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

Hao Wu¹, Xuejin Tian¹, Minghao Li¹ ², Yunxin Liu³, Ganesh Ananthanarayananan⁴, Fengyuan Xu¹*, and Sheng Zhong¹

¹Nanjing University
²Cornell University
³Microsoft Research
⁴Microsoft 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

EU’s Laying Down Harmonised Rules on AI and Amending Certain Union Legislative Acts

California Consumer Privacy Act (CCPA)

EU’s GDPR

Data Security Law (DSL) of the People’s Republic of China
Privacy Protection Requirements

A case in the traffic scenario:
Privacy Protection Requirements

A case in the traffic scenario:

Original frame

Protected frame

Network

**Backend**: human inspection, automated analytics.

- **Privacy Enhancement**
- **Network**
- **Original frame**
- **Protected frame**

**Requirements**
Privacy Protection Requirements

A case in the traffic scenario:

Original frame → Privacy Enhancement → Protected frame → Authorized Forensic → Reconstructed frame

Network

**Backend**: human inspection, automated analytics.
Privacy Protection Requirements

A case in the traffic scenario:

Original frame → Protected frame → Reconstructed frame

Network: human inspection, automated analytics.

Unauthorized Reconstruction

Authorized Forensic

Backend: human inspection, automated analytics.
Privacy Protection Requirements

A case in the traffic scenario:

Original frame → Privacy Enhancement → Protected frame → Network → Unauthorized Reconstruction → Reconstructed frame

Authorized Forensic → Reconstructed frame

Semantics Preerved

Backend: human inspection, automated analytics.
Privacy Protection Requirements

A case in the traffic scenario:

1. Semantics Prevserved
2. Securely Recoverable

Network

Original frame

Protected frame

Reconstructed frame

Reconstructed frame

Privacy Enhancement

Authorized Forensic

Unauthorized Reconstruction

Backend: human inspection, automated analytics.
Privacy Protection Requirements

A case in the traffic scenario:

1. **Semantics Preerved**
   - **Backend**: human inspection, automated analytics.

2. **Real Time**
   - **Privacy Enhancement**

3. **Securely Recoverable**
   - Unauthorized Reconstruction

Network:
- Original frame
- Protected frame
- Reconstructed frame
- Authorized Forensic
- Unauthorized Reconstruction
Privacy Protection Requirements

A case in the traffic scenario:

- **Original frame**
- **Protected frame**
- **Reconstructed frame**
- **Unauthorized Reconstruction**

- **Privacy Enhancement**
- **Authorized Forensic**

- **Semantics Preerved**
- **Backend**: human inspection, automated analytics.

- **Real Time**
- **Securely Recoverable**
- **Bandwidth Friendly**

- **Network**
- **Unencrypted**

- **Requirements**
  - Real Time
  - Securely Recoverable
  - Bandwidth Friendly
  - Semantics Preerved
  - Backend: human inspection, automated analytics.
Privacy protection efforts on visual data in DL scenario.

MobiCom2021: PECAM: Privacy-Enhanced Video Streaming and Analytics via Securely-Reversible Transformation

Related Works
Privacy protection efforts on visual data in DL scenario.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Usability</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Deployment costs</td>
<td>User Experience</td>
</tr>
<tr>
<td>HE-based solution</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>TEE-based solution</td>
<td>✓</td>
<td>◎</td>
</tr>
<tr>
<td>Model partition-based</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Input transformation-based solution</td>
<td>✓</td>
<td>◎</td>
</tr>
</tbody>
</table>

- ✓ yes
- ✗ no
- ◎ partial

Inference Results

- Encryption
- Decryption
- Video
- Image
- Users
Privacy protection efforts on visual data in DL scenario.

### Related Works

<table>
<thead>
<tr>
<th><strong>Scenario</strong></th>
<th><strong>Usability</strong></th>
<th><strong>Effectiveness</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Deployment costs</strong></td>
<td><strong>User Experience</strong></td>
</tr>
<tr>
<td>HE-based solution</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>TEE-based solution</td>
<td>✗</td>
<td>◎</td>
</tr>
<tr>
<td>Model partition-based solution</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Input transformation-based solution</strong></th>
<th><strong>ROI Removal</strong></th>
<th><strong>Non-adaptive Noise</strong></th>
<th><strong>Scenario-adaptive Transformation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✓</td>
<td>◎</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>◎</td>
<td>✓</td>
</tr>
</tbody>
</table>

✓ yes, ✗ no, ◎ partial
Privacy protection efforts on visual data in DL scenario.

### Related Works

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Usability</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Deployment costs</td>
<td>User Experience</td>
</tr>
<tr>
<td>HE-based solution</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>TEE-based solution</td>
<td>✗</td>
<td>◎</td>
</tr>
<tr>
<td>Model partition-based solution</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Input transformation-based solution</th>
<th>ROI Removal</th>
<th>Non-adaptive Noise</th>
<th>Scenario-adaptive Transformation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✓</td>
<td>◎</td>
<td>◎</td>
</tr>
</tbody>
</table>

✓ yes, ✗ no, ◎ partial
Input transformation-based solution

- ROI Removal
  - (manually) define, find, and remove privacy info

- Non-adaptive Noise
  - Drop information according 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

---

### Table: Input Transformation-Based Solution

<table>
<thead>
<tr>
<th></th>
<th>Usability</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Deployment costs</td>
<td>User Experience</td>
</tr>
<tr>
<td>HE-based solution</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>TEE-based solution</td>
<td>×</td>
<td>◎</td>
</tr>
<tr>
<td>Model partition-based solution</td>
<td>×</td>
<td>✓</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>ROI Removal</th>
<th>Non-adaptive Noise</th>
<th>Scenario-adaptive Transformation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input transformation-based solution</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

- ✓ yes, × no, ◎ partial
Privacy Protection VS Forensic Collection

A case in the traffic scenario:

- **Original frame**
- **Protected frame**
- **Reconstructed frame**
- **Reconstructed frame**

- **Privacy Enhancement**
- **Authorized Forensic**
- **Unauthorized Reconstruction**

- **Real Time**

- **Semantics Prethesized**

- **Backend**: human inspection, automated analytics.

- **Bandwidth Friendly**

- **Securely Recoverable**

**Requirements**

MobiCom2021· PECAM: Privacy-Enhanced Video Streaming and Analytics via Securely-Reversible Transformation
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

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.

1: Determine Style

2: Learn Style
Technology 2: Securely-recoverable style transformation

1: Introduce “secert”

2: SSIM Loss
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

1: Lithewight Network

The workflow of the protection procedure.

Original Video → Recoverable? → Transformer (Alice) → Protected Video

Protected Video

Original Video

Yes

No

Transformer (Alice)

FastTranser

As Alpha Channel

Yes

No

X

Y

Key Design

MobiCom2021· PECAM: Privacy-Enhanced Video Streaming and Analytics via Securely-Reversible Transformation·
Technology 3: Real-time protection with limited resources

1: Litewight Network

2: Fast transformer

The workflow of the protection procedure.
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.  

2: “Denoise” the recoverable frames.

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.

2: “Denoise” the recoverable frames.

Directly using the H.264 codec to compress the transformed frames generated by Transformer significantly reduces the reconstruction’s quality.
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. Semantic maintenance:
   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

Original video
(People Detection & Face recognition)

Transformed video
(People Detection)
Detection Success

Transformed video
(Face recognition)
Recognition Fail

P1  P2  P3  P4  P5  P6  P7  P8  P9  P10  P11  P12
DEMO

Original video
(People Detection & Face recognition)

Transformed video
(People Detection)
Detection Success

Transformed video
(Face recognition)
Recognition Fail

P1
P2
P3
P4
P5
P6
P7
P8
P9
P10
P11
P12
P13
P14
P15
P16
P17
P18
P19
P20
P21
P22
P23
P24
Take away

1. Semantics Preerved

Privacy Enhancement

Real Time

Network

Semantics Preerved: human inspection, automated analytics.

Authorized Forensic

Securely Recoverable

Unauthorized Reconstruction

Bandwidth Friendly

Thanks!