Selective encryption for H.264/AVC Video streams

WORKLETID:24VI59IITJ

Agenda

- Work Done
- KPIs achieved
- Challenges faced
- Results and Observations

Work Done

Successfully employed three schemes for selective encryption based approach

Scheme 1

Encrypts and decrypts I-frames of a video using a XOR-based encryption and column permutation scheme.

Scheme 2

Selectively encrypts H.264 video and slices (NAL units of type 1 and 5) based on their macroblock QP values. It uses AES-CTR.

Back to Agenda

KPIs Achieved

Major milestones are as following

Back to Agenda

Selective Encryption

Targeted encryption of video macroblocks based on QP, preserving compression efficiency.

Successful Decryption

Ensured accurate frame recovery with no visible artifacts post-decryption.

Audio Encryption

Fully encrypted AAC stream using AES, maintaining sync and integrity

Challenges Faced

Major challenges that plagued us were

Back to Agenda

C++ Limitations

Advanced Scheme 2 required bit-level manipulation and rapid prototyping, which was cumbersome in C++, so we shifted to Python.

Bitstream Parsing Complexity

Extracting data like residuals and motion vectors needed deep parsing of the encoded H.264 bitstream, unlike QP and macroblocks which are accessible via FFmpeg.

Encryption time

Encryption time, especially for longer videos, is very long and requires waiting.

Scheme 1 Results

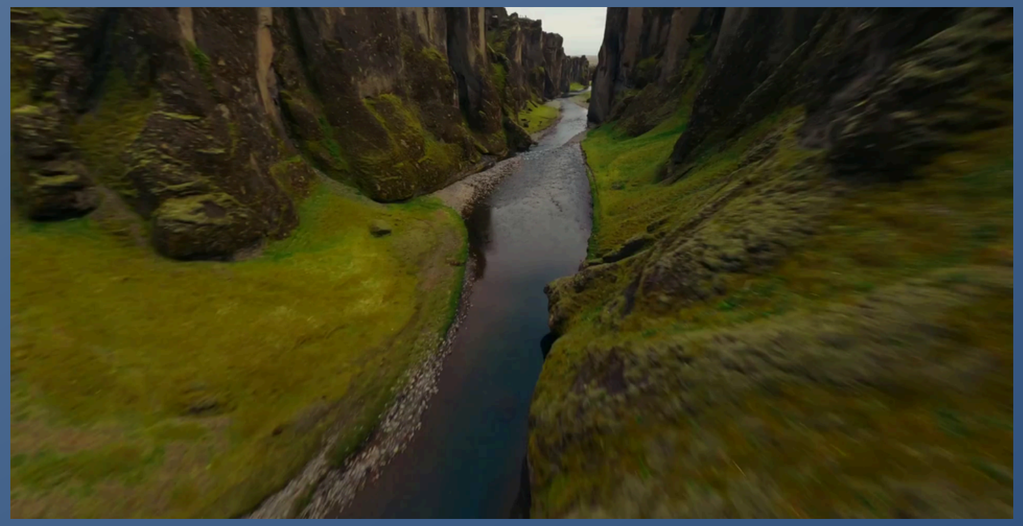
Encrypted video stream

Encrypted video is not visually recognizable as the original video.

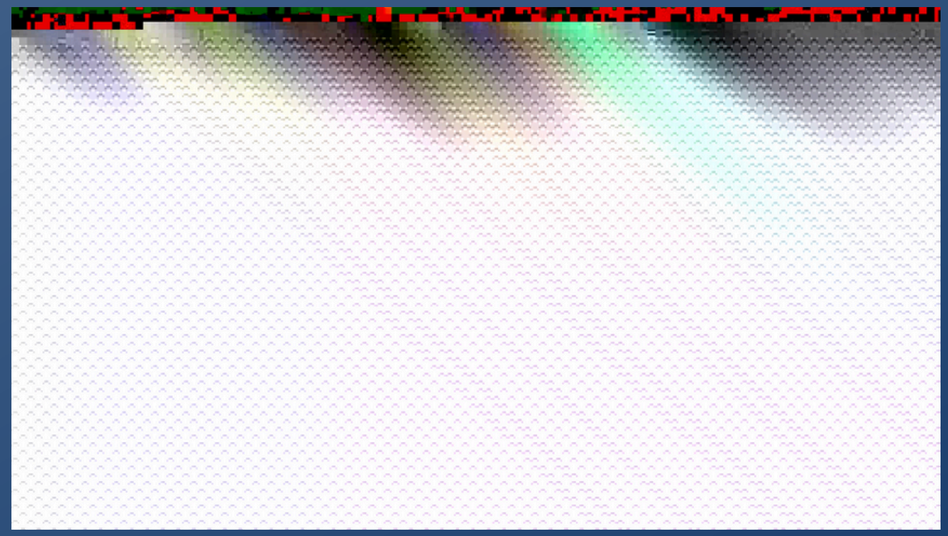
Size of file not changed as expected

```
hiteshchoudhary@Hiteshs-MacBook-Pro ~/Documents/selective_encryption/code/video/output main ● ls -lh
total 3096
-rw-r--r--@ 1 hiteshchoudhary  staff   514K  6 Mar 12:17 output.mp4
-rw-r--r--@ 1 hiteshchoudhary  staff   514K  6 Mar 12:18 output_decrypted.mp4
-rw-r--r--@ 1 hiteshchoudhary  staff   514K  6 Mar 12:18 output_encrypted.mp4
```

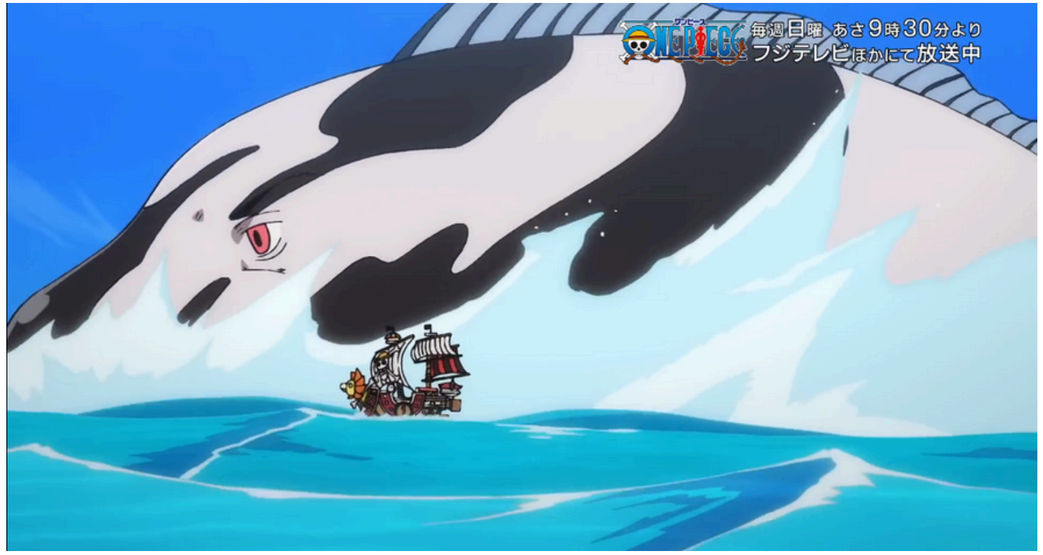
Scheme 2 Results

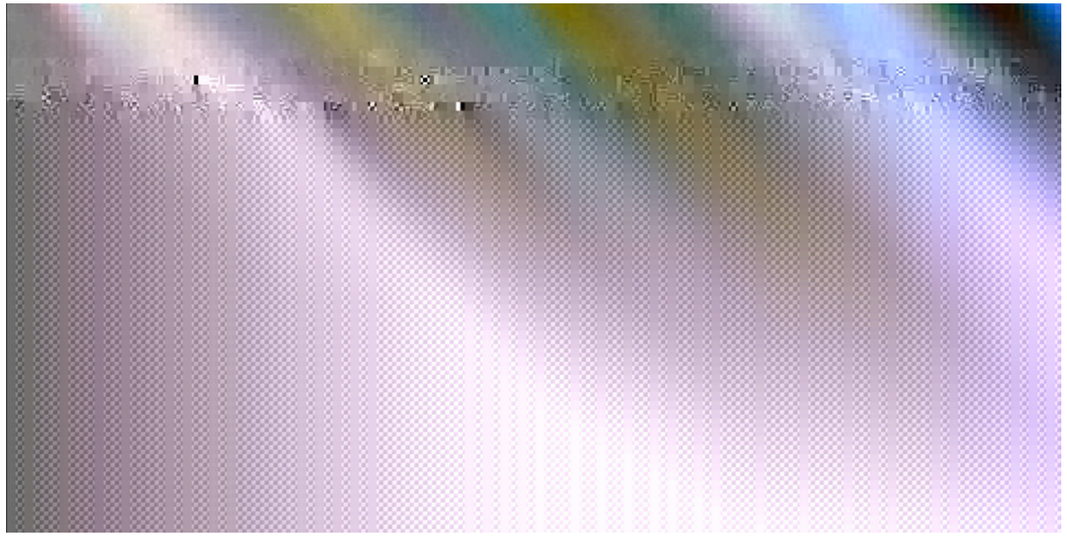


Original Frame



Encrypted Frame

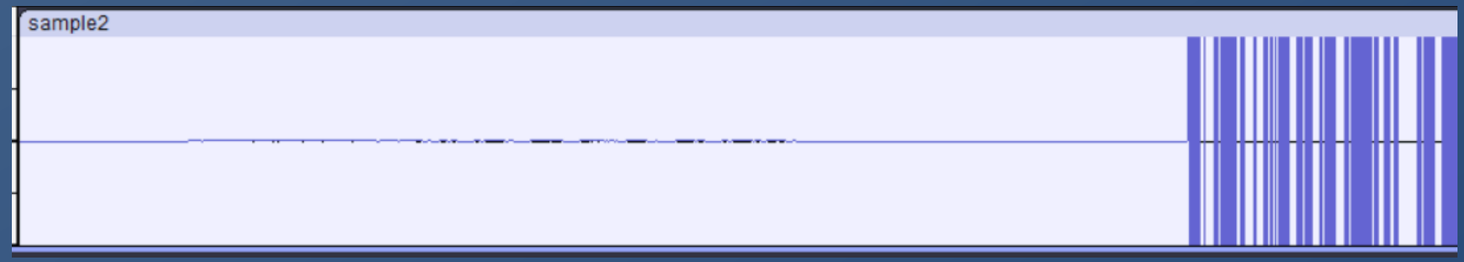




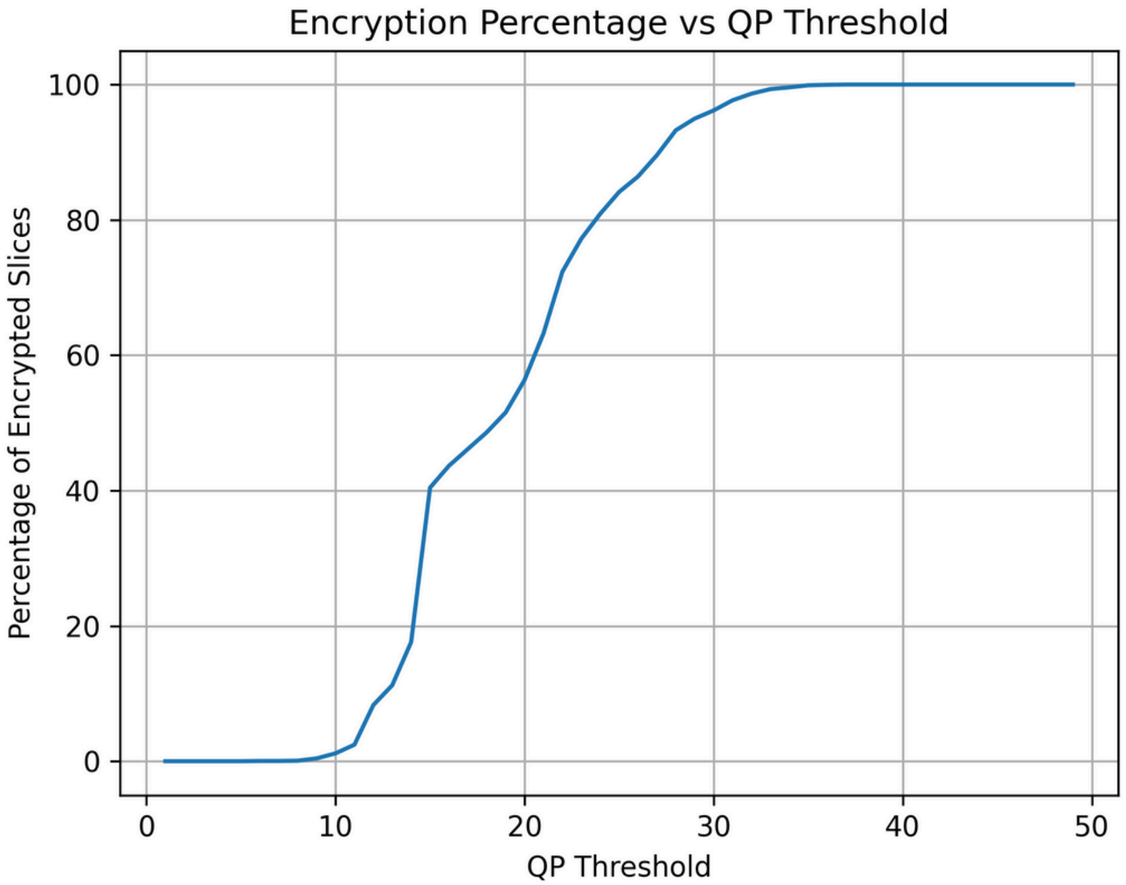
Scheme 2 Results

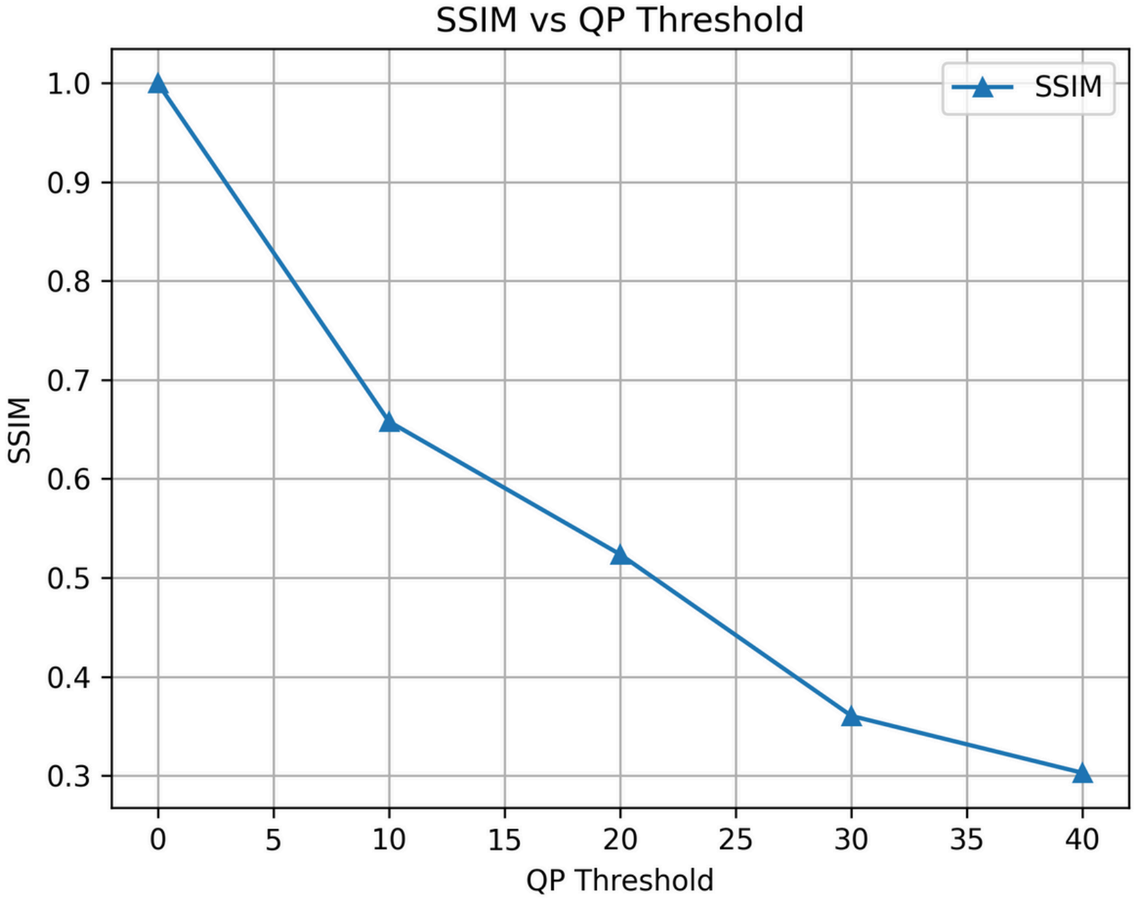
Original Audio

Encrypted Audio

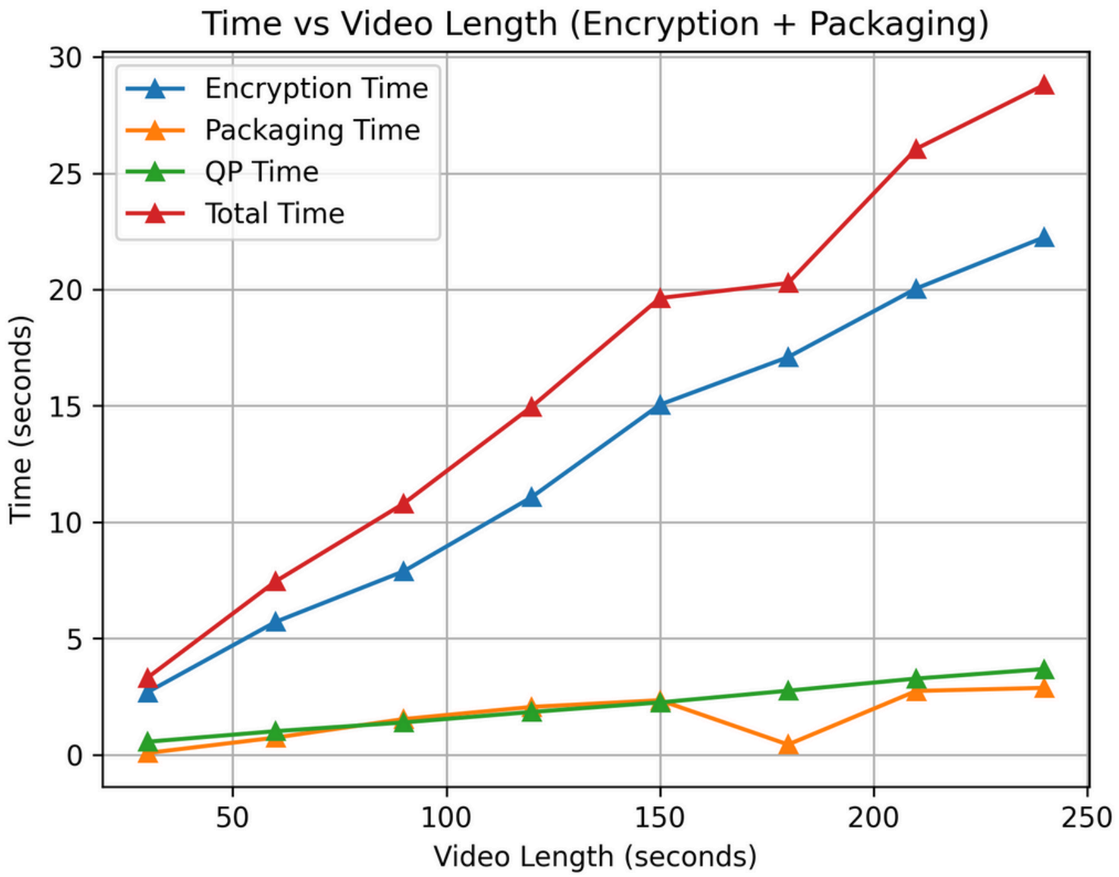


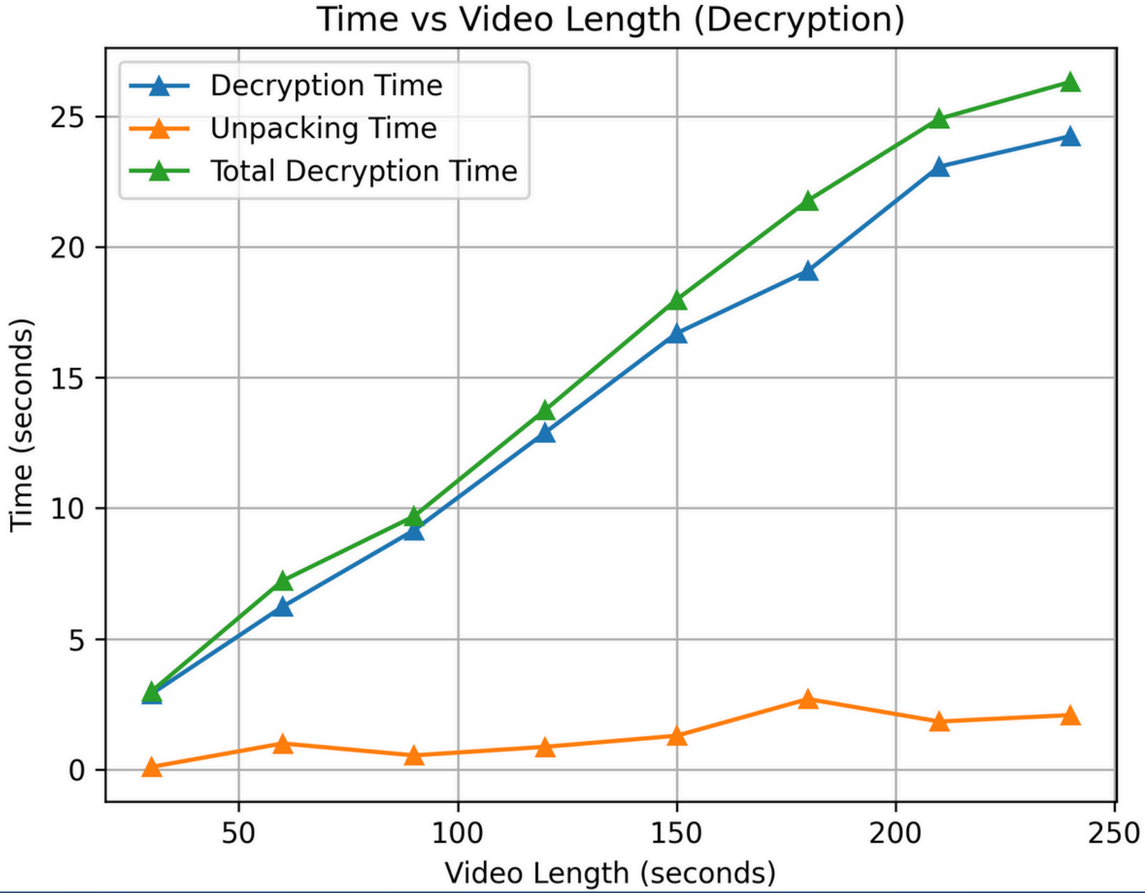
Metrics


Encryption Percentage vs QP Threshold
Percentage of Encrypted Slices
QP Threshold
0
20
40
60
80
100
0
10
20
30
40
50

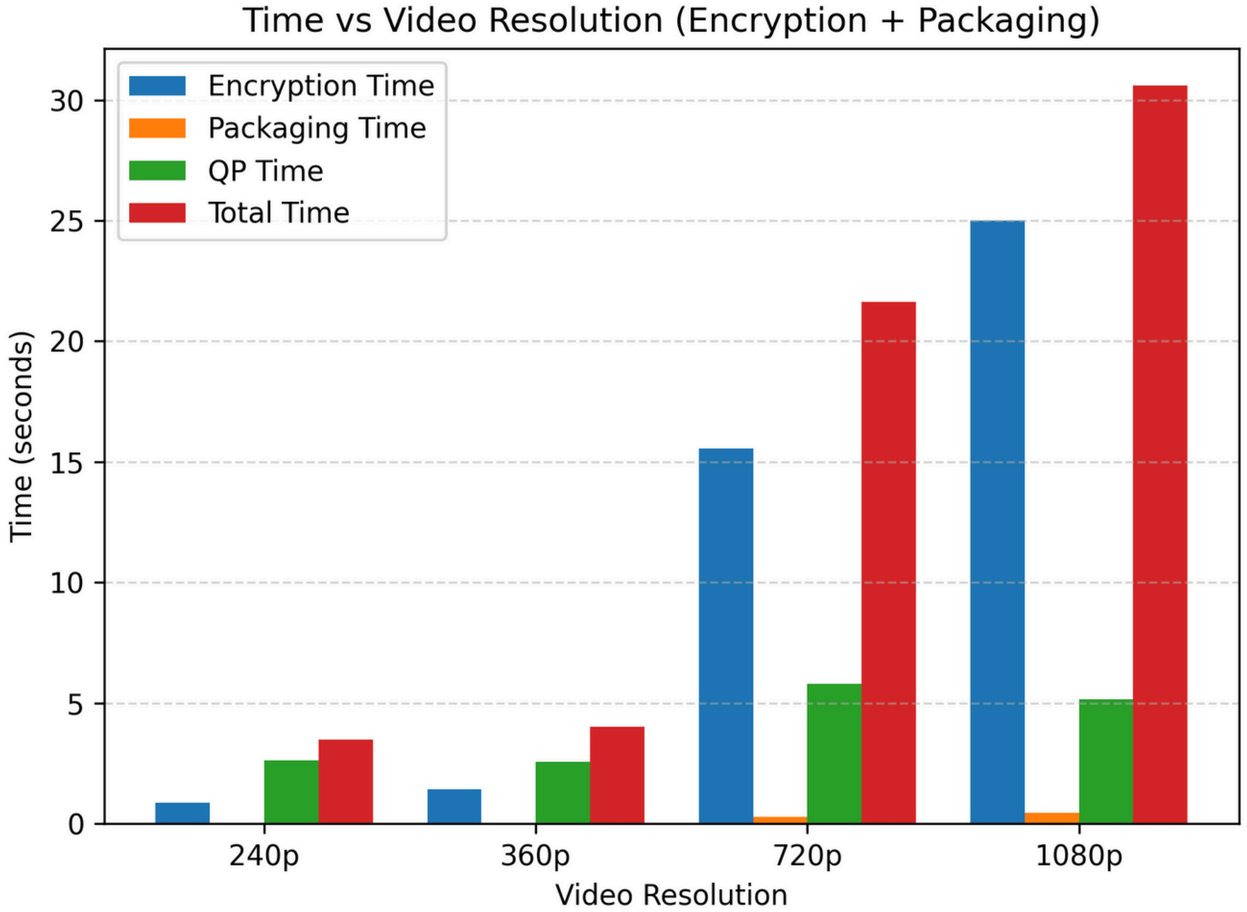

SSIM vs QP Threshold
SSIM
QP Threshold
SSIM
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1.0
0
5
10
15
20
25
30
35
40

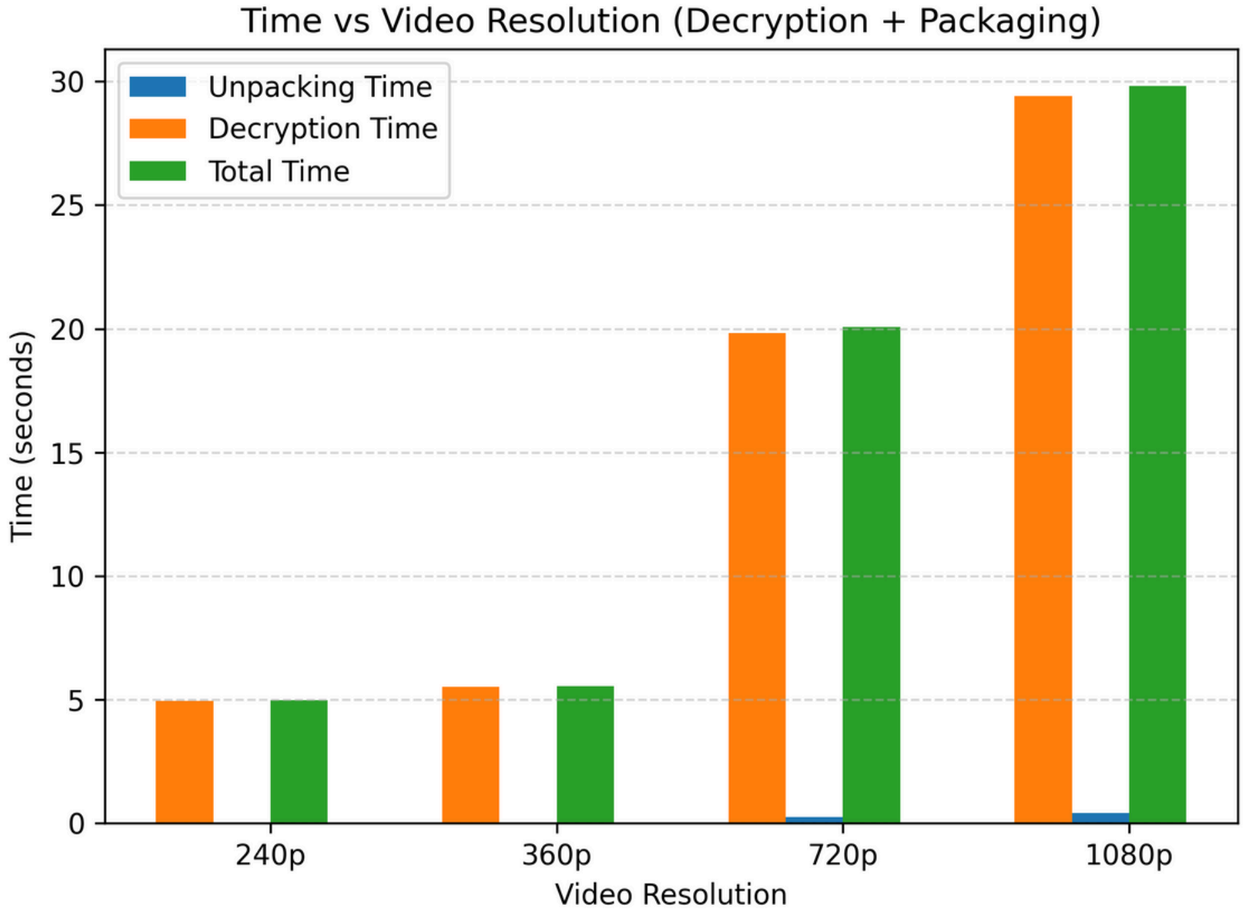
Metrics


Time vs Video Length (Encryption + Packaging)
Encryption Time
Packaging Time
QP Time
Total Time
Time (seconds)
Video Length (seconds)
0
5
10
15
20
25
30
50
100
150
200
250


Time vs Video Length (Decryption)
Decryption Time
Unpacking Time
Total Decryption Time
Time (seconds)
Video Length (seconds)
0
5
10
15
20
25
50
100
150
200
250

Metrics


Time vs Video Resolution (Encryption + Packaging)
Encryption Time
Packaging Time
QP Time
Total Time
Time (seconds)
0
5
10
15
20
25
30
240p
360p
720p
1080p
Video Resolution


Time vs Video Resolution (Decryption + Packaging)
Unpacking Time
Decryption Time
Total Time
Time (seconds)
0
5
10
15
20
25
30
240p
360p
720p
1080p
Video Resolution