14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, September 4-8, 2006, copyright by EURASIP

SUBSTITUTIVE WATERMARKING ALGORITHMS BASED ON INTERPOLATION

Vincent Martin, Marie Chabert and Bernard Lacaze

ENSEEIHT/IRIT, National Polytechnic Institute of Toulouse
2 Rue Camichel, BP 7122, 31071 Toulouse Cedex 7, France
vincent.martin, marie.chabert, bernard.lacaze@enseeiht.fr

ABSTRACT

Imperceptibility is a concern in all watermarking techniques. Consequently, most algorithms use a psychovisual mask. Interpolation techniques offer interesting perceptual properties and have been abundantly studied in image processing. This article aims at defining a class of watermarking algorithms that take advantage of this property. This class generalizes previous work on bilinear interpolation. A theoretical performance study is proposed. Moreover, optimal decoding as well as objective imperceptibility and security measures are provided for the whole class. An application to spline interpolation is studied.

1. INTRODUCTION

Digital watermarking consists in embedding data at the content-level of digital media under the constraints of imperceptibility, security and robustness to attacks. Its applications range from digital rights management to integrity protection. Watermark algorithms are either based on additive embedding, substitution by a codebook element or constraint imposition on the watermarked data. In the latter case, the embedding is substitutive and decoding consists in determining whether the received signal meets some predefined constraints. For instance, the salient points of an image can be warped to belong to a dense collection of lines [1].

In Direct Sequence (DS) Spread Spectrum watermarking, the additive mark is the secret message modulated by a pseudo-noise. The message can be detected later by correlation with this pseudo-noise. Classical spread spectrum methods are subject to host interference. Extensions provide improved performance [2] thanks to Wiener prefiltering at the detector or optimal decoding for a given host image statistical model. Informed watermarking provides better performance by using at the embedding knowledge upon both the host image and the detection technique [3]. Linear Improved Spread Spectrum (LISS) [4] uses a new modulation technique that removes the signal as source of interference. Recent advances focus on random binning inspired from Costa's work in information theory [5]. In practice, a reasonably large but suboptimal binning codebook can be constructed using quantization. In the popular Spread Transform Scalar Costa Scheme (ST-SCS) [6], robustness to noise is improved by quantizing the projection of the data onto a pseudo-random vector.

Interpolation refers to the problem of constructing a continuously defined function from given discrete data. Image interpolation techniques include, in range of increasing performance, nearest-neighbor, bilinear [7], cubic-spline and B-spline [8] interpolation. A comparison between the different interpolation techniques in terms of approximation error and execution time is provided in [7].

In watermarking schemes, interpolation acts usually as a perturbation. Interpolation is involved in most geometrical attacks such as rotation. Indeed, such attacks result in the distortion of the original data coordinates. The interpolation is then used to derive the pixel values on the original discrete grid. Interpolation is also necessary to perform watermarking in a continuous transformed domain such as the Fourier-Mellin domain [9]. More specific algorithms also refer to interpolation. A hierarchical and deterministic secret sharing procedure built on polynomial interpolation is used to construct the mark provided to an additive watermarking scheme in [10]. 3D objects are represented by non-uniform rational B-Splines that provide an insertion domain for substitutive algorithms [11]. In [12], a bilinear interpolation-based watermarking algorithm W-interp was proposed.

Let $M = [m(l)]_{l\in\{1,\dots,L\}}$ denote the binary antipodal message of size L. L is called the payload. Let I denote the original image, W the mark and I_W the watermarked image. These quantities are handled as matrices as follows:

$$I = [i(n_1, n_2)]_{n_1\in\{1,\dots,N_1\},n_2\in\{1,\dots,N_2\}}$$

The watermarked image $I_W = I + W$ is transmitted and possibly attacked, leading to the image I'_W. Under the assumption of mild attacks, the noise model amounts to the widespread AWGN channel model:

$$I'_W = I_W + B \text{ where } b(n_1, n_2) \sim \mathcal{N}(0, \sigma_B^2)$$

The simulations provide the averaged performance on the test image set composed of Lena, Baboon, Fishingboat, Peppers and Pentagon.
Let σ_W^2 denote the variance of W. For a given I, let define the document to watermark ratio (DWR), the watermark to noise ratio (WNR) and the Document to Noise Ratio (DNR):

$$\text{DWR} = \frac{\sigma_I^2}{\sigma_W^2},\ \text{WNR} = \frac{\sigma_W^2}{\sigma_B^2},\ \text{DNR} = \frac{\sigma_I^2}{\sigma_B^2}$$

DWR (resp. DNR) measures W (resp. B) imperceptibility with respect to the host image. WNR measures transmission noise and attack influence.

This paper is organized as follows: Section 2 generalizes the approach of [12] to the class W-subst of substitutive watermarking algorithms based on interpolation. Among this class, Section 3 develops the example of W-spline, based on spline interpolation, that offers better perceptual properties. An objective perceptual quality metric is introduced to assess the approach efficiency. In [12], a Gaussian approximation of the interpolation error was used to study the performance in the context of additive white Gaussian noise (AWGN) attack. Section 4 derives an optimum decoder based on the generalized Gaussian model. Section 5 provides an experimental study of the robustness of W-spline to various attacks. Section 6 proposes a new practical algorithm for a security attack specifically tailored to the proposed class of algorithms.

2. A CLASS OF WATERMARKING ALGORITHMS BASED ON INTERPOLATION

A family of substitutive, known-host state [2], informed watermarking schemes is presented in Fig.1.

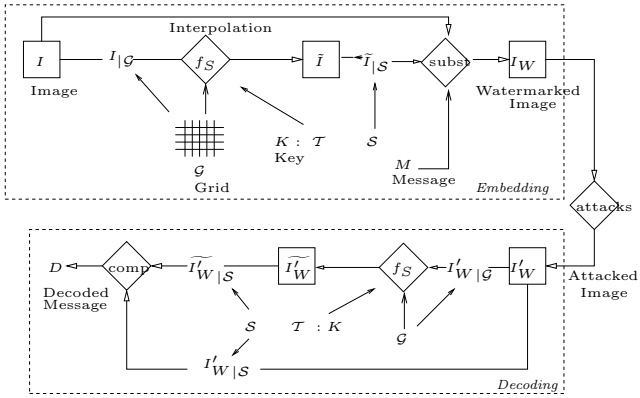

Figure 1: Class of watermarking schemes W-subst

Let select in I two non-overlapping sets of samples, of respective coordinates $\mathcal{G}$ and $\mathcal{S}$. $\mathcal{G}$ denotes the grid. The watermark is embedded in $\mathcal{S} \subset [|1, N_1|] \times [|1, N_2|] \setminus \mathcal{G}$. Let $N_{\mathcal{S}}$ denote the cardinal of $\mathcal{S}$ and $P_{\mathcal{S}} = N_{\mathcal{S}}/L$ the redundancy. $\mathcal{S}$ is divided into L non-overlapping, randomly constructed sets of size $P_{\mathcal{S}}$: $\mathcal{S} = \mathcal{S}_1 \cup ... \cup \mathcal{S}_L$, $\mathcal{S}_i \cap \mathcal{S}_j = \emptyset \quad \forall i \neq j$. $\mathcal{S}_k$ is associated to the bit $m(k)$ of the message. Let $\mathcal{T}$ denote a set of random parameters guaranteeing the security of the algorithm. The secret key K consists of the watermark coordinates $\mathcal{S}$ and the associated security parameters ($K = \{\mathcal{S}, \mathcal{T}\}$). Let $I_{|\mathcal{G}}$ denote the restriction of I to $\mathcal{G}$. Finally, let f_S denote a function

$$f_S(I_{|\mathcal{G}}; \mathcal{G}, \mathcal{T}) = \widetilde{I}$$

producing an image $\widetilde{I}$ such that $\widetilde{I}_{|\mathcal{G}} = I_{|\mathcal{G}}$ and that I and $\widetilde{I}$ are perceptually close. Note that $I_{|\mathcal{S}}$ is not provided to f_S. f_S estimates some missing samples provided a subset of I. Hence, f_S can be considered as an interpolating function.

At the embedding, the values $I_{|\mathcal{S}_l}$ of the pixels in $\mathcal{S}_l$ are substituted by their counterpart $\widetilde{I}_{|\mathcal{S}_l}$ provided by f_S if $m(l) = 1$. If $m(l) = -1$, $I_{W|\mathcal{S}_l} = I_{|\mathcal{S}_l}$.

The decoding compares $I'_{W|\mathcal{S}}$ and $\widetilde{I'_{W|\mathcal{S}}}$. Let denote $R = \widetilde{I'_{W|\mathcal{S}}} - I'_{W|\mathcal{S}}$. For a given bit $m(l)$, the mean square error $\rho^2(l) = \frac{1}{|\mathcal{S}_l|} \sum_{(n_1,n_2)\in\mathcal{S}_l} r(n_1, n_2)^2$ is compared to an image-dependent threshold ν. If $\rho^2(l) < \nu$, the decision is $d(l) = +1$, else $d(l) = -1$. ν can be chosen empirically as the mean of the decoding results: $\nu = \frac{1}{L}\sum_{l=1}^{L} \rho^2(l)$. However, a theoretical threshold is derived in section 4 under appropriate hypotheses about the interpolation error distribution.

This framework provides a blind watermarking scheme, since I is not used at the decoding. It is substitutive in the sense of constraints imposition. It is also a host-rejecting watermarking method since in the absence of any attack, perfect decoding, thus a rate $N_{\mathcal{S}}/N_1N_2$, can be achieved. It is an informed coding method since I is used during the generation of W. An informed embedding extension of W-subst should use knowledge about the detection technique during the embedding [3].

Note that f_S will be often a linear function of the elements of $\mathcal{G}$ and will act as a local filter. The condition of imperceptibility imposes that W modifies the high and middle frequencies of I. Under this assumption, f_S behaves like a low pass filter, and the watermark consists of high pass coefficients of I.

The algorithm is characterized by the choice of a lowpass function f_S, a grid $\mathcal{G}$, the positions $\mathcal{S}$, outside the grid, of $N_{\mathcal{S}}$ watermarked pixels, and the security parameters $\mathcal{T}$.

3. PARTICULAR CASE OF SPLINE INTERPOLATION

The framework presented in Section 2 generalizes the watermarking algorithm proposed in [12]. In the particular case studied in [12], f_S was derived from bilinear interpolation on a given grid $\mathcal{G}$. In this paper, the case of spline interpolation is addressed.

3.1 Spline interpolation

Suppose that a continuous signal $g(x)$ must be interpolated from given discrete, regularly spaced values $\{g(k)\}_{k\in\mathbb{Z}}$. Most techniques, such as linear interpolation, use convolution by finite-support synthesis functions. In theory, perfect reconstruction of band-limited functions could be obtained by cardinal sine interpolation. However, interpolants of infinite support cannot be used in practice. B-splines allow to implement interpolation by an infinite-support interpolant, called cardinal spline, with a reasonable computational cost [8]. They offer the best approximation performance for the least complexity [7]. Let denote η^3 the cardinal cubic spline (cf Fig. 2). Then the interpolation result $g_{\text{spline}}(x)$ is

$$g_{\text{spline}}(x) = \sum_{k=-\infty}^{+\infty} g(k)\eta^3(x-k) \qquad (1)$$

B-splines are piecewise polynomial functions whose pieces are smoothly connected together. Let denote $\beta^3(x)$ the B-spline synthesis function of degree 3 (cf Fig. 3). Let denote $\overline{x}$ the integer part of x. Then (1) is equivalent to

$$g_{\text{spline}}(x) = \sum_{k=\overline{x-2}}^{\overline{x-2}+3} c(k)\beta^3(x-k)$$

where $c(k)$ is computed from $\{g(k)\}_{k\in\mathbb{Z}}$ and the sampling of $\beta^3(x)$ by computationally efficient filtering. Moreover, a two-dimensional extension is possible [8] :

$$i_{\text{spline}}(x,y) = \sum_{k=\overline{x-2}}^{\overline{x-2}+3} \sum_{k=\overline{y-2}}^{\overline{y-2}+3} c(k,l)\beta^3(x-k)\beta^3(y-l)$$

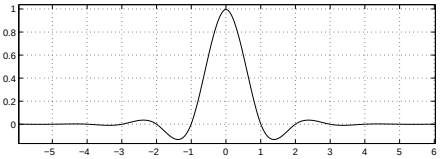

Figure 2: Cardinal B-spline of 3rd degree

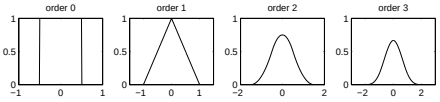

Figure 3: B-spline synthesis functions of degree 0,1,2,3

3.2 Watermarking algorithm W-spline

Like in [12], we propose to use the chessboard-like grid $\mathcal{G} = (2\mathbb{Z}+1) \times 2\mathbb{Z} \cup 2\mathbb{Z} \times (2\mathbb{Z}+1)$, which allows for a computationally efficient implementation.

If $(n_1, n_2) \in \mathcal{S}_l$ with $m(l) = 1$, $i(n_1, n_2)$ is replaced by :

$$\widetilde{i}(n_1, n_2) = i_{\text{spline}}(n_1 + \tau_x(n_1, n_2), n_2 + \tau_y(n_1, n_2))$$

where the elements of $\mathcal{T} = \{\tau_x(n_1, n_2), \tau_y(n_1, n_2)\}_{(n_1,n_2)\in\mathcal{S}}$ are independent random variables uniformly distributed over $]-\frac{1}{2}, +\frac{1}{2}[$. These random shifts are introduced to improve the security level of the algorithm (cf Section 6).

3.3 Distortion evaluation

Imperceptibility of a watermark is empirically observed for DWR> 38 dB. Let ϵ_I denote the interpolation error. In our case, DWR $= 2\sigma_I^2 N/\sigma_{\epsilon_I}^2 N_{\mathcal{S}}$. For a given DWR, one can find $N_{\mathcal{S}}$, the maximum number of pixels to be substituted. $N_{\mathcal{S}}$ depends on I and the interpolation technique. Psychovisual studies have shown that modifications in regions of high local variance is less perceptible, allowing to design perceptual masks for the classical DS technique [13]. Similarly, the use of interpolation guarantees that modifications occur mainly in these regions. Moreover, the resulting watermark is highly correlated to the host image.

Objective metrics can assess the perceptual image quality. The Structural Similarity metric (SSIM) [14] measures the degradation of structural information, ranging from 0 (no similarity) to 1 (no distortion). Experimental results (cf Tab.1) show that according to this criterion, W-spline outperforms the classical DS technique combined with the Noise Visibility Function (NVF) [13] mask or combined with embedding in the DCT domain with an appropriate psychovisual mask [2].

DS	0.9827	DS+NVF	0.9897
DS+DCT	0.9897	W-spline	0.9929
W-spline w/o $\mathcal{T}$	0.9964	W-interp w/o $\mathcal{T}$	0.9961

Table 1: Comparison of SSIM quality metric, DWR=38 dB

4. OPTIMAL DECODING

This section studies the theoretical performance of W-spline in the presence of AWGN attack. When the attack parameter σ_B^2 is known, a theoretical detection threshold is derived and performs significantly better than the empirical threshold. When σ_B^2 is unknown, the theoretical performance can as well be derived and consistency with simulations is demonstrated.

4.1 Interpolation error distribution

The histogram of the interpolation error ϵ_I for a given image I shows that the generalized Gaussian density (GGD) is an appropriate distribution model (Fig. 4). This family of pdfs, also called generalized Laplacian, is defined as:

$$f_x(x) = Ae^{-|\alpha x|^c} \ , x \in \mathbb{R}$$

A and α are function of the standard deviation σ and a shape parameter c :

$$\alpha = \frac{1}{\sigma}\left(\frac{\Gamma(3/c)}{\Gamma(1/c)}\right)^{1/2} \qquad A = \frac{\alpha c}{2\Gamma(1/c)} \ .$$

where Γ denotes the gamma function. $c = 2$ corresponds to the Gaussian density function and $c = 1$ to the Laplacian. Algorithms are available for estimating σ and c from the histogram [2]. On the test set, c varies from $c = 0.81$ to $c = 1.21$ for W-spline.

The GGD has been used in various empirical image studies in the spatial domain. The difference between the luminance of two adjacent pixels of a natural image follows a GGD [15]. Moreover, natural image are shown to be differencially Laplacian [16], i.e. a linear combination of adjacent pixels in a $k \times k$ window has a Laplacian density, provided that the sum of the coefficients is null. The bilinear interpolation functions meet this condition, as well as spline interpolation if it is approximated to a finite support. Note that a large family of lowpass functions f_S can also meet this condition. The following performance study is still valid for the corresponding watermarking algorithms.

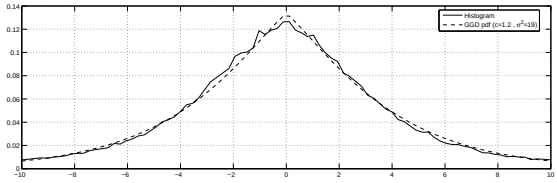

Figure 4: Histogram of the interp. error, Lena

4.2 AWGN influence

Let $r(n_1, n_2) = \epsilon_{I_W}(n_1, n_2) + \epsilon_B(n_1, n_2)$, ϵ_{I_W} and ϵ_B being the respective contributions to R of the image and the noise. The variance of $\epsilon_B(n_1, n_2)$ can be expressed as $(1 + k_{\mathcal{T}})\sigma_B^2$, where the constant $k_{\mathcal{T}}$ depends on $\mathcal{T}$:

$$k_{\mathcal{T}} = \sum_{k=-\infty}^{+\infty}\sum_{l=-\infty}^{+\infty} \mathrm{E}[(\eta^3(\tau_x - k)\eta^3(\tau_y - l))^2]$$

It can be computed numerically as $k_{\mathcal{T}} \simeq 0.58$ without shifts, $k_{\mathcal{T}} \simeq 0.77$ with uniform distribution over $]-\frac{1}{2}, +\frac{1}{2}[$. In comparison, for W-interp [12] a straightforward computation of $k_{\mathcal{T}}$ was possible: $k_{\mathcal{T}} = 4(\frac{1}{4} + \sigma_{\mathcal{T}}^2)^2$ for any distribution of $\mathcal{T}$ with zero mean and variance $\sigma_{\mathcal{T}}^2$. This leads to $k_{\mathcal{T}} = 0.25$ without shifts and $k_{\mathcal{T}} = \frac{4}{9} \simeq 0.44$ with uniform distribution. Note that the influence of the noise is reduced in the absence of any shift and that W-spline performs poorer than W-interp because of the existence of negative pixel weights.

4.3 Neyman-Pearson Detector

For simplicity and without any loss of generality, this section considers a single bit mark ($L = 1$) with $m(1) = 1$. The detection problem consists in a binary hypothesis test:
• hypothesis H_0: absence of mark,
• hypothesis H_1: presence of a mark.
Let P_d denote the probability of detection, P_{fa} the probability of false alarm. The Neyman-Pearson detector maximizes P_d for a given P_{fa} under the assumption of a GGD of R.

Under hypothesis H_1, the substitution at the embedding leads to $\epsilon_{I_W}(n_1, n_2) = 0$, thus $c_{R|H_1} = 2$ and $\sigma_{R|H_1}^2 = \sigma_{\epsilon_B}^2$. Under hypothesis H_0, $\epsilon_{I_W}(n_1, n_2)$ follows a GGD. Since the characteristic function of a GGD has no closed form, the pdf of R must be estimated numerically. Experiments show that it is also very close to a GGD. The theoretical pdf of R is computed by convolution: $f_{R|H_1} = f_{\epsilon_{I_W}} * f_{\epsilon_B}$. Then $c_{R|H_0}$ is estimated by least-square optimization.

The corresponding test statistics is given by:

$$T = \sum_{\mathcal{S}} (|\alpha_{R|H_1} r(n_1, n_2)|^{c_{R|H_1}} - |\alpha_{R|H_0} r(n_1, n_2)|^{c_{R|H_0}})$$

According to the Central Limit Theorem, T is approximately Gaussian with respective mean $\mu_{T|H_0}$, $\mu_{T|H_1}$ and variance $\sigma_{T|H_0}^2$, $\sigma_{T|H_1}^2$ that depend on $P_{\mathcal{S}}$, c, σ_B^2 and $\sigma_{\epsilon_I}^2$.

Let $Q(x) = \int_x^{+\infty} \frac{1}{\sqrt{2\pi}} e^{-u^2/2} du$ and $Q^{-1}(x)$ its inverse. The Neyman-Pearson detector decides H_0 when $T < \nu$ with

$$\nu = \sigma_{T|H_1} Q^{-1}(\mathrm{P_{fa}}) + \mu_{T|H_1}, \text{ thus } P_d = Q\left(\frac{\nu - \mu_{T|H_0}}{\sigma_{T|H_0}}\right)$$

4.4 Decoding problem

The decoding problem consists in estimating the binary original message from I'_W. The decoding performance is measured experimentally through the bit error rate (BER): BER $= (1 - \sum_{l=1}^{L} \delta(d(l), m(l)))/L$, where δ denotes the Kronecker symbol. The optimal decision threshold ν_{th} minimizes

the BER. Assuming the equiprobability of the binary message symbols, ν_{th} is solution of $\frac{\partial \text{BER}}{\partial \nu}(\nu_{\text{th}}) = 0$. This yields $\nu_{\text{th}} = \frac{\sigma_{T|H_1}\mu_{T|H_0} + \sigma_{T|H_0}\mu_{T|H_1}}{\sigma_{T|H_0} + \sigma_{T|H_1}}$. Fig. 5 displays the experimental and theoretical BER. The theoretical threshold ν_{th} is an improvement to the empirical one ν.

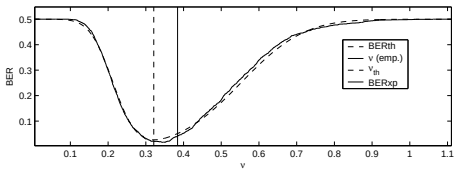

Figure 5: Choice of ν: L=2048, WNR=-4 dB, Lena

5. SUBOPTIMAL DECODING AND ROBUSTNESS

Attacks on robustness aim at distorting imperceptibly I_W in order to prevent a correct decoding. The evaluation criterion is the BER. In this section, W-spline is compared in terms of robustness to W-interp [12] and to the classical algorithms DS [2], DS with Wiener prefiltering (DS+W) [2], ST-SCS [6] and LISS [4]. Since the attack parameters are unknown to the embedder, the empirical threshold (cf Section 2) is used, which provides suboptimal decoding.

As shown by the study of $k_{\mathcal{T}}$, W-interp is more robust than W-spline to the AWGN attack. Fig.6 shows that for a reasonable WNR and high L, W-spline outperforms DS, DS+W and LISS (but not ST-SCS). When WNR and/or L are low, DS+W and LISS are more robust [12]. Note that for low BERs of Fig.6, the optimum decoder theoretical performance might not be very accurate due to the Gaussian approximation of T. The robustness of W-interp to denoising, JPEG compression and histogram equalization was demonstrated in [12]. W-spline robustness to these attacks is very similar to that of W-interp (cf Fig.7 for denoising).

The scaling attack consists changing the size of I_W. When it is re-scaled later to its original size by bilinear interpolation, this amounts to a low-pass filter. When the shrinking factor is reasonable, i.e. WNR is not too low, W-spline is robust to this attack based on interpolation (cf Fig.8). Note that a scaling factor of 0.5 corresponds to DNR=22 and to a perceptible attack.

W-spline presents the same vulnerability to desynchronizing attacks as spread-spectrum and quantization-based algorithms, as shown in [12] for W-interp and the rotation attack. Specific resynchronization techniques are to be designed.

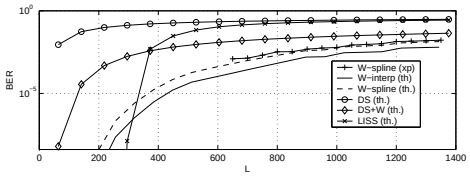

Figure 6: Robustness to AWGN, WNR=-4 dB, DWR=38 dB

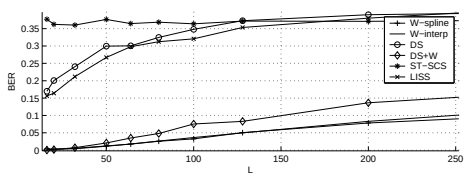

Figure 7: Robustness to denoising (DNR=24 dB), DWR=38 dB

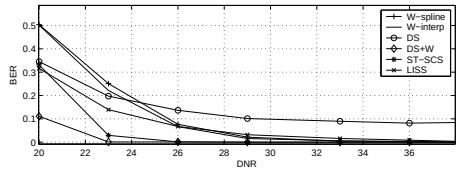

Figure 8: Robustness to scaling after resynchronization, $L = 128$, DWR=38 dB

6. SECURITY

Attacks on security aim at uncovering or estimating the secret key K from a given N_o observations of data watermarked with K. The security level of an algorithm is defined as the minimum number of observations required to estimate K with a sufficient precision. Tools based on information theory have been recently developed to assess the theoretic security level of watermarking schemes [17]. Practical algorithms implement attacks on security for the classical spread spectrum and quantization-based schemes [17]. According to the terminology of [17], W-subst does not make a perfect watermark covering, since it modifies the distribution of the interpolation error. This section proposes two security attack algorithms specifically tailored to W-subst, as well as simulations assessing its security level.

6.1 Proposed approach

In the context of digital forensics, [18] proposed to expose tampering by detecting interpolation traces. Indeed, most digital cameras use specific algorithms for missing sample interpolation. In the tampered areas of the image, this form of interpolation might disappear. Thus, one can detect and even locate digital forgeries. Unlike fragile watermarking, this technique does not resort to a prior signature insertion. An Expectation-Maximization (EM) algorithm is used to estimate simultaneously the interpolated pixels and the specific interpolation weights [18]. In the context of this paper, this EM algorithm has been adapted to estimate $K = \{\mathcal{S}, \mathcal{T}\}$.

The first security attack consists of Popescu and Farid's EM algorithm, applied to I_W ($N_o = 1$). In the unwatermarked case, the interpolation error model is the GGD rather than the uniform distribution used in [18]. The prior probability of a pixel to be in $\mathcal{S}$ is derived from the DWR. The EM algorithm provides an estimation of the weights, as well as the map of the probability that each pixel to be marked (on Fig.9, dark pixels correspond to high probabilities). The algorithm estimates also the variance σ^2_{EM} of the interpolation error on the estimated watermarked pixels and with the estimated pixel weights. When the algorithm converges to correct weights, $\sigma^2_{\text{EM}} \to 0$ since the interpolation error is null on the marked points. For a given DWR, $\mathcal{S}$ is estimated as the coordinates of the $N_{\mathcal{S}}/2$ probability map greatest values.

In the second attack, the attacker has access to $N_o > 1$ images $\{I^k_W\}_{k\in\{1..N_o\}}$ watermarked with the same key K. For each (n_1, n_2), the EM algorithm is applied to the collection $\{i^k_W(n_1, n_2)\}_{k\in\{1..N_o\}}$ and their neighborhoods. On $\mathcal{S}$, the prior probability that a pixel is marked is $1/2$. $\mathcal{S}$ consists of the points of lowest watermarked case variance since the algorithm converges on $(n_1, n_2) \in \mathcal{S}$ if N_o is sufficiently large. At the output, an estimation of $(\tau_x(n_1, n_2), \tau_y(n_1, n_2))$ is provided. The probability map allows then to decode M.

6.2 Practical results

Simulations have been performed on W-interp [12] for simplicity. Extensions to W-spline (approximated to finite interpolant support) and to other instances of W-subst are possible. Images from the test image set [19] are tiled to reach large N_o.

If $N_o = 1$, the attack is successful only if $\mathcal{T}$ is null or constant for all watermarked pixels and only for a low DWR (cf Fig.11). If $\mathcal{T}$ is randomly generated for each $(n_1, n_2) \in \mathcal{S}$, the attack fails for any DWR, which confirms that W-interp is secure when a single image is known.

If $N_o > 1$ and $\mathcal{T}$ is variable, $\mathcal{T}$ can be uncovered only when N_o is very large (cf Fig.11). However, σ^2_{EM} decreases fastly on $\mathcal{S}$ when N_o increases and a rough estimation of $\mathcal{S}$ becomes possible. If the attacker has access to less than $N_o = 10^3$ images, W-interp is secure to this attack.

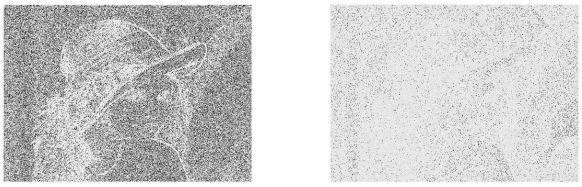

Figure 9: EM probability map, Lena, $\mathcal{T}$ constant, (left) not watermarked, (right) watermarked, DWR=32 dB

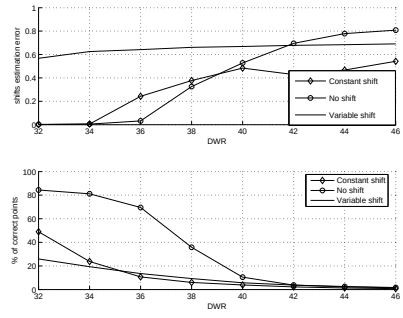

Figure 10: Attack on security, $N_o = 1$

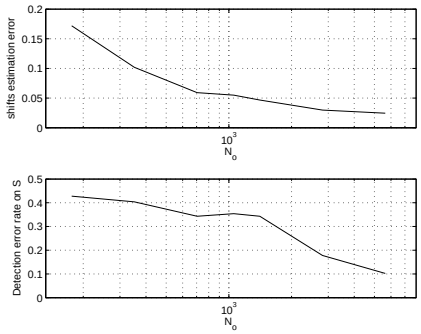

Figure 11: Attack on security, $N_o > 1$

7. CONCLUSION

A generic class of substitutive informed watermarking algorithms W-subst has been proposed. Imperceptibility of these schemes has been assessed through an objective quality metric. An optimum decoder has been derived in the context of AWGN attack. A specific practical attack on security has been designed in order to study the security level. All these tools are suitable for a large subset of W-subst.

Moreover, W-spline, a specific method based on spline interpolation, has been proposed. Objective evaluation shows that it offers good properties of security and imperceptibility. Simulations using a suboptimum decoder show that it provides good robustness to the classical waveform attacks, which was also the case of W-interp, a previously proposed algorithm based on bilinear interpolation. Specific means to improve the robustness of this kind of algorithm to geometrical attacks are under study.

An informed embedding extension of the framework W-subst is possible by the use of optimization under constraints. For instance, the perceptual quality or/and robustness to a given attack can be optimized thanks to genetic algorithms [20], where the population members differ by the algorithm parameters.

REFERENCES

[1] M.J.J.J.B. Maes and C.W.A.M Overveld, "Digital watermarking by geometric warping," *Proc. of the Int. Conf. on Image Processing (ICIP)*, vol. 2, pp. 424–426, 1998.

[2] J.R. Hernández and F. Pérez-González, "Statistical analysis of watermarking schemes for copyright protection of images," *IEEE Proc., Special Issue on Identification and Protection of Multimedia Information*, vol. 87, no. 7, pp. 1142–1166, 1999.

[3] M.L. Miller, I.J. Cox, and J.A. Bloom, "Informed embedding: Exploiting image and detector information during watermark insertion," *IEEE Int. Conf. on Image Processing - ICIP*, vol. 3, pp. 1–4, 2000.

[4] H.S. Malvar and D.A.F. Florêncio, "Improved spread spectrum: a new modulation technique for robust watermarking," *IEEE Trans. on Signal Processing*, vol. 51, no. 4, pp. 898–905, 2003.

[5] P. Moulin and R. Koetter, "Data-hiding codes," *Proc. of the IEEE*, vol. 93, no. 12, pp. 2083–2127, 2005.

[6] J.J. Eggers, R. Bauml, R. Tzschoppe, and B. Girod, "Scalar Costa Scheme for Information Embedding," *IEEE Trans. on Signal Processing*, vol. 51, no. 4, pp. 1003–1019, 2003.

[7] P. Thévenaz, T. Blu, and M. Unser, "Image interpolation and resampling," in *Handbook of Medical Imaging, Processing and Analysis*, I.N. Bankman, Ed., chapter 25, pp. 393–420. Academic Press, San Diego CA, USA, 2000.

[8] M. Unser, "Splines: A perfect fit for signal and image processing," *IEEE Signal Processing Magazine*, vol. 16, no. 6, pp. 22–38, 1999.

[9] J.J.K. Ó Ruanaith and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Signal Proc.*, vol. 66, no. 3, pp. 303–317, 1998.

[10] G. Boato, C. Fontanari, and F. Melgani, "Hierarchical deterministic image watermarking via polynomial interpolation," *Proc. of ICIP*, 2005.

[11] R. Ohbuchi, H. Masuda, and M. Aono, "A Shape-Preserving Data Embedding Algorithm for NURBS Curves and Surfaces," *Proc. of the Comp. Graphics Int. (CGI)*, pp. 170–177, 1999.

[12] V. Martin, M. Chabert, and B. Lacaze, "A novel watermarking scheme based on interpolation for digital images," *Proc. of ICASSP*, 2006.

[13] S. Voloshynovskiy, A. Herrigel, N. Baumgartner, and T. Pun, "A stochastic approach to content adaptive digital image watermarking," *International Workshop on Information Hiding*, pp. 212–236, 1999.

[14] Zhou Wang, A.C. Bovik, H.R. Sheikh, and E.P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. on Image Proc.*, vol. 13, pp. 600–612, 2004.

[15] A.B. Lee, D. Mumford, and J. Huang, "Occlusion Models for Natural Images: A Statistical Study of a Scale-Invariant Dead Leaves Model," *International Journal of Computer Vision*, vol. 41, no. 1-2, pp. 35–59, 2001.

[16] M.L. Green, "Statistics of images, the TV algorithm of Rudin-Osher-Fatemi for image denoising and an improved denoising algorithm," *CAM reports, Univ. California, Los Angeles [Online]: http://www.math.ucla.edu/applied/cam/index.html*, 2002.

[17] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security : Theory and practice," *IEEE Trans. on Signal Proc.*, vol. 53, no. 10, pp. 3976–3975, 2005.

[18] A.C. Popescu and H. Farid, "Exposing digital forgeries in color filter array interpolated images," *IEEE Trans. on Signal Processing*, vol. 53, no. 10, pp. 3948 – 3959, 2005.

[19] City University of Hong Kong Corel Image Database, "http://abacus.ee.cityu.edu.hk/ benjiman/corel_1/," .

[20] P. Kumsawat and K. Attakitmongcol, "A new approach for optimization in image watermarking using genetic algorithms," *IEEE Trans. on Signal Proc.*, vol. 53, no. 12, 2005.