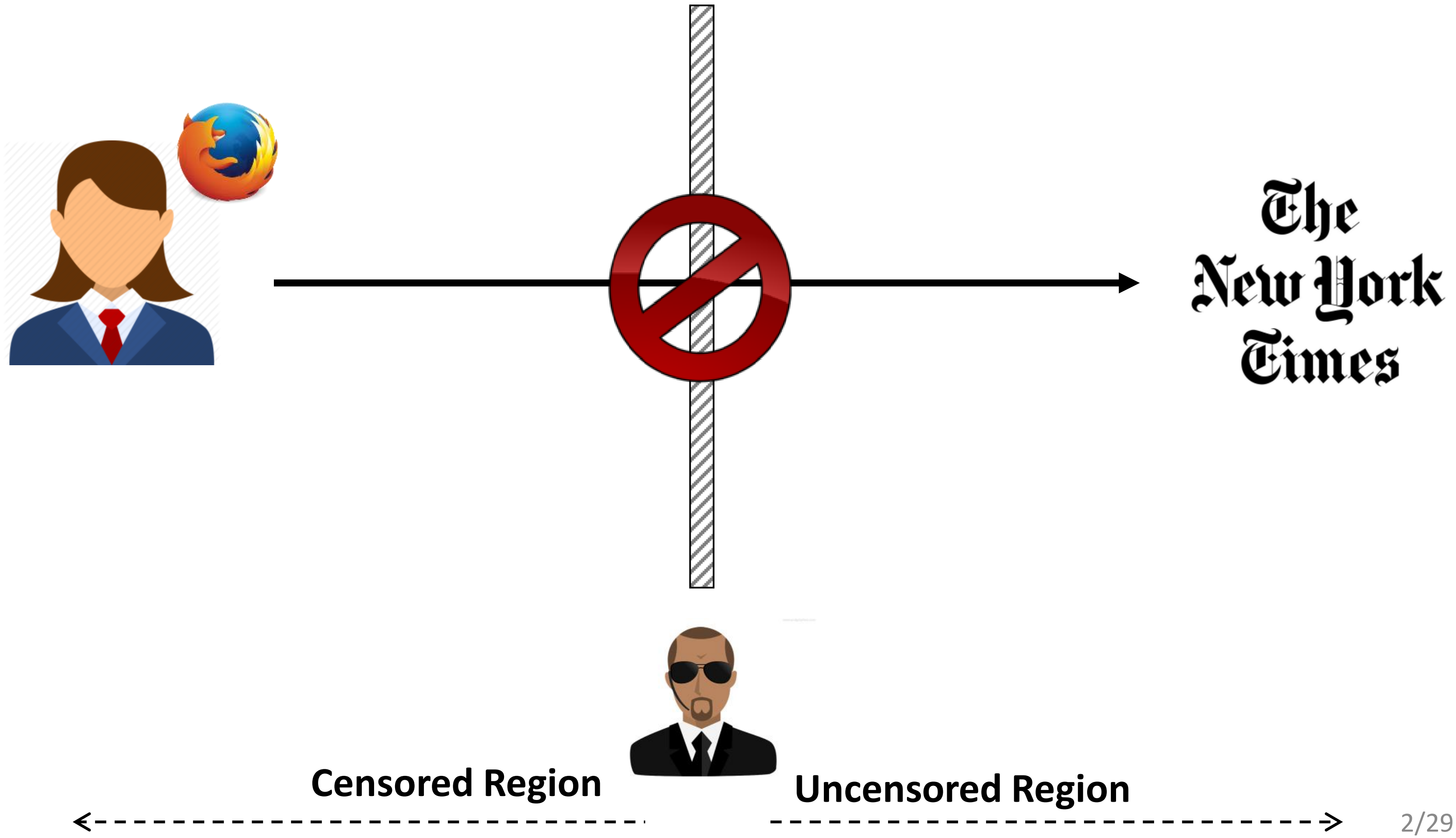
DeltaShaper
Enabling Unobservable Censorship-resistant TCP Tunneling over Videoconferencing Streams

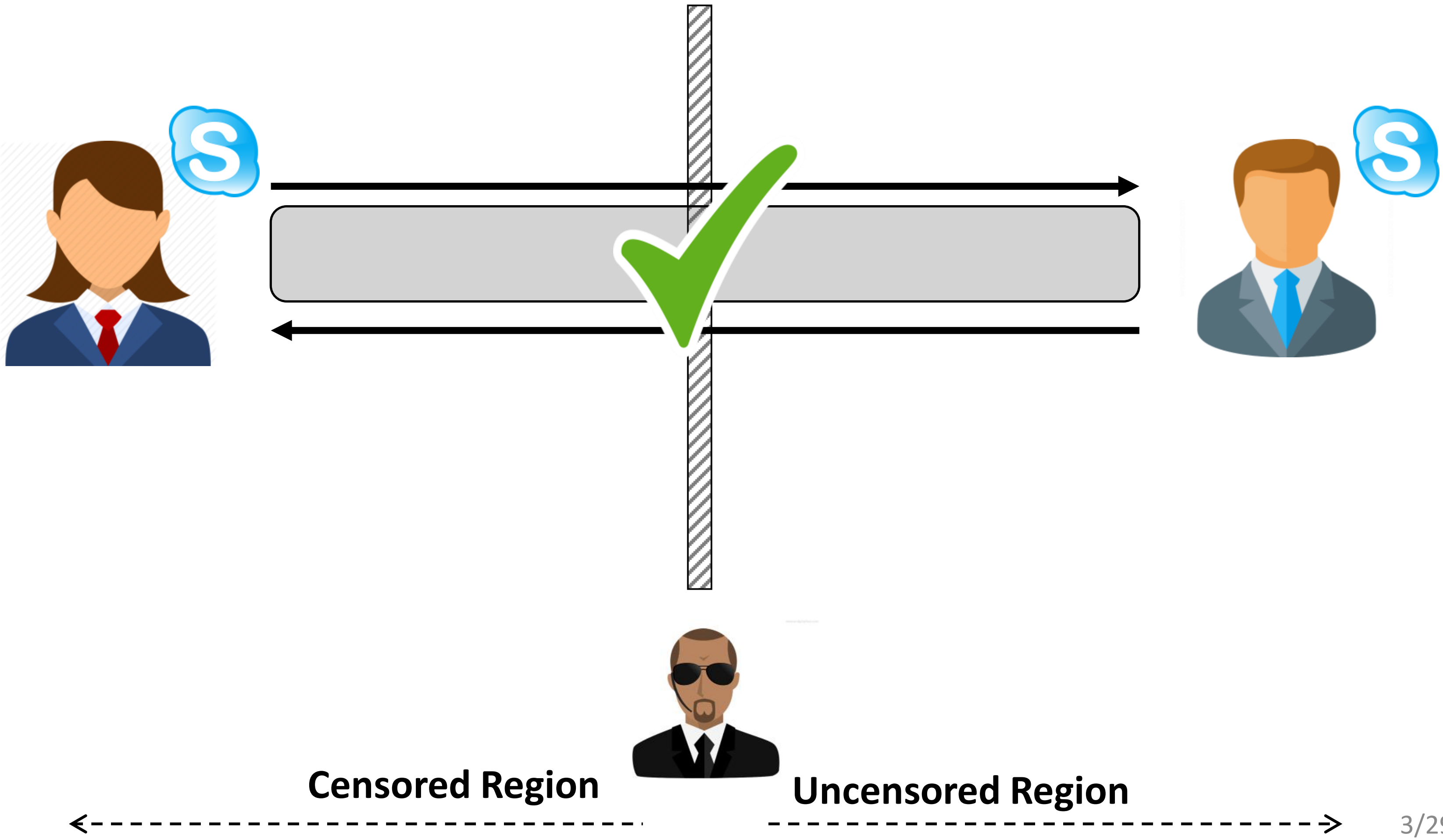
Diogo Barradas Nuno Santos Luís Rodrigues

INESC-ID, Instituto Superior Técnico, Universidade de Lisboa

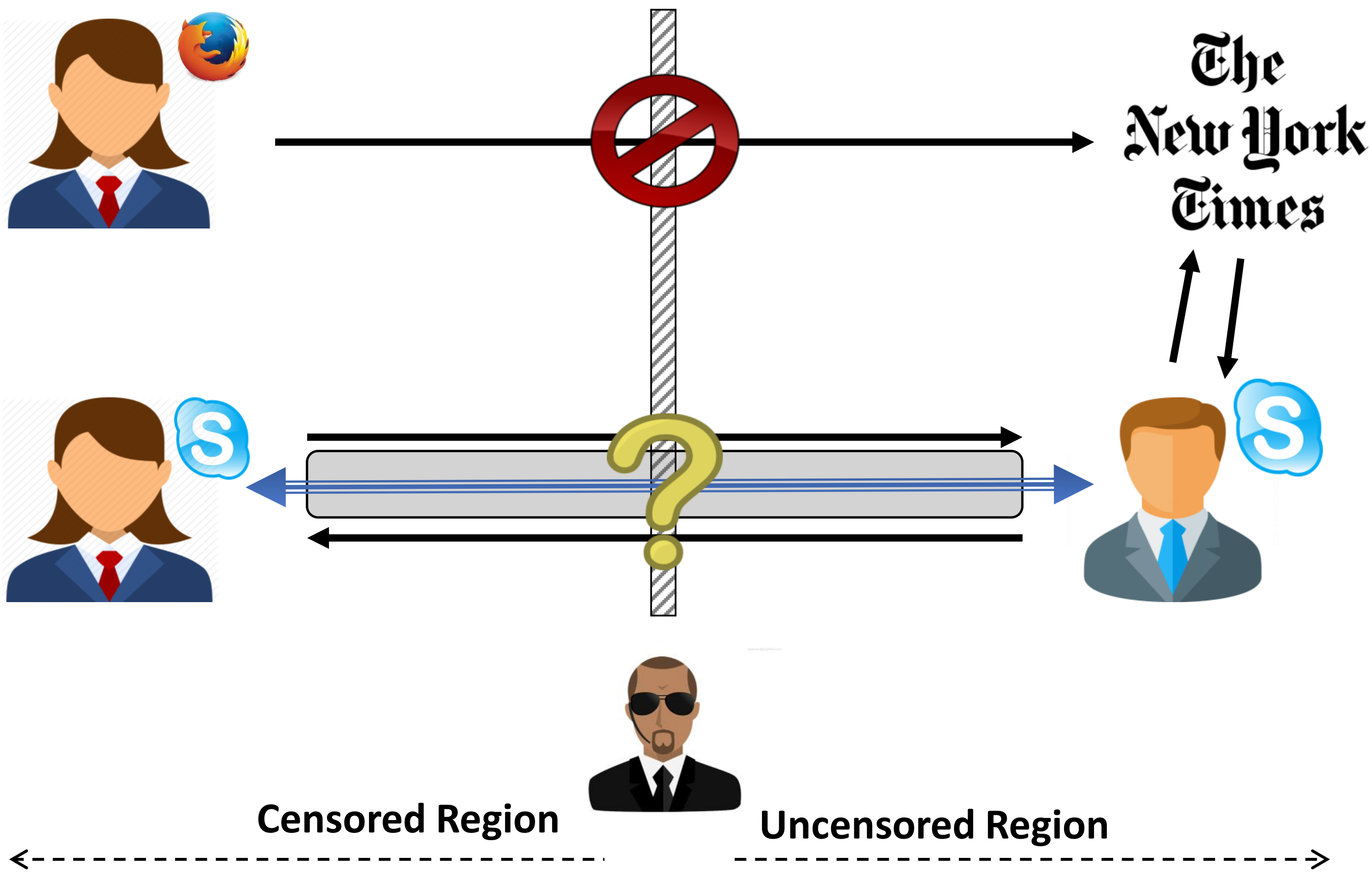
Censors monitor / control Internet access



Censors monitor / control Internet access

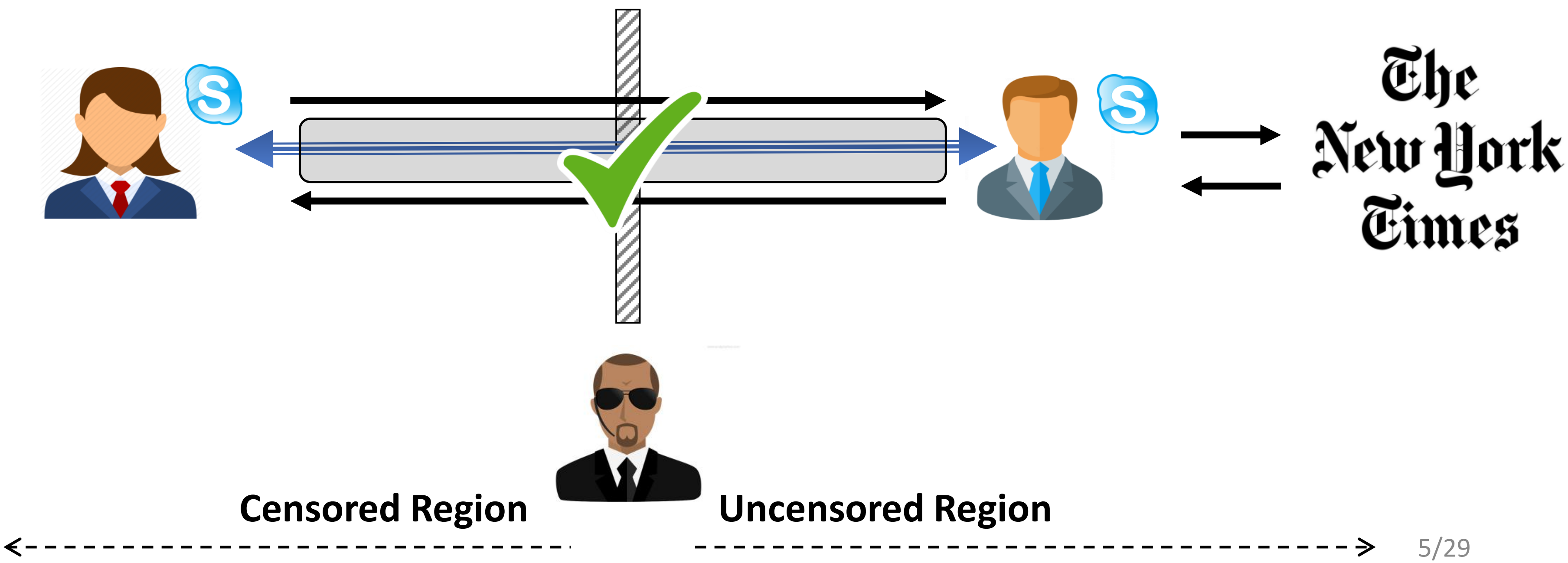


Censors attempt to block covert channels



DeltaShaper

- **Goals**
  - Establish a covert TCP/IP channel
  - Maintain unobservability
  - Resist against network perturbations



Multimedia protocol tunneling

	Security		Coverage
System / Properties	**Active/Passive Attack Resistance**	**Arbitrary Data Transmission**	**Interactive Communication**
FreeWave *(Houmansadr et al.)* *Audio Modulation*	-	✓	✓
Facet *(Li et al.)* *Video Embedding*	✓	-	-
CovertCast *(McPherson et al.)* *Video Modulation*	✓	✓	-
DeltaShaper *Video Modulation*	✓	✓	✓

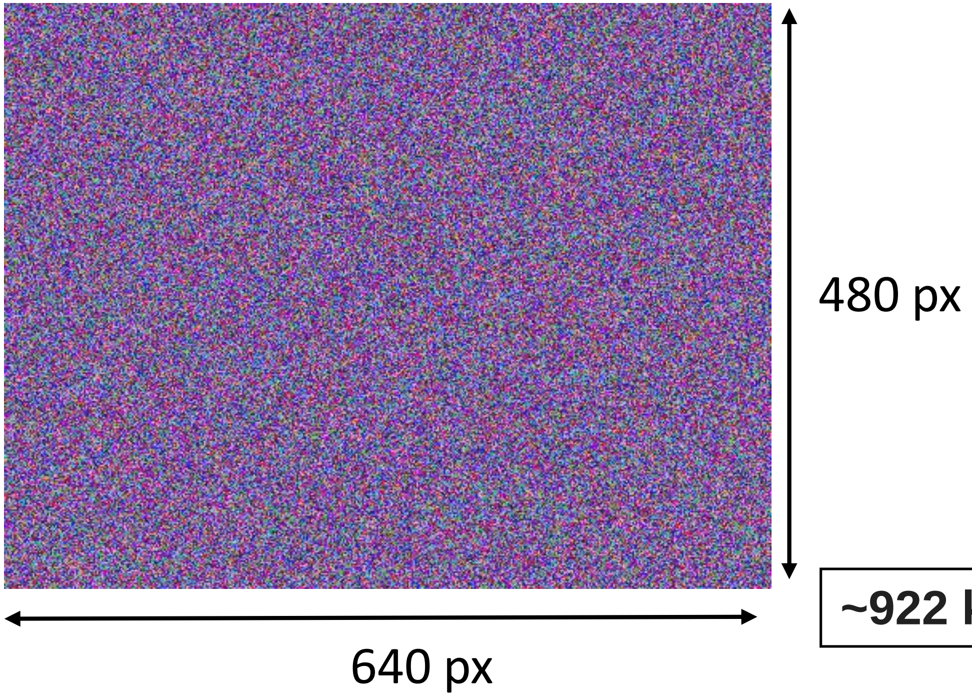
Threat model

- **Assumptions:**
  - Packets carrying multimedia data are encrypted
- **Censor's Capabilities:**
  - *Deep Packet Inspection*
  - Observe, store and analyze traffic flows
  - Apply artificial constraints on the network
- **Censor's Limitations:**
  - Unable to decipher the content of Skype packets
  - Not in collusion with the video-conferencing provider
  - Attempts to minimize collateral damage

A naïve approach at data modulation

- **Replace chat video frames**
- **Encode data in all available pixels**

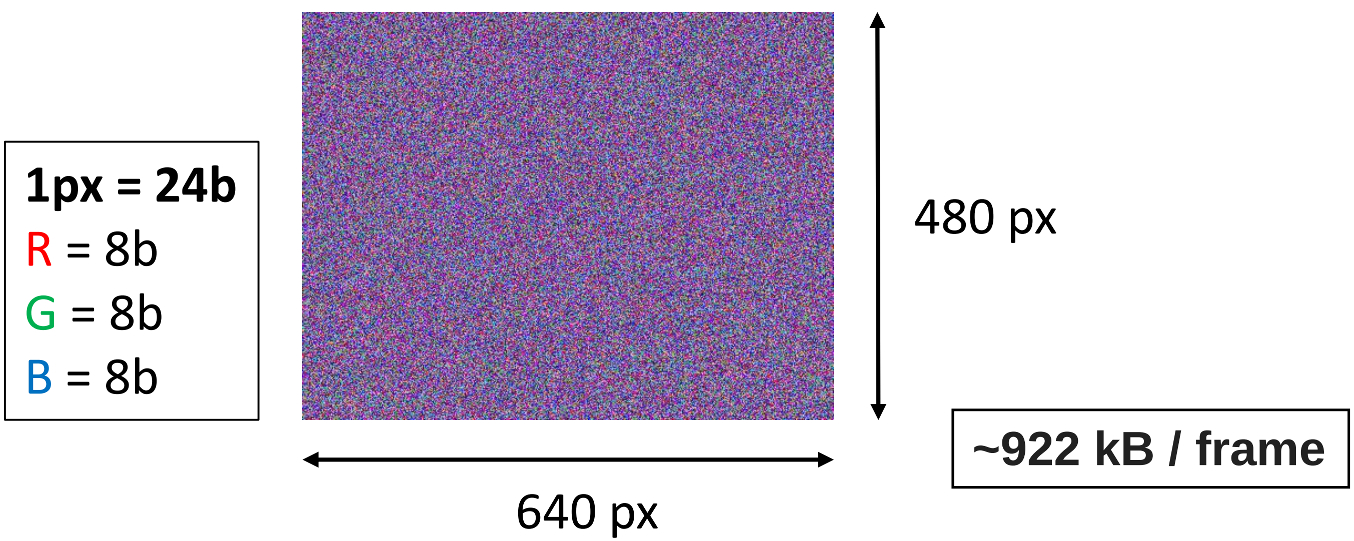
1px = 24b
R = 8b
G = 8b
B = 8b



~922 kB / frame

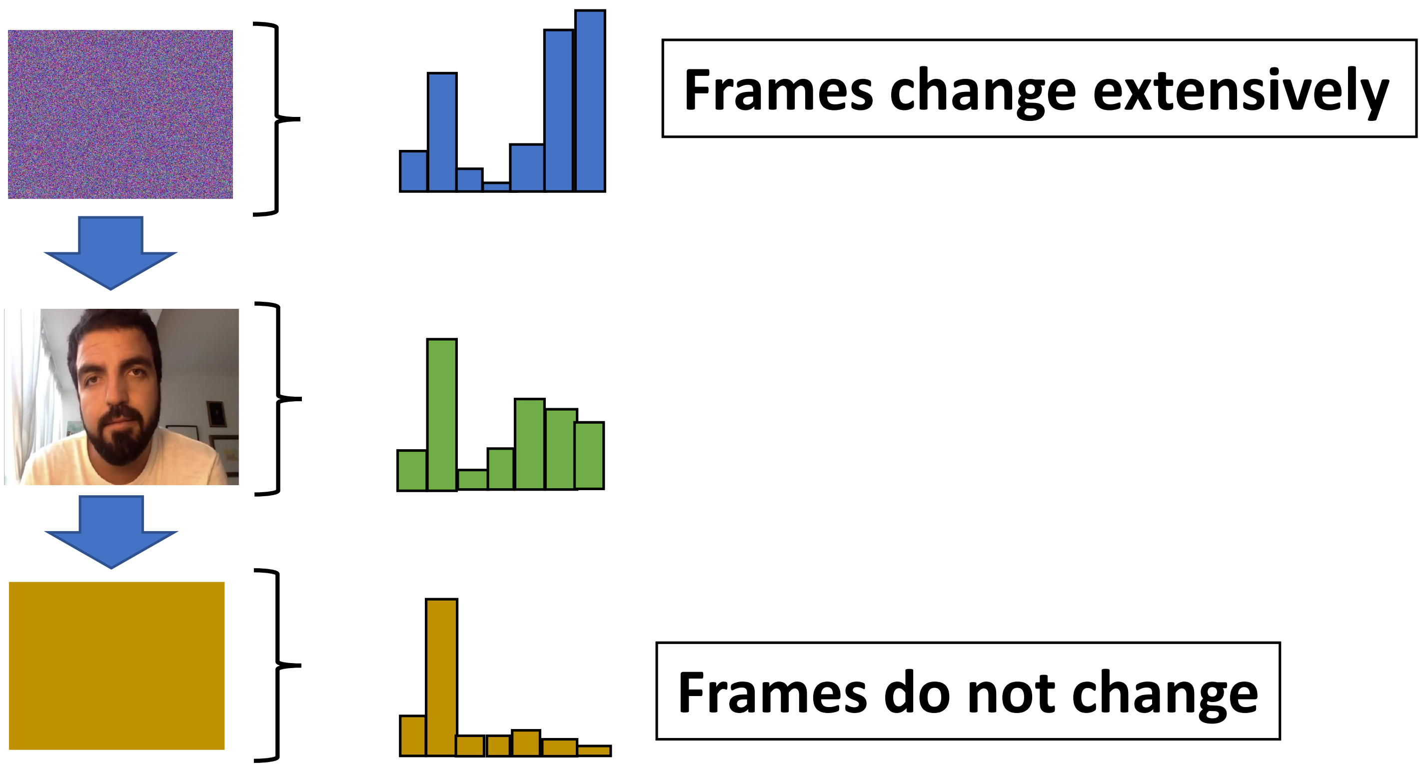
Drawbacks of naïve data modulation

- **Data loss**
  - Lossy compression (downsampling + quantization)
- **Abnormal traffic patterns**
  - Poor compression (spatial & inter-frame redundancy)

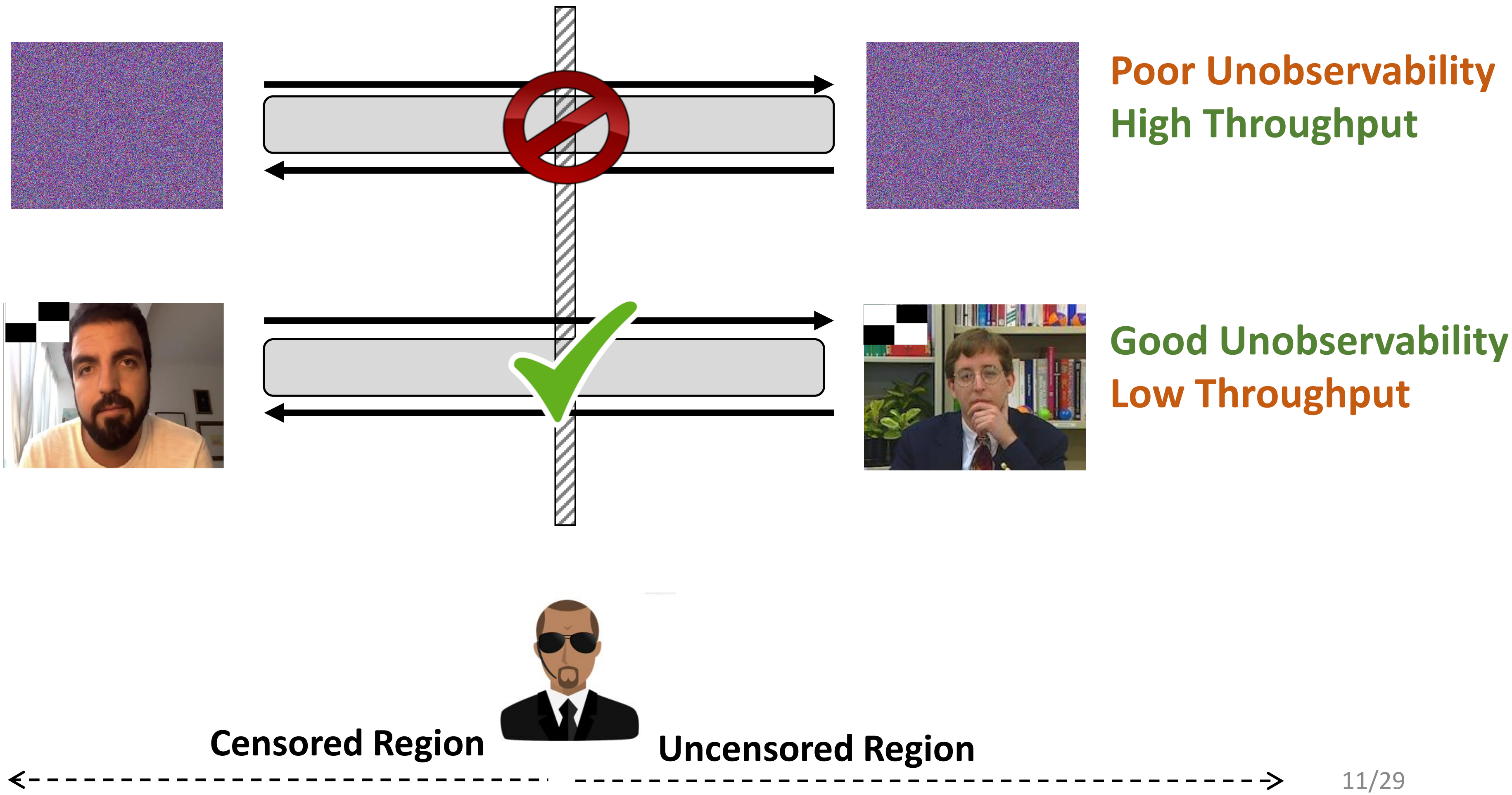


C1: Can we distinguish regular from irregular Skype streams?

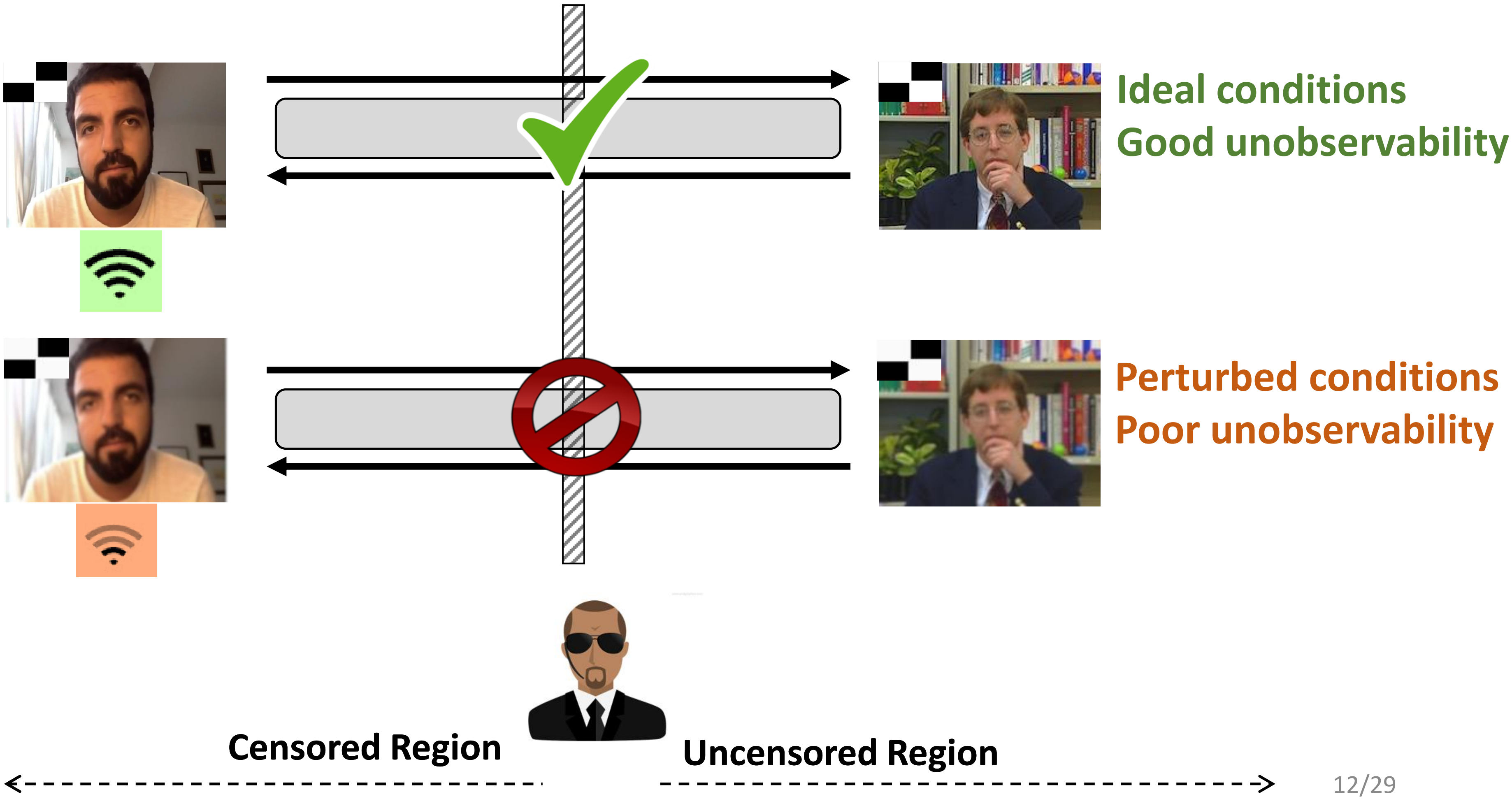
- **Traffic signatures appear to be different**
  - Packet lengths frequency distribution



C2: How much throughput can we achieve while preserving unobservability?



C3: How to maintain unobservability in adverse network conditions?

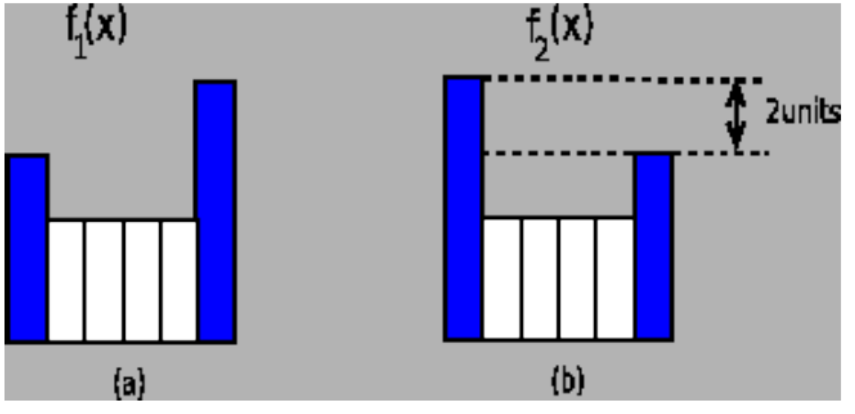


Contributions

- **DeltaShaper : A censorship-resistant system**
  - Tunnel TCP/IP data over Skype videocalls
- **Distinguish regular / irregular Skype call streams**
  - Packet frequency distribution / EMD
- **Maximize throughput and maintain unobservability**
  - Explore the space encoding parameters
- **Adaptation to network conditions**
  - Dynamic calibration of encoding parameters

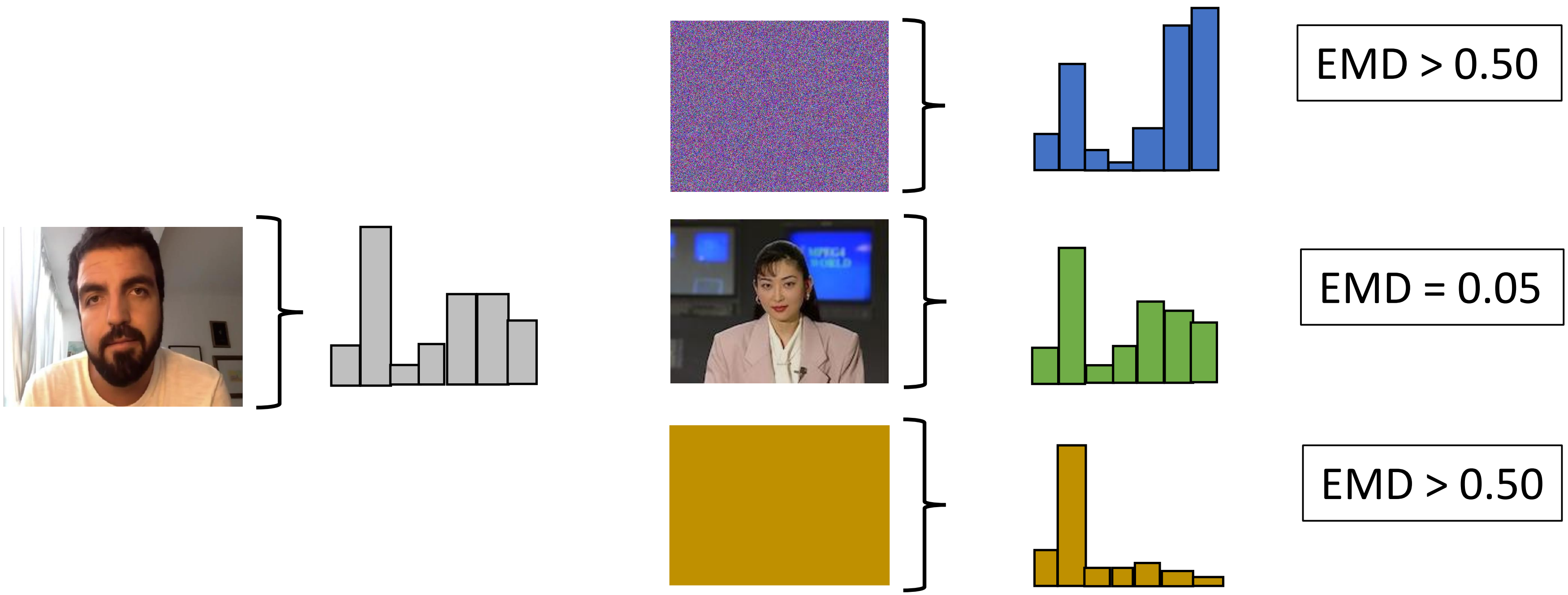
How to characterize Skype streams?

- **Characteristic Function - Create a stream signature**
  - Frequency distribution of packet lengths
- **Similarity Function - Quantify streams' differences**
  - *Earth Mover's Distance* (EMD)



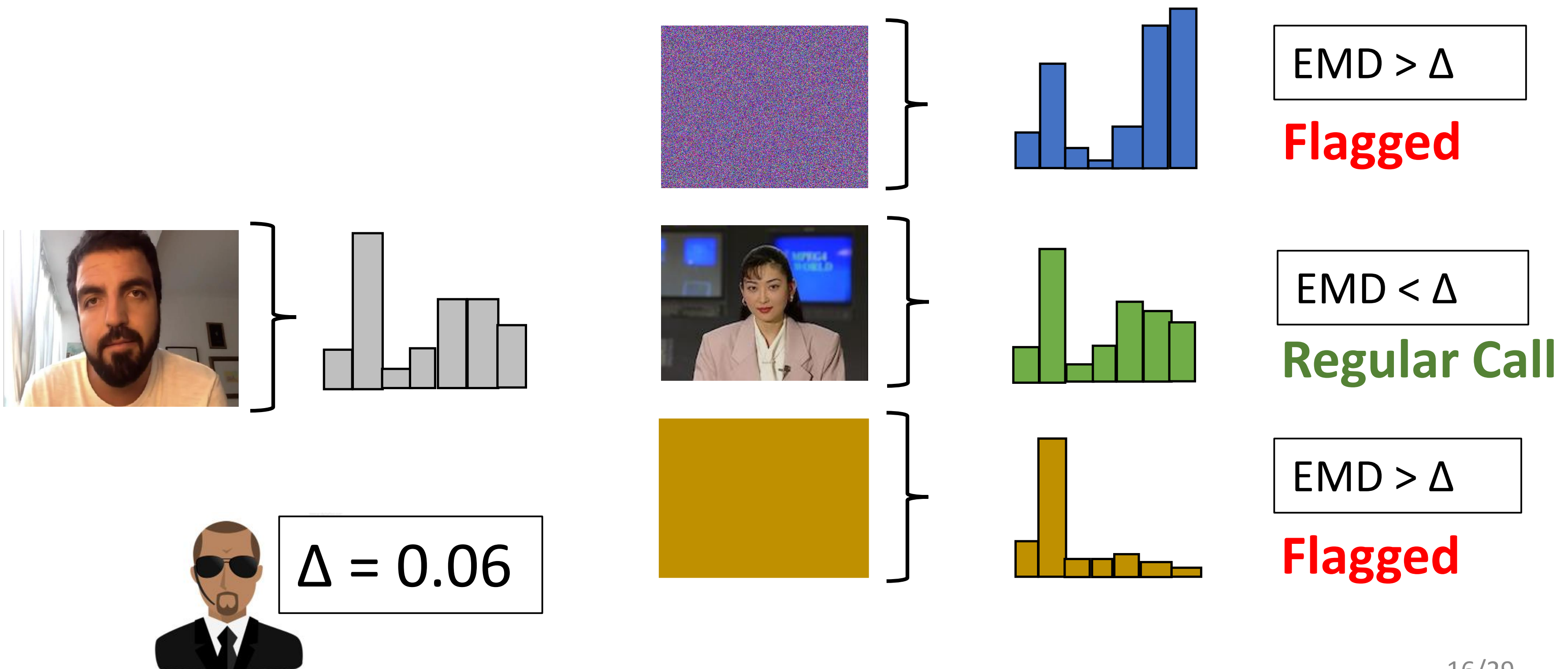
Different videos generate distinct traffic

- **Differences between signatures can be quantified**
  - *Earth Movers' Distance*



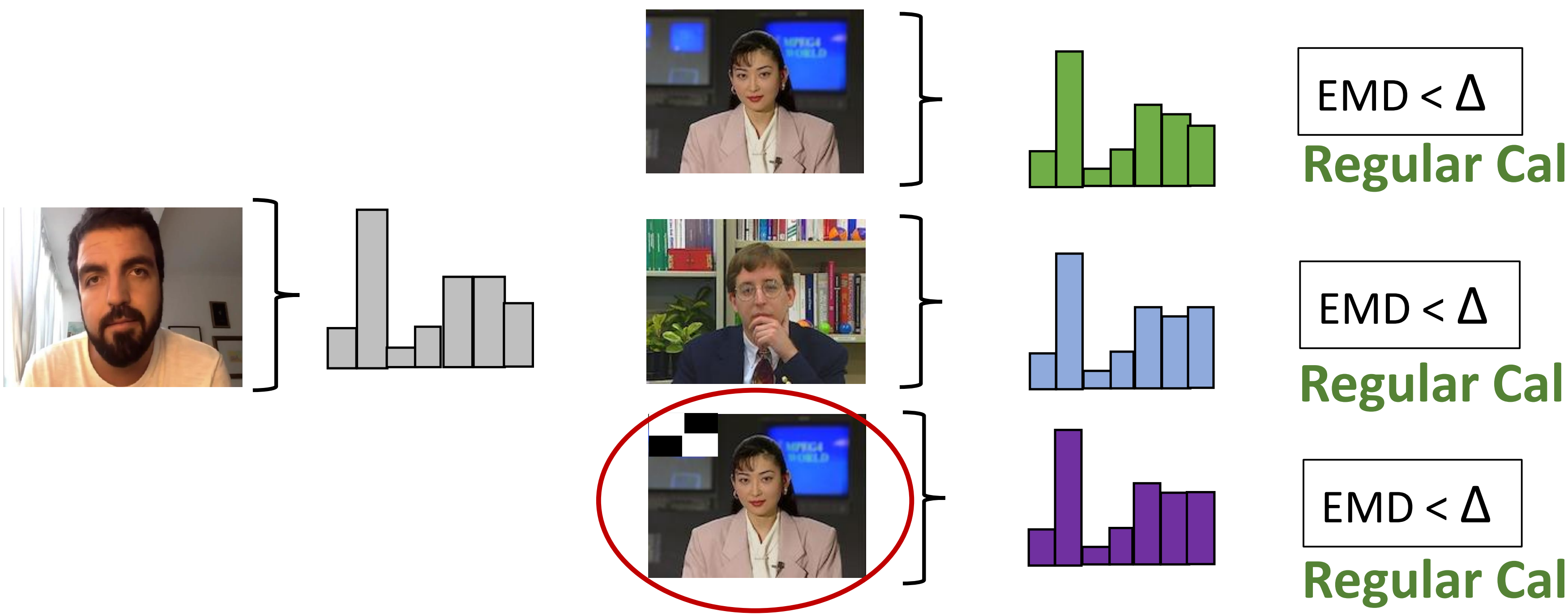
Different videos generate distinct traffic

- **Censors can identify streams with unusual traffic**



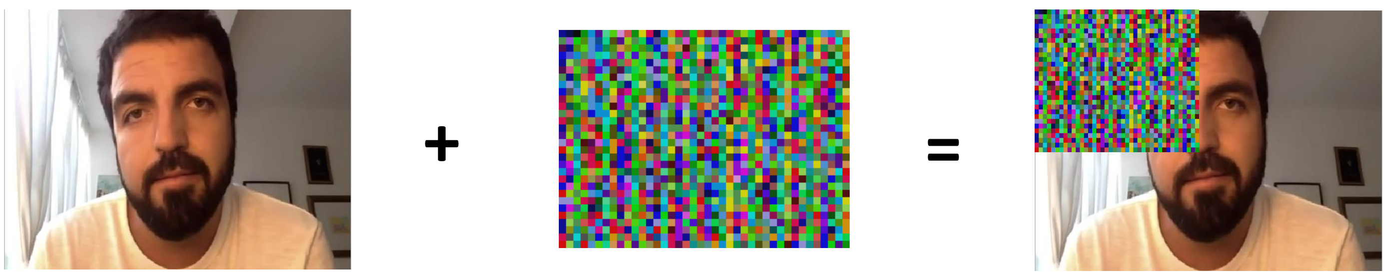
Can we encode data and maintain unobservability?

- **Strawman: Embed a small payload in each frame**
- **Generated traffic does not reflect this embedding**



A better approach for data modulation

- **Strive for unobservability**
- **Accommodate for lossy compression**

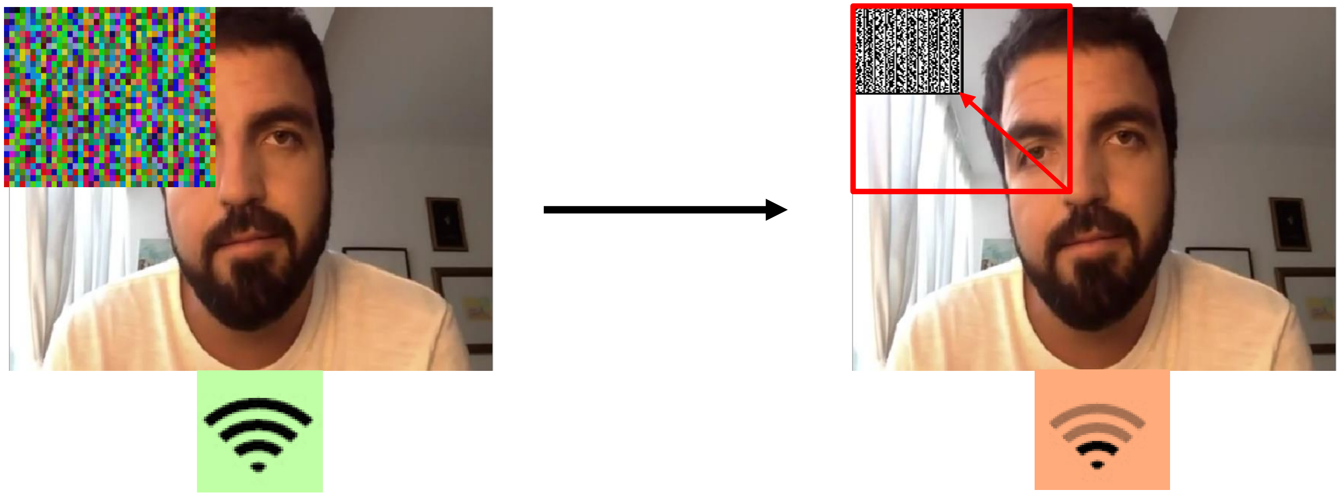


(a) Carrier Frame (b) Payload Frame (c) Covert Frame

Parameter	Description
a_p	payload frame area (pixel×pixel)
a_c	cell size (pixel×pixel)
b_c	color encoding (bits)
r_p	payload frame rate (frames/s)

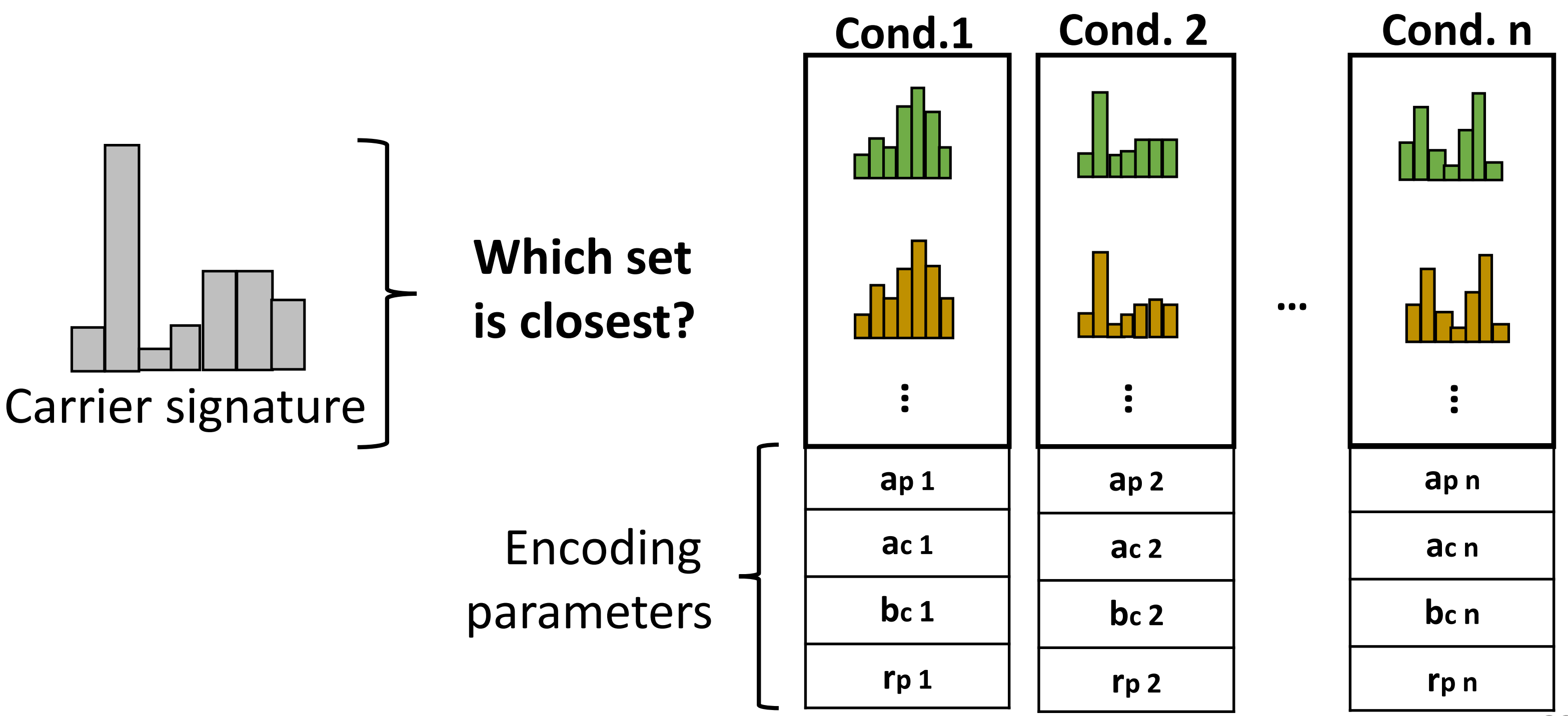
Adapt to network conditions

- **Calibrate encoding parameters**
  - Maintain unobservability
  - Modulate max. amount of data



DeltaShaper adaptation mechanism

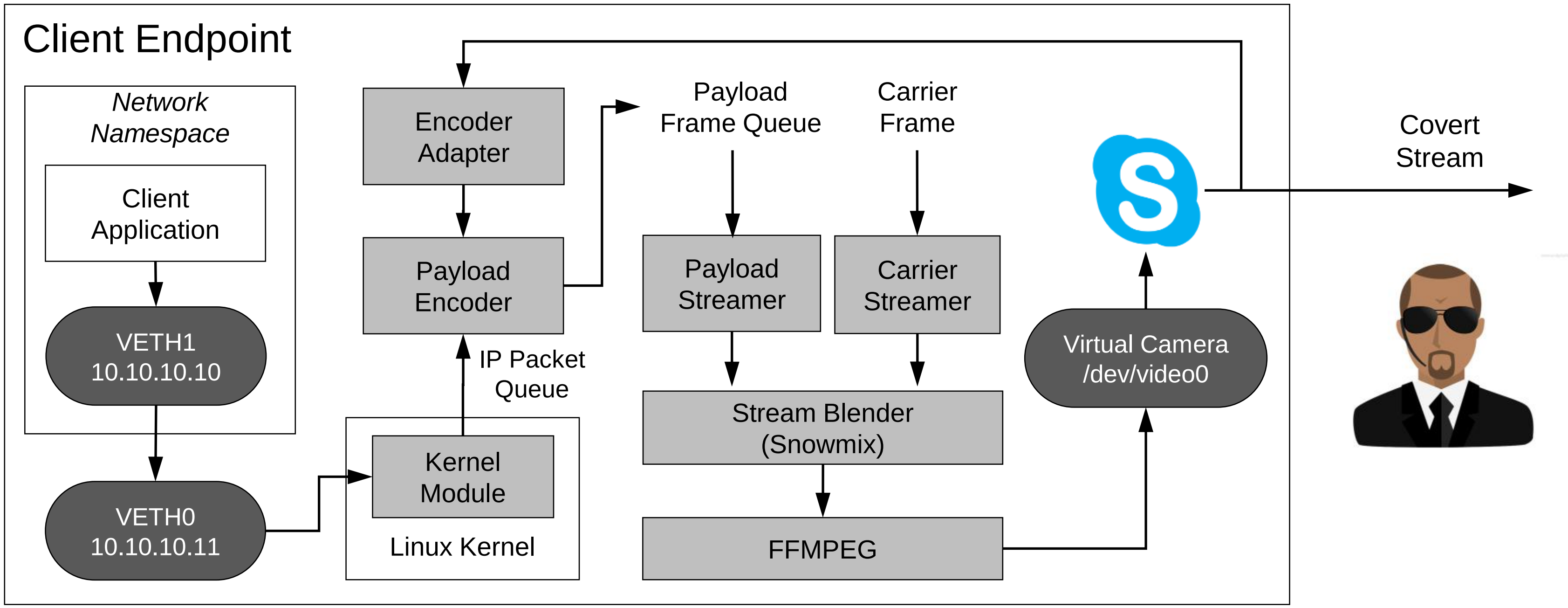
- **Periodically:**
  - Estimate network conditions from recorded baselines
  - Select adequate parameters from pre-computed table



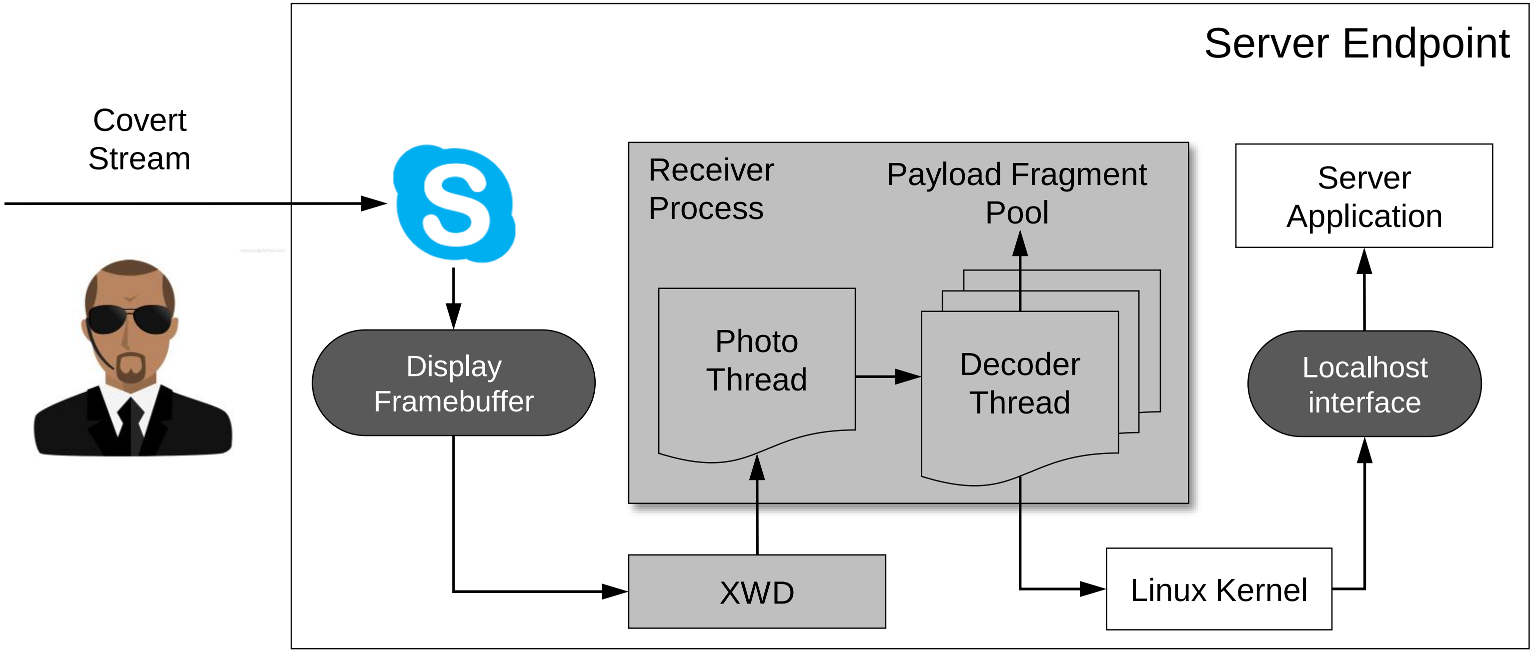
Implementation challenges

- **Network interaction**
  - Allow transparent TCP/IP communication
- **Video processing**
  - Combine carrier / payload frames
- **Video-conferencing software as a *black-box***
  - Send covert frames without modifying Skype

DeltaShaper client module



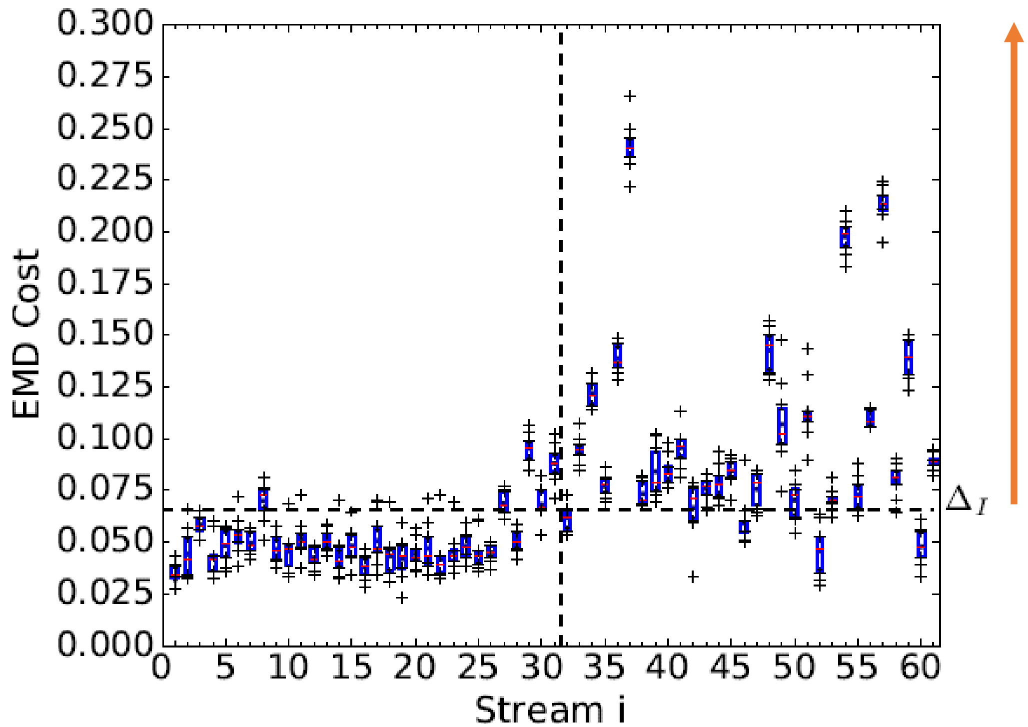
DeltaShaper server module

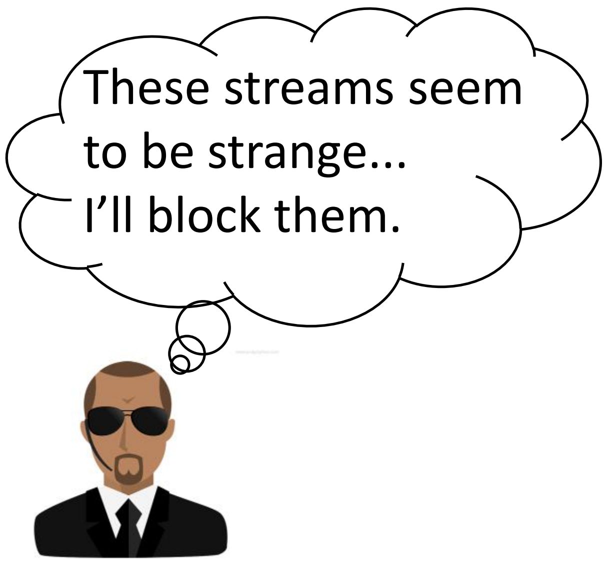


Evaluation Steps

1. **Can we distinguish Skype streams?**
2. **Can we balance throughput and unobservability?**
3. **How well does DeltaShaper perform?**

Can we distinguish Skype streams?





- **83% accuracy in distinguishing Skype streams**
- **DeltaShaper streams must remain under** Δ_I

Can we balance throughput and unobservability?

Parameter	Description	Configuration
a_p	payload frame area (pixel×pixel)	320 x 240
a_c	cell size (pixel×pixel)	8 x 8
b_c	color encoding (bits)	6
r_p	payload frame rate (frames/s)	1

How well does DeltaShaper perform?

- **Achieved configuration:**

Parameter	Description	Configuration
a_p	payload frame area (pixel×pixel)	320 x 240
a_c	cell size (pixel×pixel)	8 x 8
b_c	color encoding (bits)	6
r_p	payload frame rate (frames/s)	1

- **Performance**
  - Raw throughput: **7.2 Kbps**
  - Round-Trip-Time: **2s 973ms**

How well does DeltaShaper perform?

Use Case	Protocol Session W/ DS (mm:ss)	Protocol Session W/o DS (mm:ss)	Overhead
Wget (4kB file)	0:22	< 0:01	3,142.9 x
FTP (4kB file)	1:43	0:09	11.4 x
SSH + SMTP	2:41	0:38	4.2 x
SSH	1:29	0:06	14.8 x
Telnet	1:13	0:06	12.2 x
Netcat chat	0:01	< 0:01	166.7 x
SSH Tunnel	2:19	0:22	6.3 x

Non-interactive session
Interactive session

- **DeltaShaper allows for the execution of traditional TCP/IP applications which cover different users' needs**

Conclusions

- **DeltaShaper: A censorship-resistant system**
  - Supports high-latency / low-throughput TCP applications
- **Maximize throughput and preserve unobservability**
  - Greedy exploration of encoding configurations
- **Adaptation in multimedia protocol tunneling**
  - Provides improved unobservability
  - Could also enhance similar systems