International Journal of Multidisciplinary Research and Growth Evaluation
ISSN: 2582-7138
Received: 05-05-2021; Accepted: 25-05-2021
www.allmultidisciplinaryjournal.com
Volume 2; Issue 3; May-June 2021; Page No. 465-468

A simple method for encrypting and decrypting GIS vector data

Giao N Pham
Department of Computing Fundamentals, FPT University, Hanoi, Vietnam
Corresponding Author: **Giao N Pham**

Abstract
Nowadays, 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 producing process of a vector map is considerably complex and the maintenance of a digital map requires substantial monetary and human resources. This paper presents a simple method to encrypt and decrypt GIS vector data. In the proposed method, polylines and polygons in vector map are the target of the encryption and decryption processes. 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.

Keywords: GIS vector map; selective encryption; chaotic map; Hybrid Transform

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 [3-5]. 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. In Section 2, I explain the proposed method in detail. Section 3 contains experimental results. Finally, we conclude this paper in section 4.

The Proposed Algorithm
The schematic diagram of the proposed technique is illustrated in Fig. 1, and the step-by-step procedure is explained hereafter.
An original GIS vector map M is a set of layers: $M = \{L_i | i \in [1, |M|]\}$ with $|M|$is the cardinality of map M (In mathematics, the cardinality of a set is a measure of the "number of elements of the set").
A layer L_i is a set of objects of polylines and polygons $L_i = \{O_{ij} | j \in [1, |L_i|]\}$ with $|L_i|$ is the cardinality of a layer L_i.
An object O_{ij} has properties the total number of points (vertices) and the area of the bounding box. Calculate the area threshold (A_{i_th}) and the point threshold (B_{i_th}) for each layer. Identify the significant objects by comparing the total number of points and the area of the bounding box with thresholds.
For an insignificant object, leave it unencrypted.
For a significant object, using an encryption block to encrypt it by key sets generated from Chaotic map and user's password before changing them in DWT, DFT domain.
Many polyline/polygon objects are created from a few points and the value of the bounding box's area is very small when compared with other objects in layer. This object is very simple and mark it as an insignificant object. With objects include many points and the area of the bounding box is larger than, it also complex than and mark it as a significant object. Thus, we used probability distribution to define thresholds in each layer and identify which object is a significant or an insignificant object by comparing object's features with thresholds.
The area threshold (A_{ith}) and the point threshold (P_{ith}) in a layer L_i are defined as following:
$A_{ith} \in A_i$ and $F(A) = \sum P(A = A_{ij} \,\&\, A_{ij} > A_{ith}) = 0.5$ (1) $P_{ith} \in P_i$ and $F(P) = \sum P(P = P_{ij} \,\&\, P_{ij} > P_{ith}) = 0.5$ (2)
We used the key to create two key sets 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 bits. Other keys are generated by using the Chaotic map [6]. Therefore, we have two key sets: $a = \{a_i \mid i \in [1,8]\}, b = \{b_i \mid i \in [1,8]\}$ and DFT 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. 2.

- We arrange all X, Y coordinates into two 1D-arrays, given the length of segment is 8, the total number of segments in each array is: $n = \lfloor N/8 \rfloor$, 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: $Z_i = X_i * a_i + jY_i * b_i, i \in [1,8]$.
- Apply DWT-3 level for each segment and select all first coefficients of first transformed values and continue to apply DFT to get a set of second transformed values.
- After DFT processing, we continue to encrypt the first DFT coefficient with DFT encryption value by equation (4) and IDFT.

$$DFT^* = DFT * \left(\sum_{i=1}^{8} a_i + \sum_{i=1}^{8} b_i \right) \quad (3)$$

- Replace all first coefficients in DWT-segments by encrypted values and IDWT-3 level 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.

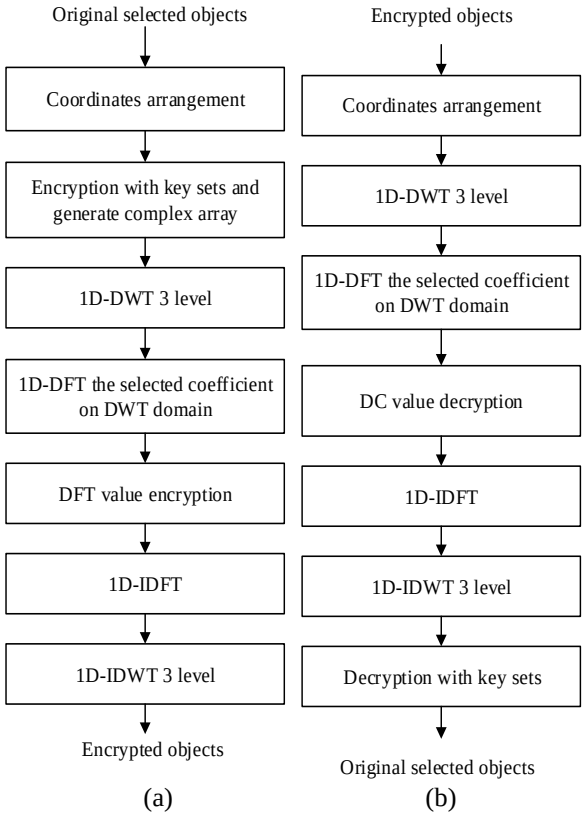
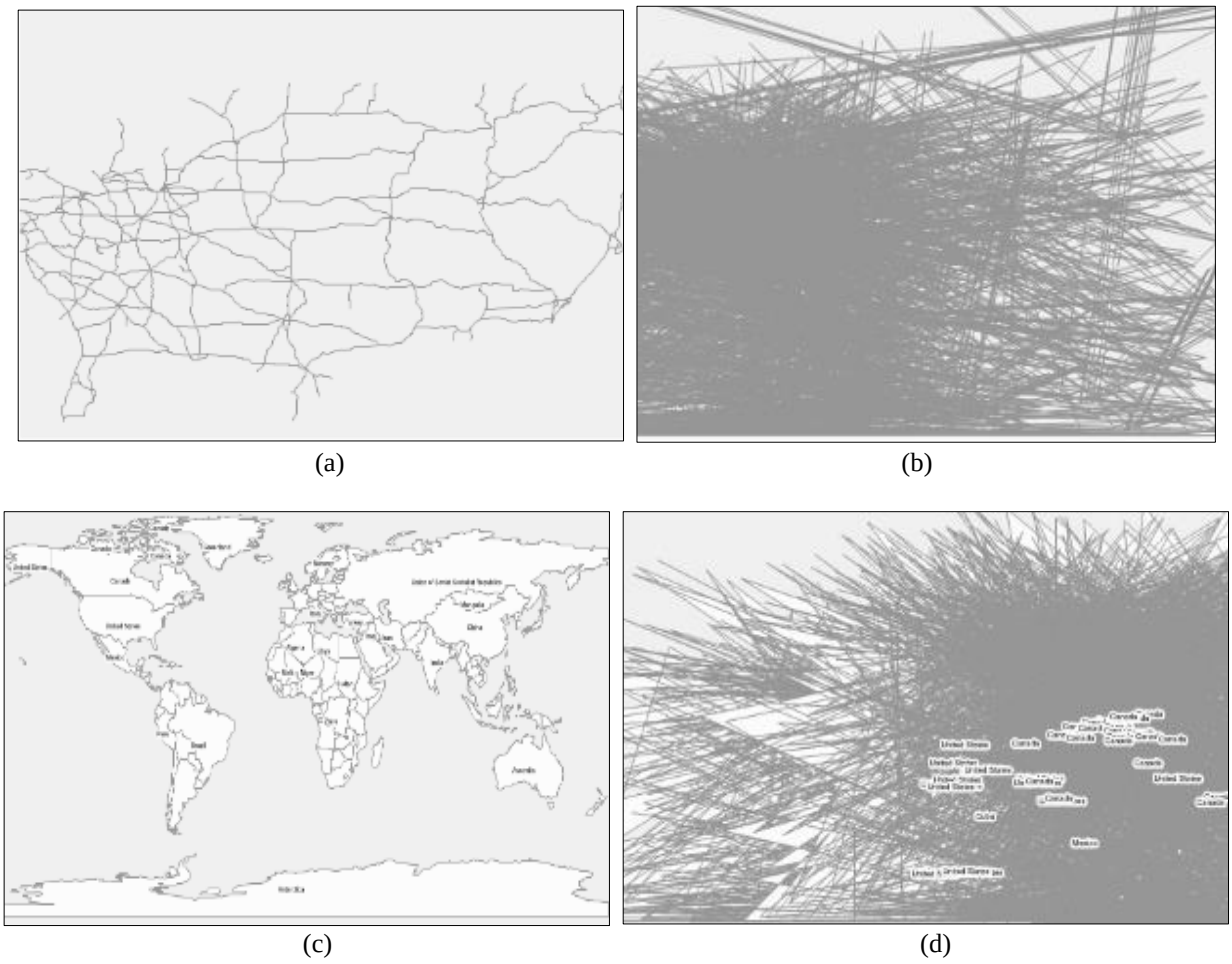


Fig 1: The Proposed Method; (a) encryption and (b) decryption.

Experimental results

Experimental results in Fig. 3 and Fig. 4 showed that the proposed method changes whole maps. The proposed method has much lower computational complexity than AES or DES because we only select some coefficients in DWT domain and one DFT value in DFT domain, encrypt it by random value. But we confirmed it effectively by experimental results which are showed from Fig. 3 and Fig. 4. Moreover, our selective encryption process changes only values of vertices in polylines and polygons of map.

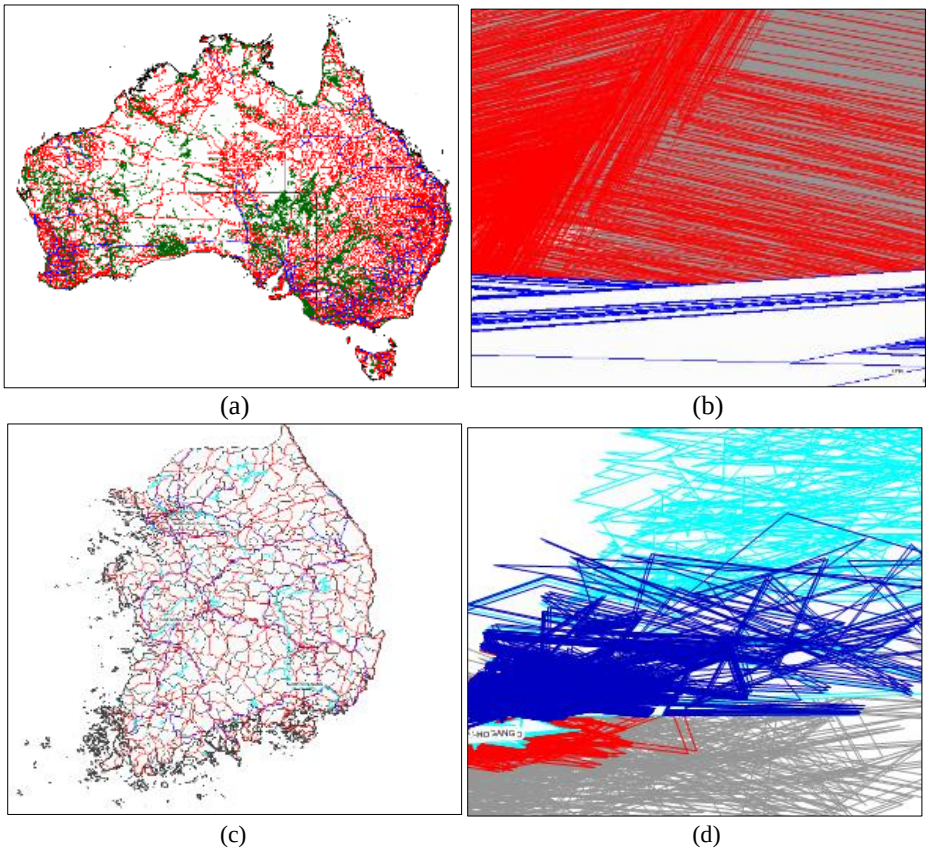
Our algorithm used discrete probability distribution to define thresholds in each layer and identify which object is a significant or an insignificant object by comparing object's features with thresholds. After that, we only select the significant objects for encryption. When we change two values (that are user-defined) in Eq. (1)-(2), threshold values are also changed and percentage of the encrypted vertices change according to this values, as shown in Fig. 4.



(a) (b)

(c) (d)

Fig 2: (a) and (c) original polyline/polygon layer; (b) and (d) encrypted polyline/polygon layer.



(a) (b)

(c) (d)

Fig 3: (a) and (c) original map; (b) and (d) encrypted map.

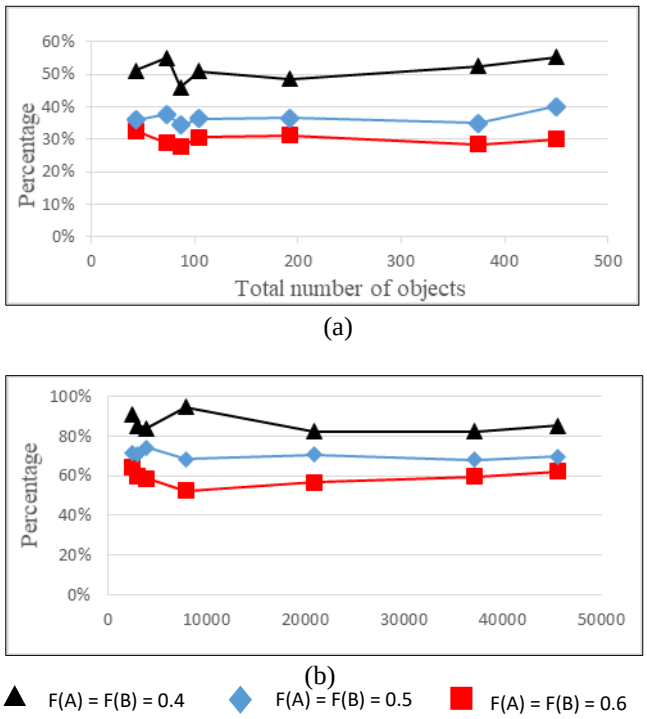


Fig 5: (a) Percentage of the significant objects, (b) Percentage of the encrypted points.

The distance between original map and encrypted map is computed by equation (4):

$$D(E^{'}, L) = \sum_{i=1}^{N} d(P_{ij}) \quad (4)$$

With L is a original map, $E^{'}(L)$ is corresponding encrypted map, N is total object in original map. And $d(P_{ij})$ is distance between corresponding objects in $E^{'}(L)$ and L, is computed by equation (5):

$$d(P_{ij}) = \sum_{j=1}^{N_{ij}} \sqrt{(|x_j^{'} - x_j|^2 + |y_j^{'} - y_j|^2)} \quad (5)$$

N_{ij} : The total number of points in object P_{ij}

We used polyline map, polygon map to experiment with different passwords K_1 # K_2. Then we calculate $D(E^{'}, L)$ distance of each experimental time, as shown in Table 1. Our selective encryption scheme only changes values of vertices in polylines and polygons of map. It did not alter the size of encrypted file. 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 is $z_n^{'}$ not absolutely equal to because sine and cosine value are not integer, as given by Table 2.

Table 1: Experimental distance measure.

Total number of points	Distance	
	User key K_1	*User key* K_2
798	35,682	39,065
2457	200,133	178,431
3900	318,270	404,741
5785	685,254	752,156

Table 2: The error between original coordinates and decrypted coordinates.

Size (kb)	Total Object	Total Point	Max error	Min error	Average error
332	76	20920	4.58763E-07	0	1.75211E-08
449	147	28162	3.70411E-07	0	1.72524E-08
751	20	47947	2.88627E-07	0	4.00043E-08
965	7011	37209	1.13562E-07	0	2.92078E-10

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. In comparison with conventional works, proposed methods response the security in various formats of vector map data, reduce complex computation and encrypted data volume, response real-time applications.

Acknowledgments

This work is supported by FPT University, Hanoi, Vietnam

Disclosure of conflict of interest

On behalf of all authors, corresponding author declares that there is no conflict of interest to publish this research.

References

1. Foote KE, Lynch M. Geographic Information Systems as an Integrating Technology: Context, Concepts, and Definitions", Last revised, 2009.
2. Goodchild MF. Twenty years of progress: GIS science in Journal of Spatial Information Science. 2010; 1:3-20.
3. Bertino E, Thuraisingham B, Gertz M, Damiani ML. Security and privacy for geospatial data: concepts and research directions, Proc. of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS, 2008, pp. 6-19.
4. Rybalov NB, Zhukovsky OI. Access to the Spatial Data in the Web-Oriented GIS," Proc. Siberian Conference on Control and Communications, 2007, 104-107.
5. Fuguang M, Yong G, Menglong Y, Fuchun X, Ding L. The fine-grained security access control of spatial data," Proc. 18th International Conference on Geoinformatics, 2010, pp. 1-4.
6. Wu F, Cui W, Chen H. A Compound Chaos-Based Encryption Algorithm for Vector Geographic Data under Network Circumstance," Proc. of Cardholder Information Security Program. 2008; 1:254-258.