Signal Processing in the Encrypted Domain

Ann Dooms

Vrije Universiteit Brussel, Brussels, Belgium

Content distribution applications such as digital broadcasting, video-on-demand services (VoD), video conferencing, surveillance and telesurgery are confronted with difficulties - besides the inevitable compression and quality challenges - with respect to intellectual property management, authenticity, privacy regulations, access control etc. Meeting such security requirements in an end-to-end video distribution scenario poses significant challenges.

If the entire content is encrypted at the content creation side, the space for signal processing operations is very limited. Decryption, followed by video processing and re-encryption is also to be avoided as it is far from efficient, complicates key management and could expose the video to possible attacks. Additionally, also when the content is delivered and decrypted, the protection is gone.

Watermarking can complement encryption in these scenarios by embedding a message within the content itself containing for example ownership information, unique buyer codes or content descriptions. Ideally, securing the video distribution should therefore be possible throughout the distribution chain in a flexible way allowing the encryption, watermarking and encoding/transcoding operations to commute. In this talk I will present the relevant techniques that are needed to implement such an end-to-end commutative security system for video distribution.

Vrije Universiteit Brussel, Department of Electronics and Informatics (ETRO),
Pleinlaan 2, 1050 Brussels, Belgium
ann.dooms@vub.ac.be