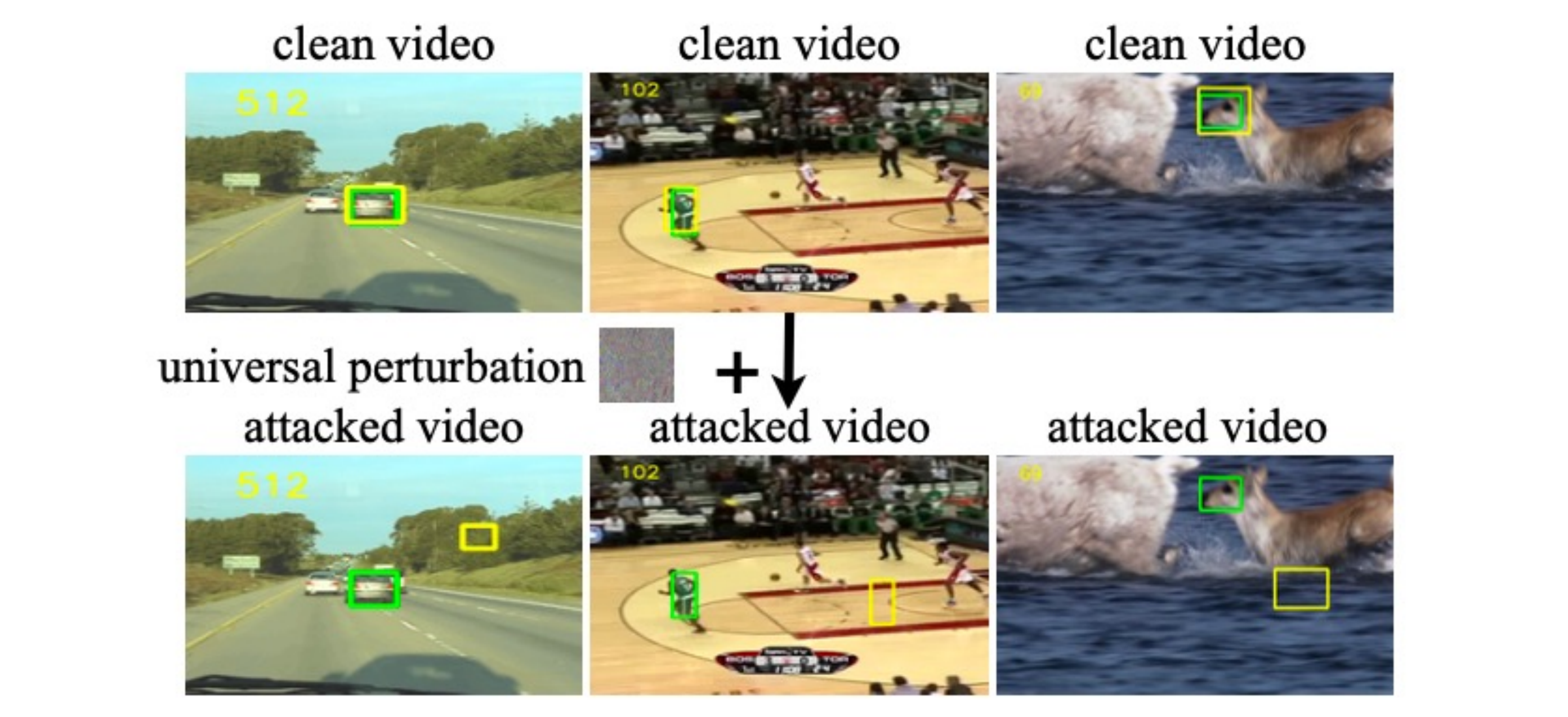
Paper Number:2015

EFFICIENT UNIVERSAL SHUFFLE ATTACK FOR VISUAL OBJECT TRACKING

Siao Liu, Zhaoyu Chen, Wei Li, Jiwei Zhu, Jiafeng Wang, Wenqiang Zhang, Zhongxue Gan

The Universal Adversarial Attack for VOT



In this work, we propose a simple technique to achieve a universal adversarial attack for visual object tracking. We just inject one perturbation in the template and search frames to fool the trackers in the whole dataset.

Problem Definition

Given an unknown target template, Siamese trackers need to predict the location and shape of the target in the subsequent frames x. Specifically, we describe the universal adversarial perturbation δ as follows:

$$\max \sum_{x \in \mathcal{X}} \mathcal{L}(x, x+\delta), \quad s.t. \quad ||\delta||_\infty \leq \epsilon$$

Triple Loss Design

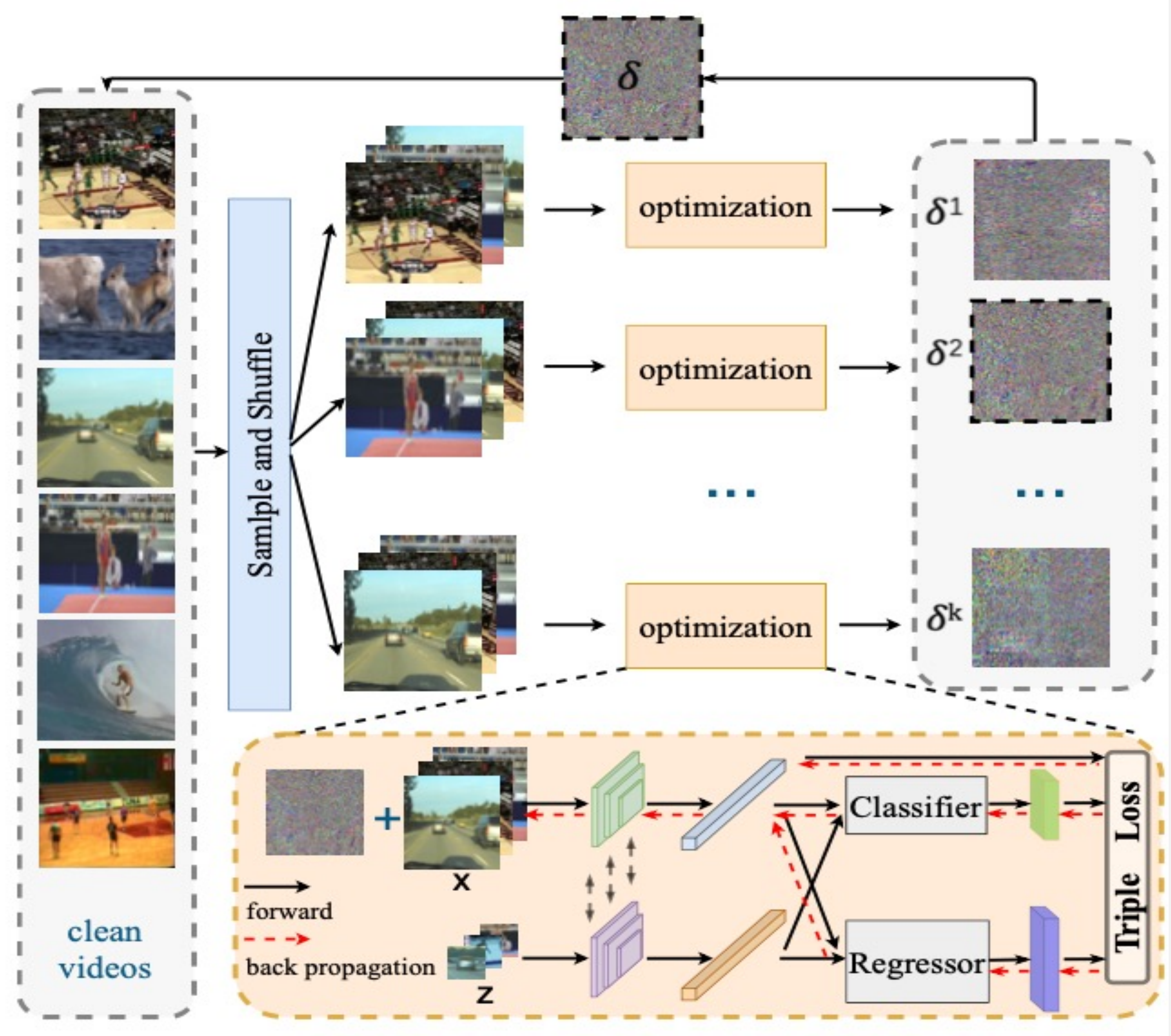
$$\mathcal{L} = \mathcal{L}_f + \lambda_1 \mathcal{L}_c + \lambda_2 \mathcal{L}_d.$$

$$\mathcal{L}_f(x, x^*) = -\sum_{i=1:C} \max(\mathrm{m_f}, \cos(\mathcal{F}_i(x), \mathcal{F}_i(x^*))).$$

$$\mathcal{L}_c(z, x^*) = -\sum_{j=1:N} C_j(\mathcal{F}(z), \mathcal{F}(x^*)).$$

$$\mathcal{L}_d(z, x^*) = -\alpha \cdot ||R^*_{scale}||_2 - || < R^*_{loc}, \vec{d} > ||_2.$$

EFFICIENT UNIVERSAL SHUFFLE ATTACK



The overview of Efficient Universal Shuffle Attack. Shuffle strategy is used to change the order of video sequences and each perturbation would be generated via gradient back propagation iteratively.

Some Ablation Studies

Table 2. Ablation study of shuffle strategy.

	Success(%) ↑				Pression(%) ↑			
sampling rate r	0.1	0.3	0.5	1	0.1	0.3	0.5	1
w/o shuffle	55.0	50.3	49.3	50.1	72.8	66.7	67.1	68.2
w/ shuffle	**39.3**	**30.2**	**26.9**	**23.6**	**55.5**	**42.3**	**38.1**	**32.7**

Table 3. Ablation study of triple loss.

$\mathcal{L}_f$		✓			✓	✓	✓
$\mathcal{L}_c$			✓		✓		✓
$\mathcal{L}_d$				✓		✓	✓
Precision(%)	90.5	59.4	54.1	54.6	51.2	50.0	**32.7**
Success rate(%)	69.6	40.0	38.4	39.0	37.1	36.2	**23.6**

Performance

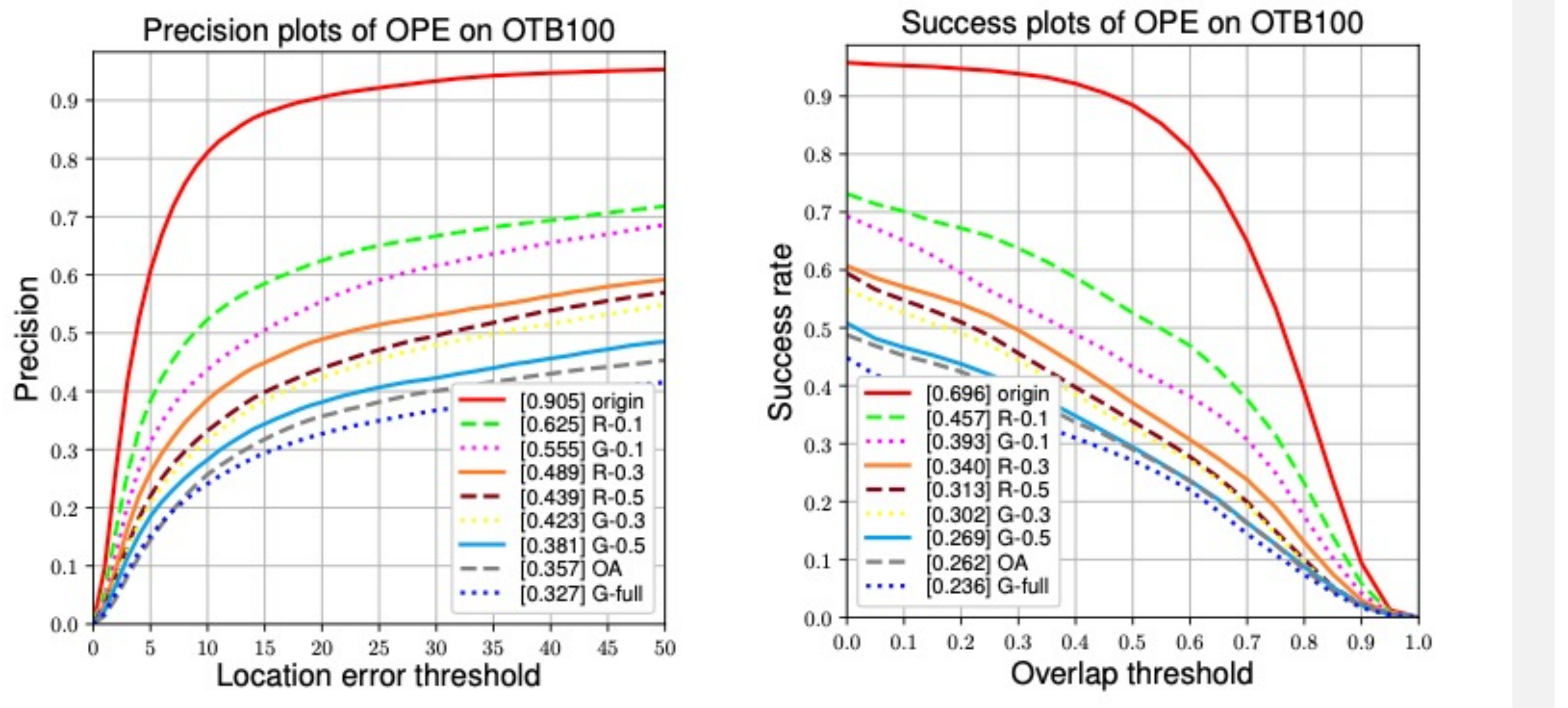
Table 1. Attack performance on OTB100.

Tracker	Precision(%) ↑			Success Rate(%) ↑		
	Org	OA	EUSA	Org	OA	EUSA
SiamRPN	87.6	27.8	**26.7**	66.8	20.4	**20.2**
SiamRPN++(R)	90.5	35.7	**32.7**	69.6	26.2	**23.6**
SiamRPN++(M)	86.4	35.3	**25.9**	65.8	26.1	**18.3**
SiamMask	83.9	65.0	**34.9**	64.7	48.1	**22.5**

Table 2. Attack performance on VOT2018.

Tracker	Accuracy(%) ↑			Robustness ↓			EAO ↑		
	Org	OA	EUSA	Org	OA	EUSA	Org	OA	EUSA
SiamRPN	57.7	46.7	**44.0**	0.309	1.733	**2.241**	0.338	0.082	**0.055**
SiamRPN++(R)	60.2	51.9	**46.1**	0.243	1.157	**2.051**	0.413	0.115	**0.072**
SiamRPN++(M)	58.9	48.3	**45.2**	0.234	1.344	**2.622**	0.411	0.101	**0.056**
SiamMask	59.8	45.5	**31.8**	0.248	0.674	**2.632**	0.406	0.165	**0.043**

Quantitative comparisons



Quantitative comparisons between various sampling rate and different sampling strategy on OTB2015 dataset. The suffix ”G” and ”R” are greedy-gradient strategy and random sample respectively. The numbers are sampling rates.