MÉTODOS PARA LA PROTECCIÓN DE PROPIEDAD INTELECTUAL EN CARTOGRAFÍA DIGITAL[1]

Cartografía, SIG, Legislación
Carlos López
carlos.lopez@ieee.org

RESUMEN:
En su forma digital, un mapa vectorial puede ser representado como una lista de registros del tipo (X, Y, atributo1, atributo2, etc.) siendo los dos primeros las coordenadas en un sistema de referencia apropiado para los puntos, mientras que los otros campos pueden tener otra información como por ejemplo el nombre de una calle, su tipo de pavimento, etc. Estos registros describen los nodos de una poligonal que podrá ser cerrada o abierta (en el primer caso, el primer y último elemento de la lista coinciden). Dos nodos consecutivos en la lista pueden imaginarse como representando un segmento de recta en el plano.
Un escáner puede producir fácilmente una versión digital de una imagen de cualquier tipo, incluso de un mapa. Sin embargo, la transformación de una imagen que está organizada en pixels al formato (X, Y, etc.) requiere un esfuerzo sustancial más allá del mero uso del escáner. Los mapas digitales en formato vectorial son caros de producir, porque su adquisición no puede ser realizada fácilmente por medios automáticos. Una vez que el mapa, plano o similar, se encuentra en formato digital, es posible realizar copias perfectas del mismo casi sin esfuerzo. Por lo tanto, al ser tan caros de producir y tan extremadamente fácil su copia, es importante encontrar algún procedimiento para proteger al productor contra la piratería de tales archivos.
Una solución típica es encriptar los datos con un procedimiento apropiado, de los que existen muchos. Los archivos digitales encriptados son ininteligibles para cualquier uso, excepto si se dispone de la clave apropiada, la cual sería lo que se le entrega al cliente legítimo. Sin embargo, eso no resuelve el problema, ya que una vez desencriptado por el primer usuario legítimo, el mapa sin protección queda expuesto a la copia.
El problema que se intenta resolver aquí es cómo insertar información sobre el productor, el cliente, la fecha de compra, el distribuidor si lo hubo, etc. de forma que esa información esté embebida en el archivo, y su presencia no sea notada. En caso de detectarse una copia supuestamente ilegal, y teniendo acceso a la misma, podría identificarse al primer cliente al que se le vendió, o al distribuidor que la entregó, etc. habilitando reclamos por la vía judicial a los mismos. La marca debe insertarse de tal forma que sea difícil de borrar, o que su borrado sea posible pero al precio de dañar sensiblemente el archivo digital.
Existen métodos especiales para cartografía temática y cartografía vectorial, donde el autor ha presentado una patente.

[1] *Presentado al V CONGRESO LATINOAMERICANO y VII NACIONAL DE AGRIMENSURA Punta del Este, Uruguay, Mayo 22, 23 y 24 de 2002*

MÉTODOS PARA LA PROTECCIÓN DE PROPIEDAD INTELECTUAL EN CARTOGRAFÍA DIGITAL[1]

Cartografía, SIG, Legislación
Carlos López
carlos.lopez@ieee.org

Resumen:

La disponibilidad creciente de softwares de SIG, computadoras con capacidad suficiente de cálculo, unidades de grabación de CD y la Internet obligan a replantear algunas hipótesis en la cartografía tradicional. En la misma, la propiedad intelectual estaba protegida de hecho por barreras técnicas, y de derecho mediante legislación explícita para este tipo de productos (Karjala, 1997). Las barreras técnicas estaban asociadas fundamentalmente a la dificultad para hacer una copia "perfecta" de un mapa a partir de un ejemplar del mismo. No es simple disponer de una copiadora tamaño A0, y nadie confunde una copia heliográfica con un original. El mercado ha obligado a los organismos productores de cartografía a incluir en su oferta la versión digital de la misma, y ha descubierto (dolorosamente) que las barreras que antes eran eficaces ahora simplemente no existen. La copia "perfecta" de una cartografía completa puede hacerse en minutos, utilizando hardware estándar y a costos irrisorios. Esto pone sobre el tapete la necesidad de los técnicos de aportar soluciones alternativas para frenar esta situación.
En este trabajo se presenta una de esas técnicas, denominada estenografía o marca de agua, la que enseña cómo insertar información en el archivo que identifique unívocamente al cliente legal que pagó por él. Diferentes clientes reciben por lo tanto ejemplares que no son idénticos y cuyas diferencias son invisibles para los usuarios y softwares normales.

Criptografía vs. Esteganografía: una breve introducción

El objetivo de la criptografía es el de proteger el contenido de un conjunto de datos contra el acceso no autorizado al mismo *durante la transmisión*, modificando el conjunto original de forma de hacerlo ilegible en un proceso que se denomina *encriptado*. Para desencriptar los archivos se requiere algún número o clave secreta. El libro de Schneier (1995) es un buen punto de partida para estos temas.

Una vez que el archivo digital ha sido desencriptado, no tiene ninguna protección: al ser digital, es posible realizar copias perfectas del original sin participación ni conocimiento del autor. Por lo tanto, la utilidad de la criptografía en el problema que se considera está limitada a la etapa de distribución. La Esteganografía es una técnica diferente, porque intenta agregar información extra al archivo, pero dejándo al mismo en condiciones de ser utilizado. En la definición más tradicional de esteganografía, un mensaje importante es ocultado dentro de otro que no lo es. En nuestro caso, ambos son importantes. Por otra parte, es obvio saber cuando un archivo ha sido encriptado; no lo es si ha sido marcado, ya que para muchos efectos luce como equivalente (Bender *et al.,* 1996; Anderson and Petitcolas, 1998).

El caso más interesante para aplicaciones cartográficas (genéricamente asociadas a los Sistemas de Información Geográficos, SIG) es aquel en que la marca no es evidente, y se discutirá luego cómo lograr esto. Mediante la inserción de la marca, el archivo tiene ahora alguna información extra que puede identificar al distribuidor (si es diferente que el del productor), el comprador, la fecha de la transacción, etc. haciendo posible el rastreo del génesis de un archivo pirateado hasta su fuente.

La marca de agua puede ser utilizada para probar integridad de los datos: si un archivo ha sido editado o modificado *luego* de que la marca fue insertada, la misma puede revelarlo, y según el caso, puede indicar las partes que han sido modificadas. Si la marca es muy sensible a los cambios en el archivo, se la denomina *frágil.* Para las aplicaciones de SIG este aspecto es importante, pero sólo ha sido considerado para el caso de modelos 3D por Yeo and Yeung (1999).

Por otra parte, si la marca de agua es capaz de sobrevivir en el archivo incluso si el mismo ha sido modificado (deliberada o inadvertidamente) la marca se denomina *robusta.* Este es el caso más interesante, porque el usuario malicioso podría adquirir una copia legítima, retocarla y distribuirla luego argumentando que le pertenece la autoría. Si la marca es robusta, la misma puede ser recobrada y utilizada para probar la autoría. Otra aplicación para las marcas de agua es para el control de uso: el ejemplo más reciente es el lanzamiento del Digital Video Disc (DVD) (Cox and Linnartz, 1998). El dispositivo reproductor y la marca de agua presente en el disco interactúan y comprueban el tiempo de uso, el número de copias de respaldo

[1] *V CONGRESO LATINOAMERICANO y VII NACIONAL DE AGRIMENSURA, Mayo 22, 23 y 24 de 2002, Punta del Este, URUGUAY*

hechas, etc. Para aplicaciones de SIG esta funcionalidad es aún de interés limitado, porque ningún software actualmente en uso espera procesar archivos de datos marcados.

El caso de marcas de agua robustas es el tema de este trabajo. Una introducción breve y buena se encuentra en el trabajo de Voyatzis and Pitas (1999). El término *robusto* debe ser interpretado con relación a un conjunto de posibles *ataques.* Un *ataque* es una transformación genérica del archivo, realizada por usuarios legítimos o no, que lo modifican en una manera u otra. En este trabajo, los ataques típicamente están pensados para remover la marca, sin importar el contenido de la misma. La literatura muestra que ninguna técnica de las que existen actualmente es inmune a todos los posibles ataques. Lo mejor que se puede lograr es elegirla entre las inmunes a cierto conjunto de ataques, lo que es altamente dependiente de las características del archivo, y la aplicación en mente.

El caso de las imágenes digitales (archivos en formato raster)

Este es un formato típico encontrado en muchas aplicaciones de SIG. Su principal característica es que existe un orden claro y definido (filas y columnas) en el archivo, en oposición a los archivos vectoriales que serán considerados después. Las imágenes de satélite (LANDSAT, SPOT, etc.) así como las fotografías aéreas caen dentro de esta clasificación.

El marcado de imágenes fijas ha recibido recientemente un gran interés por parte de la comunidad científica (Voyatzis *et al.*, 1999; volúmenes especiales de *Signal Processing* y *IEEE Journal of Selected Areas in Communication*, ambos en 1998, etc.). El motivo detrás de este esfuerzo era la protección de derechos de autor de imágenes digitales artísticas.

Las marcas de agua robustas pueden ser aplicadas en el dominio espacial o espectral. El primero aplica la marca conservando la estructura de (fila, columna) en la imagen. Es la opción requerida para el caso de las marcas que se desea sean visibles. Para el caso más común de las invisibles, las marcas aplicadas en el dominio espacial son relativamente más débiles, porque los cambios deben ser implementados en los bits menos significativos (LSB por sus iniciales en inglés) de forma de asegurar que los cambios no serán perceptibles. Una consecuencia inmediata es que se pueden insertar sólo unos pocos bits; puede verse el trabajo pionero de van Schyndel *et al.* (1994) por más detalles. Para el caso más corriente de imágenes SIG, el significado de “perceptible” y “bits menos significativos” es algo diferente. En el caso de las fotografías aéreas, las que serán procesadas por operadores, el límite de lo perceptible está vinculado con el sistema visual humano. Para el caso de imágenes de satélite, los límites del sistema visual no interesan, porque la imagen será procesada y analizada por una computadora. En ese caso, el “bit menos significativo” puede definirse con más precisión: es aquel relacionado con las propiedades del sensor (en el caso de los sensores remotos tipo satélite) o en la incertidumbre inherente a los parámetros medidos u observados.

Alterar los bits menos significativos no es la única posibilidad en el dominio espacial. Nikolaidis and Pitas (1996) han sugerido subdividir a los pixeles de la imagen en dos conjuntos A y B, mediante el uso de una partición seudoaleatoria utilizando una clave secreta. La luminancia de los pixeles del conjunto A se aumentan mediante un entero fijo k, suficientemente pequeño para producir un cambio imperceptible. Dada la clave secreta y el número k, la marca es detectada mediante comparación de la luminancia promedio en los conjuntos A y B, que será próxima a k si la marca de agua está presente, y próxima a cero en otros casos. La imagen original no se requiere al momento de detección de la marca.

Kutter *et al.* (1998) han propuesto explotar la baja sensibilidad del sistema visual humano a cambios de alta frecuencia en el color azul. Las modificaciones de los pixeles son proporcionales a la luminancia, y los bits de la marca determinan el signo de las modificaciones. Nikolaidis and Pitas (1998) reconocen que un problema significativo en todas las técnicas en el dominio espacial es que la marca de agua no sobrevive a la compresión JPEG, la cual es una típica transformación de imágenes. Esto es debido al hecho que la marca de agua es esencialmente un ruido blanco de baja potencia. Ellos modificaron por tanto su método original variando el entero k a agregar a cada pixel, pero manteniendo su suma total como antes. El conjunto A se genera en forma diferente, porque los pixeles ahora se agrupan en pequeños bloques de tamaño 2x2 o 2x4. Se puede calcular un k_{mn} óptimo para cada block_{mn} minimizando la contribución a las componentes de alta frecuencia de la Transformada Discreta del Coseno (DCT) de la imagen completa.

La otra posibilidad es guardar la marca en el dominio espectral. La imagen puede ser transformada mediante transformaciones bien conocidas y definidas (Transformada Discreta de Fourier, DCT, Wavelets, etc.). Los coeficientes pueden ser analizados y modificados de acuerdo con alguna estrategia, y la transformación inversa producirá una imagen muy similar, pero ahora con alguna información extra insertada. Se indicará como α al vector que contiene la marca, y se asumirá que sus elementos son obtenidos de una distribución

gaussiana de media cero y varianza unitaria. El método propuesto Cox *et al.* (1997) sugiere modificar sólo los coeficientes más grandes de la DCT de la siguiente forma:

$$c_i' = c_i + \varepsilon.\alpha_i \quad i = 1..n; n < N^2$$

siendo c_i' el nuevo coeficiente, c_i el original, ε un factor de escala pequeño, α_i el i-ésimo término de la marca y n el largo de la misma. La alternativa de modificar los coeficientes más pequeños de la DCT no sobrevive a la compresión JPEG, por lo que no ha sido considerada en la literatura. La idea es que, si la marca de agua no debe ser evidente, los cambios deben ser pequeños. Sin embargo, los cambios pequeños en general son fuertemente afectados por el ruido, excepto si están concentrados en los términos perceptualmente más significativos del espectro. Su método pertenece a una clase más amplia de técnicas de *amplio espectro*. En la práctica, la imagen es subdividida en partes de tamaño NxN, y la marca es aplicada independientemente a todas o algunas de las partes del mosaico. La imagen ahora marcada se regenera a través de la transformada inversa del coseno. Para detectar la marca de agua, se requiere la DCT de la imagen original de forma de verificar la relación

$$\frac{c_i^{'} - c_i}{\varepsilon} = a_i'$$

Zeng and Liu (1999) propusieron un método alternativo que no requiere la imagen original, pero que es menos robusto. Si la correlación entre $\boldsymbol{\alpha}$ y $\boldsymbol{\alpha'}$ es mayor que un umbral prefijado, se declara que la marca está presente. Este enfoque es robusto incluso frente a algunas transformaciones válidas que se usan típicamente, como la compresión JPEG, así como a impresión seguido de escaneo. En su forma más simple, este método es susceptible a ataques vía el protocolo (Craver *et al.*, 1998; Memon and Wong, 1998, etc.) .

Dos aspectos importantes son la longitud máxima de la marca, y cuantas marcas pueden ser insertadas en forma confiable en una imagen dada. Es frecuente expresar la resistencia de una clave criptográfica en bits: claves más largas implican una seguridad mayor. Si la longitud de la clave es suficientemente pequeña, la misma puede ser descubierta mediante prueba y error exhaustiva, y una vez encontrada la clave, la marca es fácilmente removible si el algoritmo de inserción es conocido. Las marcas largas son necesarias para identificar con unicidad el propietario, cliente, distribuidor, etc. Podría ser difícil producir e insertar marcas largas, porque hay límites prácticos que deben ser respetados. Servetto *et al.* (1998) asume que si los ataques pudieran ser modelados como ruido aditivo, es posible encontrar límites superiores para el largo de las marcas en bits. La estimación del número de posibles marcas distintas que pueden ponerse en la misma imagen es un problema difícil, y como antes hay que hacer hipótesis fuertes sobre el ruido.

Hay otros algoritmos que se basan en las limitaciones del sistema visual humano, como el que describen Podilchuk and Zeng (1998) o Delaigle *et al.* (1998). Para muchas aplicaciones, una imagen puede ser alterada y aún ser útil mientras que los cambios no sean notorios para los humanos. Un ejemplo es la compresión con pérdida (mediante algoritmos que degradan la calidad de la imagen original de forma de permitir compresiones muy significativas que serían imposibles de otra forma). Existen modelos de la visión que suministran un conjunto de valores umbrales que conforman las *Diferencias Casi Perceptibles (JND)*. Si las modificaciones aplicadas están por debajo de esos umbrales, la marca puede ser muy fuerte pero aún indistinguible. Como se ha mencionado antes, la utilidad de modelos basados en JND para aplicaciones de SIG está limitada a las tareas de fotointerpretación.

El autor no está al tanto de que los procesos de marcado de información SIG digital (por ejemplo) obtenida vía satélite aplicados por los productores. Ellos actualmente venden las imágenes bajo un contrato que limita al comprador en aspectos como redistribución, uso, etc. del material. No se provee ninguna información sobre otros medios o métodos (aparte del contrato) utilizados para la protección de sus derechos. Las razones pueden estar en el lado legal, lo que se verá en otra parte. El marcado de imágenes digitales estáticas es un mercado activo: existen un buen número de proveedores comerciales de software (Digimarc Inc., Blue Spike Inc., Signum Technologies, SysCoP, etc.). Es difícil establecer ninguna declaración definitiva sobre cuál es mejor que el otro, porque las compañías no proveen información detallada sobre el algoritmo con el que insertan la marca. Es posible realizar una comparación funcional analizando la resistencia a diferentes ataques. Kutter and Petitcolas (1999) proponen un test para propósitos de comparación, conectado con características del sistema visual humano. Ellos han usado el programa StirMark (Petitcolas and Kuhn, 1997) para realizar los ataques.

El caso de los datos vectoriales (mapas)

Es sorprendente que, a pesar de los grandes costos asociados a la recolección y ensamblaje de archivos vectoriales, el tema de “métodos de protección contra la copia” no haya captado el interés sostenido de la

comunidad de investigadores de SIG. Lo más cerca que se encuentra está en la creación de modelos tridimensionales para ser usados en realidad virtual y aplicaciones de CAD. Dado que algunas ideas pueden inspirar soluciones para este problema, se analizarán al menos las referencias más relevantes. Luego presentaremos los escasos trabajos específicos que hay sobre el tema.

Las escenas de Realidad Virtual (expresadas en lenguaje VRML) se están haciendo cada vez más populares en Internet. Ellas están compuestas de muestras de audio, texturas e imágenes de fondo, así como en modelos de geometría tridimensional (3D). La parte más costosa y laboriosa para implementar es esta última, y por lo tanto es el punto más interesante para un potencial pirata. Afortunadamente, también es el lugar más apropiado para colocar una marca de agua (Ohbuchi *et al.*, 1997; Benedens, 1999). Debe tenerse en cuenta que el estándar de VRML permite insertar información en los archivos a través de comentarios y anotaciones. Sin embargo, los programas que convierten entre formatos típicamente los eliminan, por lo que son inútiles a los efectos de la marca de agua.

Una característica importante de los modelos 3D es que carecen de un orden implícito. El audio, video y las imágenes estáticas son secuencias de series temporales, o matrices. Ciertamente que los vértices, bordes y caras en un modelo 3D pueden ser ordenados, pero quizá requiriendo una orientación de referencia y un origen definido de antemano. Una segunda característica es que no existe una representación única a los efectos visuales. Los vértices de un modelo 3D pueden ser movidos en proporción considerable sin cambiar la calidad visual del mismo. Para ser desplegados a una velocidad razonable, los modelos 3D son usualmente comprimidos mediante una simplificación de los mismos (Garland, 1999). En ese proceso, ellos pueden perder incluso el 86% de las caras sin cambios evidentes. Esto explica porqué es corriente guardar la misma marca más de una vez en el modelo 3D, de forma de poder recuperarla incluso luego de subdividido el modelo.

Ohbuchi *et al.* (1997) discute varias alternativas para el marcado de grillas tridimensionales. Por ejemplo, las coordenadas de los puntos y vértices pueden ser modificadas para insertar datos, o también pueden modificarse otras cantidades escalares o vectoriales (tal como el área de un triángulo, o la normal a una superficie). Sin embargo, incluso transformaciones simples podrían destruirlas, por lo que es interesante considerar sólo las cantidades que puedan ser invariantes a ciertas clases de transformaciones geométricas. Es posible establecer una jerarquía para las mismas, como se presenta en la Tabla 1. Una segunda posibilidad es insertar la marca en la topología, tomando ventaja de que carece de unicidad. Por ejemplo, dados cuatro vértices que forman un cuadrado, ellos pueden ser convertidos en dos triángulos en dos maneras diferentes. Por lo tanto, es posible codificar un bit de información dependiendo de la posición de la diagonal. Este enfoque puede sobrevivir a muchas transformaciones geométricas, pero no a transformaciones topológicas o regeneración de la malla.

La clase de transformaciones válidas y esperadas para el caso de mapas es más restringida. En algún caso, los mapas de SIG tienen coordenadas absolutas, o coordenadas relativas pero referidas a un sistema de referencia. En cualquier caso, cambiar en forma sustantiva las coordenadas pueden hacer inútil al mapa, porque el mismo no ajustaría con otros que sí respetan el sistema original. Por lo tanto, un sistema de marcado apropiado para mapas podría no tener resistencia a las transformaciones de tipo 4 y 5 sin ser por ello menos útil. Sin embargo, las coordenadas pueden ser conocidas con incertidumbre (lo que no debe ser confundido con precisión limitada por la computadora). Esto implica que cambiar al azar sus valores por una cantidad que esté por debajo de la incertidumbre pueden producir un mapa semánticamente equivalente, lugar por tanto para poner la marca.

Como ha sido sugerido antes, es posible guardar un bit de información mediante la generación de triángulos de una forma o de otra a partir de un cuadrado, o prefijando la razón de áreas de dos polígonos. Sin embargo, para ser útil, la marca de agua debería tener más bits, requiriendo por lo tanto un buen número de primitivas para guardarlas, y además con un orden (explícito o implícito) entre las mismas. Ohbuchi *et al.* (1998) considera para esto tres posibilidades: a) ya existe un orden global entre las primitivas, b) existe un orden local o c) no hay ningún orden, pero se codifica la información así como un subíndice a la vez. Por ejemplo, un orden global unidimensional podría ser obtenido ordenando los triángulos de acuerdo a su área. Un orden bidimensional podría estar basado en la conectividad en una malla irregularmente subdividida. El ordenamiento global tiende a tener más densidad de información que otros métodos. El ordenamiento local y con subíndice tienen la ventaja que la marca puede resistir a una subdivisión del modelo, ya que la misma parte de la marca puede ser insertada varias veces en la malla.

Para ilustrar esto, mostraremos como podría trabajar el método del subíndice. Primero se buscan en la malla (Fig. 1 derecha) un conjunto de cuatro triángulos que compartan cada uno un lado con otro (tal como se presenta en la Fig. 1 izquierda). El triángulo en gris será utilizado como el de referencia, y su forma es la que

indica que es parte de la marca. Por ejemplo, se modifican sus vértices de forma de forzar que sus dos ángulos más pequeños sean (por ejemplo) de 33 y 57 grados. Luego, se modifica levemente el que se indica con S de forma que tenga 20 y 60 grados, codificando de esa manera un número 3 mediante una tabla de valores previamente acordada. Este número será el subíndice, e indica que la información corresponde con el 3er elemento de la marca. Los triángulos D1 y D2 guardan la información misma, mediante la misma tabla de valores, siendo D1 el que tiene el primer elemento porque su área es mayor que la de D2. Para reconstruir la marca completa, es necesario buscar todos los triángulos con ángulos internos de "exactamente"33 y 57 grados, y que compartan un lado con sólo un triángulo. Utilizando la tabla de valores, se puede identificar el subíndice, la información de D1 y D2, y recuperar así un elemento de la marca por vez. Lo mismo se repite hasta que todos los posibles subíndices son encontrados.

De acuerdo a los autores, los cambios a la geometría original pueden ser mínimos, e imperceptibles para humanos. El conjunto de tres triángulos más el gris no puede compartir vértices con otros conjuntos similares. Además, los triángulos con ángulos internos demasiado pequeños deberían ser evitados, porque son muy inestables incluso frente a transformaciones geométricas muy simples. Para reducir el riesgo de perder partes de la marca, a misma información es guardada muchas veces, permitiendo que aún subdividido, el modelo aún contenga la mayor parte de la marca. Si se encontraran varias instancias para el mismo subíndice, se decide por mayoría simple. La marca podría ser destruida por una modificación al azar de las coordenadas, por una clase más general de transformaciones geométricas, o por transformaciones topológicas profundas como reconstrucción de la malla. Una propiedad interesante es que el modelo original no es requerido para detectar la malla. Otra propiedad importante es que, aún dado el modelo marcado y la marca, el original no puede ser obtenido de ellos. Esto tiene implicancias respecto al protocolo de autoría.

Benedens (1999) presenta también un método que opera en el dominio espacial, ya que guarda la marca de agua en las normales a la superficie del modelo. Él argumenta que esos elementos son relativamente persistentes en el modelo incluso ante moderadas modificaciones que afecten su geometría. El procedimiento transforma las normales a la superficie a la esfera unitaria, y luego modifica la posición de algunos vértices modificando la distribución de las normales. Su procedimiento sólo es posible para el caso de marcas privadas, ya que se requiere el original para detectarla. Además, requiere una reorientación bastante precisa del modelo.

Los dos métodos presentados modifican las coordenadas, por lo que pueden ser clasificados como operando en el dominio espacial. Existen, al igual que para las imágenes estáticas, métodos que operan en el dominio espectral, como por ejemplo el presentado por Date *et al.* (1999) o Praun *et al.* (1999). En el primer caso, se realiza la transformada con wavelets del modelo 3D para representarlo a diferentes resoluciones, de forma de permitir una compresión y despliegue eficiente. El principio de *amplio espectro* puede ser aplicado a los coeficientes de la transformación con wavelets, como ha sido descrito para imágenes. Tal como antes, para recuperar la marca el modelo original debe estar presente. En el segundo trabajo, los autores usan una transformación diferente pero a todos los efectos equivalente a la anterior. El modelo sospechoso y el original deben estar presentes, y ser llevados al mismo sistema de referencia, regenerando no solamente la orientación y escala, sino también la misma conectividad que el original.

Existen unos pocos trabajos específicos para el caso de mapas vectoriales. Solachidis *et al.*, (2000) trata cada poligonal como independiente, y analiza la transformada de Fourier discreta de sus coordenadas (X,Y). Esta transformada consiste en un conjunto de N coeficientes y ángulos, los que son modificados levemente de forma de contener la marca, tal como se señaló en el caso de los métodos de *amplio espectro*. Luego se realiza la transformación inversa obteniéndose nuevas coordenadas para la poligonal. Como método tiene varios inconvenientes: el peor, es que la marca se borra si se insertan vértices en la poligonal ya que cambia el número N de la transformación. Además, para reconstruir la marca es necesario acceder a la poligonal original. Por último, las coordenadas de todos los vértices cambian. Esto hace imposible ocultar la marca en los casos en que hay más de una cobertura compartiendo parcialmente una poligonal, ya que las transformaciones sobre cada una de ellas son diferentes. El esquema resiste rotaciones, traslaciones, escalamiento y transformaciones isométricas en general. Dado que la marca se inserta en todas y cada una de las poligonales, el esquema resiste la eliminación parcial de algunas de ellas en el mapa.

López, 2000 propone un método diferente, que no altera las coordenadas de los vértices pero que inserta nuevos vértices en la poligonal, siguiendo reglas definidas a partir de una clave secreta. La presencia de esos vértices en el archivo sospechoso denota la marca de agua. La clave secreta se asocia mediante una base de datos con la información del cliente, distribuidor, etc. Este método tiene como ventaja que tramos compartidos de la misma poligonal entre diferentes coberturas se marcan de la misma forma disimulando así eficazmente su presencia. Al igual que el caso anterior, el esquema es resistente a transformaciones

isométricas en general, así como a la eliminación de partes del mapa. El método está implementado como servicio comercial por el autor.

Conclusiones

La producción de cartografía digital está creciendo rápidamente. Este proceso requiere de inversiones sustanciales, las que por razones varias se espera recuperar mediante la venta de estos nuevos productos. Este esquema está sin embargo seriamente amenazado por una variedad de razones ya que el retorno de esta inversión puede diluirse rápidamente debido a la piratería. A diferencia de los productos tradicionales en papel, en la era digital existen pocos obstáculos para un potencial pirata.
Se plantea como parte de la solución la aplicación de las leyes existentes, pero apoyadas en soluciones técnicas que permitan rastrear el génesis de cada copia pirata que se encuentre, cosa imposible en la actualidad. Se ha discutido hasta aquí el estado del arte relativo a la inserción de marcas de agua robustas en imágenes, así como en mapas vectoriales y modelos 3D, señalando las similitudes y diferencias que podrían ser tomadas en cuanta al implementarlos para los mapas. Esta es aún un área poco explorada, con pocos trabajos académicos publicados y una única solución comercial disponible, lo que plantea un desafío tanto a los organismos productores de cartografía como a los académicos e investigadores del área.

Referencias

Anderson, R. J. and Petitcolas, F. A. P., 1998. On the limits of Steganography. *IEEE Journal of Selected Areas in Communications*, 16, **4**, 474-481

Benedens, O., 1999. Geometry-Based Watermarking of 3D models. *IEEE Computer Graphics and Applications.* 46-55

Bender, W.; Gruhl, D.; Morimoto, N and Lu, A., 1996. Techniques for data hiding. *IBM Systems Journal*, **35**, 3-4, 313-336

Cox, I. J.; Kilian, J.; Leighton, T. and Shamoon, T., 1997. Secure Spread Spectrum Watermarking for Multimedia. *IEEE Trans. on Image Processing*, **6**, 12, 1673-1687

Cox, I. J. and Linnartz, J. P. M. G., 1998. Some General Methods for Tampering with Watermarks. *IEEE Journal on Selected Areas in Communications,* **16**, 4, 587-593.

Craver, S.; Memon, N.; Yeo, B. L. And Yeung, M., 1998. Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks and implications. *IEEE Journal on Selected Areas in Communications*, **16**, 4, 573-586

Date, H.; Kanai, S. And Kishinami, T., 1999. Digital Watermarking for 3D polygonal model based on wavelet transform. *Proceedings of DETC'99 – 1999 ASME Design Engineering Technical Conferences. September 12-15, 1999, Las Vegas, Nevada.* DETC99/CIE-9031, 10pp.

Delaigle, J. F.; Vleeschouwer, C. D. and Macq, B., 1998. Watermarking algorithm based on a human visual model. *Signal Processing*, **66**, 3, 319-335.

Garland, M., 1999. Multiresolution Modeling: Survey & Future Opportunities. *EUROGRAPHICS'99,* ISSN 1017-4956, 111-131

Karjala, D., 1995. Copyright in electronic maps. *Jurimetrics J.*, **35**, 395-415

Kutter, M. and Petitcolas, F. A. P., 1999. A fair benchmark for Image watermarking systems. *P. W. Wong and E. J. Delp, Eds. Security and Watermarking of Multimedia Contents, ISBN 0-8194-3128*, 226-239

Kutter, M.; Jordan, F. and Bossen, F., 1998. Digital signature of color images using amplitude modulation. *Journal of Electronic Imaging,* **7**, 2, 326-332

López, C. 2000. Método para Insertar datos ocultos en archivos digitales con poligonales, y procedimientos de detección. *Solicitud de patente 26500, Uruguay*

Memon, N. and Wong, P. W., 1998. A Buyer-Seller Watermarking Protocol. *IEEE Workshop on Multimedia Signal Processing (MMSP-98), Dec. 7-9, Los Angeles, California, USA*, 278-283

Nikolaidis, N. and Pitas, I., 1996. Copyright protection of images using robust digital signatures. *IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP-96),* **4**, 2168-2171

Nikolaidis, N. and Pitas, I., 1998. Robust image watermarking in the spatial domain. *Signal Processing*, **66**, 385-403

Ohbuchi, R.; Masuda, H. and Aono, M., 1997. Watermarking Three-Dimensional Polygonal Models. *ACM Multimedia 97,* ACM Press, 261-272

Ohbuchi, R.; Masuda, H. and Aono, M., 1998. Watermarking Three-Dimensional Polygonal Models through Geometric and Topological Modifications. *IEEE J. on Selected Areas in Communications,* **16**, 4, 551-560

Podilchuk, C. and Zeng, W., 1998. Image Adaptive Watermarking Using Visual Models. *IEEE Journal on Selected Areas in Communications*, **16**, 4, 525-540

Praun, E.; Hoppe, H. and Finkelstein, A., 1999. Robust mesh watermarking. *Computer Graphics (SIGGRAPH 1999 Proceedings)*, 69-76. Also available at http://www.cs.princeton.edu/gfx/proj/meshwm.

Schneier, B. 1995, Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley & Sons, ISBN: 0471117099

Servetto, S. D.; Podilchuk, C. I. and Ramchandran, K., 1998. Capacity issues in Digital Image Watermarking. *In Proc. of the IEEE Int. Conf. on Image Processing. Chicago, IL.* 5pp.

Solachidis, V.; Nikolaidis, N. and Pitas, I. 2000. Watermarking Polygonal Lines Using Fourier Descriptors, In *IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP'2000), Istanbul, Turkey*, IV, 1955-1958, 5-9 June 2000

Special Issue on Watermarking, 1998, *Signal Processing*, **66**, 3

Special Issue, 1998, *IEEE J Selected Areas in Comm*, **16**, 4

van Schyndel, R. G.; Tirkel, A. Z. and Osborne, C. F., 1994. A digital Watermark. *Proc. of the IEEE Int. Conf. on Image Processing (ICIP´94)* vol II, 86-90

Voyatzis, G. and Pitas, I., 1999, Protecting Digital-Image Copyrights: A Framework. *IEEE Computer Graphics and Applications*, 19, **1**, 18-24

Yeo, B. L and Yeung, M. M., 1999. Watermarking 3D Objects for Verification. *IEEE Computer Graphics and Applications,* 36-45

Zeng, W. and Liu, B., 1999. A statistical watermark detection dechnique without using original images for resolving rightful ownerships of digital images. *IEEE Trans. Image Processing,* **8**, 11, 1534-1548