Digital Rights Management of Geo-Datasets
Protection against Map Piracy in the Digital Era

Suitable protection means against piracy has been a subject of interest within the cartographic community for years. The traditional threat can be described as someone else republishing a map as his own, without paying royalties. Proving authorship is the problem, and this has been achieved by inserting tiny errors only known to the author. The threat is different when considering digital maps, because any of the legitimate owners can be the source (or republisher) of an illegal copy, which in addition is an exact equivalent to the original. This raises a new problem: despite there exist contracts between providers and customers limiting the right to disseminate, they cannot be enforced in practice because tracking the illegal copy back to its source has not been possible in the past. Digital Rights Management Systems (DRMS) are being deployed to address some of the new issues.

By Dr. Carlos López, Universitario Autónomo del Sur, Uruguay

The creation of good quality maps (or GIS datasets in general) is a complex and expensive task. In many countries this is the responsibility of specialised agencies. Either government funding or sales cover development costs; the former is the prevailing way in the USA and the latter is popular in Europe. Mr. Lemmens addressed this topic in the October issue. Typical prices for vector datasets are 20-60 U$S/km^2 for rural areas, and 40.000-150.000 U$S for cities like Madrid, Rome or Brussels. The market for the data is usually restricted to a few clients (utilities, logistic companies, government, etc.) but adds many million U$S dollars. If cost recovery is to be obtained through sales, piracy is a significant problem.

Some specific features of digital GIS datasets

Once digital, data can be easily stored, copied and transferred without loosing its original characteristics in a straightforward and inexpensive way. This is a significant difference to other media (paper, film, etc.) where second generation copies are less valuable than the original. In opposition to music, videos or artistic images, the number of customers for a vector dataset is low (less than a hundred). Unlike music or films, geographic datasets requires regular updates, so a customer needs to go back to the data provider. Such after-sale service is usually considered in a standard contract signed at the beginning which create hard links between parties.

Current protection framework for cartography

The present status is that piracy is in practice only restricted by international and national legal bindings plus specific contracts between customers/suppliers. The Intellectual Property Rights (IPR) international agreements have evolved from the Berne Convention (1873) and are well suited to protect authorship. They grant the author a monopoly over the work for a limited time. Exemptions were granted to individuals and libraries under the "fair use" concept. It allows copy for personal use, research and education purposes, etc. and other non-commercial applications.

IPR as such are enforced with variable strength in different countries, and bind all inhabitants. Most countries recognise contracts between parties, which are indeed the

strongest legal barrier against piracy (at least at the national level) but limited to the parties themselves.
Practical strategies can resort in technology, law or both, and we will briefly review them.

Possible purely technical strategies
For example, Bentley have recently announced DRMS support in MicroStation V8.1. According to the press release, the system will incorporate some features based upon cryptography, like authentication, and security. Most general-purpose systems do the same: complain if a file has been changed or edited, deny rights, etc. All of the extra information required will be handled in the popular DGN format. The encrypted file can be copied, but it is likely that MicroStation will refuse to handle the data if not run in the right computer or site.

The idea of locking use of illegal datasets is analogous as the procedure built-in within the DVD players. The data itself is encrypted, and the key is hardcoded in the device. The second barrier is weaker: the device recognises the existence of an imperceptible watermark in the data and proceeds accordingly, denying playback, copy or both. In order to have a similar system, GIS software vendor should include routines which recognise valid datasets which might be locked to an individual CPU, or have flags specifying rights levels like "read-only", "disable save-as", "print", "edit", etc. which even might vanish after some date. This requires policy as well as technological changes, and agreements between vendors. Policy is implied because this measures are intended to protect the data producers, but users (customers who pay for the software) might have different interests, and might prefer formats and software which does not enforce such protections. The technological side is also complex, and has also policy implications.

The system might work fine if all software vendors agree to work only with DGN format, or to extend the new capabilities to their own formats. Otherwise, once exported to another format, the dataset will be unprotected. In addition there might exist legal impediments to the producer to offer just one proprietary format to customers, or not to offer transformation routines instead.

Possible purely legal strategies
Due to the lack or weakness of present technological barriers, it is fit to consider again legal ones. One possible trend is to reinforce and expand the subjects already covered by present legislation, including new figures and more stringent punishment. The U.S. DMCA added new rights to content authors, and made a federal crime circumvent copyright protection schemes and/or remove copyright notices from the dataset.
The European Database Directive of 1997 created new rights to the database makers that essentially add copyright-like protection schemes to non-creative work as collecting data from the environment. Earlier legislation only protected the structure of the database, but not its content (data).

Possible mixed strategies
It is not enough to have the proper law. Assume that you have distributed just two instances of a map. If you find a third one, identical to those distributed, but you have

not granted access to the holder, what you might do? The problem is not of *authorship* but on breaking contracts. You might start a trial, but who will be accused? The problem is to identify which one of your legal customers has provided the illegal copy (either deliberately or not) to the present holder. If map instances are identical, little could be done.

The solution to this legal dilemma comes from technology. Let´s assume that you can produce equally functional copies of the same map, but holding hidden information like a serial number. If the information is hidden, it is likely to remain unnoticed in every copy taken from the same original. If it is noticeable it can be removed, so this is a crucial property. The science behind this is named steganography, and the technology is known by the general name of watermarking. If you add different marks to every instance of the map, the name fingerprinting is also used.

Conclusions

Watermarking is one of the technologies incorporated in the DVD players; its research is a subject of hot interest for images, audio and video, and we envision a strong interest for digital cartography. It might be the solution to track back to its source an illegal map. The watermarking technology is specific to each data type; solutions valid for audio or video are not suitable for vector datasets. Its applicability is not based only on either national or international IPR law, but on commercial-like contracts already admitted by courts in all countries.

Further Reading

- López, C., 2002, Watermarking of Digital Geospatial datasets: a review of Technical, Legal and Copyright issues, International Journal of Geographic Information Science, 16, 6, 589-607.
- Intellectual Property Protection of Digital Vector Cartography, TheDigitalMap Ltd., Accessed 30 October 2002 http://www.thedigitalmap.com
- Cox, I. J. and Miller, M. L., 2002, The First 50 Years of Electronic Watermarking, EURASIP J. of Applied Signal Processing, 2002, 2, 126-132, 2002

Biography of the Author

Dr. Carlos López holds an Industrial Engineering and M.Sc. degree from University of the Republic, Uruguay and a Ph.D. degree from Royal Institute of Technology, Stockholm, Sweden. Dr. López is Project Coordinator and professor at the Universitario Autónomo del Sur, where he leads the DRMS group. His research areas include watermarking, accuracy improvement of GIS datasets, neural networks, numerical methods, etc. As a private consultant he has been instrumental in setting up the Uruguayan ClearingHouse. He is also Regional Correspondent of GIM International

Affiliation

Dr. Carlos López
Universitario Autónomo del Sur
Uruguay 1225, Montevideo, URUGUAY
Email: carlos.lopez@universitario.edu.uy

Tel: +598 99 138259