DRAFT AMENDMENT

ISO/IEC 23000-21:2019/DAM 1

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

Secretariat: **JISC**

Voting begins on:
2020-03-31

Voting terminates on:
2020-06-23

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

Part 21:
Visual identity management application format

AMENDMENT 1: Conformance and reference software

ICS: 35.040.40

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC 23000-21:2019/DAM 1:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
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

Add a new normative Annex B with the following text:

Annex B
(normative)

Conformance and reference software

B.1 Introduction

This annex provides a verification toolset for the method called "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 implement elements of the standard.

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

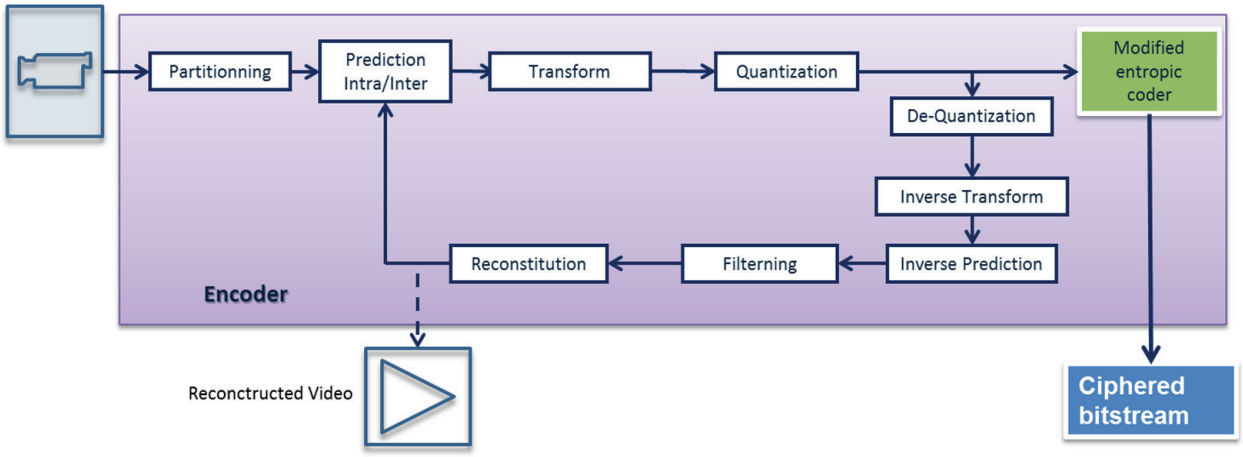
At the difference with those previous encryption schemes, Content Sensitive Encryption considers the coding structure of the video compressed bitstream and encrypts only the most sensitive information in the video bitstream. And CSE generates protected bitstreams that can be decoded by any compliant decoder without requiring access to the encryption key. So since the Content Sensitive Encryption takes place inside codec, the reference software is based on JM (ISO/IEC 14496-5 or Rec. ITU-T H.264.2) and HM (ISO/IEC 23008-8 or Rec. ITU-T H.265.1) reference software for AVC (ISO/IEC 14496-10 or Rec. ITU-T H.264.1) and HEVC (ISO/IEC 23008-2 or Rec. ITU-T H.265) 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 VIMAF reference software encoder ciphers the 'cipherable' bits with a pseudo-randomized bitstream file (i.e. ciphertext file) as input.

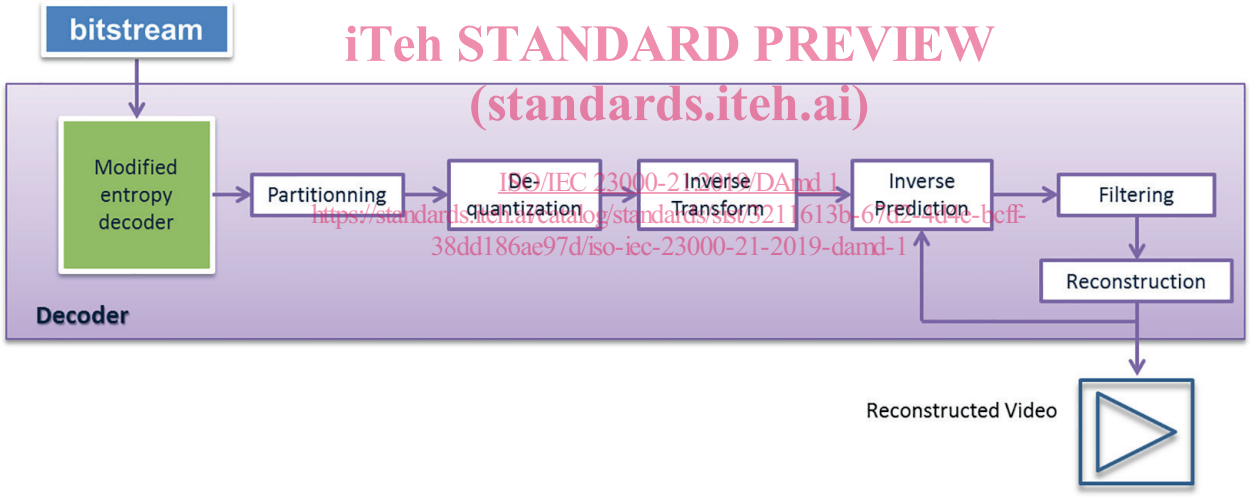
The modified JM or HM reference software encoder only change the entropy coding as described in following figure.



B.2.3 Reference Software decoder

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

The modified JM or HM reference software decoder only change the entropy decoding as described in following figure.



B.2.4 Source code

The VIMAF reference software and the conformance files are published in MPEG Gitlab repository: http://mpegx.int-evry.fr/software/whamidou/MPEGA-CSE.git

The repository contains the modified JM and HM 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) must be added in the command line to generate encrypted bitstream (or to decrypt the bitstream).

B.3 Conformance points

Conformant files is a set of encrypted bitstream (with CSE), and must be readable by the VIMAF reference software decoder and by original JM or HM reference software decoder. But in only VIMAF reference software decoder can reconstruct perfectly the deciphered video, while the original JM or HM 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 is also available. Those files contain the encrypted bitstream and all the encryption information (as defined in CENC ISO/IEC 23001-7) necessary to decrypt properly the media.