

SELECTIVE ENCRYPTION FOR H.264/AVC VIDEO STREAMS

WORKLET ID:24VI59IITJ

Presentation outline

Work Done
KPIs achieved
Challenges faced
Results and Observations
Upcoming plans

Work done

Scheme 1

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

Github link: [Link](#)

Compression

Compresses a video using the H.264 codec with FFmpeg's libav library.

Scheme 2

Paper given in worklet. Not working properly right now, needs some resolving

“A Selective Video Encryption Scheme Based on Coding Characteristics Shuli Cheng”

Decompression

Decompresses and re-encodes a video using FFmpeg with lossless H.264 compression

KPIs achieved

Video Encryption

The video stream undergoes full encryption, where all frames are securely encrypted using the AES algorithm to ensure data confidentiality and protection against unauthorized access.

Successful decryption

The decrypted video maintains complete visual integrity, ensuring that there are no perceptible differences between the original and decrypted versions, thereby preserving quality and user experience.

Audio Encryption

The audio stream is fully encrypted using the AES algorithm

Challenges faced

Scheme 2

Not able to parse macroblocks currently, resulting in compression/decompression issues

Average Encryption Time

Time is currently very high as all frames are being encrypted

Selective Encryption

Currently encrypting all frames, instead of selective ones

Audio Decryption

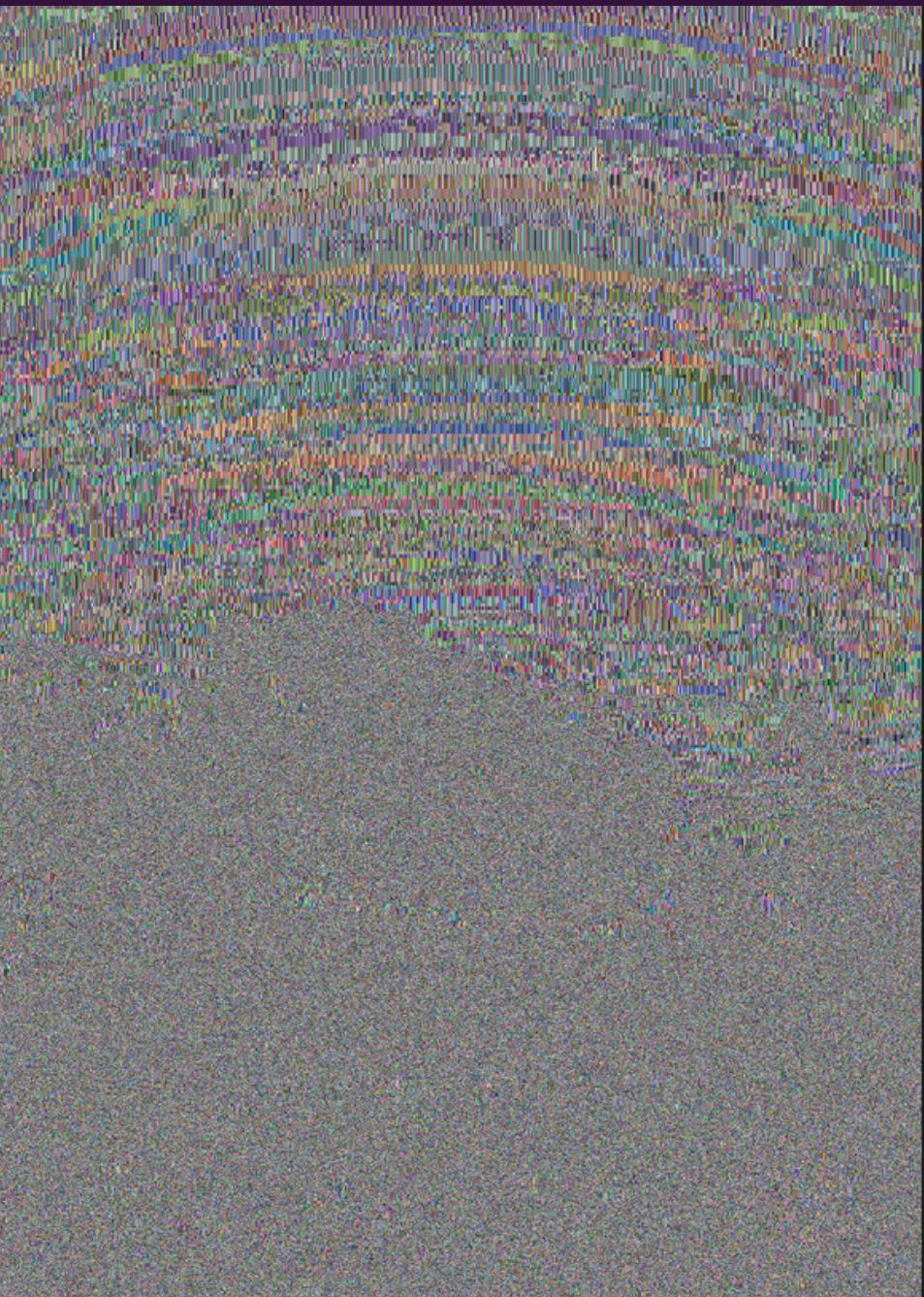
Decrypted audio files currently are very different from original ones

Results

Encrypted video stream

Encrypted video is not visually recognizable as
the original video.

However encryption takes a lot of time and
space



• • •
• • •
• • •
• • •
• • •

Metrics

Original Video and Decrypted video

PSNR 28.20 dB

SSIM 0.47

Metrics

Schemes 1 and 2 do not change size of files 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
```

Results

Original audio stream



Encrypted audio stream



Upcoming plans

Selective encryption and performance optimization

- Implement selective encryption to encrypt only the intended portions of frames.
- Optimize encryption and decryption time for better performance.
- Integrate video and audio encryption together

Upcoming plans

Proper implementation of Scheme 2 and others

- Fix bugs in scheme 2 implementation
- Test few more schemes and compare the results

Upcoming plans

Testing & Validation

- Test and validate selective encryption effectiveness.
- Address any compatibility issues with playback.
- Conduct security analysis to ensure robustness.