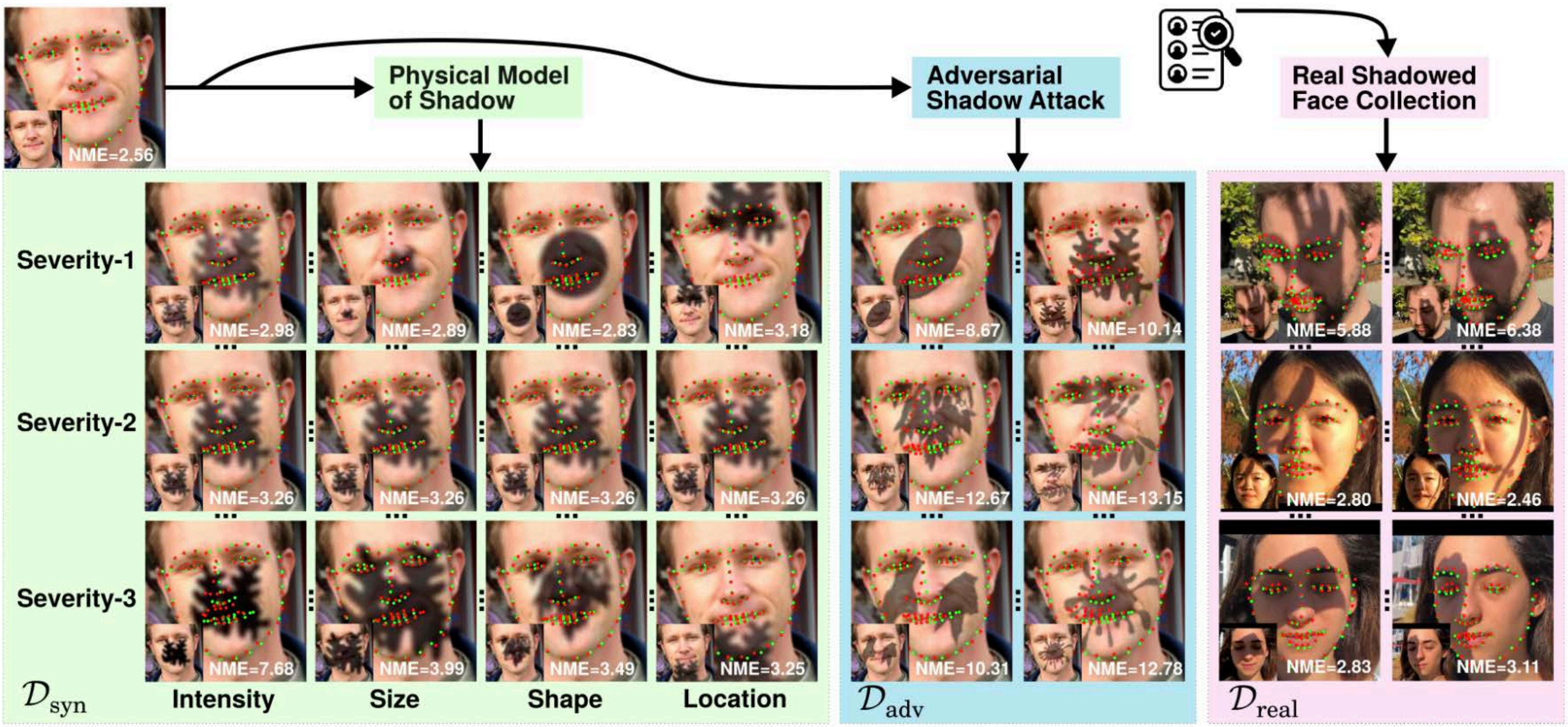
Task-aware Data Restoration – Night2Day



L. Fu, H. Yu, F. Juefei-Xu, J. Li, **Q. Guo***, Song Wang. Let There be Light: Improved Traffic Surveillancevia Detail Preserving Night-to-day

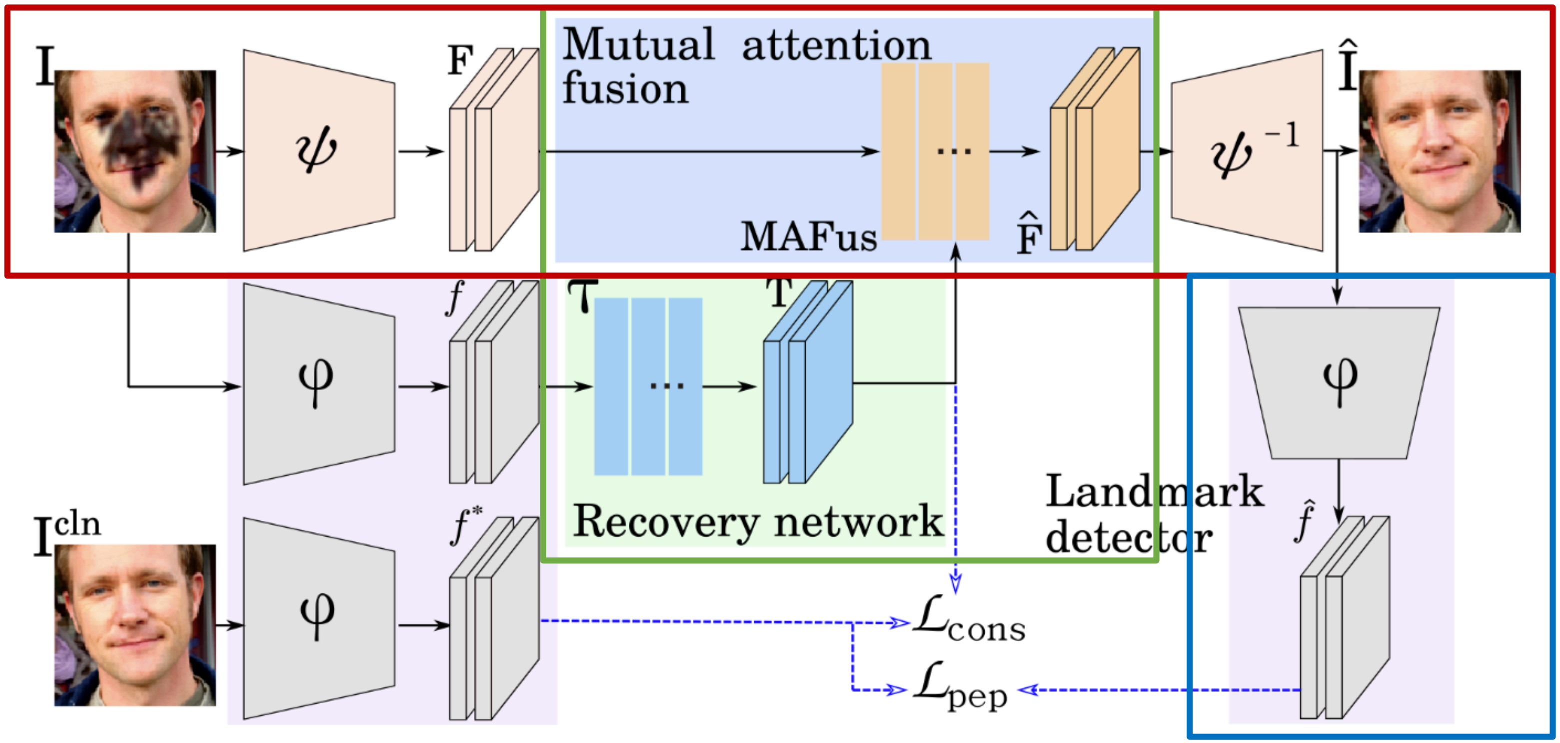
Robustness Enhancement

Task-aware Data Restoration – Shadow Removal



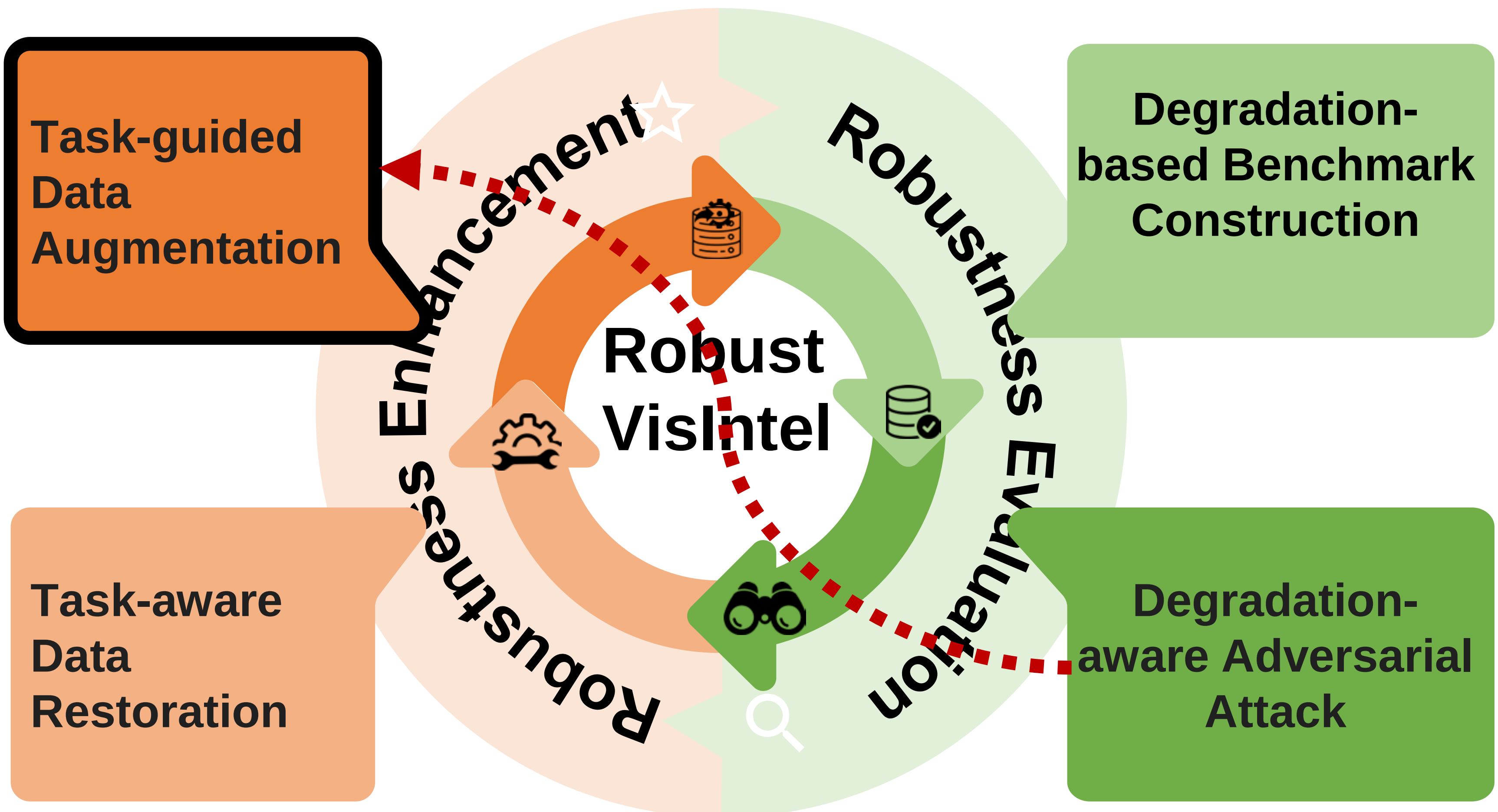
Robustness Enhancement

Task-aware Data Restoration – Shadow Removal



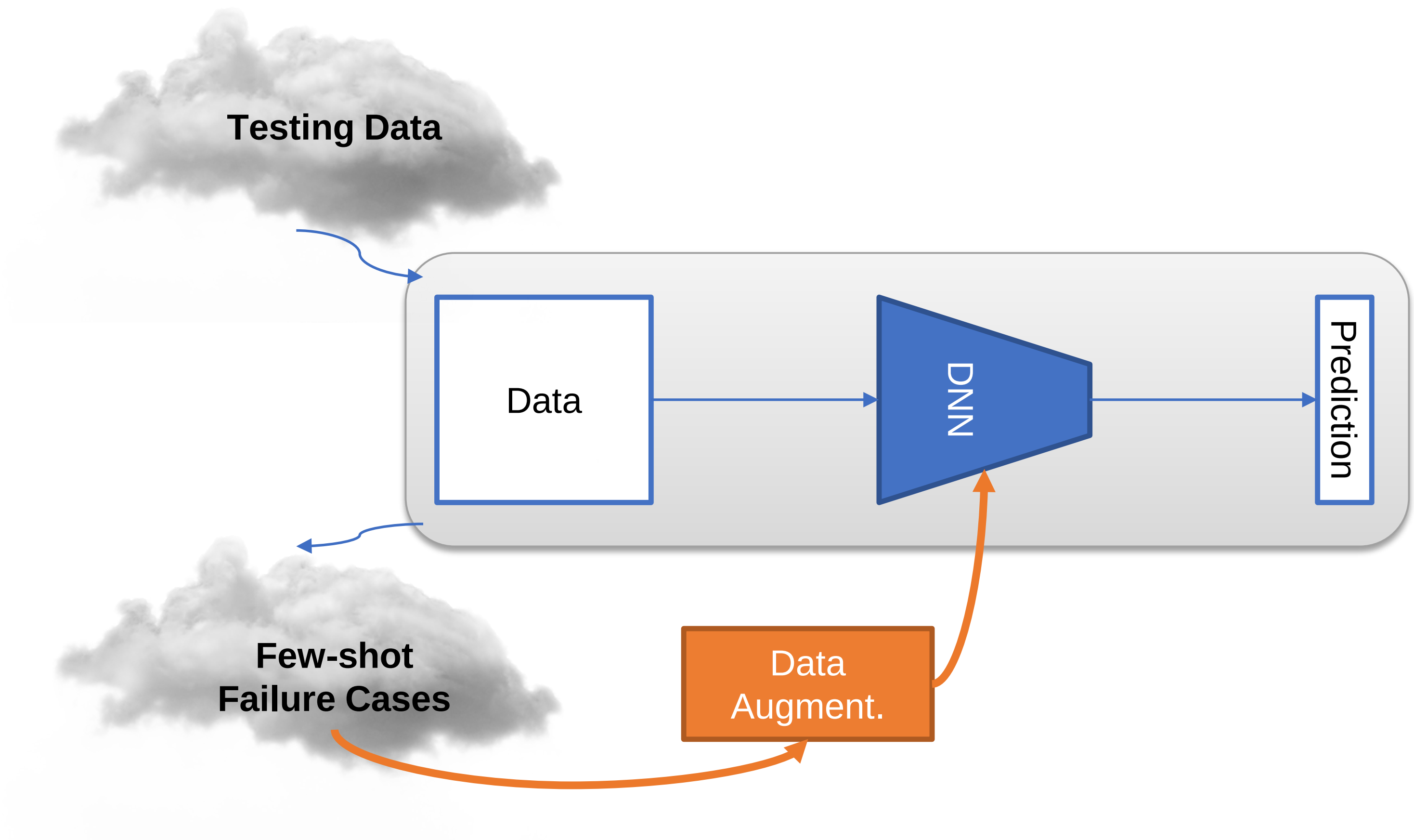
Robustness Enhancement

***Goal:** Robustness __Evaluation__ and __Enhancement__ of Visual Intelligence to __Real-world Degradation:__*



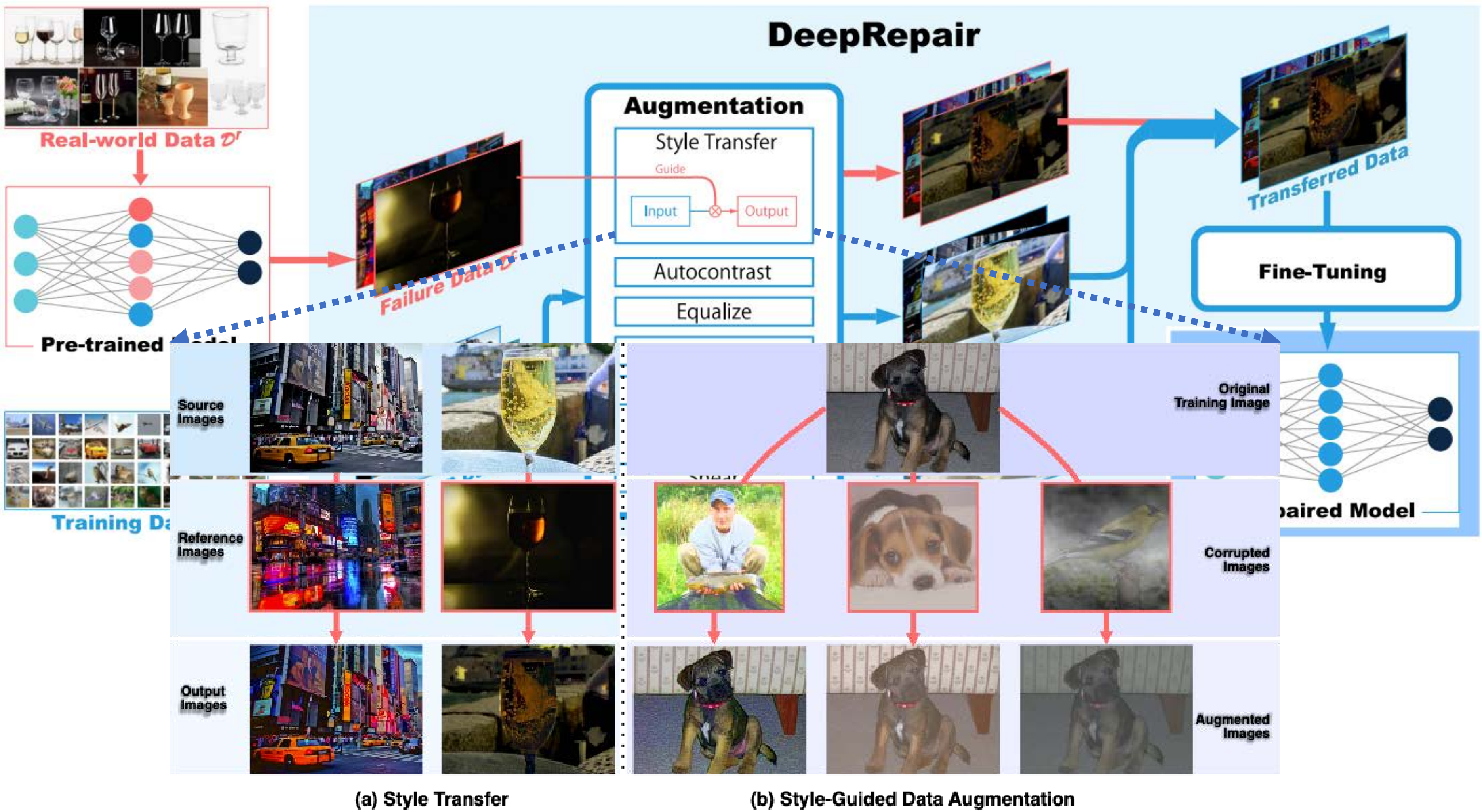
Robustness Enhancement

Failure-set Guided Data augmentation



Robustness Enhancement

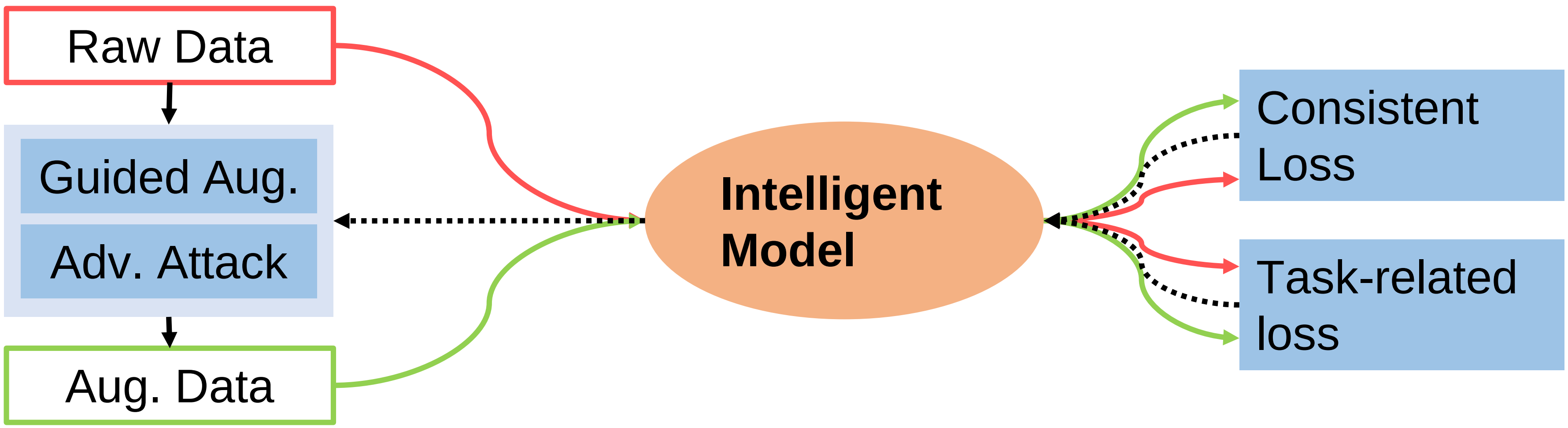
Failure-set Guided Data augmentation



B. Yu, H. Qi, **Q. Guo***, F. Juefei-Xu, X. Xie, L. Ma, and J. Zhao. DeepRepair: Style-Guided Repairing for DNNs in the Real-world Operational Environment. IEEE Trans. on Reliability, 2021.

Robustness Enhancement

Task-guided Data Augmentation

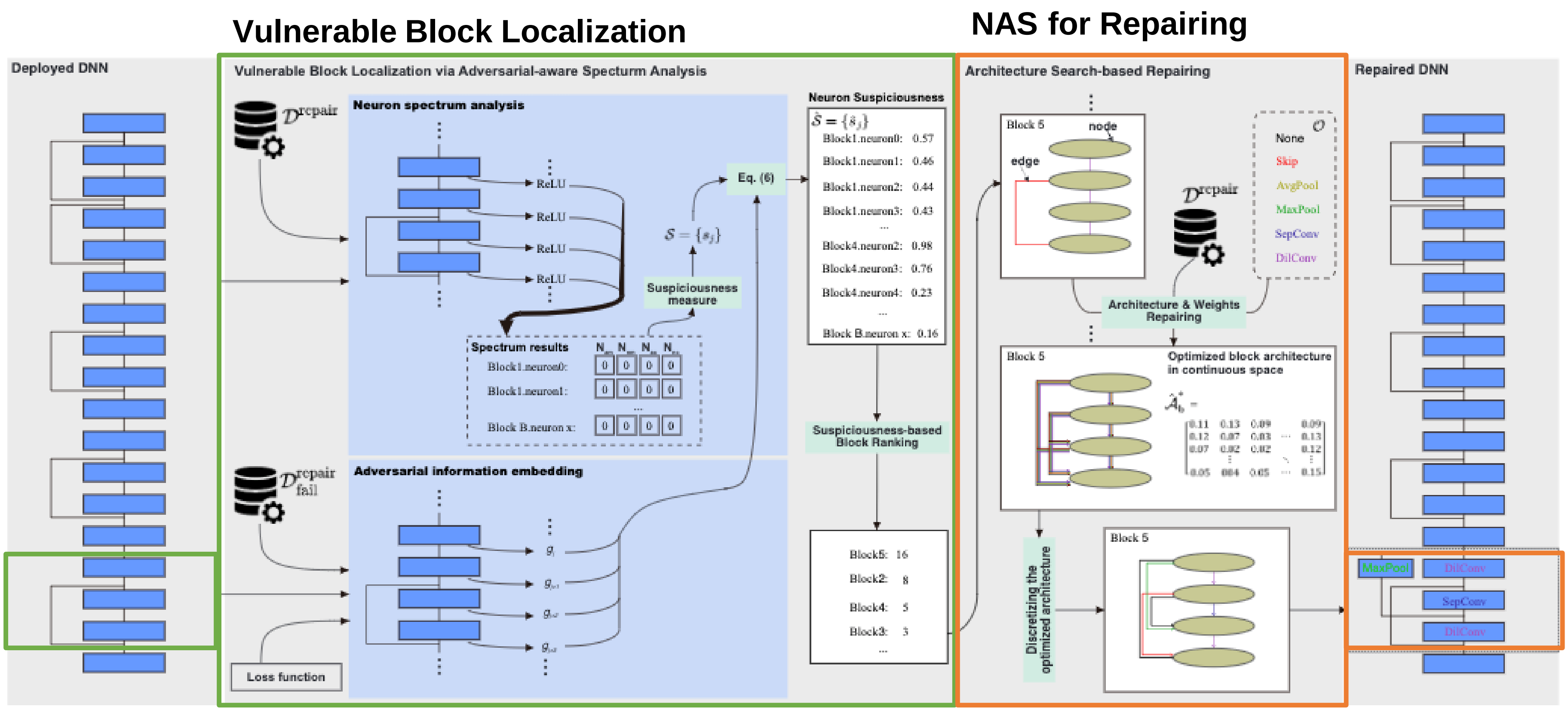


Robustness Enhancement

Solution2: Task-guided Data Augmentation

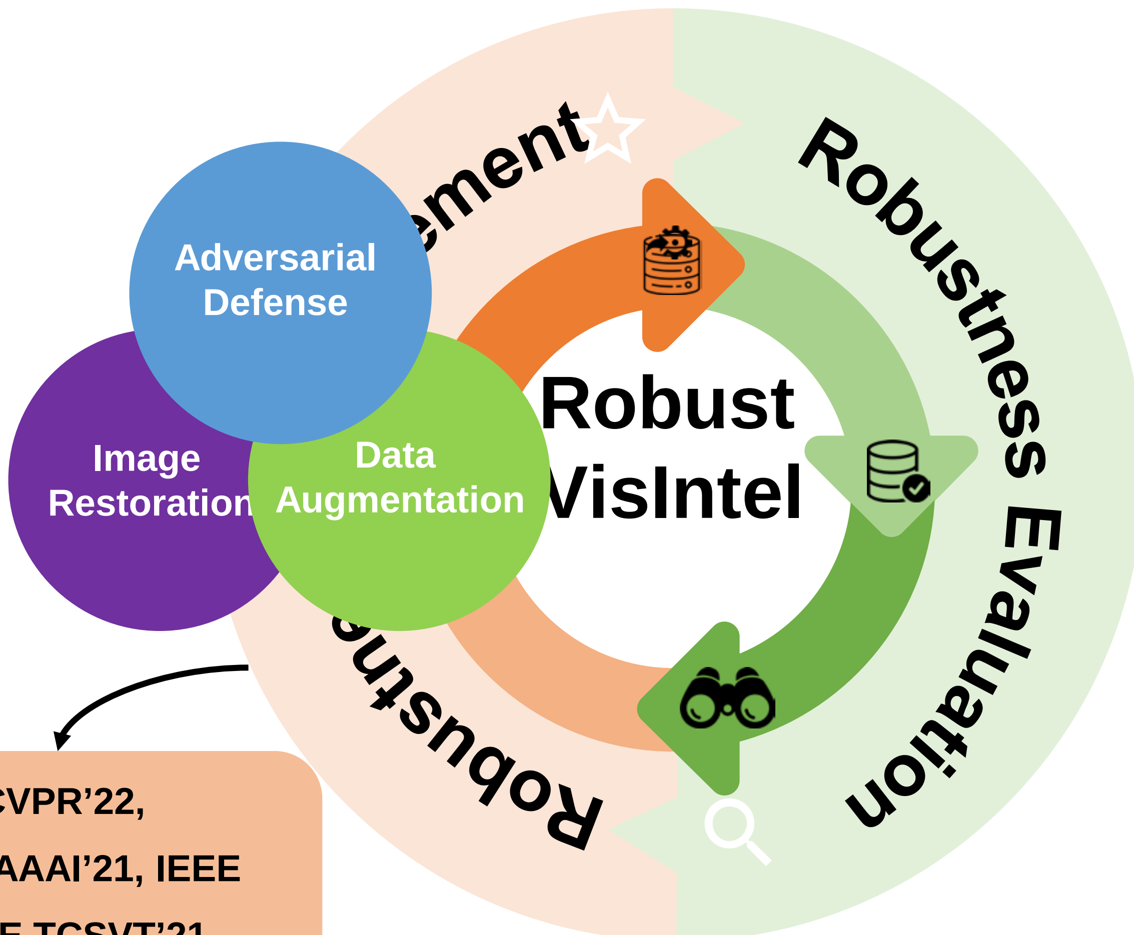
➢ **Generalizing Data Repair to Architecture Repair via NAS**

ArchRepair for unknown failure patterns

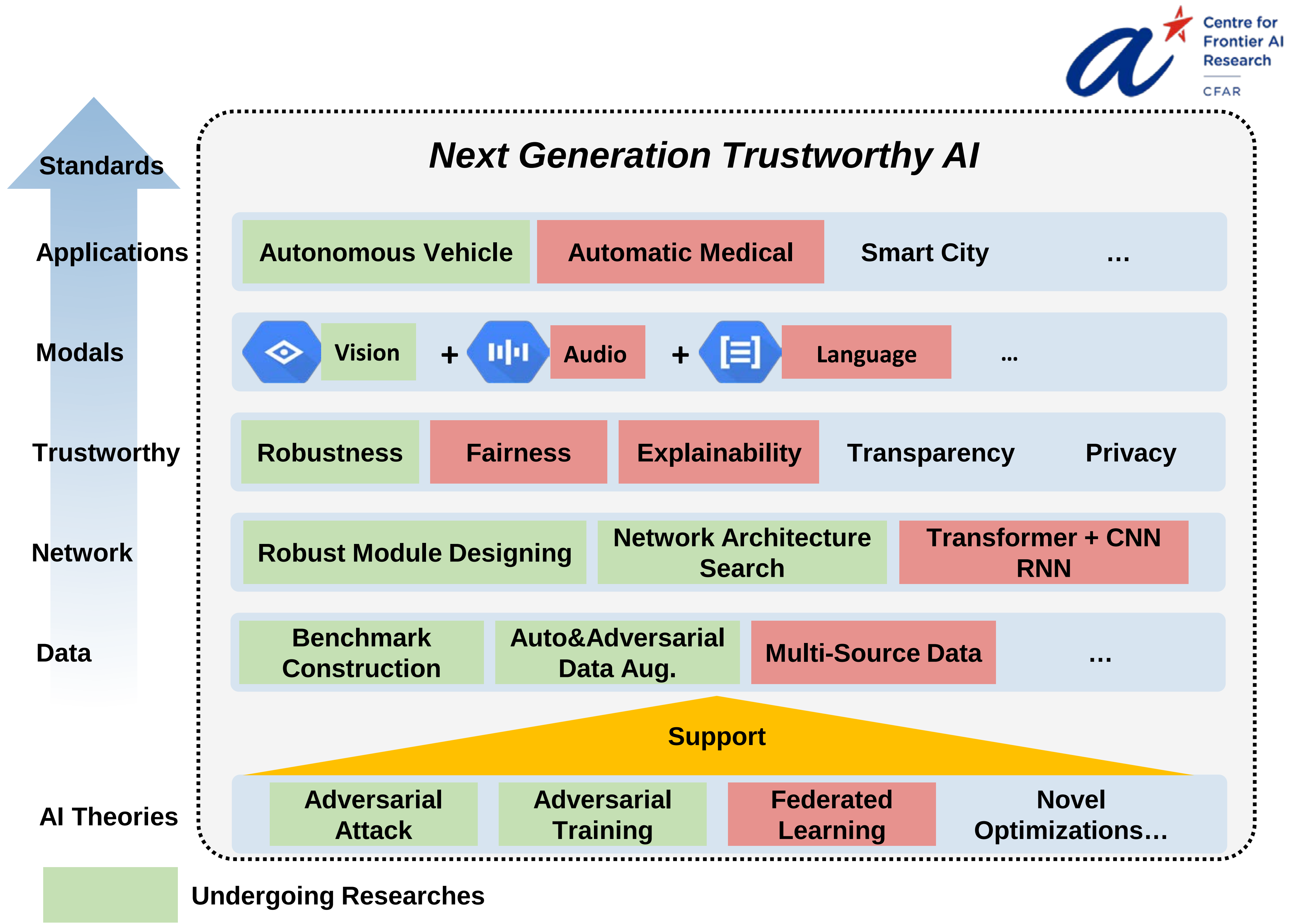


Robustness Enhancement

Goal: *Robustness <u>Evaluation</u> and <u>Enhancement</u> of Visual Intelligence to <u>Real-world Degradation:</u>*



AAAI'23, CVPR'22, CVPR'21, AAAI'21, IEEE TR'21, IEEE TCSVT'21, ACMMM'20-b, '21-a,b



Centre for Frontier AI Research
CFAR
Next Generation Trustworthy AI
Standards
Applications
Autonomous Vehicle
Automatic Medical
Smart City
...
Modals
Vision
+
Audio
+
Language
...
Trustworthy
Robustness
Fairness
Explainability
Transparency
Privacy
Network
Robust Module Designing
Network Architecture Search
Transformer + CNN RNN
Data
Benchmark Construction
Auto&Adversarial Data Aug.
Multi-Source Data
...
Support
AI Theories
Adversarial Attack
Adversarial Training
Federated Learning
Novel Optimizations...
Undergoing Researches

Centre for Frontier AI Research

CFAR

Thank You!
Q & A

GUO Qing, CFAR

tsingqguo@ieee.org

https://tsingqguo.github.io/

CREATING GROWTH, ENHANCING LIVES