Light Weight Video Fingerprints for Video Playback Verification in MPEG DASH

Zhu Li and Imed Bouazizi
Multimedia Standards Research
Samsung Research America
Outline

• Motivation
• Ads Playback Verification
• Light Video Fingerprint for Verification
• Simulation Results
• Conclusion & Future Work
MPEG DASH System

- MPEG DASH Video System
  - Client “pull” based solution
  - HTTP Server with minimum intelligence on the server side
- MPD – Media Presentation Description
Ads in MPEG DASH

- Ads in DASH
  - Pre-spliced into the content
  - Period based Ads segments

- DASH is an open and client driven system, how to verify that ads are actually played out at the client?
  - Create content period/segment serving dependence at the server
Playback Verification in DASH

- Introduce a playback verification server
  - Client playback the content, will compute a fingerprints and send to the server for verification
Challenges

• The fingerprint extraction and verification should have minimum computational complexity for the client and verification server, such that the solution is scalable.
• The communication overhead of fingerprints should be very small
• Invariant to different rates of the ads period
• Should have very high True Positive Rate (TPR)
• The False Positive Rate (FPR) should be very low
Eigen Appearance Trajectory

- Motivated by the Eigenface work, bring video sequences to the Eigen appearance space

\[ f_k \]  
\[ A \]  
\[ X \]  
\[ X_k \]
Differential Eigen-Appearance Signature

- Ads sequences are typically of high activities,
- The differentials of the Eigenappearance trajectories captures a very useful signature for verification

\[ dx(k) = \begin{cases} 0, & \text{if } k = 1 \\ A\hat{f}_{k+1} - A\hat{f}_k, & \text{else} \end{cases} \]
Fingerprints Verification

- Distance metric between two $m$-frame fingerprints
  \[ d(dx^1, dx^2) = \frac{1}{m} \sum_k (dx^1(k) - dx^2(k)) \]
- Verification by thresholding on $d(dx^1, dx^2)$
  - Rejecting different sequences, while accommodating rates variations
Noise suppression

- Ads sequences usually have many cuts

- Differential signature value at cuts are noisy, remove by,

\[
dx(k) = \begin{cases} 
0, & \text{if } k = 1 \\
d_{\text{max}}, & \text{else if } A(f_{k+1} - f_k) > d_{\text{max}} \\
A(f_{k+1} - f_k), & \text{else}
\end{cases}
\]
Simulation Setup

• Data Set:
  – 4000 ads clips of durations 15s, 30s and 60s
  – Simulating 3 DASH streaming rates: 480, 640, and 800kbps
  – 100+ hours of distraction video data sets from youtube, TRECVID, coded at various rates between 300kbps to 1mbps

• Probes set up, for each test ads sequence,
  – Positive probes: lower rates sequence probing 800kbps
  – Negative probes: randomly select 10 sequences from the distraction set
Simulation Results

• **Signature Computing:**
  – 1-d signature from 6-dim Eigen Appearance space
  – Approximately 200bits/sec for 25fps sequence, regardless of its frame size and bit rate, very small overhead

• **Computation complexity**
  – At client, less than 0.5% of ffmpeg decoding
  – At verification server, O(m), very small
Simulation Results

• Accuracy
  – For 100% TPR, i.e, no positive probes are rejected, the FPRs are,

<table>
<thead>
<tr>
<th>R</th>
<th>t=60s</th>
<th>t=30s</th>
<th>t=15s</th>
</tr>
</thead>
<tbody>
<tr>
<td>640kbps</td>
<td>0.15%</td>
<td>0.52%</td>
<td>1.30%</td>
</tr>
<tr>
<td>480kbps</td>
<td>0.15%</td>
<td>0.60%</td>
<td>3.15%</td>
</tr>
</tbody>
</table>
Conclusion & Future Work

• Conclusion
  – Introduced a DASH video playback verification system and protocol
  – Developed a light weight, robust video fingerprints for video playback verification, the performance in accuracy is good, while at minimum computation and communication overhead

• In the future,
  – develop a binarized fingerprints for even faster verification
  – Automatic token hash generation
Q&A

• Questions....

Thanks/Gracias