FINAL DRAFT

AMENDMENT

ISO/IEC 23000-21:2019 FDAM 1

ISO/IEC JTC **1**/SC **29**

Secretariat: JISC

Voting begins on:
2021-03-03

Voting terminates on:
2021-04-28

Information technology — Multimedia application format (MPEG-A) —

Part 21: Visual identity management application format

AMENDMENT 1: Conformance and reference software

Partie 21: Format pour application de gestion d'identité visuelle

AMENDEMENT 1: Titre manque

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/IEC 23000-21:2019/FDAM 1:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Information technology — Multimedia application format (MPEG-A) —

Part 21:
Visual identity management application format

AMENDMENT 1: Conformance and reference software

Clause 2

Add the following new 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*

Subclause 6.1, fifth paragraph

Replace the first sentence with the following:

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 Annexes A and B.

Annex A

At the end of Annex A, add a new Annex B:

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/23000/-21/ed-1/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. Since the content sensitive encryption takes place inside codec, the reference software is based on ISO/IEC 14496-5 and ISO/IEC 23008-5, which provide 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 that ciphered bits maintain this capacity in every coded bitstream. 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 swap the bit(s) configuration with 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 23008-5) is modified by only changing the entropy coding as described in Figure B.1.

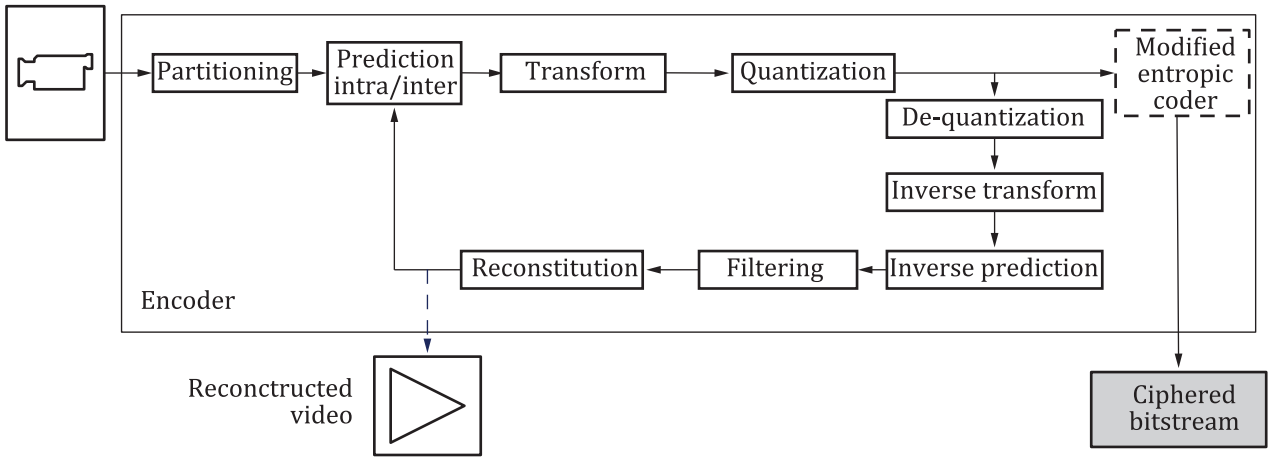

Figure B.1 — Reference software encoder

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 23008-5) is modified by only changing the entropy decoding as described in Figure B.2.

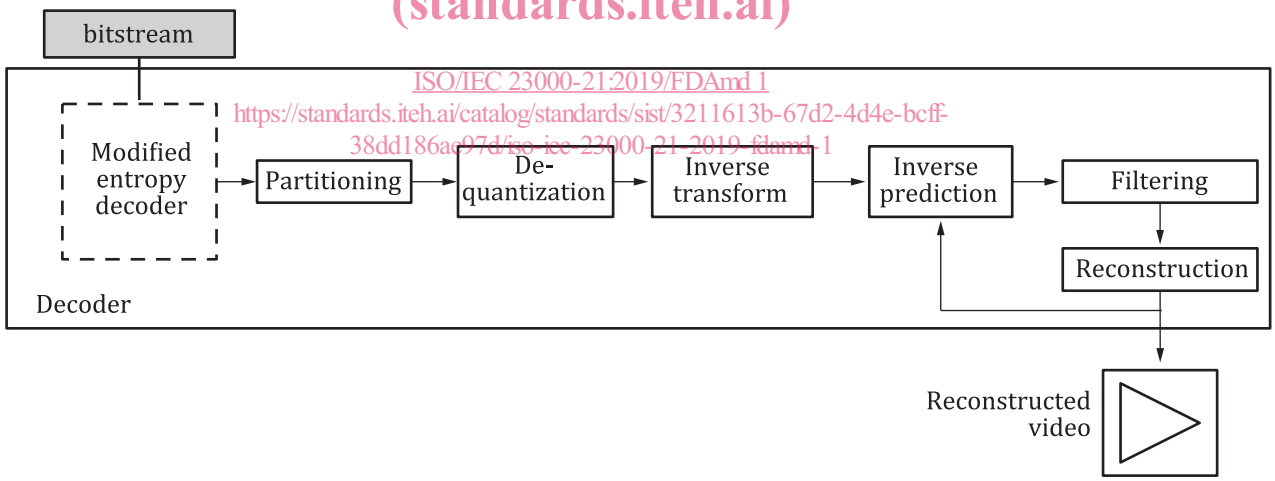

Figure B.2 — Reference software decoder

B.2.4 Source code

The reference software and 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 23008-5 reference software with the same original structure, and the associated command lines. A readme.txt is provided to explain how to produce executables 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 23008-5 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 23008-5 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.