Tsinghua University

JUNE 18-22, 2023 CVPR VANCOUVER, CANADA

IEEE/CVF International Conference on Computer Vision and Pattern Recognition (CVPR 2023)

Physically Realizable Natural-Looking Clothing Textures Evade Person Detectors via 3D Modeling

Zhanhao Hu∗, Wenda Chu∗, Xiaopei Zhu, Hui Zhang, Bo Zhang, Xiaolin Hu

Tag: THU-AM-047

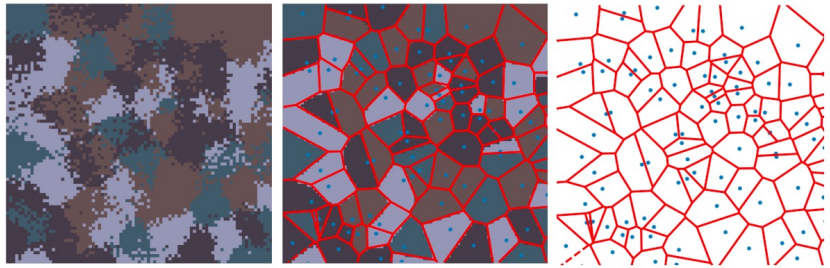
Overview:

We craft natural-looking clothing textures via 3D modeling in the physical world that can evade person detectors at multiple angles

Limitations of previous work:

1. Adversarial textures (Fig.(d)) are conspicuous to humans.
2. 3D modeling adversarial textures are not robust when applied to non-rigid objects.

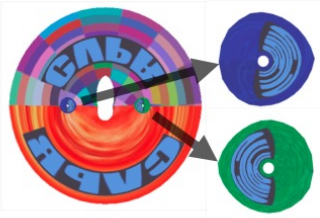
- Texture parameterization



Camouflage pattern | Color cluster | Voronoi diagram

- 3D augmentation by

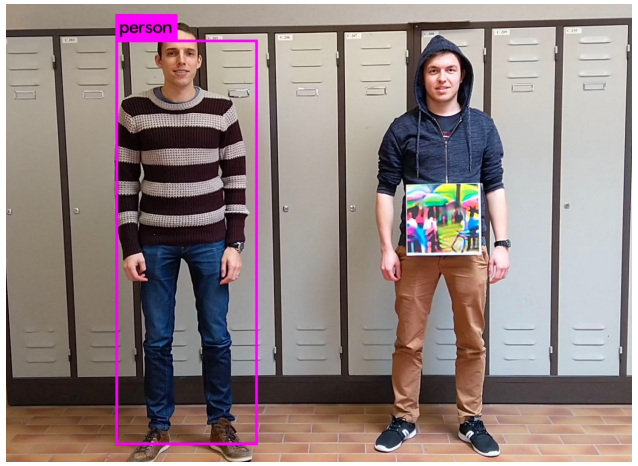
GeoProj



TopoProj

Related work :

1. patch-based attack, single viewing angle



Thys et al., 2019

Xu et al., 2020

Hu et al., 2021

2. texture-based attack, multiple viewing angles

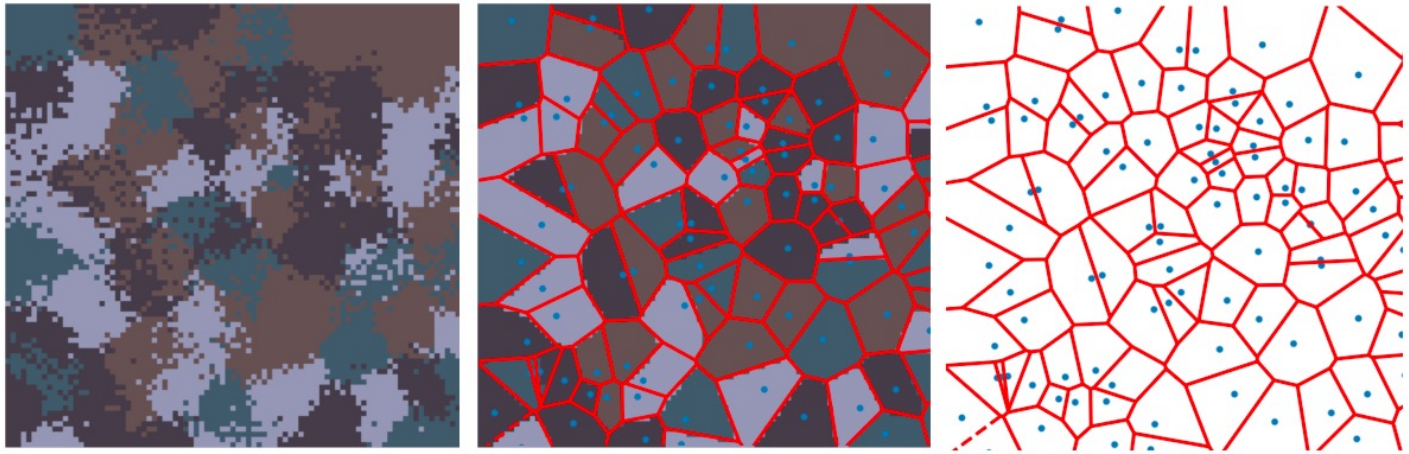
Rigid object
(3D printed)

Athalye et al. 2018

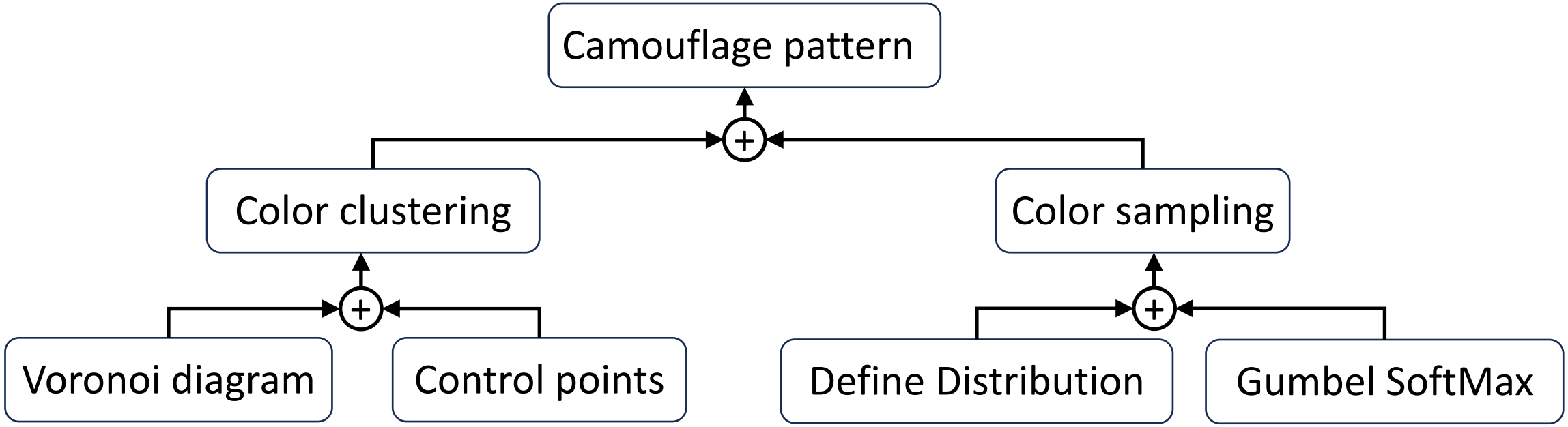
Non-rigid
Clothing textures

Ours, 2022

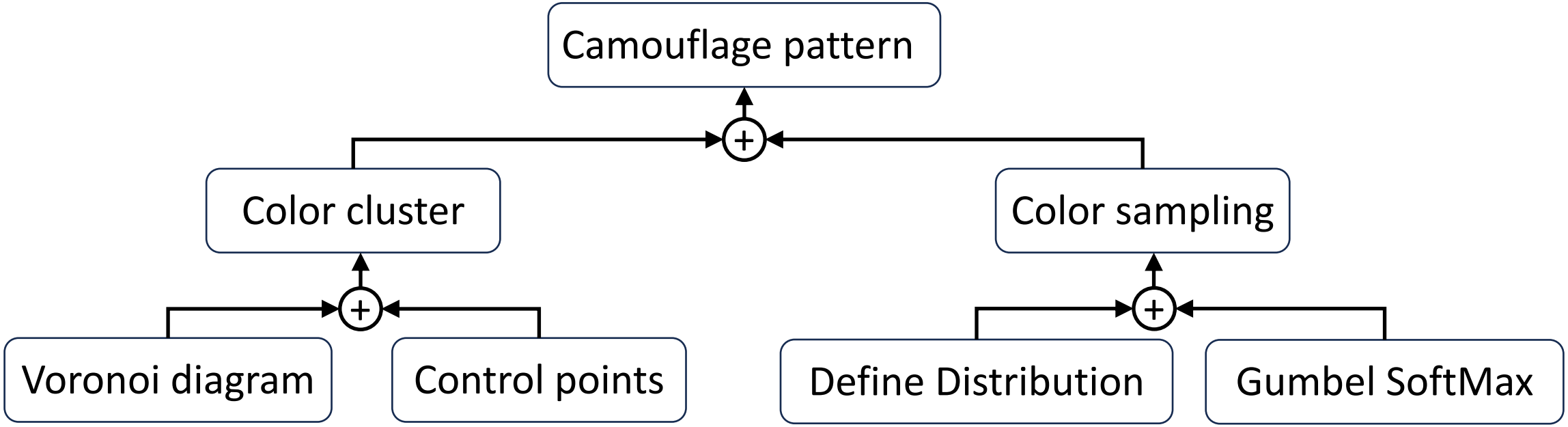
Method Part 1: Texture parameterization



Camouflage pattern Color cluster Voronoi diagram



Method Part 1: Texture parameterization



- The Distribution is Distance-determined

$$p_k^{(x)} = \frac{w_k^{(x)}}{\sum_{i=1}^{N_C} w_i^{(x)}}, k = 1, \ldots, N_C, \quad (1)$$

$$w_i^{(x)} = \sum_{j=1}^{N_P} \exp\left(-\frac{\|x - b_{ij}\|_2}{\alpha}\right), \quad (2)$$

- Gumbel SoftMax with a trainable seed

$$c^{(x)} = \sum_{i=1}^{N_C} c_i \cdot \mathrm{Softmax}\left(\frac{g_i + \log p_{c_i}^{(x)}}{\tau}\right), \quad (5)$$

$$g_i = -\log(-\log(\lambda \cdot u_i^{(\mathrm{fix})} + (1-\lambda) \cdot u_i^{(\mathrm{train})})), \quad (6)$$

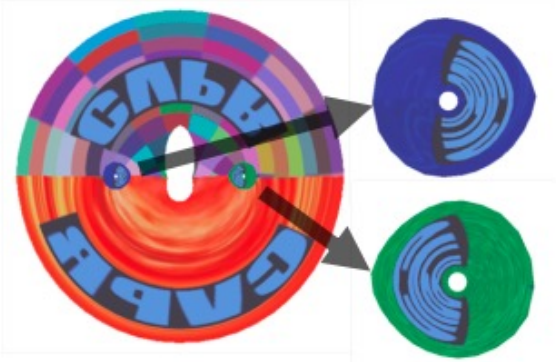
Method Part 2: 3D augmentation

- Problem: 3D textures are not robust when applied to non-rigid objects.
- Solution: Augment rendered image by GeoProj & TopoProj.

  GeoProj: Typical UV coordinates of the vertices

  TopoProj: Created by us

Geometrically plausible



Topologically plausible

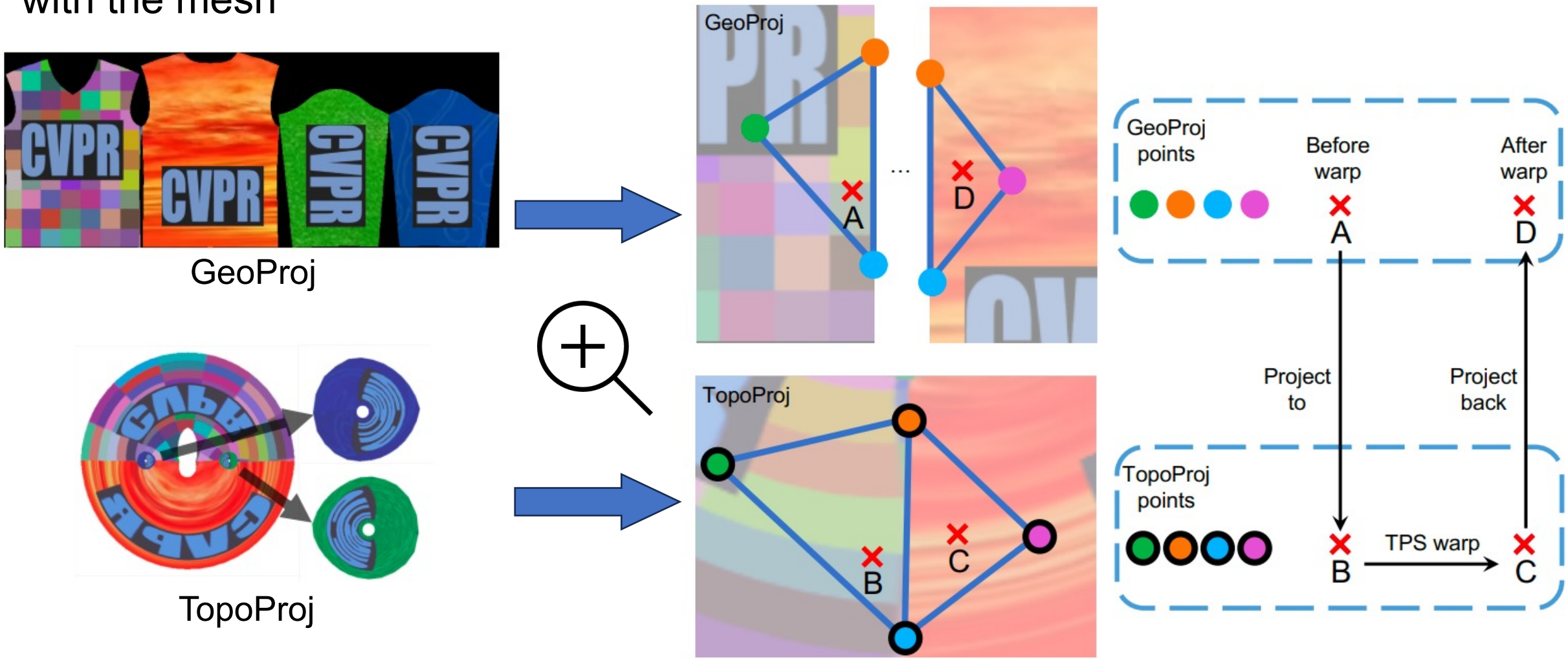
No aug

Bad aug
(without TopoProj)

Good aug
(with TopoProj)

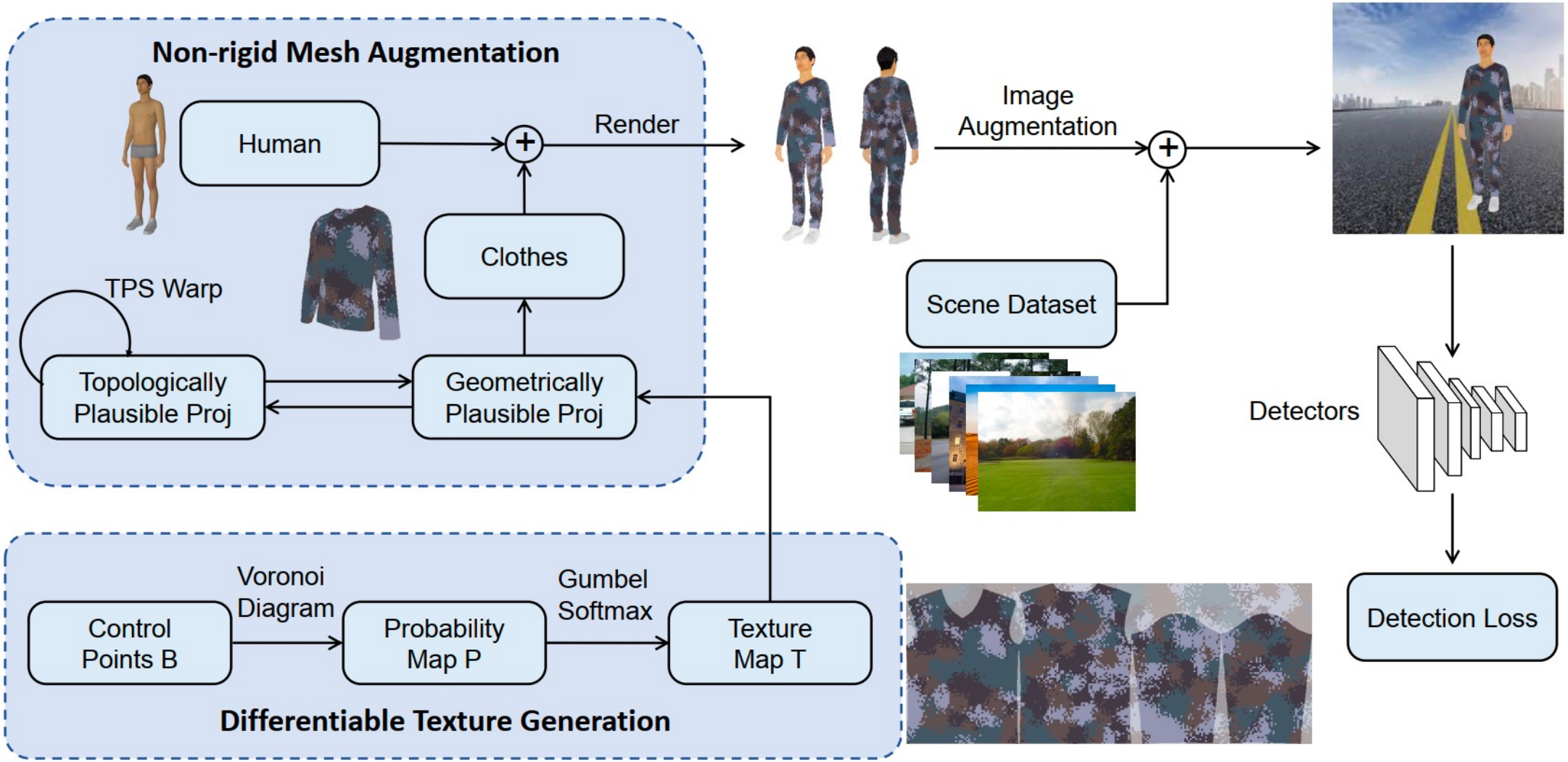
Method Part 2: 3D augmentation

- Instead of simulating the movement of 3D vertices, we warp the texture during the rendering
- Each pixel corresponds to a light path which may have intersections with the mesh



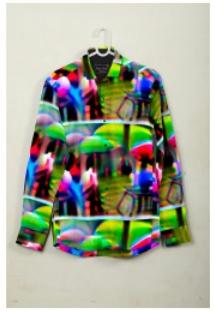
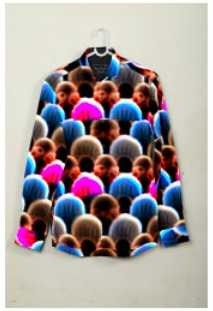
Overall Pipeline:

- Texture parameterization + 3D augmentation



Result: Subjective test

- 7-level Likert scale (1 = not natural at all to 7 = very natural)

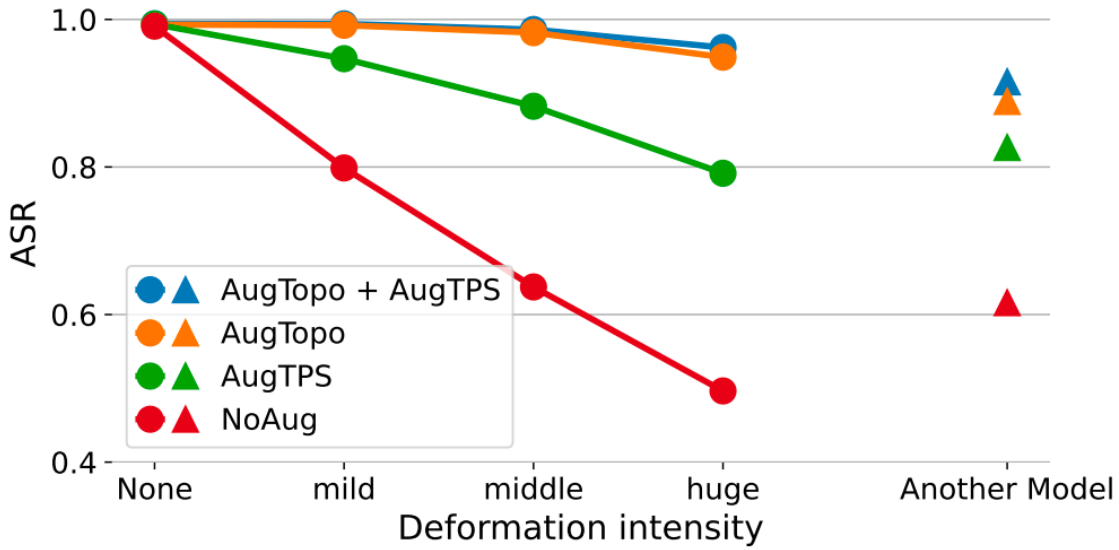
Images								
Score	6.08 ± 1.00	5.05 ± 1.39	2.05 ± 1.06	1.75 ± 1.09	1.72 ± 0.98	1.69 ± 0.95	2.54 ± 1.23	4.89 ± 1.39
Source	common texture	common camouflage	AdvPatch [38]	AdvTshirt [43]	AdvTexture yolo [19]	AdvTexture faster [19]	NatPatch [18]	AdvCaT (ours)

Result: Digital world

- Adversarial Success Rates (ASRs) with different IoU threshold

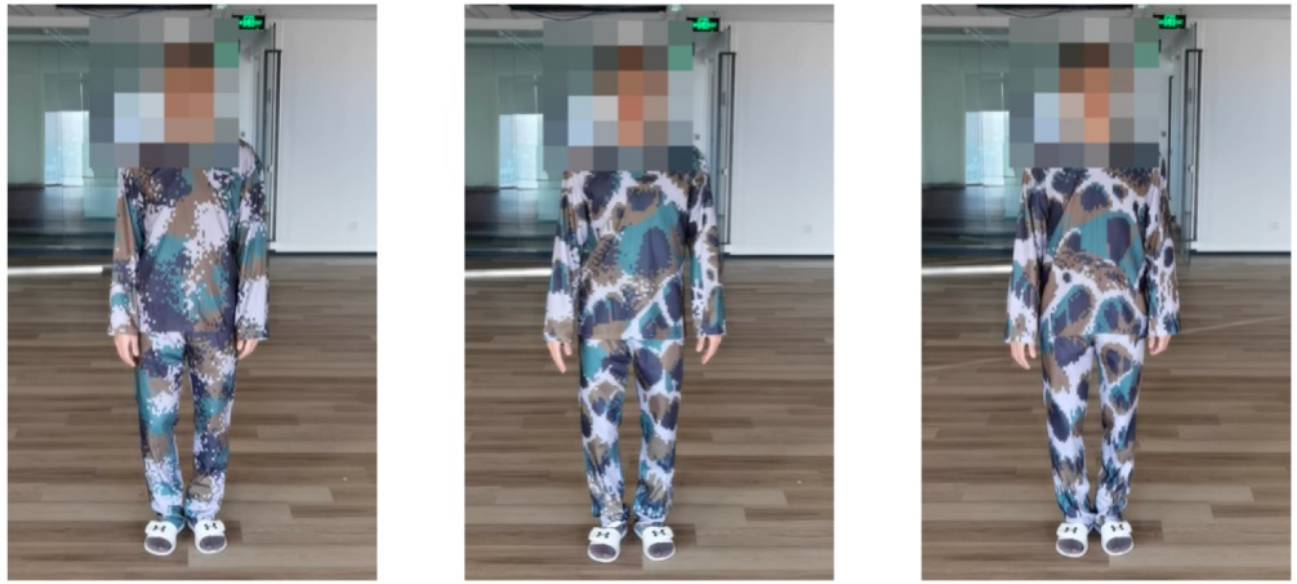
Method	IoU0.01	IoU0.1	IoU0.3	IoU0.5
RandColor	0.13	0.13	0.13	0.17
RandCaT	1.02	1.02	1.04	1.10
AdvPatch	69.33	72.27	75.80	85.97
NatPatch	42.47	43.66	45.41	67.40
AdvTexture	1.44	21.73	87.05	**99.98**
AdvCaT (ours)	**95.18**	**99.21**	**99.40**	99.52

- Ablation study of 3D augmentations



Result: Physical world

- Visualization and Attack Success Rates (ASRs)

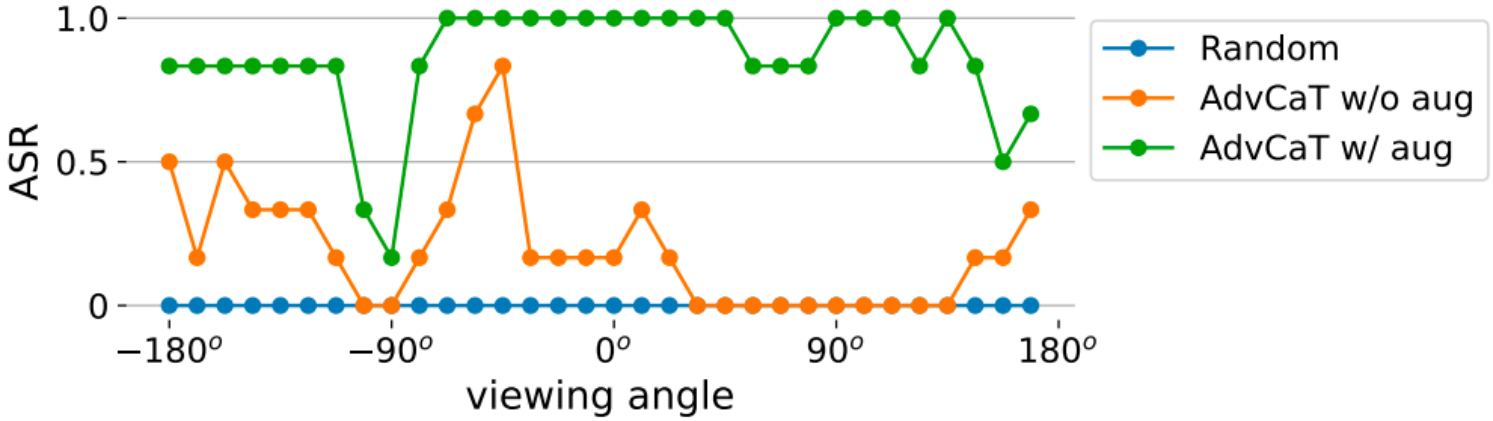


Random
ASR=0.00 %

AdvCaT w/o aug
ASR=19.27 %

AdvCaT w/ aug
ASR=85.94 %

- ASRs at different viewing angles



Result: Video demo

- Turning circles & twisting

Turning circles

Twisting

Thank you!

For more details, please look at our paper

Zhanhao Hu∗, Wenda Chu∗, Xiaopei Zhu, Hui Zhang, Bo Zhang, Xiaolin Hu

{huzhanha17, chuwd19, zxp18}@mails.tsinghua.edu.cn
fzyzhh@bift.edu.cn, {dcszb, xlhu}@mail.tsinghua.edu.cn