

Are 128 bits long keys possible in Watermarking?

Patrick Bas^{1*} and Teddy Furon²

¹ CNRS-LAGIS, Ecole Centrale de Lille, France
`patrick.bas@ec-lille.fr`

² INRIA Research Centre Rennes Bretagne Atlantique, France
`teddy.furon@inria.fr`

The question raised in this poster is the following: is the key length of a watermarking system proportional to the key length of the seed used to generate the watermark? For example, if a watermark is generated from a binary sequence of size n , does it mean that the key length is 2^n ?

As we shall see in this poster, the answer is no! We will show how the key-length in Watermarking strongly relies on

- (1) the robustness of the watermarking scheme,
- (2) the embedding and decoding functions,
- (3) the observations available to the adversary.

The goal of this poster is to propose techniques to practically compute the key-length of a watermarking scheme. To do so we first compute the probability p that the adversary has access to the watermarking channel by picking a random key. This probability can be computed using three mathematical subsets: the embedding region, the decoding region and the region of equivalent keys, the latter being defined w.r.t both the embedding and decoding region. With this formulation, p is the probability that a random key belongs to the region of equivalent keys and the effective key length is given by

$$\ell = -\log_2 p.$$

We will illustrate in the poster how to practically compute ℓ on various popular watermarked schemes (Spread Spectrum, Improved Spread Spectrum, Distortion Compensated Quantization Index Modulation, Normalized Correlation) using different means such as mathematical derivations, Monte-Carlo simulations or geometrical estimation, and under different scenarios such as without any observation or taking into account a set of watermarked contents.

More informations about this work on <http://arxiv.org/abs/1202.3562>.

* P. Bas' work was partly founded by the French National Research Agency program referenced ANR-10-CORD-019 under the Estampille project.