Journal of Korea Multimedia Society Vol. 18, No. 7, July 2015(pp. 818-826)
http://dx.doi.org/10.9717/kmms.2015.18.7.818

Selective Encryption Scheme for Vector Map Data using Chaotic Map

N.V. Bang[†], Kwang-Seok Moon[††], Sanghun Lim[†††],
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. 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 the selective encryption scheme using hybrid transform for GIS vector map data protection to store, transmit or distribute to authorized users. In proposed scheme, polylines and polygons in vector map are targets of selective encryption. We select the significant objects in polyline/polygon layer, and then they are encrypted by the key sets generated by using Chaotic map before changing them in DWT, DFT domain. Experimental results verified the proposed algorithm effectively and error in decryption is approximately zero.

Key words: GIS Vector Map, Selective Encryption, DWT, DFT, Chaotic Map.

1. INTRODUCTION

The vector map, is also called GIS vector map, is a vector - based collection of Geographic Information System (GIS) data about earth at various levels of detail. Vector map is created and developed by the merging system of cartography, statistical analysis, and database technology based on vector model [1,2]. 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; has a high spatial resolution and graphic representation spatial data closely likes handed map; easily for making projection and coordinates transformation [3,4]. For those advantages, vector map is used in many domains, and GIS applications use vector map have provided general users with easy access to services via mobile devices or internet access. But the producing process of a vector map is considerably complex and the maintenance of a digital map requires substantial monetary and human

※ 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 : Apr 10, 2015, Revision date : May 16, 2015
Approval date : Jun 1, 2015
[†] Dept. of IT Convergence and Applications Eng., Pukyong National University
(E-mail : nguyenbang1619@gmail.com)
[††] Dept. of Electronics Eng., Pukyong National University
(E-mail : ksmoon@pknu.ac.kr)
[†††] Korea Institute of Civil Engineering and Building Technology (E-mail : slim@kict.re.kr)
[††††] Dept. of Information Security, Tongmyong University
(E-mail : skylee@tu.ac.kr)
[†††††] Dept. of IT Convergence and Applications Eng., Pukyong National University
※ 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), IT/SW Creative research program supervised by the NIPA (NIPA-2014-1195), and a grant from a Strategic Research Project (Development of a road weather information retrieval system based on automotive sensors) funded by the Korea Institute of Civil Engineering and Building Technology.

resources. And any companies can buy it, make illegal copies from them and distribute or sell them easily many times without taking any permission from the original GIS data provider. 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.

Our paper is organized as follows. In section 2, 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

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 [5,6], 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. Polyline is used to represent objects as road, contour line, and railway, so on. Polygon is used to represent objects as building, area, lake, boundaries and so on. 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 [7-11]. The second part is the protected part; it is encrypted.

From these reasons, our algorithm only performs selective encryption for polylines and polygons in GIS vector map. Only authorized users have access to protected part. Polylines and polygons are selected, and encrypted by the key sets generate from Chaotic map before changing them in DWT, DFT domain based on their geographical features [12,13]. Our algorithm encrypts only some coefficients in DWT domain by changing DC value in DFT domain but it changes the whole map.

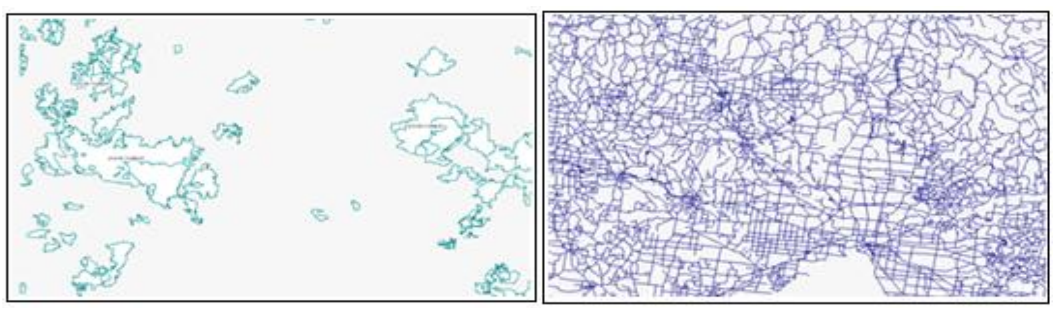
3. PROPOSED ALGORITHM

Our method aim to encrypt GIS vector map perceptually and entirely using a few of selected values, it is called as vector map selective encryption.

3.1 Encryption process

The schematic diagram of the proposed technique is illustrated in Fig. 2, and the step-by-step procedure is explained hereafter.

- An original GIS vector map is $M=\{L_i|i\in[1,N_M\}]$ with N_M layers in a map. A layer L_i is a set of



(a) (b)

Fig. 1. An example GIS vector map; (a) Forest layer, (b) Road layer.

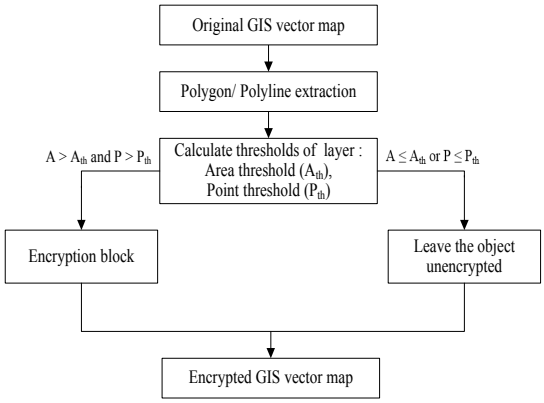


Fig. 2. Schematic diagram for proposed encryption technique.

objects of polylines and polygons $L_i = \{O_{ij} | j \in [1, N_i]\}$ with N_i is the total number of objects in L_i.

- An object O_{ij} have properties the total number of points (vertices) and the area of bounding box. Calculate the area threshold ($A_{i_{th}}$) and the point threshold ($P_{i_{th}}$) for each layer.
- Identify the significant objects by comparing the total number of points and the area of bounding box with two thresholds. For an insignificant object, leave it unencrypted. For a significant object, using encryption block to encrypt it by key sets generated from Chaotic map and user's password before changing them in DWT, DFT domain.

3.1.1 Object classification

Our algorithm only performs selective encryption for polyline/polygon in GIS vector map. However, each polyline/polygon layer has many objects and if we encrypt all of them, we also need many computation time. Each object has attributes such as the number of points (P), the area of bounding box (A), as shown in Fig. 3(a). Many objects are created from a few points and the value of bounding box's area is very small when compare with other objects in a layer. This object is very simple and mark it as an insignificant object, as shown in Fig. 3(b). With objects include many points and the area of bounding box is larger than, it also complex than and mark it as a significant object, as shown in Fig. 3(c).

Thus, we used probability distribution to define thresholds in each layer and identify which object is a significant or insignificant object by comparing object's features with thresholds.

The area threshold ($A_{i_{th}}$) and the point threshold ($P_{i_{th}}$) in a layer are defined as following:

- A layer L_i: $L_i = \{O_{ij} | j \in [1, N_i]\}$, N_i is the total number of objects in L_i .
- A object O_{ij} include two features: The area of bounding box (A_{ij}) and the total number of points (P_{ij}).
- Therefore, we have: $A_i = \{A_{ij} | j \in [1, N_i]\}$ and, $P_i = \{P_{ij} | j \in [1, N_i]\}$ in layer L_i.
- We used probability distribution to find threshold in set A_i, P_i :

$$A_{i_{th}} \in A_i \text{ and } F(A) = \sum P(A = A_{ij}; A_{ij} > A_{i_{th}}) = 0.5 \quad (1)$$

$$P_{i_{th}} \in P_i \text{ and } F(P) = \sum P(P = P_{ij}; P_{ij} > P_{i_{th}}) = 0.5 \quad (2)$$

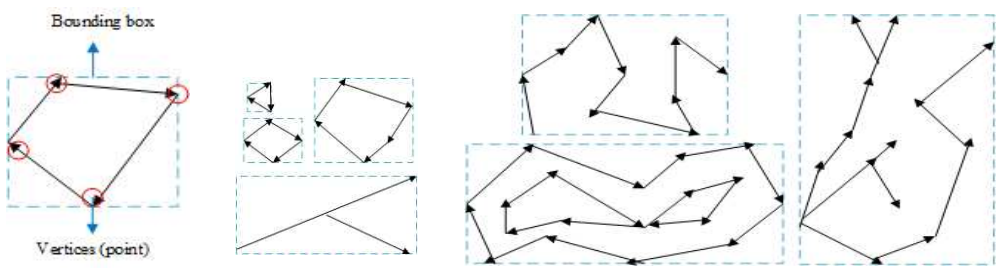


Fig. 3. An example about objects in a layer.

3.1.2 Chaotic map

The classical chaos system is a logistic map, which can be defined by following:

$$x_{k+1} = \mu x_k (1 - x_k) \quad (3)$$

Here $0 \le \mu \le 4$ is the coefficient of the map, k=0, 1, 2, . . . and all the values of $\{x_i\}$ appear in the range [0,1] for the initial value $x_0 \in [0,1]$. It is noted that Eq. (3) has the chaotic behavior [14,15] when μ appears in the range $[3.57, 4]$,and especially the chaotic behavior called Pomeau - Manneville scenario [16] when appears in the range $[3.57, 3.82]$.

3.1.3 Encryption block

We used the key to create two key sets (length of key set is 8) for a layer. It is created randomly the first key in each key set by SHA-512 algorithm from user key with key length is 512 bit. Other keys are generated by using Chaotic map as Eq. (3). Therefore, we have two key sets: $a = \{a_i | i \in [1, 8]\}$, $b = \{b_i | i \in [1, 8]\}$ and DC encryption value:

$$\left(\sum_{i=1}^{8} a_i + \sum_{i=1}^{8} b_i \right).$$

For a significant object, using encryption block to encrypt it, as shown in Fig. 4(a) and illustrate in Fig. 5, the step-by-step procedure is explained hereafter.

- We arrange all X, Y coordinates of the significant objects in a layer, into two 1D-arrays, given the length of segment is 8, the total number of segments in each array is: $n = N/8$, N is the length of 1D-array.
- With each segment, we encrypt all coordinates by using keys of two key sets a, b and create complex numbers as equation: $Z_i = X_i * a_i + j * Y_i * b_i, i \in [1,8]$.
- Apply DWT-3 level for each segment to get a set of first transformed values. In each segment, select the first coefficient of first transformed values and continue to apply DFT to get a set of second transformed values.
- After DFT processing, we continue to encrypt by multiplying the first DC coefficient with DFT encryption value by equation (4).

$$DC^* = DC^* \left(\sum_{i=1}^{8} a_i + \sum_{i=1}^{8} b_i \right) \quad (4)$$

- We perform IDFT to get a set of encrypted values of second transformed values. Replace the first coefficient in each segment by one encrypted value in step 6 and IDWT-3 level with each segment to get a set of encrypted values of first transformed values.
- Assign X, Y encrypted coordinates of the significant objects by image, real part of the encrypted complex values that is generated in step 7.

3.2 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,

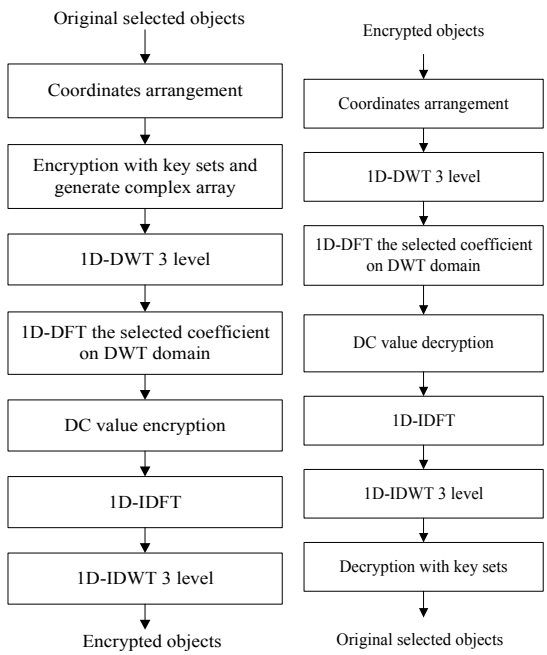


Fig. 4. Proposed (a) encryption and (b) decryption process for vector map.

as shown in Fig. 4(b). 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 Visualization

Experimental results figure 6 and figure 7 show the proposed algorithm changes whole maps. The proposed method has much lower computational complexity than AES (Advanced Encryption Standard) or DES (Data Encryption Standard) because we only select some coefficients in DWT domain and one DC value in DFT domain, encrypt it by key values.

4.2 Distance measure

The distance between original map and en-

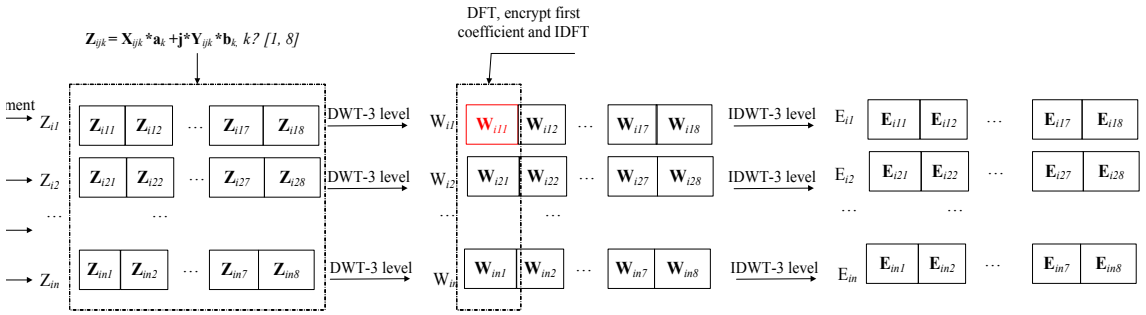
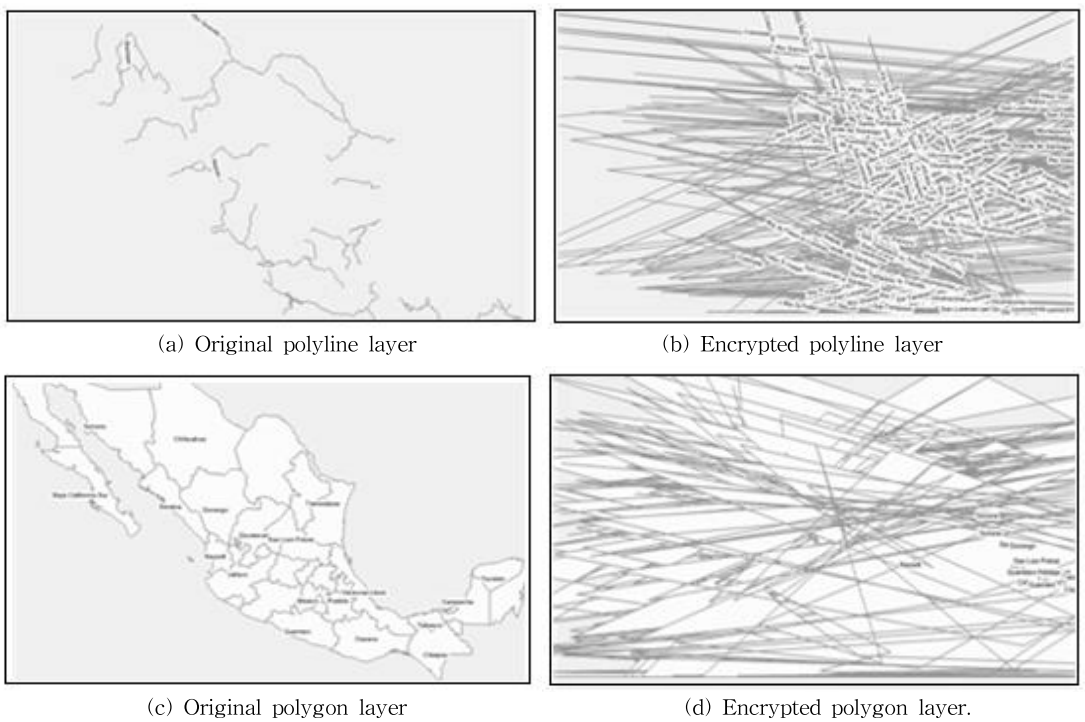


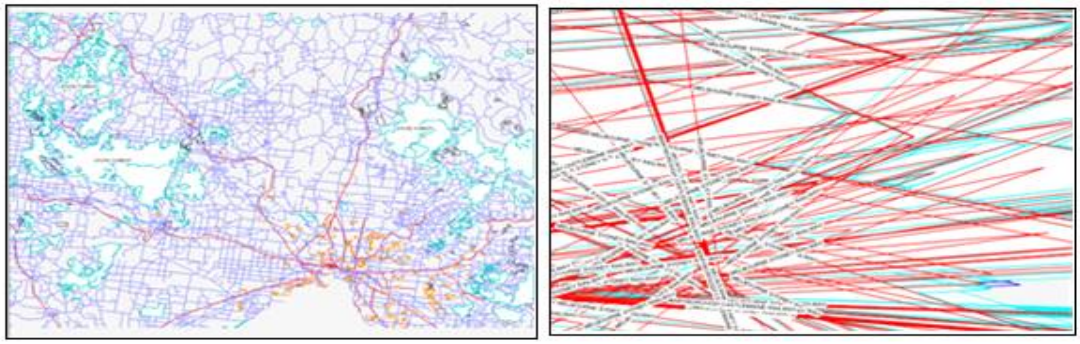
Fig. 5. Selective encryption process.



(a) Original polyline layer (b) Encrypted polyline layer

(c) Original polygon layer (d) Encrypted polygon layer.

Fig. 6. Experimental results of polyline/polygon layer.



(a) (b)

Fig. 7. Experimental result with full scaling layers 1:5000: (a) original map, (b) encrypted map.

crypted map is computed by equation (5):

$$D(E^{'},L)=\sum_{i=1}^{N} d(P_{ij}) \tag{5}$$

With L is a original map, $E^{'}(L)$ is corresponding encrypted map, N is the total number of objects in original map. And $d(P_{ij})$ is distance between corresponding objects in $E^{'}(L)$ and L.

We used same original map to experiment with different passwords K1 # K2. Then we calculate $D(E^{'},L)$ distance of each experimental time, as show in Table 1. .

4.4 Decryption error

Our selective encryption scheme only changes values of vertices in polylines and polygons of map. It did not alter the size of encrypted file, as shown in Table 2. In addition, we use hybrid transform to encrypt coordinates, that means, if we have an input sequence z_n, and we perform DFT to get Z_k, and next we perform IDFT to get input sequence again $z_n^{'}$, it shows that $z_n^{'}$ is not absolutely equal to z_n because sine and cosine value are 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 3.

Table 1: Experimental distance measure

Map	Original (kb)	Encryption (kb)
Polyline	45	45
Polygon	198	198
Map 1:10000	1526	1526
Map 1:100000	1753	1753

4.5 Security

Cryptographic security: In our algorithm, by using dynamic thresholds to define a significant object in a layer, about 70% of data is encrypted by using the key sets are generated from user's password and Chaotic map. It would be very difficult to break the encryption algorithm or try to predict the encrypted part.

Key sensitivity analysis: We test to encrypt the original layer with a slightly different encryption key, and evaluates the difference between the obtained encrypted layers.

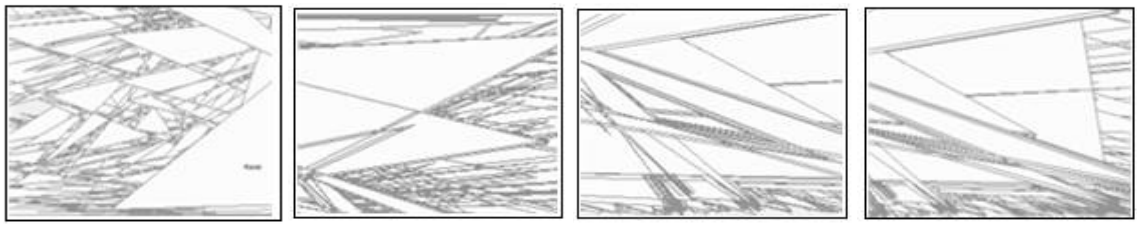
To perform these test, slightly different keys are generated by modifying coefficient μ in Eq. (3) and a pair of first key in each key set a, b. In the modified keys, excluding one are kept same as that of original key. For the original key $K_1(3.52, 0.34, 0.62)$

Table 2. The result of loss accuracy

Total numbers of objects in map	Distance	
	User key K1	User key K2
98	35,682	39,065
249	53,018	50,682
1457	200,133	178,431
1967	233,311	200,644
2900	318,270	404,741

Table 3. The error between original coordinates and decrypted coordinates.

Original coordinates	Decryption coordinates	Error
144.13473	144.134729999	5.00222E-12
-37.32319	-37.3231899999	2.27942E-11
-118.820662	-118.820662001	3.4799541026E-10
……	……..	……
-37.45185	-37.45185000002	1.75006675817713E-11
145.31026	145.3102600009	9.00001850823173E-10



(a) (b) (c) (d)

Fig. 8. Key sensitivity analysis for encryption process: (a)-(d) Encrypted layer with corresponding key K_1, K_2, K_3 and K_4.

(Key K is represented by three parameters (μ, a_1, b_1)), the modified keys are expressed as $K_2(3.42, 0.34, 0.62)$, $K_3(3.52, 0.44, 0.62)$ and $K_4(3.52, 0.34, 0.52)$. The original layer (Fig. 6(c)) is initially encrypted with key sets are generated from K_1. The encrypted layer for this case is shown in Fig. 8(b). The original layer is then encrypted with key sets are generated from slightly modified key K_2, K_3 and K_4. Fig. 8(b)-(d) indicates the corresponding encrypted layers. It is observed that layers encrypted with slightly different keys are completely incomprehensible.

5. CONCLUSION

Our paper focuses on the issues how to encrypt GIS vector map selectivity with low complexity. This considers the properties of object in a layer and selectively encrypts only the significant objects by key sets in DWT, DFT domain. Only some values are selected to encrypt but 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. The proposed 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. Next time, we will continue to improve our algorithm by reducing number of selective values to reduce complexity while not change effectively.

REFERENCE

[1] Geographic Information Systems (GIS), https://en.wikipedia.org/wiki/Geographic_information_system , (accessed Mar., 2015).

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

[3] Vector Data, https://www.qgis.org/en/docs/gentle_gis_introduction/vector_data.html, (accessed Mar., 2015).

[4] Vector Map, http://bgis.sanbi.org/gis-primer/page_19.htm (accessed Mar., 2015).

[5] E. Bertino and M.L. Damiani, "A Controlled Access to Spatial Data on Web," *Proceeding of AGILE Conference on Geographic Information Science,* pp. 369-377, 2004.

[6] S.C. Chena, X. Wangb, N. Rishea, and M.A. Weiss, "A Web-based Spatial Data Access System using Semantic R-trees," *Journal of Information Sciences,* Vol. 167, Issues 1-4, pp. 41-61, 2003.

[7] E. Bertino, B. Thuraisingham, M. Gertz, and M.L. Damiani, "Security and Privacy for Geospatial Data: Concepts and Research Directions," *Proceeding of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS*, pp. 6-19, 2008.

[8] N.B. Rybalov and O.I. Zhukovsky, "Access to the Spatial Data in the Web-Oriented GIS," *Proceeding of Siberian Conference on Control and Communications*, pp. 104-107, 2007.

[9] M. Fuguang, G. Yong, Y. Menglong, X. Fuchun, and L. Ding, "The Fine-grained Security Access Control of Spatial Data," *Proceednig of 18th International Conference on Geoinformatics,* pp. 1-4, 2010.

[10] 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.

[11] 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, No 2, pp. 210-218, Feb. 2011.

[12] Ch. Zhu, Ch. Yang, and Q. Wang, "A Watermarking Algorithm for Vector Spatial Geo-Data based on Integer Wavelet Transform," *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences,* Vol. 37, No. B4, pp. 15-18, 2008.

[13] A. Li, B. Lin, Y. Chen, and G. Lu, "Study on Copyright Authentication of GIS Vector Data Based on Zero-Watermarking," *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences,* Vol. 37, No. B4, pp. 1783-1786, 2008.

[14] S.L. Chen, T. Hwang, and W.W. Lin, "Randomness Enhancement using Digitalized Modified Logistic Map," *IEEE Transactions on Circuits and SystemsII: Express Briefs*, Vol. 57, No. 12, pp. 996-1000, 2010.

[15] S.M. Chang, M.C. Li, and W.W. Lin, "Asymptotic Synchronization of Modified Logistic Hyper-chaotic Systems and its Applications," *Nonlinear Analysis: Real World Applicaions*, Vol. 10, No. 2, pp. 869-880, 2009.

[16] Z. Liu, Q. Guo, L. Xu, M.A. Ahmad, and S. Liu, "Double Image Encryption by using Iterative Random Binary Encoding in Gyrator Domains," *Optics Express*, Vol. 18, No. 11, pp. 12033-12043, 2010.

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 Pukyong National University. His research interests include video processing & application, GIS applications, data security, and smart system.

Sanghun Lim

He received a B.S. degree in Electrical Engineering from Yonsei University in 1996 and a M.S., and Ph.D. degrees in Electrical & Computer Engineering from Colorado State University in 2002 and 2006, He worked research associate at CSU from 2006-2011 and research scientist at NOAA/CIRA in USA from 2011-2012. He is currently research fellow, Korea Institute of Civil Engineering and Building Technology. His research interests include radar meteorology/hydrology, radar system and signal processing.

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 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.

Kwang-Seok Moon

He received the B.S., and M.S., and Ph.D degrees in Electronics Engineering in Kyungpook National University, Korea in 1979, 1981, and 1989 respectively. He is currently a professor in department of Electronic engineering at Pukyong National University. His research interests include digital image processing, video watermarking, and multimedia communication.