A Scheme of Watermarking for Digital Vector Map

Jacky Jiang 2012.9.26

Background

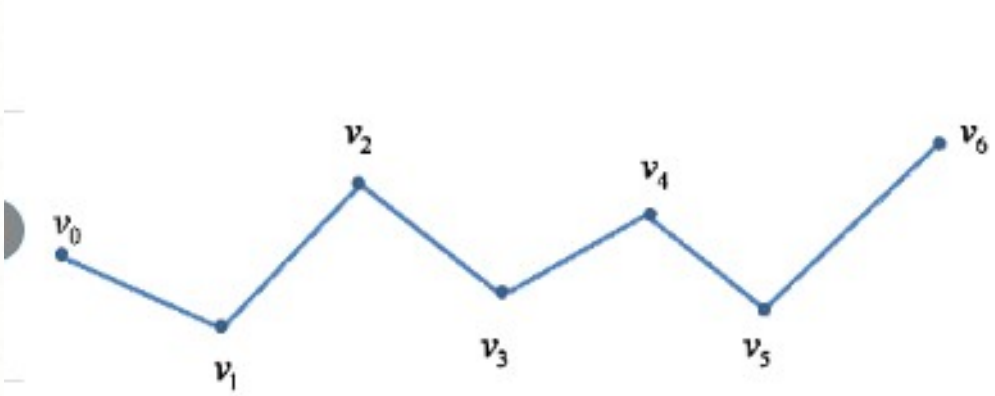
Digital vector map, for example, digital road map

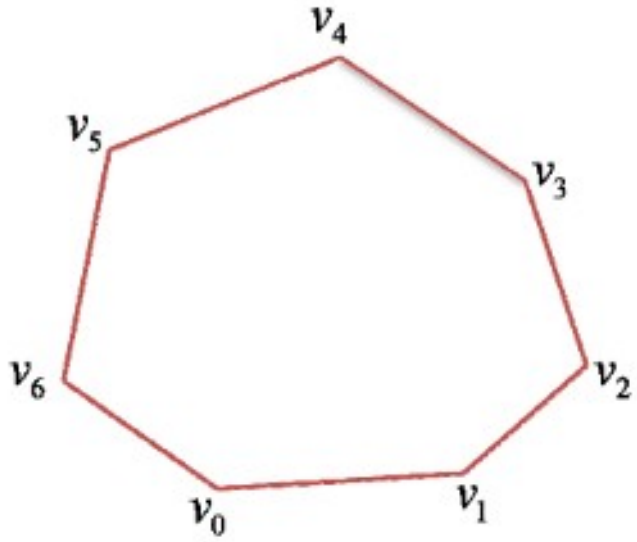
Structure of Digital Vector Map

1. Objects: Generally a object is depicted by polyline and polygon. Both of them are stored as a series of vertexes(x,y).

2.Features: Each object has some distinct features, eg. Street name of a street

Polyline and Polygon



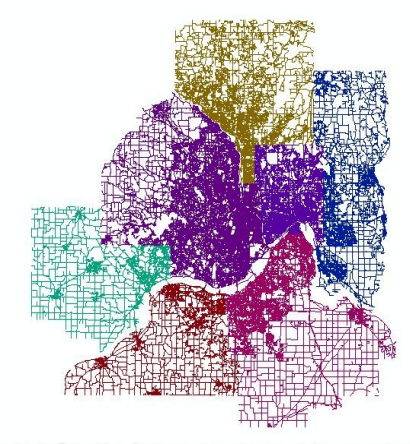


Why watermarking?

- Generally GIS vector maps are extremely expensive to produce. However, on the other hand, the digital nature of any vector map leaves it vulnerable to being copied and resold by a 3rd party without permission.
- Protect copyright of digital maps, watermarking is a good choice.

What is Watermark?

Watermark from 100 yuan RMB, helping us distinguish real notes from fakes



001001110

How to evaluate a watermark algorithm?

- A good watermark algorithm is to insert a "digital watermark" into a digital vector map with some strategies to make the watermark robust to most kinds of attack.

Some Possible Attacks

1. Subset Alteration

- An attacker gets rid of a watermark by selecting a subset of the data.
- By altering this subset, the attacker hopes to render the watermark ineffective.
- This portion of data can be very small compared to the original dataset.

Some Possible Attacks

2. Subset Selection

- An attacker hopes to select a sub-set from the original dataset and use it illegally.
- For a digital road map, randomly selecting a subset is meaningless. The most likely type of a subset selection attack is to select most of the data from one subarea.

Some Possible Attacks

3. Subset Addition

- Adding an extra subset to the original dataset. In the digital road map domain, this means adding extra roads on the map, which is not acceptable generally.
- Another subset addition attack is to split one road segment into several pieces. This way, the semantics of the road map will not change.

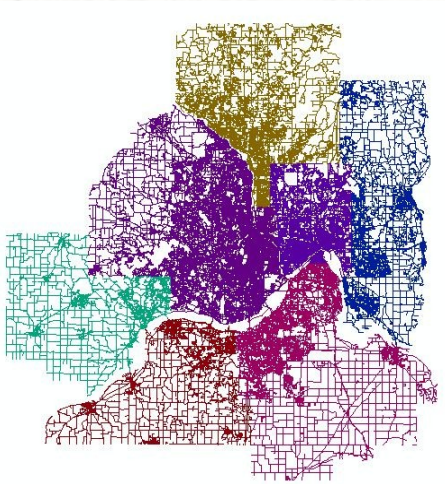
Some Possible Attacks

4. Subset Re-sorting

- Reordering the data items in the original dataset and hoping this reordering will cause watermarking to fail.
- This kind of attack will work if the watermarking algorithm depends on the order of items.

The Problem We Want to Solve

An attacker may take different subregions of the same area from different maps, and finally combine them together to make a new map.



Main Purpose

Propose a watermarking scheme which can survive most attacks and the problem mentioned before—to dedide whether there are subregions which are cropped from the original watermarked map.

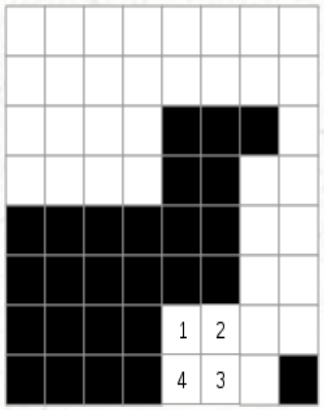
Partition

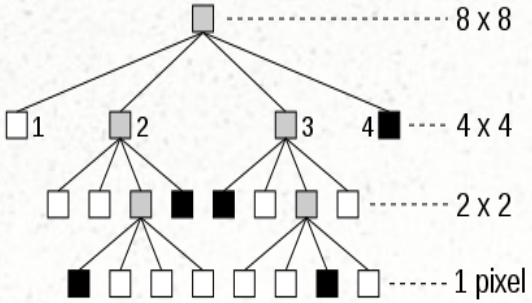
- We partition the map according to Quadtree structure. The watermark is possible to be inserted with the local information.
- **Input :**

  G: Secret grid frame

  S: Input dataset
- **Output :**

  PO: Partitioned dataset





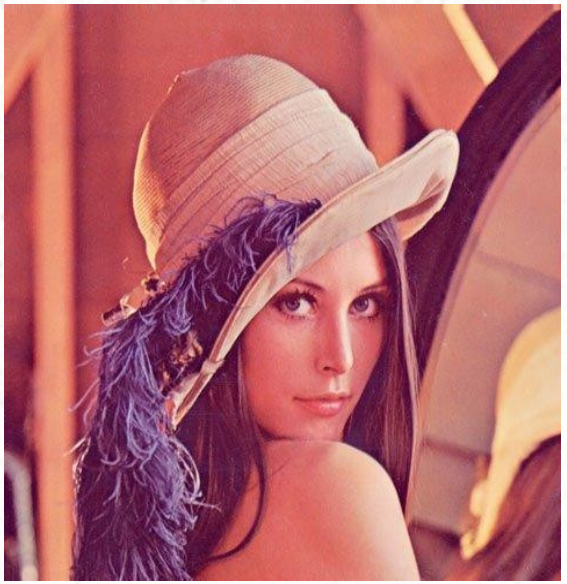
In other words, a list of subregions which contain less than 4m length of roads

Insertion

INSERTION(S, G, l, m)
PO = PARTITION(G,S)
for Every region in PO in which the length of segments > m
Select point P that is closest to the center of region
Draw a square Q of side length l centered at P
Calculate sum sl of line segments intersecting Q
j = Hash(k , sl)
Set the jth LSB of P to 1

LSB

- LSB is short for Least Significant Bit
- Digital image is stored as binary bit.
- When a LSB is changed, the degradation of image quality is very slightly.



Detection

DETECTION(G,V)

- PO = PARTITION(G,V,T)
- for Every region in PO containing more than m miles of road segments
- Select point P closest to the center of region
- Draw a square Q of side length l centered at P
- Calculate sum sl of line segments intersecting Q
- j = Hash(k , sl)
- if the j th LSB of P == 1
- Mark this region as "MATCH"
- MARK_QUADTREE(T)
- DF_TRAVERSE(T)

Detection

- Traverse the Quadtree in Post-Order
  Mark the sub-node which is suspicious to be a copy of ours.

- Depth-First Traverse the Quadtree and find the largest subregion that is marked.

Thanks!