BLIND CITY MAPS WATERMARKING UTILIZING ROAD WIDTH INFORMATION

Elias Horness, Nikos Nikolaidis and Ioannis Pitas

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

ABSTRACT

Geographic Information System (GIS) data is a valuable asset that should be protected using digital rights management (DRM) techniques. This paper introduces a new technique for watermarking city maps by altering a basic parameter of a road segment, namely its width to length ratio. A watermark is embedded in the map using an appropriate quantization of this ratio. The watermarked map retains its visual quality since the quadrilateral shape of the buildings and their alignment with road boundaries are maintained. The proposed approach performs blind detection through correlation of the detected watermark with the watermark under investigation and is robust against several attacks such as rotation, translation, uniform scaling and additive white Gaussian noise (AWGN) .

1. INTRODUCTION

Maps based on GIS data are accurate representations of a geographical region and are used for many purposes such as military and civil cartography, urban planning, forestry etc. In such maps, each geographical entity, like a mountain or a river, is defined by a certain number of vertices set in a specific order. Generation of GIS data is labour intensive. Thus, GIS data constitute a valuable asset which should be protected from digital piracy. Digital watermarking has lately emerged as an efficient way of digital rights management (DRM).

When watermarking GIS data, it is important to keep the data distortion low, i.e. the coordinates of the vertices defining the various geographical entities must remain as close as possible to their values in the original non-watermarked map. For vector data maps two watermarking approaches can be taken: spatial domain techniques and transform domain techniques. The spatial domain techniques work directly on the coordinates of vertices [2] [3], while the transform domain techniques first translate the spatial data to a transform domain and then apply the watermark in that domain. Various transforms, like the Fourier descriptors [7] [8], wavelet transform [6] or mesh-spectral domain [5] have been used in the literature.

The aim of this work is to provide a new method for watermarking city maps for DRM purposes, e.g. intellectual property rights protection or traitor tracking. City maps, also called urban maps, are usually abstract representations of real cities (Figure 1). They usually do not hold exact geographical data like other types of GIS maps but useful visual information in order to let a person to orientate and reach his destination. Thus, city maps, although directly related to, and usually generated from, GIS data, are distinct from such data.

There is a lack of watermarking techniques for city maps. Applying the methods proposed for general vector maps mentioned above will most likely produce a high visual distortion, due to the fact that such techniques do not take into account the two basic characteristics of city maps, namely the regularity of the shapes and the alignment of the buildings with the roads present in the map. More specifically, the most common entities in city maps are the buildings which are usually represented as quadrilaterals, or more specifically rectangles. This implies that only four points are enough to represent them (even if more points are used, just four are essential). Any small change on the coordinates of a building may make it to stand out from the line of the rest of the buildings of the road. Moreover, the shape of the building will deviate from the standard rectangular shape. If this happens in multiple instances, then the perceived visual distortion will be big, even if the distortion in terms of coordinates is kept low.

Figure 1: Example of a city map.

Our approach is to work directly with what gives a map its characteristic grid-like appearance: the edges of the buildings and the roads. We embed the watermark information by modifying the width of a road segment, which is formed by the edges of two buildings that are facing each other. This modification ensures that the buildings retain their shape. Furthermore, by altering only slightly the width of a road segment, we keep the visual "straightness" of the roads and thus make visual distortions extremely low or even imperceptible. Such an approach might introduce more alterations on the coordinates than other general GIS watermarking techniques. However, since as mentioned above, visual quality precedes over accuracy in city maps, the proposed approach is a valid and efficient one.

The proposed technique is robust against uniform scaling, rotation, translation, AWGN and insertion and deletion of vertices (while keeping the geometry of an entity).

2. METHOD DESCRIPTION

The proposed method embeds a binary watermark sequence, generated from a key, in the width of the road segments using a quantization technique. Each watermark bit is embedded in a different road segment of the map. The overview of the proposed method is as follows. First the map is analyzed and road segments are extracted. A road segment is formed by the two edges of two buildings that are facing each other. Once we have all the road segments, we rotate the map according to the most common direction α_{mcd}, so that this primary direction coincides with the horizontal direction. Then we rotate the map again by a rotation angle β_{Wkey}, whose value is de-

termined by the watermark key, order the road segments according to their starting positions on the map and select the road segments which will hold the watermark using the watermark key. We embed the sequence by modifying the road segment width according to the watermark bit they must hold. Finally we inversely rotate the map to set it to its original orientation.

The watermark detection procedure is quite similar. Again, the map is analyzed and the road segments are extracted. The most common direction α_{mcd} is computed and the map is rotated to match it with the horizontal direction. Afterwards we rotate the map according to the angle determined by the watermark key β_{Wkey}. We order the road segments and select the road segments which were watermarked using the watermark key. Finally we extract the watermark bits from the width of the road segments. Once we have the retrieved sequence, we correlate it with the watermark sequence generated from the given key in order to decide whether the map has been watermarked or not using that key.

The various steps of the method are presented in detail in the paragraphs below.

2.1 Road Segment Detection

Typically, explicit road entities do not exist in a map (Figure 1). The road is the perception a person gets when seeing all the buildings aligned along two imaginary parallel lines that delimit the borders of the road. We define road segments as sections of a road. A road segment is formed by two edges of two buildings that are facing each other. To establish that two edges of such buildings may form a road segment the following criteria are applied.

- The ratio of the projection of one edge on the other versus the length of this edge must exceed a certain threshold, set to 80% in our work.
- No map entities (i.e. buildings) should reside between these edges.

2.2 Watermark Embedding

Before embedding the watermark, the map is rotated twice, once for achieving robustness against rotation and another for preventing the non-authorized watermark retrieval.

To achieve rotation robustness we first compute the most common direction α_{mcd} of all edges in the map by finding the highest peak of the histogram of the direction angles. Subsequently the map is rotated so that α_{mcd} coincides with the horizontal direction. As will be described in Section 2.3, the same procedure is applied before watermark detection in order to cancel any rotation that has been applied on the map. This renders the method robust against rotation.

We perform a second rotation of the map by an angle β_{Wkey} which is computed from the input watermark key. The overall rotation angle is defined as:

$$\delta_{rotation} = \beta_{Wkey} - \alpha_{mcd} \tag{1}$$

For the actual watermark embedding we define the width to length ratio R_0 of the road segment:

$$R_0 = \frac{W}{L} \tag{2}$$

If the edges of the road segments are not parallel, the width of the road segment is defined as the average of the width at the beginning and at the end of the road segment. Since most of the times the length is bigger than the width, R_0 obtains small values. For this reason we evaluate a new ratio using the following function:

$$R = a \cdot R_0 \cdot 10^k - b \tag{3}$$

where the values of the parameters a, b and k depend on the value of R_0 and are selected so that $R \in (0,1]$.

Once the map has been rotated, all the road segments are ordered with respect to their starting point. The start point of a road segment A is the average between the two start points, SP_{edge1}, SP_{edge2}, of its two forming edges:

$$\begin{aligned} SP_{roadA,x} &= \tfrac{1}{2} \cdot \left(SP_{edge1,x} + SP_{edge2,x}\right) \\ SP_{roadA,y} &= \tfrac{1}{2} \cdot \left(SP_{edge1,y} + SP_{edge2,y}\right) \end{aligned} \tag{4}$$

The ordering of the road segments is arranged by the value of the x coordinate of their starting point. If two road segments have the same x coordinate then the y coordinate is used to establish the order. As it will be explained later, it is not possible to watermark all road segments so only a subset is selected for being watermarked. Since the ordering is established after map rotation according to the watermark key, the ordering is key-dependant, and thus difficult for an attacker to estimate.

The watermark sequence is a binary pseudorandom sequence generated by using the secret watermark key. In order to perform embedding we traverse all road segment using the order defined above and embed one bit of the watermark sequence in each selected road segment. Bit embedding is performed as follows: the range of values of the width to length ratio R is linearly quantized in N intervals of size B_s and each interval (bin) is assigned a binary value, 0 or 1, by alternating between 0's and 1's as shown in figure 2. The number N of intervals is proportional to the watermark's robustness to noise and inversely proportional to the visual error caused by the watermark.

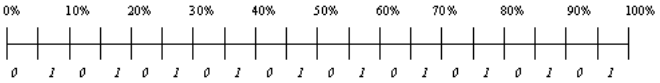

Figure 2: Quantization of the width to length ratio R.

If the ratio of a road segment that should encode bit "0" ("1") falls in the interval that corresponds to "0" ("1"), no operation is performed, otherwise, the width of the road segment is modified in order to move its ratio R to the closest appropriate bin. In [11] the authors apply a similar quantization approach for the watermarking of 3D meshes.

The width of the road segment is modified by moving the two edges that form the road segment by the same amount in opposite directions. The movement is perpendicular to the line segment defined from the start and end points of the road segment. Performing the modification in such a way prevents us from altering the order of the road segments since the start (end) point of the road segment, defined by (4), will have the same coordinates after the modification. Furthermore such a modification retains the visual "straightness' of the roads.

Finally we perform an inverse rotation to leave the map with its original orientation.

By modifying the width of a road segment we are also modifying the length of the two other road segments attached to it, making those two road segments useless for watermarking. This is exemplified in figure 3. If we decide to watermark segments A and C then segments B and D cannot be watermarked since a change of the width of A or C will affect the length of the road segments B and D and thus the corresponding ratios R. Thus, road segments are divided into two groups and watermark embedding is performed using only segments belonging to one of the groups.

2.3 Watermark Detection

In order to perform watermark detection, road segments are detected and the most common direction α_{mcd} of the map is evaluated. Subsequently the map is rotated so that the most common direction is aligned with the horizontal axis in order to cancel any rotation that has been applied to it. Finally the map is rotated by β_{Wkey}, the road segments are ordered and those road segments that are candidates for holding watermark bits, are selected following the same procedure used during embedding. Having these road segments in

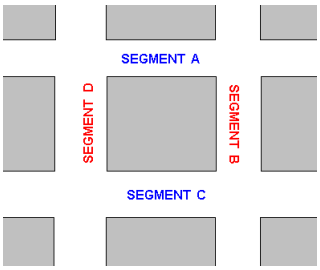

Figure 3: Modifications of the width of segments A and C modify the length of segments B and D

order, the watermark ratio R is computed for each road segment in sequence and the bit embedded on this road segment is extracted according to the bin where R falls in. To decide if the map has been watermarked with the given key K or not, the retrieved watermark sequence is correlated with the sequence generated by K. If the value of the correlation exceeds a certain threshold the map is considered watermarked.

It should be noticed that since an angle of $(\pi+\alpha)$ can be found instead of α for the α_{mcd} angle, the map after the rotation could be set upside-down with respect to the map used for watermark embedding. Consequently, the watermark detection is performed twice, both for angles α and $(\pi+\alpha)$, and the highest correlation value is considered as the output.

As already mentioned, the proposed scheme is robust to rotation due to the alignment of the most common direction with the horizontal direction described above.

Robustness against translation is also achieved since, when the watermarked map suffers a translation attack, the values of the ratio R_0, do not change since nor the length, nor the width are being modified. In case of uniform scaling attack, the length and the width are increased/decreased by the same scalar factor, and thus the ratio R suffers no modifications.

The method is also sufficiently robust to noise addition on the vertex coordinates as far as this distortion is not big enough to cause significant movements of the ratios R of many road segments from one road segment ratio quantization bin to another. Intuitively, the bigger the size B_s of the road segment ratio quantization bins the better the robustness against noise but the worse the perceived visual quality.

3. EXPERIMENTAL RESULTS

To verify the performance of the proposed algorithm, tests have been performed on real maps of cities like the ones shown in figures 4a and 4b[1]. The length of the watermark that can be embedded in a map depends on the structure and size of the map. For example, in the map depicted in Figure 4a 390 road segments suitable for holding watermark bits were selected, while in the map depicted in Figure 4b 1200 road segments were suitable for watermarking. The original map and the watermarked version have almost no visible differences, as can be seen in figure 5. The visual quality is very high, the quadrilateral shape of the buildings and their alignment with the road segment borders are perceptually maintained, being very difficult to spot the modifications, especially without the original map, even at large zoom factors (Figures 6).

In order to test the detection performance of the algorithm, the following procedure has been applied. The original map is watermarked using a watermark key K_A and the watermark detection is performed using both the correct key K_A and a different watermark key K_B. The same experiment is repeated multiples times, in our case, more than 6.000 times, each time using a different key.

(a)

(b)

Figure 4: Two maps from Detroit, MI, (a) a 390 bits long watermark was embedded, (b) a 1200 bits long watermark was embedded.

[1] http://www.ci.detroit.mi.us/plandevl/advplanning/cinfo/adv/gislayers.htm

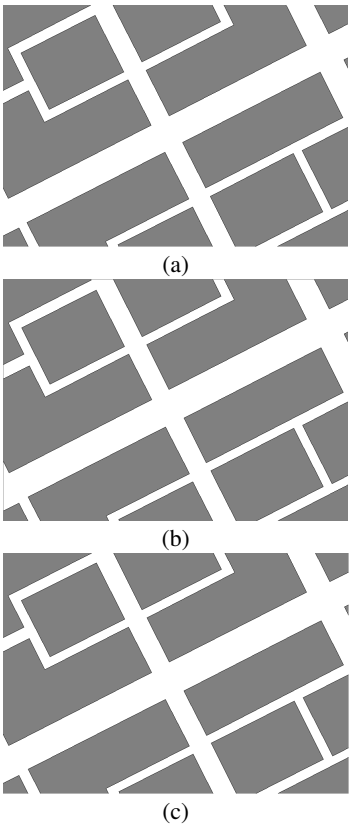

Figure 5: Detail of the map shown in Figure 4a, (a) non-watermarked map, (b) watermarked map with B_s = 0.10 (c) watermarked map with B_s = 0.05.

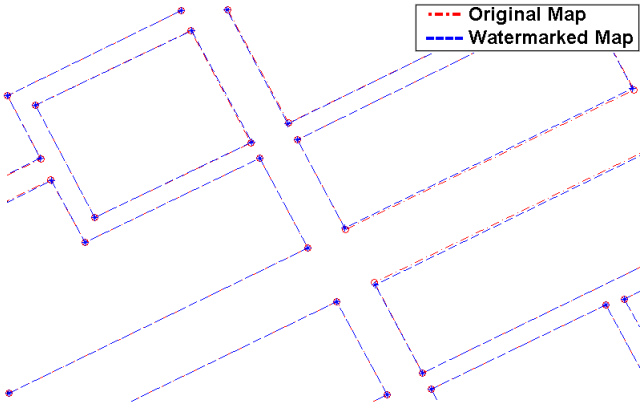

Figure 6: Changes introduced by the watermark on road segments, seen with a very large zoom factor. Red lines: original road segments from Figure 5a. Blue lines: watermarked road segments from Figure 5b.

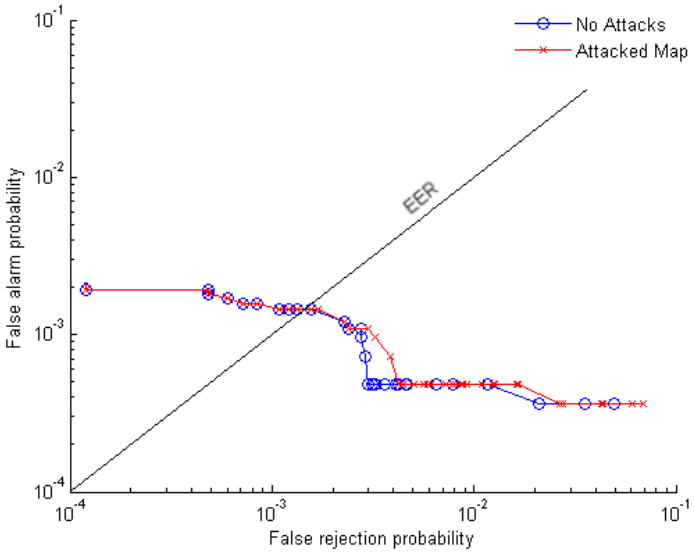

Figure 7: ROC curves. Blue line: map without attacks. Red line: map scaled by 2, rotated 90° and moved 1000 units along x axis and 2000 along y axis

The performance of the system can be judged in Figures 7 and 8 where the Receiver Operating Characteristic (ROC) curves are depicted. The ROC curve is a plot of the probability of false alarm $P_{fa}(T)$ (namely the probability to decide that a watermark exists in a signal that is not watermarked or, is watermarked with a different watermark) given a certain threshold T, versus the probability of false rejection $P_{fr}(T)$ (namely the probability of failing to detect a watermark in a signal that is watermarked) for the same threshold T. The Equal Error Rate (EER) is the point of the ROC curve where P_{fa}= P_{fr}. The lower the EER, the better the performance of the algorithm.

Figure 7 depicts the ROC curves for a map that has not been distorted and a map that has been scaled by a factor of 2, rotated by 90° and translated 1000 units along the x axis and 2000 units along the y axis. It is obvious that the method, as expected, is practically no affected by rotation, translation and uniform scaling as well as their combinations. The small differences between the two ROC curves can be attributed to numerical errors caused mainly by the rotation operation which can result in changes of the ordering of the road segments in a few cases. The EER for both the distortion-free map and the attacked map is equal to $1.4E^{-3}$.

In order to test the robustness of the algorithm against noise we have performed two different sets of experiments using additive white Gaussian noise (AWGN). In the first set of experiments we applied AWGN to all vertices in the map (vertex noise) while in the second set of experiments the noise altered the width of the road segments (width noise) modifying it in the same way the proposed method does. Since the algorithm is based on the width to length ratio of the road segments, the variance of the noise was chosen as a percentage of the average width to length ratio R_0 of the road segments of the map. Different bin sizes B_s were also tested. The noise variance values were set to 0.05%, 1% and 5% of the average ratio R_0 and the bin sizes B_s were set to 0.025, 0.05 and 0.10. In Figure 8 two ROCs obtained for a bin size B_s of 0.05 and a noise variance of 1% are depicted. The blue curve corresponds to the map attacked by adding noise to all the vertices, whereas the red curve corresponds to a map where the noise has been added to the width of all road segments. It is obvious that the method is more robust against width modifications than against random changes in the position of the vertices. The EER are $4.7E^{-3}$ for noise applied on vertices and $2.5E^{-3}$ for noise applied on road widths. Results obtained from the other bin size/noise variance combinations, show

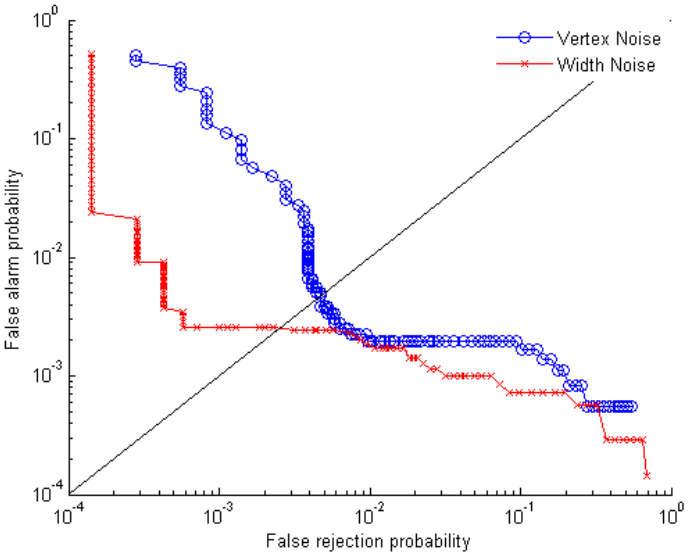

Figure 8: ROC curves for 1% noise and a bin size B_s of 0.05. Blue line: noise applied on vertices. Red line: noise applied on road widths.

that a bigger bin size B_s is required if a more severe noise is applied to the data.

4. CONCLUSIONS AND FUTURE WORK

A new technique for blind watermarking of city maps that is robust against uniform scaling, rotation, translation and AWGN has been presented in this paper. The main characteristic of the method is that, unlike other methods proposed for general GIS data, it keeps the visual quality of city maps, i.e. retains the rectangular structure of buildings and their perceptual alignment with the road borders.

Robustness against cropping could be achieved by partitioning the map into a number of areas and embedding the same watermark in each area. In the future, the method will be extended towards this direction.

Acknowledgment

This work has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT.

REFERENCES

[1] A. Giannoula, N. Nikolaidis, I. Pitas, “Watermarking of sets of polygonal lines using fusion techniques” in Proceedings of IEEE International Conference on Multimedia and Expo 2002 (ICME ’02), Volume 2 Page(s): 549 - 552

[2] I. Kitamura, S. Kanai, T. Kishinami, “Copyright protection of vector map using digital watermarking method based on discrete Fourier transform” IEEE Geoscience and Remote Sensing Symposium, 2001 (IGARSS ’01), Volume 3, Page(s): 1191 - 1193

[3] Kang Hwan Il, Kim Kab Il, Choi Jong Uk, “A map data watermarking using the generalized square mask” in Proceedings of IEEE International Symposium on Industrial Electronics, 2001 (ISIE ’01), Volume 3, Page(s): 1956 - 1958

[4] Ho-Hsun Chang, Tsuhan Chen, Kou-Sou Kan, “Watermarking 2D/3D graphics for copyright protection” in Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing, 2003 (ICASSP ’03), Volume 4, Page(s): IV - 720 - 3

[5] R. Ohbuchi, H. Ueda, S. Endoh, “Watermarking 2D vector maps in the mesh-spectral domain”, Shape Modeling International, 2003, Page(s): 216 - 225

[6] Yuanyuan Li, Luping Xu, “A blind watermarking of vector graphics images”in Proceedings of Fifth International Conference on Computational Intelligence and Multimedia Applications, 2003 (ICCIMA ’03), Page(s): 424 - 429

[7] V. Solachidis, N. Nikolaidis, I. Pitas, “Fourier Descriptors Watermarking Of Vector Graphics Images” in Proceedings of IEEE International Conference on Image Processing, 2000, Volume 3, Page(s): 9 - 12

[8] V. Solachidis, I. Pitas, “Watermarking polygonal lines using Fourier descriptors”, IEEE Computer Graphics and Applications, Volume 24, Issue 3, May-Jun 2004 Page(s): 44 - 51

[9] Hongmei Gou, Min Wu, “Data hiding in curves with application to fingerprinting maps”, IEEE Transactions on Signal Processing, Volume 53, Issue 10, Part 2, Oct. 2005 Page(s): 3988 - 4005

[10] V. Doncel, N. Nikolaidis, I. Pitas “An Optimal Detector Structure for the Fourier Descriptors Domain Watermarking of 2D Vector Graphics”, IEEE Transactions on Visualization and Computer Graphics, Volume 13, Issue 5, Sep.-Oct. 2007

[11] F. Cayre, B. Macq, “Data hiding on 3-D triangle meshes”, IEEE Transactions on signal Processing Volume 51, Issue 4, Apr. 2003 Page(s): 939 - 949