PECAM: Privacy-Enhanced Video Streaming and Analytics via Securely-Reversible Transformation

Hao Wu[1], Xuejin Tian[1], Minghao Li[1 2], Yunxin Liu[3], Ganesh Ananthanarayanan[4], Fengyuan Xu[1*], and Sheng Zhong[1]

[1]*Nanjing University*

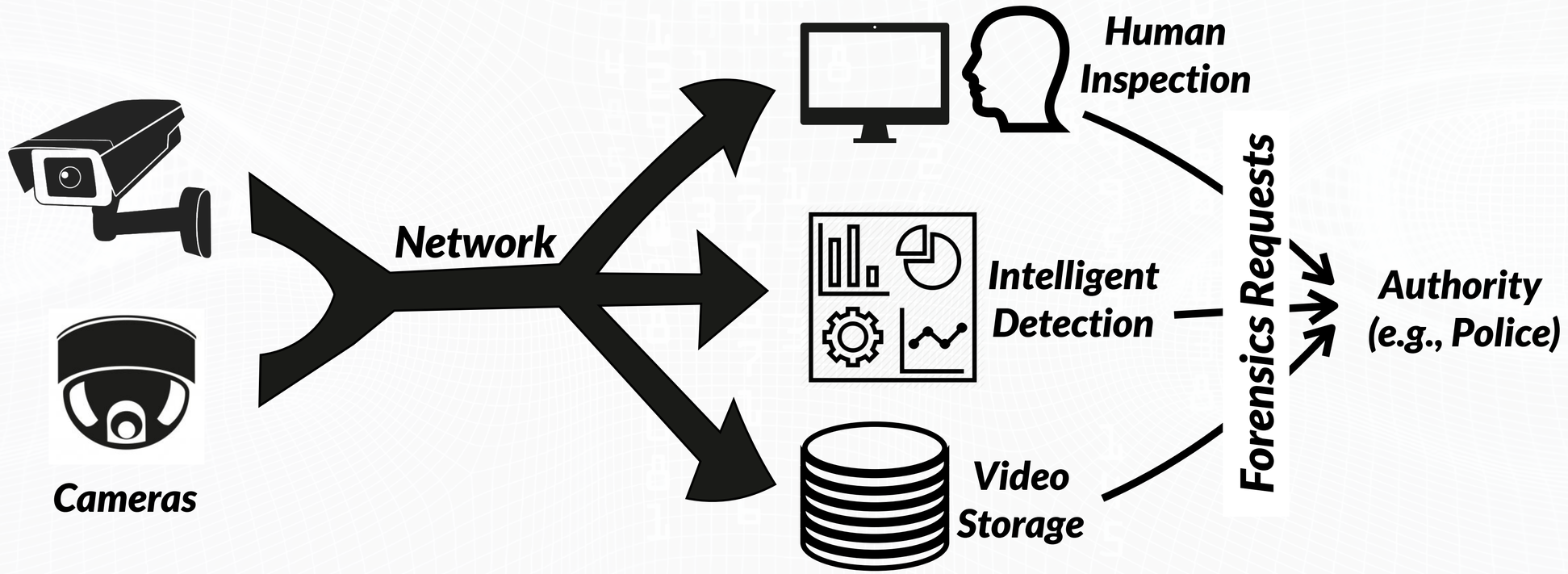
[2]*Cornell University*

[3]*Microsoft Research*

[4]*Microsoft Azure for Operators*

**Corresponding author: fengyuan.xu@nju.edu.cn*

VSA brings privacy concerns



A typical Video Streaming & Analytics (VSA) system.

Laws and regulations about data protection

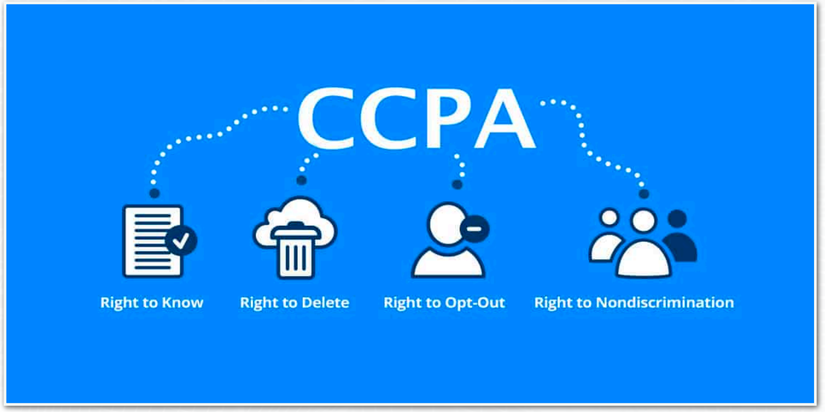

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

EU's Laying Down Harmonised Rules on AI and Amending Certan Union Legislative Acts



California Consumer Privacy Act (CCPA)

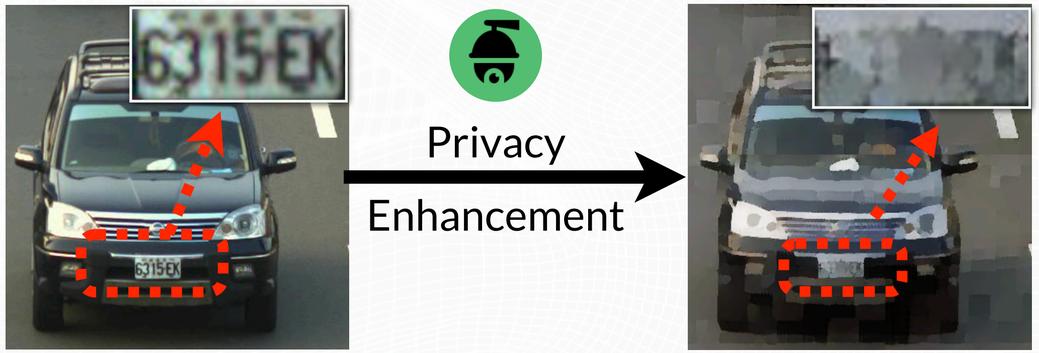
EU's GDPR


全 国 人 民 代 表 大 会
The National People's Congress of the People's Republic of China
首页 | 宪法 | 人大机构 | 栗战书委员长 | 代表大会会议 | 常委会会议 | 委员长会议 | 权威发布 | 立法 | 监督 | 代表
对外交往 | 选举任免 | 法律研究 | 理论 | 机关工作 | 地方人大 | 图片 | 视频 | 直播 | 专题 | 资料库 | 国旗 | 国歌 | 国徽
当前位置： 首页
中华人民共和国数据安全法
(2021年6月10日第十三届全国人民代表大会常务委员会第二十九次会议通过)

Data Security Law (DSL) of the People's Republic of China

Privacy Protection Requirements

A case in the traffic scenario:

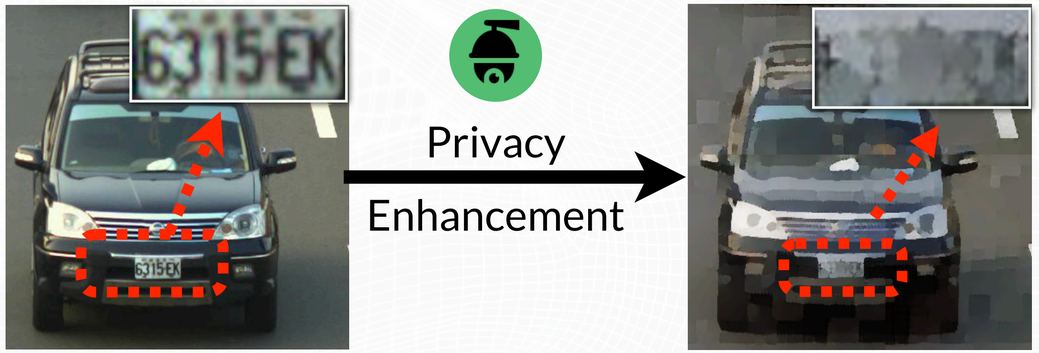


Original frame

Protected frame

Privacy Protection Requirements

A case in the traffic scenario:



Original frame

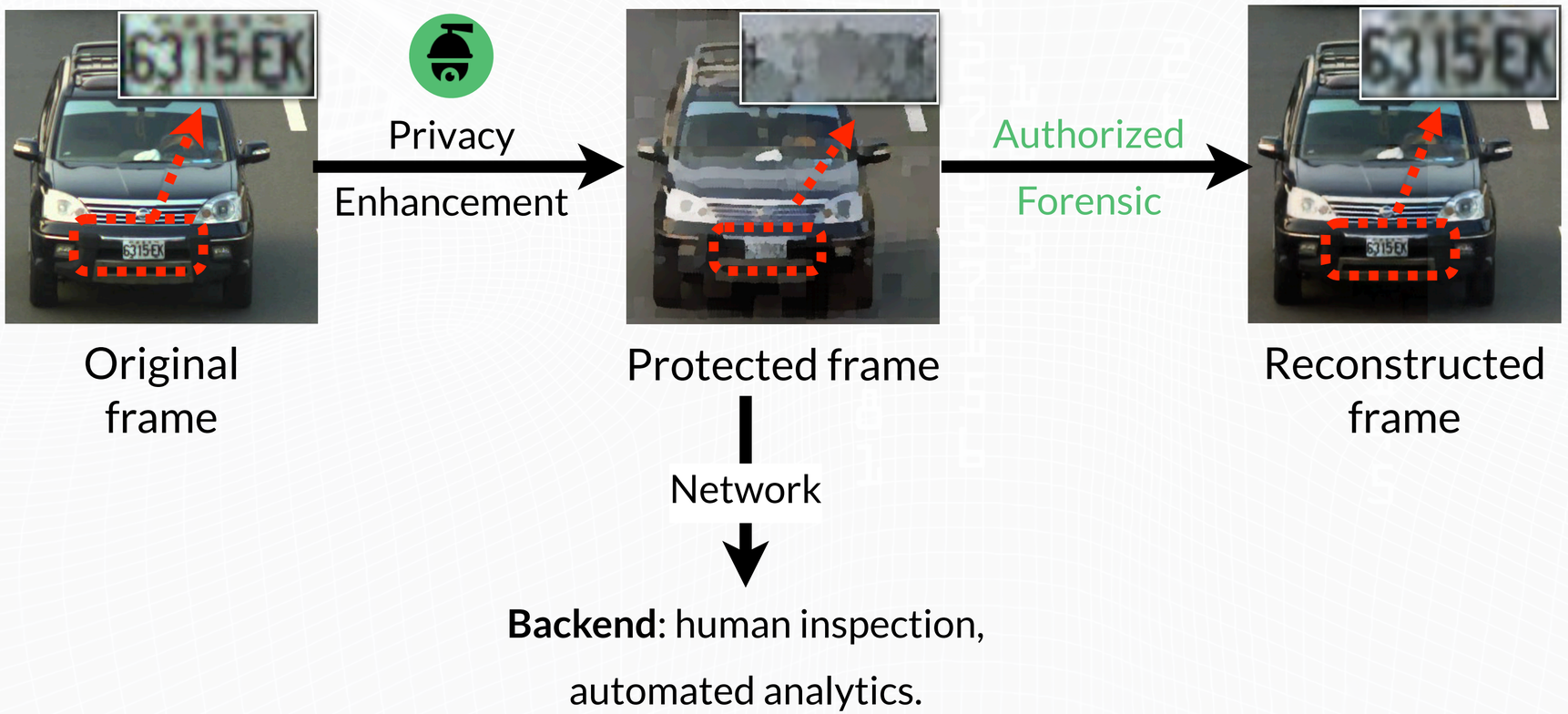
Protected frame

Network

Backend: human inspection, automated analytics.

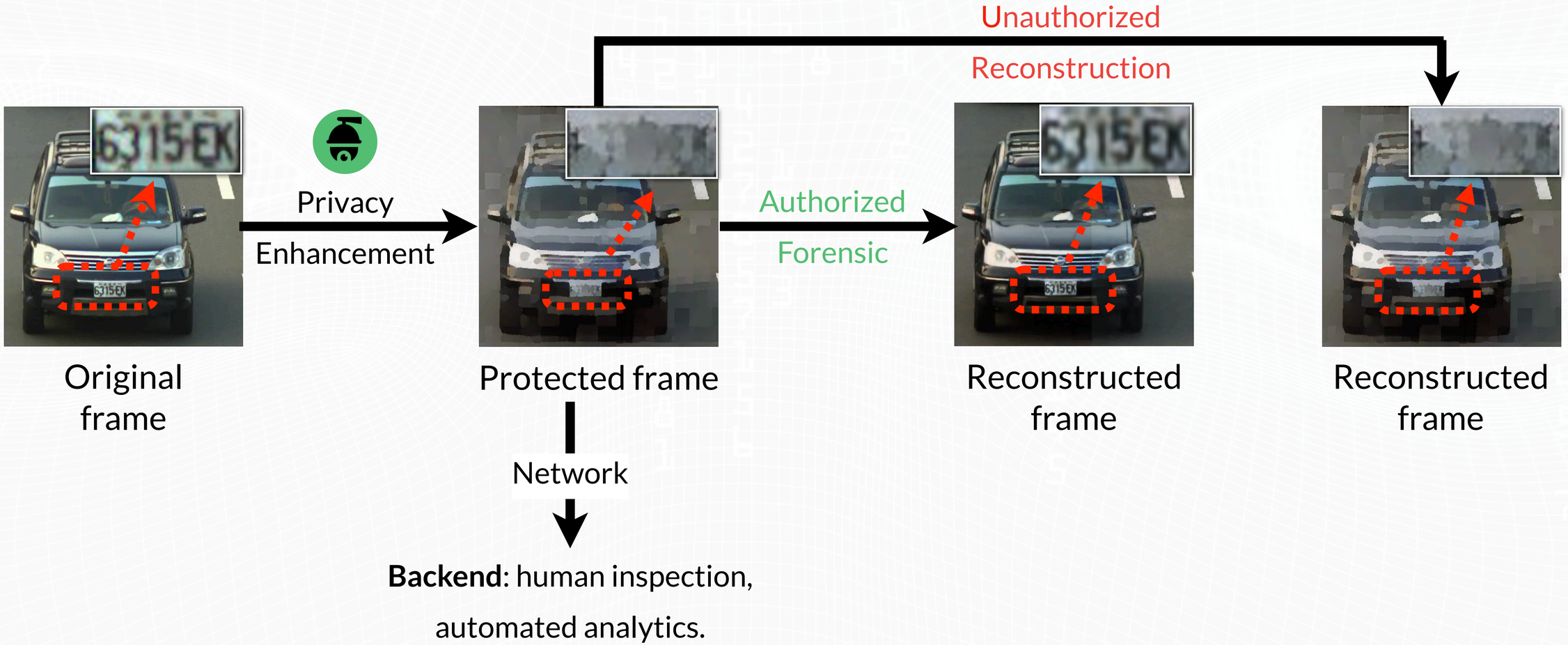
Privacy Protection Requirements

A case in the traffic scenario:



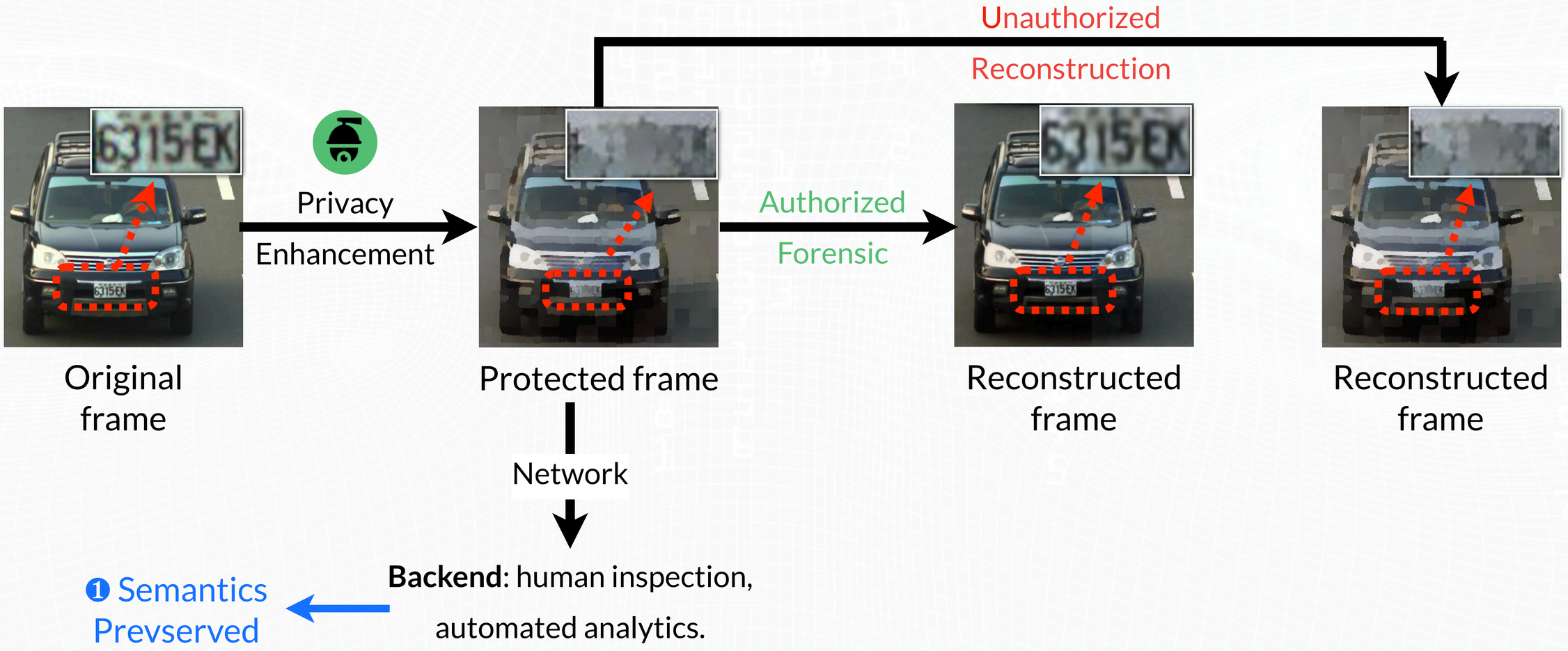
Privacy Protection Requirements

A case in the traffic scenario:



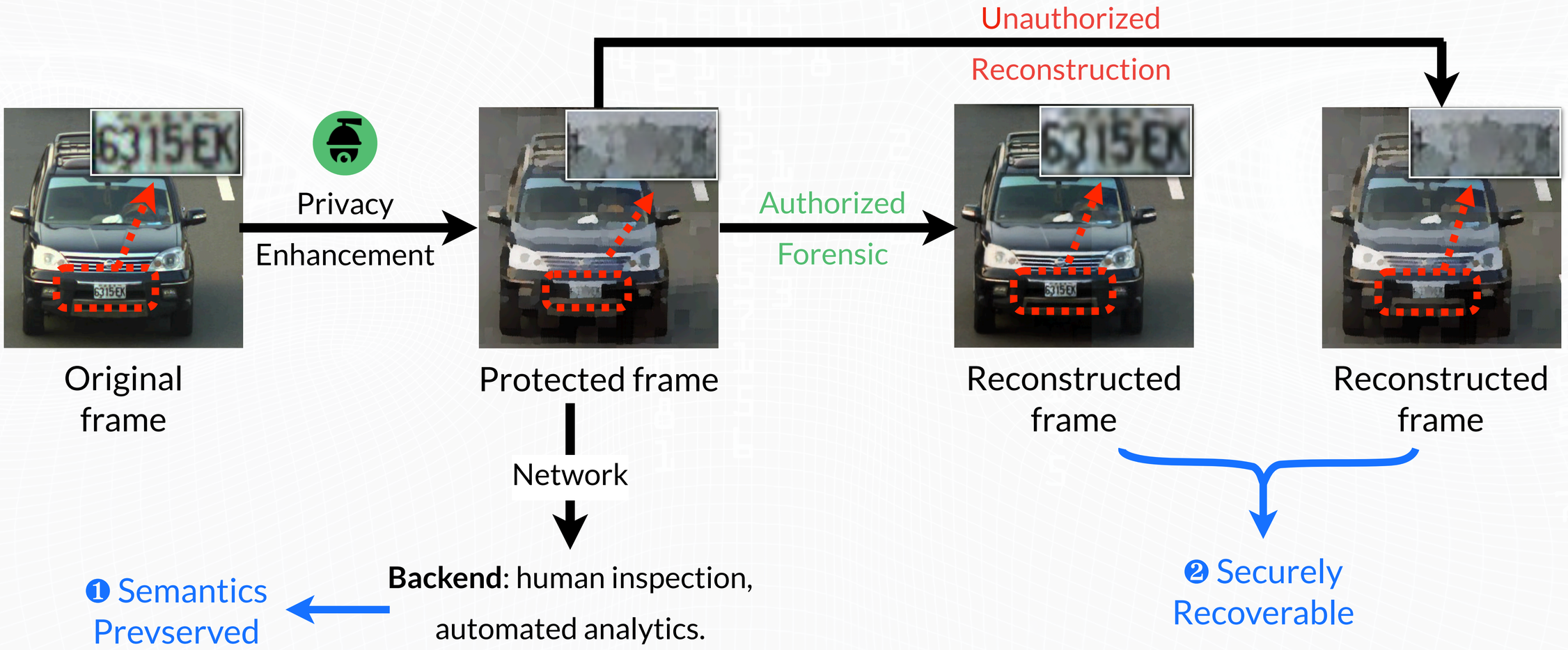
Privacy Protection Requirements

A case in the traffic scenario:



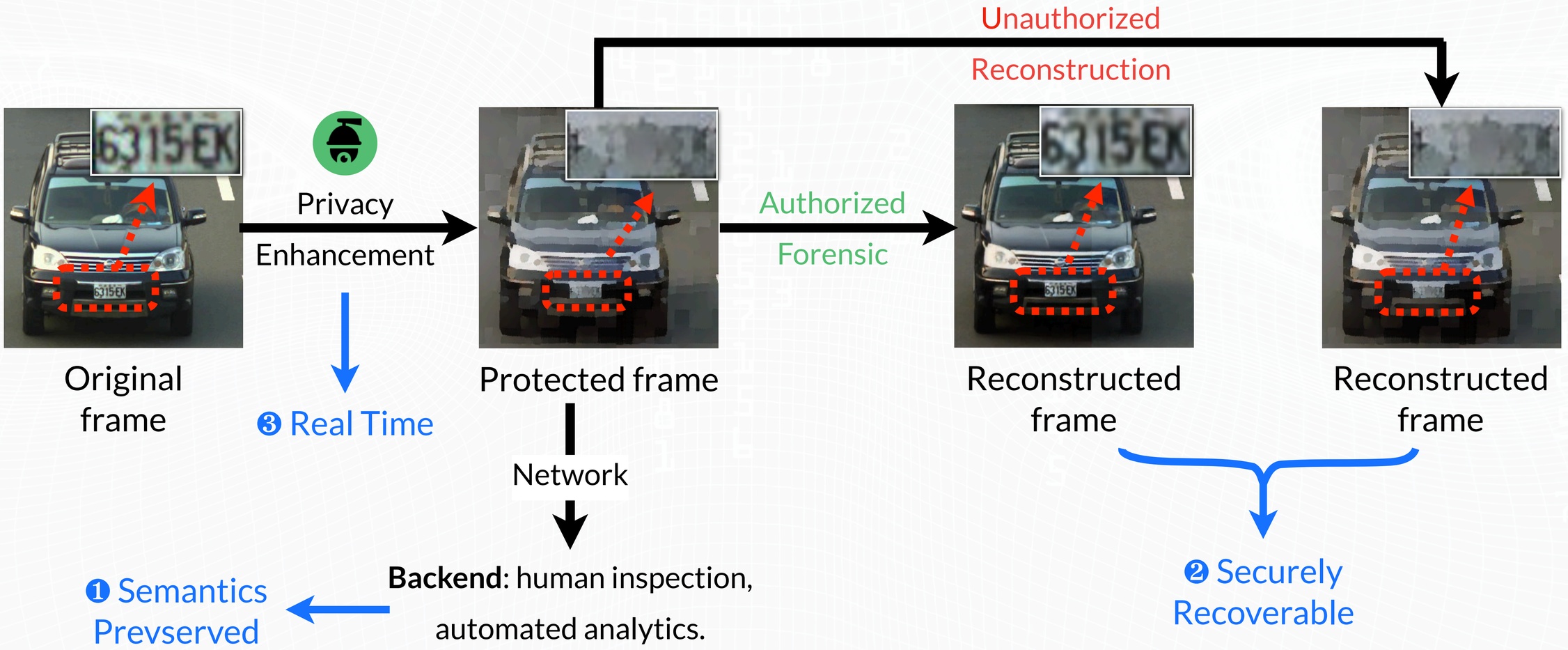
Privacy Protection Requirements

A case in the traffic scenario:



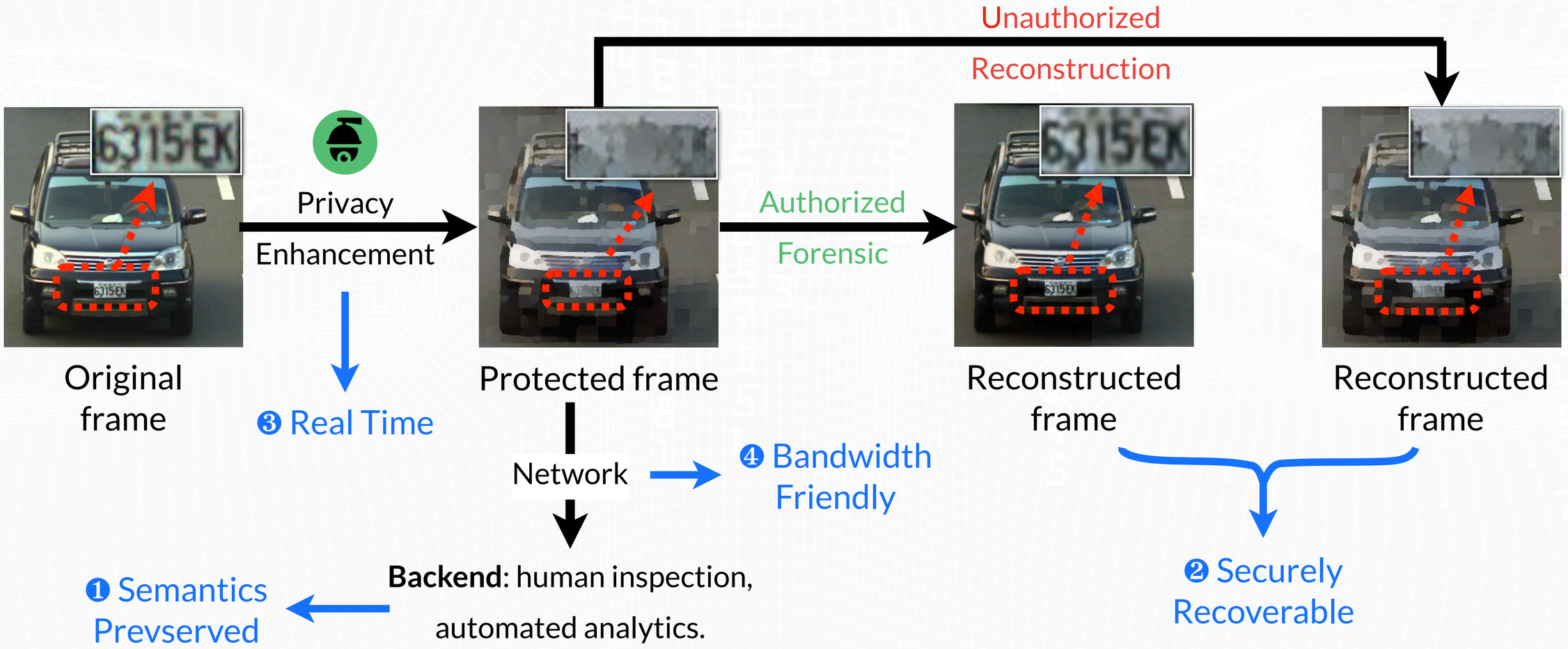
Privacy Protection Requirements

A case in the traffic scenario:

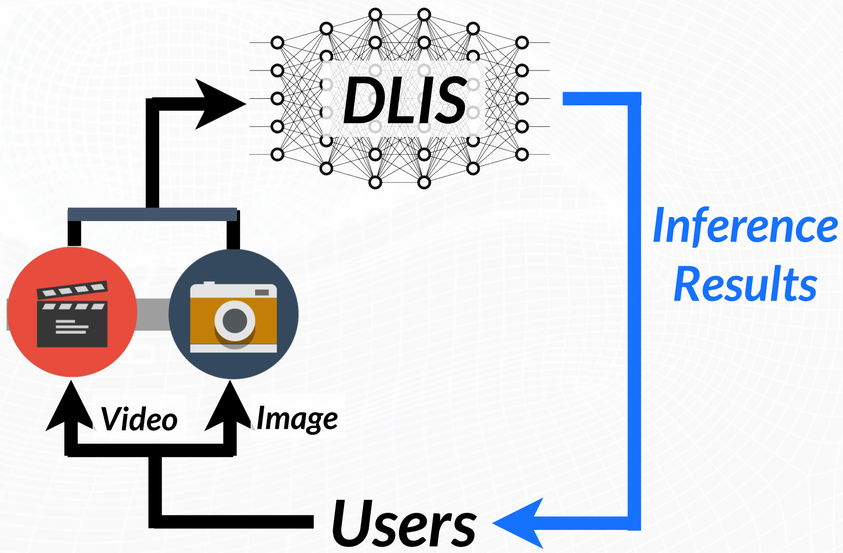


Privacy Protection Requirements

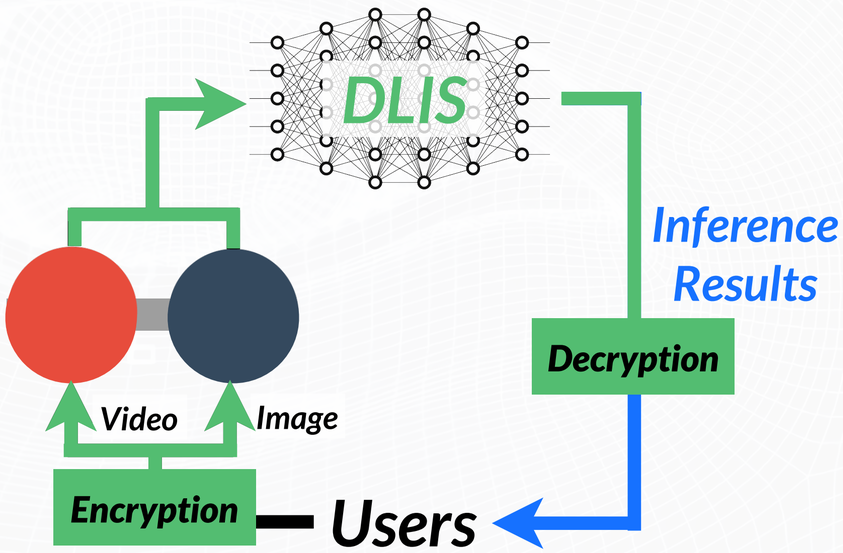
A case in the traffic scenario:



Privacy protection efforts on visual data in DL scenario.



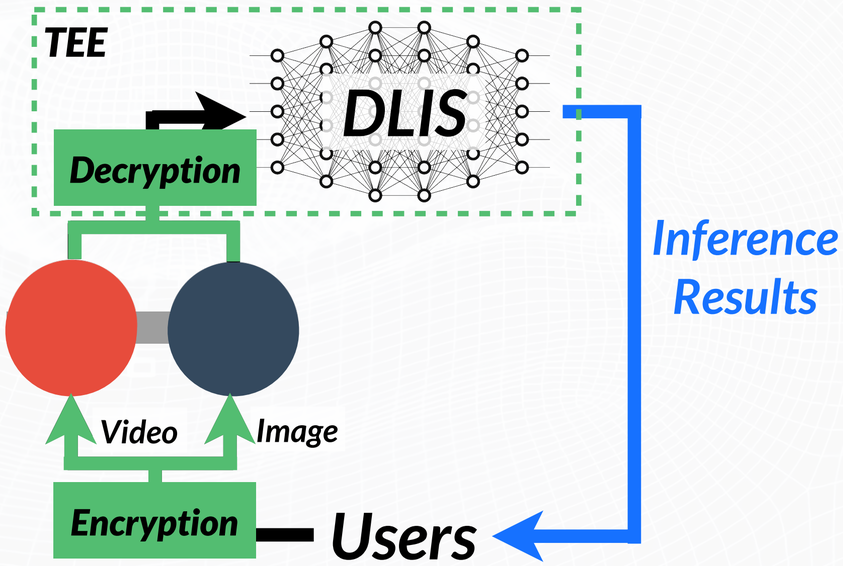
Privacy protection efforts on visual data in DL scenario.



		Usability		Effectivness		Scenario
		Deployment costs	*User Experience*	Protection Effect	Security	
HE-based solution		✗	✗	✓	✓	◎
TEE-based solution		✗	◎	✓	✓	◎
Model partition-based solution		✗	✓	◎	◎	◎
Input transformation-based solution	ROI Removal	✓	◎	◎	✓	✓
	Non-adaptive Noise	✓	◎	◎	◎	✓
	Scenario-adaptive Transformation	✓	✓	✓	✓	✓

✓ *yes*, ✗ *no*, ◎ *partial*

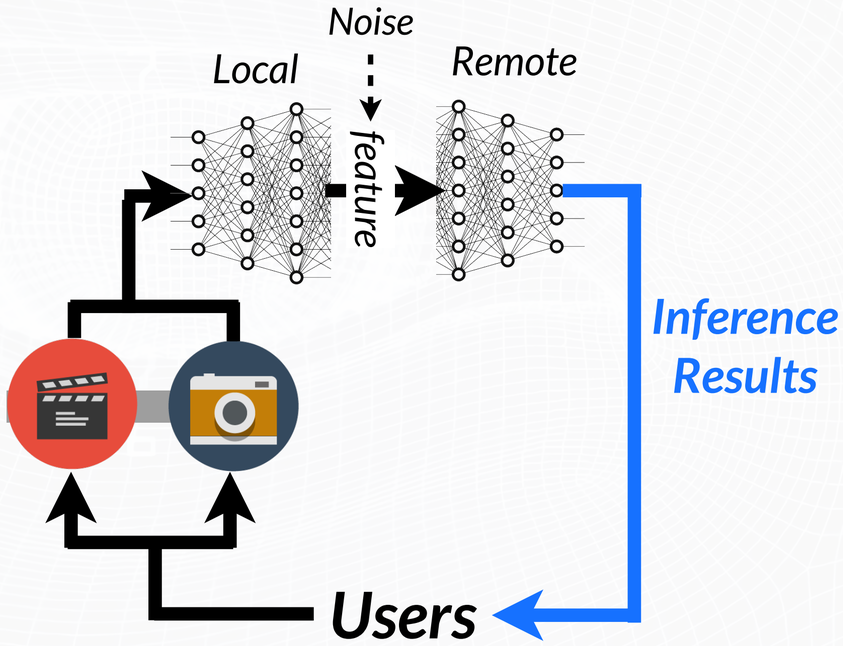
Privacy protection efforts on visual data in DL scenario.



		Usability		Effectivness		Scenario
		Deployment costs	*User Experience*	Protection Effect	Security	
HE-based solution		✗	✗	✓	✓	◎
TEE-based solution		✗	◎	✓	✓	◎
Model partition-based solution		✗	✓	◎	◎	◎
Input transformation-based solution	ROI Removal	✓	◎	◎	✓	✓
	Non-adaptive Noise	✓	◎	◎	◎	✓
	Scenario-adaptive Transformation	✓	✓	✓	✓	✓

✓ *yes*, ✗ *no*, ◎ *partial*

Privacy protection efforts on visual data in DL scenario.



		Usability		Effectivness		Scenario
		Deployment costs	*User Experience*	Protection Effect	Security	
HE-based solution		✗	✗	✓	✓	◎
TEE-based solution		✗	◎	✓	✓	◎
Model partition-based solution		✗	✓	◎	◎	◎
Input transformation-based solution	ROI Removal	✓	◎	◎	✓	✓
	Non-adaptive Noise	✓	◎	◎	◎	✓
	Scenario-adaptive Transformation	✓	✓	✓	✓	✓

✓ *yes*, ✗ *no*, ◎ *partial*

Input transformation-based solution

ROI Removal

→ *(manully) define, find, and remove privacy info*

Non-adaptive Noise

→ *Drop information accorrding to data distribution*

Scenario-adaptive Transformation 1

→ *(automatically) define, find, and remove privacy info*

Scenario-adaptive Transformation 2

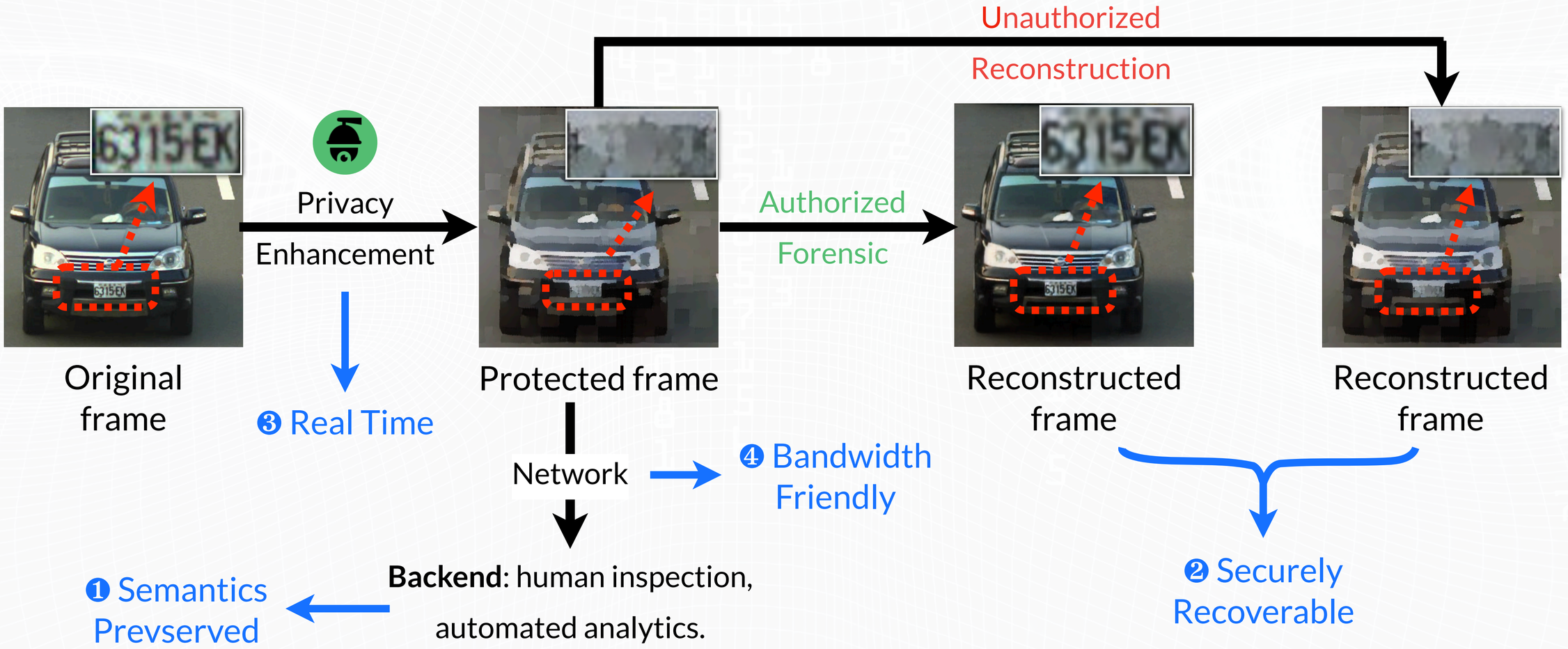
→ *Remove task unrelated info as much as possible*

		Usability		Effectivness		Scenario
		Deployment costs	*User Experience*	Protection Effect	Security	
HE-based solution		✗	✗	✓	✓	◎
TEE-based solution		✗	◎	✓	✓	◎
Model partition-based solution		✗	✓	◎	◎	◎
Input transformation-based solution	ROI Removal	✓	◎	◎	✓	✓
	Non-adaptive Noise	✓	◎	◎	◎	✓
	Scenario-adaptive Transformation	✓	✓	✓	✓	✓

✓ *yes*, ✗ *no*, ◎ *partial*

Privacy Protection VS Forensic Collection

A case in the traffic scenario:

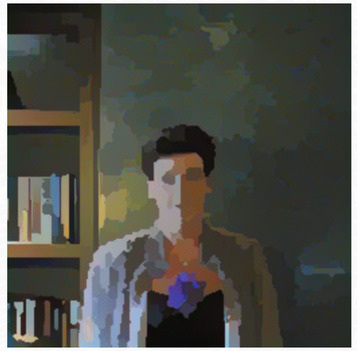
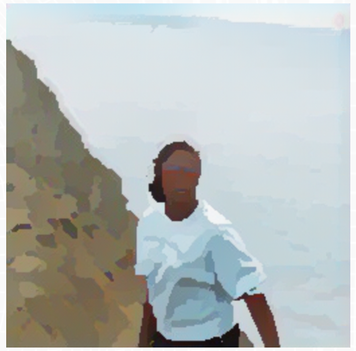


Technology 1: Semantic-preserved privacy protection

1: Determine Style **Video Analytics** *(People Tracking、People/Car Counting、Fall Detection)*

↓

Remove instance-level information, e.g., texture; Preserve category-level information, e.g., shape and color;
Maintain semantic information.e.g, spatial and pose information.

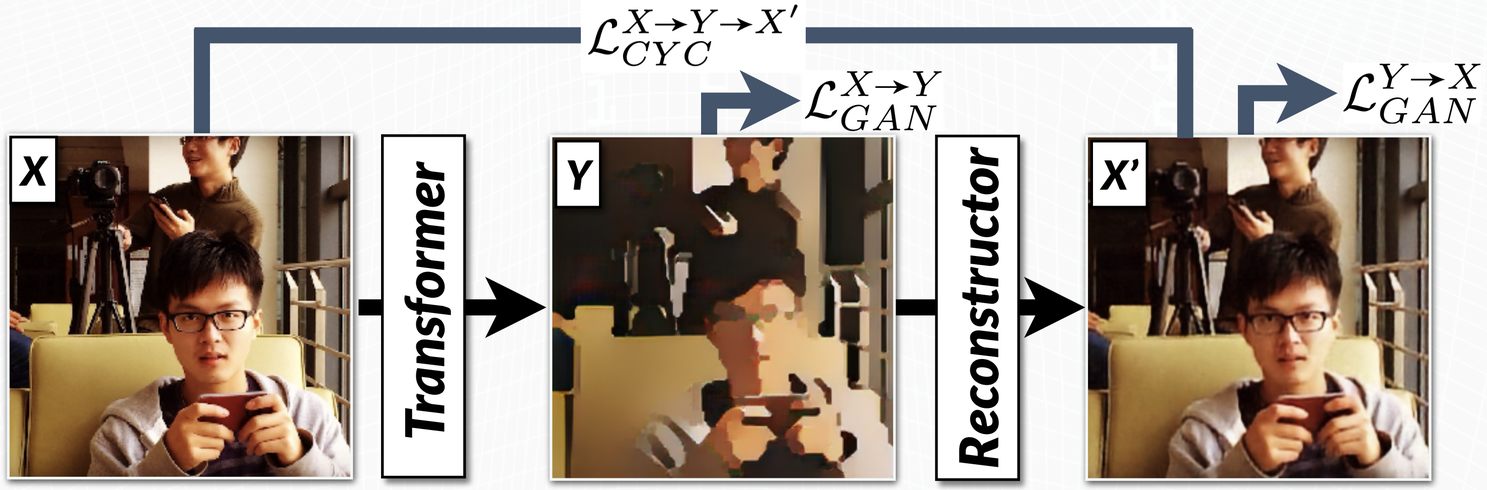

Technology 1: Semantic-preserved privacy protection

1: Determine Style **Video Analytics** *(People Tracking、People/Car Counting、Fall Detection)*

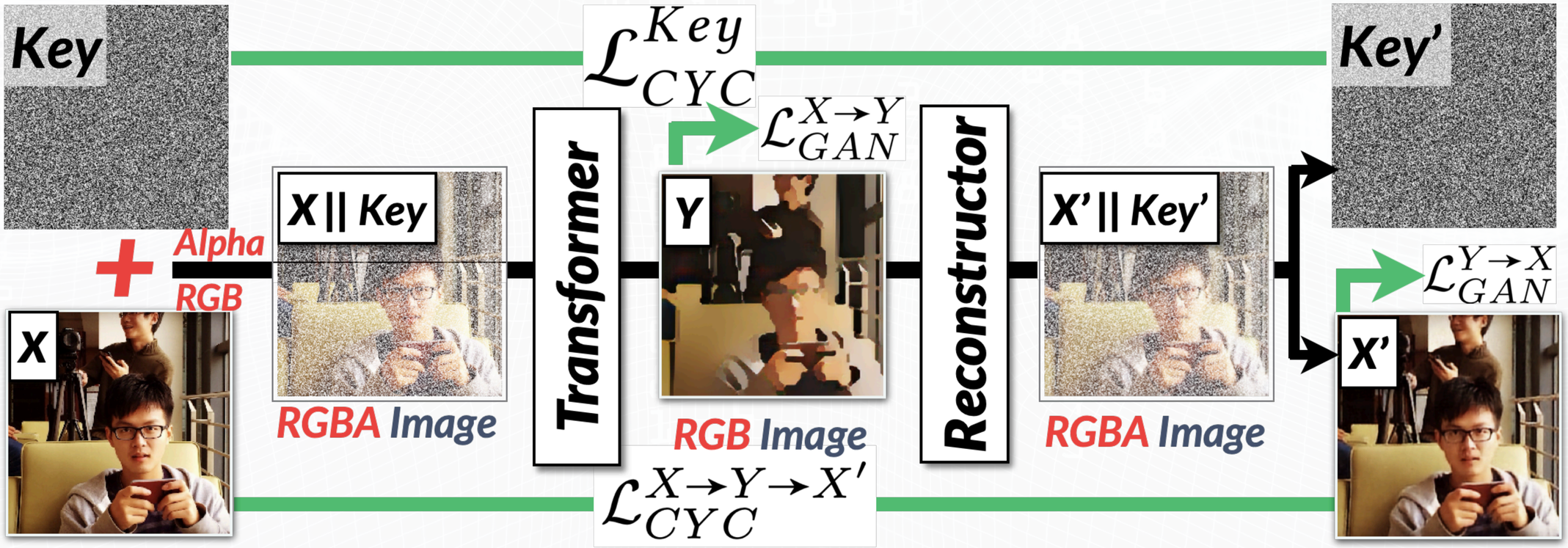
↓

Remove instance-level information, e.g., texture; Preserve category-level information, e.g., shape and color; Maintain semantic information.e.g, spatial and pose information.

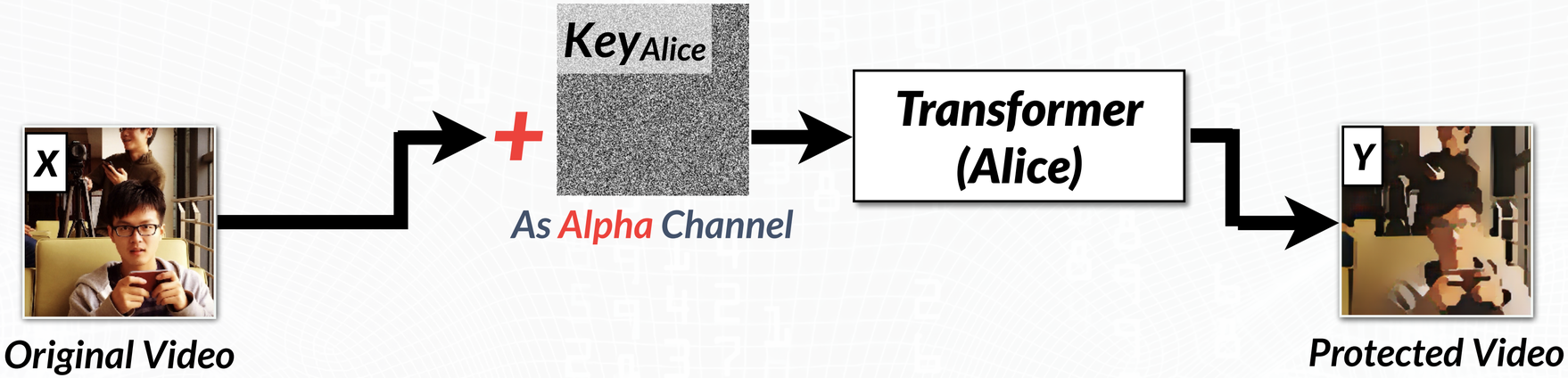
2: Learn Style



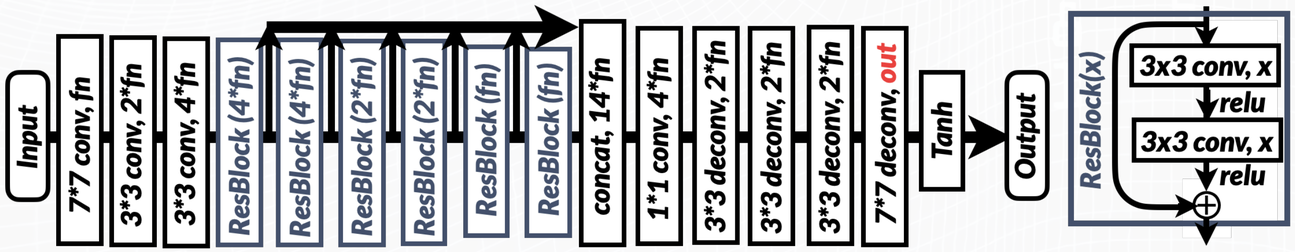
Technology 2: Securely-recoverable style transformation



Technology 3: Real-time protection with limited resources

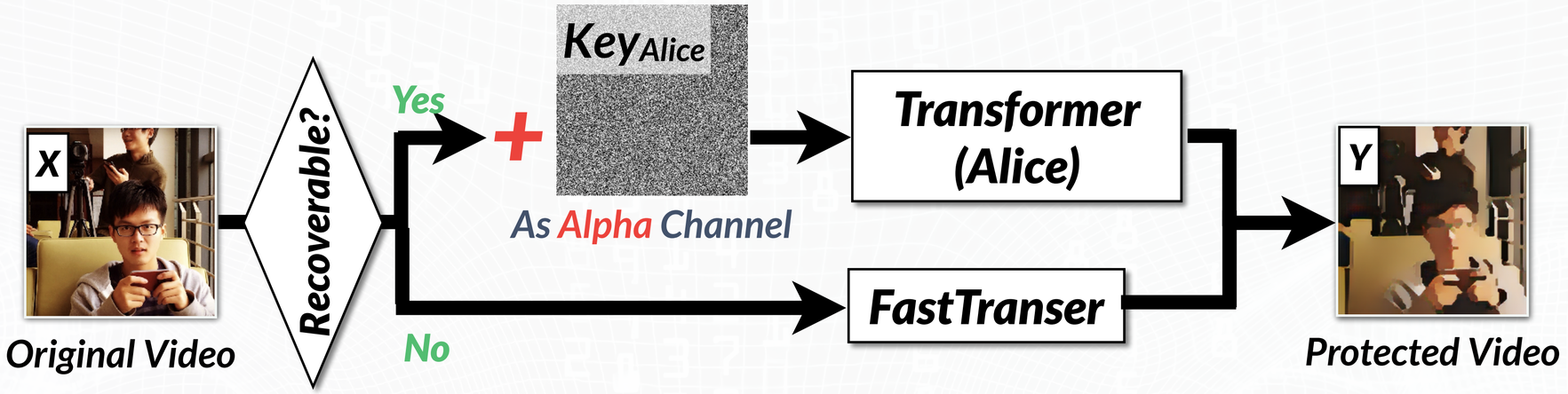


The workflow of the protection procedure.

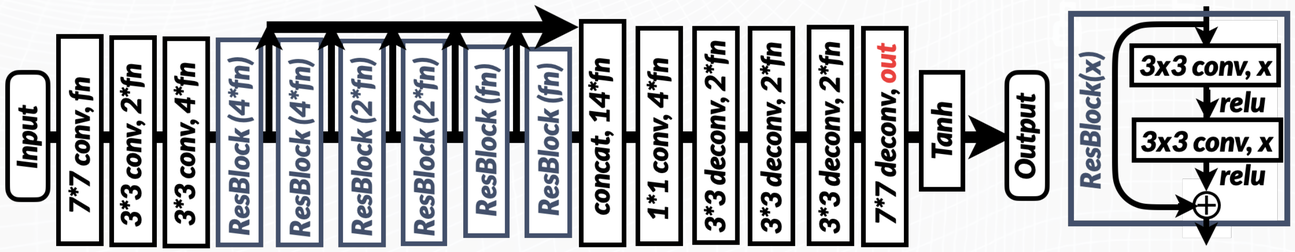


1: Litewight Network

Technology 3: Real-time protection with limited resources

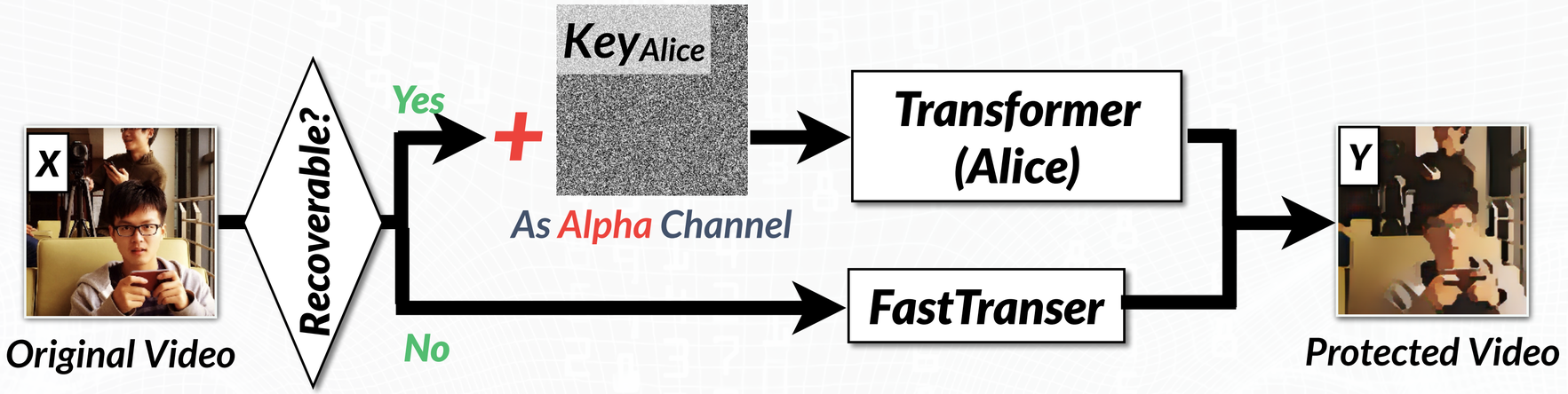


The workflow of the protection procedure.

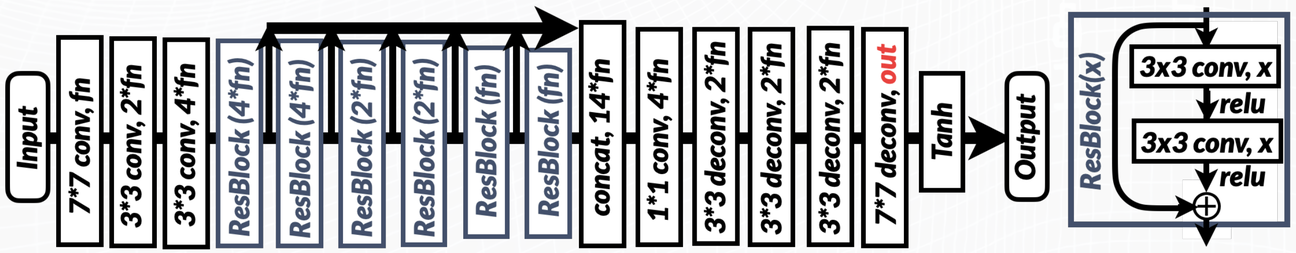


1: Litewight Network

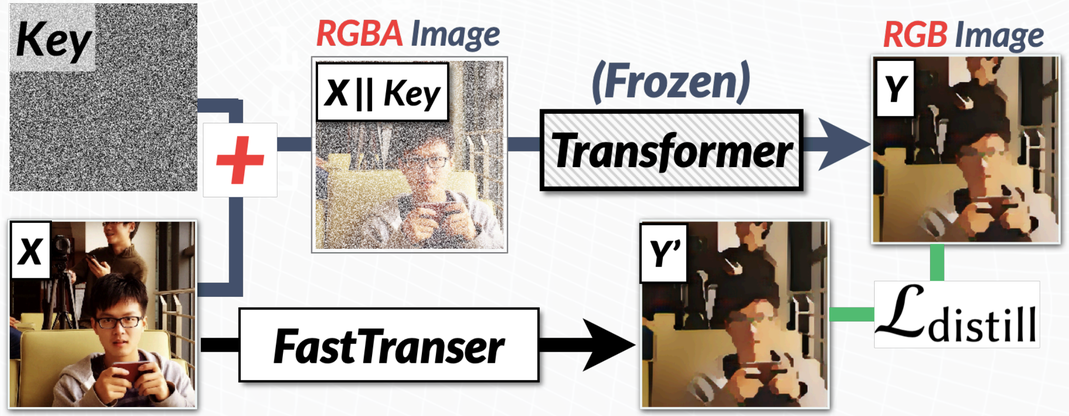
Technology 3: Real-time protection with limited resources



The workflow of the protection procedure.

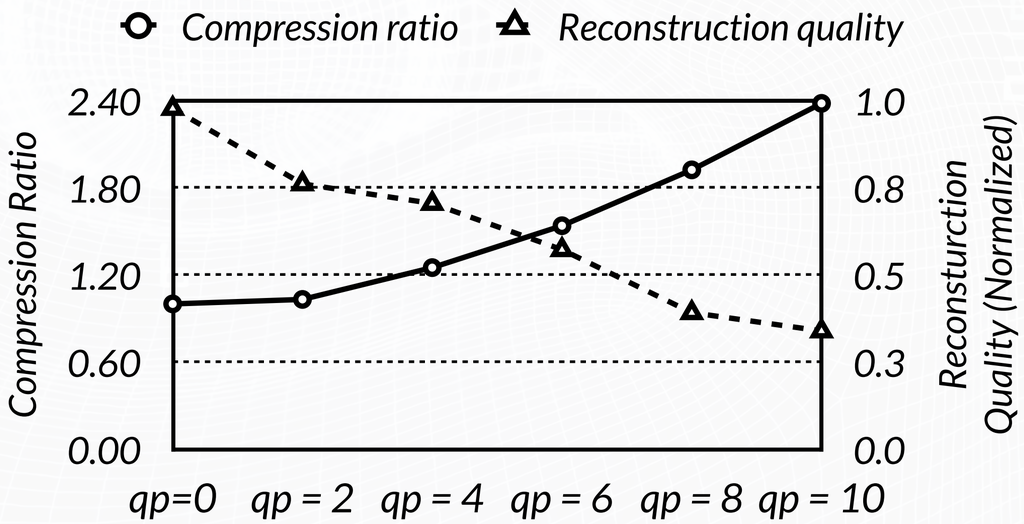


1: Litewight Network



2: Fast transformer

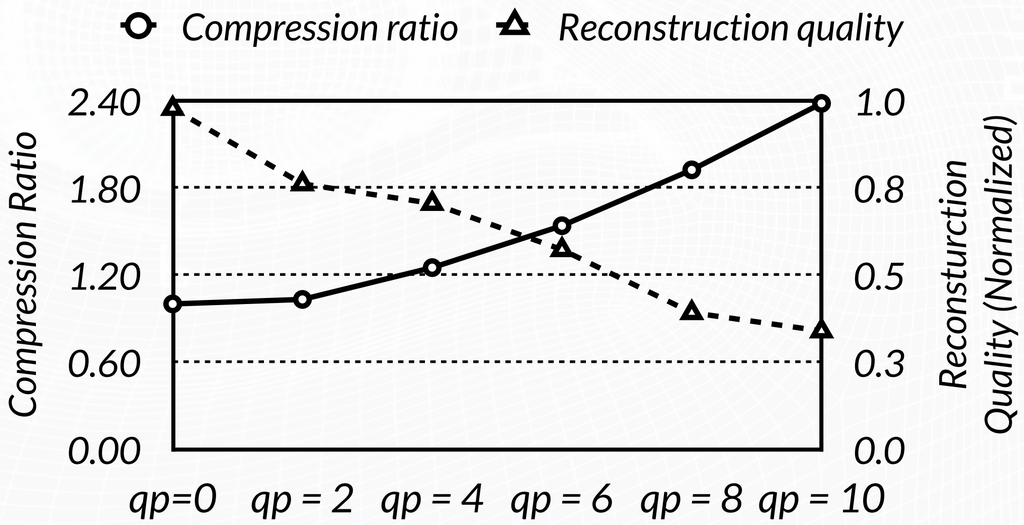
Technology 4: Bandwidth Usage Friendly Video Codec



Directly using the H.264 codec to compress the transformed frames generated by Transformer significantly reduces the reconstruction's quality.

Technology 4: Bandwidth Usage Friendly Video Codec

1: Losslessly and lossy encode the frames, adaptively.

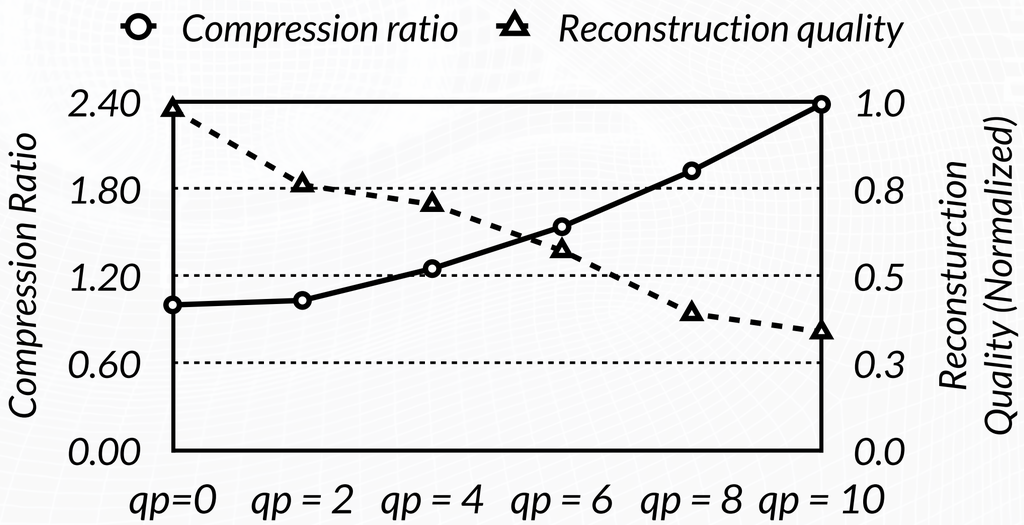


Directly using the H.264 codec to compress the transformed frames generated by Transformer significantly reduces the reconstruction's quality.

2: "Denoise" the recoverable frames.

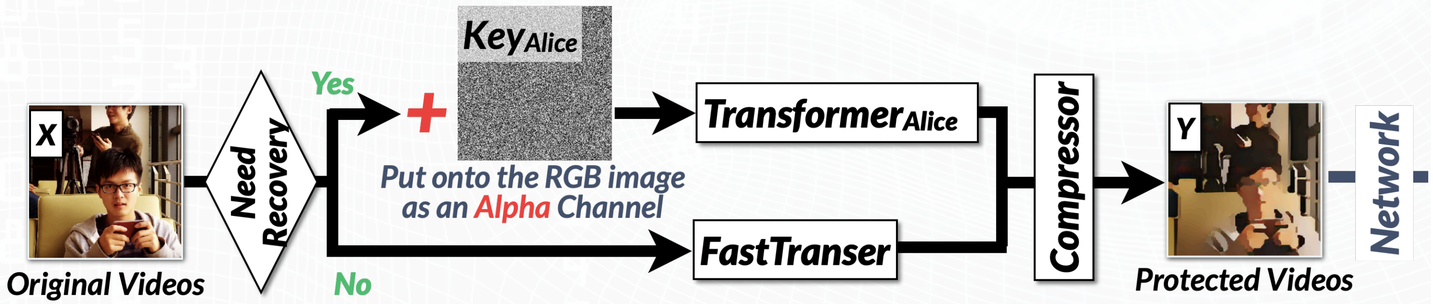
Technology 4: Bandwidth Usage Friendly Video Codec

1: Losslessly and lossy encode the frames, adaptively.



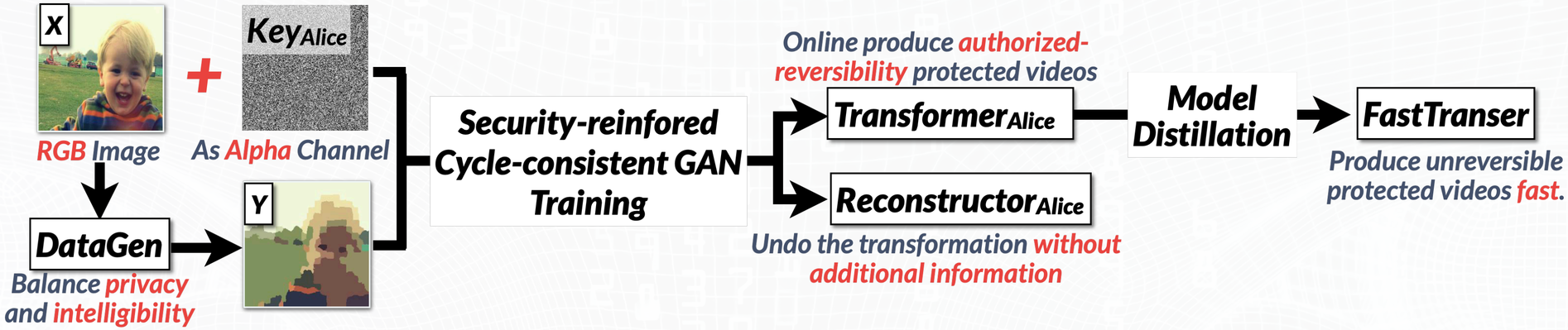
Directly using the H.264 codec to compress the transformed frames generated by Transformer significantly reduces the reconstruction's quality.

2: "Denoise" the recoverable frames.

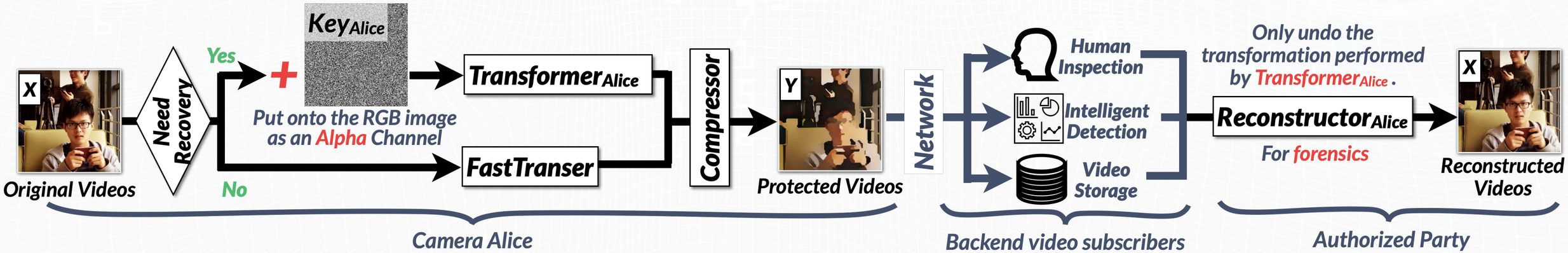


The video encoding procedure.

PECAM's workflow



(a) Preparation Stage of PECAM System.



(b) In-use Stage of PECAM system.

Is it much more difficult for an adversary to reverse the transformation?

Attacker1: *The adversary ignores the existence of secret and attempts to train an RGB-2-RGB transformation.*

Attacker2: *The adversary randomly chooses a secret to train another PECAM reconstructor.*

Attack results.

Evaluations

1. **Sematic maintaince:**

   Up to **96%** that of the original video.

2. **Privacy enhancement:**

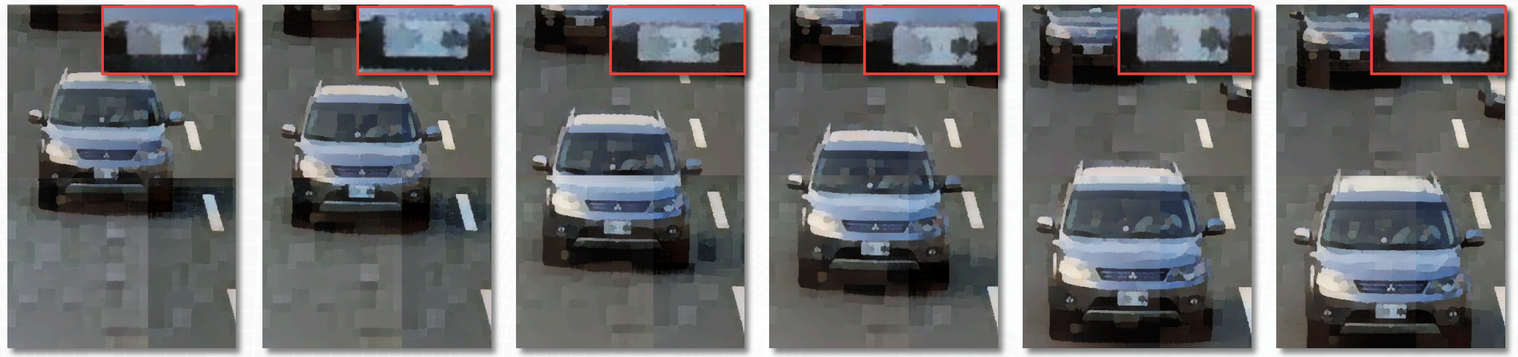
   Neither be **directly extracted** nor **indirectly reconstructed**.

3. **Bandwidth usage:**

   The bandwidth efficiency is **1.8x** that of H.264.

4. **System performance:**

   Run in **real time** , **12.3x** and **46.8x** that of baseline.



The PECAM-enabled frames in traffic monitoring scenario.

The PECAM-enabled frames in indoor monitoring scenario.

DEMO

Orignal video
(People Detection & Face recognition)

Transformed video
(People Detection)

Transformed video
(Face recognition)

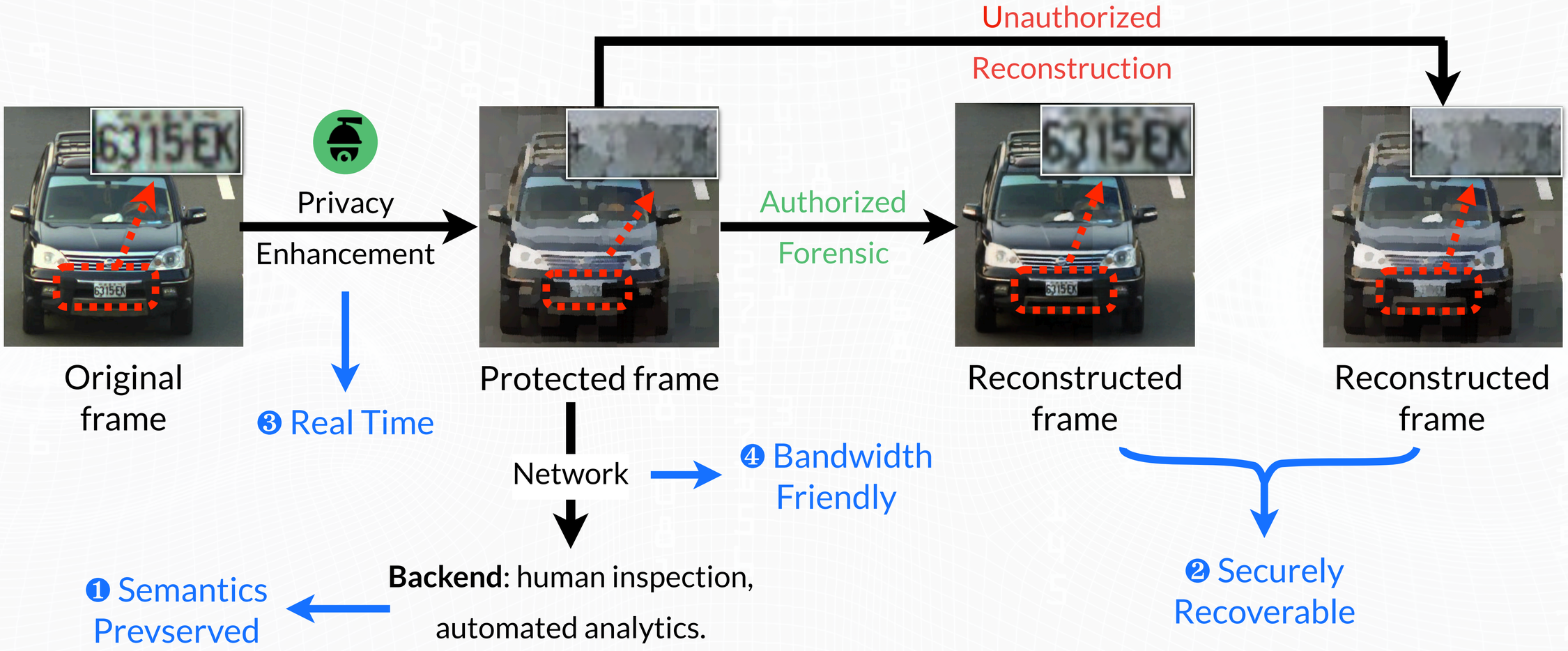
DEMO

Orignal video
(People Detection & Face recognition)

Transformed video
(People Detection)

Transformed video
(Face recognition)

Take away



Thanks!