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

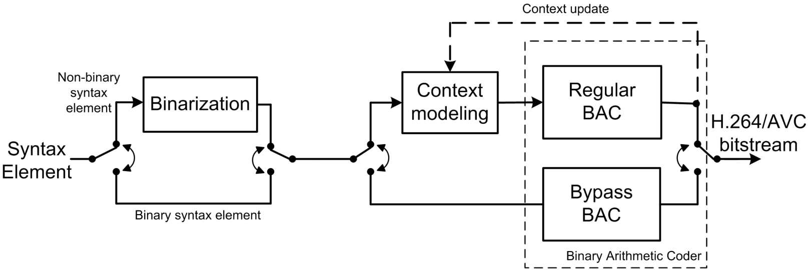
Problem Statement

- 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
  - ...

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



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

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

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

CABAC Encryption

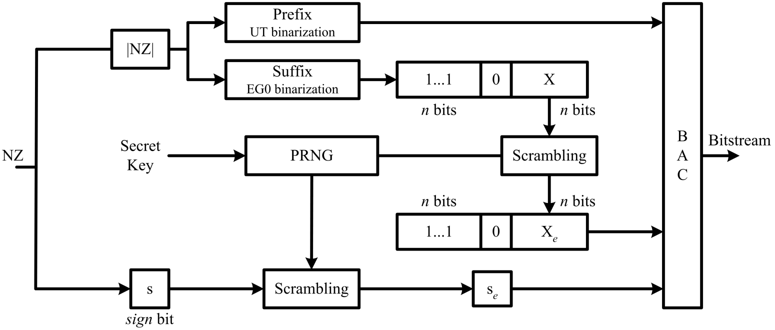
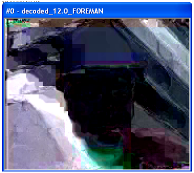
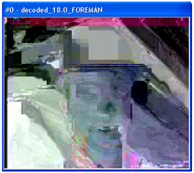


Figure: Encryption process for NZs in CABAC of H.264/AVC.

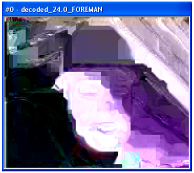
Foreman sequence encryption at different QP values



(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.

QP	PSNR (Y) (dB)		PSNR (U) (dB)		PSNR (V) (dB)	
	Without SE	With SE	Without SE	With SE	Without SE	With SE
12	50.05	8.92	49.99	24.08	50.78	23.84
18	44.43	8.42	45.62	23.87	47.42	22.14
24	39.40	8.38	41.70	24.87	43.86	22.70
30	34.93	8.92	39.38	24.60	40.99	22.71
36	30.80	8.89	37.33	24.65	38.10	22.90
42	27.03	8.93	35.87	24.24	36.41	23.94

Analysis of nine benchmark video sequences.

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

Seq.	PSNR (Y) (dB)		PSNR (U) (dB)		PSNR (V) (dB)	
	Orig.	SE	Orig.	SE	Orig.	SE
bus	44.26	7.73	45.22	25.19	46.50	26.86
city	44.28	11.52	45.83	30.50	46.76	31.86
crew	44.81	9.39	45.81	23.80	45.66	19.90
football	44.59	11.46	45.70	15.79	45.98	23.10
foreman	44.43	8.42	45.62	23.87	47.42	22.14
harbour	44.10	9.48	45.60	23.82	46.63	31.20
ice	46.56	10.37	48.70	25.42	49.19	19.73
mobile	44.45	8.42	44.14	13.47	44.04	11.11
soccer	44.26	10.84	46.59	19.69	47.82	24.83

Foreman sequence over whole range of QP values.

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

QP	PSNR (Y) (dB)		PSNR (U) (dB)		PSNR (V) (dB)	
	Without SE	With SE	Without SE	With SE	Without SE	With SE
12	49.54	8.41	49.89	23.34	50.63	22.16
18	43.91	9.23	45.50	26.06	47.55	21.11
24	38.90	8.61	42.04	24.62	44.29	21.83
30	34.59	9.19	39.84	24.02	41.56	25.18
36	30.76	8.78	37.96	25.12	38.86	23.50
42	26.61	8.31	36.34	25.30	36.92	27.06

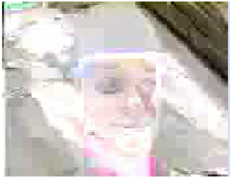
Nine benchmark video sequences results at same QP vlaue.

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

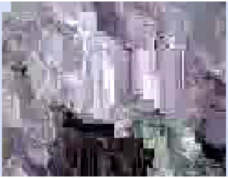
Seq.	PSNR (Y) (dB)		PSNR (U) (dB)		PSNR (V) (dB)	
	Orig.	SE	Orig.	SE	Orig.	SE
bus	43.72	7.44	45.10	25.06	46.44	28.03
city	43.80	10.84	45.73	30.07	46.78	32.24
crew	44.45	8.83	45.81	23.00	45.71	20.34
football	44.15	11.52	45.71	12.65	46.05	23.50
foreman	43.91	9.23	45.50	26.06	47.55	21.11
harbour	43.70	9.71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

CABAC Encryption - Example

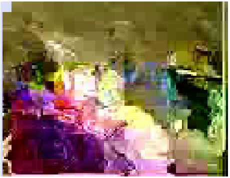
Foreman



Foreman QP = 18



City QP = 18



Football QP = 18

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 birate).
  - Handheld devices (minimal set of computational requirements).
  - Encrypted bitstream browsing (H.264/AVC compliant bitstream).
- Protection of ROI.
- Medical image transmission.