Journal of Korea Multimedia Society Vol. 19, No. 8, August 2016(pp. 1453-1459)
http://dx.doi.org/10.9717/kmms.2016.19.8.1453

Encryption Algorithm using Polyline Simplification for GIS Vector Map

N.V. Bang[†], Suk-Hwan Lee[††], Kwang-Seok Moon[†††], Ki-Ryong Kwon[††††]

ABSTRACT

Recently, vector map has developed, used in many domains, and in most cases vector map data contains confidential information which must be kept away from unauthorized users. Moreover, the manufacturing process of a vector map is complex and the maintenance of a digital map requires substantial monetary and human resources. This paper presents the selective encryption scheme based on polyline simplification methods for GIS vector map data protection to store, transmit or distribute to authorized users. Main advantages of our algorithm are random vertices and transformation processes but it still meets requirements of security by random processes, and this algorithm can be implement to many types of vector map formats.

Key words: GIS Vector Map, Selective Encryption, DWT, Randomization.

1. INTRODUCTION

Vector map is created and developed by the merging system of cartography, statistical analysis, and database technology based on vector model [1, 2]. Vector map stores and manages all kinds of the geographic information data as geometric factor, topology and metadata by vector data.

Vector data provide a way to represent real world features within the GIS environment because vector data has advantages as need a small space or place for storage data; easily makes connection between topology and network; has a high spatial resolution and graphic representation spatial data closely likes handed map; easily for making projection and coordinates transformation. But the producing process is considerably complex and the maintenance of a digital map requires substantial monetary. So vector map is necessary to be protected and prevent illegal duplication and distribution of it. Moreover, applications of vector map in military domain require the high security, and must be kept away from unauthorized users. So vector map is necessary to be protected and prevent illegal duplication and distribution of it. In proposed algorithm, vector map is separated to select polyline/polygon layer. The three simplification algorithms are used to define the feature points in each object. After that, the randomly vertices of objects are selected based on the ratio of the feature points. Finally, it is randomized by randomization values and encrypted by using DWT transform.

Our paper is organized as follows. In section 2,

※ Corresponding Author : Kwang-Seok Moon, Address: (608-737) (599-1) Daeyeon-3dong, Namgu, Busan, Korea, TEL : +82-51-629-6257, FAX : +82-51-629-6230, E-mail : ksmoon@pknu.ac.kr

Receipt date : Jul. 28, 2016, Approval date : Aug. 12, 2016

[†] Dept. of IT Convergence and Applications Engineering, Pukyong National University
(E-mail : nguyenbang1619@gmail.com)

[††] Dept. of Information Security, Tongmyong University
(E-mail : skylee@tu.ac.kr)

[†††] Dept. of Electronics Engineering, Pukyong National University

[††††] Dept. of IT Convergence and Applications Engineering, Pukyong National University
(E-mail : krkwon@pknu.ac.kr)

※ This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2014R1A1A4A01006663)

we discuss the related works and in section 3, we explain the proposed selective encryption algorithm in detail. Then, in section 4 we perform experiments and discuss about the experimental results, evaluate the performance of algorithm. Finally, we conclude this paper in section 5.

2. RELATED WORKS

According to the recent growth of network digital media, data are needed to protect from distribution and illegal copying. Many approaches are researched for this issues; these include authentication, encryption, and time stamping.

Digital watermarking has been researched to solve the issues in vector map since 2000s. The traditional method embed secret information in some locations of vector map: [3] proposes certain rules, they help to select a set of coordinates of vertices, and editing them by using a certain range of precision; [4] modify coefficients in the frequency domain to complete watermarking hiding that is one of the important solution of watermarking algorithm, but the disturb to the vector map content is also existing, the resistance performance to data fitting, interpolation, scaling is poor. Due to the vector map high precision requirement, traditional watermarking algorithm can't meet the demand of practical application.

The full encryption algorithms usually encrypt all components of original data to change whole data. Wu et al. [5] consider characteristics of the storage, parameters and initial values of chaotic map. After that, he proposed a new compound encryption method, this process is not available to any type formats of data and object indexing. Li et al. [6] selected the vector dataset in external Oracle DBMS for encryption, and he used standard cryptography DES combining with an R-Tree spatial index. This algorithm encrypts the spatial index when the GIS dataset is transmitted to the client and designs the key management of public and private keys on a PKI system. In this process, the key length is short so it can not keep data on the DBMS with high security. Dakroury et al. [7] also described better the encrypting algorithm, AES and RSA cryptography are combined along with watermarking method that used in internet online service. This algorithm encrypts all parts of a shape-file using 256 bit for private key of a block cipher AES. But, this algorithm uses whole shape-files for encryption and they do not consider important features, it is taking a long time to handle.

The general approach is to separate the content into two parts. The first part is the public part, it is left unencrypted and made accessible to all users. The second part is the protected part; it is encrypted. Only authorized users have access to protected part. One important feature in selective encryption is to make the protected part as small as possible. The control factor (threshold value) helps to control encrypted data ratio in algorithm, by this way we can make security better. In the main, perceptual process is created based on partial encryption algorithms.

For vector map perceptual encryption, B.-J Jang et al. [8] presented a method, which encrypts parameters mean point and direction of mini coding objects in compression domain by XOR operator. The aim of this method is to select parameters after compression to encrypt by XOR operator. Giao et al. [9] select all vertices in a complex layer and they randomize them before to encrypt in DCT domain, they did not consider the important part in each layer. For these reasons, a new algorithm is proposed in selective encryption topic for multimedia applications, transmission and storage of vector

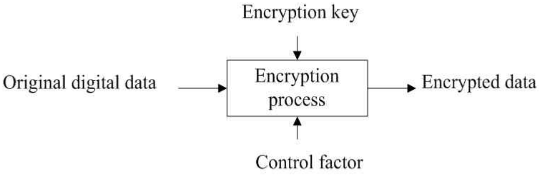


Fig. 1. The concept of selective encryption.

map data.

3. PROPOSED ALGORITHM

In our paper, the proposed method selects randomly vertices for encryption based on simplification algorithms. In Fig. 2, we show the schematic of algorithm, and the step-by-step is explained in detail:

The vector map data includes layers and each layer includes geometry feature which is illustrated by geometric objects, and attribute features. Attribute data describes specific map features but is not inherently graphic. The geographic information used a set of coordinates to provide position and shapes of objects as point, polyline and polygon. Thus, we consider the content of layers in a map consists of two parts. The first part includes insignificant information as text and annotation. The second part is the geometric data needed to protect, includes geometric objects as point, polyline and polygon.

Moreover, the point only uses a pair of coordinates to represent simple, small and zero-dimensional objects in the real on the map while polylines and polygons use a set of coordinate to represent complex structure and huge objects. Therefore, polylines and polygons are targets to select for vector map security.

3.1 Backbone of object

As you know, a layer is set of objects and an objectis a set of vertices $O_{ij} = \{v_{ijk} | k \in [1, |O_{ij}|]\}$ with $|O_{ij}|$ is the cardinality of the object. The object is separated to m groups $G = \{G_k | k \in [1, m]\}$, $m = |O_{ij}|/n$, n is the total of vertices in one group. Object's backbone is set of vertices with a vertex is average point between two continuous vertices in a group, as shown in Fig. 3. Therefore, backbone $B = \{B_k | k \in [1, m]\}$ with $\boldsymbol{B_k}$ is a backbone section in group $\boldsymbol{G_k}$.

3.2 Breakpoint definition

We use the scale factor α for controlling the simplification quantity and for generating breakpoints with different ratios. Thus, we set parameters for the three simplification algorithms using the scale factor and initial parameters:

$$\delta = \delta_0 * (1 + \alpha) \text{ for DP} \quad (1)$$

$$\epsilon = \epsilon_0 * (1 + \alpha) \text{ for SF} \quad (2)$$

$$\gamma = \gamma_0 * (1 + \alpha) \text{ for LA} \quad (3)$$

where $\delta_0, \epsilon_0,$and γ_0 are the initial distance thresholds for DP, SF, and LA. The scale factor α controls the number of breakpoints. If α=-1 ,a backbone is not simplified. If α increases from -1, the total number of breakpoints also increase.

Given a backbone $\boldsymbol{B}$ of object, let us consider

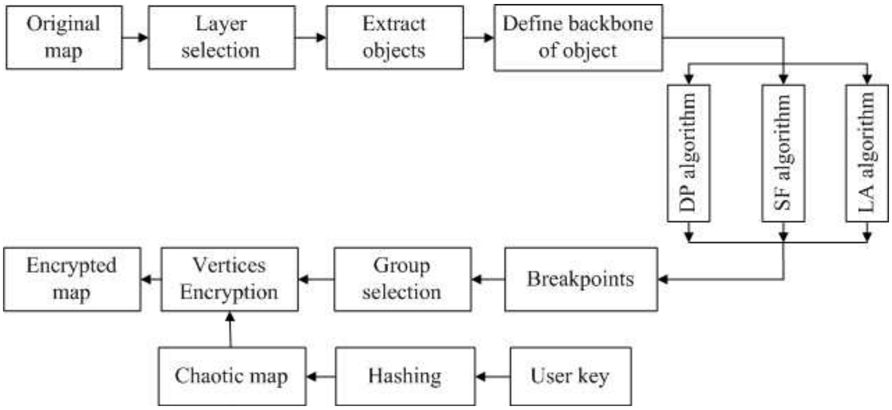
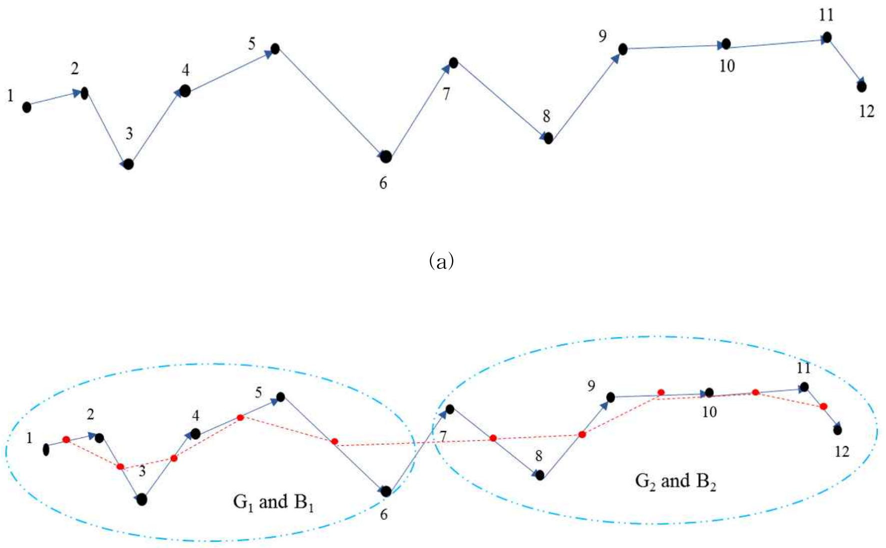


Fig. 2. The proposed encryption process of vector map data.



(a)

(b)

Fig. 3. Object' s backbone definition: (a) object and (b) backbone n=6.

that $\boldsymbol{B}$ consists of N vertices, $B=\{v_{b1},v_{b2},\ldots,v_{bN}\}$, and a vertex has two coordinate values $v_{bi}=\{x_{bi},y_{bi}\}$. We generate three simplified backbones of backbone $\boldsymbol{B}$ using the DP, SF, and LA algorithms: $B_{DP}, B_{SF}, \text{and} B_{LA}$

Breakpoints $\boldsymbol{B}'$ for a backbone $\boldsymbol{B}$ as vertices that exist in three simplified backbone:

$$B' = B_{DP}\cap B_{SF}\cap B_{LA} = \{v'_{bk}|k\in[1,N_B]\} \quad (4)$$

Thus, breakpoints are common vertices in three simplified backbone of a backbone. This mean that they represent the main shape of the polyline and should be kept simplified. N_B is the number of vertices in the breakpoints. In the next step, breakpoints is used to select vertices group for encryption.

3.3 Vertices encryption

In mathematics, a chaotic map is a map that exhibits some sort of chaotic behavior, by following:

$$x_{k+1}=\eta x_k(1-x_k) \quad (5)$$

We use the user key to create random coefficients R_i and key values for a layer. These values are created randomly the first values by SHA-512 process using key given by user [9], 512 bit key size. And other values are generated by using Chaotic map as equation (5).

In group G_k, if the total number of vertices of backbone section B_k bigger than N_B/m (N_B is the number of breakpoints, m is the number of groups), we select all vertices in the selected group G_k and encrypt them by steps, as follow:

- We arrange all the first vertex of the selected groups in a layer into 1D-array $V=\{v_{i1},v_{j1},\ldots,v_{k1}\}$.
- These vertices are randomized by multiplying them using random coefficients R_i.
- After that, we apply DWT-k level to get DWT coefficients. In DWT domain, we encrypt level k coefficient and inverse DWT-k level. We get $V'=\{v'_{i1},v'_{j1},\ldots,v'_{k1}\}$.
- With the selected group G_k, other vertices are changed following the variation of the first vertex in this group by equation:

$$v'_{n*(k-1)+i}=v_{n*(k-1)+i}+(-1)^{n*(k-1)+i*}v'_{k1} \quad (6)$$

3.4 Decryption process

The reverse process is applied to decrypt the encrypted map. To perform decryption, after we calculate thresholds in a layer, we use the decryption block to decrypt the encrypted significant objects. If correct key is employed at the time of decryption, then the decrypted map would by a replica of the original map. In the case of an incorrect decryption key, the output map is vary.

4. EXPERIMENTAL RESULTS

4.1 Vertices selection

Our method select randomly vertices based on different precisions by adjusting the scale factor α in Eq. (1)-(3) (that determines the quantity of simplification). $\alpha=-1$ means that our method by passes the simplification. $\alpha=0$ means that our method simplifies a map using the initial parameters $(\delta_0, \epsilon_0, \gamma_0)$of the DP, SF, and LA algorithms. Fig. 4 shows the ratio of breakpoint number and encrypted vertices calculated by formula: number of breakpoints/ number of vertices of object's backbone.

4.2 Visualization

Experimental results Fig. 5 and Fig. 6 show the proposed algorithm changes whole maps. The proposed method has much lower computational complexity than AES or DES because we only select and encrypt some vertices in objects.

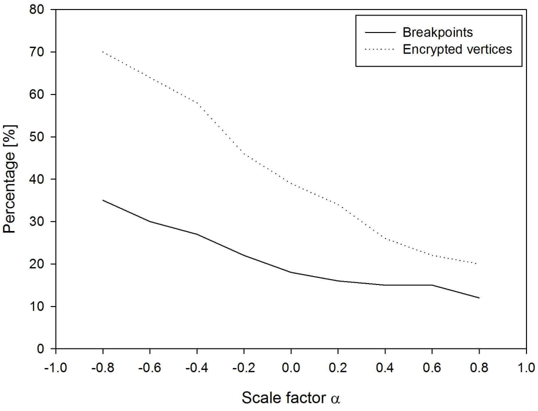


Fig. 4. Ratio of breakpoints and encrypted vertices.

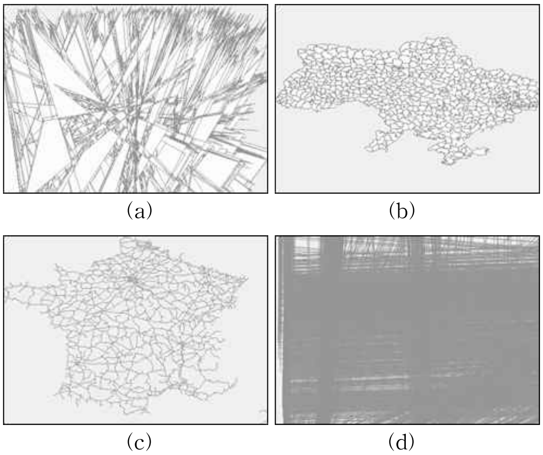


Fig. 5. (a),(c) original polyline/polygon layer; (b),(d) encrypted polyline/polygon layer.

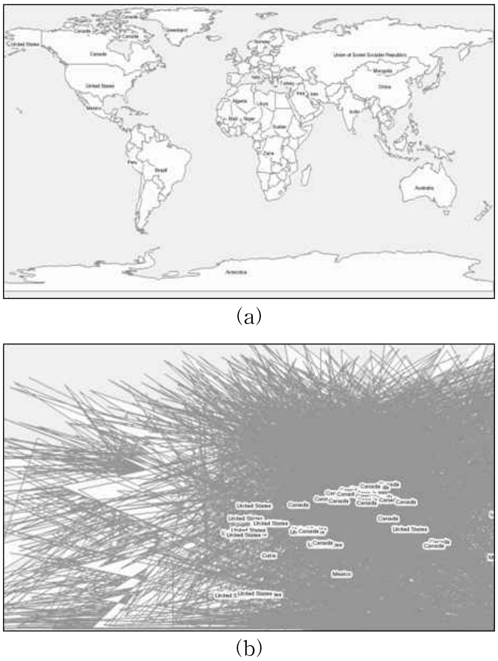


Fig. 6. Experimental result with full scaling layers 1: 5000: (a) original map, (b) encrypted map.

4.3 Algorithm comparison

The proposed method is compared with two existing algorithms Giao [10] and Bang [11]. In these

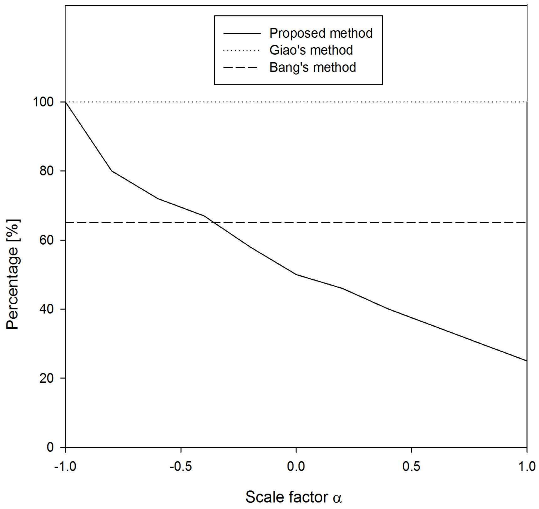


Fig. 7. Ratio of the encrypted data in our method and the existing methods.

papers, first author encrypted all data in original file and he did not consider important part in each layer. The second author selected all vertices of the significant objects (defined based on threshold value) in a layer for encryption, it seem quite easily to attack, because he defined threshold value very simple lead to the algorithm is so weak. Our method select randomly some vertices (that is defined by owner based on scale factor α and three initial parameters) for encryption, attacker will be very difficult to determine the encrypted data and predict key. Fig. 7 shows the ratio of encryption data in comparison with two existing methods.

5. CONCLUSION

In our paper, we created a new method which aim to reduce ratio of encrypted data in GIS vector map but still assure performance and high security. This considers how to select randomly vertices of object in a layer and encrypts randomly components by simplification algorithm and Chaotic-map in DWT domain. This process encrypt some level-k DWT coefficients lead to change whole map. We also confirm that: Human perception do not see any information in encrypted map, poor error in decryption step, computation time is less than it in the existing methods, high security and a large amount of GIS vector map data can be protected by this algorithm.

REFERENCE

[1] M.F. Goodchild, “Twenty Years of Progress: GIS Science in 2010,” *Journal of Spatial Information Science,* No. 1, pp. 3-20, 2010.

[2] GIS Vector Map, http://www.mapmart.com/Products/DigitalVectorMapping.aspx, (accessed Mar. 2016).

[3] R. Ohbuchi, H. Ueda, and S. Endoh, “Robust Watermarking of Vector Digital Maps,” *Proceeding of IEEE International Conference on Multimedia and Expo,* Vol. 1, pp. 577-580, 2002.

[4] C. Wang, Z. Peng, Y. Peng, L. Yu, J. Wang, and Q. Zhao, “Watermarking Geographical Data on Spatial Topological Relations,” *Proceeding of Multimedia Tools and Applications*, Vol. 57, Issue 1, pp. 67-69, 2012.

[5] F. Wu, W. Cui, and H. Chen, “A Compound Chaos-Based Encryption Algorithm for Vector Geographic Data under Network Circumstance,” *Proceeding of Cardholder Information Security Program,* Vol. 1, pp. 254-258, 2008.

[6] G. Li “Research of Key Technologies on Encrypting Vector Spatial Data in Oracle Spatial,” *Proceeding of International Conference on Industrial Electronics and Computer Science*, pp.1-4, 2010.

[7] Y. Dakroury, I.A. El-ghafar, and A. Tammam, “Protecting GIS Data Using Cryptography and Digital Watermarking,” *International Journal of Computer Science and Network Security,* Vol. 10, No. 1, pp. 75-84, 2010.

[8] B. Jang, S. Lee, and K. Kwon, “Perceptual Encryption with Compression for Secure Vector Map Data Processing,” *Journal Digital Signal Processing,* Vol. 25, pp. 224-243, 2014.

[9] RSA Laboratories, *PKCS #5 v2.1: Password-Based Cryptography Standard*, 2006.

[10] G.P. Ngoc, G.C. Kwon, S.H. Lee, and K.R. Kwon, "Selective Encryption Algorithm Based on DCT for GIS Vector Map," *Journal of Korea Multimedia Society*, Vol. 17, No. 7, pp. 769-777, 2014.

[11] N.V. Bang, K.S. Moon, S.H. Lee, and K.R. Kwon, "Selective Encryption Scheme Based on DFT, DWT Domain for GIS Vector Map Data," *Proceeding of The 11th International Conference on Multimedia Information Technology and Applications*, pp. 115-117, 2015.

Bang Nguyen Van

He received a B.S. degree in School of Electronic & Telecommunication from Hanoi University of Science & Technology (HUST) in 2014. Currently, he is a Master student in Multimedia Communication & Signal Processing Lab in PKNU. His research interests include video processing & application, GIS applications, data security, and smart system.

Suk-Hwan Lee

He received a B.S., a M.S., and a Ph. D. degrees in Electrical Engineering from Kyungpook National University, Korea in 1999, 2001, and 2004 respectively. He is currently an associate professor in Department of Information Security at Tongmyong University. His research interests include multimedia security, digital image processing, and computer graphics.

Kwang-Seok Moon

He received the B.S., M.S., and Ph.D. degrees in electronics engineering from Kyungpook National University in 1979, 1981, and 1989 respectively. He worked at Tokyo University in 1988. He is currently a professor in Department of Electronics Engineering at the Pukyong National University. He has researched Jackson State University in USA on 2000~2002 with visiting professor. His research interests are in the area of digital image processing, adative signal processing, and multimedia communication.

Ki-Ryong Kwon

He received the B.S., M.S., and Ph.D. degrees in electronics engineering from Kyungpook National University in 1986, 1990, and 1994 respectively. He worked at Hyundai Motor Company from 1986-1988 and at Pusan University of Foreign Language from 1996-2006. He is currently a professor in Department of IT Convertgence and Application Engineering at the Pukyong National University. He has researched University of Minnesota in USA on 2000~2002 with Post-Doc. and Colorado State University on 2011~2012 with visiting professor. He is currently the President of Korea Multimedia Society. His research interests are in the area of digital image processing, multimedia security and watermarking, bioinformatics, weather radar information processing.