VICTOR: Dataset Copyright Auditing in Video Recognition Systems

Quan Yuan[1], Zhikun Zhang[1], Linkang Du[2], Min Chen[3], Mingyang Sun[4], Yunjun Gao[1], Shibo He[1], and Jiming Chen[1,5]

1 ZHEJIANG UNIVERSITY

2 XI'AN JIAOTONG UNIVERSITY

3 VU UNIVERSITY AMSTERDAM

4 PEKING UNIVERSITY

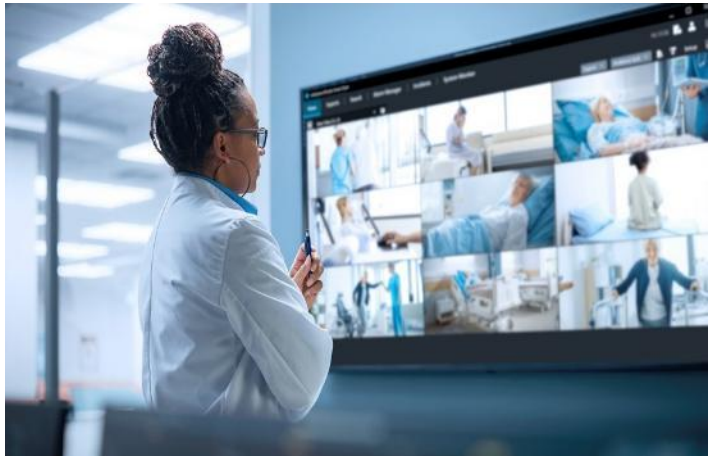
5 HANGZHOU DIANZI UNIVERSITY

Background

- Video recognition
  - Numerous applications

Autonomous driving

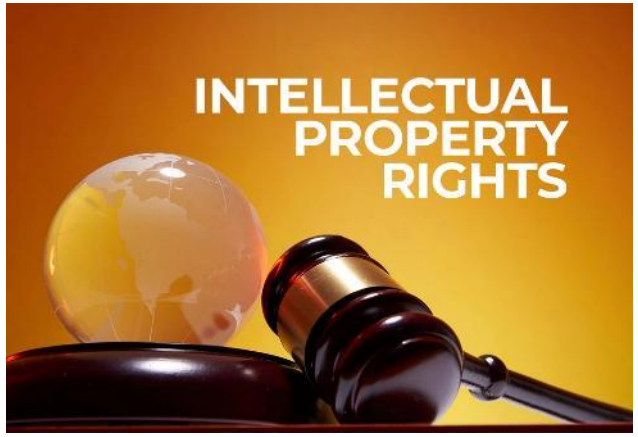
Security surveillance



Healthcare monitoring

Background

- Possible misuse
  - Privacy concerns



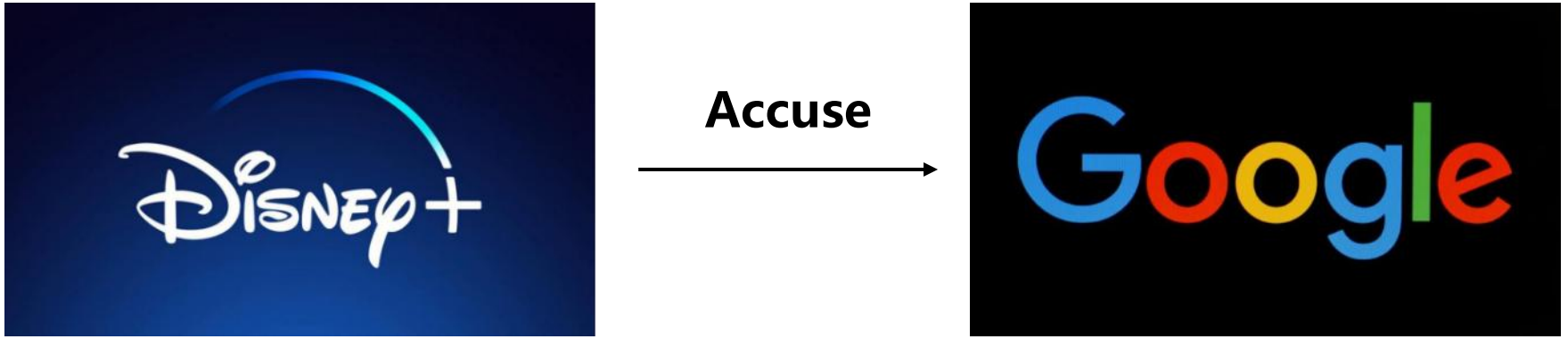
Intellectual property

Legal risk

Ethical issue

Background

- Copyright lawsuit
  - On December 10, 2025, Disney sent Google a cease-and-desist letter accusing its AI services of copyright infringement

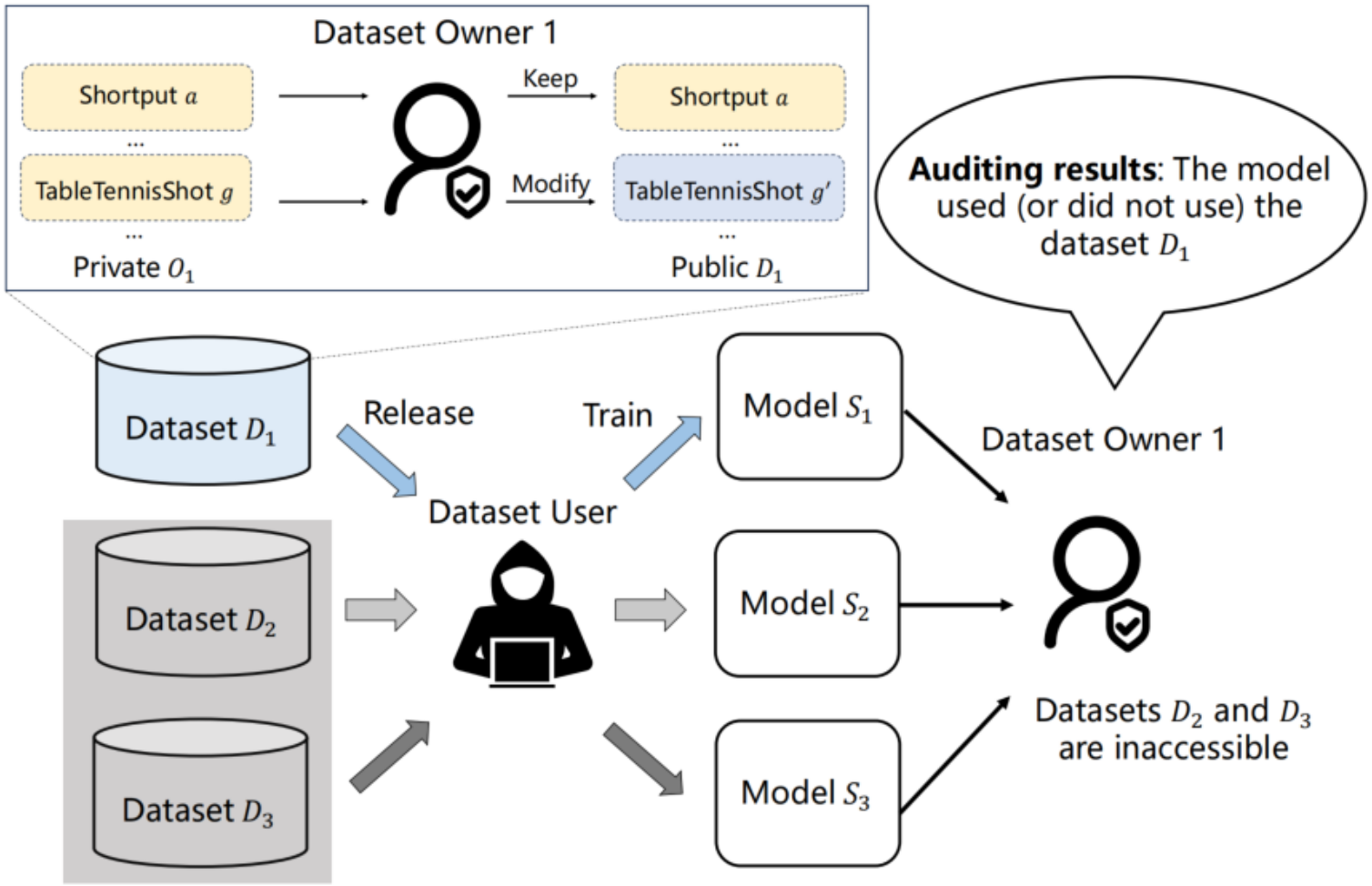


Disney **Google**

Dataset copyright auditing is important!

Problem Definition

- Dataset copyright auditing in video recognition



Method

Challenge

- Can image auditing methods apply to video?

Limitation

- **Flexible lengths**
- **Complex models**
- **Harmful backdoor**

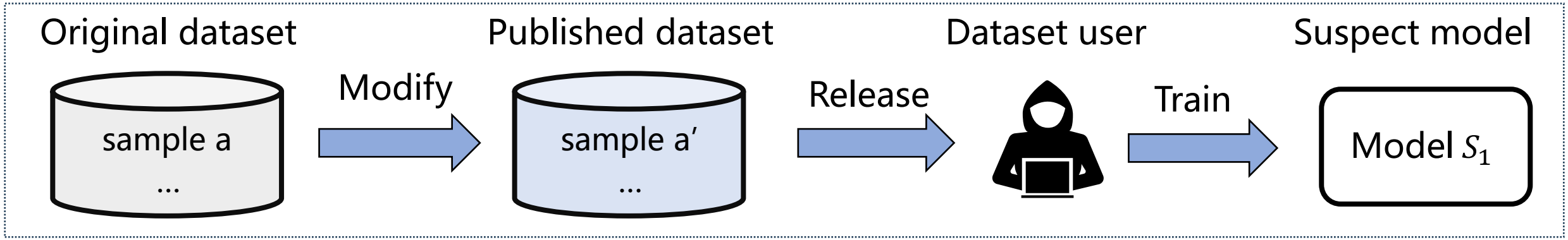
Our aim

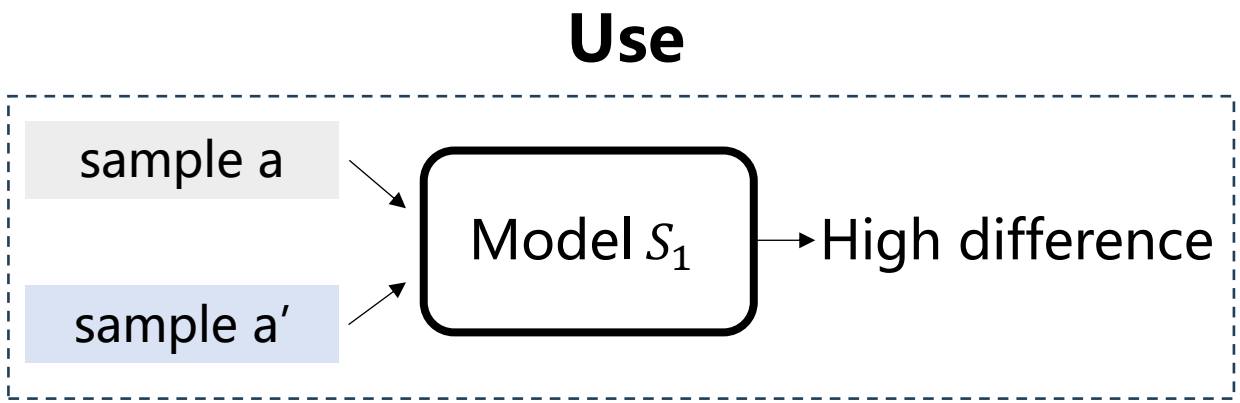
- **Low cost**
- **High robustness**
- **Harmless effect**

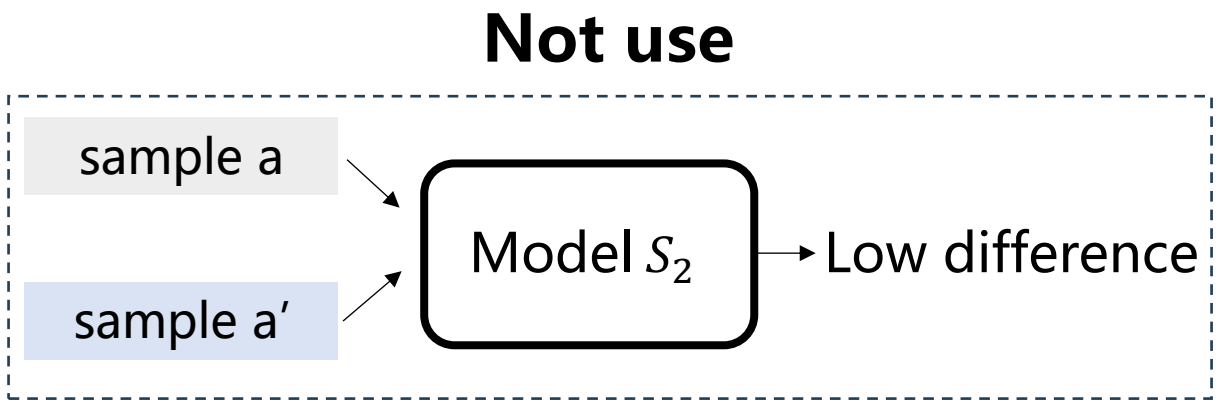
Method

Core idea

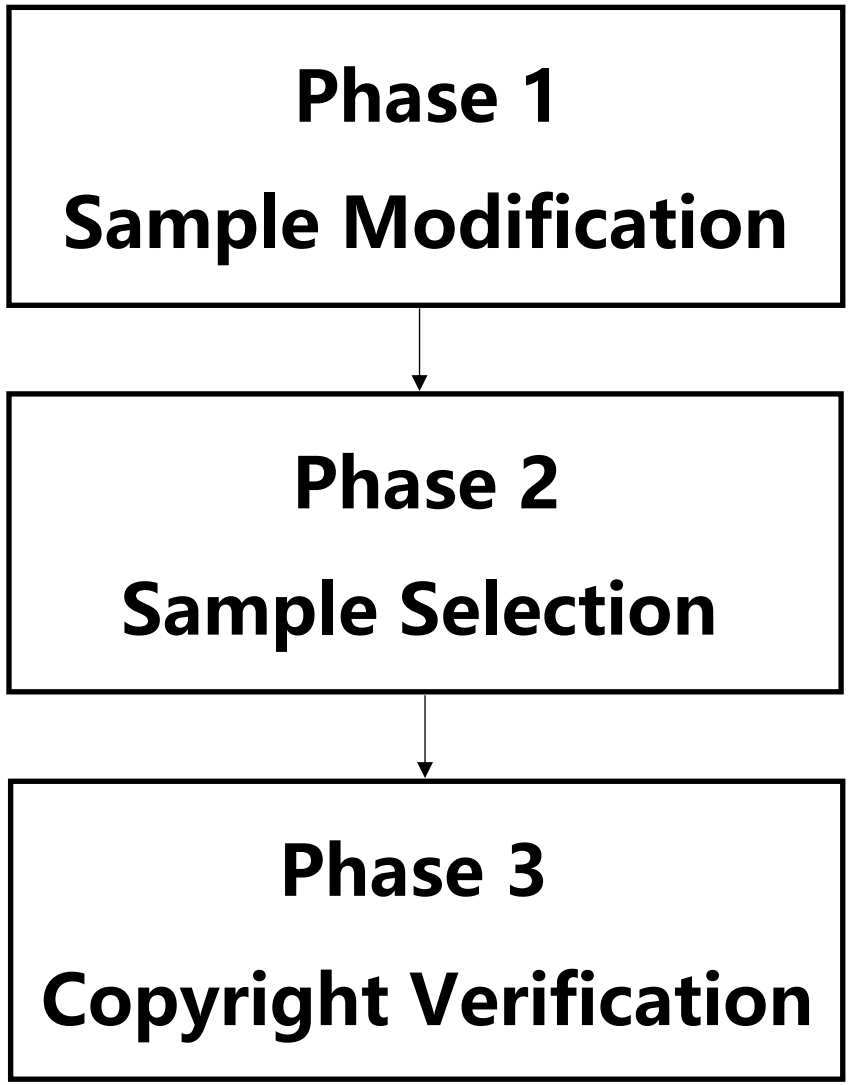
- Amplify the behavioral differences of the published samples





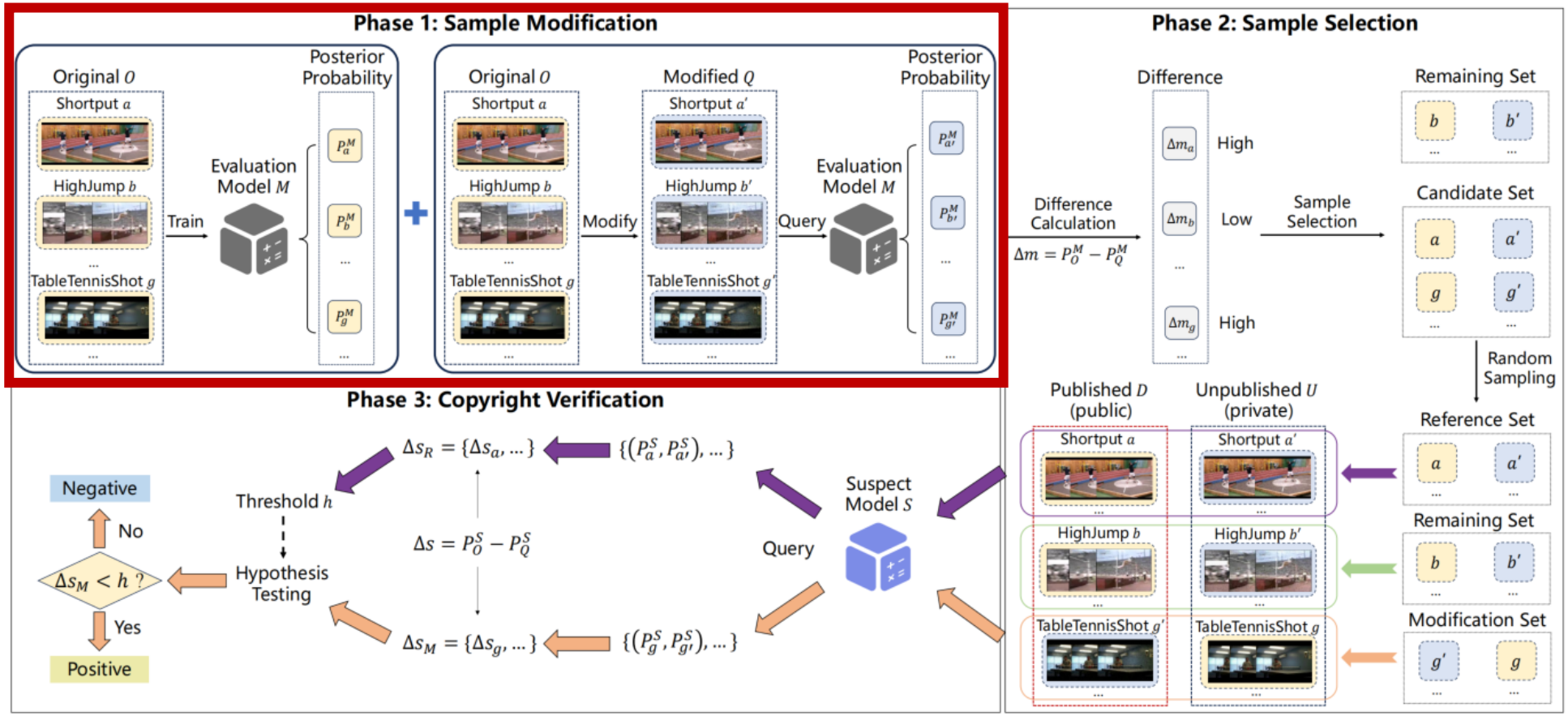


Workflow of VICTOR



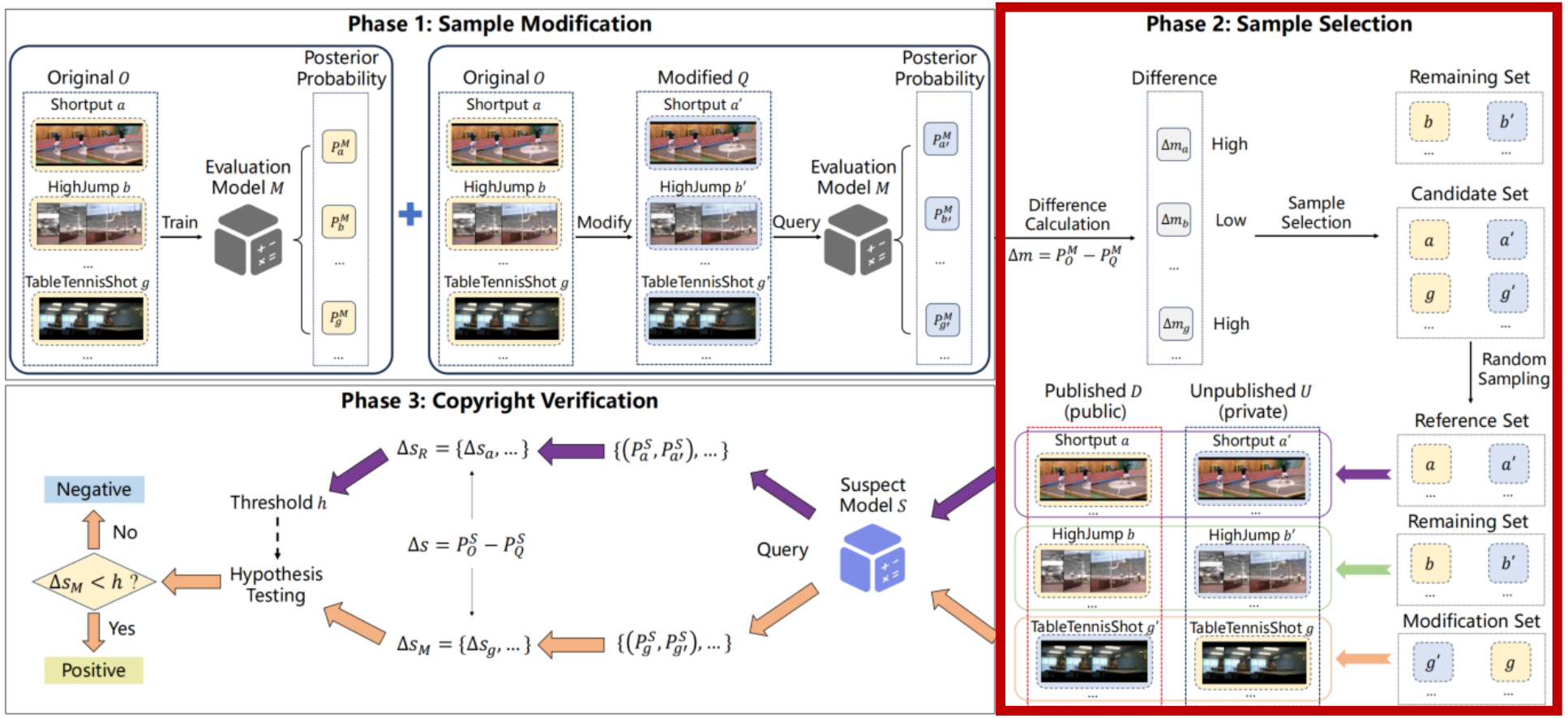
Workflow of VICTOR

- Phase 1: Sample Modification
- Phase 2: Sample Selection
- Phase 3: Copyright Verification



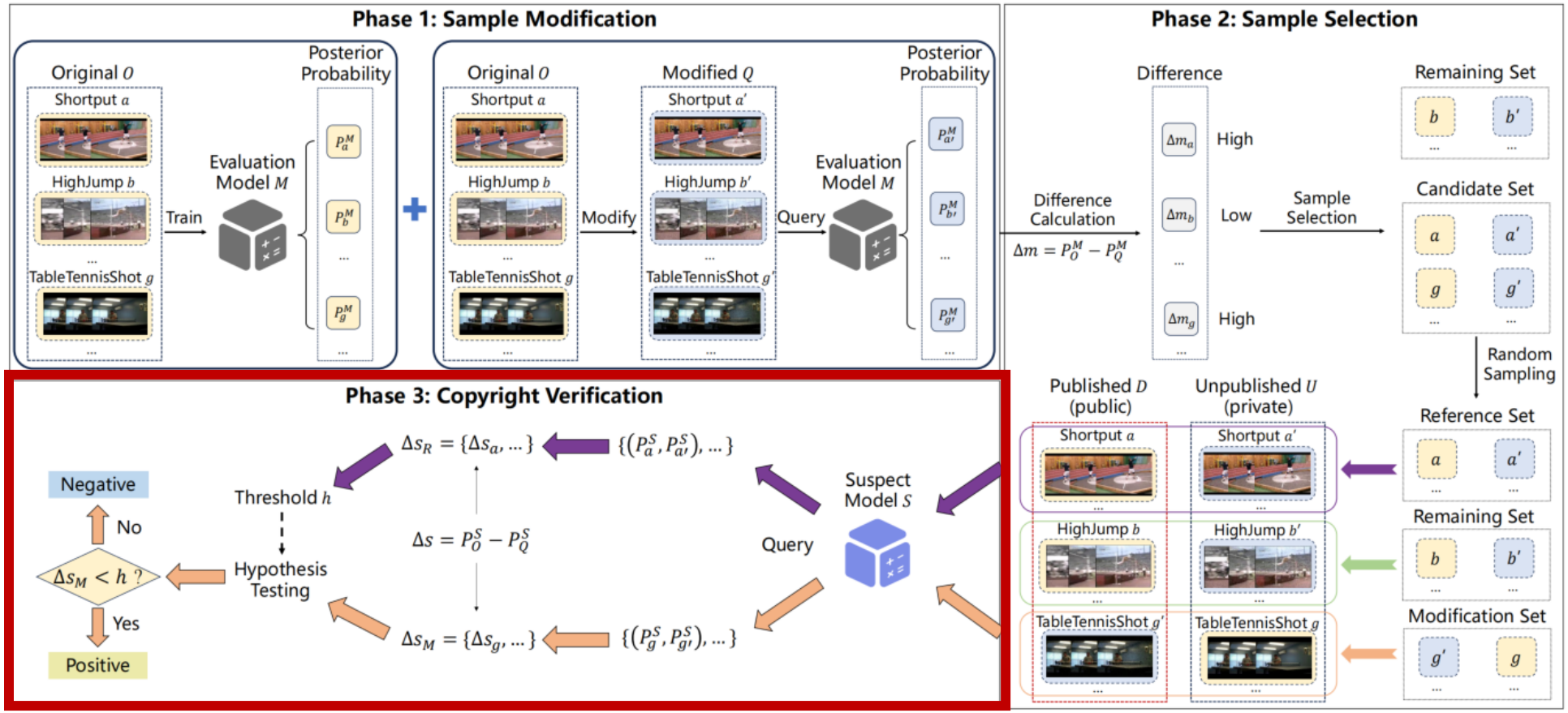
Workflow of VICTOR

- Phase 1: Sample Modification
- Phase 2: Sample Selection
- Phase 3: Copyright Verification



Workflow of VICTOR

- Phase 1: Sample Modification
- Phase 2: Sample Selection
- Phase 3: Copyright Verification



Experiment Setup

Dataset

- HMDB51: 6,849 videos, 51 categories
- UCF101: 13,320 videos, 101 categories
- SSv2: 220,847 videos, 174 categories

Model

- I3D: 3D CNN-based
- SlowFast: 3D CNN-based
- TSM: 2D CNN+RNN-based
- TimeSformer: Transformer-based

Experiment Setup

Metrics

- Δacc
- TPR
- F1 score
- FPR

Competitors

- ML-DA[1]
- MT[2]

[1] 2024 CCS A General Framework for Data-Use Auditing of ML Models

[2] 2025 CCS Anonymity Unveiled: A Practical Framework for Auditing Data Use in Deep Learning Models

Performance

◻ Overall auditing performance

Dataset	Model	I3D			SlowFast			TSM		
	Method / Metric	ML-DA [16]	MT [41]	VICTOR	ML-DA [16]	MT [41]	VICTOR	ML-DA [16]	MT [41]	VICTOR
HMDB-51	Δacc	-0.063	-0.065	**-0.020**	-0.072	-0.052	**-0.042**	-0.043	-0.044	**-0.032**
	TPR	0.400	**1.000**	**1.000**	0.000	**1.000**	**1.000**	0.000	**1.000**	**1.000**
	F1 Score	0.308	0.500	**1.000**	N/A	0.294	**1.000**	N/A	0.357	**1.000**
	FPR	0.120	0.200	**0.000**	**0.000**	0.480	**0.000**	0.100	0.360	**0.000**
UCF-101	Δacc	-0.024	-0.038	**-0.021**	-0.014	-0.036	**-0.012**	-0.015	-0.038	**-0.011**
	TPR	0.000	0.700	**1.000**	0.000	0.800	**1.000**	0.000	0.800	**1.000**
	F1 Score	N/A	0.609	**1.000**	N/A	0.229	**1.000**	N/A	0.889	**1.000**
	FPR	0.040	0.060	**0.000**	0.210	0.520	**0.000**	**0.000**	**0.000**	**0.000**

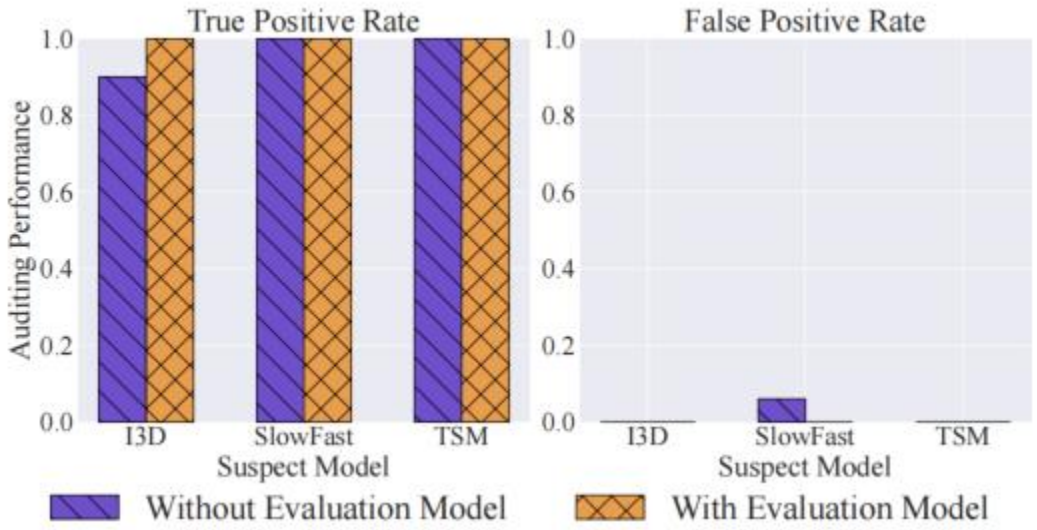
Remarks

- VICTOR achieves great performance across various models and datasets
- MT performs better than ML-DA, but exhibits obvious distortion

Performance

◻ Effectiveness of evaluation model

Dataset: UCF101



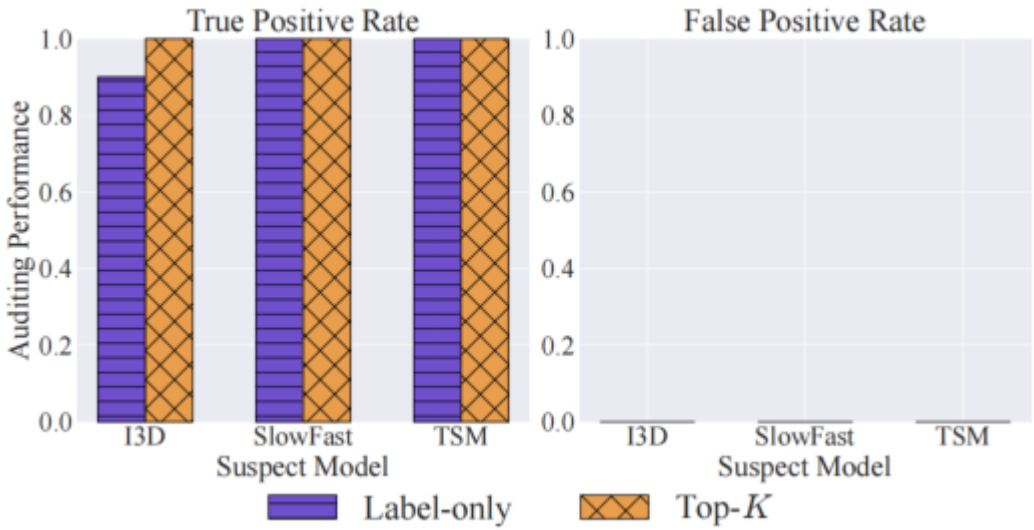
Remarks

- The evaluation model is helpful to enhance auditing effectiveness
- VICTOR can still achieve competitive performance without the evaluation model

Performance

◻ Top-K and label-only settings

Dataset: UCF101



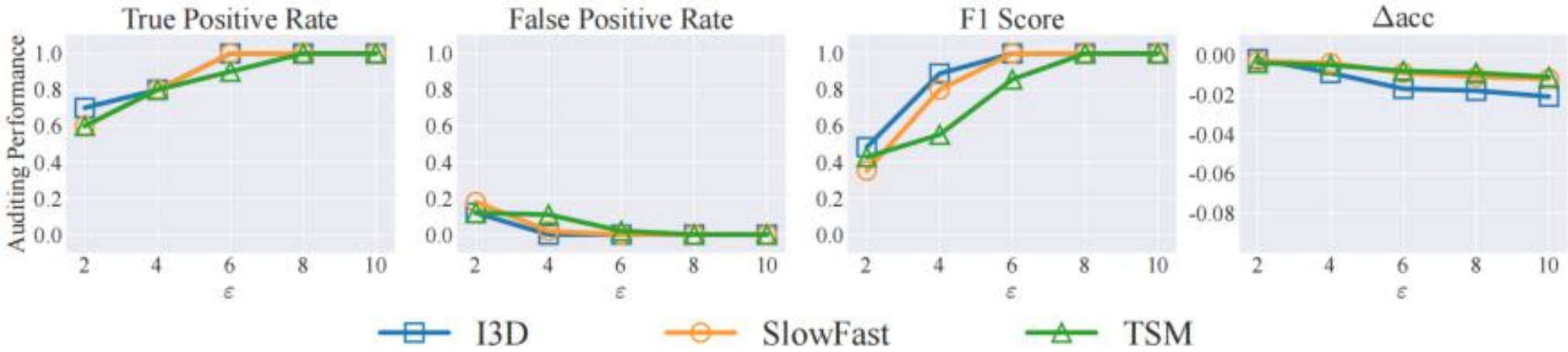
Remarks

- High TPR
- Low FPR

Performance

◻ Impact of perturbation budget

Dataset: UCF101



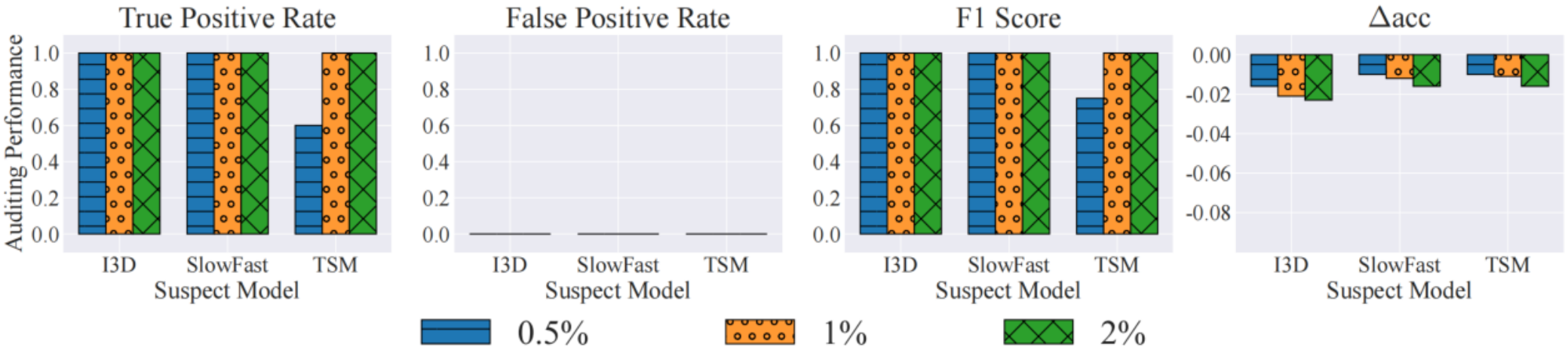
Remarks

- Higher budget, better auditing performance
- When $\varepsilon \geq 6$, VICTOR can obtain promising auditing performance

Performance

◻ Impact of modification ratio

Dataset: UCF101



Remarks

- VICTOR maintains a high level of auditing accuracy
- Tradeoff between auditing accuracy and normal performance

Performance

◻ Robustness to input perturbation

Dataset	Metric \ Model	I3D	SlowFast	TSM
HMDB-51	Δacc	-0.053	-0.068	-0.052
	TPR	1.000	0.900	0.900
	F1 Score	1.000	0.947	0.947
	FPR	0.000	0.000	0.000
UCF-101	Δacc	-0.060	-0.045	-0.028
	TPR	1.000	1.000	1.000
	F1 Score	1.000	1.000	1.000
	FPR	0.000	0.000	0.000

Remarks

- TPR slightly decreases, low FPR
- Accuracy for normal tasks shows greater reduction

Performance

Robustness to early stopping

Dataset	Metric \ Model	I3D	SlowFast	TSM
HMDB-51	Δacc	-0.162	-0.361	-0.185
	TPR	0.500	0.300	0.400
	F1 Score	0.667	0.462	0.571
	FPR	0.000	0.000	0.000
UCF-101	Δacc	-0.160	-0.388	-0.073
	TPR	1.000	0.600	1.000
	F1 Score	1.000	0.750	1.000
	FPR	0.000	0.000	0.000

Remarks

- TPR decreases, low FPR
- Accuracy for normal tasks shows significant reduction

Performance

◻ Robustness to post-adjustment

Dataset	Type	Fine-tuning			Model pruning			Output noise		
	Model / Metric	I3D	SlowFast	TSM	I3D	SlowFast	TSM	I3D	SlowFast	TSM
HMDB-51	Δacc	-0.032	-0.018	-0.047	-0.370	-0.396	-0.424	-0.181	-0.287	-0.222
	TPR	0.800	1.000	0.900	0.500	0.100	0.600	1.000	0.800	0.900
	F1 Score	0.889	1.000	0.947	0.667	0.182	0.750	1.000	0.889	0.947
	FPR	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
UCF-101	Δacc	-0.041	-0.002	-0.011	-0.593	-0.582	-0.616	-0.156	-0.185	-0.126
	TPR	1.000	0.900	1.000	1.000	0.900	1.000	1.000	1.000	1.000
	F1 Score	1.000	0.947	1.000	1.000	0.947	1.000	1.000	1.000	1.000
	FPR	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

Remarks

- TPR decreases, low FPR
- Accuracy for normal tasks shows significant reduction

Conclusion

- The first dataset copyright auditing approach for video recognition systems
- A label-invariant perturbation mechanism and a behavior difference-based verification to enable effective auditing
- An extensive evaluation on multiple datasets and models to illustrate the effectiveness and robustness of VICTOR

VICTOR: Dataset Copyright Auditing in Video Recognition Systems

Full paper

Thank you for your attention!