DRM systems in wireless environment

Rita Móga, Tamás Polyák, and István Oláh

Nowadays there is a growing interest in achieving security in digital rights management (DRM). That means there is a need for securing, watermarking and authenticating video streams. Transmitting a video stream ciphered ensures that only the addressed recipient can view the content. Authentication is needed, to be sure of the sender's identity and also of the quality. Watermarking is for detecting image manipulation and for tracking the way of the media. Creating such a system suiting the needs of the wireless environment is a great challenge, as the wireless transmission channel can easily be attacked or spoofed, and it is noisy, so much higher bit error ratio (BER) is to be expected, than a wired transmission channel. The existing algorithms in ciphering, watermarking and authentication cannot handle the elevated BER, plus they are too complex to be applied in mobile phones or PDAs all at the same time. They either need to be redesigned, or new algorithms shall be created.

In our paper we discuss ciphering, authenticating and watermarking solutions more detailed with some tests proving our results. We also show how these three solutions can work together to give a complete solution on the problems related to secure video transmission in wireless environment.

For ciphering, the major problem is that the whole video stream cannot be ciphered, as it would have too high demand on resources. The algorithm known as Video Encryption Algorithm is suitable for our purposes, as it only ciphers the I frames. According to our measurements, utilizing the statistical randomness of the compressed video information the really expensive ciphering computations (ciphering with AES or RC4) can be reduced to one selected half of the I frames. For the other half non-expensive XOR operation is used for encryption.

The challenge of the authentication is that due the higher BER in wireless environment, the methods of the wired environment cannot be used, because of their sensitivity to single bit errors. In real-time video transmission throwing away too many frames due to single bit errors would be a waist. In our paper we propose a novel approximate authentication algorithm, which is able to accept not just exact, but closely similar match as well.

To protect the stored media stream we should improve security using watermarking. Aside from imperceptibility, a very important property of the watermark is its robustness. As we said, in wireless environment the transmitted media can suffer many different distortions and attacks. We proposed a method to improve the robustness of the watermark-embedding algorithm. To achieve this we hide information bits in larger blocks instead of pixels. The algorithm also uses synchronization information to resist to attacks in the time domain, like frame dropping.

According to our measurements the proposed methods work well together in wireless environments, they offer enough protection to the media, and are suitable to run on devices low on computing resources.