FEATURES

The service offered by **The Digital Map** is characterized by:

- **It does** not modify in any perceivable way **the digital map**, even if printed.
- The watermark is inserted in the geometry, without altering the attributes of the polylines.
- The watermark is independently inserted in each layer.
- **It is possible to insert more than one watermark**, an useful property which allows the identification of a reseller who also inserts a watermark for its customers
- **The watermark is immune to isometric transformations**, like rotation, translation and uniform scaling.
- The watermark might survive even to the deletion or division of some polylines in the dataset. The allowable modifications include deleting some polylines, change of attributes as well as small change of coordinates.
- The detection process does not require access to the original dataset, which is kept secret.
- The watermarking process does not depend neither rely on the dataset format (DXF, DWG, DGN, etc.), number of bits used to represent data, etc. but only on the geometric information.

The Digital Map Ltda.

http://www.thedigitalmap.com

The Digital Map Ltda.

A solution for the copyright protection of digital maps

Introduction

In digital format, a vector map can be represented as a list of registers like (X, Y, attribute1, attribute2, etc.) being the first two the coordinates in a suitable reference frame.

Digital maps in vector format are expensive to produce because its acquisition cannot be easily achieved by purely automated means.

The transformation of an image organized in pixels (like the one produced by a scanner) to the (X, Y, etc.) format requires a substantial effort.

Once the map, plan or similar is in digital format, it is possible to produce perfect copies with almost no effort.

Thus, because they are so expensive to produce and so easy to copy it is important to find a suitable procedure to protect the data producers against piracy of such datasets

Solution

A typical solution is to encrypt the dataset with a suitable procedure. The encrypted files are useless for all purposes, except if you provide the appropriate key. However, encryption is not the solution of the piracy problem because once decrypted by the first legitimate customer, the exposed dataset has no protection against copy.

Steganography is a different technique because it attempts to add extra information to the dataset, but leaving it as useful as the original. In the most traditional definition of steganography an important message is hidden within another, unimportant one. In our case, both are important.

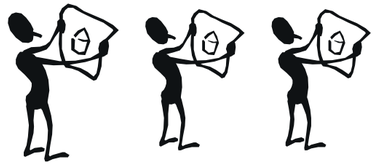
The process of inserting hidden information in the file is denoted as "watermarking" and the information itself is named **"watermark"**.

By the way, it is obvious to notice that a dataset is encrypted. It is not so if it has been watermarked, because for almost all applications it is equivalent to the original.

" Digital vector datasets are expensive to produce "

"... it is important to protect the data producers against piracy..."

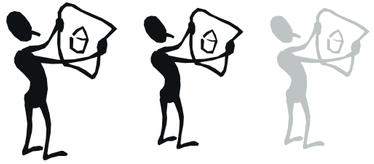
1



2

3

4



Goal

The problem is **how to embed information** in the file **without being noticed**. If an illegal copy is found, and by analyzing it, it is possible to extract the serial number («the watermark») and thus identify the first customer who received it, the distributor who delivered it, or both.

how to embed information without being noticed

Features

The detection stage produces a binary answer: given the map and a secret key only known to the author, there exist an algorithm who states whether or not the serial number is there. The watermark is inserted more than once in the dataset, allowing detection even from an edited version of the map.

In order to insert the watermark a pseudo random number generator seeded with an appropriate value is used. The seed is the secret key, and might be provider by the author. For each customer, a different seed is used. The database holding the seeds, serial numbers, customers, date, file characteristics, version, etc. is kept secret in order to use its values to identify the customer.

The watermark itself is a binary number, which length needs to be agreed in advance. The best length depends on the map itself. A typical value should be larger than 20 bits, allowing more than 2 ^ 20 different possibilities. It is believed that this is a large enough space to distinguish among customers.