USE OF SYNCHRONISATION PATTERNS TO ESTIMATE GEOMETRIC DISTORTIONS IN DIGITAL WATERMARKING

Séverine Baudry[1,2] *,Philippe Nguyen*[1] *, Henri Maître*[2]

[1]Thales Communications, 66 rue du Fosse Blanc, 92231 Gennevilliers, France
{severine.baudry, philippe.nguyen}@fr.thalesgroup.com
[2]ENST, 46 rue Barrault, 75013 Paris, France
{severine.baudry, henri.maitre}@enst.fr

ABSTRACT

Watermarking can be modeled as a transmission through a steganographic channel. Most of the channel studied up to now in the literature were additive or substitutive channels where the noise modifies the data values. But other modifications occur frequently during the watermark life, namely geometric distortions: images may be cropped, scaled and even non-linearly distorted by digital/analog conversion or by an attacker. We model here the geometric transformations by a geometric channel and introduce a random variable, the index variable, to model geometric deformations. We propose to use a synchronisation pattern to estimate geometric distortions caused by the jitter attack, and describe an optimal estimation algorithm, named Forward-Backward.

1. INTRODUCTION

It is now well known that watermarking can be modeled as furtive communication through a steganographic channel. The steganographic channel may comprise *additive noise*, which modifies the *value* of data samples, but also *geometric noise*, which modifies the *location* of data samples. Some methods have been developped to enhance the watermark retrieval after a geometric attack [1][2][3]. We here propose a general model geometric channels, by introducing a random field, named the index variable. The law followed by this variable determines the type of transform (e.g. local or global transform). We here address the jitter attack, and propose to model it by a Markov law for the index variable. We embed a known synchronisation pattern, and use this pattern at the receptor side to estimate the modification caused by the jitter, based on the above model. To perform this, we propose an optimal estimation algorithm named Forward-Backward.

2. A CHANNEL MODEL FOR GEOMETRICAL ATTACKS

2.1. General models for geometric channels : the index variable

Let $\mathbf{X}$ be the original cover data and $\mathbf{Y}$ be the resulting cover data after a geometric transformation. For images, $\mathbf{X}$ and $\mathbf{Y}$ are 2-dimensional arrays, not necessarily of the same size. To model the geometric channel, we introduce the 2-dimensional random field $\mathbf{J}$ such that, for every pixel at location (x, y) in $\mathbf{Y}$, $\mathbf{J}(x, y)$ gives the location of the corresponding pixel in $\mathbf{X}$, i.e.

$$Y(x, y) = X\left(J^x(x, y), J^y(x, y)\right)$$

where $\mathbf{J}(x, y) = (J^x(x, y), J^y(x, y))$.

The random law on $\mathbf{J}$ determines the type of transformation. In particular, the correlations between elements of $\mathbf{J}$ are of greatest importance. for instance, elements of $\mathbf{J}$ are *globally correlated* in global transformations (there is only a few degrees of freedomfor the whole field). In local transforms, the value of $\mathbf{J}(x, y)$ can not, in a realistic case, be “too far” from the values of $\mathbf{J}(x + 1, y)$, $\mathbf{J}(x, y + 1)$, $\mathbf{J}(x - 1, y)$ etc.

2.2. A Markov model for the jitter attack

We study here the jitter attack described by Petitcolas [4], where an attacker tries to desynchronize the watermark by duplicating or deleting randomly some lines of the image. Note that here a one-dimensional index variable is sufficient to describe the transformation (see Figure 2). For the sake of simplicity, we will thus from now on consider $\mathbf{X}$, $\mathbf{Y}$, and $\mathbf{J}$ as a 1-D sequences. The probability of row deletion is noted p_{del} and the probability of row copy is noted p_{copy}.

Note that, for the jitter attack, we have $J_{j+1} \geq J_j$ for all j, that is to say that the jitter preserves the order between rows. Moreover, as copies and deletions are independant, the value taken by J_j only depends on the value taken by

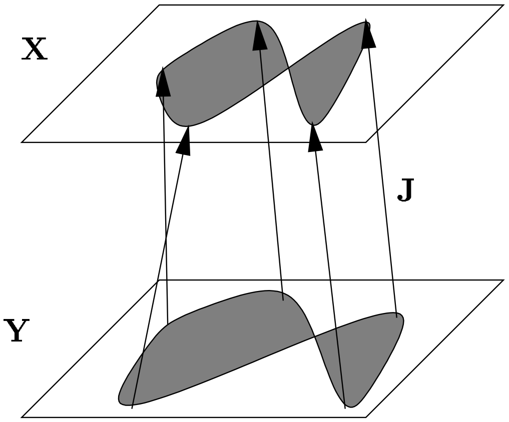

Fig. 1. Example of a geometric transformation : the image $\mathbf{X}$ has been deformed into $\mathbf{Y}$. The arrows represent the value taken by the index variable $\mathbf{J}$, which maps pixels of $\mathbf{Y}$ into the corresponding pixels in $\mathbf{X}$.

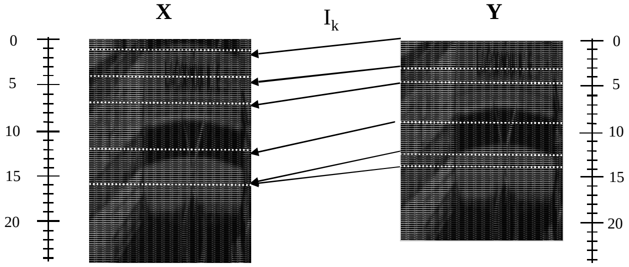

Fig. 2. Example of a jitter on a sequence $\mathbf{X}$, producing the output sequence $\mathbf{Y}$, and the corresponding index variables J_j

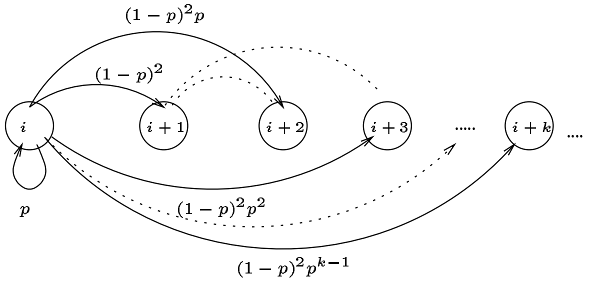

Fig. 3. Markov chain representation of the jitter attack. The states of the chain are the values taken by J_j

J_{j-1}, i.e. :

$$P(J_j/J_{j-1},\ldots,J_0) = P(J_j/J_{j-1}) \tag{1}$$

otherwise saying, the $\{J_j\}_j$ form a *Markov chain*. The probabilities of transition between states have been computed in [5], and the state graph of the Markov chain is represented in figure 3.

A realistic channel model for a watermarking system is the *compound channel*, made up of a jitter channel (or more generally any geometric channel) followed by an additive noise channel . We model the noise (due to the image) as AWGN (of course the method can be adapted to any type of noise). In the following, we will restrict to the case where the sample of the noise are independent (i.e. the noise is white).

3. SYNCHRONISATION WATERMARK FOR THE JITTER CHANNEL

3.1. Synchronisation pattern embedding

We propose to use a synchronisation watermark to estimate the geometric transforms. The synchronisation pattern is a matrix $\mathbf{X}$, following a gaussian law with zero mean and variance σ^2, whose size is the same than the cover-image. $\mathbf{X}$ is embedded inside the cover-image by a spatial additive method. The resulting picture is then watermarked with the useful message, to produce image $\mathbf{I}_w$. $\mathbf{I}_w$ is transmitted over the watermark channel, where jitter as well as additive noise may occur. Additive noise has variance σ_b^2 and is supposed to be white.

3.2. MAP estimation : the Forward-Backward algorithm

The receiver gets the possibly modified picture $\mathbf{Z}$, and, based on the synchronisation pattern $\mathbf{X}$, has to estimate the jitter realization, i.e. the index of the deleted lines and copied lines. We propose here to perform the MAP for each component of $\mathbf{J}$, i.e. we try to maximise

$$P\left(J_k/\mathbf{X};\mathbf{Z}\right) \tag{2}$$

for every line k of $\mathbf{Z}$. By applying Bayes formula, the locally estimated index variable is given by

$$\forall k \quad \hat{J}_k = \arg\left\{\max_{J_k} P(J_k;\mathbf{Z}/\mathbf{X})\right\} \tag{3}$$

We introduce two families of pdf, $\alpha_k(m)$ et $\beta_k(m)$, defined by

$$\alpha_k(m) \quad = \quad P(\mathbf{Z}_1^k; J_k = m/\mathbf{X}) \tag{4}$$

$$\beta_k(m) \quad = \quad P(\mathbf{Z}_{k+1}^n/J_k = m;\mathbf{X}) \tag{5}$$

We show now that $P(I_k; \mathbf{Z}/\mathbf{X})$ can be expressed with $\alpha_k(m)$ and $\beta_k(m)$:

$$\begin{aligned} P(J_k = m; \mathbf{Z}/\mathbf{X}) &= P(\mathbf{Z}_{k+1}^n / J_k = m; \mathbf{Z}_1^k; \mathbf{X}) \\ &\quad .P(J_k = m; \mathbf{Z}_1^k / \mathbf{X}) \qquad (6) \\ &= \beta_k(m).\alpha_k(m) \qquad (7) \end{aligned}$$

where we use the fact that $\mathbf{J}$ follows a Markov law and $\mathbf{Z}$ is white.

We now have to evaluate $\alpha_k(m)$ and $\beta_k(m)$ for all k and for all m. We show that they can be computed recursively[1]

First, we compute $\alpha_{k+1}(m)$ using the values of $\alpha_k(j)$:

$$\begin{aligned} \alpha_{k+1}(m) &= \sum_j P(Z_{k+1}/J_{k+1} = m; J_k = j; \mathbf{Z}_1^k) \\ &\quad .P(J_{k+1} = m/J_k = j; \mathbf{Z}_1^k).P(J_k = j; \mathbf{Z}_1^k) \\ &= P(Z_{k+1}/J_{k+1} = m) \\ &\quad .\sum_j P(J_{k+1} = m/J_k = j)\alpha_k(j) \end{aligned}$$

The equation 8 is obtained by taking the marginal over variable J_k and applying Bayes theorem. We then use the Markov property and the whiteness of additive noise to deduce equation 8.

In a similar way, we can compute $\beta_{k-1}(m)$ recursively from the values of $\beta_k(j)$, by explointing the jitter markovianity and the whiteness of additive noise. We have :

$$\begin{aligned} \beta_{k-1}(m) &= \sum_j P(\mathbf{Z}_{k+1}^n / J_k = j; J_{k-1} = m; Z_k) \\ &\quad .P(Z_k/J_k = j; J_{k-1} = m).P(J_k = j/J_{k-1} = m) \\ &= \sum_j P(Z_k/J_k = j)P(J_k = j/J_{k-1} = m)\beta_k(j) \end{aligned}$$

4. EXPERIMENTS AND RESULTS

4.1. Registration performances

To caracterise the performances of the algorithms, we will use the rate of mis-registered lines, defined as follows :

$$\tau = \frac{1}{N} \sum_{j=0}^{N} \mathbb{1}_{\hat{J}_j \neq J_j}$$

$\mathbf{J}$ being the real value of the jitter parameters and $\hat{\mathbf{J}}$ being the estimated value. The tests have been performed on ten gray-level pictures of size 500x500, with $p_{del} = p_{copy} = p$.

The influence of the jitter parameter p is shown on Figure 4, for $\sigma^2 = 1.0$, $\sigma^2 = 4.0$ and $\sigma^2 = 10.0$. We see that, even when the strength of the synchronisation pattern is low, the algorithm enables to lower the rate of mis-registered lines. Figure 5 shows the influence of the JPEG quality factor Q . Note that the results are better at high Q for σ^2 high, and are better at low Q for σ^2. This can be explained by the fact that the noise caused by JPEG is neither additive, nor white. Thus, the method may be improved by taking into account the specificity of the noise caused by JPEG.

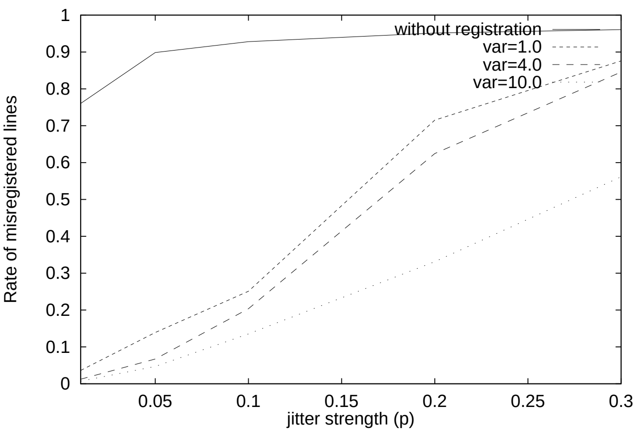

Fig. 4. Percentage of mis-registered lines in function of the jitter parameter p

4.2. Improvement on the user-watermark decoding

We have studied the influence of the jitter and the compensation on the user-watermark. We use here the block-based modulation technique derived from the one proposed by Zhao and Koch [6]. We have then applied the watermark decoding algorithm, on the one hand on the jittered image, on the other hand on the jittered, then forward-backward compensated image. The watermark decoding has been performed in a bit-by-bit fashion, and then we have computed the capacity of the equivalent channel, i.e. the jitter channel in the first case, and the combined "jitter-compensation" channel in the second case.

The results[2] are given on Figure 6. One can see that even a slight jitter greatly affects the user-watermark decoding. The compensation algorithms deeply enhance the watermark decoding at low jitter.

5. CONCLUSION

In this paper we propose a new methodology to describe geometric attacks. We model geometric distortions by considering the data indexes as random variables. More precisely, in the jitter case, these indexes form a Markov chain. We

[1] In the following, for the sake of clarity, we will suppress the reference to the synchronisation pattern $\mathbf{X}$ (all the probabilities are conditionnal to $\mathbf{X}$).

[2] The capacity is measured in Shannon by 8x8 block

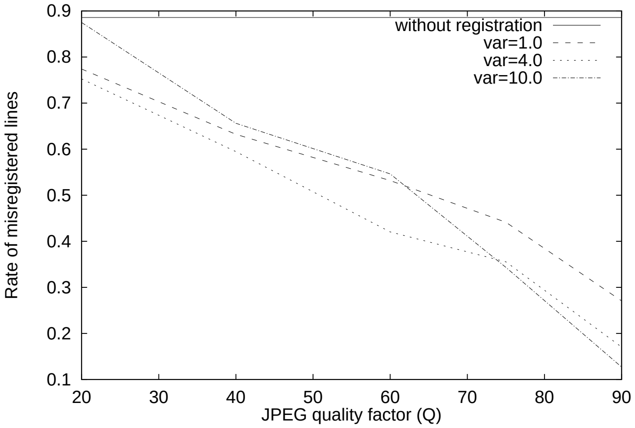

Fig. 5. Evolution of the percentage of mis-registered lines with the JPEG quality factor (Q)

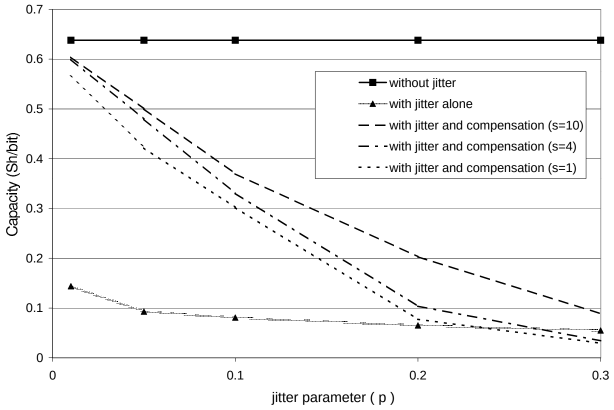

Fig. 6. Capacity of the equivalent channel after a jitter attack and after a combined jitter-compensation transformation

then use a compound channel, combining geometric noise and additive noise, to provide a realistic model of the attacks undergone by the watermark. We propose an algorithm, using a synchronisation pattern known at the receptor size, to estimate the jitter realization. Experiments show that the retrieval of the useful watermark is improved on the registered images obtained by "undoing" the jitter, based on the above estimation.

The principles of the proposed algorithms can be apply to more complex geometric transforms. The StirMark attacks may forinstancebe considered : in this case, we would use a Markov field model instead of Markov chains, and could use algorithms like ICM or to estimate the transfomration.

6. REFERENCES

[1] T. Kalker, G. Depovere, J. Haitsma, and M.J. Maes, "A video watermarking system for broadcast monitoring," in *Proc. of SPIE, Security and Watermarking of Multimedia content*, 1999, vol. 3657, pp. 103–112.

[2] J. O'Ruanaidh and T. Pun, "Rotation, scale and translation invariant digital image watermarking," in *IEEE-ICIP'97*, Santa Barbara (Cal) (USA), 1997, vol. 1, pp. 536–539.

[3] J.K. Su, F. Hartung, and B. Girod, "A channel model for a watermark attack," in *Security and Watermarking of multimedia contents, SPIE*, San-Jose (CA, USA), Jan. 1999, vol. 3657, pp. 159–170.

[4] F.A. Petitcolas, R.J. Anderson, and M.G. Kuhn, "Attacks on copyright marking systems," in *Inf. hiding 2nd workshop,*, Springer Verlag LNCS, Ed., 1998, vol. 1525, pp. 219–239.

[5] S. Baudry, P. Nguyen, and H. Maitre, "A soft decoding algorithms for watermarks subject to a jitter attack," in *Proc. of SPIE, Image Security Technologies and Applications*, San Diego, CA, July 2001, vol. 4472.

[6] J. Zhao and E. Koch, "Embedding robust label into images for copyright protection," in *Proc. Int. Cong. on Intellectual Property Rights for Specialised Information*, Vienna (Austria), Oct. 1995.