INTERNATIONAL ORGANISATION FOR STANDARDISATION

ORGANISATION INTERNATIONALE DE NORMALISATION

ISO/IEC JTC 1/SC 29/WG 11

CODING OF MOVING PICTURES AND AUDIO

ISO/IEC JTC 1/SC 29/WG 11 N19458

Summary

This document is the text of FDAM 1 for MPEG A-VIMAF, ISO/IEC 23000-21, containing a new annex for the Reference software and Conformance points.

**Information technology — Multimedia application format (MPEG-A) — Part 21: Visual identity management application format**

**Amendment 1: Conformance and reference software**

*Add the following references in §2 Normative references:*

*ISO/IEC 14496-5, Information technology -- Coding of audio-visual objects -- Part 5: Reference software*

*ISO/IEC 23008-5, Information technology -- High efficiency coding and media delivery in heterogeneous environments -- Part 5: Reference software for high efficiency video coding*

*In clause 6.1 replace:*

*“*

Thus, to ensure perfect decryption and reconstruction, the exact process to encrypt (and decrypt) protected bitstream by content sensitive encryption is described in ‎6.2‎ and 6.3, and shall be carried out as specified in Annex A.

“

*With*

“

Thus, to ensure perfect decryption and reconstruction, the exact process to encrypt (and decrypt) protected bitstream by content sensitive encryption is described in ‎6.2‎ and 6.3, and shall be carried out as specified in Annex A and in Annex B.

“

*Add a new normative Annex B with the following text:*

**Annex B**  
(normative)  
  
**Conformance and reference software**

**B.1 General**

This annex provides a verification toolset for content sensitive encryption (CSE) as described in Annex A. It contains the following components:

— Reference software: Implementations which demonstrate the CSE method for AVC and HEVC.

— Test vectors: Stand-alone compliant content that implements elements of the document.

This software is available at <https://standards.iso.org/iso-iec/15444/-5/ed-2/en/amd/1>

**B.2 Content sensitive encryption reference software**

**B.2.1 Reference software presentation**

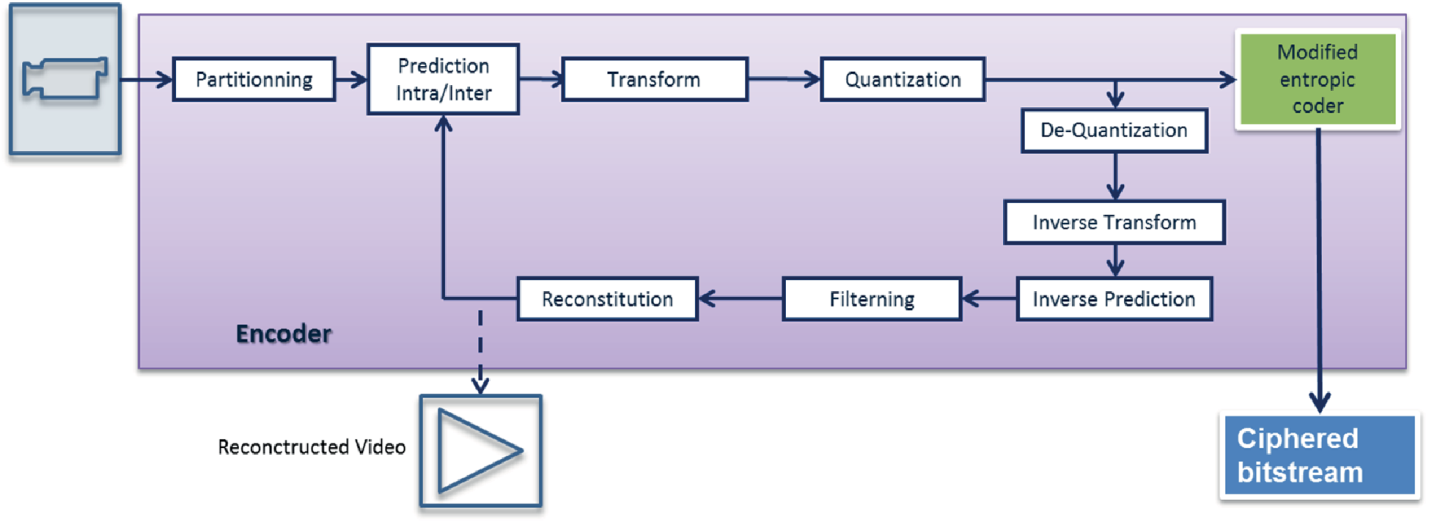
Unlike previous encryption schemes, content sensitive encryption considers the coding structure of the video compressed bitstream and encrypts only the most sensitive information in the video bitstream. Also, CSE generates protected bitstreams that can be decoded by any compliant decoder without requiring access to the encryption key. So since the content sensitive encryption takes place inside codec, the reference software is based on ISO/IEC 14496-5 and ISO/IEC 23008-8 reference software for AVC (Rec. ITU-T H.264 | ISO/IEC 14496-10) and HEVC (Rec. ITU-T H.265 | ISO/IEC 23008-2) codecs respectively.

To be sure that the ciphered bitstream follow the rules defined in Annex A, it is important to note that ciphered bits maintain this capacity in every coded bitstream. So the CSE reference software indicates the bits ‘selected for encryption’ (also called ‘cipherable’) that will correspond to cases where several code-words of same length are available with no major context change when shifting from one to another, and the ciphering will consist to swap on of the bit(s) configuration by another.

**B.2.2 Reference software encoder**

To cipher the bits ‘selected for encryption’ as defined in Annex A, the reference software encoder ciphers the ‘cipherable’ bits with a pseudo-randomized bitstream file (i.e. ciphertext file) as input.

The reference software encoder ISO/IEC 14496-5 or ISO/IEC 23008-8 are modified by only changing the entropy coding as described in Figure B.1.

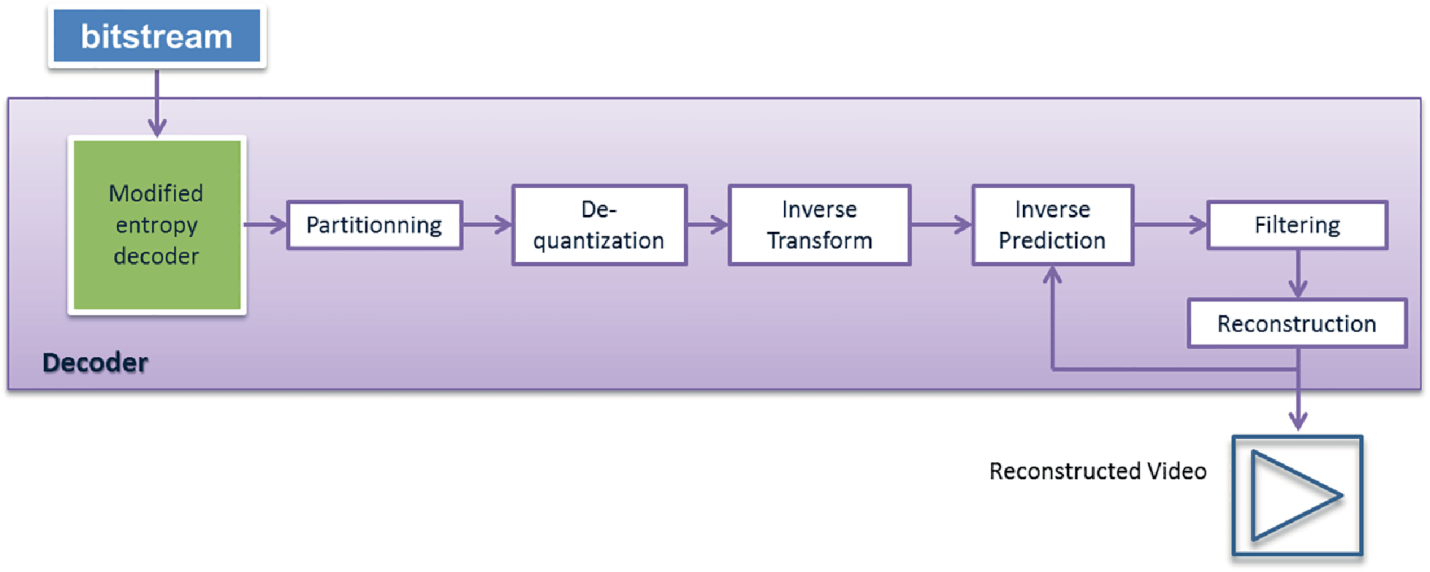


**Figure B.1 — Reference Software Encoder**

**B.2.3 Reference software decoder**

To decode and decrypt bitstream where the bits ‘selected for encryption’ are ciphered, the reference software decoder deciphers the ‘cipherable’ bits defined in Annex A with a pseudo-randomized bitstream file (i.e. ciphertext file) as input.

The reference software encoder ISO/IEC 14496-5 or ISO/IEC 23008-8 are modified by only changing the entropy decoding as described in Figure B.2.



**Figure B.2 — Reference Software Decoder**

**B.2.4 Source code**

The reference software and the conformance files are available at: <https://standards.iso.org/iso-iec/15444/-5/ed-2/en/amd/1>.

The repository contains the modified ISO/IEC 14496-5 and ISO/IEC 23008-8 reference software with the same original structure, and the associated command lines. A readme.txt is provided to explain how to produce the executable in a Windows or Linux environment. But to encrypt (and decrypt), the parameter ‘--Encryption’ (and ‘--Decryption’ respectively) needs to be added in the command line to generate encrypted bitstream (or to decrypt the bitstream).

**B.3 Conformance points**

Conformant files are a set of encrypted bitstreams (with CSE) and can be readable by the reference software decoder and by the original ISO/IEC 14496-5 or ISO/IEC 23008-8 reference software decoder. But only the reference software decoder provided by this annex can reconstruct perfectly the deciphered video, while the original ISO/IEC 14496-5 or ISO/IEC 23008-8 reference software decoder can only display non-intelligible content.

To ensure conformance and verify the correct reconstruction after deciphering, each encrypted file with CSE is associated with a reconstructed YUV file.

Moreover, a set of ISOBMFF file format files is also available. Those files contain the encrypted bitstream and all the encryption information (as defined in ISO/IEC 23001-7) necessary to decrypt properly the media.