Content protection: combining watermarking with encryption

Paula Steinby

Illegal copying of digital data is a big problem in today's "information society". Unauthorized copying and purchase of such material are claimed to cause a loss of billions of euros for the legal distributors. Content protection systems have been designed to protect media producers and distributors. The existing tools are limited: data encryption, digital watermarking, tamper-resistant and special-purpose devices. The ultimate goal is to make producing illegal copies impossible. While this remains unachievable, we are seeking for methods which make producing, distributing and using illegal copies of some data unattractive: difficult and/or risky.

We consider a scheme where a digital article is distributed over an insecure channel. Due to different interests of the parties involved, we will want to encrypt, watermark and compress the data. Encryption contributes to the privacy of the parties as well as makes the data useless for those without means to decrypt it. Watermarking enables one to distinguish between each copy of the data; this is useful mainly for the purposes of copyright protection. Compression is needed to facilitate the transmission and storage of the data.

In the paper we combine compression, encryption and watermarking to obtain a scheme with the following properties.

- Merchant M has data I for sale. M encrypts (the ready compressed) I into $enc(I)$ with a key K_{enc}. Then $enc(I)$ is set for distribution.
- Buyer B has a Device D to display the data. Each D is assumed to possess a key K_D.
- *Purchase:* B sends an index k for M to compute K_D. M returns B a unique decryption key K_{decB}. Applying K_D to $enc(I)$, D receives a copy of I with a unique watermark W_B.
- *Tracing:* Suppose B illegally redistributes his copy of I. He can be traced on the basis of the watermark W_B, which can be extracted only from the copies originating from his version of I.
- One encryption of I can be distributed to all buyers, but each decryption key is bound to a certain buyer with a certain device. The unique watermarking is forced to be done along the decryption.
- We also sketch a variant of the system for asymmetric fingerprinting with help of a trusted third party.

We assume the data in the scheme to be an image. The compression method is fixed to be a version of JPEG. Therefore, encryption and watermarking are performed on the discrete cosine transformed (DCT) coefficients of I.