



iBRAIN
Intelligent BBrain Analysis
through Images and Networks

<http://ibrain.nuaa.edu.cn/>



Vision-Language Model IP Protection via Prompt-based Learning

Lianyu Wang, Meng Wang, Huazhu Fu, Daoqiang Zhang

IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2025.



Background

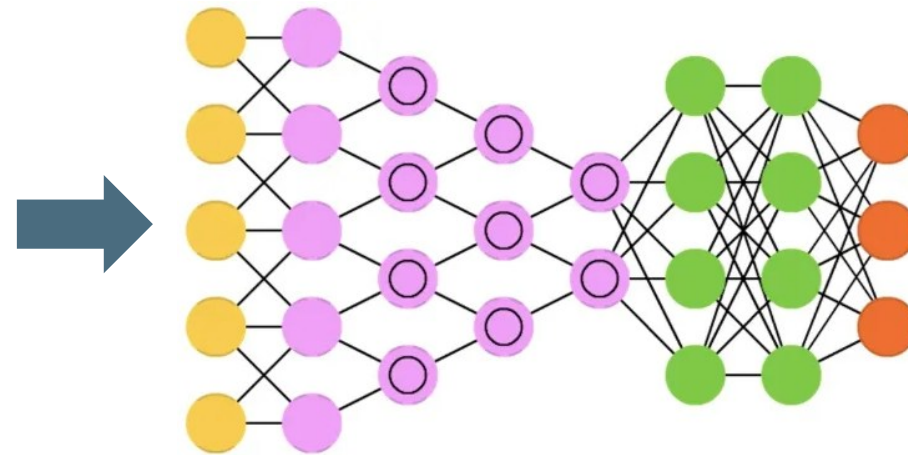
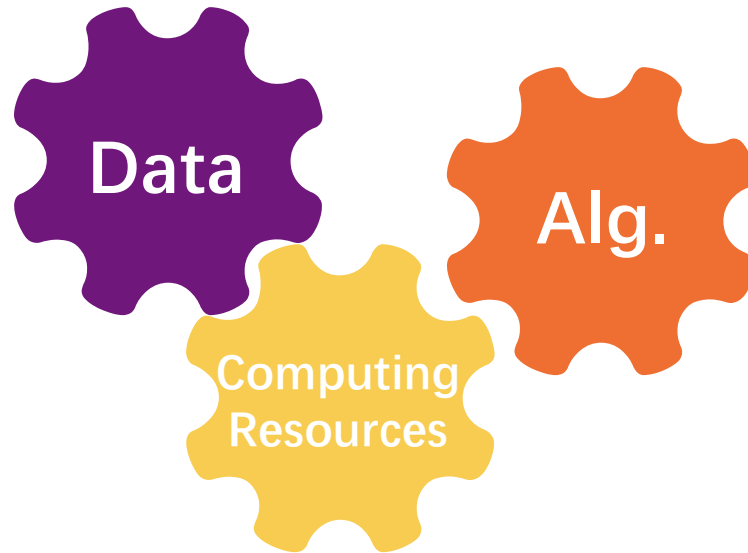
Autonomous
Driving



Smart Home
System



Intelligent
Healthcare



01

Intrinsic characteristics of models

high cost, easy replication

02

Innovation reward crisis

Deprivation of Recognition/Rewards, Discouraging innovation

03

Industry's vicious competition:

product homogenization, bottom-end competition

04

Global legislative trends

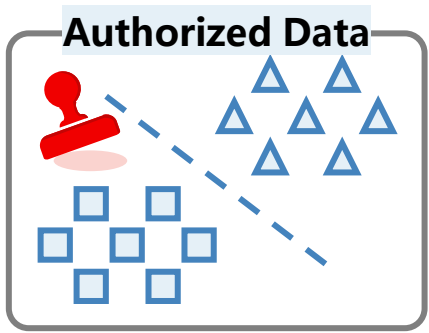
WIPO, China, EU, etc.

The Role of IP Protection



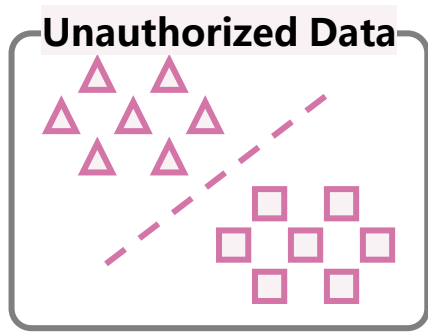
Innovator

Design and train the model.

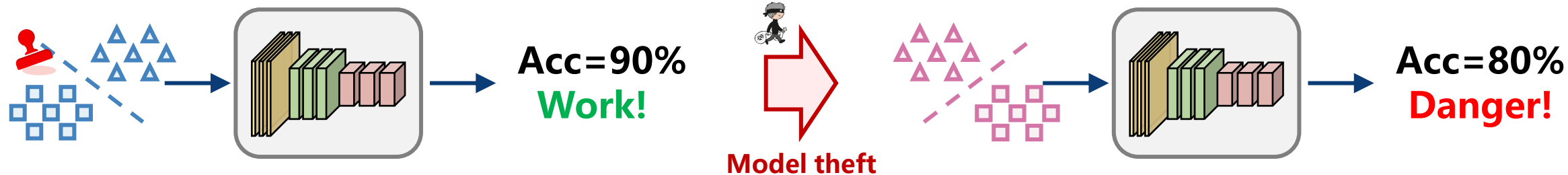


Thief

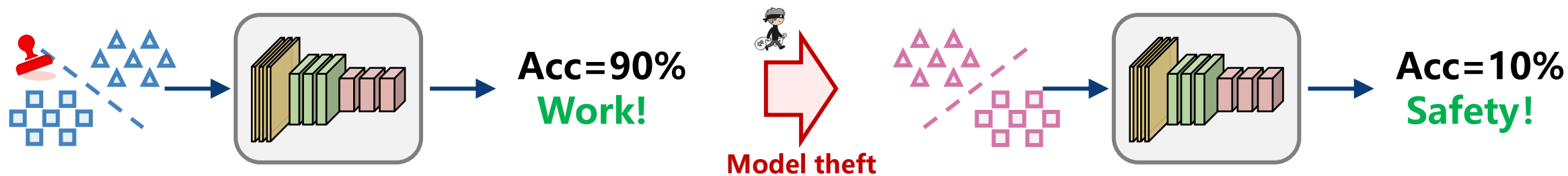
Stealing models or claiming ownership.



VLMs without IP protection



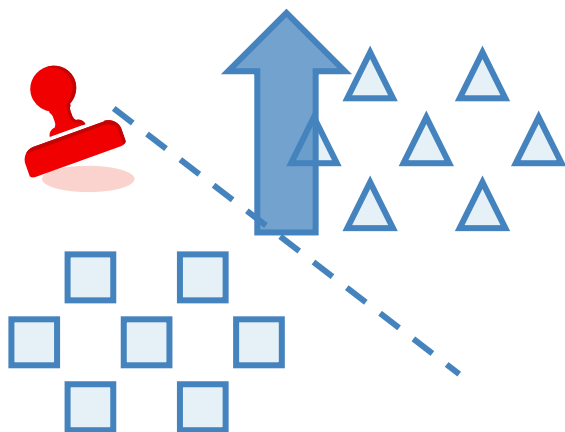
VLMs with IP protection



The Goals of IP Protection

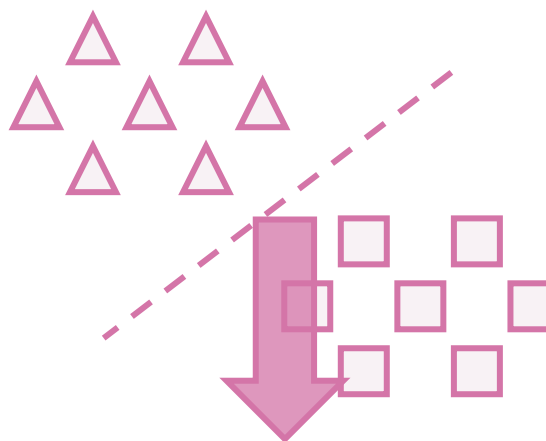
Target 1

Improve performance
on **authorized** data



Target 2

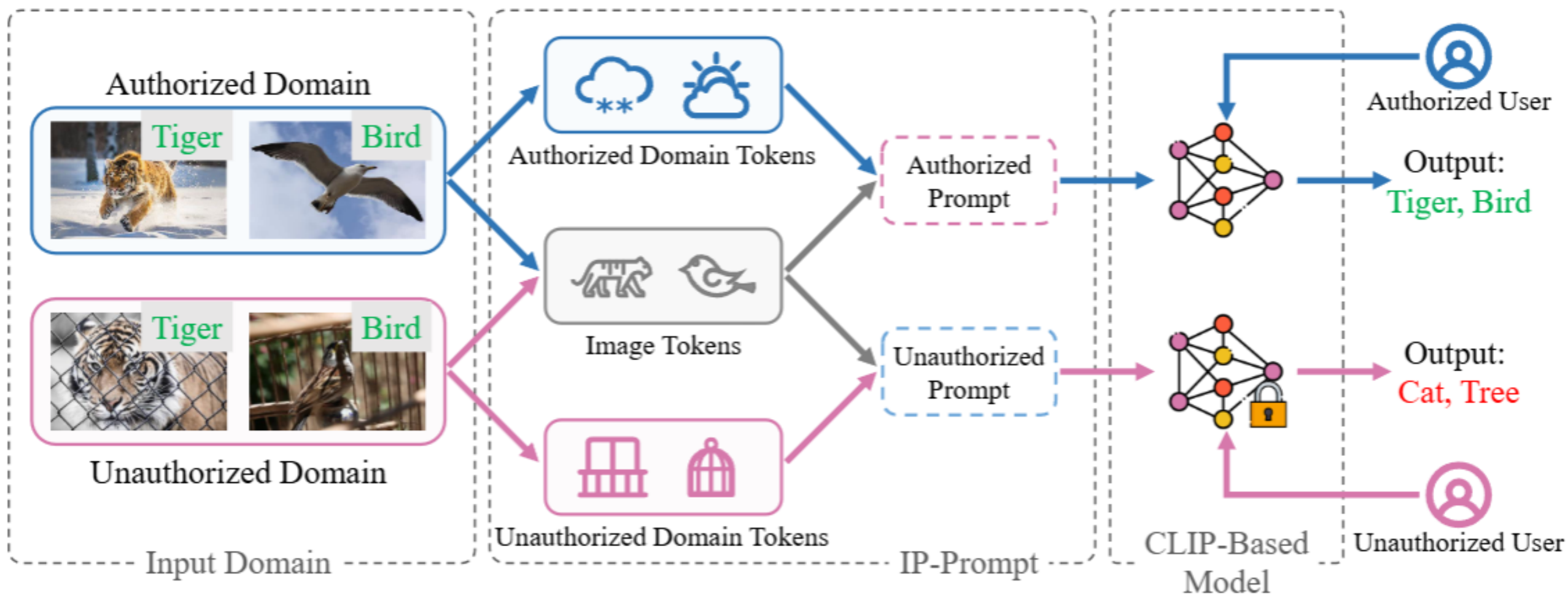
Reduce performance
on **unauthorized** data

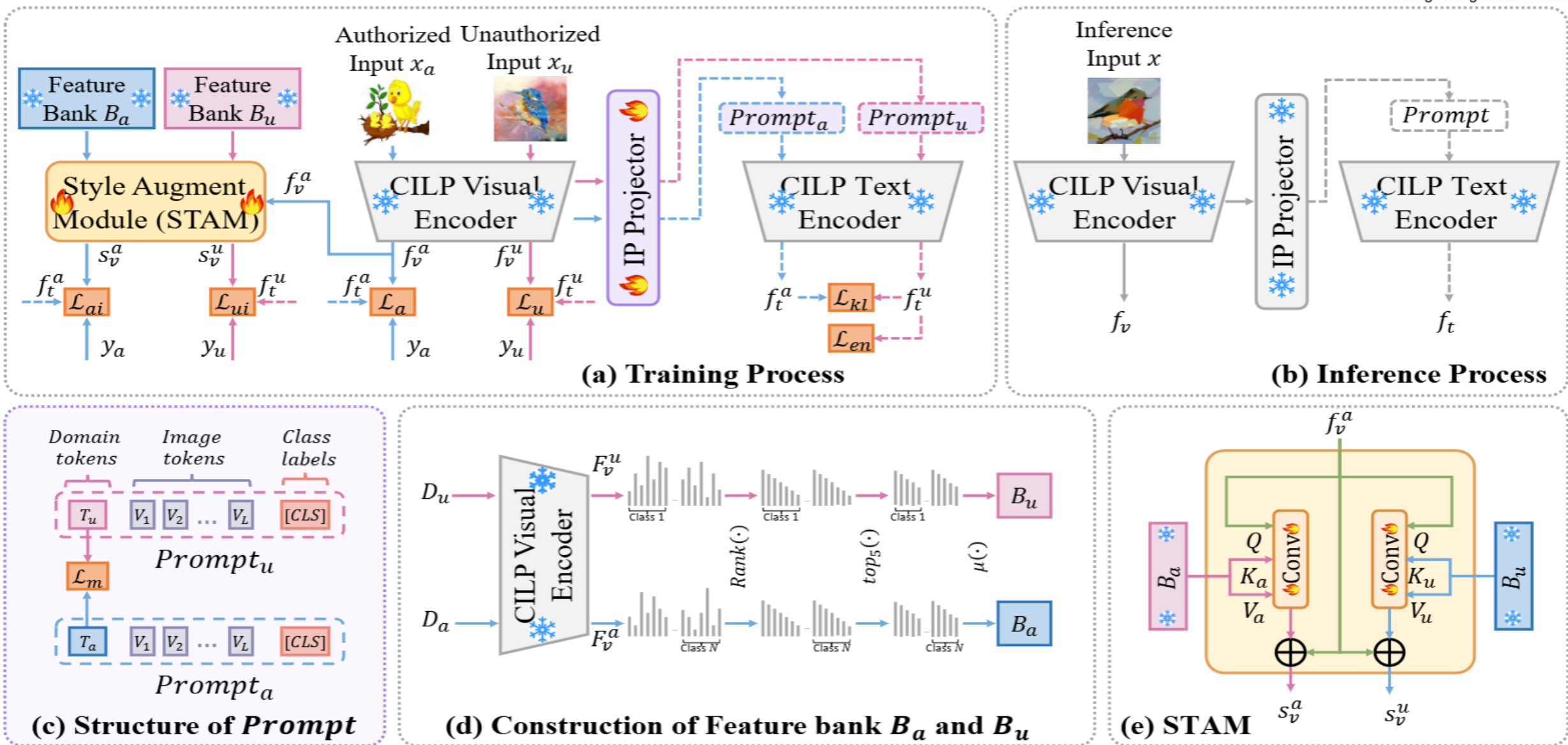


Target 3

Tracking **Illegal Use**

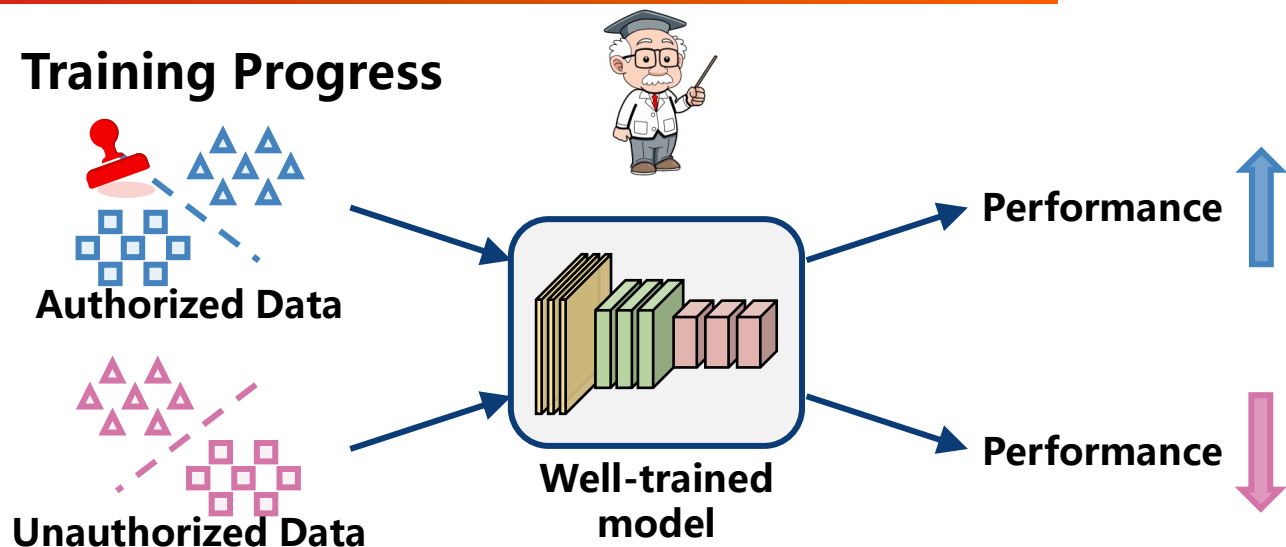




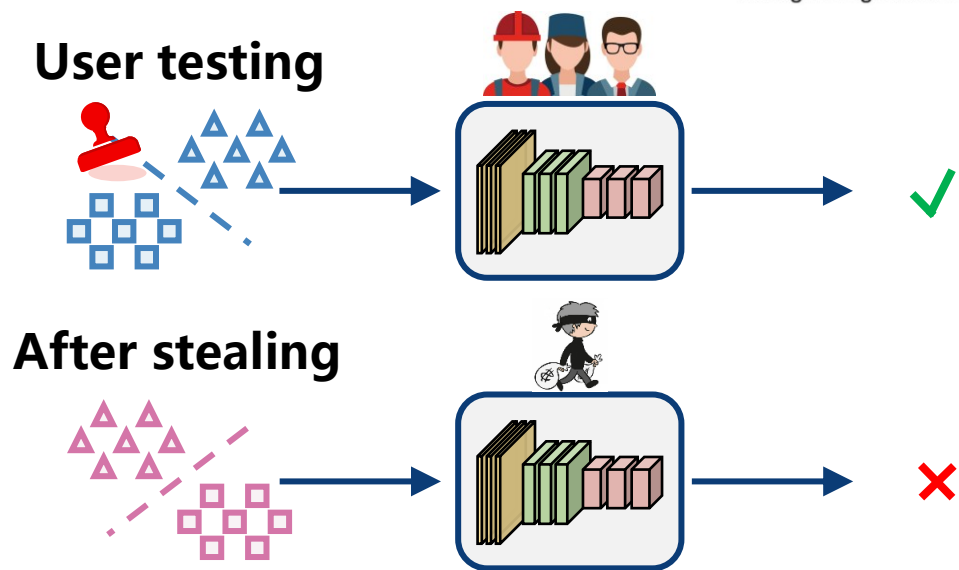


Scenario 1: Single-Domain IP Protection

Training Progress



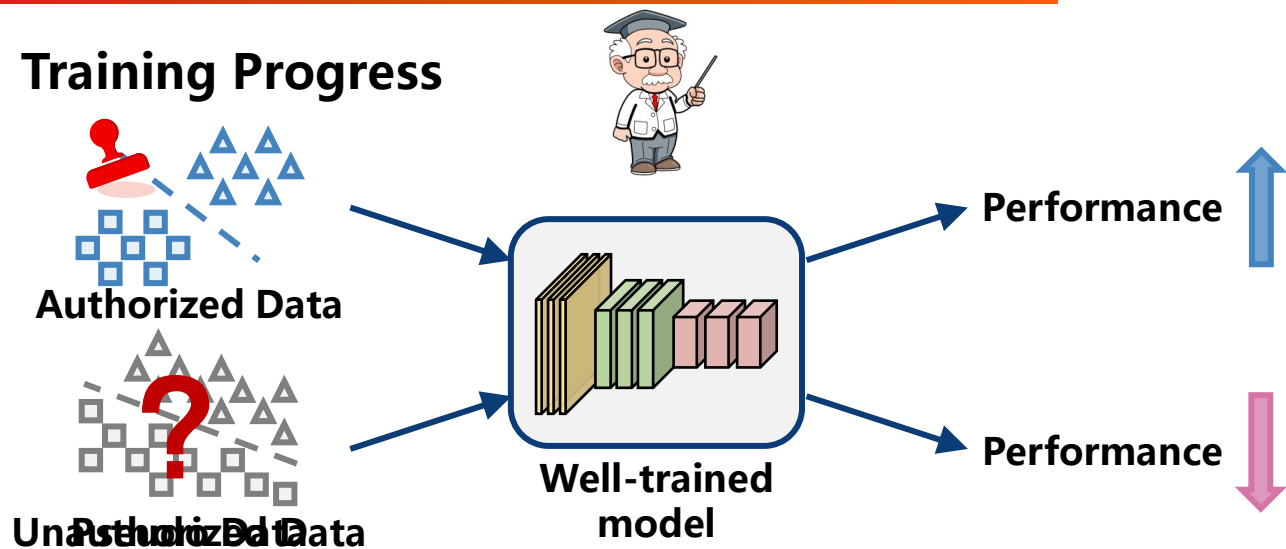
User testing



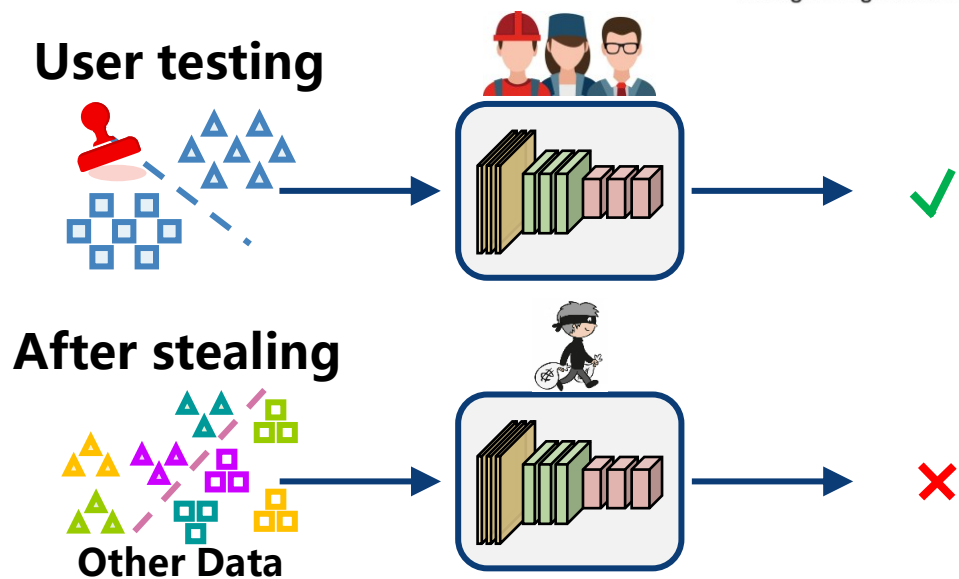
Datasets	Authorized Domain	$W_{ua} \uparrow$					$D_u \uparrow$					$D_a \downarrow$				
		NTL [27]	CUTI [28]	NLT [†] [27]	CUTI [†] [28]	IP-CLIP	NTL [27]	CUTI [28]	NLT [†] [27]	CUTI [†] [28]	IP-CLIP	NTL [27]	CUTI [28]	NLT [†] [27]	CUTI [†] [28]	IP-CLIP
Office-31 [25]	Amazon	41.37	60.94	56.34	62.06	63.52	55.50	74.40	75.80	79.35	80.00	3.10	0.80	1.80	0.60	0.00
	Dslr	70.94	75.33	76.09	80.13	82.54	74.20	81.90	77.35	85.05	86.25	1.55	0.80	1.30	0.70	0.00
	Webcam	74.02	74.02	32.50	75.24	78.45	75.80	38.70	75.80	84.38	83.10	0.00	0.00	3.10	2.50	0.00
	Mean	62.11	70.09	54.98	72.48	74.84*	68.50	76.32	65.00	82.93	83.12	1.55	0.53	2.07	1.27	0.00*
Office-Home-65 [26]	Art	27.53	35.62	13.44	41.58	52.00	37.27	47.16	15.83	53.40	61.33	0.80	0.30	0.10	3.00	0.30
	Clipart	43.23	45.67	48.83	53.37	56.45	54.31	57.35	65.67	72.40	75.47	0.20	0.20	0.30	0.63	0.10
	Product	41.31	41.78	39.90	56.82	58.71	45.01	45.82	43.00	61.83	63.77	0.30	0.50	0.00	0.37	0.30
	RealWorld	22.93	35.87	28.87	49.41	53.25	30.37	42.95	34.67	57.33	59.33	2.40	0.30	1.90	1.50	0.10
	Mean	33.75	39.73	32.76	50.29	55.10*	41.74	48.32	39.79	61.24	64.98*	0.43	0.33	0.57	1.38	0.20
Mini-DomainNet [33]	Clipart	25.63	30.29	38.62	50.26	51.47	36.60	40.87	46.30	59.40	61.00	2.10	0.80	0.60	0.20	0.30
	Painting	19.53	19.88	41.66	46.88	53.85	32.37	33.23	53.80	66.90	67.07	0.50	0.70	1.60	5.30	0.50
	Real	29.26	31.52	52.29	54.77	58.82	35.87	38.40	59.03	62.30	65.27	1.20	1.10	0.80	1.10	0.20
	Sketch	29.37	30.18	33.78	51.09	54.59	45.77	46.90	42.77	64.57	68.57	1.00	0.96	0.60	0.70	0.50
	Mean	25.95	27.97	41.59	50.75	54.68*	37.65	39.85	50.48	63.29	65.48*	1.27	0.87	1.00	2.20	0.33*

Scenario 2: Multi-Domain IP Protection

Training Progress



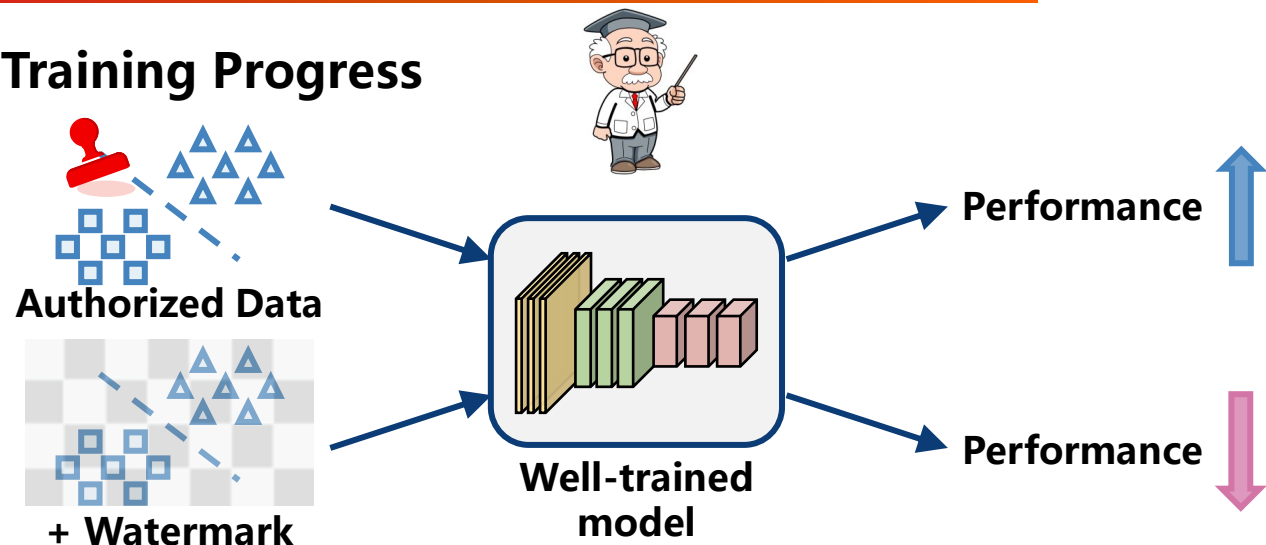
User testing



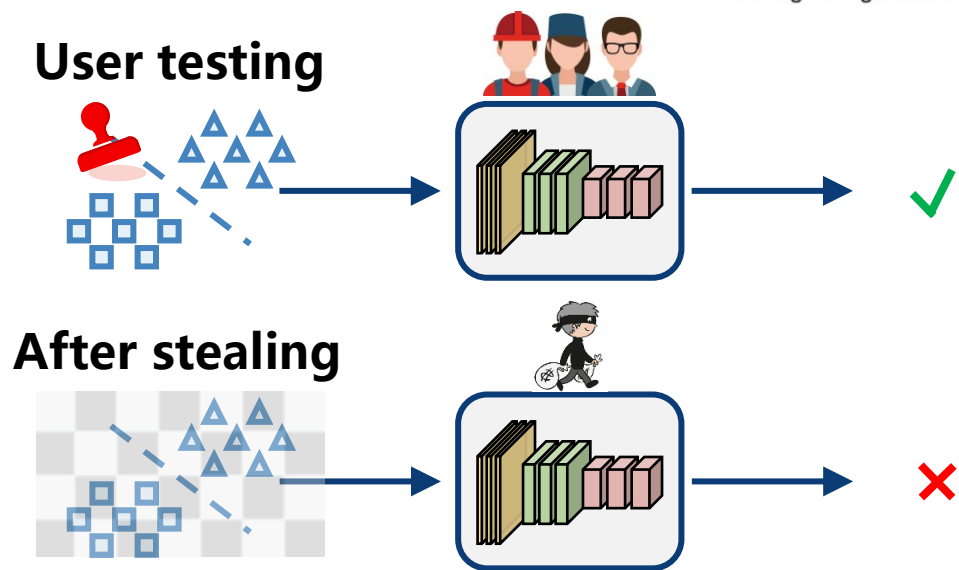
Datasets	Authorized Domain	$W_{ua} \uparrow$					$D_u \uparrow$					$D_a \downarrow$				
		NTL [27]	CUTI [28]	NTL [†] [27]	CUTI [†] [28]	IP-CLIP	NTL [27]	CUTI [28]	NTL [†] [27]	CUTI [†] [28]	IP-CLIP	NTL [27]	CUTI [28]	NTL [†] [27]	CUTI [†] [28]	IP-CLIP
Office-31 [25]	Amazon	0.56	4.69	11.90	25.60	50.32	7.80	13.30	17.25	36.65	64.10	7.05	7.05	1.90	3.10	0.40
	Dslr	6.88	6.83	36.72	38.83	44.89	9.40	9.35	43.90	43.30	47.50	2.30	2.30	3.90	1.90	0.40
	Webcam	2.90	2.95	45.80	30.95	65.17	8.60	5.45	50.95	33.60	72.35	5.45	2.35	1.60	0.60	1.90
	Mean	3.45	4.82	31.47	31.80	53.46*	8.60	9.37	37.37	37.85	61.32*	4.93	3.90	2.47	1.87	0.90
Office-Home-65 [26]	Art	0.10	-0.19	-0.71	-0.65	4.82	1.93	6.53	2.83	3.40	12.07	1.80	6.80	3.70	4.20	6.00
	Clipart	0.75	1.36	0.30	5.19	14.88	1.34	8.24	0.90	8.23	19.83	0.40	6.40	0.50	1.20	0.00
	Product	3.13	4.21	14.08	12.57	23.67	6.08	13.08	19.03	18.50	30.40	2.60	8.10	3.30	4.30	3.80
	RealWorld	2.39	3.72	13.07	3.82	20.41	2.83	8.83	17.67	5.50	22.93	0.00	4.20	2.70	1.20	0.20
	Mean	1.59	2.28	6.68	5.23	15.95*	3.05	9.17	10.11	8.91	21.31*	1.20	6.38	2.55	2.73	2.50
Mini-DomainNet [33]	Clipart	-3.25	-1.85	-0.89	2.24	2.95	11.80	5.30	3.50	7.07	7.63	17.30	8.00	4.60	4.30	4.00
	Painting	-0.52	0.27	0.39	0.21	0.97	7.53	3.87	4.40	3.57	3.93	8.50	3.40	3.90	3.30	2.70
	Real	2.60	2.05	4.46	5.86	13.77	5.73	6.00	9.37	8.93	18.13	2.60	3.50	4.20	2.30	2.50
	Sketch	2.44	-1.63	3.07	1.29	3.74	14.53	6.70	7.37	5.17	8.23	10.20	9.56	3.40	3.50	3.40
	Mean	0.32	-0.29	1.76	2.40	5.36*	9.90	5.47	6.16	6.18	9.48	9.47	4.97	4.23	3.30	3.07*

Scenario 3: Ownership Verification

Training Progress

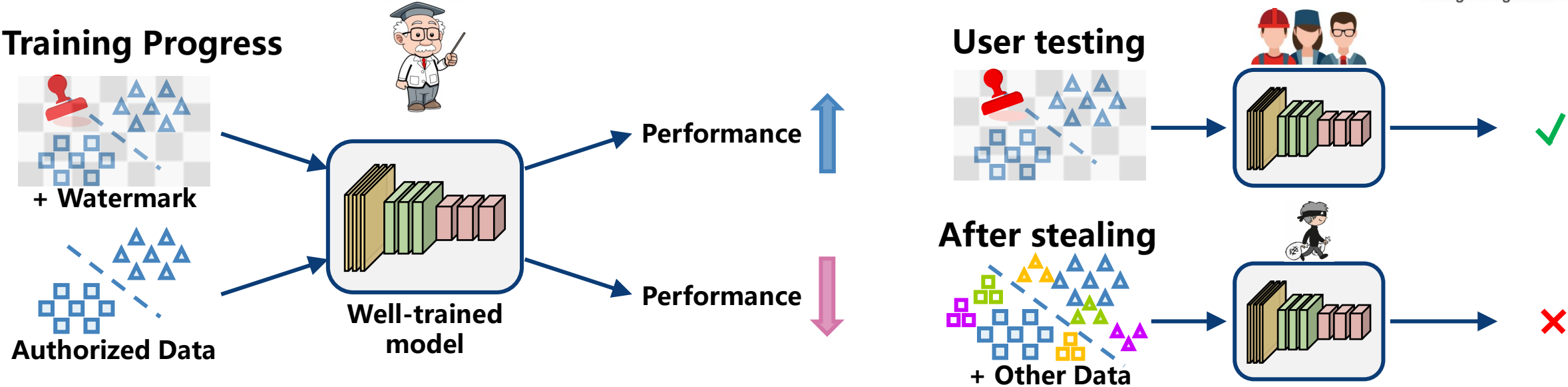


User testing



Datasets	Authorized with / without Patch	CNN-Based Models					CLIP-Based Models							
		SL-CNN A_u/A_a	NTL [27] A_u/A_a $O_{ua} \uparrow$		CUTI [28] A_u/A_a $O_{ua} \uparrow$		SL-CLIP [23] A_u/A_a	NTL [†] [27] A_u/A_a $O_{ua} \uparrow$		CUTI [†] [28] A_u/A_a $O_{ua} \uparrow$		IP-CLIP A_u/A_a $O_{ua} \uparrow$		
Office-31 [25]	Amazon	59.4 / 78.1	3.1 / 67.2	38.1	1.6 / 78.1	45.4	80.0 / 81.3	15.0 / 77.5	50.0	3.8 / 80.0	61.0	3.8	81.3	62.0
	Dslr	50.0 / 98.4	0.0 / 92.2	46.1	4.7 / 93.8	44.6	97.5 / 98.8	5.0 / 95.0	87.8	2.5 / 95.0	90.2	3.8	97.5	91.4
	Webcam	62.5 / 95.3	1.6 / 93.8	57.6	4.7 / 92.2	54.7	95.0 / 97.5	2.5 / 93.8	86.7	7.5 / 95.0	83.1	1.3	96.3	90.3
Office-Home-65 [26]	Art	54.7 / 76.8	1.6 / 45.6	24.1	1.6 / 76.0	40.7	83.5 / 85.5	16.5 / 87.3	59.1	6.0 / 87.0	67.6	5.0	87.5	68.9
	Clipart	70.8 / 78.1	1.6 / 54.9	37.7	3.1 / 69.0	46.7	73.8 / 74.3	5.5 / 73.5	50.2	17.0 / 73.3	41.5	5.5	73.5	50.2
	Product	65.9 / 92.2	2.3 / 69.8	44.5	2.6 / 91.1	58.3	90.5 / 94.0	60.5 / 92.5	29.0	31.0 / 93.0	56.1	2.0	92.8	82.2
	RealWorld	61.2 / 82.6	1.8 / 77.3	46.2	0.3 / 83.6	51.0	87.5 / 88.5	17.5 / 87.8	61.5	5.0 / 86.3	71.1	6.5	92.0	74.8
Mini-DomainNet [33]	Clipart	50.3 / 65.5	0.8 / 37.8	18.6	1.6 / 67.8	33.3	84.0 / 85.1	57.1 / 86.4	24.6	13.7 / 85.2	60.1	5.6	85.4	67.0
	Painting	39.6 / 57.6	0.8 / 46.1	17.9	1.0 / 56.9	22.1	79.5 / 81.9	31.1 / 80.0	38.9	4.1 / 78.8	59.4	4.1	81.1	61.2
	Real	50.2 / 82.6	0.0 / 40.3	20.2	0.5 / 83.2	41.5	88.9 / 89.4	26.2 / 91.9	58.4	11.4 / 92.1	71.7	5.9	89.7	74.5
	Sketch	57.6 / 63.5	0.3 / 57.4	32.9	0.7 / 61.3	34.9	81.0 / 81.0	39.7 / 79.7	32.4	4.8 / 79.7	60.7	2.5	79.1	62.0
Mean		/	/	34.9	/	43.0	/	/	52.6	/	65.7	/	71.3*	

Scenario 4: Applicability Authorization



Dataset	Authorized Domain	$D_{ua} \uparrow$					$A_u \downarrow$					$A_a \uparrow$				
		NTL [27]	CUTI [28]	NTL [†] [27]	CUTI [†] [28]	IP-CLIP	NTL [27]	CUTI [28]	NTL [†] [27]	CUTI [†] [28]	IP-CLIP	NTL [27]	CUTI [28]	NTL [†] [27]	CUTI [†] [28]	IP-CLIP
Office-31 [25]	Amazon	1.63	27.95	15.67	29.26	37.46	5.21	0.52	37.43	20.83	3.53	15.63	53.13	62.50	65.50	63.00
	Dslr	9.23	72.92	39.25	54.47	82.42	4.69	4.17	50.50	36.53	9.77	32.81	87.50	92.80	94.30	95.80
	Webcam	11.82	40.01	54.59	40.56	56.45	0.00	37.00	21.30	30.60	15.53	34.38	84.40	85.30	80.80	83.30
	Mean	7.56	46.96	36.50	41.43	58.78*	3.30	13.90	36.41	29.32	9.61*	27.60	75.01	80.20	80.20	80.70
Office-Home-65 [26]	Art	8.75	35.25	49.47	54.95	60.12	63.93	1.04	20.45	10.38	3.88	75.52	59.90	81.30	79.50	79.50
	Clipart	4.98	14.78	9.74	16.86	26.52	50.39	0.72	27.70	20.88	10.48	58.85	38.80	48.00	52.80	57.00
	Product	17.49	33.27	44.44	39.53	57.74	58.40	0.78	27.48	35.38	8.40	80.21	58.07	81.80	83.00	80.30
	RealWorld	15.83	3.15	51.50	62.87	71.17	64.97	31.32	19.20	7.83	5.20	83.85	39.32	82.00	83.30	87.00
	Mean	11.76	21.61	38.79	43.55	53.89*	59.42	8.46	23.71	18.61	6.99*	74.61	49.02	73.28	74.65	75.95*
Mini-DomainNet [33]	Clipart	11.96	13.75	38.45	22.77	50.88	58.06	60.53	17.54	44.08	7.35	74.18	78.13	71.40	74.60	75.10
	Painting	7.47	6.47	32.78	24.48	40.33	58.26	45.15	24.18	34.73	10.93	69.08	56.58	70.60	69.80	69.20
	Real	21.08	22.62	35.66	33.56	54.06	57.03	58.43	37.90	34.83	18.40	82.57	85.03	81.60	77.90	83.30
	Sketch	7.72	7.00	38.66	48.18	48.27	58.47	57.24	16.55	9.45	8.20	69.57	67.60	71.00	74.30	73.70
	Mean	12.06	12.46	36.39	32.25	48.39	57.96	55.34	24.04	30.77	11.22	73.85	71.83	73.65	74.15	75.33

Visualization

Label:	Computer	Candles	Flipflops	Exit Sign	Alarm Clock	Bottle	Desk Lamp
Image of Authorized Domain:							
CLIP:	Computer	Candles	Flipflops	Exit Sign	Alarm Clock	Bottle	Desk Lamp
IP-CLIP:	Computer	Candles	Flipflops	Exit Sign	Alarm Clock	Bottle	Desk Lamp
Image of Unauthorized Domain:							
CLIP:	Computer	Candles	Flipflops	Notebook	Alarm Clock	Bottle	Lamp Shade
IP-CLIP:	Clipboards	Flowers	Bottle	Refrigerator	Webcam	Push Pin	Screwdriver

- Framework: **IP-CLIP**
- Core: **Domain Token, Image Augmentation Branch**
- **Diverse Strategy** for Application Scenarios
- **Lightweight** Parameters
- **Adaptability** for Downstream Tasks

Vision-Language Model IP Protection via Prompt-based Learning

Lianyu Wang, Meng Wang, Huazhu Fu, Daoqiang Zhang

IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2025.

Paper: <https://arxiv.org/abs/2503.02393>

Code: <https://github.com/LyWang12/IP-CLIP>

Google scholar : <https://scholar.google.com/citations?user=0rPdR2oAAAAJ&hl=zh-CN>

Related researches:

- [1] Lianyu Wang, Meng Wang, Daoqiang Zhang, & Huazhu Fu. (2023). Model barrier: A compact un-transferable isolation domain for model intellectual property protection. *In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 20475-20484.
- [2] Lianyu Wang, Meng Wang, Huazhu Fu, & Daoqiang Zhang. (2024). Say No to Freeloader: Protecting Intellectual Property of Your Deep Model. *IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI)*, vol. 46, no. 12, pp. 11073-11086.