FAST PROTECTION OF H.264/AVC BY SELECTIVE ENCRYPTION OF CABAC FOR I & P FRAMES

Z. SHAHID, M. CHAUMONT, W. PUECH

LIRMM, UMR CNRS 5506, Université de Montpellier II

EUSIPCO 2009
Outline

- Problem Statement
- CABAC
- Proposed Approach
- Results
- Experiments
- Conclusions & Prospects
Problem Statement

- To perform selective encryption (SE) of CABAC for real-time protection of H.264/AVC bitstream.
  - Same bitrate
  - No increase in processing power
  - Browseable bitstream
  - ...

LIRMM, UMR CNRS 5506, Université de Montpellier II
Our approach

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

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

- Encrypted bitstream is completely compliant to H.264/AVC format. (ONLY MB data is encrypted.)
CABAC block diagram

- Binarization
- Context modeling
- Regular BAC
- Bypass BAC
- Context update

Syntax Element → Non-binary syntax element → Binarization → Binary syntax element

Output: Context modeling → Regular BAC → Bypass BAC → H.264/AVC bitstream
Binarization:
It is performed in one of the following ways:

- The unary code (for \( x \), \( x \) no. of 1's)
- The truncated unary code (1 - 14)
- The kth order Exp-Golomb code
- The fixed length code (for header information)

Context modeling

Binary Arithmetic Coding
**CABAC**

- **Binarization:**
  It is performed in one of the following ways:
  - The unary code (for \( x \), \( x \) no. of 1's)
  - The truncated unary code (1 - 14)
  - The kth order Exp-Golomb code
  - The fixed length code (for header information)

- **Context modeling**

- **Binary Arithmetic Coding**
**CABAC**

- **Binarization:**
  It is performed in one of the following ways:
  - The unary code (for $x$, $x$ no. of 1's)
  - The truncated unary code (1 - 14)
  - The kth order Exp-Golomb code
  - The fixed length code (for header information)

- **Context modeling**

- **Binary Arithmetic Coding**
Binarization:
It is performed in one of the following ways:

- The unary code (for \(x\), \(x\) no. of 1's)
- The truncated unary code (1 - 14)
- The kth order Exp-Golomb code
- The fixed length code (for header information)

Context modeling

Binary Arithmetic Coding
CABAC

Binarization:
It is performed in one of the following ways:
- The unary code (for \( x \), \( x \) no. of 1's)
- The truncated unary code (1 - 14)
- The kth order Exp-Golomb code
- The fixed length code (for header information)

Context modeling

Binary Arithmetic Coding
Binarization:
It is performed in one of the following ways:

- The unary code (for \( x \), \( x \) no. of 1's)
- The truncated unary code (1 - 14)
- The kth order Exp-Golomb code
- The fixed length code (for header information)

Context modeling

Binary Arithmetic Coding
**Figure:** Encryption process for NZs in CABAC of H.264/AVC.
Foreman sequence encryption at different QP values

(a) QP = 12  (b) QP = 18  (c) QP = 24
(d) QP = 30  (e) QP = 36  (f) QP = 42
**Foreman** sequence over whole range of QP values.

Comparison of PSNR without encryption and with SE for *foreman* sequence at different QP values.

<table>
<thead>
<tr>
<th>QP</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>12</td>
<td>50.05</td>
<td>8.92</td>
<td>49.99</td>
<td>24.08</td>
<td>50.78</td>
<td>23.84</td>
</tr>
<tr>
<td>18</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>24</td>
<td>39.40</td>
<td>8.38</td>
<td>41.70</td>
<td>24.87</td>
<td>43.86</td>
<td>22.70</td>
</tr>
<tr>
<td>30</td>
<td>34.93</td>
<td>8.92</td>
<td>39.38</td>
<td>24.60</td>
<td>40.99</td>
<td>22.71</td>
</tr>
<tr>
<td>36</td>
<td>30.80</td>
<td>8.89</td>
<td>37.33</td>
<td>24.65</td>
<td>38.10</td>
<td>22.90</td>
</tr>
<tr>
<td>42</td>
<td>27.03</td>
<td>8.93</td>
<td>35.87</td>
<td>24.24</td>
<td>36.41</td>
<td>23.94</td>
</tr>
</tbody>
</table>
Analysis of nine benchmark video sequences.

Comparison of PSNR without encryption and with SE of benchmark video sequences at QP 18.

<table>
<thead>
<tr>
<th>Seq.</th>
<th>PSNR (Y) (dB)</th>
<th>PSNR (U) (dB)</th>
<th>PSNR (V) (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Orig.</td>
<td>SE</td>
<td>Orig.</td>
</tr>
<tr>
<td>bus</td>
<td>44.26</td>
<td>7.73</td>
<td>45.22</td>
</tr>
<tr>
<td>city</td>
<td>44.28</td>
<td>11.52</td>
<td>45.83</td>
</tr>
<tr>
<td>crew</td>
<td>44.81</td>
<td>9.39</td>
<td>45.81</td>
</tr>
<tr>
<td>football</td>
<td>44.59</td>
<td>11.46</td>
<td>45.70</td>
</tr>
<tr>
<td>foreman</td>
<td>44.43</td>
<td>8.42</td>
<td>45.62</td>
</tr>
<tr>
<td>harbour</td>
<td>44.10</td>
<td>9.48</td>
<td>45.60</td>
</tr>
<tr>
<td>ice</td>
<td>46.56</td>
<td>10.37</td>
<td>48.70</td>
</tr>
<tr>
<td>mobile</td>
<td>44.45</td>
<td>8.42</td>
<td>44.14</td>
</tr>
<tr>
<td>soccer</td>
<td>44.26</td>
<td>10.84</td>
<td>46.59</td>
</tr>
</tbody>
</table>

Analysis at different QP values

*intra* frames

*intra* and *inter* frames.
**Foreman** sequence over whole range of QP values.

Comparison of PSNR without encryption and with SE for *foreman* sequence at different QP values.

<table>
<thead>
<tr>
<th>QP</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>12</td>
<td>49.54</td>
<td>8.41</td>
<td>49.89</td>
<td>23.34</td>
<td>50.63</td>
<td>22.16</td>
</tr>
<tr>
<td>18</td>
<td>43.91</td>
<td>9.23</td>
<td>45.50</td>
<td>26.06</td>
<td>47.55</td>
<td>21.11</td>
</tr>
<tr>
<td>24</td>
<td>38.90</td>
<td>8.61</td>
<td>42.04</td>
<td>24.62</td>
<td>44.29</td>
<td>21.83</td>
</tr>
<tr>
<td>30</td>
<td>34.59</td>
<td>9.19</td>
<td>39.84</td>
<td>24.02</td>
<td>41.56</td>
<td>25.18</td>
</tr>
<tr>
<td>36</td>
<td>30.76</td>
<td>8.78</td>
<td>37.96</td>
<td>25.12</td>
<td>38.86</td>
<td>23.50</td>
</tr>
<tr>
<td>42</td>
<td>26.61</td>
<td>8.31</td>
<td>36.34</td>
<td>25.30</td>
<td>36.92</td>
<td>27.06</td>
</tr>
</tbody>
</table>
Nine benchmark video sequences results at same QP value.

Comparison of PSNR without encryption and with SE of benchmark video sequences at QP 18.

<table>
<thead>
<tr>
<th>Seq.</th>
<th>PSNR (Y) (dB)</th>
<th>PSNR (U) (dB)</th>
<th>PSNR (V) (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Orig. SE</td>
<td>Orig. SE</td>
<td>Orig. SE</td>
</tr>
<tr>
<td>bus</td>
<td>43.72 7.44</td>
<td>45.10 25.06</td>
<td>46.44 28.03</td>
</tr>
<tr>
<td>city</td>
<td>43.80 10.84</td>
<td>45.73 30.07</td>
<td>46.78 32.24</td>
</tr>
<tr>
<td>crew</td>
<td>44.45 8.83</td>
<td>45.81 23.00</td>
<td>45.71 20.34</td>
</tr>
<tr>
<td>football</td>
<td>44.15 11.52</td>
<td>45.71 12.65</td>
<td>46.05 23.50</td>
</tr>
<tr>
<td>foreman</td>
<td>43.91 9.23</td>
<td>45.50 26.06</td>
<td>47.55 21.11</td>
</tr>
<tr>
<td>harbour</td>
<td>43.70 9.71</td>
<td>45.44 26.05</td>
<td>46.57 32.52</td>
</tr>
<tr>
<td>ice</td>
<td>46.13 9.85</td>
<td>48.63 24.37</td>
<td>49.14 21.27</td>
</tr>
<tr>
<td>mobile</td>
<td>43.84 8.94</td>
<td>44.15 12.74</td>
<td>44.06 11.52</td>
</tr>
<tr>
<td>soccer</td>
<td>43.53 10.76</td>
<td>46.45 20.12</td>
<td>47.75 23.84</td>
</tr>
</tbody>
</table>
CABAC Encryption - Example

- Foreman QP = 18
- City QP = 18
- Football QP = 18

Analysis at different QP values *intra* frames
*intra* and *inter* frames.
Conclusions & Prospects

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).
- Protection of ROI.
- Medical image transmission.