WATERMARKING OF SETS OF POLYGONAL LINES USING FUSION TECHNIQUES

A. Giannoula, N. Nikolaidis, I. Pitas

Department of Informatics, Aristotle University of Thessaloniki,
Box 451, Thessaloniki 540 06, GREECE
e-mail: {gianoula,nikolaid,pitas}@zeus.csd.auth.gr

ABSTRACT

A blind watermarking method for the copyright protection of sets of polygonal lines in vector graphics images and GIS data (elevation contour maps) is presented in this paper. The paper focuses mainly on the use of simple fusion rules for combining the detector outputs from each polygonal line in order to come up with a global detection result. Experimental comparison of the various fusion methods using both synthetic and real data (elevation maps) is provided.

1. INTRODUCTION

Copyright protection by watermarking has recently emerged as a challenging research area and a promising tool against digital piracy [1, 2]. Watermarking research focuses mainly on bitmap images. Other digital media, such as vector images (images where the various objects are represented by means of a set of geometric primitives, e.g., polygonal lines) and Geographical Information Systems (GIS) data (3-D meshes, depth/elevation values on grids, elevation contour maps), received limited attention so far. Both these data categories are of high commercial value, since their generation is usually labor and resource intensive. Furthermore, GIS data used in military applications are usually classified and thus tracing a possible leakage is of utmost importance. A blind method for the watermarking of individual polygonal lines, by modifying the magnitude of the Fourier descriptors, has been proposed recently [3]. Due to the properties of Fourier descriptors, the technique is invariant to several geometric distortions (scaling, translation, rotation, change of starting point, reflection). The present paper attempts to generalize the proposed algorithm, in order to handle sets of polygonal lines, e.g., a set of contour lines in an elevation map. Obviously, a strategy for combining the watermark detection results obtained from each polygonal line, i.e., a data fusion strategy, needs to be devised in order to deal with such sets.

The data fusion methods that will be examined belong to the centralized fusion category [4, 5], where local sensors send the unprocessed observations to the fusion center which proceeds with the global decision-making procedure. Centralized fusion methods have usually better performance than decentralized ones, since decentralized (local) decision-making results in loss of information that might have been useful if sent for further processing to the fusion center. In the context of watermarking of multiple data sets, centralized fusion means that no binary decision on whether each individual line is watermarked or not is taken, but the soft detector outputs (detection statistics) are combined to obtain a global decision. Decentralized fusion for combining multiple detectors has been treated in [6]. A number of simple fusion rules are proposed and their relative performance is experimentally evaluated. It should be noted that the results on the performance of the various fusion rules obtained in this paper can be applied in other circumstances that involve multiple watermark detectors, e.g., for fusing detector outputs from multichannel audio, multiple video objects in an MPEG4 video sequence, or from different audio or video segments belonging to the same sequence.

The outline of this paper is as follows: section 2 reviews the polygonal line watermarking algorithm. The fusion rules that have been used are presented in section 3. Detailed experimental results are included in section 4. Conclusions are drawn in section 5.

2. POLYGONAL LINE WATERMARK EMBEDDING AND DETECTION

Consider a set of M closed polygonal lines $L_i,\ i = 0, \ldots, M-1$, so that L_i consists of N_i vertices, each represented as a coordinate pair $(x_i(n), y_i(n))$. By combining these coordinates, a complex signal $z_i(n) = x_i(n) + j \cdot y_i(n)$ is constructed. Let $Z_i(k),\ k = 0, \ldots, N_i - 1$, be the Fourier descriptors of L_i, i.e., the discrete Fourier transform coefficients corresponding to $z_i(n)$ [7]. The algorithm proposed in [3] embeds a watermark $W_i(k)$ at each polygonal line, by modifying the magnitude $|Z_i(k)|$ of the corresponding Fourier descriptors, using an embedding function of the form:

$$|Z_i'(k)| = |Z_i(k)| \oplus p \cdot W_i(k) \tag{1}$$

where $\oplus$ denotes an additive or multiplicative superposition rule and constant p is usually called embedding power and controls the watermark strength. The watermark signal $W_i(k)$ for each polygonal line affects certain mid-frequency terms and is generated using the following formula:

$$W_i(k) = \begin{cases} W^0(k), & if\ aN_i < k < bN_i\ or \\ & (1-b)N_i < k < (1-a)N_i \\ 0, & otherwise \end{cases} \tag{2}$$

where $0 < a < b \leq 0.5$ control the frequency terms that will be affected and W^0 is a binary watermark (± 1) generated by a pseudorandom number generator using a suitable key K.

The procedure described above results in the generation of a set of watermarked lines $L_i^{'}$. Watermark detection on each line is performed by evaluating the correlation between the watermark sequence $W_i(k)$ and the magnitude of the Fourier descriptors $|Z_i'(k)|$:

$$c_i = \sum_{k=0}^{N_i - 1} W_i(k)|Z_i'(k)|, \quad i = 0, \ldots, M-1 \tag{3}$$

c_i are then normalized so as to be confined in the $[0...1]$ interval. Thus, at the end of this stage, we come up with a set of M normalized correlator outputs $c_i^{'}$, one for each polygonal line.

3. DATA FUSION RULES

The aim of the data fusion module is to combine the individual correlator outputs obtained in the previous stage in order to reach a global binary decision on whether the set of polygonal lines under investigation is watermarked or not. In other words, we seek a suitable function f in order to derive a single value c out of the M values ${c'}_0, \ldots, {c'}_{M-1}$:

$$c = f({c'}_0, \ldots, {c'}_{M-1}) \tag{4}$$

c is consequently compared to a properly selected threshold T in order to decide on the watermark existence. In the following subsections, a number of empirical fusion rules and the Neyman-Pearson test for a set of observations are described.

3.1. Likelihood Ratio Test

The Neyman-Pearson hypothesis test (the test that minimizes false rejection probability for a fixed false alarm probability) for a set of observations c_i (in our case, the individual non-normalized correlator outputs) is equivalent to the Likelihood Ratio (LR) test for these observations:

$$c = LR = \frac{P(c_0, .., c_{M-1}|H_1)}{P(c_0, .., c_{M-1}|H_0)} \tag{5}$$

where $P(c_0, .., c_{M-1}|H_1), P(c_0, .., c_{M-1}|H_0)$ are the conditional joint probability density functions of c_i under the two hypotheses (H_1: the set of lines bears the watermark under investigation, H_0: the set of lines hosts a different watermark than the one under investigation). In order to proceed with the evaluation we have assumed that c_i are independent, normally distributed random variables. Under these assumptions the Likelihood Ratio can be expressed as follows:

$$c = \frac{P(c_0|H_1)..P(c_{M-1}|H_1)}{P(c_0|H_0)..P(c_{M-1}|H_0)} \tag{6}$$

where:

$$P(c_i|H_j) = \mathbf{N}(\mu_{c_i|H_j}, \sigma_{c_i|H_j}), \;\; i = 0, \ldots, M-1, \;\; j = 0, 1 \tag{7}$$

The conditional mean and variance of the correlator output for the multiplicative embedding scheme have been evaluated to be [8]:

$$\begin{aligned} \mu_{c_i|H_1} &= 2\,(b-a)\,N\,p \\ \sigma^2_{c_i|H_1} &= 2\,(b-a)\,(\mu^2_{|Z_i|} + \sigma^2_{|Z_i|}) \\ \mu_{c_i|H_0} &= 2\,(b-a)\,N\,p\,\mu_{|Z_i(k)|} \\ \sigma^2_{c_i|H_0} &= 2\,(b-a)\,(\mu^2_{|Z_i|} + \sigma^2_{|Z_i|})(1+p^2) \end{aligned} \tag{8}$$

Since the Fourier descriptors Z_i of the original (non watermaked) polygonal line are not available during detection, the conditional mean and variance values were evaluated using the watermarked sequence Z'_i, i.e. we assume that $Z_i \approx Z'_i$ which is a reasonable assumption, given the fact that the alterations introduced by the watermark are very small.

3.2. Empirical Fusion Rules

Besides the Likelihood Ratio test, the following ad hoc empirical fusion rules were tested as well:

1. Mean value of $c_i^{'}, \;\; i = 0, \ldots, M-1$.
2. Median value of $c_i^{'}$.
3. Minimum value of $c_i^{'}$.
4. Maximum value of $c_i^{'}$.
5. Trimmed mean value of $c_i^{'}$ [9]. This fusion rule orders $c_i^{'}$, rejects a percentage a of the smaller and bigger observations and evaluates the mean of the remaining ones.

$$c = \frac{1}{M(1-2a)} \sum_{i=aM}^{M-aM-1} c_{(i)}^{'} \tag{9}$$

where $c_{(0)}^{'} \leq c_{(1)}^{'} \leq \ldots \leq c_{(M-1)}^{'}$.
By doing so, outlying correlator outputs that can lead the global decision towards false alarms (big values) or false rejections (small values) are rejected. In our experiments, the two biggest and smallest correlator outputs were rejected.

6. Modified trimmed mean of $c_i^{'}$. According to this rule, the correlator outputs, whose distance from the median value exceeds a certain threshold (set to 0.03 in our case) are rejected and the mean value of the remaining samples is evaluated:

$$c = \frac{\sum_{i=0}^{M-1} a_i c_{(i)}^{'}}{\sum_{i=0}^{M-1} a_i} \tag{10}$$

where the coefficients a_i are chosen according to the rule:

$$a_i = \begin{cases} 1 & \text{if } \mid c_{(i)}^{'} - med\{c_i^{'}\} \mid \leq q \\ 0, & \text{otherwise} \end{cases} \tag{11}$$

The effect of this operator is similar to that of the trimmed mean operator.

7. Weighted mean of $c_i^{'}$:

$$c = \frac{\sum_{i=0}^{M-1} w_i c_i^{'}}{\sum_{i=0}^{M-1} w_i} \tag{12}$$

Obviously, the performance of this fusion rule depends on the choice of the weights w_i. Since the reliability of the correlator detector increases with the number of samples in the correlation sum (3), w_i's were chosen accordingly. Two different choices were tested:
a) $w_i = N_i$, i.e., the weight corresponding to the correlator output for the line L_i is chosen to be equal to the number of vertices N_i of L_i. If line vertices are assumed to be equidistant, N_i is directly related to the length of curve L_i. This selection of weights emphasizes the contribution of long lines in the evaluation of the total detection statistic c and limits the impact of detector outputs from short lines, which are not very reliable.
b) $w_i = N_i^2$, i.e. w_i are chosen to be equal to the square of the number of vertices of the corresponding line L_i. Obviously this choice of weights further increases the contribution of long lines in the final detector output.

Table 1: EERs for various line lengths and embedding powers.

Length / Emb.Power	0.4	0.5	0.6
1000	$10^{-3.5}$	10^{-5}	10^{-7}
1500	10^{-4}	10^{-7}	10^{-10}
2000	$10^{-5.5}$	10^{-14}	10^{-16}
2500	10^{-8}	10^{-12}	10^{-18}

Figure 1: Original version of the Hortiatis mountain elevation map.

8. Trimmed weighted mean of $c_i^{'}$. This is a combination of the trimmed and weighted mean ($w_i = N_i$) approaches presented above. The correlator outputs $c_i^{'}$ are ordered, a percentage of the smaller and bigger values are rejected and the weighted mean of the remaining samples is evaluated. Weights w_i were chosen to be equal to the length N_i of the corresponding line. The two biggest and smallest correlator outputs were rejected.

4. EXPERIMENTAL RESULTS

The first set of experiments aimed at investigating the influence of the number of line vertices and the watermark strength parameter p on the algorithm performance. Our goal was to find the minimum polygonal line length and the maximum watermark embedding power that allow for credible detection while guaranteeing imperceptible embedding. Thus, the algorithm was applied with different embedding power values p on individual polygonal lines of various lengths and the ROC (Receiver Operating Characteristics) curves (plots of the probability of false alarm P_{fa} versus the probability of false rejection P_{fr}), as well as the corresponding Equal Error Rate points (the points on the ROC curve where the probability of false alarm equals the probability of false rejection) were evaluated (Table 1). Visual inspection demonstrated that distortions are almost impossible to be observed when p is smaller than 0.45. Furthermore, we have assumed that a single-line EER equal or smaller than 10^{-4} is sufficient for most applications, bearing in mind that the EER point obtained for a set of lines is considerably better than that obtained for an individual line (see subsequent experiments). Using the experimental data and the reliability and invisibility constraint that we have imposed, we have decided to use $p = 0.45$ and to watermark only polygonal lines consisting of at least 1000 vertices.

Figure 2: Watermarked version of the Hortiatis mountain elevation map.

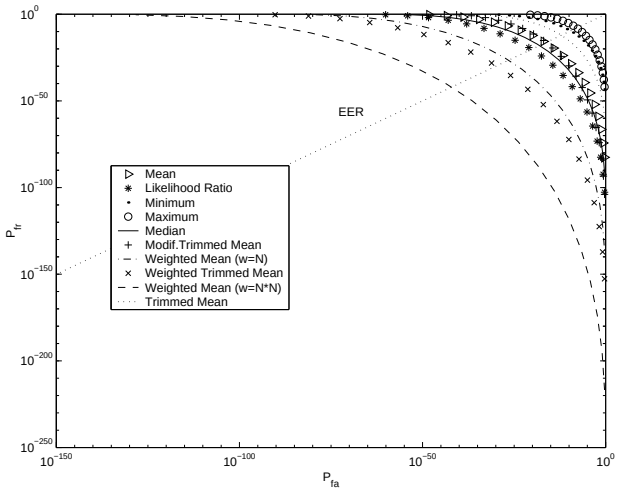

Figure 3: ROC curves for the Hortiatis map for various fusion rules.

In order to judge the relative performance of the fusion rules presented in Section 3, experiments were conducted on the elevation contour map of the Hortiatis mountain, Thessaloniki, Greece (Figure 1). The embedding parameters were chosen to be $a = 0.1$, $b = 0.3$, $p = 0.45$. Lines having length smaller than 1200 vertices were not watermarked. Thus, only 18 curves were watermarked, their number of vertices ranging between 1200 and 14500. The watermarked elevation map can be seen in Figure 2. Obviously no visible changes can be seen neither at this scale, nor in bigger magnifications. The ROC curves for the various fusion methods and the corresponding EER points can be seen in Figure 3 and the first column of Table 2, correspondingly. Experiments were also conducted, on a set of 9 artificially generated lines having length between 1000 and 2450 vertices. The corresponding EER points can be seen in the second column of Table 2.

Table 2: EERs of the various fusion rules for the Hortiatis mountain elevation map (set 1) and a set of the nine small polygonal lines (set 2).

Fusion Rule	Set 1	Set 2
Maximum	10^{-8}	$8 \cdot 10^{-7}$
Minimum	10^{-10}	10^{-7}
Mod. Trimmed Mean	10^{-16}	$6 \cdot 10^{-8}$
Median	10^{-18}	$3 \cdot 10^{-8}$
Mean	10^{-16}	$2 \cdot 10^{-8}$
Trimmed Mean	10^{-12}	10^{-8}
Likelihood Ratio	10^{-20}	10^{-8}
Weight.Trim.Mean	10^{-30}	$8 \cdot 10^{-9}$
Weighted Mean($w_i = N_i$)	10^{-27}	$5 \cdot 10^{-9}$
Weighted Mean($w_i = N_i^2$)	10^{-42}	$4 \cdot 10^{-10}$

Table 3: EERs for various attacks and the best two fusion rules.

Attack	Weight.Mean(N_i)	Weight.Mean(N_i^2)
Rotation	$5 \cdot 10^{-9}$	$4 \cdot 10^{-10}$
Mean	10^{-7}	$1.8 \cdot 10^{-8}$
Median	$4 \cdot 10^{-8}$	$8 \cdot 10^{-9}$
No attack	$5 \cdot 10^{-9}$	$4 \cdot 10^{-10}$

By inspecting the experimental results, one can easily conclude that even for a few lines of relatively small length (set 2) the obtained EERs are very satisfactory. Results are drastically better in the case of the elevation map, that involves a bigger number of larger lines. Among the various fusion rules, the best performance was achieved by the weighted mean rule, using as weights the square of the number of line vertices. The weighted mean rule using weights equal to the number of line vertices and the weighted trimmed mean rule were interchanged in the second and third performance ranks. This ranking indicates that the line length is indeed an important factor for the algorithm performance and that the global decision should be based mainly on results obtained by the larger lines. The LR test, which one could expect to achieve the best results, was ranked fourth. This was probably due to the assumptions that were made and the fact that the estimation of the required conditional mean and variance were only approximate.

In a final set of experiments, the robustness of the best two fusion rules on attacks was investigated. The following distortions were induced to the set of nine lines (set 2): line smoothing using 1-D mean and median filtering (window size 3) of the line point coordinates on each coordinate x, y separately and rotation by 30^o. The corresponding EER points can be seen in Table 3. The fact that the EER values for the rotated lines are identical to those of the distortion-free lines proves that the method is invariant to rotation. Similar results (insignificant changes to the EER values) were obtained for the other geometrical distortions to which the method is invariant to (scaling, translation, rotation, change of starting point, reflection) [3]. Furthermore, the results prove that the method is robust to line smoothing.

5. CONCLUSIONS

In this paper, a blind method for the watermarking of sets of polygonal lines that can be used for the copyright protection of vector graphics images and GIS elevation contour maps is presented. Research focused on finding a proper scheme to fuse the partial detector outputs corresponding to each line and to obtain the optimal global decision for the whole set. Experimental results demonstrate the superiority of the weighted mean fusion rule using weights that are equal to the square of the number of vertices of the corresponding polygonal line. The robustness of the technique to various distortions is also exemplified.

6. ACKNOWLEDGEMENTS

This work has been partially funded by the EU project IST-1999-10987 CERTIMARK. Elevation map data were provided by the Greek Army Geographical Service (GYS).

7. REFERENCES

[1] M.D. Swanson, M. Kobayashi, and A.H. Tewfik, "Multimedia data embedding and watermarking technologies," *Proceedings of the IEEE*, vol. 86, no. 6, pp. 1064–1087, June 1998.

[2] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1079–1107, July 1999.

[3] V. Solachidis, N. Nikolaidis, and I. Pitas, "Watermarking polygonal lines using fourier descriptors," *IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP'2000)*, vol. 4, pp. 1955–1958, June 2000.

[4] Belur V. Dasarathy, *Decision Fusion*, IEEE Computer Society Press, The Institute of Electrial and Electronic Engineer, Inc., 1994.

[5] Z. Chair and P.K. Varshney, "Optimal data fusion in multiple sensor detection systems," *IEEE Transactions on Aerospace and Electronic Systems*, vol. AES-22, pp. 98–101, June 1986.

[6] R.Chandramouli and N. D. Memon, "A distribution detection framework for watermark analysis," *ACM Multimedia Workshop on Multimedia and Security*, 30 Oct-4 Nov 2000.

[7] A.K. Jain, *Fundamentals of digital image processing*, Prentice Hall, 1989.

[8] V. Solachidis and I. Pitas, "Circularly symmetric watermark embedding in 2-d dft domain," in *Proc. of ICASSP'99*, Phoenix, Arizona, USA, 15-19 March 1999, vol. 6, pp. 3469 – 3472.

[9] I. Pitas and A.N. Venetsanopoulos, *Nonlinear Digital Filters: Principles and Applications*, Kluwer Academic, 1990.