Selective Encryption of AVS for I & P frames

Zafar SHAHID

LIRMM Labs, France
ICME 2010

23 July 2010

Outline

- Introduction
- Proposed Scheme
- Results
- Security Analysis
- Comparative Analysis
- Conclusions & Prospects

There is a need for selective encryption?

Full encryption (FE) Maximum Security

- Video is a huge data, FE will at least double the required processing
- FE before Video Codec - Bitrate will increase.
- FE after Video Codec - No more format compliant.

C2DVLC

- Real-time constraints:
  - Same bitrate
  - Minimal increase in processing power
  - Browseable bitstream

C2DVLC

- Real-time constraints:
  - Same bitrate
  - Minimal increase in processing power
  - Browseable bitstream

- Our Approach:
  - SE is performed in entropy coding module of AVS Video Codec.
  - Same bitrate is achieved through scrambling of only equal length codewords/binstrings.
  - Encrypted bitstream is completely compliant to respective video codec format.
  - AES Cipher has been used in CFB mode for SE of codewords.

C2DVLC

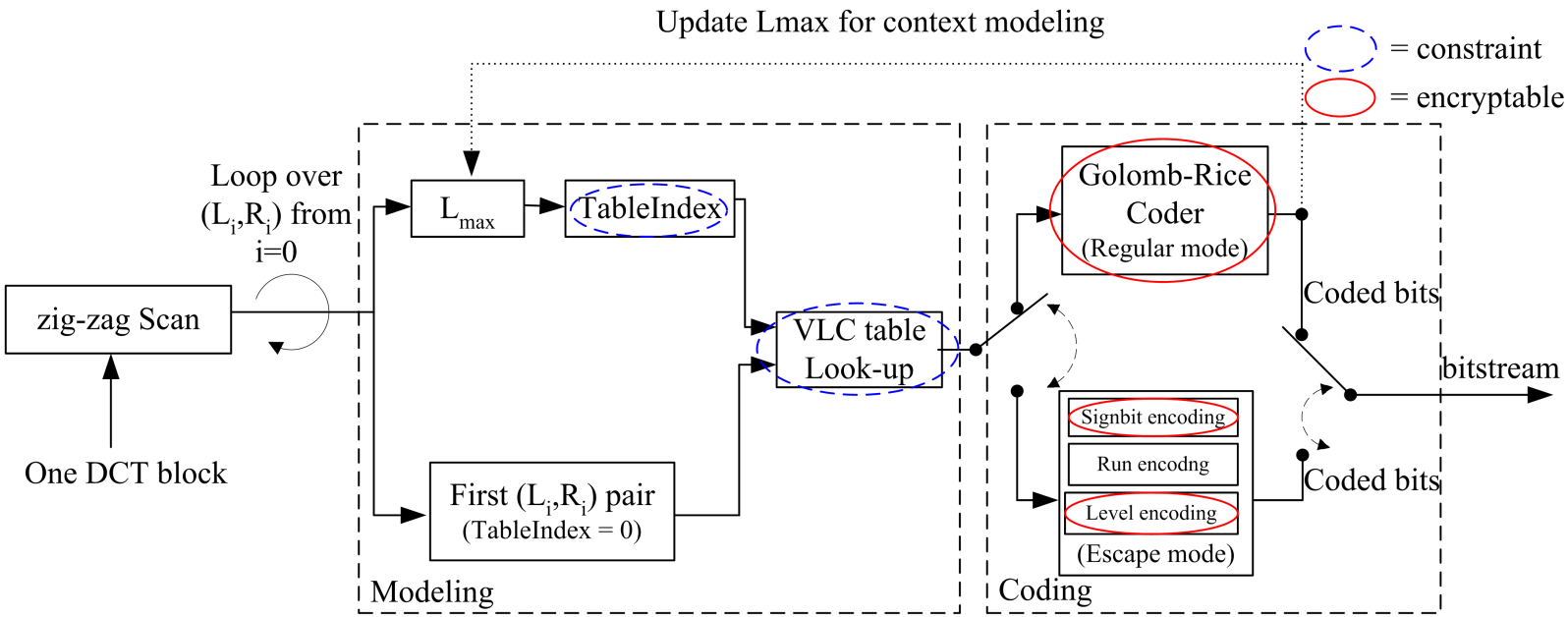


Figure: Block diagram of C2DVLC

C2DVLC regular and escape mode

- Regular mode:
  - (L_i, R_i pair mapped to *Codenumber*).
  - *Codenumber* is coded using Exp-Golomb code.
- Escape mode:
  - L_i is coded separately using Exp-Golomb code.
  - R_i & $Sign(L_i)$ is coded separately using Exp-Golomb code.

C2DVLC limitations

- In (L_i, R_i) pair, only L_i can be encrypted.
- L_{max} should be in the same interval:

$$TableIndex = \quad j, \quad \text{if } (Th[j+1] \dot{>} L_{max} \geq Th[j]) \quad (1)$$

with the threshold for each table given as:

$$Th[0 \ldots 7] = \begin{cases} (0,\ 1,\ 2,\ 3,\ 5,\ 8,\ 11,\ \infty) & \textit{intra\_luma} \\ (0,\ 1,\ 2,\ 3,\ 4,\ 7,\ 10,\ \infty) & \textit{inter\_luma} \\ (0,\ 1,\ 2,\ 3,\ 5,\ \infty,\ \infty,\ \infty) & \textit{chroma} \end{cases} \quad (2)$$

- Length of encrypted codeword must be equal to original one.

Encryption of C2DVLC

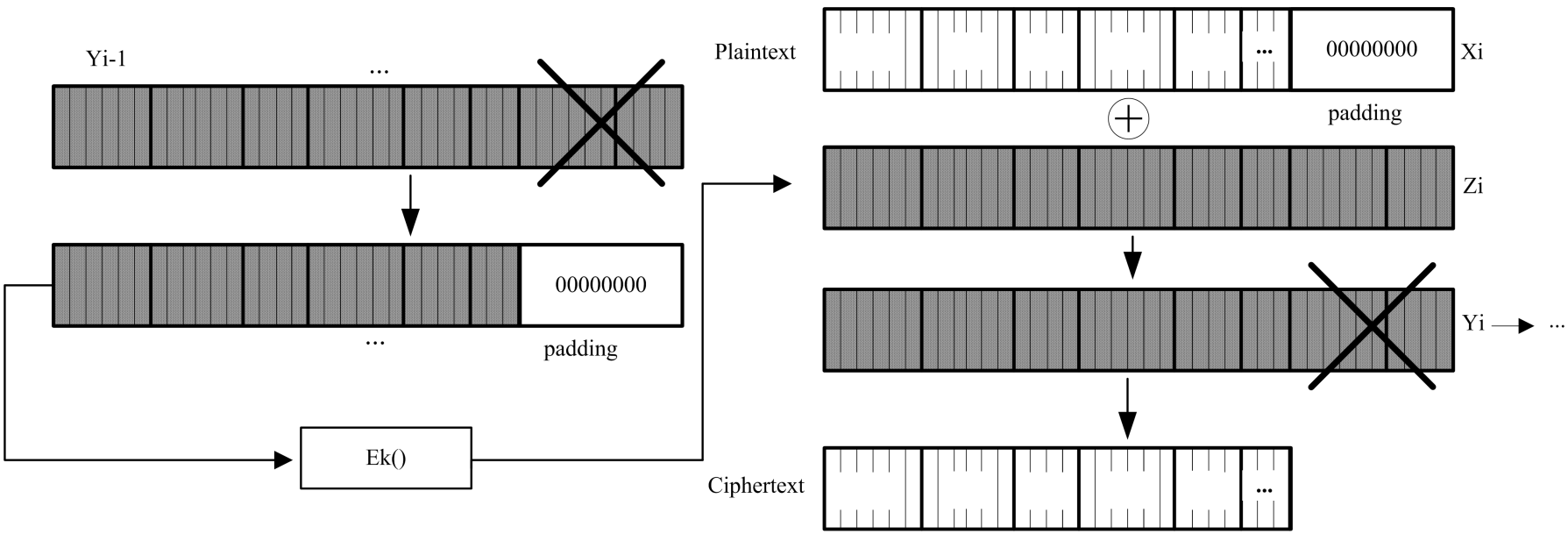


Figure: Encryption of C2DVLC stream with AES cipher in CFB mode.

Encryption constraints - Example

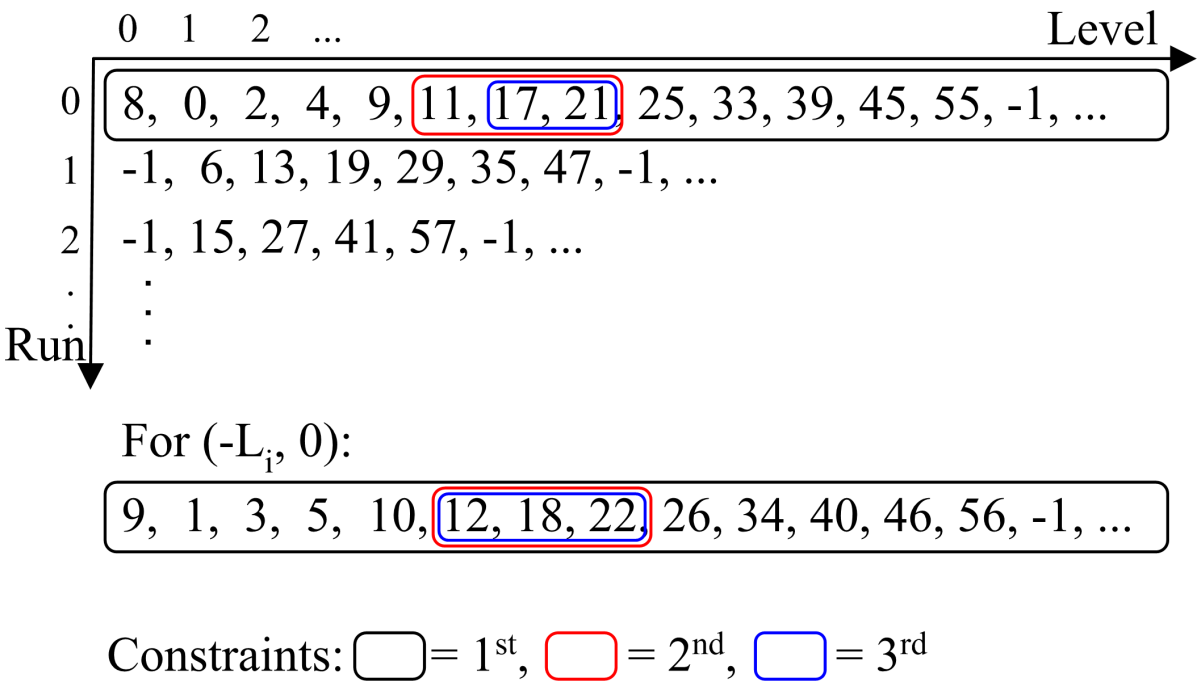


Figure: Encryption of $(L_i, R_i) = (6, 0)$ pair in *regular mode* of C2DVLC for *TableIndex* $= 3$.

SE of C2DVLC Encryption (I + P).

foreman sequence at different QP values with intra period=10.

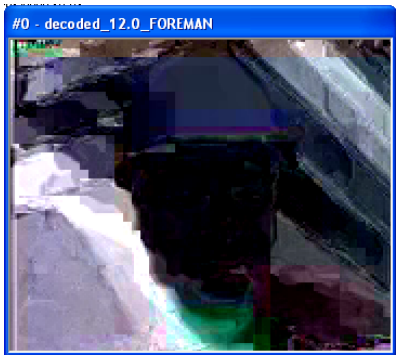
QP	PSNR (Y) (dB) Orig.	SE	PSNR (U) (dB) Orig.	SE	PSNR (V) (dB) Orig.	SE
12	47.19	9.32	50.01	25.05	50.46	23.53
20	42.74	8.94	46.01	26.36	47.66	20.62
28	37.92	8.55	42.36	24.94	44.15	26.05
36	34.01	8.11	39.53	23.92	40.53	21.62
44	30.42	9.56	37.27	25.36	37.69	20.13
52	26.97	10.71	35.65	24.39	36.00	19.85

PSNR Analysis (I + P)

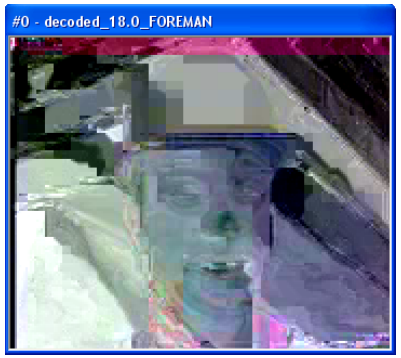
Benchmark video sequences at QP 28 with intra period=10.

Seq.	PSNR (Y) (dB) Orig.	SE	PSNR (U) (dB) Orig.	SE	PSNR (V) (dB) Orig.	SE
bus	36.49	7.96	41.84	25.22	43.07	27.94
city	36.87	12.06	43.20	31.08	44.44	31.69
crew	38.27	13.42	41.97	25.41	40.93	22.36
football	37.89	11.79	41.50	15.15	42.41	23.34
foreman	37.92	8.55	42.36	24.94	44.15	26.05
harbour	36.20	9.79	42.43	25.01	43.85	31.35
ice	40.20	10.32	44.70	26.39	44.98	18.56
mobile	36.06	8.53	38.78	14.84	38.46	12.33
soccer	37.15	11.48	43.05	20.39	44.47	24.15
avg.	37.45	10.43	42.20	23.16	42.97	24.20

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

SE-C2DVLC (I+P) football sequence at QP=28.

Original

SE-C2DVLC

Comparative Analysis with other SE schemes

Video SE Scheme	Format compliant	Trans-coding robust	Domain	Bitrate change	Codec free	Encryption algorithm
Scrambling for privacy protection [?]	Yes	No	Transform	Yes	Yes	Pseudorandom sign inversion
NAL unit encryption [?]	No	No	Bitstream	No	No	Stream Cipher
MB header encryption [?]	No	No	Transform	No	No	Stream Cipher
Reversible encryption of ROI [?]	Yes	Yes	Pixel	Yes	Yes	Pixel permutations
I frame encryption [?]	No	No	Bitstream	No	No	AES
Multiple Huffman tables [?]	No	No	Bitstream	Yes	No	Huffman Table permutations
Our scheme	Yes	No	Bitstream	No	No	AES (CFB mode)

Conclusions & Prospects

For SE of AVS, encouraging results in the following contexts:

- Equally efficient algorithm over whole range of QP values.
- Real-time constraints successfully handled for:
  - Ideal for Heterogeneous networks (exactly the same bitrate).
  - Handheld devices (minimal set of computational requirements).
  - Encrypted bitstream browsing like FF, FB, (AVS compliant bitstream).

Conclusions & Prospects

For SE of AVS, encouraging results in the following contexts:

- Equally efficient algorithm over whole range of QP values.
- Real-time constraints successfully handled for:
  - Ideal for Heterogeneous networks (exactly the same bitrate).
  - Handheld devices (minimal set of computational requirements).
  - Encrypted bitstream browsing like FF, FB, (AVS compliant bitstream).

References