Background Buster: Peeking through Virtual Backgrounds in Online Video Calls

Mohd Sabra*, Anindya Maiti**, and Murtuza Jadliwala*

* University of Texas at San Antonio
** University of Oklahoma
Video Calls

Cisco Webex

Skype

Zoom

Microsoft Teams
Virtual Background
Virtual Background Not Prefect
Virtual Background Not Prefect
Adversary’s Goals

Attack 1: Reconstruct leaked background
Adversary’s Goals

**Attack 1:** Reconstruct leaked background

**Attack 2:** Determine location from pre-set possibilities?
Adversary’s Goals

Attack 1: Reconstruct leaked background

Attack 2: Determine location from pre-set possibilities?

Attack 3: Detect if a specific object exists in leaked background?
Adversary’s Goals

Attack 1: Reconstruct leaked background

Attack 2: Determine location from pre-set possibilities?

Attack 3: Detect if a specific object exists in leaked background?

Attack 4: Detect generic objects in the leaked background?
Adversary’s Goals

**Attack 1:** Reconstruct leaked background

**Attack 2:** Determine location from pre-set possibilities?

**Attack 3:** Detect if a specific object exists in leaked background?

**Attack 4:** Detect generic objects in the leaked background?

All Yes! (to a certain degree)
Adversary’s Goals

Attack 1: Reconstruct leaked background

Attack 2: Determine location from pre-set possibilities?

Attack 3: Detect if a specific object exists in leaked background?

Attack 4: Detect generic objects in the leaked background?

All Yes! (to a certain degree)
Leaked Background Reconstruction

- Video
  - VB Mask
    - Highest Match
    - VB Mask
      - D
  - BB Mask
    - Radius Filter
    - Person Filter
  - LB Mask
    - Color
    - Color Filter
    - Recovered Background
    - Possible Recovered Backgrounds
  - Repeat for all frames

- Same VB other videos
- Virtual Reconstruction
  - R
- Original
  - Virtual Background
- Blend Blur
  - Video Caller
  - Leaked Background

IEEE/IFIP DSN 2022
Leaked Background Reconstruction

- Video
  - Same VB other videos
- VB Mask
  - Highest Match
  - Virtual Reconstruction
- BB Mask
  - Radius Filter
  - Repeat for all frames
- LB Mask
  - Person Filter
  - Color Filter
  - Recovered Background

Possible Recovered Backgrounds
Leaked Background Reconstruction

Video

VB Mask

D

Highest Match

Virtual Reconstruction

R

Same VB other videos

BB Mask

Radius Filter

Person Filter

Color Filter

Recovered Background

Possible Recovered Backgrounds

LB Mask

Color

Repeat for all frames
Leaked Background Reconstruction

Video

VB Mask

D

Highest Match

Virtual Reconstruction

R

Same VB other videos

BB Mask

Radius Filter

Person Filter

Color Filter

Recovered Background

LB Mask

Color

Possible Recovered Backgrounds

Repeat for all frames
Leaked Background Reconstruction

Video

Same VB other videos

Virtual Reconstruction

Highest Match

D

Radius Filter

Repeat for all frames

Recovered Background

Person Filter

Color Filter

Color

LB Mask

Possible Recovered Backgrounds

BB Mask

Radius Filter

Video

VB Mask

R

 IEEE/IFIP DSN 2022
Leaked Background Reconstruction

- Video
  - VB Mask
    - D
    - Highest Match
    - Virtual Reconstruction
      - R
    - Same VB other videos
  - BB Mask
    - Radius Filter
    - Person Filter
  - LB Mask
    - Color
    - Color Filter
    - Recovered Background
      - Possible Recovered Backgrounds

Repeat for all frames
DeepLab V3
Why Person Detection?
Leaked Background Reconstruction

Video

Same VB other videos

VB Mask

Highest Match

BB Mask

Radius Filter

Virtual Reconstruction

Person Filter

Color Filter

LB Mask

Color

Recovered Background

Possible Recovered Backgrounds

Repeat for all frames
Leaked Background Reconstruction

Video

VB Mask
- Highest Match
- Virtual Reconstruction

BB Mask
- Radius Filter

LB Mask
- Person Filter
- Color Filter
- Recovered Background

Same VB other videos

Possible Recovered Backgrounds

Repeat for all frames
Adversary’s Goals

**Attack 1:** Reconstruct leaked background

**Attack 2:** Determine location from pre-set possibilities?

**Attack 3:** Detect if a specific object exists in leaked background?

**Attack 4:** Detect generic objects in the leaked background?
## Experimental Setup

<table>
<thead>
<tr>
<th>E1</th>
<th>E2 Passive</th>
<th>E2 Active</th>
<th>E3</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 participants</td>
<td>5 participants</td>
<td>5 participants</td>
<td>N/A</td>
</tr>
<tr>
<td>Controlled</td>
<td>Partial Controlled</td>
<td>Partial Controlled</td>
<td>Uncontrolled</td>
</tr>
<tr>
<td>Different Actions and Background Settings</td>
<td>Non-Interactive Video Caller</td>
<td>Interactive Video Caller</td>
<td>Videos in the Wild</td>
</tr>
<tr>
<td>163 videos</td>
<td>20 videos</td>
<td>5 videos</td>
<td>50 videos</td>
</tr>
</tbody>
</table>
E1 Reconstructed Background Recovery Rate (RBRR)

Participants 1 2 3 4 5

Actions

RBRR

IEEE/IFIP DSN 2022
Example
RBRR E2 and E3

Participants:
- Passive
- Active
- Wild

RBRB:
- 0
- 20
- 40
- 60
- 80
- 100

Avg:
- 1
- 2
- 3
- 4
- 5
Adversary’s Goals

**Attack 1:** Reconstruct leaked background

**Attack 2:** Determine location from pre-set possibilities?

**Attack 3:** Detect if a specific object exists in leaked background?

**Attack 4:** Detect generic objects in the leaked background?
Location Inference

- Adversary have $n$ possible backgrounds
- Adversary have reconstructed backgrounds
- Apply modified Iterative closest point (ICP) Alg. that takes two metrics: color and distance for all reconstructed backgrounds and possible backgrounds
- Rank matches based on the color/distance to the matches after modified ICP.
Location Inference Results

![Bar chart showing the percentage of dictionary for different inference methods: Passive, Active, Wild, Random (Wild). The chart compares Top-1, Top-5, Top-10, and Top-25 results.]
Adversary’s Goals

Attack 1: Reconstruct leaked background

Attack 2: Determine location from pre-set possibilities?

Attack 3: *Detect if a specific object exists in leaked background?*

Attack 4: Detect generic objects in the leaked background?
Specific Matching
Adversary’s Goals

**Attack 1:** Reconstruct leaked background

**Attack 2:** Determine location from pre-set possibilities?

**Attack 3:** Detect if a specific object exists in leaked background?

**Attack 4:** Detect generic objects in the leaked background?
Generic Object Matching

TextFuseNet

COCO and RetinaNet
Adversary’s Goals

Attack 1: Reconstruct leaked background

Attack 2: Determine location from pre-set possibilities?

Attack 3: Detect if a specific object exists in leaked background?

Attack 4: Detect generic objects in the leaked background?

How can we stop an adversary??
Dynamic Virtual Background

• Make it harder to differentiate virtual background from leaked background

• Modify virtual background using the changes from the real background that it masks.
  • brightness and saturation

• Fluctuate hue values over multiple close hue values
Dynamic Virtual Background Results
Dynamic Virtual Background Location Results

![Bar chart showing the percentage of videos for different categories: Passive, Active, Wild, Random (Wild)]

- **Top-1**
- **Top-5**
- **Top-10**
- **Top-25**

Percentage of videos: 0, 20, 40, 60, 80, 100
Take away message

• Virtual Background feature does not guarantee privacy in online video calls and real background reconstruction is possible.

• Significant motion such as leaving the room during an online video call can leak more background compared to other activities.

• Virtual background attacks could be mitigated using dynamic virtual background.
Questions?