Journal of Korea Multimedia Society Vol. 17, No. 7, July 2014(pp. 769-777)
http://dx.doi.org/10.9717/kmms.2014.17.7.769

Selective Encryption Algorithm Based on DCT for GIS Vector Map

P.N. Giao[†], Gi-Chang Kwon[††], Suk-Hwan Lee[†††], Ki-Ryong Kwon[††††]

ABSTRACT

With the rapid interest in Geographic Information System (GIS) contents, a large volume of valuable GIS dataset has been distributed illegally by pirates, hackers, or unauthorized users. Therefore the problem focus on how to protect the copyright of GIS vector map data for storage and transmission. At this point, GIS security techniques focusing on secure network and data encryption have been studied and developed to solve the copyright protection and illegal copy prevention for GIS digital map. But GIS vector map data is very large and current data encryption techniques often encrypt all components of data. That means we have encrypted large amount of data lead to the long encrypting time and high complexity computation. This paper presents a novel selective encryption scheme for GIS vector map data protection to store, transmit or distribute to authorized users using K-means algorithm. The proposed algorithm only encrypts a small part of data based on properties of polylines and polygons in GIS vector map but it can change whole data of GIS vector map. Experimental results verified the proposed algorithm effectively and error in decryption is approximately zero.

Key words: GIS Vector Map, Selective Encryption, K-means Algorithm, Vector Map Security

1. INTRODUCTION

GIS is a system which designed to capture, store, manipulate, analyze, and manage all kinds of the geographic information and it is the merging system of cartography, statistical analysis, and database technology [1-2]. It consists of hardware, software, and GIS data. GIS allows us to view, understand, question, interpret, and visualize data in many ways that reveal relationships, patterns, and trends in the form of maps, globes, reports, and charts.

GIS has been used in military and commercial applications for many years. The main component of GIS is the data. The GIS data has two important properties. Firstly, the effort it takes to put it in a form suitable for use in the GIS applications. This effort increases its cost. Secondly, in most cases the GIS Data contains confidential information which must be kept away from unauthorized users. Such confidential information includes GIS layers containing troop locations and additional information like movements and mines places in a tactical environment. Hence, it is very important to protect the GIS data. Moreover, the GIS data is too expensive so we have to prevent illegal duplication and distribution of it. Nowadays, it is too easy for a company to buy some GIS layers, make

※ Corresponding Author : Ki-Ryong Kwon, Address: (608-737) (599-1) Daeyeon-3dong, Namgu, Busan, Korea, TEL : +82-51-629-6257, FAX : +82-51-629-6230, E-mail : krkwon@pknu.ac.kr
Receipt date : Mar. 14, 2014, Revision date : May. 9, 2014
Approval date : Jun. 5, 2014
[†] Dept. of IT Convergence and Applications Eng., Pukyong National University
(E-mail : ngocgiaofet@gmail.com)
[††] Dept. of IT Cooperative System, Gyeongbuk Provincial College
(E-mail : kwon0819@daum.net)
[†††] Dept. of Information Security, Tongmyong University
(E-mail : skylee@tu.ac.kr)
[††††] Dept. of IT Convergence and Applications Eng., Pukyong National University
(E-mail : krkwon@pknu.ac.kr)
※ This work was supported by a Research Grant of Pukyong National University (2013Year)

illegal copies from them and distribute or sell them many times without taking any permission from the original GIS data provider. So we have to enforce some kinds of access control on it because the GIS data is sensitive and must not be accessed by unauthorized users.

In section 2, we introduce related works, and in section 3 we present selective encryption scheme for GIS vector map data protection. Finally, we implement the proposed scheme, and show experimental results in section 4.

2. RELATED WORKS

The GIS vector map data includes layers. Each layer is a basic unit of geographical objects which are described and managed in a map. These objects describe the topography and geographical features of real objects or a certain place. Each layer consists of an amount of vector data which uses pairs of coordinates to describe as point, polyline and polygon [3-4], as shown Fig. 1. Officially, the point is used to present simple or small objects in the reality on the map while polyline and polygon are used to present complex and large objects. Thus, our algorithm only performs selective encryption for polylines and polygons in GIS vector map.

The general approach of selective encryption is to separate the content into two parts. The first part is the public part, which is un-encrypted and accessible by all users [5-11]. The second part is the protected part; it is encrypted. Only authorized users have access to protected part. Polylines and polygons are selected, and encrypted by random keys combine with randomization and clustering process by K-means algorithm [12], random algorithms in DCT domain based on their geographical features [13]. Our algorithm encrypts only some selective DC values of polylines, polygons in DCT domain but it changes the whole map.

3. PROPOSED SELECTIVE ENCRYPTION ALGORITHM

Our method aims to encrypt GIS vector map perceptually and entirely using a few of selected

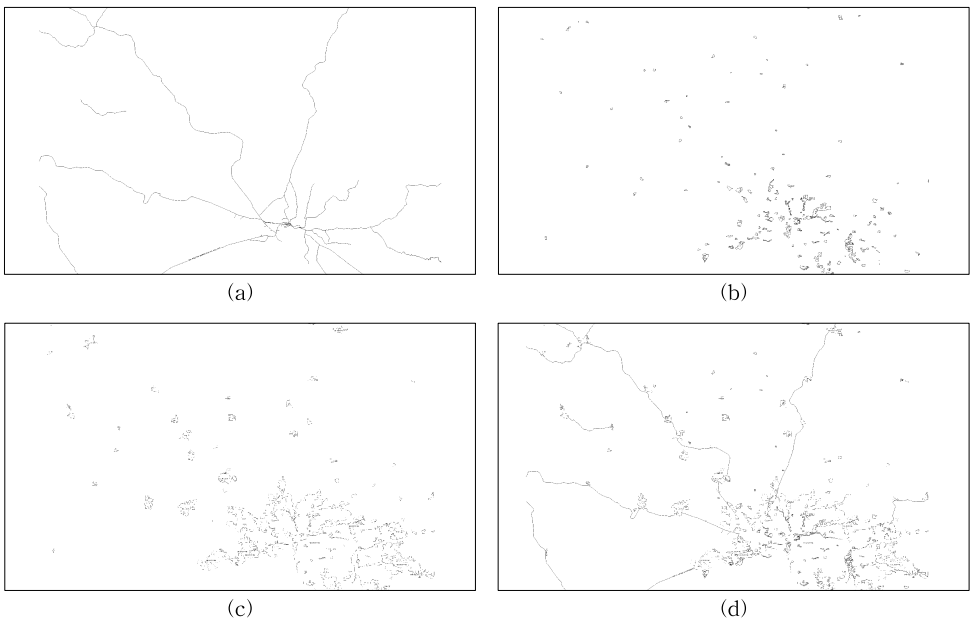

Fig. 1. An example GIS vector map with city, river and country layers; (a) Railway layer, (b) Lake layer, (c) Building layer, and (d) Railway + Lake + Building layers.

values, it is called as vector map selective encryption.

3.1 Selective Encryption Process

The selective encryption algorithm follows as Fig. 2. Our algorithm consists of processes as data extraction to have polylines and polygons, polylines and polygons clustering using K clusters, vertices randomization of polylines and polygons by random coefficients using random key. Next, it applies DCT processing for randomized vertices to get DCT coefficients, and then multiply DC coefficients of each cluster with a random value which is created by another random key. Finally, it performs inverse discrete cosine transform (IDCT).

In order to encrypt selectivity, we compute the total number of polylines N_{PLi}, total number of polygons N_{PGi} in i^{th} layer. Each polyline/polygon has attributes such as the number of parts and the number of points. These attributes in each polyline/polygon is different. So, we used them to classify N_{PLi} polylines, N_{PGi} polygons into K clusters using K-means algorithm. We have N_{PLi} polylines, N_{PGi} polygons in i^{th} layer, and we need to cluster them into K groups where $K=\{k_g|g\in[1,K]\}$. Each group k_g in K groups is described by a centroid $C_g=\{x_{cg},y_{cg}\}$. Considering number of parts N_{pa-ij}

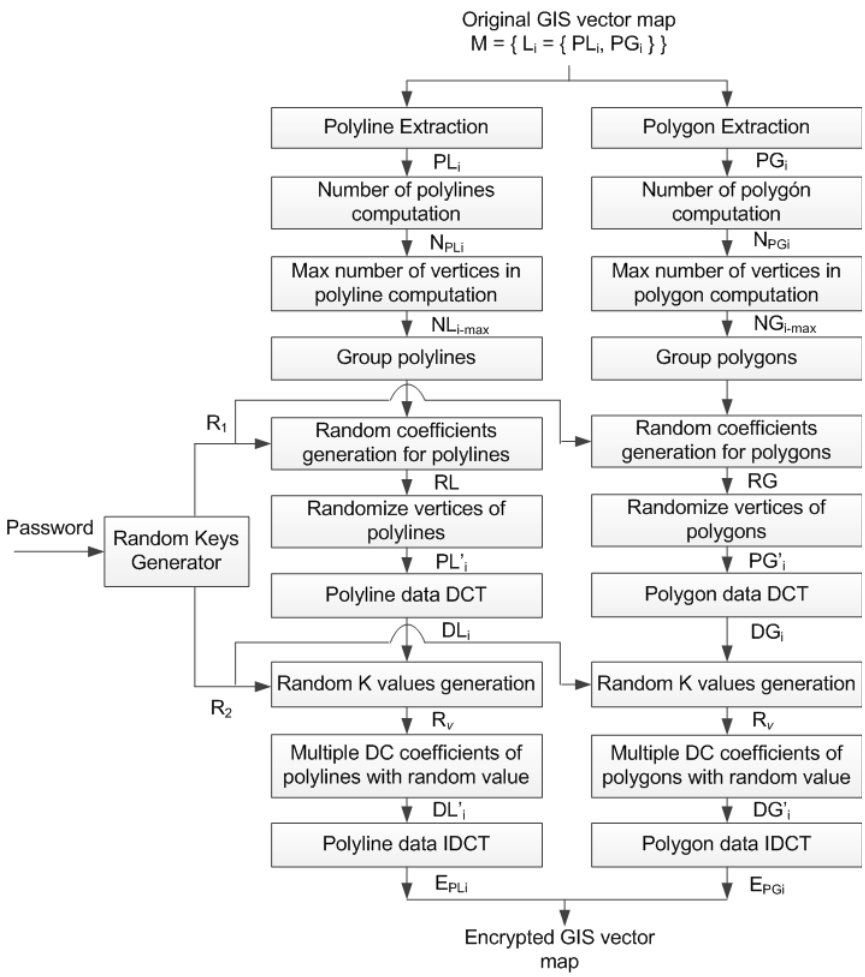

Fig. 2. Selective encryption algorithm for polyline/polygon.

and number of points N_{po-ij} in j^{th} polyline/polygon are coordinates in two dimensional space. And j^{th} polyline/polygon is represented as a point which has coordinates (N_{pa-ij}, N_{po-ij}) in that two dimensional space. The j^{th} polyline/polygon is classified in group k_g using the shortest Euclidean distance to C_g follow as equation (1). D_{jg} is the Euclidean distance from j^{th} polyline/polygon to centroid C_g, and calculated by equation (2).

$$pl_{ij}/pg_{ij} \in k_g | g \in [1, K], \quad \text{if } D_{jg} = \min\{D_{j1}, \cdots, D_{jK}\} \quad (1)$$

$$D_{jg} = \sqrt{(N_{pa-ij} - x_{cg})^2 + (N_{po-ij} - y_{cg})^2} \quad (2)$$

Then, we find $NL_{i-\max}$ of the max number of vertices in a polyline, and $NG_{i-\max}$ of the max number of vertices in a polygon in i^{th} layer. With values $NL_{i-\max}$, $NG_{i-\max}$ and K, we generated random $NL_{i-\max}$ coefficients where $RL = \{rl_k | k \in [1, NL_{i-\max}]\}$ for polylines, random $NG_{i-\max}$ coefficients where $RG = \{rg_k | k \in [1, NG_{i-\max}]\}$ for polygons by random key R_1 using equations (3) and (4):

$$RL = \{rl_k = Random(R_1, k) | \ k \in [1, NL_{i-\max}]\} \quad (3)$$

$$RG = \{rg_k = Random(R_1, k) | \ k \in [1, NG_{i-\max}]\} \quad (4)$$

From $NL_{i-\max}$ and $NG_{i-\max}$ coefficients, we randomize them with vertices in polylines, polygons follow as equations (5) and (6). These random coefficients will be applied to all polylines/polygons in a layer depend on the number of vertices in a polyline/polygon because number of vertices in a polyline $NL_i \le NL_{i-\max}$, number of vertices in a polygon $NG_i \le NG_{i-\max}$. And each layer will be applied different random coefficients. After randomization step polylines/polygons are encrypted by random key R_1, and we receive N_{PLi} new polylines with $PL_i' = \{pl_{ij}' | \ j \in [1, N_{PLi}]\} = \{vl_{i,j,k}' | \ j \in [1, N_{PLi}], k \in [1, NL_{ij}]\}$, and N_{PGi} new polygons with $PG_i' = \{pg_{ij}' | \ j \in [1, N_{PGi}]\} = \{vg_{i,j,k}' | \ j \in [1, N_{PGi}], k \in [1, NG_{ij}]\}$. Fig. 3(a) shows a randomized example for polyline.

$$PL_i' = PL_i \times RL = \{vl_{i,j,k}' = vl_{i,j,k} \times rl_k | \ j \in [1, N_{PLi}], k \in [1, NL_{ij}]\} \quad (5)$$

$$PG_i' = PG_i \times RG = \{vg_{i,j,k}' = vg_{i,j,k} \times rg_k | \ j \in [1, N_{PGi}], k \in [1, NG_{ij}]\} \quad (6)$$

We continue to apply DCT for these new polylines/polygons to get a set of transformed polylines DL_i by equation (7) and a set of transformed polygons DG_i by equation (8).

$$DL_i = DCT[PL_i'] = \{dl_{ij} | j \in [1, N_{PLi}]\} = \{dvl_{i,j,k} | \ j \in [1, N_{PLi}], k \in [1, NL_{ij}]\} \quad (7)$$

$$DG_i = DCT[PG_i'] = \{dg_{ij} | j \in [1, N_{PGi}]\} = \{dvg_{i,j,k} | \ j \in [1, N_{PGi}], k \in [1, NG_{ij}]\} \quad (8)$$

After DCT processing, we continue to encrypt polylines/polygons one more time by multiplying DC coefficients of transformed polylines/polygons with one corresponding random value to their group, from K random values follow as equations (9), (10) and Fig. 3(b). K random values are $R_v = \{rv_g | g \in [1, K]\}$, and generated by random key R_2

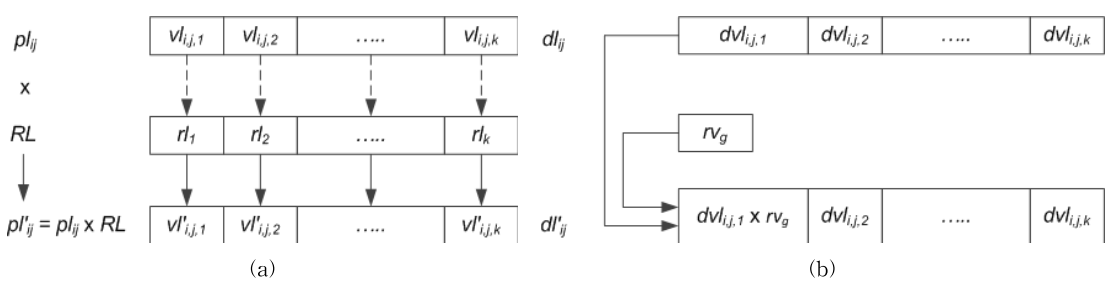

Fig. 3. Example of randomization and multiplication for polyline, (a) Randomized example for polyline, (b) Multiplying DC coefficient with random value.

using the used random algorithm above.

$$DL_i^{'} = \{dvl_{i,j,1} \times rv_g, dvl_{i,j,2}, \cdots, dvl_{i,j,NL_{ij}} |\ j \in [1, N_{PLi}], g \in [1, K]\} \quad (9)$$

$$DG_i^{'} = \{dvg_{i,j,1} \times rv_g, dvg_{i,j,2}, \cdots, dvg_{i,j,NG_{ij}} |\ j \in [1, N_{PGi}], g \in [1, K]\} \quad (10)$$

$$R_v = \{rv_g = Random(R_2, g) | g \in [1, K]\} \quad (11)$$

Finally, we perform IDCT to get encrypted polylines E_{PLi}, polygons E_{PGi} by equations (12) and (13).

$$E_{PLi} = IDCT(DL_i^{'}) = \{el_{ij} |\ j \in [1, N_{PLi}]\} = \{evl_{i,j,k} |\ j \in [1, N_{PLi}], k \in [1, NL_{ij}]\} \quad (12)$$

$$E_{PGi} = IDCT(DG_i^{'}) = \{eg_{ij} |\ j \in [1, N_{PGi}]\} = \{evg_{i,j,k} |\ j \in [1, N_{PGi}], k \in [1, NG_{ij}]\} \quad (13)$$

for $i \in [1, N_M]$.

3.2 Selective decryption process

The decryption algorithm for these polylines and polygons shown by Fig. 4 is the inverse process of selective encryption given at Fig. 2. Similar with the selective encryption process, we must also extract the protected data which consists of encrypted polylines and encrypted polygons, compute number of polylines and polygons, and find maximum number of vertices in polylines and polygons.

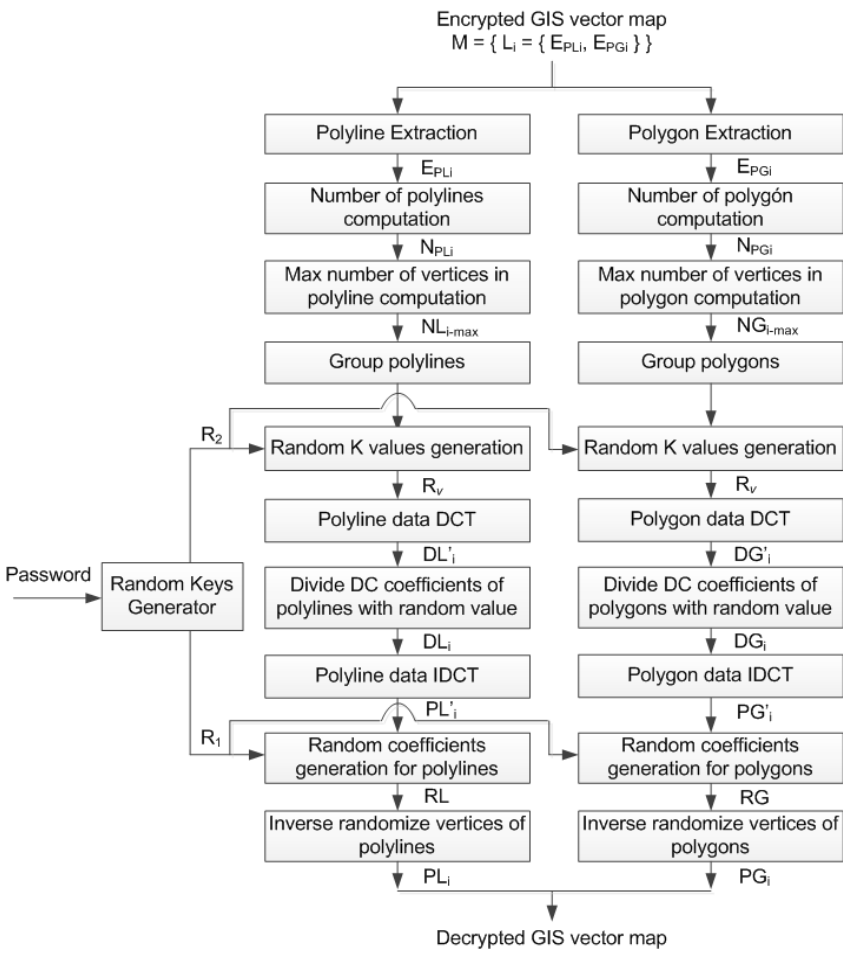

Fig. 4. Selective decryption algorithm for polyline/polygon.

The next step is to divide them into several groups by using K-means algorithm, similar with the encryption process, because the encryption changes the value of vertices only. Then, random coefficients and random values are generated again by random generator using random keys. Firstly, encrypted polylines and encrypted polygons are transformed using DCT and the DC coefficients are divided by random values. Secondly, they are inversed using IDCT to get randomized polylines and polygons again. Finally, we perform inverse randomization by dividing values of polylines/polygons in IDCT domain for random coefficients to have decrypted polylines and polygons.

4. EXPERIMENTAL RESULTS

We used 1:5000, 1:10000, and 1:100000 scaling maps in our experiments. Firstly, we experimented with each polyline layer and polygon layer with the scale of 1:5000. Then, we tested the full layers of 1:10000 and 1:100000 scale. Experimental results with polyline layer, polygon layer and full maps show that all maps are changed as given by Fig. 5 and Fig. 6. Unauthorized user cannot see anything on map because we changed polylines and polygons through four processes: randomization, DCT, multiplication, and IDCT using random keys R_1, R_2.

Table 1. The result of loss accuracy

Map	Original (Kb)	Encryption (Kb)
Polyline layer	68	68
Polygon layer	449	449
Map 1:10000	2724	2724
Map 1:100000	45,938	45,938

Our selective encryption scheme only changes values of vertices in polylines and polygons of the map. It did not alter the size of encrypted file. The result of loss accuracy is shown in Table 1. In addition, DCT and IDCT are not processes absolutely.

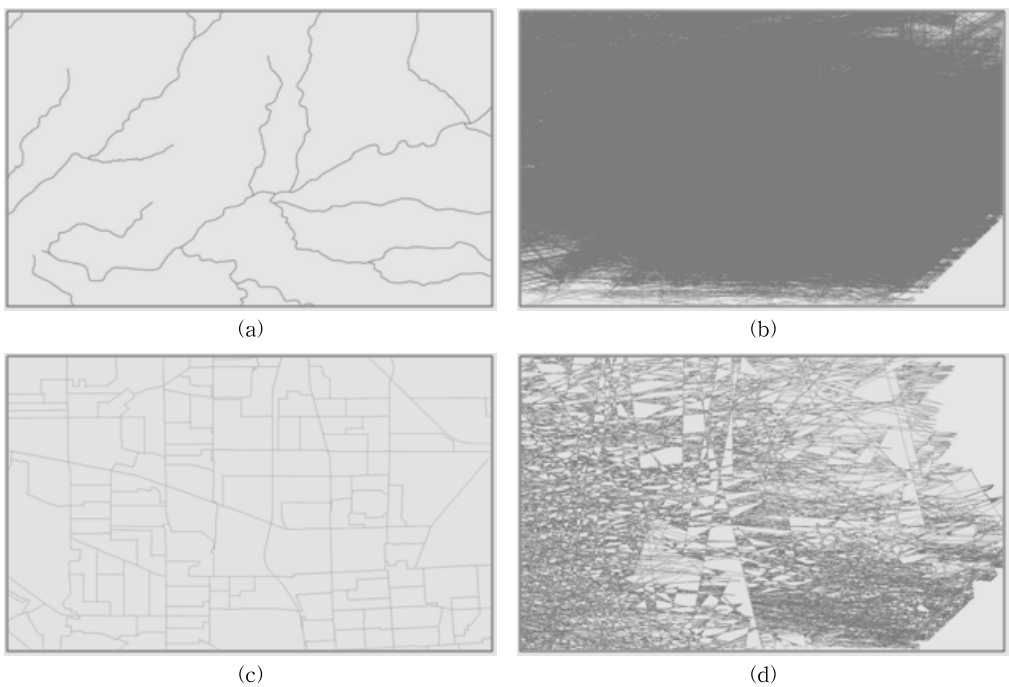

Fig. 5. Experimental result with scaling layers 1:5000; (a) original polyline layer, (b) encrypted polyline layer, (c) original polygon layer, and (d) encrypted polygon layer.

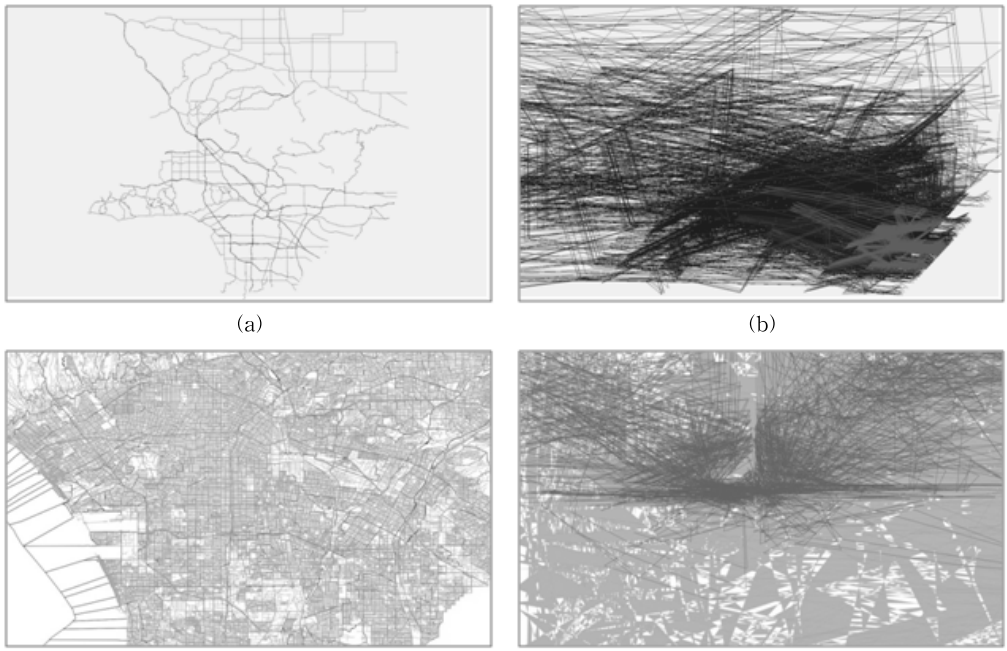

Fig. 6. Experimental result with full scaling map 1:10000, 1:100000; (a) original map 1:10000, (b) encrypted map 1:10000, (c) original map 1:100000, and (d) encrypted map 1:100000.

That means, if we have an input sequence x_n, and we perform DCT to get X_k, and next we perform IDCT to get input sequence again $x_n^{'}$, it shows that $x_n^{'}$ is not absolutely equal to x_n because the cosine value is not integer. However, in GIS vector map data, vertices are stored in double type such that the errors between original vertices and decrypted vertices values are approximately zero as given by Table 2.

Table 2. The error between original coordinates and decrypted coordinates

Original	Decryption	Error
30.389433636	30.389433636…	3.5171865420125E-12
31.441894545	31.441894544…	2.57927013080916E-12
30.395796636	30.395796635…	1.24096288800501E-11
31.440130545	31.440130545…	8.66862137627322E-13
…	…	…
31.842996636	31.8429966359…	1.56319401867222E-13
31.523812545	31.523812545…	4.9737991503207E-14

Finally, the distance between maps d_M is computed by equation (14):

$$d_M = \max\left\{dL_i(E_{Li}^{'}, E_{Li}^{''}) \mid i \in [1, N_M]\right\} \quad (14)$$

We used polyline map, polygon map to experiment other three times. Each time, we encrypted maps with different passwords which are used to create random keys as figure 3. Then we calculate d_M distances of each experimental time. In Table 3, experimental results show that d_M distance of two maps which are encrypted by different passwords from an original map is depend on passwords.

5. CONCLUSION

Our paper focuses on the issues how to encrypt GIS vector map selectivity with low complexity. We classified objects and encrypted them by random algorithms in DCT domain. Only some values are selected to encrypt by random processes but

Table 3. Experimental distance measure

Map	Distance		
	1st time	2nd time	3rd time
Polyline	1050.01961499225	2386.52934150553	2699.70358307989
Polygon	99578.4832826132	144041.811211162	41445.7732723328
Polyline+Polygon	243101064.262096	182060978.120168	61040175.5321669

it made changing whole map. Experimental results showed that the proposed algorithm has very effective with a large volume of GIS dataset. Decrypting results also show the error in decryption process approximates zero. Our algorithm can be applied to various file formats or standard vector map because only polyline and polygon objects are encrypted and can be used for map database security of GIS map service on/off-lines. Furthermore, our algorithm can be applied to various vector contents such as CAD and 3D content fields. Next time, we will continue to improve our algorithm by reducing number of selective values to reduce complexity while not change effectively.

REFERENCE

[1] K.E. Foote and M. Lynch, *Geographic Information Systems as an Integrating Technology: Context, Concepts, and Definitions*, June 2011.

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

[3] Geographic Information System(2004), http://en.wikipedia.org/wiki/Geographic_information_ system. (accessed Nov. 2013)

[4] GIS Vector Map(2006), http://en.wikipedia.org/wiki/Vector_map. (accessed Nov. 2013)

[5] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, and J.-J.Quisquater, "Overview on Selective Encryption of Image and Video: Challenges and Perspectives," *Hindawi Publishing Corporation EURASIP Journal on Information Security*, Vol. 2008, No. 5, Article ID:179290, pp. 18, 2008.

[6] M. Abomhara, *Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standard*, University of Malaya, Kuala Lumpur, 2011.

[7] M.Y. Hasan, F.A. Ahmed, and K. Abdelhamid, "Image Adaptive Selective Encryption of Vector Quantization Index Compression," *Proceeding of IEEE International Conference on Image Processing*, pp. 1277-1280, 2009.

[8] W. Puech and J.M. Rodrigues, "Crypto-Compression of Medical Images By Selective Encryption of DCT," *Proceeding of European Signal Processing Conference*, Vol. 1, pp. 225-228, 2005.

[9] S. Sharma and P. Pateriya, "A Study on Different Approaches of Selective Encryption Technique," *International Journal of Computer Science & Communication Networks*, Vol. 2, Issue 6, pp. 658-662, 2012.

[10] B.J. Jang. K.S. Moon. S.H. Lee. and K.R. Kwon. "Effective Compression Technique for Secure Transmission and Storage of GIS Digital Map," Journal of Korea Multimedia Society Vol.14. No2. pp.210-218, Feb. 2011.

[11] M.G Nazneen, S. Banu, Z. Tabassum, K. Fatima, and A. Shariff, "Selective Bitplane Encryption for Secure Transmission Of Image Data In Mobile Environment," *International Journal of Scientific & Technology Research*, Vol. 2, Issue 6, pp. 92-96, June 2013.

[12] Mac Queen, *Some Methods for Classification and Analysis of Multivariate Observations*, University of California Press, Berkeley, Calif., Vol. 1, pp. 281-297, 1967.

[13] G. Strang, "The Discrete Cosine Transform,"

Society for Industrial and Applied Mathematics, Vol. 41, No. 1, pp. 135-147, 1999.

Giao Pham Ngoc

Giao Pham Ngoc received a B.S. degree in School of Electronic & Telecommunication from Hanoi University of Science & Technology (HUST) in 2011, and Master degree from Pukyong National University (PKNU) in 2014. Currently, he is an researcher in Multimedia Communication & Signal Processing Lab in PKNU. His research interests include video processing & application, GIS applications, data security, and smart system.

Gi-Chang Kwon

Gi-Chang Kwon received a B.S., a M.S., and Ph.D. degrees from Andong National University in 1985, Daegu Univsrsity in 1993, and Yeongnam University in 2000. Currently, he is a professor in Department of IT Cooperative System at Geongbuk Provincial College. His research interests include multimedia contents and image processing, digital contents 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.

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 General Affair Vice 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.