# Privacy-Aware Video Anomaly Detection through Orthogonal Subspace Projection

Lei Wang[1,2] Wenxiang Diao[3] Andrew Busch[1] Jun Zhou[1] Yongsheng Gao[1]

[1]Griffith University [2]Data61/CSIRO [3]UNSW Sydney

July 8, 2026

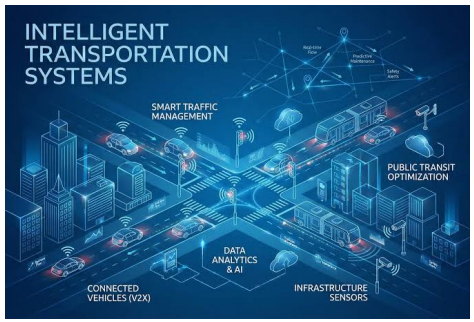



# Motivation

**Why Privacy Matters in Video Anomaly Detection (VAD)?**

VAD is increasingly deployed in:

- Public safety
- Intelligent transportation
- Public surveillance



Despite impressive detection performance, existing VAD models often encode privacy-sensitive information, such as facial identity and appearance, which is unnecessary for anomaly detection.

**Research question**

- Can we remove privacy-sensitive information while preserving anomaly detection performance?

# Motivation (cont.)

**The Problem with Existing VAD Models**

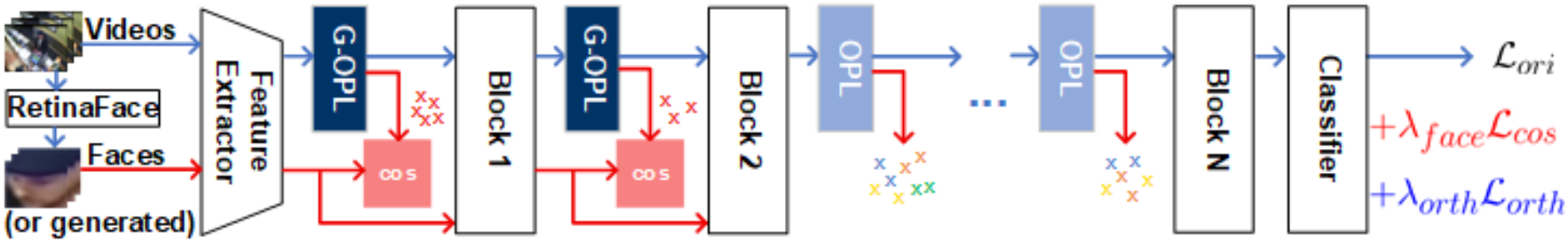
| **Keep** (Anomaly-relevant) | **Remove** (Unnecessary/Sensitive) |
|---|---|
| Motion | Facial identity |
| Object interactions | Appearance & clothing |
| Scene dynamics | Background & lighting |

**Existing solution**

- Face blurring
  - Removes useful visual context
  - Protects only the input image
  - Does not prevent feature-level privacy leakage

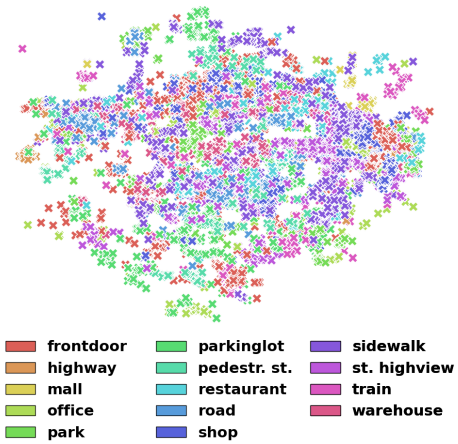
**Our idea**: Remove privacy-sensitive information within the learned feature representation, rather than only masking the input image.

# Our Method

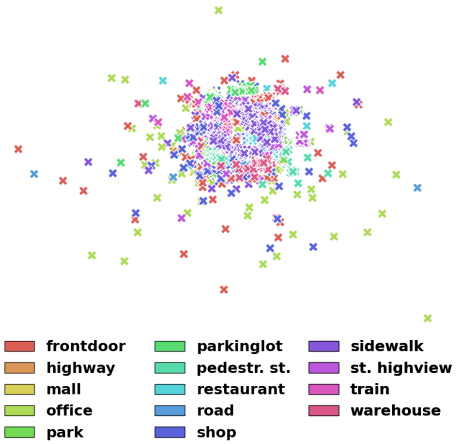



- **OPL**
  - Learns nuisance feature directions
  - Removes background, lighting, and camera variations
  - Preserves anomaly-relevant information
- **Guided OPL (G-OPL)**
  - Uses weak face-presence supervision
  - Identifies privacy-sensitive feature directions
  - Suppresses facial information while preserving motion and pose
- **Advantages**
  - Lightweight and fully differentiable
  - Plug-and-play for existing VAD models
  - No identity labels or adversarial training

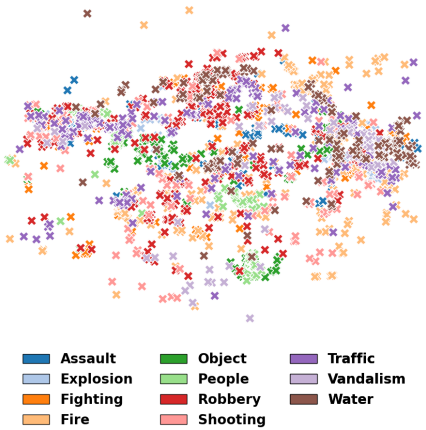
# Why It Works



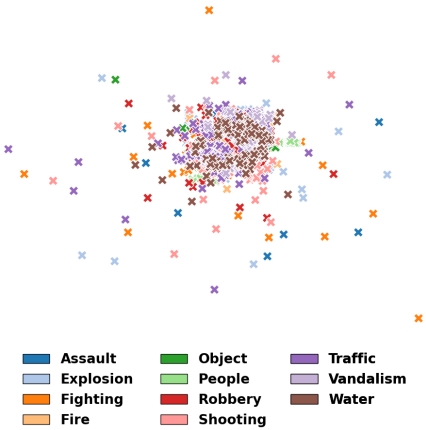

OPL(scenario)




G-OPL(scenario)




OPL(anomaly)




G-OPL(anomaly)

**Key observations**

| OPL | G-OPL |
|---|---|
| Removes nuisance factors | Removes privacy-sensitive information |
| Dispersed clusters reflect scene-specific variations | Compact, overlapping clusters indicate facial information is suppressed |
| Preserves anomaly-relevant features | Preserves anomaly-relevant features while reducing privacy leakage |

# Detection Performance

## Performance by anomaly type on MSAD.

| Method | Assault | | Explosion | | Fighting | | Fire | | Obj. Fall | | People Fall | | Robbery | | Shooting | | Traffic Acc. | | Vandalism | | Water Inc. | | **Overall** | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | AUC | AP | AUC | AP | AUC | AP | AUC | AP | AUC | AP | AUC | AP | AUC | AP | AUC | AP | AUC | AP | AUC | AP | AUC | AP | AUC | AP |
| RTFM (I3D) | 53.9 | 66.4 | 66.0 | 76.6 | 79.8 | 88.6 | 44.9 | 71.1 | 84.6 | 89.3 | 45.7 | 52.6 | 70.2 | 88.0 | 87.5 | 89.2 | 64.1 | 57.7 | 74.9 | 73.0 | 98.1 | 99.6 | 86.6 | 68.4 |
| MGFN (SwinT) | 50.2 | 49.6 | 50.9 | 58.1 | 57.2 | 67.1 | 51.4 | 74.2 | 41.3 | 51.6 | 44.4 | 40.3 | 40.1 | 68.5 | 51.4 | 63.9 | 50.4 | 42.3 | 42.6 | 40.9 | 58.6 | 87.2 | 69.3 | 33.6 |
| MGFN (I3D) | 53.9 | 60.2 | 59.1 | 66.5 | 80.6 | 89.5 | 66.1 | 82.9 | 89.9 | 94.6 | **53.6** | 44.9 | 72.2 | 85.4 | 68.3 | 80.6 | 66.9 | 54.7 | 84.4 | 78.5 | 81.9 | 96.1 | 81.2 | 59.3 |
| UR-DMU | 56.9 | 64.5 | 67.9 | 74.5 | 83.9 | 90.4 | 61.2 | 82.9 | 92.1 | 95.8 | 42.5 | 43.7 | 63.5 | 79.3 | 81.4 | 87.8 | 62.0 | 55.6 | 84.7 | 77.0 | 98.5 | 99.5 | 85.0 | 68.3 |
| EGO | 52.2 | 57.5 | 57.6 | 74.4 | 66.5 | 72.8 | 62.9 | 86.7 | 92.3 | 94.8 | 35.4 | 43.8 | 64.8 | 87.5 | 68.6 | 78.4 | 69.9 | **64.3** | 88.1 | 81.4 | 81.9 | 95.4 | 87.3 | 64.4 |
| IEF-VAD | 66.0 | - | 66.3 | - | 79.8 | - | 49.4 | - | 75.9 | - | 42.5 | - | 66.9 | - | 86.9 | - | **70.1** | - | 75.8 | - | 88.9 | - | 82.1 | - |
| RTFM-OPL (I3D) | 57.0 | 62.4 | **77.7** | **85.7** | 74.1 | 84.8 | 49.6 | 75.5 | 87.7 | 92.1 | 53.3 | 50.4 | **72.4** | **89.0** | 84.1 | 89.5 | 69.5 | 58.7 | 84.8 | 80.9 | **99.2** | **99.8** | 86.5 | 68.2 |
| MGFN-OPL (SwinT) | 59.1 | 56.5 | 52.7 | 57.0 | 44.3 | 55.2 | 63.0 | 76.4 | 58.3 | 59.3 | 40.6 | 36.0 | 49.5 | 70.7 | 55.3 | 62.1 | 49.1 | 39.6 | 60.8 | 53.7 | 44.4 | 78.9 | 78.2 | 47.5 |
| MGFN-OPL (I3D) | **71.3** | **69.4** | 61.8 | 73.0 | 87.8 | **92.8** | **81.0** | **93.0** | **94.3** | **96.5** | 45.9 | 45.0 | 65.1 | 81.1 | 82.7 | 89.1 | 64.2 | 55.2 | **90.8** | **86.4** | 68.7 | 92.0 | 86.2 | 68.3 |
| RTFM-G-OPL/OPL (I3D) | 50.2 | 62.4 | 69.4 | 80.6 | 69.5 | 84.4 | 71.8 | 87.0 | 88.7 | 92.4 | 52.3 | **53.3** | 71.4 | 88.2 | **87.8** | **91.0** | 62.5 | 54.7 | 82.0 | 79.6 | 97.5 | 99.4 | **88.0** | **70.9** |
| MGFN-G-OPL/OPL (I3D) | 52.4 | 59.8 | 66.5 | 76.8 | **88.8** | 92.2 | 77.2 | 89.0 | 90.5 | 95.1 | 45.9 | 42.8 | 65.4 | 80.1 | 71.9 | 81.8 | 53.9 | 46.4 | 83.1 | 75.1 | 81.5 | 96.0 | 84.0 | 65.8 |

## Performance by scenario on MSAD.

| Method | Frontdoor | | Mall | | Office | | Parkinglot | | Pedestr. st. | | Restaurant | | Road | | Shop | | Sidewalk | | St. highview | | Train | | Warehouse | | **Overall** | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | AUC | AP | AUC | AP | AUC | AP | AUC | AP | AUC | AP | AUC | AP | AUC | AP | AUC | AP | AUC | AP | AUC | AP | AUC | AP | AUC | AP | AUC | AP |
| RTFM (I3D) | 81.8 | 79.3 | 88.1 | 76.6 | 76.6 | **72.8** | 80.7 | 45.8 | 94.0 | 48.5 | 88.3 | 79.1 | 84.3 | 57.9 | 85.3 | 75.6 | **88.3** | **68.8** | 72.0 | 28.5 | 51.4 | 3.3 | 82.7 | 57.0 | 86.6 | 68.4 |
| MGFN (SwinT) | 59.5 | 51.7 | 18.5 | 20.1 | 64.1 | 52.3 | 67.9 | 19.0 | 75.9 | 9.7 | 67.9 | 44.0 | 70.6 | 26.3 | 62.7 | 43.0 | 69.0 | 25.9 | 75.3 | 23.3 | 65.4 | 5.2 | 70.1 | 30.1 | 69.3 | 33.6 |
| MGFN (I3D) | 82.5 | 80.8 | 73.8 | 71.3 | 71.5 | 58.2 | 68.9 | 14.8 | 94.8 | 36.2 | 95.1 | **91.3** | 76.5 | 35.8 | 85.6 | 78.4 | 78.5 | 57.2 | 77.9 | 29.3 | 40.3 | 2.1 | 58.3 | 24.2 | 81.2 | 59.3 |
| UR-DMU | 84.8 | 82.8 | **91.0** | 83.8 | 77.8 | 67.3 | 91.4 | 53.9 | 81.9 | 11.5 | 93.1 | 87.4 | 83.0 | 64.4 | 81.3 | 64.5 | 86.5 | 64.1 | 85.0 | 37.7 | 59.0 | 3.1 | 81.2 | 59.1 | 85.0 | 68.3 |
| EGO | 85.2 | 81.6 | 82.3 | 73.4 | **80.0** | 71.7 | **96.8** | **75.2** | **97.5** | 52.0 | 94.3 | 73.9 | **89.8** | **64.6** | 83.4 | 72.2 | 87.1 | 45.0 | 28.2 | 10.1 | 80.8 | 7.8 | 84.7 | 46.6 | 87.3 | 64.4 |
| IEF-VAD | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 82.1 | - |
| RTFM-OPL (I3D) | **85.6** | 82.3 | 85.6 | 80.2 | 77.2 | 72.0 | 76.9 | 26.4 | 96.6 | 50.5 | 90.2 | 81.3 | 76.9 | 53.3 | 88.6 | **82.8** | 84.9 | 56.5 | 66.8 | 26.7 | 42.4 | 2.3 | 86.1 | 66.8 | 86.5 | 68.2 |
| MGFN-OPL (SwinT) | 68.5 | 57.8 | 89.0 | 61.8 | 68.4 | 55.4 | 79.4 | 39.0 | 74.5 | 5.0 | 51.6 | 36.1 | 67.3 | 28.1 | 77.1 | 60.3 | 81.1 | 41.9 | 87.1 | 45.8 | **83.5** | 11.9 | 83.8 | 52.4 | 78.2 | 47.5 |
| MGFN-OPL (I3D) | 84.4 | **84.1** | 80.2 | 74.7 | 74.7 | 65.0 | 87.0 | 30.9 | 93.5 | **53.1** | 91.2 | 87.6 | 80.0 | 55.7 | 82.1 | 69.4 | 86.8 | 63.8 | **98.1** | **95.1** | 70.8 | 9.1 | **89.9** | 76.1 | 86.2 | 68.3 |
| RTFM-G-OPL/OPL (I3D) | 82.0 | 79.3 | **91.0** | 81.4 | 74.3 | 72.0 | 79.4 | 27.2 | 86.9 | 36.1 | 90.3 | 81.4 | 72.4 | 46.7 | **89.0** | 82.5 | 87.0 | 65.1 | 84.9 | 37.8 | 70.4 | **12.0** | 86.3 | **79.6** | **88.0** | **70.9** |
| MGFN-G-OPL/OPL (I3D) | 84.4 | 83.3 | 90.0 | **84.8** | 75.9 | 62.3 | 70.4 | 16.9 | 90.5 | 25.8 | **95.7** | 90.2 | 71.4 | 43.1 | 79.7 | 64.5 | 83.8 | 63.3 | 87.7 | 41.3 | 44.7 | 2.3 | 64.8 | 41.1 | 84.0 | 65.8 |

# Privacy Evaluation

**Why is it needed?**

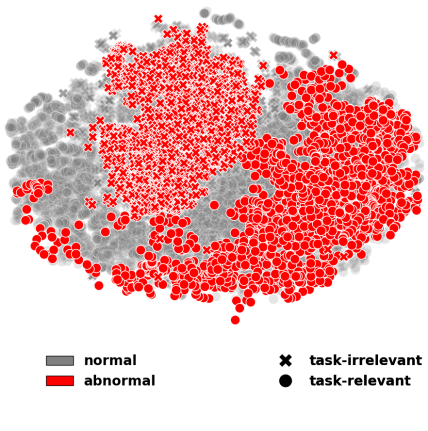
Detection accuracy alone is not sufficient.

| Metric | Measures |
|---|---|
| SSC ↑ | Is sensitive information captured by the projection subspace? |
| ARD ↓ | Is anomaly detection performance preserved after projection? |
| PD/FPD ↓ | How effectively is sensitive information suppressed across the network? |

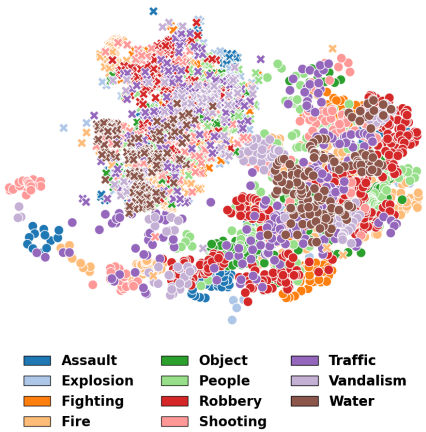
**Comparison with representative privacy-preserving strategies**

| Method | ShanghaiTech | | | CUHK Avenue | | UCSD Ped2 | | UCF-Crime | |
|---|---|---|---|---|---|---|---|---|---|
| | AUC ↑ | FPD ↓ | ARD ↓ | AUC ↑ | FPD ↓ | AUC ↑ | FPD ↓ | AUC ↑ | FPD ↓ |
| Baseline | 96.8 | 0.42 | 0.08 | 85.6 | 0.37 | 98.1 | 0.05 | 84.5 | 0.48 |
| + Input masking (blur) | 93.5 | **0.18** | 0.30 | 82.0 | **0.16** | 97.9 | 0.045 | 80.2 | **0.20** |
| + Differential privacy | 95.8 | 0.34 | 0.19 | 84.1 | 0.31 | 97.8 | 0.045 | 83.1 | 0.39 |
| + Feature bottleneck | 95.3 | 0.30 | 0.15 | 83.8 | 0.28 | 97.6 | 0.045 | 82.6 | 0.35 |
| + GRL (adversarial) | 95.9 | 0.33 | 0.17 | 84.2 | 0.30 | 97.7 | 0.045 | 83.4 | 0.36 |
| + OPL (Ours) | 97.1 | 0.30 | 0.07 | 87.2 | 0.28 | **98.4** | 0.045 | 85.2 | 0.34 |
| + G-OPL (Ours) | **97.3** | 0.22 | **0.06** | **89.0** | 0.21 | **98.4** | **0.042** | **85.4** | 0.29 |

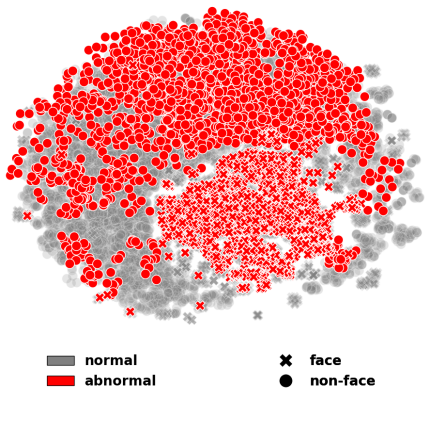
# Conclusion



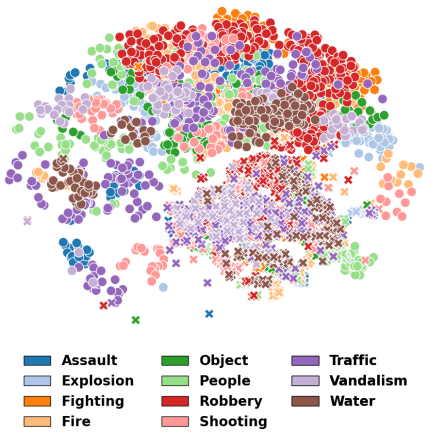

OPL




OPL(anomaly)




G-OPL




G-OPL(anomaly)

**Our contributions**

- **OPL & G-OPL**
  - Remove nuisance and privacy-sensitive information
  - Preserve anomaly-relevant representations
- **Comprehensive Privacy Evaluation**
  - Jointly evaluate utility and privacy
  - Introduce SSC, ARD, and PD
- **Extensive Experiments**
  - Consistent improvements in anomaly detection
  - Reduced privacy leakage across multiple benchmarks