WATERMARKING POLYGONAL LINES USING AN OPTIMAL DETECTOR ON THE FOURIER DESCRIPTORS DOMAIN

Víctor R. Doncel, Nikos Nikolaidis, Ioannis Pitas

Department of Informatics, Aristotle University of Thessaloniki
Thessaloniki 54124, Greece Tel,Fax: +30-2310996304
e-mail: pitas@aiia.csd.auth.gr

ABSTRACT

Polygonal lines are key graphical primitives in vector graphics. In addition, polygonal lines can be used to define the boundary of Video Objects. The ability to apply a digital watermark to such an entity would extend the benefits of copyright protection to a wide range of data, such as Geographical Information Systems (GIS) data or MPEG-4 video.

This paper builds on and extends the contour watermarking algorithm proposed in [1]. Contour watermarking is achieved by modifying the Fourier Descriptors magnitude. Watermarks generated by this technique can be successfully detected even after rotation, translation, scaling or reflection of the host polygonal line.

The detection of such watermarks had been previously carried out through a correlator detector. In this paper, the statistics of the Fourier Descriptors are considered, and their analysis is exploited to devise an optimal detector, designed according to the Bayesian decision theory.

1. INTRODUCTION

A watermark is a hidden information within a digital signal, used primarily for copyright protection of multimedia data. Its main features are the imperceptibility of the imposed modifications and its persistence against processing (attacks) that may result in its removal, either intentionally or unintentionally. A general framework for digital watermarking has been presented in [2], whereas [3] provides an excellent overview of the watermarking principles and techniques.

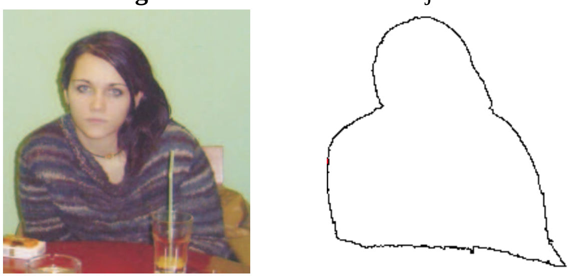
Digital watermarking has been mainly applied to still image, audio and video data. However, little work has been done in watermarking vector graphics data, that are typically used in Geographic Information Systems (GIS) or in Computer Aided Design (CAD).

The work presented was developed within VISNET, a European Network of Excellence (http://www.visnet-noe.org), funded under the European Commission IST FP6 programme.

This paper deals with the digital watermarking of polygonal lines, which are a key graphics primitive in vector graphics data and thus can be used for the copyright protection of such data. Furthermore, the method can be used for the watermarking of MPEG-4 natural video data (fig.1) by watermarking the outline of the Video Objects in MPEG-4 streams [4]. In that case, the method should be accompanied by a way of extrapolating existing textures in case the watermarked boundary defines a bigger area than the original one.

This paper extends the work presented in [1]. The same embedding method is adopted here, and efforts focus the design of a new, enhanced performance detector. Theoretical and experimental analysis show that a substantial improvement in detection performance can be achieved if the statistics of the watermarked polygon are considered.

Fig. 1. Outline of a Video Object.



2. CONTOUR WATERMARKING ALGORITHM

2.1. Watermark embedding

In the watermarking system proposed in [1] a single polygonal line is considered. The polygonal line $\mathbf{v}$ is described as a series of N vertices, $v[n] = (v_x[n], v_y[n])$, that can be seen as a complex signal $\mathbf{x} : x[n] = x_R[n] + ix_I[n]$, $n = 0, 1, ..., N-1$ whose real and imaginary parts are the 2D vertex coordinates (i.e., $x_R[n] = v_x[n]$, $x_I[n] = v_y[n]$). A complex DFT is performed on this signal, producing the

Fourier Descriptors $\mathbf{X} : X[k] = X_R[k] + iX_I[k], \ k = 0, 1, ..., N-1$. The representation of a polygonal line in terms of its Fourier Descriptors has some interesting geometric invariance properties [5] that can be exploited to devise a robust watermarking method. More specifically, the Fourier Descriptors magnitude remains the same after several geometrical transformations of the polygonal line (see Section 2.2), so it has been chosen to host the watermark.

The watermark is embedded by modifying the magnitude of the Fourier Descriptors, according to the following formula [1]:

$$|X'[k]| = |X[k]|(1 + sW[k]), k = 0, 1, ..., N-1 \qquad (1)$$

where $X'[k]$ represents a Fourier Descriptor of the watermarked polygon, the scalar s controls the watermark power $(0 < s < 1)$, and $W[k]$ is a sample of the watermark. The phase of the Fourier Descriptors is not affected by the watermark $\mathbf{W}$. The watermark is a pseudorandom signal generated from a seed integer K, which is the watermark secret key.

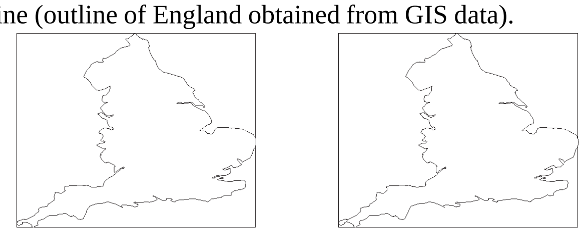
More specifically, samples $W[k], \ k = 0, 1, ..., N-1$ take randomly the values $+1$ and -1 with equal probability, whereas the samples with $W[k] = 0$ are used for low and high frequency Fourier descriptors. In other words, the watermark is not embedded in the low frequencies to avoid severe contour distortions. And it is not embedded in the high frequencies either, so that it is robust to low-pass attacks. Thus, the watermark has the form:

$$W[k] = \begin{cases} 0 & if\ k < aN\ or\ k > (1-a)N\ , \\ & or\ bN < k < (1-b)N \\ \pm 1 & else \end{cases} \qquad (2)$$

where $0 < a < b < 0.5$. The parameters a, b control the range of frequencies that will be affected by the watermark.

After watermark embedding (eq. (1)), the inverse DFT is calculated to produce the new watermarked polygon. One example is shown in fig. 2.

Fig. 2. Original (left) and watermarked (right) polygonal line (outline of England obtained from GIS data).



2.2. Robustness against manipulations

Robustness describes the degree of resistance of a watermarking method to modifications of the host signal due to either common signal processing operations or operations devised specifically in order to render the watermark undetectable (attacks).

As a direct result of the Fourier Descriptors properties, the algorithm is robust to several geometrical transformations, as well as to their combinations [1]. These transformations are:

- **Scaling, translation.** In the proposed algorithm, a normalization is carried out in every polygonal line before detection. This normalization scales and translates the polygonal line so that the mean and variance of both x and y coordinates of the vertices are 0 and 1 respectively. Thus, uniform scaling and translations, do not affect the watermark. In any case, translation is only reflected in the DC term of the Fourier transform. As the watermark is not embedded in the DC term, but in the middle frequencies, translations of the polygonal line do not affect the watermark at all.

- **Rotation.** Rotation only affects the phase of the Fourier Descriptors. Thus rotation does not change the watermark, which is embedded in the Fourier Descriptors magnitude.

- **Change of traversal starting vertex.** This is the case when traversal of the polygonal line starts from a different vertex. Again, the magnitude of the Fourier Descriptors remain the same [5] and the watermark withstands the attack.

- **Inversion of traversal direction.** If the polygonal line vertices are presented in the reverse order, the synchronization will be lost and the algorithm will not work. However, solutions to this problem exist: we can choose systematically the same traversal direction during embedding and detection (clockwise or counterclockwise), or choose watermarks that are symmetric with respect to their center, so that traversal order has no effect.

- **Mirroring.** Mirroring the polygonal line causes the Fourier Descriptors to be mirrored too. This could be overcome by performing detection on both the polygonal line and its mirrored form.

3. OPTIMAL WATERMARK DETECTION

The method in [1] used a correlator for the detection of watermarks. The test (decision) statistic of such a detector is the correlation between the watermark and the Fourier Descriptors magnitude of the polygon under test. However, the statistical detection theory states that the correlator is the optimal detector if the watermark is additive and the noise samples (in our case, the host signal, i.e. the Fourier Descriptors magnitude) are independent random variables following a Gaussian distribution. In the watermarking scheme described, neither the watermark is additive, nor the Fourier Descriptors magnitude follow the Gaussian distribution.

This better watermark detector can be designed if the statistics of the Fourier Descriptors magnitude are modelled more accurately. To this end we follow an approach similar to that in [6] and [7] , that was originally proposed in the context of 2D raster images.

3.1. Likelihood Ratio Test

Our approach is based on the Bayes decission theory, and the subsequent likelihood ratio test (LRT). Let us consider a possibly watermarked polygon; the watermark detector aims at verifying whether it hosts a certain watermark $\mathbf{W}$ or not. The watermark detection can be expressed as a hypothesis test where two hypotheses events are possible:

- H_0: The polygonal line does not host watermark $\mathbf{W}$
- H_1: The polygonal line hosts watermark $\mathbf{W}$

Let $\mathbf{M} : M[k], k = 0, 1, ..., N-1$ be the vector of the Fourier Descriptors magnitude for the polygonal line under consideration. Each component of this vector is a random variable, with conditional probability density functions $p(M[k] \mid H_0)$ and $p(M[k] \mid H_1)$.

LRT in this case can be defined as:

$$\Lambda = \frac{p(\mathbf{M} \mid H_0)}{p(\mathbf{M} \mid H_1)} \underset{H_1}{\overset{H_0}{\gtrless}} T \tag{3}$$

If $M[k]$ are assumed to be independent, the LRT has the following form:

$$\Lambda = \frac{\prod_{k=0}^{N-1} p(M[k]|H_0)}{\prod_{k=0}^{N-1} p(M[k]|H_1)} \tag{4}$$

For hypothesis H_0, and assuming that no distortions ocurred in the signal, and that the signal bears no watermark at all:

$$p(M[k]|H_0) = p(|X[k]|) \tag{5}$$

Considering the transformation (scaling) of eq. (1) applied to a random variable, the pdf of the watermarked Fourier Descriptors magnitude can be easily expressed as a function of the original Fourier Descriptor magnitude pdf:

$$p(M[k]|H_1) = \frac{1}{1+s} p(|X[k]|(1 + sW[k])) \tag{6}$$

By substituting (6) and (5) in (4), we can calculate the LRT, Λ, in terms of the pdf of the Fourier Descriptors magnitude of the original signal, $p(|X[k]|)$. This distribution will be approximated in the Section 3.2.

The watermark detection performance can be measured in terms of the probability of false alarm P_{fa} (i.e. the probability to detect a watermark in a signal that is not watermarked or, is watermarked with a different watermark) and the probability of false rejection P_{fr} (i.e. probability of erroneously neglecting the watermark existence in the signal).

If equal importance is assigned to both errors (false positive and false negative), and the prior probabilies of H_0 and H_1 are equal, then the optimal threshold T is 1.

It should be noted that certain assumptions adopted in the previous derivations (e.g. the assumption of the independence of the Fourier Descriptors magnitude) do not hold in practice. However, these assumptions were deemed necessary in order to make the derivations tractable. Similar assumptions were adopted in [6]. Moreover, the fact that the derived detector achieves very good performance as will be shown in section 4, justifies, at a certain extent, the adoption of these assumptions.

3.2. Probability density function of the Fourier Descriptors magnitude

Polygonal lines which describe real world objects, tend to avoid sharp corners. Thus it is reasonable to expect that most of the signal energy is concentrated in the low frequencies, and that components are not identically distributed.

If $X_R[k]$ and $X_I[k]$ are assumed to follow a Gaussian distribution, and if their variances are the same $\sigma_k^2 = \sigma_{X_{Rk}}^2 = \sigma_{X_{Ik}}^2$, then the magnitude $|X[k]|$ follows a Rayleigh distribution, as is proved in [5].

$$p(|X[k]|) = \frac{|X[k]|}{\sigma_k^2} \exp\left(-\frac{|X[k]|^2}{2\sigma_k^2}\right), \quad k > 0. \tag{7}$$

The variance σ_k^2 of this distribution has to be estimated for all different values of k. The signal used for the estimation might be watermarked, but we assume that the watermark does not affect significantly the estimation. The strategy we propose is to estimate its value by taking into account the surrounding samples in a small interval, $|X[i]|$, $(k-M) < i < (k+M)$ i.e. we assume in a way similar to [6] that for small M, the samples of the interval follow the same pdf. Mean and variance are estimated as:

$$\widehat{\mu}_k = \frac{\sum_{i=k-M}^{k+M} |X[i]|}{N} \tag{8}$$

$$\widehat{\sigma}_k^2 = \frac{\sum_{i=k-M}^{k+M} (|X[i]| - \widehat{\mu}_k)^2}{N-1} \tag{9}$$

One faster alternative is to evaluate the above estimators in blocks of samples, and assign the estimated values to all the samples in the block.

In practice, a value of $M = 25$ yields a good trade-off between accuracy in the variance estimation and fidelity to the actual power spectral density.

4. EXPERIMENTAL RESULTS

In order to verify the superiority of the proposed detector against the correlator, different tests were performed over several sample polygons. Among these polygons, there were the shape of a country obtained from GIS data (fig. 2), and the Video Object boundary from the frame in fig. 1. In the performed tests, a power of $s = 0.15$ was used, and a, b, were set to $a = 0.1$, $b = 0.4$.

For both detectors mentioned in this paper, i.e. the correlator detector presented in [1] and the optimal detector proposed in this paper, the output is a real number that has to be compared against a threshold. Error probabilities P_{fa} and P_{fr} depend on this threshold. By using $P_{fa}(T)$, $P_{fr}(T)$ values, we can evaluate the *Receiver Operating Characteristic* (ROC), i.e., the plot of the probability of false alarm P_{fa} versus probability of false rejection P_{fr} for different values of T.

Unfortunately $P_{fa}(T)$ and $P_{fr}(T)$ are not easy to estimate. Such an estimation actually involves counting the number of errors (erroneously detected watermarks or missed watermarks) after a large run of experiments for different T, a method that is not practical, as for the low error probabilities we are interested at, the number of trials that should be performed is too large. To proceed with the estimation, it was assumed that the output of the detector is a random variable following a Gaussian pdf. The gaussianity assumption was verified by the fact that the P_{fa}, P_{fr} values obtained from the ROC curve for a specific threshold value, and the values found by counting the erroneously detected and missed watermarks after a large number of experiments were in agreement.

The mean and variance of the detector output for watermarked and not watermarked polygonal lines were estimated through a set of experiments performed on several polygons, each involving 10000 trials. Polygons consisted of a number of vertices between $N = 1000$ and $N = 20000$. The ROC curves for the test polygons shown in fig.1 and fig.2, for both the correlator and the optimal detector, can be seen in fig.3. It is obvious that the optimal detector performs in all cases better than the correlator.

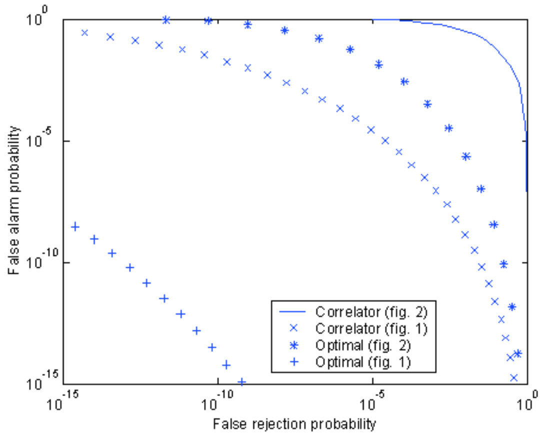
In addition, several attacks were tried, to assess the robustness of the watermark against manipulations. Translations, rotations and isotropic scaling were applied on the polygonal lines, and did not affect the watermark, i.e., the ROC curve did not change at all.

5. CONCLUSIONS

A method for watermarking polygonal lines has been presented in this paper. Due to its general nature, the algorithm can be applied in several different contexts, like GIS data or Video Objects. The reliability of the system was assessed in terms of detection error probabilities and ROC curves. A comparison was established between the correlator detector proposed in [1], and the optimal detector proposed here, showing the superiority of the latter.

Currently, the algorithm is not sufficiently robust to the vertex removal (polygonal line simplification) operation. Future work will try to deal with this drawback.

Fig. 3. ROCs for the correlator and optimal detectors



6. REFERENCES

[1] V. Solachidis and I.Pitas, "Watermarking polygonal lines using fourier descriptors," *IEEE Computer Graphics and Applications*, vol. 24, no. 3, May/June 2004.

[2] G. Voyatzis and I. Pitas, "Protecting digital-image copyrights: A framework.," *IEEE Computer Graphics and Applications*, vol. 19, no. 1, pp. 18–24, January/February 1999.

[3] I.J. Cox, J. Bloom, M. Miller, and I. Cox, *Digital Watermarking: Principles & Practice*, Morgan Kaufmann.

[4] D. Nicholson, P. Kudumakis, and J.F. Delaigle, "Watermarking in the mpeg-4 context.," in *ECMAST*, 1999, pp. 472–492.

[5] A. Papoulis, *Probability and Statistics*, Prentice Hall, 1991.

[6] M. Barni, F. Bartolini, A. De Rosa, and A. Piva, "A new decoder for the optimum recovery of nonadditive watermarks," *IEEE Transactions on Image Processing*, vol. 10, no. 5, pp. 755–767, May 2001.

[7] Q. Cheng and T. S. Huang, "Robust optimum detection of transform domain multiplicative watermarks," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 906–925, April 2003.