Real-Time Selective Encryption of AVS for I & P Frames

Zafar SHAHID (PhD student)

Supervised by:
William Puech, Marc Chaumont

LIRMM Labs, France

EUSIPCO 2010

27 August 2010

Outline

- Introduction
- Selective encryption
- Real-time SE approaches
- 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

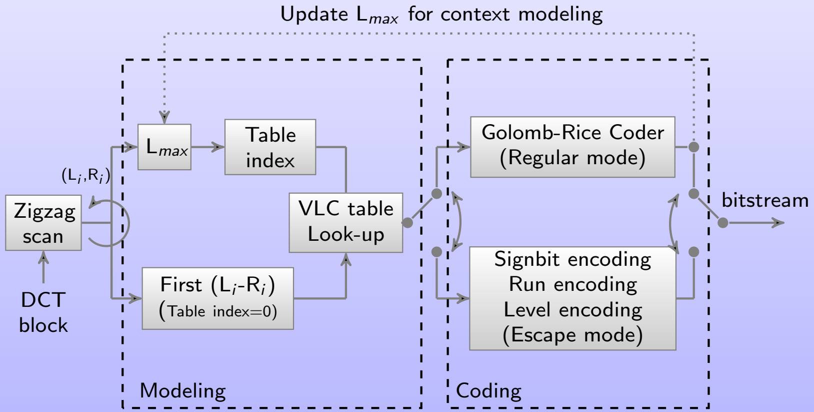
Our Approach:

- SE is performed in C2DVLC of AVS Video Codec.
- Same bitrate is achieved through scrambling of only equal length codewords.
- Encrypted bitstream is completely format compliant.
- AES Cipher has been used in CFB mode for SE of codewords.

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


Update L_{max} for context modeling
L_{max}
Table index
VLC table Look-up
First (L_i-R_i) (Table index=0)
(L_i,R_i)
Zigzag scan
DCT block
Modeling
Golomb-Rice Coder (Regular mode)
Signbit encoding
Run encoding
Level encoding
(Escape mode)
bitstream
Coding

Constraints for SE-C2DVLC

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

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

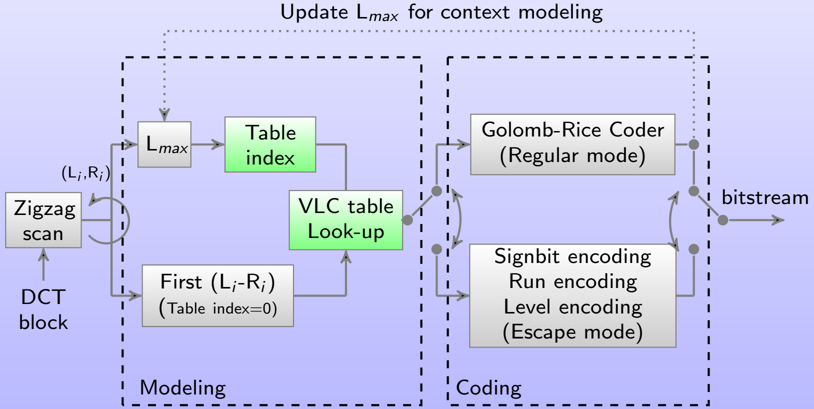
with the threshold for each table given as:

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

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

Constraints for SE-C2DVLC

🟩 =constraint



Update L_{max} for context modeling

L_{max}

Table index

VLC table Look-up

First (L_i-R_i)
(Table index=0)

(L_i,R_i)

Zigzag scan

DCT block

Golomb-Rice Coder
(Regular mode)

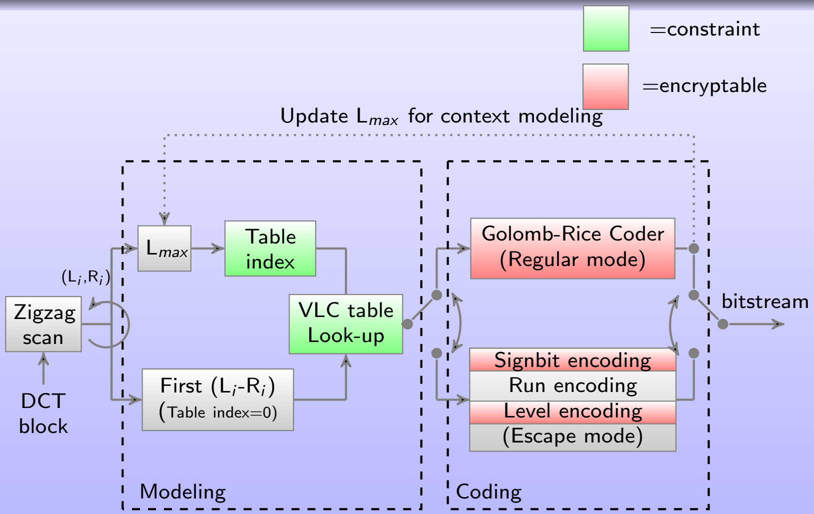
Signbit encoding
Run encoding
Level encoding
(Escape mode)

bitstream

Modeling

Coding

SE-C2DVLC



🟩 =constraint

🟥 =encryptable

Update L_{max} for context modeling

DCT block

Zigzag scan

(L_i,R_i)

L_{max}

Table index

First (L_i-R_i) (Table index=0)

VLC table Look-up

Modeling

Golomb-Rice Coder (Regular mode)

Signbit encoding

Run encoding

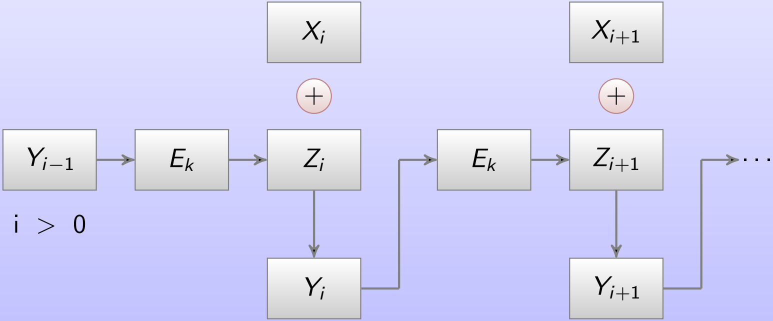
Level encoding

(Escape mode)

Coding

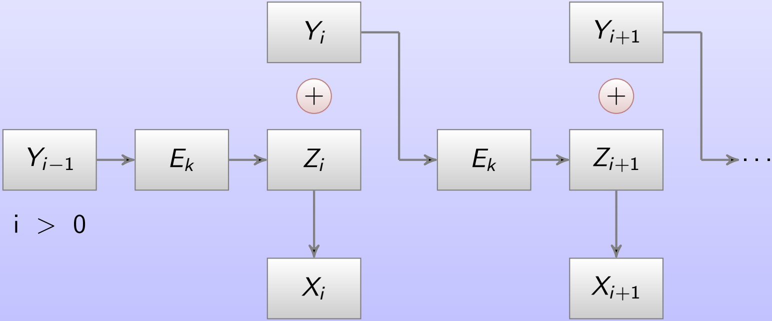
bitstream

AES encryption



i > 0

AES decryption



i > 0

Selective encryption of pair $(L_i, R_i) = (6, 0)$ with Table[3]

Level

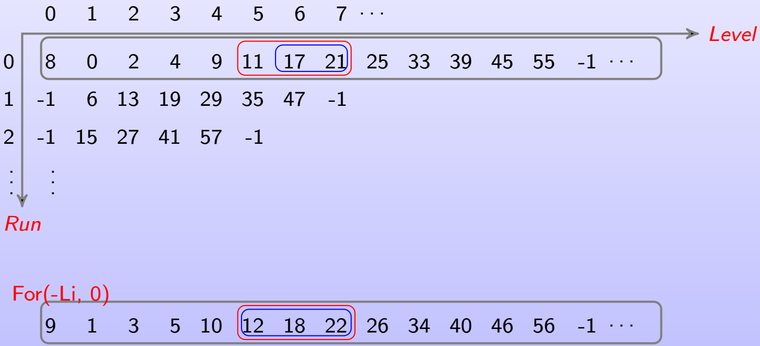
	0	1	2	3	4	5	6	7	···						
0	8	0	2	4	9	11	17	21	25	33	39	45	55	-1	···
1	-1	6	13	19	29	35	47	-1							
2	-1	15	27	41	57	-1									
⋮	⋮														

Run

For(-Li, 0)

9 1 3 5 10 12 18 22 26 34 40 46 56 -1 ···

Selective encryption of pair $(L_i, R_i) = (6, 0)$ with table[3]



	0	1	2	3	4	5	6	7 ⋯							
0	8	0	2	4	9	11	17	21	25	33	39	45	55	-1	⋯
1	-1	6	13	19	29	35	47	-1							
2	-1	15	27	41	57	-1									
⋮	⋮														

For(-Li, 0)

9	1	3	5	10	12	18	22	26	34	40	46	56	-1	⋯

Constraints: ▢ $=1^{st}$, 🟥 $=2^{nd}$, 🟦 $=3^{rd}$,

Constraints for real-time SE-C2DVLC

Code space not contiguous:

e.g., for $L_i = \{5, 6, 7, 8\}$, codeNumbers $= \{11, 17, 21, 25\}$.
Solution: Replace levelsindices and encrypt indices:

$$Y_i = Encrypt(X_i) = T^{-1}[\mathcal{E}(T(X_i))], \tag{3}$$

$$X_i = Decrypt(Y_i) = T^{-1}[\mathcal{D}(T(Y_i))], \tag{4}$$

where $\mathcal{E}(.)/\mathcal{D}(.)$ = AES encryption/decryption functions,
$T(.)$ = a bijective mapping between levels with same code-length and indices.

Constraints for real-time SE-C2DVLC

Code space not contiguous:

e.g., for $L_i = \{5, 6, 7, 8\}$, codeNumbers $= \{11, 17, 21, 25\}$.
Solution: Replace levelsindices and encrypt indices:

$$Y_i = Encrypt(X_i) = T^{-1}[\mathcal{E}(T(X_i))], \tag{3}$$

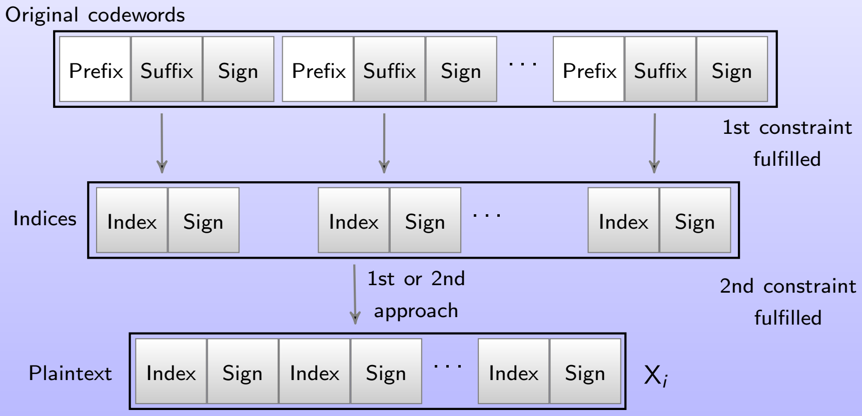
$$X_i = Decrypt(Y_i) = T^{-1}[\mathcal{D}(T(Y_i))], \tag{4}$$

where $\mathcal{E}(.)/\mathcal{D}(.)$ = AES encryption/decryption functions,
$T(.)$ = a bijective mapping between levels with same code-length and indices.

Encryption space not always full:

- For example, ES may be 14, 19, 31.
- Two solutions are proposed here: RSE-I & RSE-II.

Plaintext for real-time SE-C2DVLC



1st Real-time SE-C2DVLC approach (RSE-I)

- Utilizes all available encryption space.
- An increased required processing power.
- A plaintext is prepared with all the indices (non-full).

1st Real-time SE-C2DVLC approach (RSE-I)

- Utilizes all available encryption space.
- An increased required processing power.
- A plaintext is prepared with all the indices (non-full).
- After encryption with AES cipher in CFB mode, valid encrypted indices substitutes the original indices in the bitstream.
- Encrypted indices which are not valid are encrypted again, till they lie in the valid range.
- On decoder side, same number of iterations are required to decrypt the original index and it will be the first valid index.

2nd Real-time SE-C2DVLC approach (RSE-II)

Less required processing, while utilizing less ES

0	1	2	3	4	5	6	7	8	9	10	11	12	13

ES=14

2nd Real-time SE-C2DVLC approach (RSE-II)

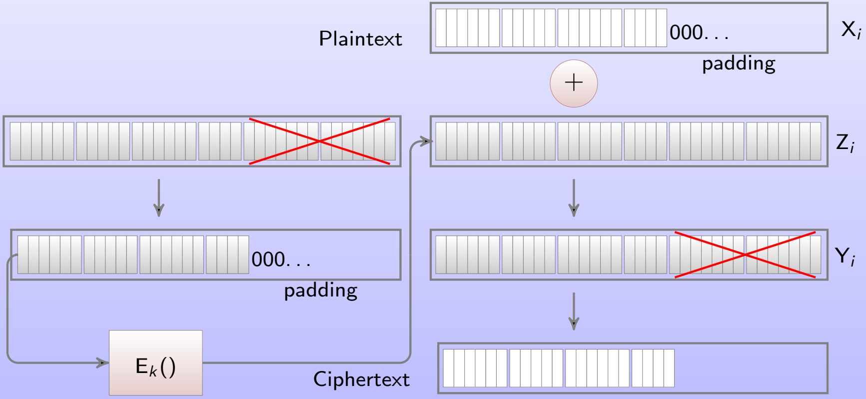
Less required processing, while utilizing less ES

0	1	2	3	4	5	6	7	8	9	10	11	12	13

ES=14 Full code spaces ☐ $=1^{st}$, 🟥 $=2^{nd}$, 🟦 $=3^{rd}$,

Index	**Encryption space** (ES)	**Encrypted ES**
5	1^{st} code-space (0,1,...,7)	1^{st}(0,1,...,7)
9	2^{nd} code-space (8,9,..,11)	2^{nd}(8,9,..,11)
13	3^{rd} code-space (12,13)	3^{rd}(12,13)

SE-C2DVLC



PSNR for RSE-I and RSE-II at QP=28 (I frames)

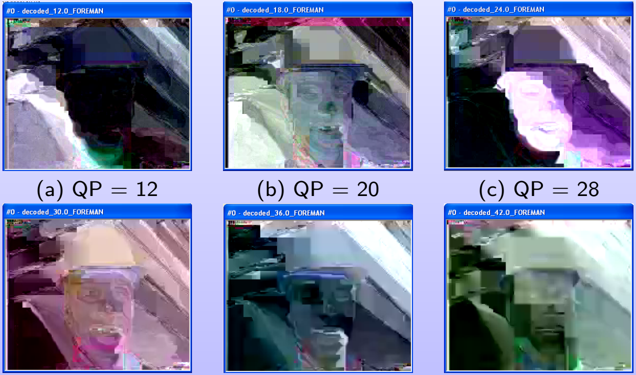
Seq.	**PSNR (Y) (dB)**			**PSNR (U) (dB)**			**PSNR (V) (dB)**		
	Orig.	**RSE-I**	**RSE-II**	**Orig.**	**RSE-I**	**RSE-II**	**Orig.**	**RSE-I**	**RSE-II**
bus	37.9	7.8	8.5	41.6	26.0	26.4	42.8	27.9	27.9
city	38.1	12.3	12.6	42.9	30.7	30.7	44.2	31.1	31.0
crew	39.5	10.2	10.3	41.8	25.0	25.2	40.8	22.2	22.4
football	39.1	11.9	12.0	41.5	16.3	16.1	42.3	24.1	23.8
foreman	38.9	9.1	8.8	42.1	23.8	24.1	43.9	26.2	26.9
harbour	37.8	9.8	9.9	42.2	24.4	25.1	43.6	32.5	31.8
ice	41.4	10.7	10.8	44.5	26.2	25.8	44.8	20.3	19.1
mobile	37.9	8.7	8.8	38.6	14.5	14.5	38.4	11.8	12.1
soccer	38.3	11.4	11.3	42.9	22.1	20.8	44.3	24.1	24.4
avg.	38.8	10.2	10.3	42.0	23.2	23.2	42.8	24.5	24.4

PSNR for RSE-I and RSE-II at diff QPs (I frames)

Foreman sequence at diff QPs.

QP	**PSNR (Y) (dB)**			**PSNR (U) (dB)**			**PSNR (V) (dB)**		
	Orig.	**RSE-I**	**RSE-II**	**Orig.**	**RSE-I**	**RSE-II**	**Orig.**	**RSE-I**	**RSE-II**
12	49.6	9.0	8.8	50.1	24.8	24.4	50.8	21.5	21.1
20	44.1	8.9	8.7	45.7	26.3	25.9	47.4	22.1	22.8
28	38.9	9.1	8.8	42.1	23.8	24.1	43.9	26.2	26.9
36	34.4	8.9	9.0	39.3	23.8	23.9	40.2	22.0	21.5
44	30.6	9.1	9.7	37.1	23.9	23.9	37.3	21.7	21.3
52	27.0	10.0	9.8	35.3	25.5	25.1	35.9	20.8	20.1

SE-C2DVLC foreman # 0 at different QP values



(a) QP = 12 (b) QP = 20 (c) QP = 28

(d) QP = 36 (e) QP = 44 (f) QP = 52

PSNR for RSE-I and RSE-II at QP=28 (I+P frames)

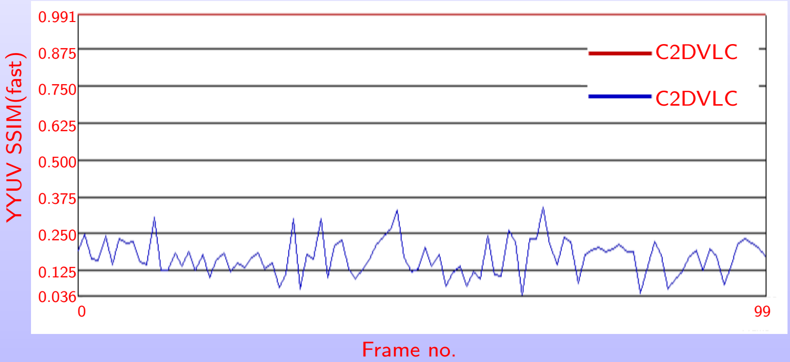
Seq.	**PSNR (Y) (dB)**			**PSNR (U) (dB)**			**PSNR (V) (dB)**		
	Orig.	**RSE-I**	**RSE-II**	**Orig.**	**RSE-I**	**RSE-II**	**Orig.**	**RSE-I**	**RSE-II**
bus	36.5	8.0	7.0	41.8	25.2	26.0	43.1	28.0	27.4
city	36.9	12.1	12.3	43.2	31.1	30.4	44.4	31.7	30.9
crew	38.3	13.4	10.4	42.0	25.4	25.4	40.9	22.4	23.5
football	37.9	11.8	12.8	41.5	15.2	16.9	42.4	23.4	23.8
foreman	37.9	8.6	8.2	42.4	25.0	24.4	44.2	26.1	27.2
harbour	36.2	9.8	9.9	42.4	25.0	28.0	43.9	31.4	33.3
ice	40.2	10.3	10.8	44.7	26.4	26.1	45.0	18.8	19.8
mobile	36.1	8.5	9.1	38.8	14.8	12.8	38.5	12.3	11.8
soccer	37.2	11.5	10.5	43.1	20.4	19.9	44.5	24.2	25.5
avg.	37.5	10.4	10.1	42.2	23.2	23.3	43.0	24.2	24.8

PSNR for RSE-I and RSE-II (I+P frames)

Foreman sequence at diff QPs.

QP	PSNR (Y) (dB)			PSNR (U) (dB)			PSNR (V) (dB)		
	Orig.	**RSE-I**	**RSE-II**	**Orig.**	**RSE-I**	**RSE-II**	**Orig.**	**RSE-I**	**RSE-II**
12	47.2	9.3	8.7	50.0	25.0	24.7	50.5	23.5	21.2
20	42.8	8.9	8.3	46.0	26.4	27.5	47.7	20.6	23.1
28	37.9	8.6	8.2	42.4	24.9	24.4	44.2	26.1	27.2
36	34.0	8.1	8.7	39.5	23.9	24.9	40.5	21.6	22.3
44	30.4	9.8	8.2	37.3	25.4	23.3	37.7	20.1	23.5
52	27.0	10.7	9.1	35.7	24.4	25.0	36.0	19.8	22.2

Framewise SSIM comparison for foreman sequence



Encryption space for RSE-I and RSE-II at QP=28

	ES for (I)		**ES for (I+P)**	
Seq.	**RSE-I** (%)	**RSE-II** (%)	**RSE-I** (%)	**RSE-II** (%)
bus	31.89	28.64	11.93	11.22
city	27.19	25.46	13.38	12.93
crew	20.80	19.80	12.58	12.33
football	26.88	24.47	16.06	14.94
foreman	24.89	22.91	13.61	13.01
harbour	32.10	28.75	12.38	11.72
ice	27.27	24.78	13.07	12.36
mobile	33.20	28.86	11.12	10.28
soccer	24.65	23.02	12.22	11.76
avg.	27.65	25.19	12.93	12.28

Processing requirement for RSE-I & RSE-II (I+P frames)

	Encoder-side		**Decoder-side**	
Seq.	**RSE-I** (%)	**RSE-II** (%)	**RSE-I** (%)	**RSE-II** (%)
bus	1.38	0.80	5.66	4.04
city	1.00	0.62	5.04	3.67
crew	0.62	0.41	3.78	2.66
football	0.82	0.43	5.19	3.91
foreman	0.94	0.57	4.79	3.59
harbour	1.10	0.66	5.48	3.90
ice	0.82	0.46	4.74	3.55
mobile	1.52	1.01	6.50	4.84
soccer	0.88	0.53	4.76	3.44
avg.	1.01	0.61	5.10	3.73

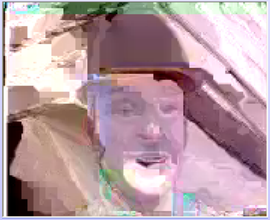
SE-C2DVLC (I+P) football sequence at QP=28.

Original

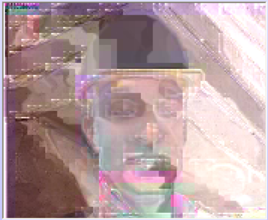
SE-C2DVLC

Removal of encrypted data

Foreman frame # 0:



(a) Original
YUV = {10.01, 26.86, 25.24} dB

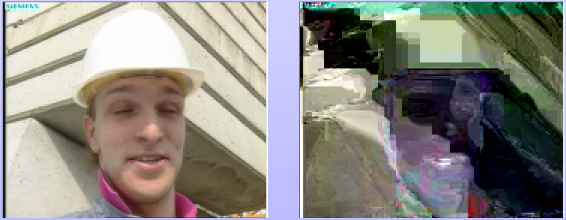


(b) Attacked
YUV = {8.87, 27.3, 26.3} dB

Key sensitivity test

Foreman frame # 0:

Key	PSNR (Y) (dB)	PSNR (U) (dB)	PSNR (V) (dB)
Original key	44.60	45.73	47.35
1-bit different key	8.31	25.13	24.82



(a) Original key (b) 1-bit different key

Comparative analysis with other SE schemes

Video SE Scheme	**Format compliant**	**Transcoding robust**	**Domain**	**Bitrate change**	**Codec free**	**Encryption algorithm**
Scrambling for privacy protection [1]	Yes	No	Transform	Yes	Yes	Pseudorandom sign inversion
NAL unit encryption [2]	No	No	Bitstream	No	No	Stream Cipher
MB header encryption [3]	No	No	Transform	No	No	Stream Cipher
Reversible encryption of ROI [4]	Yes	Yes	Pixel	Yes	Yes	Pixel permutations
I frame encryption [5]	No	No	Bitstream	No	No	AES
Multiple Huffman tables [6]	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

F. Dufaux and T. Ebrahimi,
"Scrambling for privacy protection in video surveillance systems,"
IEEE Transactions on Circuits and Systems for Video Technology, vol. 18, no. 8, pp. 1168 –1174, aug. 2008.

C. Li, X. Zhou, and Y. Zong,
"NAL Level Encryption for Scalable Video Coding,"
Lecture notes in Computer Science, Springer, , no. 5353, pp. 496–505, 2008.

Shiguo Lian, Zhongxuan Liu, Zhen Ren, and Haila Wang,
"Commutative Encryption and Watermarking in Video Compression,"
IEEE Transactions on Circuits and Systems for Video Technology, vol. 17, no. 6, pp. 774–778, June 2007.

P. Carrillo, H. Kalva, and S. Magliveras,
"Compression Independent Reversible Encryption for Privacy in Video Surveillance,"
EURASIP Journal on Information Security, vol. 2009, pp. 13, 2009.

M. Abomhara, O. Zakaria, O. Khalifa, A. Zaiden, and B. Zaiden,
"Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standard,"
International Journal of Computer and Electrical Engineering, vol. 2, no. 2, pp. 223–229, 2010.

C.-P. Wu and C.-C.J. Kuo,
"Design of Integrated Multimedia Compression and Encryption Systems,"
IEEE Transactions on Multimedia, vol. 7, pp. 828–839, 2005.