Security, Encryption and Intellectual Property Management Systems

Professor Harlan J. Onsrud
Spatial Information Science and Engineering
University of Maine

Cyberlaw Text and Cases, Ferrera, et. al., Ch. 11

Goals of Information Security

- Confidentiality
- Authenticity
- Integrity

(The Digital Dilemma, Appendix E)

Security Objectives

• privacy and confidentiality • data integrity • authentication or identification • message authentication • signature • authorization • certification • witnessing • receipt • confirmation • ownership • anonymity • non-repudiation • revocation

- What is a firewall?

- What are some means of authenticating individuals in a transactional security system?

- Primary means of ensuring confidentiality of message while in route?

- Purpose of cryptography?

Recommended supplementary reading:
The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography
by Simon Singh

How many of you are using PGP?

- Is cryptography speech?

- What is steganography?

Technical Direction Options for GI Public Commons Project

Outline:

A. Attaching an Invisible Number to Standard GIS files
   1. Vendor Independent Options
   2. Vendor Dependent Options

B. Visible Indication that File is in the Public Commons
   1. Vendor Independent Options
   2. Vendor Dependent Options

A. Attaching an Invisible Number to Standard GIS files

1. Vendor Independent Options

• a number or metadata can be attached to and travel hidden with a contributor's raster file.

• hidden information does not interfere with the file (nor does it typically change the file size significantly) yet can be recalled at anytime

What are typical methods used to hide the information?

Steganographic Methods

• lowest bit method - insert message in least significant bit plane of a carrier file (JPEG, GIFF, TIFF, PNG, WAV, BMP)
• adding spaces, tabs or white spaces to ends of lines - easily detected (ASCII)
• insertion of special characters and unnecessary punctuation marks - easily detected (text and PDF)

Encryption - Hidden message typically is encrypted and password required to read.

Popular software using these methods:

Steganos
- works with all Windows operating systems

Invisible Secrets 2002, Neobytes Solutions
- JPEG, PNG, BMP, HTML and WAV files

Datamark Technologies
- digital images in JPEG, PNG, BMP, GIF, PDF, Tiff and TGA can contain a watermark
- retriever works on hard copy

SNOW
-hides messages in ASCII using white spaces

Developing identifier system for popular format GIS files?

(e.g. shape, coverage, geodatabase, DEM, TIN, etc.)

Our Approach:

- Use progressive series of redundant multiple identification approaches to tag and later identify the file

1. Start with standard steganographic methods

   - works with raster (e.g. .DRG files) if image is used "as is" or perhaps minimally manipulated
   - does not work with vector (e.g. standard manipulations drop insignificant coordinate digits where info might be hid)

2. Next store ID in unused bits (if possible)

- unused bits can be found in most GIS file formats by consulting detailed specifications
- example: shape file has unused bits in main header file which are never seen by typical user

3. Derive a single number representing multiple identifiers drawn from the attribute table
- does not involve inserting any information
- for typical size GIS file, the multiple non-redundant identifiers will represent a unique key

In submitting to facility
- exact match of key indicates an unchanged previously submitted file
- substantial but inexact match evidences a derivative work

Approach three should work even if rows are added or dropped. Will not work if columns added or dropped (i.e. attributes added to file)

4. If no match of the key under 3, continue search for key using more computationally intense search approach.

Conclusion:

Identifier system need not be fool proof since goal is to provide evidence that a file is in public commons rather than in private ownership.

- little incentive to strip unobtrusive IDs since everyone can use file for free anyway

- only potential thief tempted to strip IDs might be business trying to capture past contributions of others …. yet similar earlier files would exist in archives