WATERMARKING PADA PRODUK INFORMASI GEOSPASIAL VEKTOR

(Watermarking in Vector Geospatial Information Product)

Fahmi Amhar, Sobar Sutisna, Niendyawati
Badan Informasi Geospasial
Jl. Raya Jakarta-Bogor Km. 46 Cibinong, Jawa Barat, Indonesia 16911
email: famhar@yahoo.com

Diterima (received): 25 September 2014; Direvisi (revised): 2 Oktober 2014; Disetujui dipublikasikan (accepted): 20 November 2014

ABSTRAK

Adanya UU No. 4 tahun 2011 diprediksi akan membuat produk informasi geospasial "*booming*". Tidak hanya BIG yang akan menjadi lebih terkenal sebagai sumber informasi geospasial dasar, namun juga industri geospasial tematik atau turunan akan ikut menikmatinya. Namun, fenomena ini suka tidak suka akan memunculkan "penumpang gelap", yaitu pemalsuan dan pembajakan. Untuk mengatasinya, diperlukan metode dan teknologi yang disebut dengan "*Watermarking*". Teknologi ini sudah lama digunakan pada uang kertas, juga pada produk fotografi, audio dan video. Intinya adalah, agar orang semakin sulit menjual produk palsu, atau menggandakan produk asli untuk mendapatkan keuntungan secara ilegal. Pada makalah ini akan ditunjukkan beberapa metode *watermarking* yang sudah ada saat ini, yang dapat dicoba pada produk informasi geospasial vektor, seperti Peta Rupabumi Indonesia dan sejenisnya. Sebuah software akan memproduksi watermark untuk ditempelkan pada data, atau didaftarkan pada sebuah situs registrasi. Ketika orang mendapatkan suatu data, maka dia bisa mengujikan dengan software otentifikasi, untuk memastikan bahwa data itu asli, atau pemiliknya memang mendapatkannya secara legal. Beberapa keunggulan dan kelemahan setiap metode tersebut akan didiskusikan dalam makalah ini.

Kata Kunci: tanda air, informasi geospasial, vektor

ABSTRACT

The existence of Law Number 4 / 2011 is predicted to create "booming" geospatial information products. Not only BIG will become more famous as a source of basic geospatial information, but also thematic or derived geospatial industry will come to enjoy it. However, like it or not this phenomenon will bring up the "dark passenger", namely falsification and piracy. To overcome this, required methods and technologies called "watermarking". This technology has been used on paper money, also in product photography, audio and video. The objective is, in order people are getting difficult to sell counterfeit products, or duplicate original product to get profit illegally. In this paper will be shown several watermarking methods that already exist today, which can be tried on the vector geospatial information products, such as Topographic Map of Indonesia and any kind of map. A software will produce a watermark to be attached to the data, or registered at a registration site. When people get the data, then he could be testing the authentication software, to ensure that the original data, or the owner did get it legally. Some of the advantages and disadvantages of each of these methods will be discussed in this paper.

***Key Words**: watermarking, Geospatial Information, Vector*

PENDAHULUAN

Setiap hal yang bagi sebagian masyarakat dianggap bermanfaat, akan mengalami fenomena "*booming*". Dan setiap "*booming*", akan memunculkan "penumpang gelap". Misalnya pada kasus uang kertas, karena dianggap memiliki nilai manfaat tinggi, muncullah uang palsu; Produk VCD yang laku keras, kemudian diperbanyak dan dijual secara ilegal dengan VCD bajakan; Demikian juga dengan produk informasi geospasial (IG) pasca disahkannya UU No. 4 tahun 2011, akan menjadi incaran "penumpang gelap". Fenonena pemalsuan dan pembajakan adalah persoalan serius di dunia karya cipta.

Sebagaimana gambar (pada uang), foto, audio dan film-video (pada VCD), Informasi Geospasial (IG) adalah produk karya cipta yang rawan pemalsuan dan pembajakan. Pemalsuan bertujuan mendapatkan keuntungan secara tidak sah dari reputasi pencipta yang asli. Data yang sebenarnya bukan produk Badan Informasi Geospasial (BIG) misalnya, diaku sebagai produk BIG supaya orang percaya (dan mungkin mau membayar dengan harga yang lebih tinggi). Atau seseorang yang sudah membeli produk BIG secara legal, namun kemudian memperbanyaknya dan menjualnya secara illegal. Pertanyaannya, bagaimana cara BIG, atau siapapun melindungi produk IG-nya secara teknis, agar tahan terhadap pemalsuan dan pembajakan. Atau setidaknya, agar siapa saja yang berniat memalsukan dan membajak produk IG akan mengalami kesulitan.

Pada produk uang, keaslian uang secara teknis dilindungi dengan menggunakan teknik percetakan tingkat tinggi, yang jumlah mesin yang dapat melakukannya di dunia sangat terbatas. Uang-uang dengan nilai tinggi dicetak dengan hologram yang hanya bisa dilihat dengan sinar ultraviolet, memiliki tanda air *(watermark)*

yang hanya dapat diterawang, memiliki benang pengaman, menggunakan tulisan mikro, dan semua dilengkapi dengan nomor seri yang berbeda. Karena itu uang palsu yang dicetak dengan mesin cetak biasa, relatif mudah dikenali.

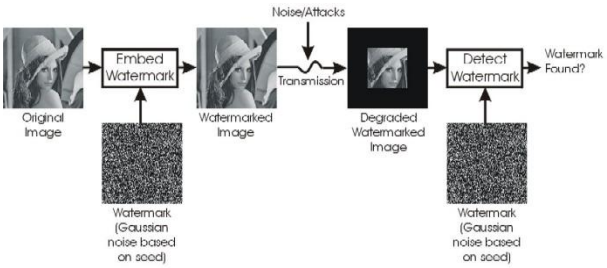
Teknik penyisipan tanda air *(watermarking)* ini yang kemudian diterapkan pada produk digital yang lain. Pada karya fotografi, foto yang dilindungi secara sederhana, bisa dilengkapi dengan tanda *copyright* atau nama pemiliknya yang membayang (nyaris transparan) di dalam gambar, sehingga siapapun yang mengcopynya, pasti ikut mengcopy tulisan tersebut. Karena tulisan itu ada di dalam bagian utama gambar, tidak mudah menghapusnya atau memotongnya. Atau dapat juga tulisan dibuat sangat kecil tetapi ditaruh merata di dalam gambar (Frank, 2008).

Gambar 1. Contoh foto yang diberi watermark visual (dengan *software* TSR Watermark, *www.watermark-image.com*).

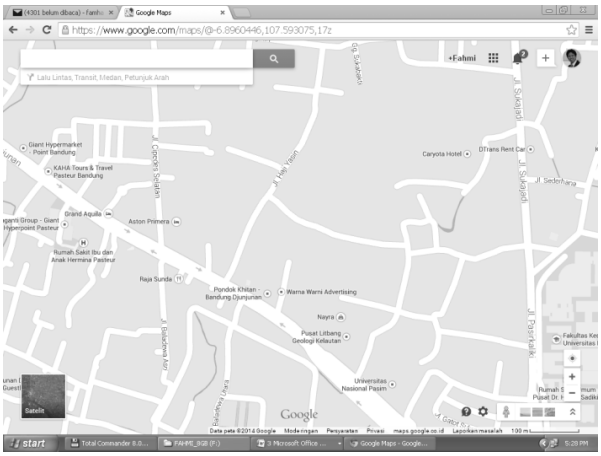
Untuk foto/citra yang akan diolah lebih lanjut, semisal pada citra *remote sensing*, tentunya penulisan tanda atau tulisan *copyright* akan mengganggu analisis. Karena itu, dilakukan pengamanan dengan *watermark* yang tidak kelihatan secara visual, dan juga tidak akan banyak mempengaruhi hasil analisis. Namun *watermark* hanya dapat disisipkan dan dikenali lagi dengan sebuah *software* khusus (Toshikazu et.al, 2009).

Demikian juga dengan produk audio atau video, *watermarking* dilakukan dengan sebuah *software*, sehingga oleh manusia yang menggunakannya, tanda air tersebut nyaris tidak dikenali (Tirkel et.al, 1993)

Pertanyaannya kini, bagaimana memasukkan tanda ini pada produk IG vektor yang terdiri dari titik, garis dan luasan? IG vektor ada yang digunakan hanya sebatas tampilan visual untuk navigasi (semisal *Google Map*), ada yang untuk diolah lanjut (semisal untuk analisis spasial dengan *software* Sistem Informasi Geografis/SIG). Bila untuk sekedar tampilan, maka *software* penampil baik versi *stand-alone* maupun internet, bisa menyisipkan tulisan *copyright* seperti lazim pada *Google Map*.



Gambar 2. Algoritma *watermarking* pada foto atau citra digital *(http://www.psiva.ca/Research/DigitalWaterrmarking/digitalWatermarking.html).*



Gambar 3. Tanda "Google" di setiap tampilan IG Vektor di dalam Google Map *https://www.google.com/maps/@-6.8960446,107.593075,17z.*

Adapun ketika IG vektor itu akan diolah lanjut dengan *software* SIG, maka tanda air itu tidak boleh hilang oleh proses apapun yang terjadi. Tanda air (*watermark*) itu juga tidak boleh dikenali oleh pengguna biasa, karena bila bisa dikenali, maka tentu saja bisa dihilangkan atau dimanipulasi (Halder et.al, 2010). Bila tanda air pada uang di-*crop* (dihilangkan), maka uang itu jadi tidak laku. Namun pada IG, *cropping* sebagian isinya tetap masih bisa memberikan manfaat. Jadi tanda air harus memiliki dua fungsi sekaligus. Pertama menguji otensitas bahwa itu adalah produk resmi dari penciptanya. Kedua mempersulit pembajakan, bahwa yang membawa IG tersebut memang terdaftar memiliki ijin (lisensi) resmi penggunaannya (Tao, 1973).

METODE

Kajian ini akan menggunakan metode pustaka yang didapatkan dari berbagai publikasi yang ditemukan di internet (*Google.Scholar*, *SciDirect*). Beberapa contoh dan *software* yang ditemukan di internet kemudian diunduh dan dicoba. *Software* yang dapat diunduh gratis biasanya memiliki

kemampuan yang terbatas dari sisi volume dan format data yang dapat diolah, varian *watermark* yang dapat disisipkan, atau di setiap hasilnya selalu tampak identitas dari pembuatnya sebagai promosi.

Secara umum metode *watermarking* pada IG vektor ada dua macam, yaitu: (1) penyisipan unsur renik ke dalam data; dan (2) registrasi karakteristik data pada server di *cloud* (*zero watermark*).

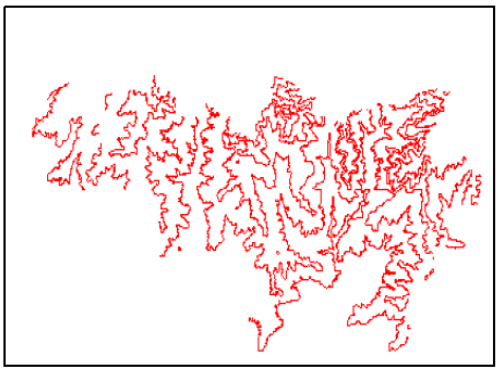
HASIL PEMBAHASAN

Metode penyisipan unsur renik ke dalam data

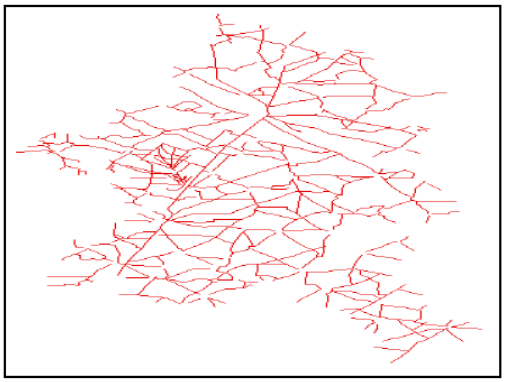
Beberapa software menyisipkan objek geometri sangat renik ke dalam data (Chaudhari et.al, 2012). Ini prinsipnya seperti pada fotografi. Misalnya bila di dalam data terdapat unsur garis atau luasan, maka ke dalam garis atau luasan itu disisipkan titik (*vertex*) yang menjadi satu dengan garis, dan hanya mempunyai simpangan yang amat sangat kecil, sehingga baik secara visual maupun untuk analisis, titik baru itu seperti tidak ada. Titik itu hanya dikenali kembali, ketika dalam suatu garis yang "lurus", ditemukan titik baru, seolah-olah orang kelebihan titik akibat melakukan digitasi dengan *streaming mode*. Namun *software watermark* menyisipkan titik-titik baru itu pada suatu jarak tertentu dari ujung garis. Dalam suatu data, ada sekian banyak garis yang dimanipulasi. Ini untuk mengantisipasi ketika pengguna menghapus satu dua objek garis dari dalam data. *Watermark* tetap terbawa untuk garis sisanya.

Sebaran titik *watermark* dan jaraknya dari ujung garis itu disimpan dalam suatu rumus, yang merupakan kunci *watermark* bagi data tersebut, yang akan digunakan untuk uji keaslian dan uji tidak ada pelanggaran hak cipta (Neyman et.al, 2013). Sekalipun ada garis yang di-*crop* atau diedit, namun bila dalam suatu data masih ditemukan sejumlah garis yang memiliki ciri *watermark* yang sesuai kunci, maka data itu dapat dipastikan berasal dari produsennya. Tinggal dilihat, apakah pemegang data tersebut berada dalam daftar penerima lisensi yang sah atau tidak. Bila tidak, maka data tersebut telah dimiliki secara tidak sah.

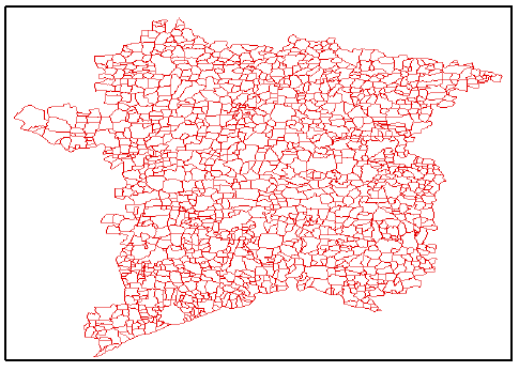
Data geospasial vektor akan diberi *watermark* secara *layer* demi *layer*. –Kapasitas setiap *layer* yang akan di-*watermark* ditentukan oleh kepadatan informasi dalam *layer* tersebut. Bila *layer* itu nyaris kosong, maka tidak mungkin ada *watermark* dapat ditanam di situ (Chaudhari et.al, 2014).



(a) Polyline Layer

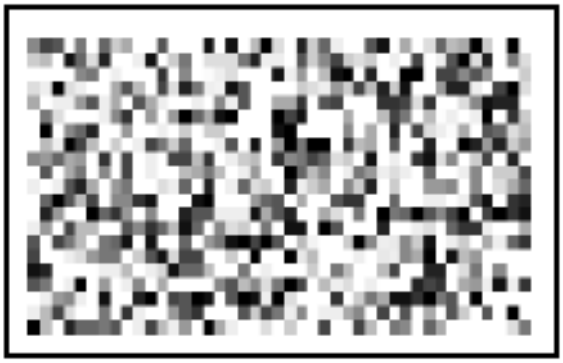


(b) Road Segment Layer



(c) Polygon Layer

Gambar 4. *Input Vector data set (Zope-Chaudari, et al, 2014).*



Gambar 5. *Watermark* asli dan yang tersandi di dalam data *(Zope-Chaudari, et al, 2014)*.

Dengan demikian, untuk uji keaslian, penguji wajib memiliki kunci keaslian. Bisa saja kunci keaslian dibuat sama untuk seluruh data. Atau kunci itu berbeda-beda sesuai dengan pihak yang diberi lisensi.

Efektivitas suatu *watermark* sangat tergantung sejauh mana dia bertahan (*robust*) pada saat terjadi "serangan" (*attack*) operasi geometri pada data tersebut seperti *noise*, kompresi, translasi, rotasi, *scaling*, *cropping*, sampai penambahan atau penghapusan hingga 10% dari data.

Tabel 1. Evaluasi: Ketangguhan menghadapi "serangan" (*attack*), (Zope-Chaudhari, et al, 2014).

Attacks		***Extracted Watermark* (*Proposed scheme*)**	***Normalized Correlation* (NC)**
Noise			0.903269
Compression			0.876492
Translation			1
Scalings	*Up Scaling*		1
	Down Scaling		1
Coordinate Addition			1
Coordinate Deletion (5%)			0.954062
Cropping (25%)			0.999430
Cropping (40%)			0.978564

Bila seseorang mendigitasi data IG sendiri lalu mengklaim bahwa data itu berasal dari BIG, maka data itu dapat dipastikan tidak memiliki *watermark* (uji keaslian gugur). Namun bila ada seseorang yang pernah mendapatkan data secara resmi dari BIG, tetapi lalu menggandakan dan menjualnya, maka uji keaslian masih lulus, tetapi ada pelanggaran hak cipta (gugur di uji hak cipta). Untuk itu, penguji wajib memiliki daftar penerima ijin/lisensi.

Agar kunci dan daftar penerima lisensi selalu dapat diakses, ada baiknya tersedia server yang khusus didesain untuk itu. Namun ketika *watermarking* ini sudah melibatkan suatu server, maka dapat diterapkan metode ke-2, yaitu *Zero Watermarking*.

Metode *Zero Watermarking*

Gagasannya adalah sama sekali tidak ada penyisipan unsur asing ke dalam data (*zero watermarking*) (Li et.al, 2006). Namun karakteristik data dipelajari lalu diberikan suatu rumus yang disimpan di server. Karakteristik itu misalnya jarak suatu objek dengan objek yang lain, lebar sungai di beberapa tempat, atau jumlah nama unsur rupabumi di dalam sebuah area. Rumus ini tentu *invariant*, artinya akan tetap sama sekalipun keseluruhan data ditransformasi (digeser, diputar atau diubah skalanya). Data yang akan diuji, dibaca oleh *software* untuk didapatkan rumus karakteristiknya, lalu dibandingkan dengan rumus yang telah disimpan di server. Prinsipnya seperti mendapatkan sidik jari (*finger print*).

Metode seperti ini masih perlu diuji di lapangan. Karena bisa terjadi, ada wilayah yang hanya memiliki terlalu sedikit unsur rupabumi, sehingga siapapun yang memetakannya, akan mendapatkan hasil yang sama (semisal satu titik bangunan atau seruas jalan). Bisa saja orang yang mendapatkan data itu dengan survei mandiri, diduga mengambilnya (secara ilegal) dari data BIG, karena *software* tidak bisa membedakan karakteristiknya dengan data asli milik BIG.

Idealnya, dalam penelitian ini, *software* yang ada itu dapat dicoba dengan data riil, semisal 1 lembar peta RBI yang memiliki unsur cukup lengkap. Pilihan lokasi adalah bebas, yang penting berbagai unsur peta RBI terwakili yaitu hipsografi (kontur), perairan, nama rupabumi, batas administrasi, transportasi dan utilitas, gedung dan bangunan, dan penutup lahan ada semua. Perlu dicari daerah dengan kerapatan informasi minimum, maksimum dan rata-rata untuk membandingkan kinerja algoritma (Ganic et.al, 2004).

Setelah itu *software* dijalankan, data dibaca, dibandingkan dengan data yang belum disisipi *watermark*, kemudian diolah kembali ke *software* untuk dibaca *watermark*-nya. Perlu juga, data yang telah disisipi *watermark*, diolah lagi, diganti nama *layer*-nya, ditransformasi (digeser, diputar, diubah skalanya), disisipi unsur baru, atau dihapus sebagian isinya, baru kemudian dilihat, apakah masih ada *watermark* yang dikenali? Berapa persen kepastian bahwa data itu "asli", atau "diolah dari yang asli"? (Khan et.al, 2007).

Penelitian ini masih berjalan, dan *software* yang digunakan masih dalam pengembangan dan pengujian.

KESIMPULAN

Proses *watermarking* untuk menguji keaslian dalam rangka melindungi suatu produk data IG vektor dari usaha-usaha pemalsuan dan pembajakan masih dalam pengembangan. Metode yang dipakai adalah penyisipan unsur renik dan pendaftaran karakteristik ke sebuah server. Metode ini sedang diuji untuk melihat efektifitasnya setelah data mengalami berbagai manipulasi.

UCAPAN TERIMA KASIH

Ucapan terima kasih kepada Pusat Penelitian, Promosi dan Kerjasama Badan Informasi Geospasial yang mendukung serta membiayai penelitian ini.

DAFTAR PUSTAKA

Frank, Y. Shih: Digital watermarking and steganography: fundamentals and techniques. Taylor & Francis, Boca Raton, FL, USA, 2008

Toshikazu Wada, Fay Huang, Stephen Lin, Advances in Image and Video Technology, pp. 340–341, ISBN 978-3-540-92956-7, 2009

A.Z.Tirkel, G.A. Rankin, R.M. Van Schyndel, W.J.Ho, N.R.A.Mee, C.F.Osborne. "Electronic Water Mark". DICTA 93, Macquarie University. p.666-673

Raju Halder, Shantanu Pal, and Agostino Cortesi, Watermarking Techniques for Relational Databases: Survey, Classification and Comparison, The Journal of Universal Computer Science, vol 16(21), pp. 3164-3190, 2010.

Shen Tao: Watermarking Gis Data for Digital Map Copyright Protection, Canadian Cartographer, 1973, 10(2), pp. 112-122.

Sangita Zope- Chaudhari, P. Venkatachalam (2012): Robust Watermarking for Protection of Geospatial Data. 2012 IACSIT Hong Kong Conferences IPCSIT vol. 29 (2012)

Shelvie Nidya Neyman, Benhard Sitohang, Sobar Sutisna. Reversible Fragile Watermarking based on Difference Expansion Using Manhattan Distances for 2D Vector Map. Procedia Technology Volume 11, 2013, Pages 614–620. 4th International Conference on

Electrical Engineering and Informatics, ICEEI 2013

Zope-Chaudhari, S., P. Venkatachalam, K. M. Buddhiraju (2014): Robustness and Accuracy Assessment of Invisible Watermarking over Geospatial Vector Data. ACRS Procedding, Nay Pyi Taw.

Anbo Li , Bingxian Lin, Ying Chen, Guonian Lu: Study On Copyright Authentication of GIS Vector Data Based on Zero-Watermarking, Education Press, Beijing, China, 2006

Emir Ganic, Ahmet M. Eskicioglu. Robust DWT-SVD domain image watermarking: embedding data in all frequencies. Proceedings of the 2004 workshop on Multimedia and security Pages 166-174 ACM New York, 2004

Khan, A. and Mirza, A. M. 2007. Genetic perceptual shaping: Utilizing cover image and conceivable attack information during watermark embedding. Inf. Fusion 8, 4 (Oct. 2007), 354-365