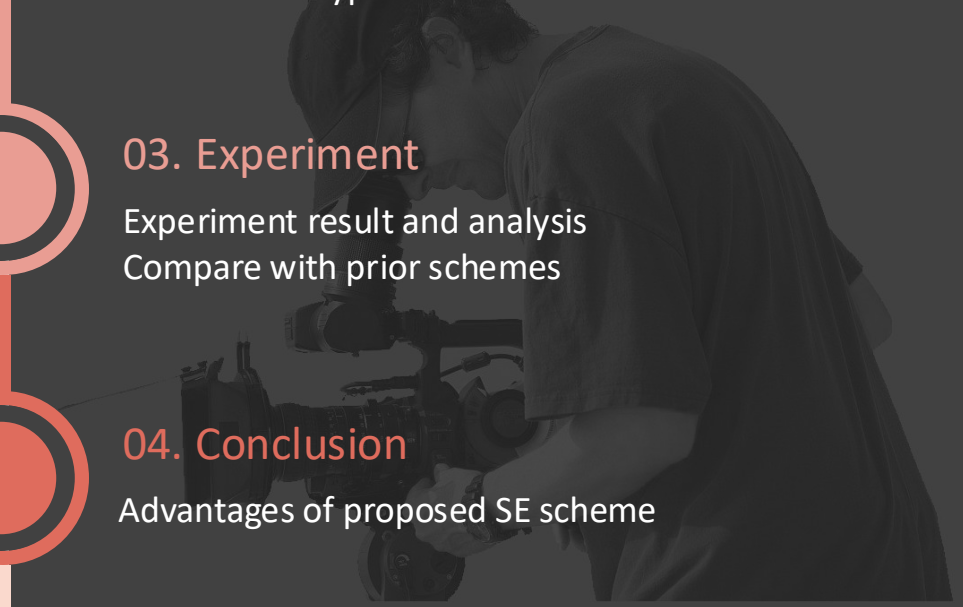
Selective Encryption of H.264/AVC Based on Block Weight Model

Mengdie Huang, Postgraduate
Media Security and Smart Interaction Lab
Communication University of China, Beijing

CONTENT

Consist of four parts

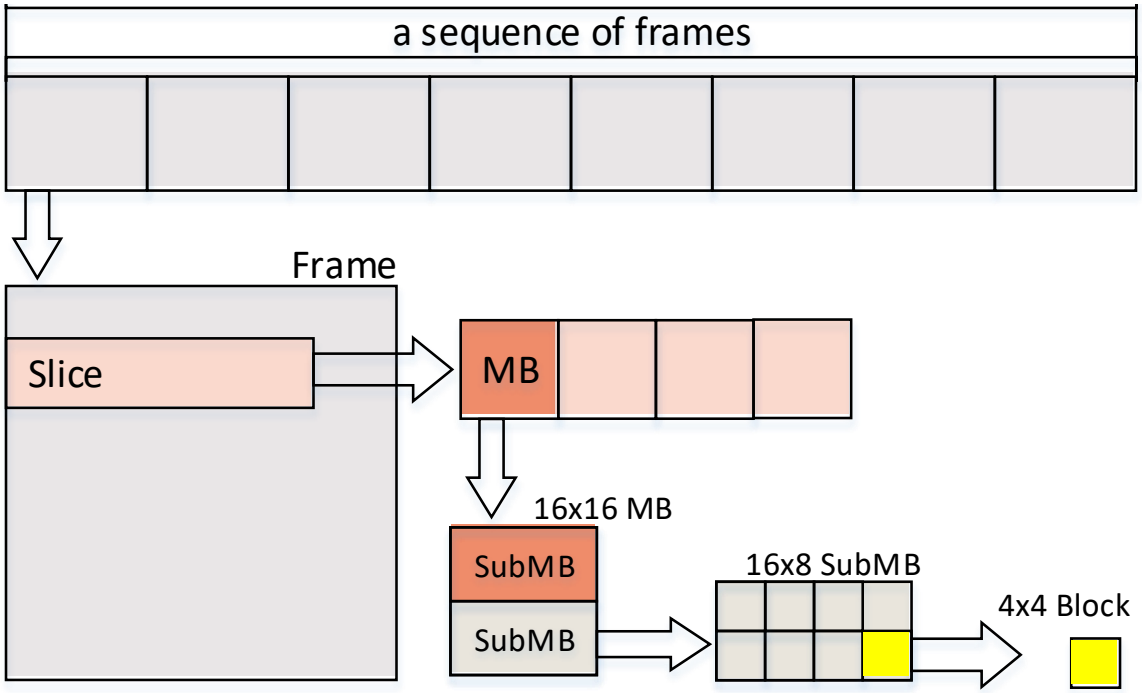


video meeting

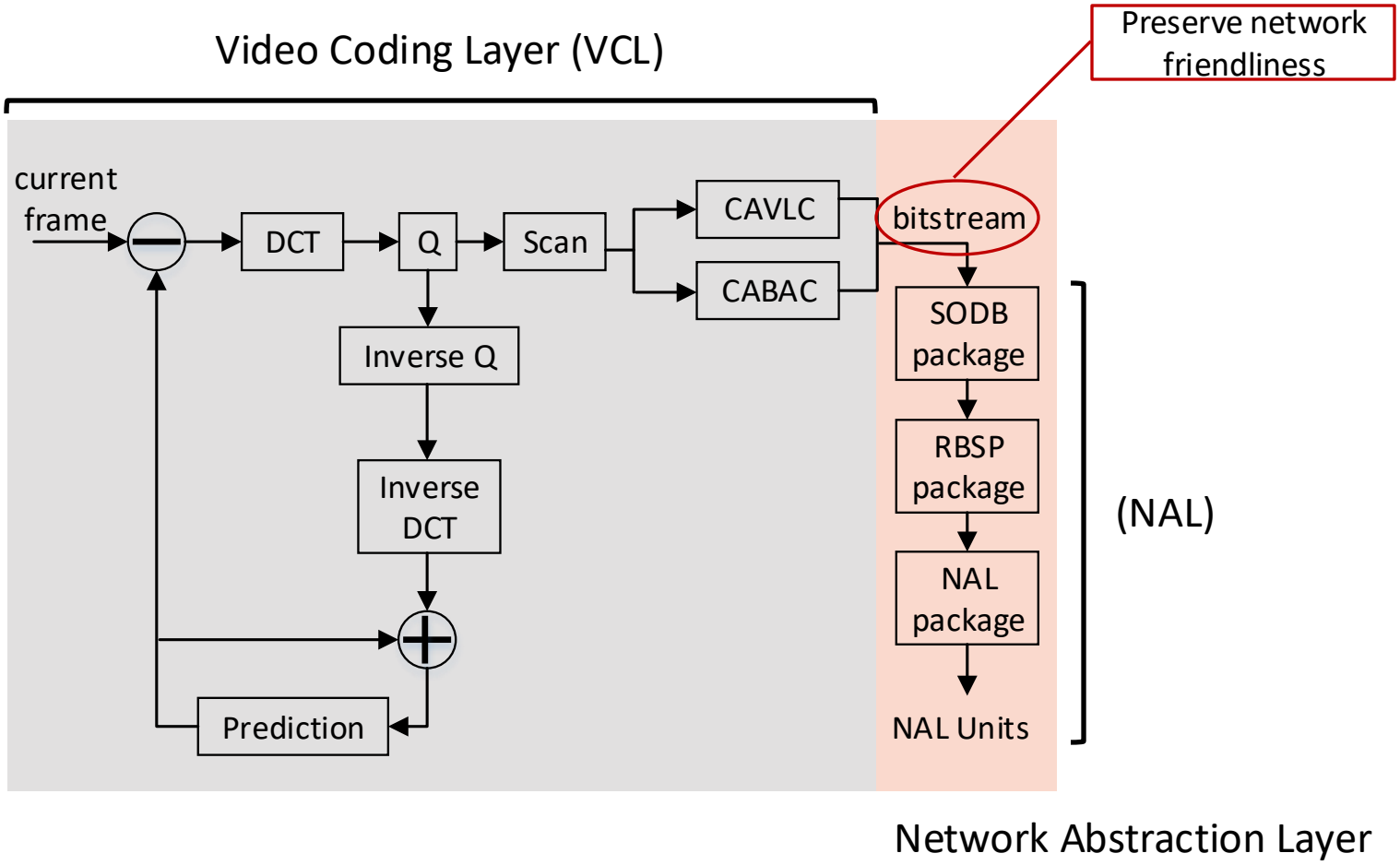
legal viewing of surveillance video

Video Security Problem

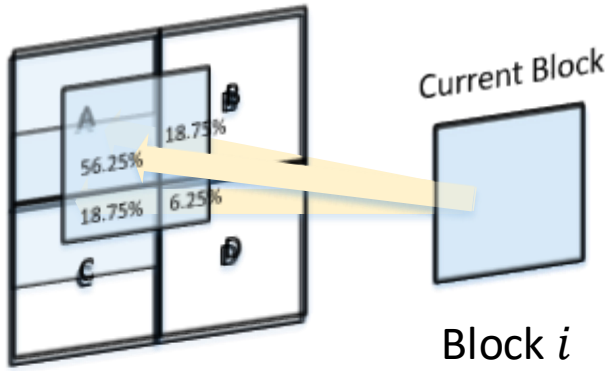
H.264/AVC Bitstream Structure



H.264/AVC Coding Process



Proposed Block Weight (BW) Model



Block i

The proportion of block x referenced by block i is defined as

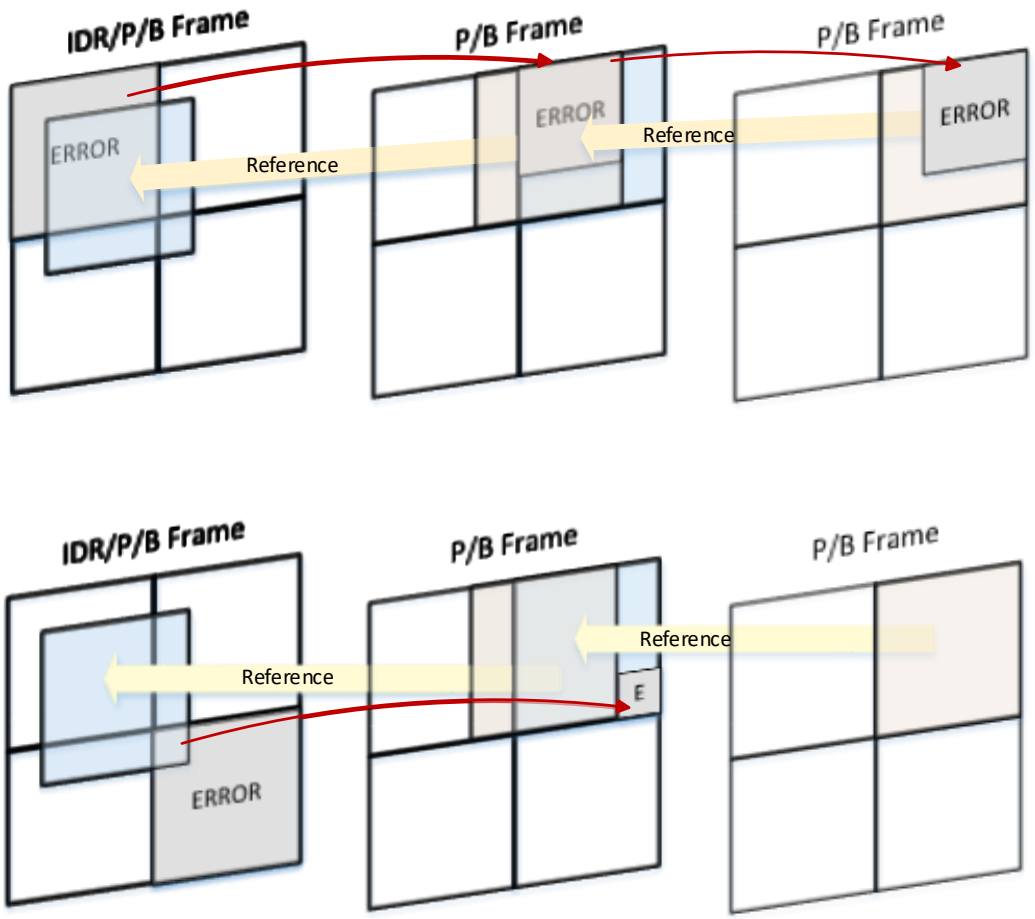
$$P_{(x,i)} = \frac{S_{(x,i)}}{16}$$

e.g. If current block is block i , the proportion is calculated as

$$P_{(A,i)} = \frac{S_{(A,i)}}{16} = \frac{3 \times 3}{16} = 56.25\%$$

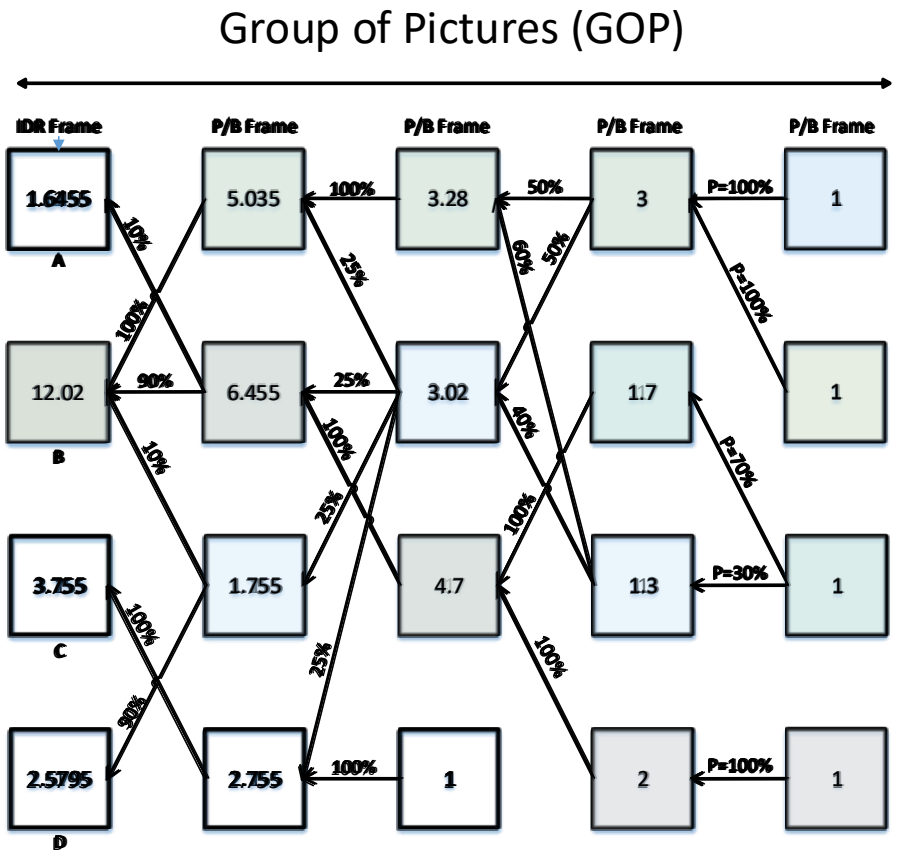
$$P_{(D,i)} = \frac{S_{(D,i)}}{16} = \frac{1 \times 1}{16} = 6.25\%$$

Proposed Block Weight (BW) Model



Proposed Block Weight (BW) Model

4X4 pixels Block



The BW of Block x is defined as

$$W_b(x) = \begin{cases} 1 + \sum_{i=1}^{n} P_{(x,i)} W_b(i), & n \neq 0 \\ 1, & n = 0 \end{cases}$$

Proposed Block Weight (BW) Model

4X4 pixels Block x

$W_b(x,1)$	$W_b(x,2)$	$W_b(x,3)$	$W_b(x,4)$
$W_b(x,5)$	$W_b(x,6)$	$W_b(x,7)$	$W_b(x,8)$
$W_b(x,9)$	$W_b(x,10)$	$W_b(x,11)$	$W_b(x,12)$
$W_b(x,13)$	$W_b(x,14)$	$W_b(x,15)$	$W_b(x,16)$

16X16 pixels MB x

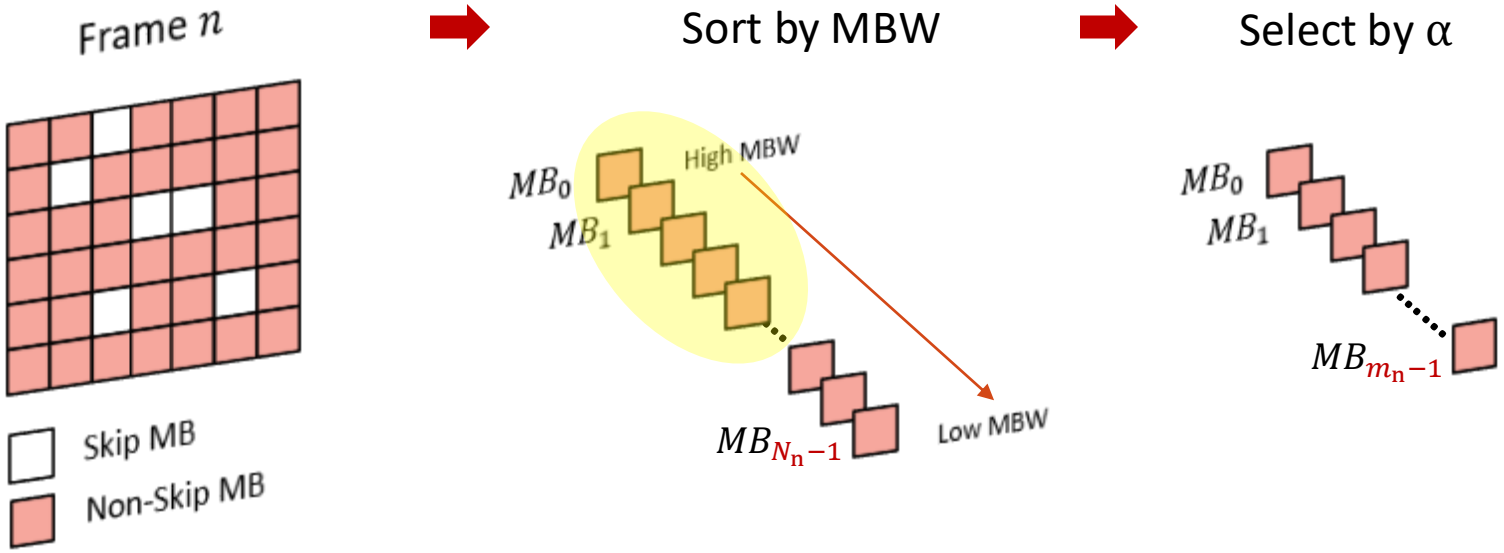
The BW of Block x is defined as

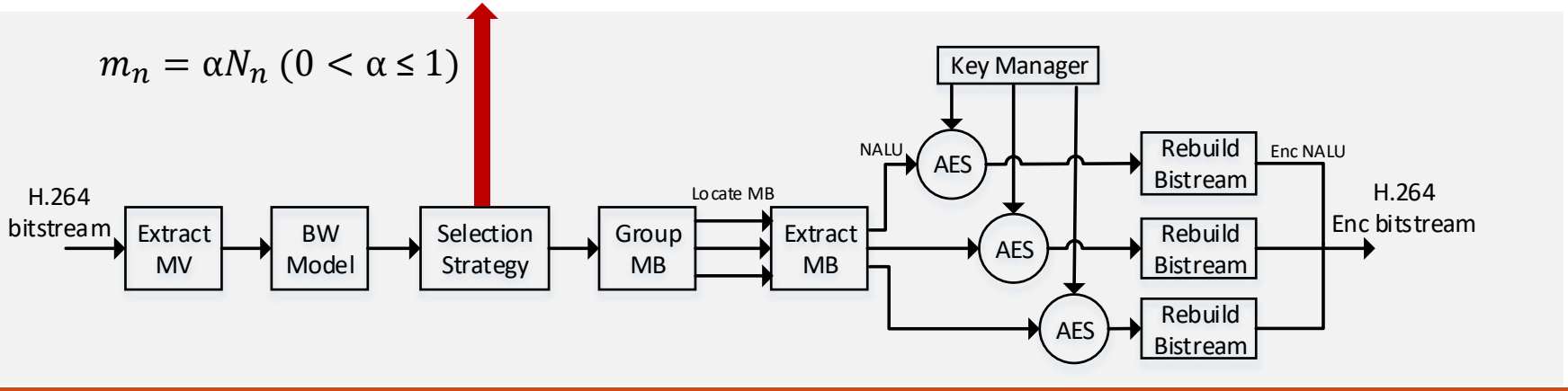
$$W_b(x) = \begin{cases} 1 + \sum_{i=1}^{n} P_{(x,i)} W_b(i), & n \neq 0 \\ 1, & n = 0 \end{cases}$$

The MB Weight (MBW) of MB x is defined as

$$W_{mb}(x) = \frac{\sum_{i=1}^{16} W_b(x,i)}{16}$$

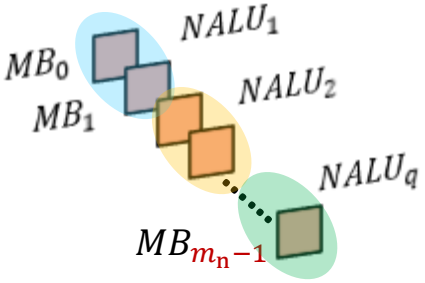
Proposed Selective Encryption (SE) Method



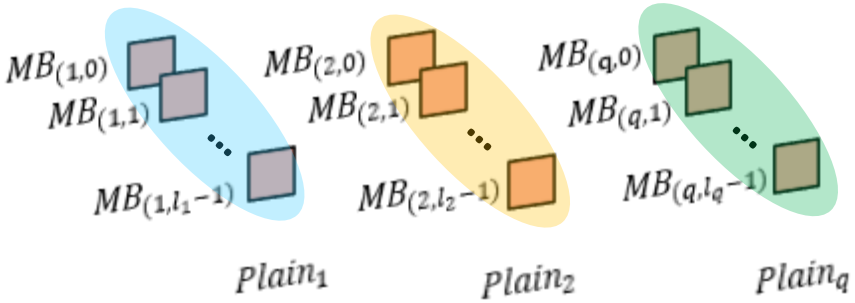


Proposed Selective Encryption (SE) Method

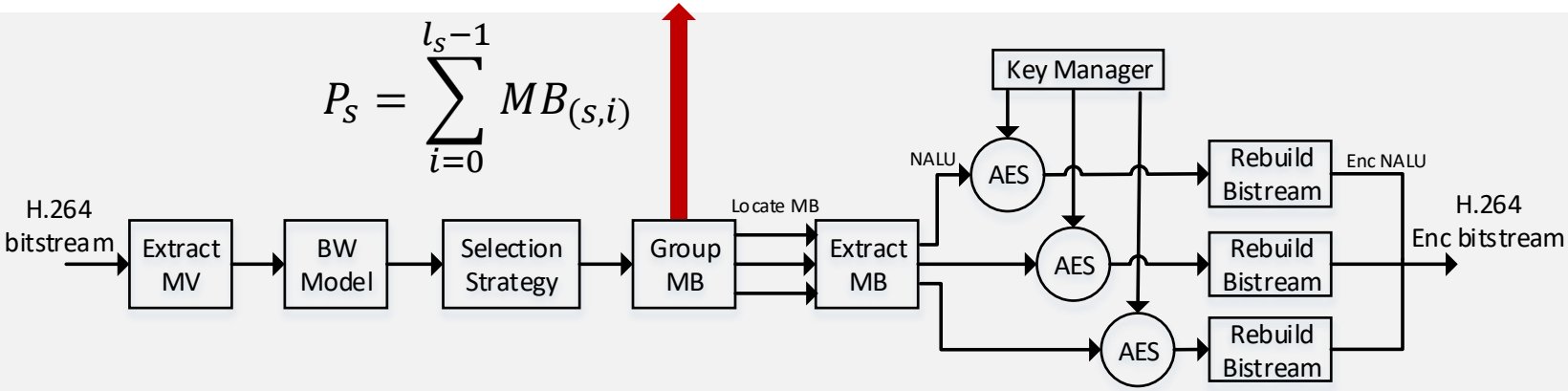
Selected MBs



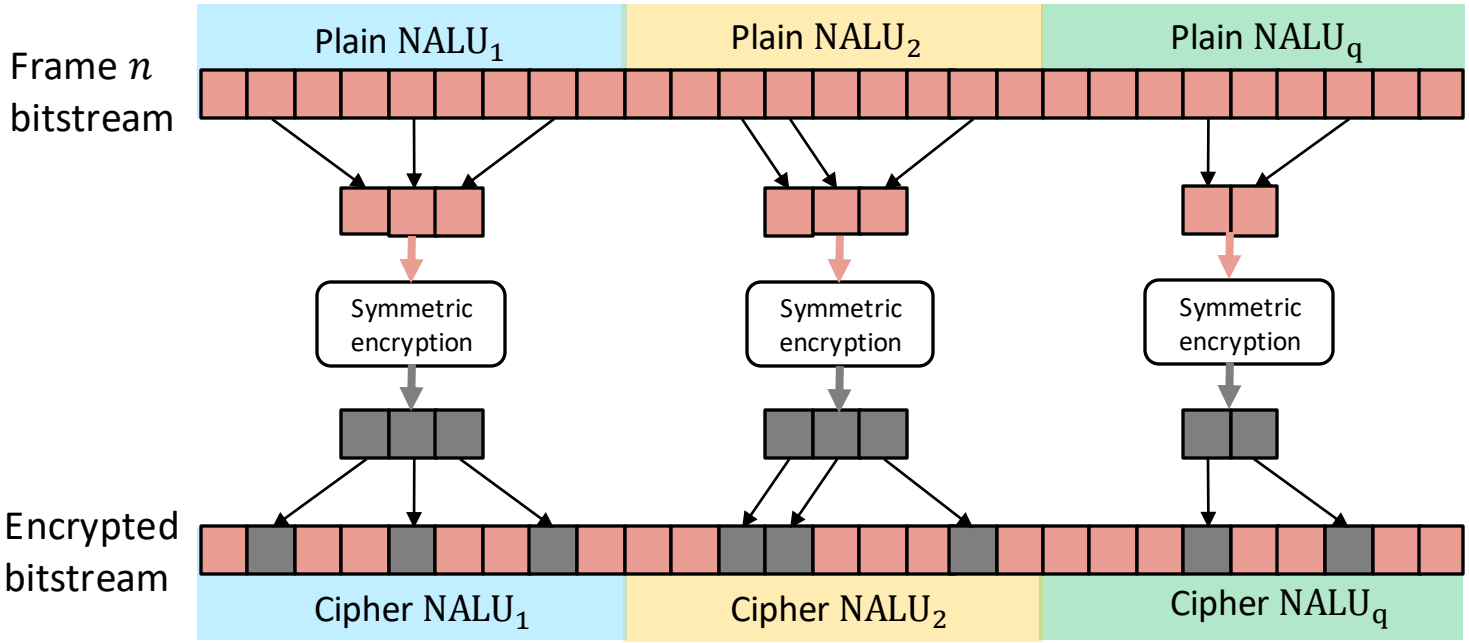
Group by NALU



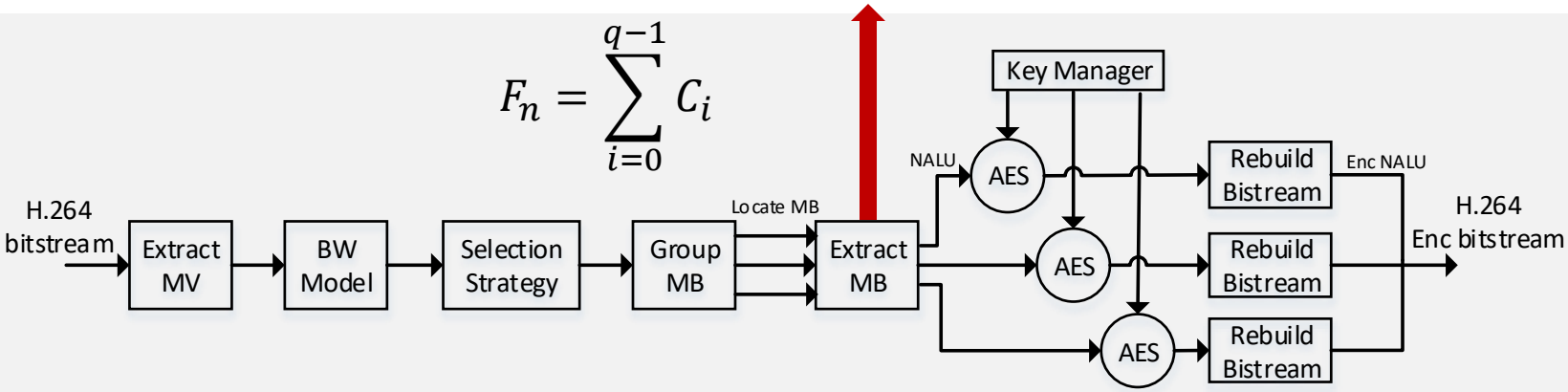
$$P_s = \sum_{i=0}^{l_s-1} MB_{(s,i)}$$



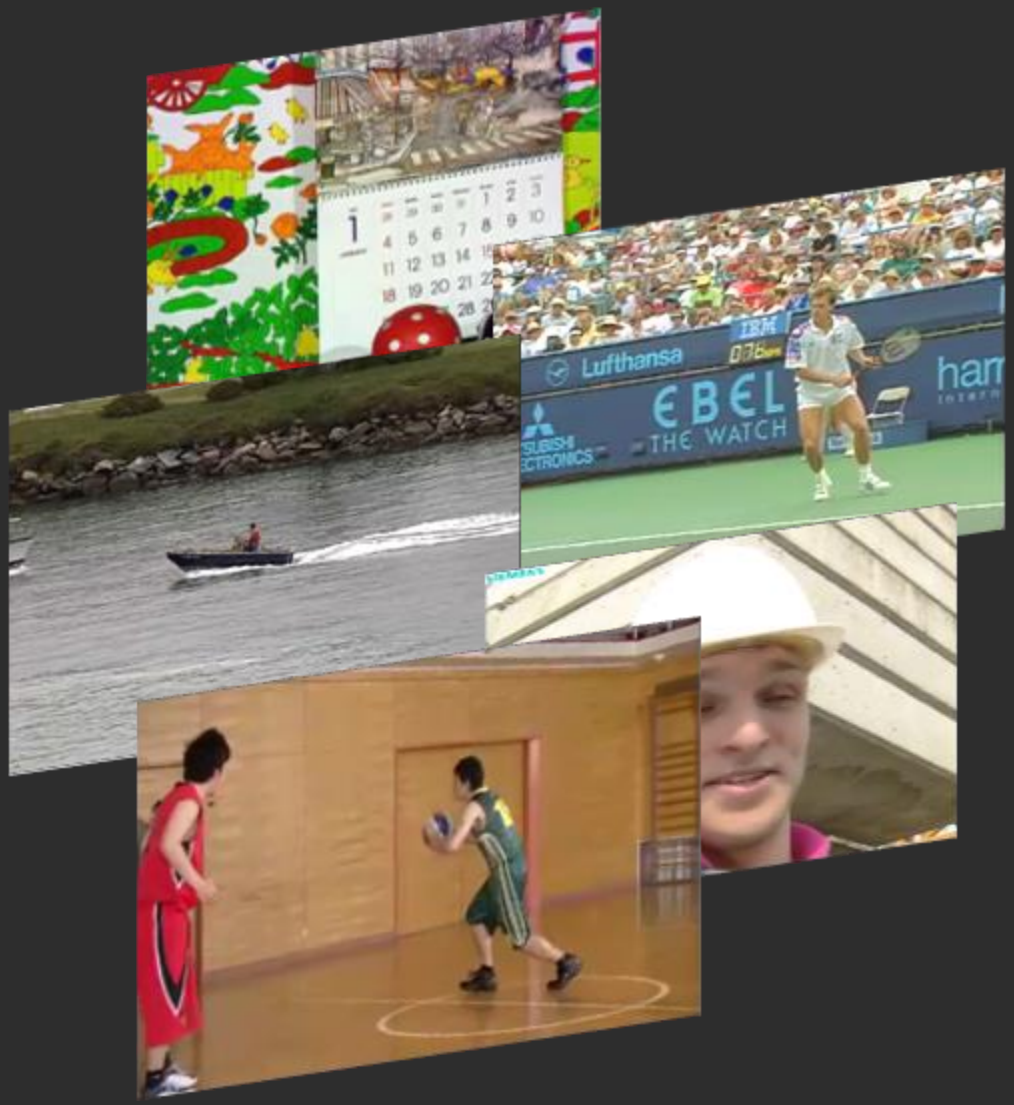
Proposed Selective Encryption (SE) Method



$$F_n = \sum_{i=0}^{q-1} C_i$$



Experiment



- CIF benchmark videos
- *Mobile, Stefan, Coastguard, Basketball Pass, Foreman*
- JM18.6
- Parameter setting

  GOP period 50 frames

Experient Result

Original Video

Proposed Method

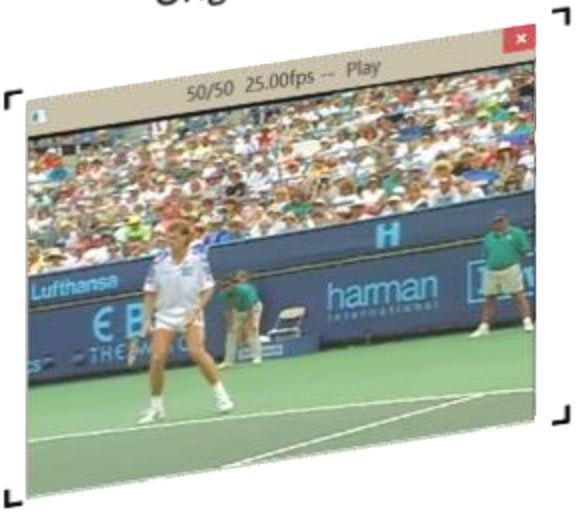
IDR Frame: α=0.5

Last Frame:α=0.5

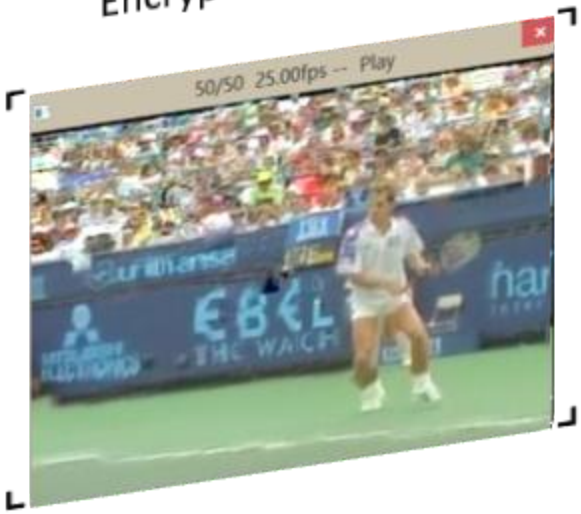
Other Frames:α=0.05

Experient Result

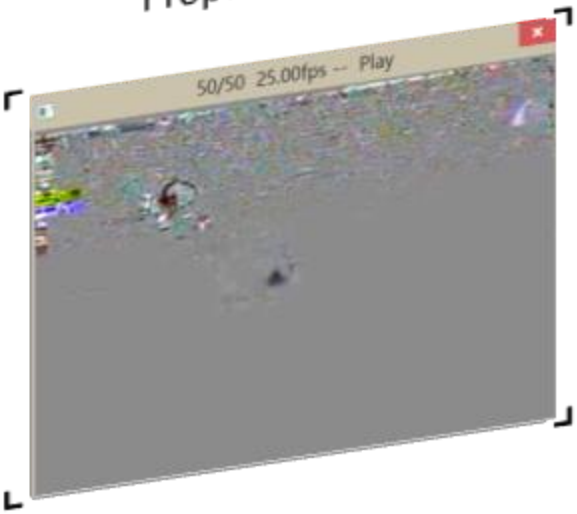
Original Video



Encrypted P/B Frames



Proposed Method



IDR Frame: α=0.5

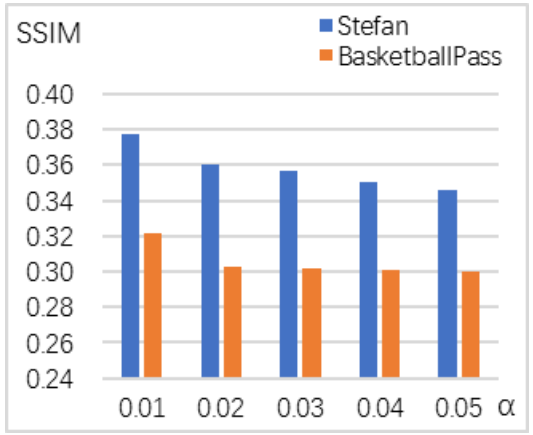
Last Frame:α=0.5

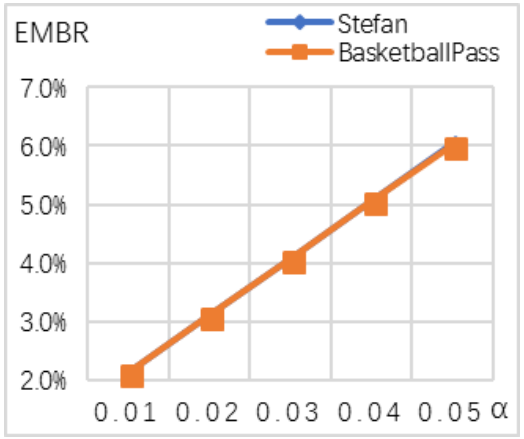
Other Frames:α=0.05

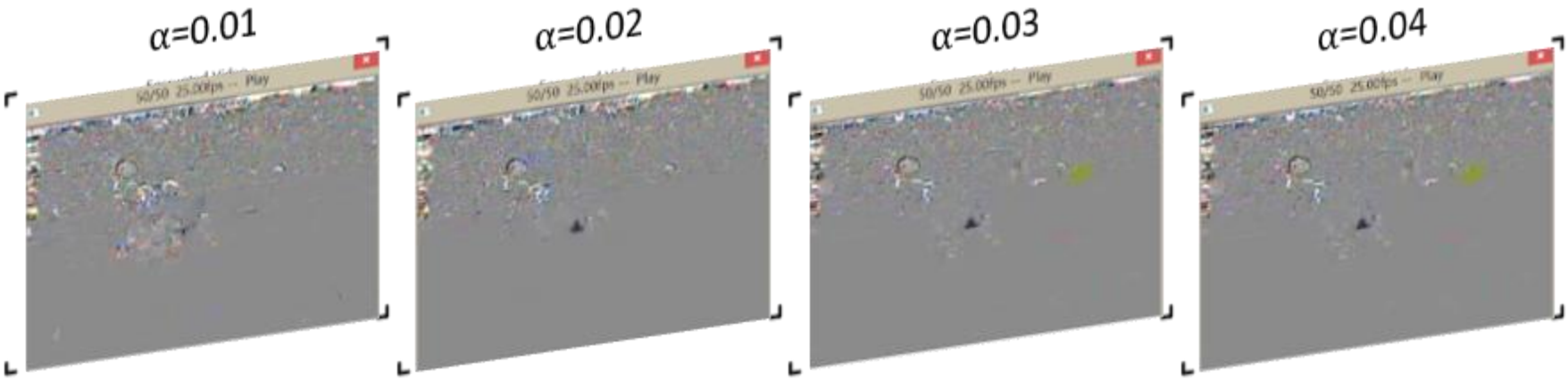
Experient Result

- Adjust parameter α
- Encrypted MB ratio is defined as

$$EMBR = \frac{Enc\ MB\ number}{sum\ MB\ number}$$







Comparison with Prior SE Methods

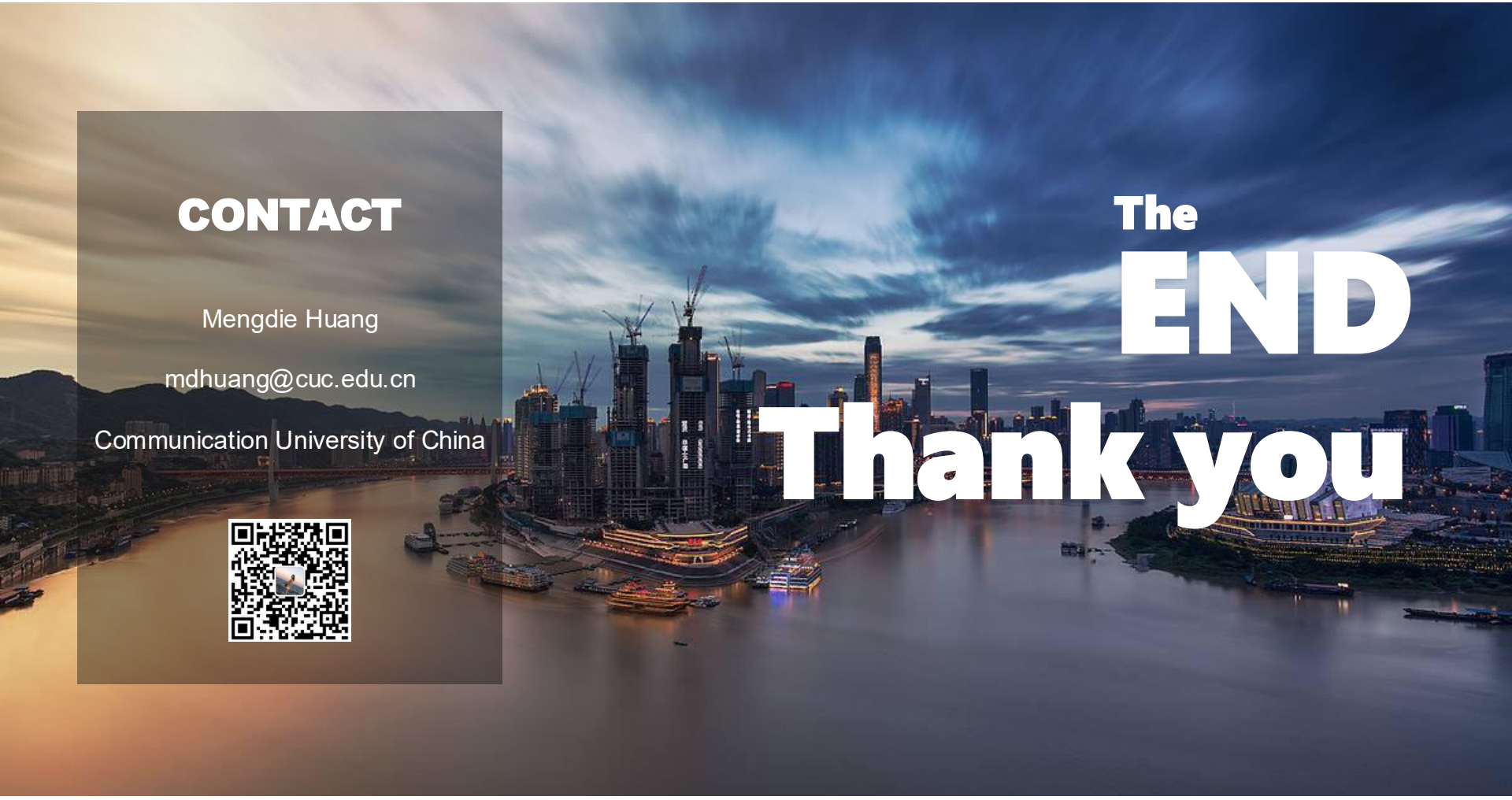
Sequence	Shen SE		Proposed SE	
	EMBR (%)	EDR (%)	EMBR (%)	EDR (%)
Mobile	54.0	5.30	**5.97**	6.07
Stefan	33.0	5.15	**6.03**	7.03
Foreman	42.7	8.86	**6.10**	9.94

Sequence	Khlif SE		Proposed SE	
	Mobile	*Foreman*	*Mobile*	*Foreman*
Original PSNR	29.84	35.92	35.264	37.603
Encrypted PSNR	8.99	10.67	12.003	12.109
EDR (%)	49.640	49.175	**6.07**	**9.94**
PSNR Difference	20.850	25.250	**23.261**	**25.584**

Conclusion

A novel SE method for H.264/AVC video bitstream

- ✓ Non-information leakage
- ✓ Network friendliness
- ✓ No effect on compressed efficiency
- ✓ Support custom security level
- ✓ Resist brute force attack and sketch attack


CONTACT
Mengdie Huang
mdhuang@cuc.edu.cn
Communication University of China
The
END
Thank you