

The «Secure Media SIM» bitstream structure for video encryption and fingerprinting

Marc Antonini, Marco Cagnazzo, Marie Oger

I3S laboratory

UMR 6070 University of Nice-Sophia Antipolis and CNRS

Abstract

The steady growth in computer computational power and network bandwidth and their diffusion among research institutions, enterprises and common people, has been a compelling acceleration factor in multimedia processing research. Indeed, users want an ever richer and easier access to multimedia content and in particular to video. So, a huge amount of work has been deployed in this field, and compression has been one of the most important issues. This work produced many successful international standards, including JPEG and JPEG2000 for still image coding, and the MPEG and H.26x families for video coding. In particular, MPEG-2 has been the enabling technology for digital video broadcasting and for optical disk distribution of high quality video contents; MPEG-4 has played the same role for medium and high quality video delivery over low and medium bandwidth networks; the H.26x family enabled the implementation of teleconferencing applications.

In this paper, we will address two issues raised during the Secure Media SIM project (<http://www.securemediasim.org>). First, we will describe the syntax extension facilities provided by MPEG-2 and H.264, with the target of enabling the insertion of a fingerprint command in the encoded bitstream. If the decoder is not able to recognize it, this information will be simply skipped. Otherwise, a «Secure Media SIM» decoder can recognize this command and use it to insert a fingerprint in the decoded video. Then, we will show how motion vectors in MPEG-2 and H.264 syntax can be replaced by scrambled, encrypted or null values (see fig.1). Indeed, both MPEG-2 and H.264 standards provide ways to insert non-standard information into the bitstream, such that compliant decoders just discard it, while a suitably modified decoder can use it to perform tasks not originally available into the standard, such as the insertion of fingerprint information into the decoded stream (see fig.2).

The paper will describe how this can be done in these standards, in the context of the «Secure Media SIM» project.

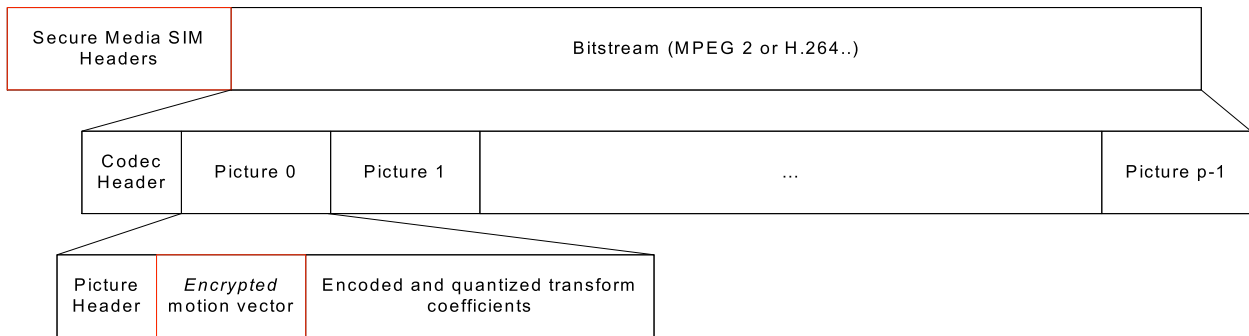


Fig. 1: The «Secure Media SIM» compliant bitstream structure

