Optimization of Natural Watermarking Using Transportation Theory

Benjamin Mathon, Patrick Bas, François Cayre, Benoît Macq

Optimization of Natural Watermarking Using Transportation Theory

Benjamin Mathon
GIPSA-LAB, dept. IS – UMR CNRS 5216
961 rue de la Houille Blanche
Domaine universitaire – BP 46
F-38402 Saint-Martin d'Hères cedex
benjamin.mathon@gipsa-lab.grenoble-inp.fr

Patrick Bas
GIPSA-LAB, dept. IS – UMR CNRS 5216
961 rue de la Houille Blanche
Domaine universitaire – BP 46
F-38402 Saint-Martin d'Hères cedex
patrick.bas@gipsa-lab.grenoble-inp.fr

François Cayre
GIPSA-LAB, dept. IS – UMR CNRS 5216
961 rue de la Houille Blanche
Domaine universitaire – BP 46
F-38402 Saint-Martin d'Hères cedex
francois.cayre@gipsa-lab.grenoble-inp.fr

Benoît Macq
TELE
Bâtiment Stévin
Place du Levant 2
B-1348 Louvain-la-Neuve
benoit.macq@uclouvain.be

ABSTRACT

This article presents a new approach to use secure spread-spectrum watermarking in the Watermarked Only Attack (WOA) framework (the adversary owns several marked contents and wants to estimate the secret key). Because security of watermarking schemes relies on the distribution of marked contents in a private subspace, we use the transportation theory in order to derive a mapping that will minimize the global distortion of Natural Watermarking (NW) while keeping the same security level. Contrarily to another technique presented in [13], the embedding does not depend on computationally demanding pre-computed mapping. Moreover, we show that this method does not reduce the robustness of the classical NW scheme and enables to decrease the WCR by several dBs regarding former implementations. Tests are made on 2000 Gaussian signals.

Categories and Subject Descriptors

H.4.m [**Information Systems Applications**]: Miscellaneous; D.2.8 [**Software Engineering**]: Metrics—*complexity measures, performance measures*

General Terms

Algorithms, Security, Theory

Keywords

Natural Watermarking, Security, Transportation problem, Hungarian method

1. INTRODUCTION

The transition from analog to numerical data have permitted a best storage and indexation of multimedia contents. However, the expansion of internet and sharing networks have accelerated the piracy on intellectual property. Watermarking is a mean to solve this problem. It consists in embedding information into a digital content (audio, image or video). This mark can be used to link a content to its owner, to allow or not copies of the content or to trace any running copies on illegal sharing networks. It is obvious that this mark must be *imperceptible*, nobody shall recognize that the content is watermarked. Another constraint is the *robustness* of the scheme. In the case of copyright protection, the mark must resist common media processing (for example a JPEG compression on images). The last constraint is the *security* of the scheme which has received more and more attention in the watermarking community [9][7][5][3][2]. Security respects the Kerckhoffs' principle: a key is the only unknown parameter of the embedding scheme to an adversary. Security attacks relate to estimation of a part or all the secret key. According to the degree of estimation, the adversary can delete the mark, make it unreadable, or guess an important part of the secret message.

This article deals with the WOA (Watermarked Only Attack) framework: an adversary has access to several marked (with the same private key) contents. The secret key we use are codewords location in a secret subspace [15]. To embed a content, its projection in the secret subspace must be moved to a decoding region which corresponds to the right message. Security in watermarking is linked with the conditional distribution of the marked contents given the secret key [4]. We propose in this article an optimization of a secure spread-spectrum technique: Natural Watermarking (NW) [1] from

the distortion point of view. This new method uses results of transportation theory: it consists in computing the optimal way to match the distribution of host contents to a distribution of marked contents (given the secret key) by minimizing the global square euclidean distance. Section 2 recalls basics on spread-spectrum watermarking schemes and more particularly on the NW modulation. The link between security in the WOA framework and distributions of marked contents in the secret subspace is also presented. Section 3 details how we use results of transportation theory to minimize the distortion. Finally section 4 exhibits experiments on 2000 Gaussian signals to quantify the performance of this new method.

2. NATURAL WATERMARKING SPREAD-SPECTRUM

2.1 Notations

This section lists the different notations used in this article. Data are written in italic fonts, functions are noted in roman fonts and vectors and matrices are set in bold fonts. Vectors are written in small letters and matrices in capital ones. $\mathbf{x}(i)$ is the i-th component of a vector $\mathbf{x}$ and $(\mathbf{x}(0), \mathbf{x}(1), \mathbf{x}(2), \dots)$ is the content of a vector $\mathbf{x}$. P_δ and f_δ denote respectively the cumulative distribution function (cdf) and the probability density function (pdf) of a probability measure δ. $\sigma^2_{\mathbf{x}}$ denotes the variance of a signal $\mathbf{x}$ and $\langle .|. \rangle$ denotes the usual scalar product.

2.2 Spread-spectrum watermarking: assumptions and definitions

We consider a host Gaussian signal $\mathbf{x} \in \mathbb{R}^{N_v}$ and a binary message $\mathbf{m} \in \mathbb{F}_2^{N_c}$ we want to hide into $\mathbf{x}$. The secret key we use for the embedding are N_c carriers $\mathbf{u}_i$ which are generated thanks to a pseudo random number generator (PRNG) seeded with $K \in \mathbb{N}$. These carriers come as Gaussian vectors obtained with the PRNG and are further orthogonalized (using Gram-Schmidt procedure) with unit variance in order to provide a basis of the private subspace i.e. $\forall i \neq j$, $\langle \mathbf{u}_i | \mathbf{u}_j \rangle = 0$. The marked signal $\mathbf{y}$ is obtained by adding the host signal with a watermark signal $\mathbf{w}$ and it is constructed as follows:

$$\mathbf{y} = \mathbf{x} + \mathbf{w} = \mathbf{x} + \sum_{i=0}^{N_c-1} \mathrm{s}(\mathbf{m}(i), \mathbf{x}) \mathbf{u}_i, \tag{1}$$

where $\mathrm{s} : \mathbb{F}_2 \times \mathbb{R}^{N_v} \to \mathbb{R}$ is a modulation. As a convention, we set $\mathrm{s}(1, \mathbf{x}) < 0$ and $\mathrm{s}(0, \mathbf{x}) > 0$. The WCR (Watermark-to-Content Ratio) measures the distortion embedding power and is defined as:

$$WCR_{[dB]} = 10 \log_{10} \left(\frac{\sigma^2_{\mathbf{w}}}{\sigma^2_{\mathbf{x}}} \right). \tag{2}$$

Decoding is achieved by the normalized correlation z between each secret carrier and the marked signal:

$$\mathrm{z}_{\mathbf{y},\mathbf{u}_i} = \frac{1}{N_v} \langle \mathbf{y} | \mathbf{u}_i \rangle = \frac{1}{N_v} \sum_{j=0}^{Nv-1} \mathbf{y}(j) \mathbf{u}_i(j). \tag{3}$$

The i-th estimated bit equals 1 if $\mathrm{z}_{\mathbf{y},\mathbf{u}_i} < 0$ and 0 if $\mathrm{z}_{\mathbf{y},\mathbf{u}_i} > 0$. We also denote the normalized correlation vector $\mathbf{z}$ for a vector $\mathbf{y}$:

$$\mathbf{z}_{\mathbf{y}} = \left(\mathrm{z}_{\mathbf{y},\mathbf{u}_0}, \dots, \mathrm{z}_{\mathbf{y},\mathbf{u}_{N_c-1}} \right). \tag{4}$$

We measure the performance of decoding using Bit Error Rate (BER); if $\hat{\mathbf{m}}$ denotes the estimated message we have:

$$BER = \frac{\mathrm{card}\left(\{ i : \mathbf{m}(i) \neq \hat{\mathbf{m}}(i) \} \right)}{N_c}. \tag{5}$$

If we use the terminology of [4], we want to reach the "stego-security". It means that the distribution of the host contents and the marked contents is the same. We have $\mathrm{D}_{KL}(\mathbf{X} || \mathbf{Y}) = 0$, with D_{KL} denotes the Kullback-Leibler divergence.

2.3 Natural Watermarking

Natural Watermarking (NW) [1] is a spread-spectrum technique which enables to keep (possibly) scaled versions of the original $\mathrm{z}_{\mathbf{x},\mathbf{u}_i}$ distributions. This distribution is supposed to have circular pdf, possibly scaled by a factor $\eta \geq 1$ (in order to set distortion):

$$\mathrm{s}_{NW}(\mathbf{m}(i), \mathbf{x}) = \left(\eta (-1)^{\mathbf{m}(i)} \mathrm{sign}\left(\mathrm{z}_{\mathbf{x},\mathbf{u}_i} \right) - 1 \right) \mathrm{z}_{\mathbf{x},\mathbf{u}_i}, \tag{6}$$

with:

$$WCR = 10 \log_{10} \left(\frac{N_c (1 + \eta^2)}{N_v - 1} \right). \tag{7}$$

If $\eta = 1$, NW belongs to the stego-security class [4].

2.4 Carriers estimation and BSS problem

Our works focus on the WOA (Watermarked Only Attack) framework: the adversary has access to N_o contents (marked with different messages but with the same private key) and he/she knows the full source code of the watermarking algorithm (following Kerckhoffs' principle). The only parameter he/she does not know is the secret key (*i.e.* the carriers in spread-spectrum schemes). If we write the spread-spectrum formula considering the N_o contents, we have the matrix relation:

$$\mathbf{Y} = \mathbf{X} + \mathbf{W} = \mathbf{X} + \mathbf{U}\mathbf{S}, \tag{8}$$

with: $\mathbf{Y} \in \mathcal{M}_{N_v,N_o}(\mathbb{R})$ the watermarked signals,
$\mathbf{X} \in \mathcal{M}_{N_v,N_o}(\mathbb{R})$ the host signals, $\mathbf{W} \in \mathcal{M}_{N_v,N_o}(\mathbb{R})$ the watermark signals, $\mathbf{U} \in \mathcal{M}_{N_v,N_c}(\mathbb{R})$ the carriers,
$\mathbf{S} \in \mathcal{M}_{N_c,N_o}(\mathbb{R})$ the modulations of embedded messages. Security attacks in spread-spectrum schemes consist in obtaining as much information as possible about $\mathbf{U}$. The problem of disclosing $\mathbf{U}$ is known as a Blind Source Separation (BSS) problem. Principal Component Analysis (PCA) allows for an adversary to estimate the N_c-dimensional private subspace spanned by the carriers $\mathbf{U}$ (the private key), if the embedding alters the covariance matrix of the contents. PCA involves the calculation of the eigenvalues of the covariance matrix of $\mathbf{Y}$ (taken column-wise). PCA aims at finding the optimal linear transformation for keeping the subspace that has the largest variance (message embedding increases the variance of the signal in the directions of the carriers). This technique deals with subspace-security and it allows an adversary to tamper with the hidden messages of the contents. We use the "normalized chordal distance" [6][16] to measure the precision of the estimation of the subspace spanned by the carriers. If $\hat{\mathbf{U}}$ denotes the estimated carriers (after orthogonalization), the normalized chordal distance between $\mathbf{U}$ and $\hat{\mathbf{U}}$ is defined by:

$$\mathrm{d}_c = \frac{1}{\sqrt{N_c}} \left(\sum_{i=0}^{N_c-1} \sin^2(\theta_i) \right)^{1/2}, \tag{9}$$

where $\theta_0 \dots \theta_{N_c-1}$ denote the principal angles between $\mathbf{U}$ and $\hat{\mathbf{U}}$ [16]. The normalized chordal distance d_c equals 0 when the subspaces spanned by the both matrices are the same and equals 1 (its maximum) when the matrices are orthogonal.

2.5 Previous works: minimization distortion via a pre-computed mapping

In order to guarantee security, we revisit the embedding as a way to push the host content into the right decoding regions while fitting the appropriate statistical model. We aim at using a model-based embedding which can ensure the level of security we want while minimizing the global distortion.

In [13] we have proposed to use a matching $\mathrm{M} : \mathcal{X} \to \mathcal{Y}$ between N_m host correlation vectors $\mathcal{X}$ and N_m marked correlation vectors $\mathcal{Y}$ (over the secret carriers) with a minimal square euclidean distance on average. This triplet $(\mathcal{X}, \mathcal{Y}, \mathrm{M})$ is called an N_m-map. For each host signal $\mathbf{x}$ we want to watermark, we find the nearest neighbour of $\mathbf{z_x}$ in $\mathcal{X}$ (for example $\mathbf{z}_{\mathbf{x}_{i_0}}$) and we compute $\mathbf{z_y} = \mathrm{M}(\mathbf{z}_{\mathbf{x}_{i_0}})$, the correlations of the corresponding marked signal in $\mathcal{Y}$. Fig. 1 shows an example of this process. This optimal matching (from the distortion point of view) was to be found by the $O({N_m}^3)$ Hungarian algorithm [8]. The previous technique is more detailed in [13] and was performed successfully for secure watermarking of white Gaussian signals, this optimization was enabled to reduce the WCR distortion by at least 2.6 dB while keeping the same security level. However, this method exhibits the following disadvantages:

- the N_m-map (host and marked correlations and optimal matching) must be stored somewhere, it is very restrictive because it depends on the number of bits N_c the user wants to hide,
- the cubic complexity of the Hungarian method can be a real problem in a practical case when N_m grows up.

We propose in the next section a new method for matching host and marked correlations in an optimal way based on transportation theory. Contrarily to the Hungarian method, we consider the probability measures of the host and the marked correlations for the computation of an optimal matching.

3. THE TRANSPORTATION THEORY APPLIED TO SECURE SPREAD-SPECTRUM WATERMARKING

3.1 The Monge-Kantorovich transportation problem

The transportation theory can be considered as an engineering problem, defined by Monge [14] in 1781: we have piles of clay $\mathcal{X} \subset \mathbb{R}^{N_c}$ with distribution μ we want to move into holes $\mathcal{Y} \subset \mathbb{R}^{N_c}$ with distribution ν (μ and ν being probability measures). We consider a cost function c:

$$\begin{array}{rccc} \mathrm{c}: & \mathbb{R}^{N_c} \times \mathbb{R}^{N_c} & \to & [0, +\infty[\\ & (\mathbf{x}, \mathbf{y}) & \mapsto & \mathrm{c}(\mathbf{x}, \mathbf{y}), \end{array} \tag{10}$$

where $\mathrm{c}(\mathbf{x}, \mathbf{y}) = \mathrm{h}(\mathbf{x} - \mathbf{y})$ represents the cost for moving a unit mass of clay from $\mathbf{x}$ to $\mathbf{y}$. The goal is to find a bijection $\mathrm{T} : \mathcal{X} \to \mathcal{Y}$ with $\nu = \mathrm{T}_\sharp \mu = \mu \circ \mathrm{T}^{-1}$ (T pushes μ forward to ν) which minimizes the total cost to move the clay to the holes. Formally we search a minimizer T for:

$$\inf_{\mathrm{T}} \left\{ \int_{\mathbb{R}^{N_c}} \mathrm{c}\left(\mathbf{x}, \mathrm{T}\left(\mathbf{x}\right)\right) \mu(\mathbf{x}) \mathrm{d}\mathbf{x} \mid \nu = \mathrm{T}_\sharp \mu \right\}. \tag{11}$$

A solution T of this problem is called an optimal transport map. This problem is called the Monge-Kantorovitch problem because it was first formalized by Monge and principal contributions were done by Kantorovitch [10][11].

For $N_c = 1$, an optimal transport map T for a convex cost function h is given by:

$$\mathrm{T} = \mathrm{P}_\nu^{-1} \circ \mathrm{P}_\mu, \tag{12}$$

More generally, for any N_c, we have the following theorem [12]:

THEOREM 1. *Knott-Smith optimality criterion: if μ (resp. ν) represents the distribution of $\mathcal{X}$ (resp. $\mathcal{Y}$), sufficient conditions that* T *minimizes the Monge-Kantorovitch transportation problem with* $\mathrm{c}(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|^2$ *are that:*

i) $\mathrm{T}(\mathcal{X})$ *has distribution* ν*,*

ii) the Jacobian matrix $\mathbf{J}_\mathrm{T}(\mathbf{x})$ *of* T *is symmetric and positive semidefinite.*

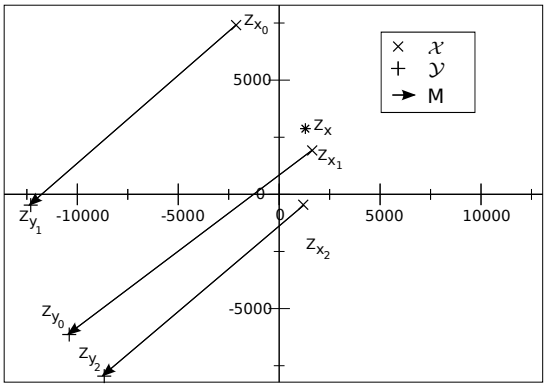

Figure 1: Hungarian based watermarking ($N_c = 2, N_m = 3$): the correlations of the signal we want to watermark is $\mathbf{z_x}$, its nearest neighbour is $\mathbf{z}_{\mathbf{x}_1}$. Thanks to the optimal matching (from the square euclidean distance point of view), we find $\mathbf{z_y} = \mathbf{z}_{\mathbf{y}_0}$, the correlations of the marked signal.

We have seen that security of spread-spectrum schemes relies on the distribution of the correlations z between the marked signals and the carriers. Moreover, we have the analytic expression of this distribution for NW [1], we are now able to use the previous theorem in order to match the host correlations to the marked correlations minimizing distortion constraint.

3.2 Application to Natural Watermarking

One property of NW is that the distribution of the correlations over the secret carriers before and after watermarking can be modeled by Gaussian distributions (host signals are Gaussian distributed). From [1], we have:

$$\mathrm{z}_{\mathbf{x},\mathbf{u}_i} \sim \mathcal{N}(0, \frac{\sigma_\mathbf{x}^2}{N_v}) = \mu. \tag{13}$$

We consider we embed the constant message $\mathbf{m} = (0, \ldots, 0)$ for each host content. We have:

$$\mathrm{z}_{\mathbf{y},\mathbf{u}_i} \sim \widetilde{\mathcal{N}}(0, \frac{\eta^2\sigma_{\mathbf{x}}^2}{N_v}) = \nu, \tag{14}$$

where, if $\delta = \mathcal{N}(0, \frac{\eta^2\sigma_{\mathbf{x}}^2}{N_v})$, the distribution $\nu = \widetilde{\mathcal{N}}(0, \frac{\eta^2\sigma_{\mathbf{x}}^2}{N_v})$ is given by its cdf:

$$\mathrm{P}_\nu(t) = \begin{cases} 0 \text{ if } t < 0, \\ 2\mathrm{P}_\delta(t) - 1 \text{ if } t \geq 0. \end{cases} \tag{15}$$

Then an application of the previous results about transportation theory is relevant, we want to find an optimal transport map T_0 which matches the distribution of $\mathrm{z}_{\mathbf{x},\mathbf{u}_i}$ to the distribution of $\mathrm{z}_{\mathbf{y},\mathbf{u}_i}$. The strategy is to use an optimal transport map for each dimension of the N_c dimensional private subspace thanks to Eq. 12. The computation of the optimal transport map T_0 for embedding the message $(0, \ldots, 0)$ is given by:

$$\begin{array}{rccc} \mathrm{T}_0: & \mathbb{R}^{N_c} & \rightarrow & \mathbb{R}^{N_c} \\ & \mathbf{z_x} & \mapsto & \mathbf{z_y} = \mathrm{T}_0(\mathbf{z_x}), \end{array} \tag{16}$$

where

$$\mathrm{T}_0 \begin{pmatrix} \mathbf{z_x}(0) \\ \vdots \\ \mathbf{z_x}(N_c - 1) \end{pmatrix} = \begin{pmatrix} \mathrm{P}_\nu^{-1} \circ \mathrm{P}_\mu(\mathbf{z_x}(0)) \\ \vdots \\ \mathrm{P}_\nu^{-1} \circ \mathrm{P}_\mu(\mathbf{z_x}(N_c - 1)) \end{pmatrix}. \tag{17}$$

We have:

$$\mathrm{P}_\mu(t) = \frac{1}{2}\left(1 + \mathrm{erf}\left(\frac{t\sqrt{N_v}}{\sigma_{\mathbf{x}}\sqrt{2}}\right)\right), \tag{18}$$

and

$$\mathrm{P}_\nu^{-1}(t) = \mathrm{P}_\delta^{-1}\left(\frac{t}{2} + \frac{1}{2}\right) = \frac{\eta\sigma_{\mathbf{x}}\sqrt{2}}{\sqrt{N_v}}\mathrm{erf}^{-1}\left(t - \frac{1}{2}\right). \tag{19}$$

The constructed function T_0 is an optimal transport map because it respects the conditions of Th. 1 (the proof is given in appendix). Thanks to the property of symmetry of spread-spectrum, to embed others message than $(0, \ldots, 0)$, sign changes must be made on the coefficients of $\mathbf{z_x}$ in the indices that have undergone symmetries. Afterwards, inverse symmetry must be performed after watermarking in order to embed the correct message $\mathbf{m}$. Formally, the corresponding optimal transport map $\mathrm{T}_\mathbf{m}$ for any message $\mathbf{m}$ is given by:

$$\mathrm{T}_\mathbf{m}(\mathbf{z_x}) = \mathbf{R}^{-1}(\mathrm{T}_0(\mathbf{R}\mathbf{z_x})), \tag{20}$$

with:

$$\mathbf{R} \in \mathcal{M}_{N_c,N_c}(\mathbb{R}), \mathbf{R}(i,j) = \begin{cases} 0 \text{ if } i \neq j, \\ (-1)^{\mathbf{m}(i)} \text{ if } i = j. \end{cases} \tag{21}$$

We can now define a new spread-spectrum technique based on transportation theory, namely Transportation Natural Watermarking (TNW), the corresponding modulation is given by:

$$\mathrm{s}_{TNW}(\mathbf{m}(i), \mathbf{x}) = \mathrm{T}_\mathbf{m}(\mathbf{z}_{\mathbf{x},\mathbf{u}_i}) - \mathbf{z}_{\mathbf{x},\mathbf{u}_i}. \tag{22}$$

One can see that we have considerably reduced the complexity of the problem of optimal matching: instead of using $O(N_m^3)$ algorithm, the matching is directly given by Eq. 20. Fig. 2 shows the modulations s_{NW} and s_{TNW} functions of $\mathrm{z}_{\mathbf{x},\mathbf{u}_0}$ $(N_c = 1, N_v = 512, \eta = 2, \sigma_{\mathbf{x}}^2 = 1)$. Contrarily to NW, the modulation of TNW is not piecewise linear.

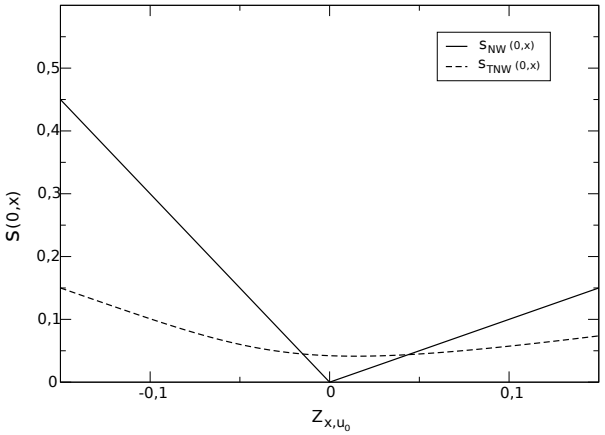

Figure 2: Modulations s_{NW} and s_{TNW} functions of $\mathrm{z}_{\mathbf{x},\mathbf{u}_0}$ $(N_c = 1, N_v = 512, \eta = 2, \sigma_{\mathbf{x}}^2 = 1)$. Contrarily to NW, the modulation of TNW is not piecewise linear.

4. EXPERIMENTS

In this section we generate several Gaussian signals and we watermark them with independent messages by using classical Natural Watermarking (NW), Hungarian Watermarking (HNW, see Sec. 2.5) and Transportation Natural Watermarking (TNW). On the one hand we want to show that TNW does not modify the security and the robustness of the classical NW. On the other hand, one shall keep in mind that we are targeting the same security level as with HNW but with significantly lower algorithmic complexity.

4.1 Assessments

We generate $N_o = 2000$ $\mathcal{N}(0,1)$ Gaussian signals of $N_v = 512$ components. For HNW, we use an 10000-map constructed with different standardized Gaussian signals. We hide $N_c = 10$ bits into each signal. We model robustness attacks by adding a Gaussian noise $\mathbf{n}$ to $\mathbf{y}$. Attack strength is assessed by means of the $WCNR$ (Watermarked Content-to-Noise Ratio):

$$WCNR_{[dB]} = 10\log_{10}\left(\frac{\sigma_{\mathbf{y}}^2}{\sigma_{\mathbf{n}}^2}\right). \tag{23}$$

4.2 Security

4.2.1 Distribution of host and marked signals

Fig. 3 shows the distribution of the correlations of the host, NW and TNW signals over the two secret carriers for $\eta = 1$. Obviously, distributions of NW and TNW are identical to that of the host distribution. Therefore, we conclude that TNW does not impair the security of the scheme.

4.2.2 Principal Component Analysis

Principal Component Analysis can be used to estimate the subspace defined by the secret carriers. If an attacker can construct a basis of this subspace, he can make embedded messages unreadable (by nullifying the projections on the estimated subspace). More precisely, he recovers an orthogonal base with a PCA: $\hat{\mathbf{U}}$ of the subspace defined by the carriers $\mathbf{U}$. This estimation depends on the strength of the embedding [16]. Fig. 4 shows the normalized chordal

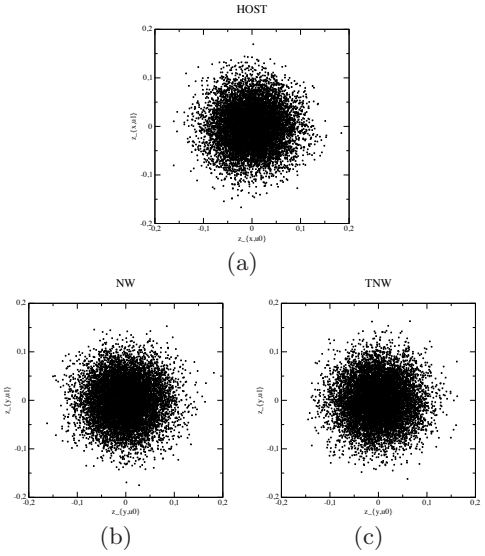

Figure 3: Normalized correlations of host (a), NW (b) and TNW (c) over the first two secret carriers, $N_o = 2000$ observations.

distance between the secret and the estimated carriers by PCA functions of the parameter η by using NW and TNW. As can be seen, the estimation of the carriers subspace for TNW closely follows that of NW.

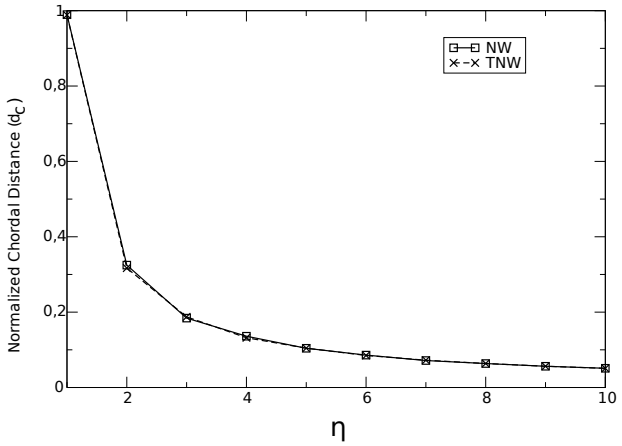

Figure 4: Normalized chordal distance between the secret and the estimated carriers by PCA functions of the parameter η for NW and TNW. As can be seen, the estimation of the carriers subspace for TNW closely follows that of NW, $N_c = 10$.

4.3 Robustness

Fig. 5 depicts the BER (expectation on the 2000 marked signals) w.r.t. the $WCNR$. For two values of $\eta = 1, 2$ we can see that the robustness against AWGN attack is the same for NW and TNW.

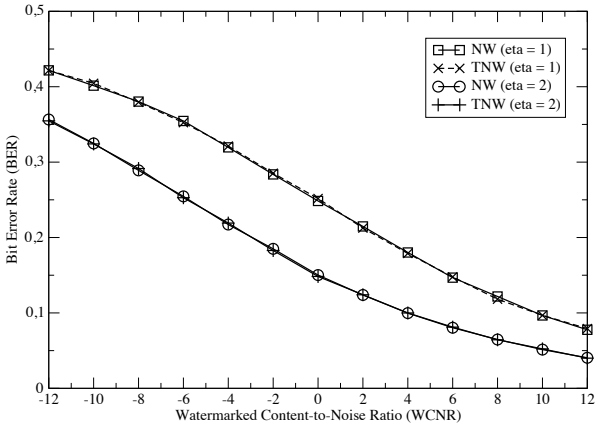

Figure 5: BER w.r.t. $WCNR_{[dB]}$ for NW and TNW with $\eta = 1, 2$, $N_c = 10$.

	$\eta = 1$	$\eta = 2$
NW	-14.09	-10.06
HNW	-16.74	-12.29
TNW	-17.85	-12.79

Table 1: WCR distortion for NW, HNW and TNW for $\eta = 1, 2$, $N_c = 10$.

4.4 Distortion

Tab. 1 quantify the distortion (by means of the WCR) of NW, HNW and TNW for two values of $\eta = 1, 2$). As expected, using an optimal transport map enables to reduce the original NW distortion by 3.76 dB when $\eta = 1$. Fig. 6 shows the WCR distortion of HNW and TNW functions of N_c. As can be seen the improvement regarding WCR distortion is better when we use TNW instead of HNW when N_c grows up. The reason is that even if the Hungarian method is optimal to find the matching which minimizes the total cost; HNW computes the embedding by looking for the nearest point registered in the pre-computed optimal mapping; the square euclidean distance between one point and the closest point recorded in the host correlations of the used N_m-map grows with respect to the dimension (N_c).

5. CONCLUSIONS

In this article we have developed an improvement of natural watermarking: transportation theory has been used in order to derive an optimal embedding formula for embedding N_c bits. This new mapping enables us to minimize the global distortion by keeping the same security and the same robustness as the classical scheme. Moreover this embedding method is better (regarding the distortion) and faster (regarding the complexity) than the Hungarian-based watermarking technique proposed in [13].

6. ACKNOWLEDGMENTS

Benjamin Mathon, Francois Cayre and Patrick Bas are partly supported by the National French projects ANR-06-SETIN-009 Nebbiano, ANR-05-RIAM-O1903 Estivale and ARA TSAR. Moreover Benjamin Mathon is partly supported by BCRYPT project, a Belgian Interuniversity Attraction

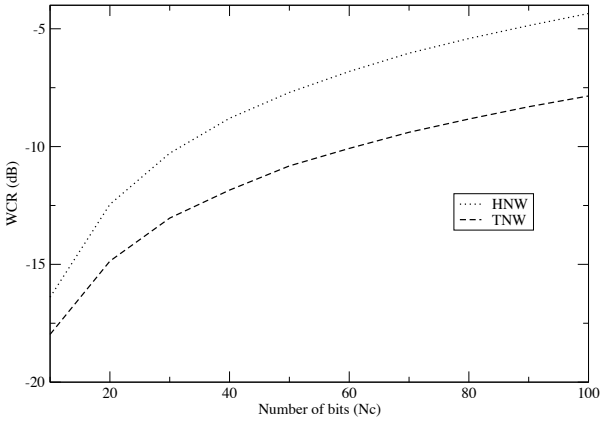

Figure 6: WCR w.r.t. N_c for HNW and TNW modulation. As can be seen, the improvement of distortion is better for TNW than HNW when N_c grows up. For HNW, we lost optimality of Hungarian method by selecting nearest neighbours of our host correlations in the N_m-map, $\eta = 1$.

Pole IAP-VI fund programme. We acknowledge fruitful discussions with Cedric Villani (Ecole Normale Superieure de Lyon) on optimal transportation theory (particularly about the Knott-Smith criterion applied with N_c 1-dimensional transport maps).

7. REFERENCES

[1] P. Bas and F. Cayre. Natural watermarking: a secure spread spectrum technique for woa. In *Proc. Information Hiding*, Alexandria, VA, July 2006.

[2] P. Bas and G. J. Doërr. Practical security analysis of dirty paper trellis watermarking. In *Proc. Information Hiding*, pages 174–188, 2007.

[3] P. Bas and J. Hurri. Vulnerability of dm watermarking of non-iid host signals to attacks utilising the statistics of independent components. In *Information Security, IEE Proceedings*, volume 153, pages 127–139, Sept. 2006.

[4] F. Cayre and P. Bas. Kerckhoffs-based embedding security classes for woa data hiding. *IEEE Trans. Inf. For. Sec.*, 3(1):1–15, Mar. 2008.

[5] F. Cayre, T. Furon, and C. Fontaine. Watermarking security: Theory and practice. *IEEE Trans. Sig. Proc.*, 53(10):3976–3987, Oct. 2005.

[6] J. H. Conway, R. H. Hardin, and N. J. A. Sloane. Packing lines, planes, etc.: packings in grassmanian spaces. In *Experimental Mathematics*, volume 5(2), pages 139–159, 1996.

[7] T. Furon, J. Oostven, and J. V. Bruggen. Security analysis. *European Project IST-1999-10987 CERTIMARK, Deliverable D.5.5*, 2002.

[8] H. W. Kuhn. The Hungarian method of solving the assignment problem. *Naval Res. Logistics Quart.*, 2:83–97, 1955.

[9] T. Kalker. Considerations on watermarking security. *Proc. MMSP*, pages 201–206, Oct. 2001.

[10] L. Kantorovitch. On the translocation of masses. *C.R. (Doklady) Acad. Sci. URSS (N.S.)*, 37:199–201, 1942.

[11] L. Kantorovitch. On a problem of monge (in russian). *Uspekhi Math. Nauk.*, 3:225–226, 1948.

[12] M. Knott and C. S. Smith. On the optimal mapping of distributions. *Journal of Optimization Theory and Applications*, 43:39–49, May 1984.

[13] B. Mathon, P. Bas, F. Cayre, and F. Pérez-González. Distortion optimization of model-based secure embedding schemes for data-hiding. In *Proc. Information Hiding*, Santa-Barbara, CA, USA, May 2008.

[14] G. Monge. Mémoire sur la théorie des déblais et des remblais. *Histoire de l'Académie Royale des Sciences de Paris, avec les Mémoires de Mathématique et de Physique pour la même année*, pages 666–704, 1781.

[15] P. Moulin and R. Koetter. Data-hiding codes. *Proceedings of the IEEE*, 93(12):2083–2126, Dec. 2005.

[16] L. Pérez-Freire and F. Pérez-González. Spread-spectrum watermarking security. *IEEE Trans. Inf. Forensics Security*, 4(1):2–24, March 2009.

APPENDIX

In this appendix, we consider $\mu = \mathcal{N}(0, \frac{\sigma_{\mathbf{x}}^2}{N_v})$ and $\nu = \widetilde{\mathcal{N}}(0, \frac{\eta^2\sigma_{\mathbf{x}}^2}{N_v})$.

Optimality of the transport map constructed in Eq. 17.

We want to show that

$$\mathrm{T}_0 \begin{pmatrix} \mathbf{x}(0) \\ \vdots \\ \mathbf{x}(n-1) \end{pmatrix} = \begin{pmatrix} \mathrm{P}_\nu^{-1} \circ \mathrm{P}_\mu(\mathbf{x}(0)) \\ \vdots \\ \mathrm{P}_\nu^{-1} \circ \mathrm{P}_\mu(\mathbf{x}(n-1)) \end{pmatrix}, \qquad (24)$$

is an optimal transport map by applying the Th. 1. The condition *i)* is verified because a signal $\mathbf{x}$ is Gaussian iff each coordinate $\mathbf{x}(i)$ is Gaussian (we use the separability of the multidimensional Gaussian distribution). For the condition *ii)*, we introduce the Jacobian matrix of T_0:

$$\mathbf{J}_{\mathrm{T}_0}(\mathbf{x}(0)\dots\mathbf{x}(n-1))$$

$$= \begin{pmatrix} \frac{\partial\left(\mathrm{P}_\nu^{-1}\circ\mathrm{P}_\mu(\mathbf{x}(0))\right)}{\partial\mathbf{x}(0)} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \frac{\partial\left(\mathrm{P}_\nu^{-1}\circ\mathrm{P}_\mu(\mathbf{x}(n-1))\right)}{\partial\mathbf{x}(n-1)} \end{pmatrix}. \qquad (25)$$

Show that this matrix is symmetric and positive semidefinite. The symmetry is trivial by construction of the transport map T_0. A matrix $\mathbf{J}$ is positive semidefinite iff the eigenvalues of $\mathbf{J}$ are positive or null. So we must prove that $\left(\mathrm{P}_\nu^{-1} \circ \mathrm{P}_\mu\right)'(t) \geq 0$. We have:

$$\left(\mathrm{P}_\nu^{-1} \circ \mathrm{P}_\mu\right)'(t) = \left(\mathrm{P}_\nu^{-1}\right)'(\mathrm{P}_\mu(t))\,\mathrm{f}_\mu(t). \qquad (26)$$

$\mathrm{f}_\mu(t)$ is positive (pdf) and $\mathrm{P}_\nu^{-1}(t)$ is a non-decreasing function so $\left(\mathrm{P}_\nu^{-1}\right)'(t) \geq 0$. Then $\left(\mathrm{P}_\nu^{-1} \circ \mathrm{P}_\mu\right)'(t) \geq 0$ and the Jacobian matrix of T_0 is positive semidefinite. The conditions *i)* and *ii)* of the Th. 1 are verified: T_0 is an optimal transport map.