SWIN BUR NE

CENTRE FOR ADVANCED INTERNET ARCHITECTURES

An Evaluation of Current MPEG-1 Ciphers and their Applicability to Streaming Video

Jason But
jbut@swin.edu.au

Why MPEG-1 Encryption

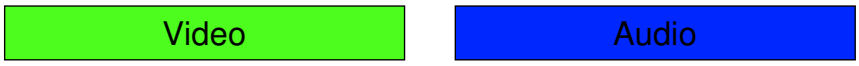
- Format maturity
- Greater range of existing ciphers
- Requirements remain valid
  - We want compatibility with existing streaming video systems
- Principles are the same
  - A suitable MPEG-1 cipher can be modified for MPEG-2 or MPEG-4

Copyright

- Protects the content owner:
  - Dictate how their content may be used
  - Need not necessarily be commercial
  - GNU License an example of the best known "free" Copyright protection license
- Important with streaming multimedia
  - Higher cost of content generation
  - Higher value of content
  - Greater potential for commercialisation

The MPEG-1 Standard

- ISO Standard – ISO/IEC 11172-x
- Separate Video and Audio Streams



- Packetised

- Multiplexed into a single System Stream

- Similar approach for other encoding standards

Video Stream Format

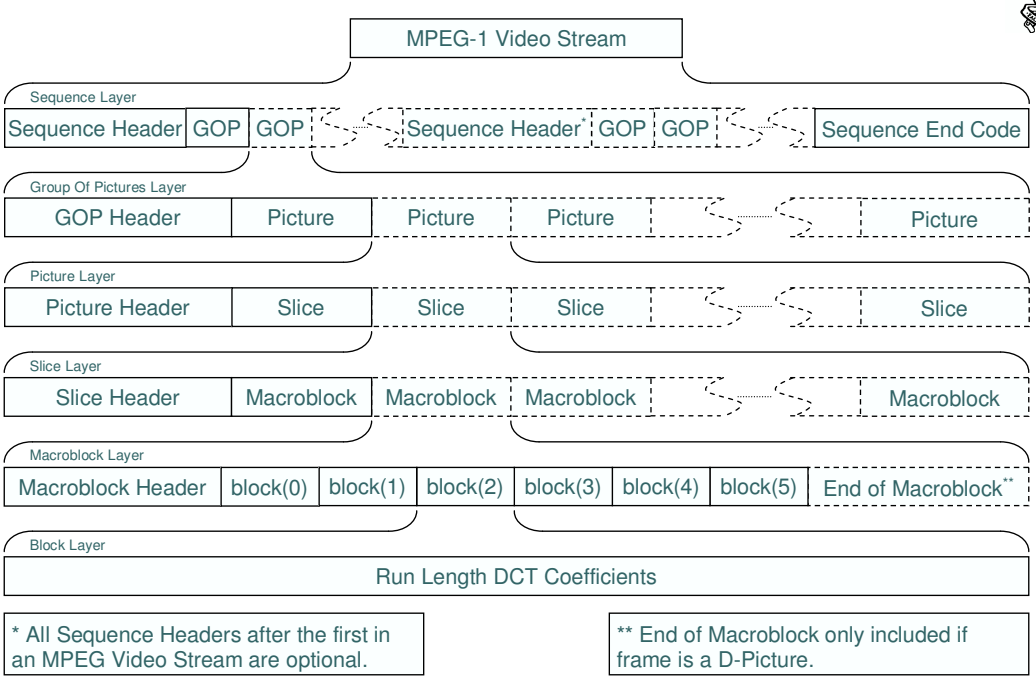
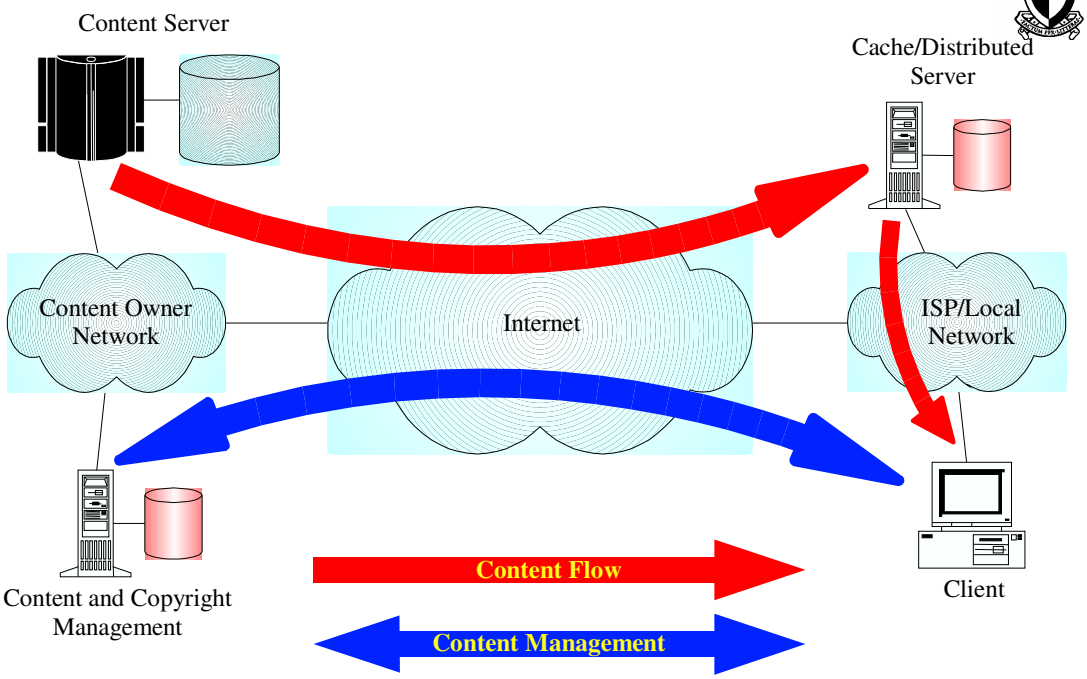


Diagram modified from original in:
Mitchell, J. L., Pennebaker, W. B., Fogg, C. E. and LeGall, D. J., *MPEG Video Compression Standard*, Chapman & Hall ISBN 0-412-08771-5.

Distributed Streaming Video

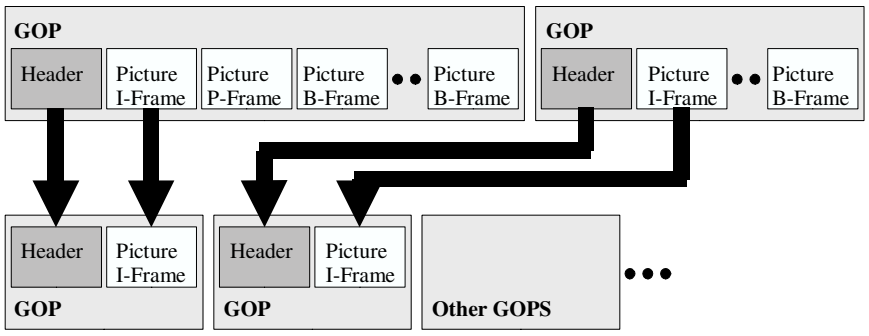


Requirements

- It must be possible to extract the Video and Audio Streams from the encrypted bitstream and to decrypt these streams independently, without requiring changes to existing streaming server implementations.
- The encrypted bitstream must have valid MPEG-1 bitstream syntax.
- The streaming server must be able to locate each GOP in the encrypted bitstream.
- The cipher must be able to resynchronise itself such that decryption can correctly occur at allowable indexation points within the Video Stream.

Requirements

- The Streaming Server must be able to locate each I-Frame within the encrypted bitstream.
- The cipher must be able to resynchronise itself such that decryption can correctly occur during high-speed playback modes.



Requirements

- Encrypting the bitstream must not affect the maximum number of concurrent streams that the server can support.
- The cipher module should not form an explicit part of the decoder.
- The cipher should be secure against attack.

Existing MPEG-1 Ciphers

Cipher	Encrypted bitstream can be stored on server	Scalable to support multiple concurrent streams	No changes required to Server Implementat-ion	Encrypted bitstream can be served in Inedexed Playback modes	Encrypted bitstream can be served in High-Speed Playback modes	Cipher can be resyncrhon-ised during Indexed Playback	Cipher can be resynchron-ised during High-Speed Playback	Cipher can be efficiently implemented externally to the MPEG-1 decoder implementa-tion	Cipher is secure against attack
IPSec	N/A	▯	▯	N/A	N/A	N/A	N/A	N/A	N/A
SSL	N/A	▯	▯	N/A	N/A	N/A	N/A	N/A	N/A
Full Encryption	N/A	▯	▯	N/A	N/A	N/A	N/A	N/A	N/A
SECMPEG	▯	▯	▯	▯	▯	▯	▯	▯	▯
Zig-Zag Permutation Algorithm	▯	▯	▯	▯	▯	▯	▯	▯	▯
Video Encryption Algorithm	▯	▯	▯	▯	▯	Unknown	Unknown	▯	▯
Video Encryption Algorithm – Number 2	▯	▯	▯	▯	▯	▯	▯	▯	▯
Frequency Domain Scrambling Algorithm	▯	▯	▯	▯	▯	Unknown	Unknown	▯	▯
A Unique Cipher	▯	▯	▯	▯	▯	▯	▯	▯	▯
Multi Layer Encryption	▯	▯	▯	▯	▯	Unknown	Unknown	▯	▯
Selective Macroblock Encryption	▯	▯	▯	▯	▯	▯	▯	▯	▯
AEGIS	▯	▯	▯	▯	▯	Unknown	Unknown	▯	▯

*Unknown – The cipher designers have not specified how synchronisation takes place.

Conclusions

- No existing ciphers are suitable…
- Where to from here?
  - A cipher should be developed that meets all of the listed specifications
  - The general ideas should apply to all video compression formats
  - Take into account streaming video server design and implementation
  - Provide a solution to Copyright protection – remove a potential impediment to widespread streaming video implementation