FAST PROTECTION OF H.264/AVC BY SELECTIVE ENCRYPTION OF CABAC

Zafar SHAHID, Marc CHAUMONT, William PUECH
(zafar.shahid@lirmm.fr)
LIRMM, UMR CNRS 5506, Université Montpellier II
Talk Outline

✓ Problem Statement
✓ CABAC
  ✓ Block diagram
  ✓ Binarization
✓ Proposed Approach
  ✓ Proposed scheme in H.264/AVC
  ✓ Proposed scheme for non-zero coefficients
  ✓ Encryption process
✓ Results
  ✓ Visual comparison of encrypted frames at different QPs
  ✓ Foreman sequence encryption at different QPs
  ✓ Nine benchmark video sequences results at same QP.
✓ Conclusions
Problem Statement

To perform selective encryption (SE) of CABAC for real-time protection of H.264/AVC bitstream.

Constraints:

✓ Same bitrate
✓ No increase in processing power
✓ Browseable bitstream
Our Approach

1. SE is performed in Context-based Adaptive Binary Arithmetic Coding (CABAC) module.

2. Same bitrate is achieved through scrambling of only equal length binarized code words.

3. Encrypted bitstream is completely compliant to H.264/AVC format. (ONLY MB data is encrypted.)
Talk Outline

- Problem Statement
- **CABAC**
  - Block diagram
  - Binarization
- Proposed Approach
  - Proposed scheme in H.264/AVC
  - Proposed scheme for non-zero coefficients
  - Encryption process
- Results
  - Visual comparison of encrypted frames at different QPs
  - Foreman sequence encryption at different QPs
  - Nine benchmark video sequences results at same QP.
- Conclusions
CABAC

Context modeling

Binarization

Regular BAC

Bypass BAC

Syntax Element

Binary syntax element

Non-binary syntax element

H.264/AVC bitstream

Context update

Binary Arithmetic Coder
CABAC codes the input data in the following steps:

1. **Binarization**
   It is performed in one of the following ways:
   1. The unary code
   2. The truncated unary code
   3. The kth order Exp-Golomb code
   4. The fixed length code

2. **Context modeling**

3. **Binary Arithmetic Coding**
Talk Outline

✓ Problem Statement
✓ CABAC
  ✓ Block diagram
  ✓ Binarization
✓ Proposed Approach
  ✓ Proposed scheme in H.264/AVC
  ✓ Proposed scheme for non-zero coefficients
  ✓ Encryption process
✓ Results
  ✓ Visual comparison of encrypted frames at different QPs
  ✓ Foreman sequence encryption at different QPs
  ✓ Nine benchmark video sequences results at same QP.
✓ Conclusions
Proposed Algorithms

Input Video → Integer Transform → Quantization → CABAC Encoding (with cipher) → Encrypted Bitstream

Secret Key → PRNG → CABAC Decoding (with decipher) → Inverse Quantization

Decoded Video → Inverse Transform → CABAC Decoding (with decipher) → Inverse Quantization → Quantization → Integer Transform → PRNG → Secret Key
Proposed Algorithms

- **Prefix UT binarization**
- **Suffix EGO binarization**
- **PRNG**
- **Scrambling**
- **Bitstream**

Diagram:
- NZ
- Secret Key
- |NZ|
- s
- sign bit
- 1...1
- 0
- X
- n bits
- se
- n bits
- se
- B A C
- Bitstream
Encryption Process

- NZs are scrambled with only those NZs whose EGO (0th order Exp-Golomb code) codes have the same length.

- For encryption process:
  - Let $x$ be a suffix part of absolute level of NZ. It is encrypted with the encrypted coefficient $y$:
    - $y = (x + \gamma) \mod \log_2(x + 1)$,
    - Where
      - $\gamma = \text{rand()} \mod \log_2(x + 1)$.

- For decryption process:
  - For the decryption of NZs in H.264/AVC decoder:
    - $x = (y + \log_2(n + 1) - \gamma) \mod \log_2(y + 1)$. 
Talk Outline

✓ Problem Statement
✓ CABAC
  ✓ Block diagram
  ✓ Binarization
✓ Proposed Approach
  ✓ Proposed scheme in H.264/AVC
  ✓ Proposed scheme for non-zero coefficients
  ✓ Encryption process
✓ Results
  ✓ Visual comparison of encrypted frames at different QPs
  ✓ Foreman sequence encryption at different QPs
  ✓ Nine benchmark video sequences results at same QP.
✓ Conclusions
Results: Foreman 1\textsuperscript{st} Frame at diff. QPs

QP = 18

QP = 24

QP = 30

QP = 36
<table>
<thead>
<tr>
<th>QP</th>
<th>PSNR (Y) (dB)</th>
<th>PSNR (U) (dB)</th>
<th>PSNR (V) (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Without SE</td>
<td>With SE</td>
<td>Without SE</td>
</tr>
<tr>
<td>18</td>
<td>44.43</td>
<td>8.42</td>
<td>45.62</td>
</tr>
<tr>
<td>24</td>
<td>39.40</td>
<td>8.38</td>
<td>41.70</td>
</tr>
<tr>
<td>30</td>
<td>34.93</td>
<td>8.92</td>
<td>39.38</td>
</tr>
<tr>
<td>36</td>
<td>30.80</td>
<td>8.89</td>
<td>37.33</td>
</tr>
</tbody>
</table>
## Results – Nine seq. at QP = 18

<table>
<thead>
<tr>
<th>Seq.</th>
<th>PSNR (Y) (dB) Without SE</th>
<th>PSNR (Y) (dB) With SE</th>
<th>PSNR (U) (dB) Without SE</th>
<th>PSNR (U) (dB) With SE</th>
<th>PSNR (V) (dB) Without SE</th>
<th>PSNR (V) (dB) With SE</th>
</tr>
</thead>
<tbody>
<tr>
<td>bus</td>
<td>44.26</td>
<td>7.73</td>
<td>45.22</td>
<td>25.19</td>
<td>46.50</td>
<td>26.86</td>
</tr>
<tr>
<td>city</td>
<td>44.28</td>
<td>11.52</td>
<td>45.83</td>
<td>30.50</td>
<td>46.76</td>
<td>31.86</td>
</tr>
<tr>
<td>crew</td>
<td>44.81</td>
<td>9.39</td>
<td>45.81</td>
<td>23.80</td>
<td>45.66</td>
<td>19.90</td>
</tr>
<tr>
<td>football</td>
<td>44.59</td>
<td>11.46</td>
<td>45.70</td>
<td>15.79</td>
<td>45.98</td>
<td>23.10</td>
</tr>
<tr>
<td>foreman</td>
<td>44.43</td>
<td>8.42</td>
<td>45.62</td>
<td>23.87</td>
<td>47.42</td>
<td>22.14</td>
</tr>
<tr>
<td>harbour</td>
<td>44.10</td>
<td>9.48</td>
<td>45.60</td>
<td>23.82</td>
<td>46.63</td>
<td>31.20</td>
</tr>
<tr>
<td>ice</td>
<td>46.56</td>
<td>10.37</td>
<td>48.70</td>
<td>25.42</td>
<td>49.19</td>
<td>19.73</td>
</tr>
<tr>
<td>mobile</td>
<td>44.45</td>
<td>8.42</td>
<td>44.14</td>
<td>13.47</td>
<td>44.04</td>
<td>11.11</td>
</tr>
<tr>
<td>soccer</td>
<td>44.26</td>
<td>10.84</td>
<td>46.59</td>
<td>19.69</td>
<td>47.82</td>
<td>24.83</td>
</tr>
</tbody>
</table>
Talk Outline

✓ Problem Statement
✓ **CABAC**
  ✓ Block diagram
  ✓ Binarization
✓ **Proposed Approach**
  ✓ Proposed scheme in H.264/AVC
  ✓ Proposed scheme for non-zero coefficients
  ✓ Encryption process
✓ Results
  ✓ Visual comparison of encrypted frames at different QPs
  ✓ Foreman sequence encryption at different QPs
  ✓ Nine benchmark video sequences results at same QP.
✓ **Conclusions**
Conclusions

Encouraging results in the following contexts:

✓ Equally efficient algorithm over whole range of QP values.

✓ Real-time constraints successfully handled for:
  ✓ Heterogeneous networks (exactly the same bitrate),
  ✓ Handheld devices (minimal set of computational requirements),
  ✓ Encrypted bitstream browsing (H.264/AVC compliant bitstream).

✓ The work can be extended for:
  ✓ Protection of ROI,
  ✓ Medical image transmission,
  ✓ Protection of P and B frames in H.264/AVC.