Natural Watermarking: A Secure Spread Spectrum Technique for WOA

Patrick Bas[1,2] and François Cayre[2]

[1] CIS / Helsinki University of Technology
P.O. Box 5400
FI-02015 HUT FINLAND
[2] LIS/INPG
961, rue de la Houille Blanche BP 46
F-38042 St. Martin d'Hères Cedex, France

Abstract. This paper presents a spread spectrum (SS) watermarking technique that is secure against carriers estimation in a Watermark Only Attack framework. After reviewing the sufficient conditions to design secure algorithms for watermarking and steganography, we present a setup based on Blind Source Separation (BSS) theory to assess the lack of security of classical SS techniques such as classical SS or ISS. We motivate a new SS watermarking algorithm called Natural Watermarking (NW) where the estimation of the secret carriers is impossible and which achieves perfect secrecy thanks to unchanged Gaussian distributions of the secret carriers. The theoretical evaluation of the NW security is carried out and the case of multi-bit embedding is addressed. Finally, a robust extension of NW is presented and the properties of NW and Robust-NW are both practically verified.

1 Introduction

Robustness, *capacity* and *imperceptibility* have always been considered, since the very beginning of watermarking, as the main three constraints to respect in order to build a valuable watermarking scheme. Recently the watermarking community has thrown light on the problem of *security* which appears also to be a fundamental constraint to respect in order to guaranty the usability of a watermarking technology. Several authors [1][2][3] showed that some information about the secret key may leak from several observations of watermarked pieces of content. Using this information, it may be possible to estimate the secret key, and then to destroy the security of the considered scheme by removing, copying or altering the embedded messages. Several studies address also the security of practical watermarking techniques for digital images [4][5].

In this paper, we tackle the problem of security for the well-known class of spread spectrum (SS) watermarking schemes. In this case, the secret key which practically is the seed of a random generator, corresponds to the set of secret carriers that is used to convey the information. It is important to note that an attacker does not need the seed used to initialiaze the random number generator: the secret carriers are good enough to attack the watermark. We propose a

J. Camenisch et al. (Eds.): IH 2006, LNCS 4437, pp. 1–14, 2007.

watermarking scheme that is secure (e.g. it does not offer information leakage of the secret key) for the class of Watermark Only Attacks (WOA). This class of attacks, proposed by [1], considers an attack that is based on the observation of watermarked contents, watermarked with the same key but conveying different messages. We named the proposed scheme *natural spread spectrum watermarking* because embedding is achieved without altering the natural distribution of each secret carrier before and after embedding. As shown in the paper, this characteristic enables to achieve perfect secrecy. Moreover, when embedding several bits, we show that if each carrier is embedded in the contents with an amplitude following a Gaussian distribution, it is impossible to individually estimate the carriers.

The rest of the paper is divided into five sections. First, the security of classical SS techniques for WOA are analysed as a Blind Source Separation (BSS) problem: in section 2 we show that the characterisation of the distributions of each carrier for the observed contents enables to estimate the different carriers. Section 3 presents the constraints, principles and characteristics of Natural Watermarking (NW). The embedding, decoding and distortion related to NW are presented and the link with the Scalar Costa's Scheme, another scheme preserving perfect secrecy, is outlined. An extension of NW to increase the robustness is presented in section 4, the implications in term of security are also mentioned. Section 5 presents a comparison between the estimations of the secret carriers for different SS watermarking schemes including NW. We show that for NW it is impossible to estimate the carriers. For Robust-NW only the estimation of the watermark subspace is possible. Finally section 6 concludes this paper and presents open research lines for future works.

2 Assessing the Security of Spread-Spectrum Techniques Using BSS Techniques

2.1 Notations

Vectors are denoted in bold face ($\mathbf{v}$) and coefficients of vectors with parenthesis ($\mathbf{v}(i)$ is the coefficient number i in vector $\mathbf{v}$). Matrices are denoted in capital bold face and are generally composed of several realizations of vectors of the same name, column-wise: the columns of $\mathbf{V}$ are several realizations $\mathbf{v}_1 \dots \mathbf{v}_N$ of a "template" vector $\mathbf{v}$.

Let us denote $\mathbf{x}$ the host vector of N_v coefficients into which we want to hide a binary message vector $\mathbf{m}$ of N_c bits. The resulting watermarked vector is denoted $\mathbf{y}$. To this aim, we use $\mathbf{u}_i$ orthogonal carriers, $1 \leq i \leq N_c$. The decoded message is denoted $\hat{\mathbf{m}}$. It is to be estimated from $\mathbf{y}'$, a potentially degraded version of $\mathbf{y}$. Let us further denote $z_{\mathbf{v},\mathbf{u}_i}$ the correlation between a vector $\mathbf{v}$ and a carrier $\mathbf{u}_i$:

$$z_{\mathbf{v},\mathbf{u}_i} =< \mathbf{v}|\mathbf{u}_i >= \frac{1}{N_v}\sum_{k=1}^{N_v}\mathbf{v}(k)\mathbf{u}_i(k) \tag{1}$$