FACTA UNIVERSITATIS (NIŠ)
Ser. Math. Inform. Vol. 35, No 4 (2020), 1205–1217
https://doi.org/10.22190/FUMI2004205S

ENCRYPTION OF 3D PLANE IN GIS USING VORONOI-DELAUNAY TRIANGULATIONS AND CATALAN NUMBERS

Faruk Selimović, Predrag Stanimirović,
Muzafer Saračević, and Selver Pepić

Abstract. A method for encryption of the 3D plane in Geographic Information Systems (GIS) is presented. The method is developed using Voronoi-Delaunay triangulation and properties of Catalan numbers. The Voronoi-Delaunay incremental algorithm is presented as one of the most commonly used triangulation techniques for the random point selection. On the basis of the multiple application of Catalan numbers in solving combinatorial problems and their "bit-balanced" characteristic, the process of encrypting and decrypting the coordinates of points using the Lattice Path method (walk on the integer lattice) or LIFO model is given. The triangulation of the plane started using decimal coordinates of a set of given planar points. Afterward, the resulting decimal values of the coordinates are converted to corresponding binary records and the encryption process starts by random selection of the Catalan key according to the LIFO model. These binary coordinates are again converted into their original decimal values, which enables the process of encrypted triangulation. The original triangulation of the plane can be generated by restarting the triangulation algorithm. Due to its exceptional efficiency, *Java* programming language enables efficient implementation of the proposed method.
Keywords: Encryption of 3D plane; Voronoi-Delaunay triangulation; Catalan numbers; Lattice Path method; Java Net- Beans environment.

1. Introduction

Owing to the achieved progress of the GPS navigation systems and robotics, the encryption of a 3D plane takes an important role in the field of data protection in the development of GIS (*Geographic Information Systems*). The increasing role of the GIS in processing and analysis of spatial data as well as in control systems of defense and public security, the *Delaunay triangulation* represents the basic model

Received October 24, 2020; accepted November 14, 2020
2020 *Mathematics Subject Classification.* Primary 68U05; Secondary, 32B25

for creating of TIN (*Triangulated Irregular Network*) in the process of obtaining a digital model of terrain (DMT) [1]. In fact, a DMT is an organized set of data on terrain heights recorded in a digital form.

The subject of research in the paper is to investigate possibilities, properties, and applications of the Catalan numbers in generating keys for encryption of the 3D plane triangulation with the Voronoi-Delaunay triangulation. Our intention is to consider and explain the application of the existing knowledge of Catalan numbers in the process of encryption and decryption of the TIN network of the 3D plane.

Catalan numbers (C_n) are most commonly used entities in geometry. They also appear in solutions to a large number of combinatorial problems. Catalan numbers are calculated according to the following formula [2]:

$$C_n = \frac{(2n)!}{(n+1)!n!} = \frac{1}{n+1}\binom{2n}{n}, \ n \geq 0. \tag{1.1}$$

Many combinatorial problems are based on the Catalan sequence, such as: the *ballot* problem, the problem of roads in the network (Lattice Path), the problem of paired parenthesis [7, 8, 9]. An original contribution of our research is the usage of the sequence of the Catalan numbers as a key generator for encryption and decryption of coordinates of the 3D points in a GIS. We note that the integer n is a basis of the generated keys, and C_n is the number of all key combinations on that basis.

For example, the basis $n = 28$ implies the space of $C_{28} = 263747951750360$ keys satisfying the *bit-balance* property. It is known that the key space is growing by increasing the base. In order to verify the validity of the Catalan numbers property, we will exploit their binary records. The fundamental property that one number must satisfy to be labeled as a Catalan number is the *bit-balance bits* property in the binary file corresponding to a specified number C_n. In other words, the binary record of any Catalan number involves identical number of bits "0" and "1" and starts with the bit "1".

If a binary record of a Catalan number is associated with the balanced parenthesis notation, then the bit "1" becomes an open parenthesis, while the bit "0" represents a closed parenthesis. Moreover, each left parenthesis is closed, which implies that each bit "1" assumes its own pair which is just the bit "0". The binary record of an arbitrary Catalan number can also be represented in the form of stack permutations. In this case, the bit "1" represents the *PUSH* command while the "0" is the *POP* command.

For example, the set of $C_n = 14$ values satisfy the Catalan numbers property for $n = 4$: 170, 172, 178, 180, 184, 202, 204, 210, 212, 216, 226, 228, 232, 240. Based on their binary records 10101010, 10101100, 10110010, 10110100, 10111000, 11001010, 11001100, 11010010, 11010100, 11011000, 11100010, 11100100, 11101000, 11110000 we determine the *bit-balance* property corresponding to the Catalan number.

Observing the binary notations of the given numbers, we can notice that each number has the same number of bits "1" and "0"; in other words, there is a balance between them, which is the main property of Catalan numbers. In addition, the number of pairs 1 and 0 is basically n, while the length of the key is always $2n$. In this example, the base is 4, which means that the key length is 8 bits.

As it was already mentioned, the Catalan number can be modeled by many combinatorial problems [2], such as paired parenthesis "(() () (()))" or a ballot record "AABBABAB", graphically in the form of walking through an integer network (*Lattice Path*) or through the stack permutation. Below we present Stack Permutation as a method for encoding the coordinates of $3D$ points.

The remainder sections of the paper are presented in the following order. The encryption of 3D plane coordinates by means of Catalan numbers is described in Section 2. Section 3 is intended to a description of the Voronoi diagram and Delaunay triangulation of the 3D plane. Also, we describe the main reasons for using this kind of triangulation in the proposed method. Section 4 presents Spatial Data Structure in GIS. Section 5 describes the implementation of the 3D plane encryption algorithm in the Java-Net Beans environment. It is also aimed to the analysis of the Java source code and experimental results.

2. Encryption of 3D plane coordinates with Catalan numbers

The stack is an abstract type of data structure that is based on the principle *LIFO* (*last in, first out*) and on two basic operations *push* and *pop*. The stack permutation, as a method for solving combinatorial issues, can be generated using Catalan numbers.

In [3], it was shown that a number of permutations satisfying the given conditions correspond to Catalan numbers. On the basis of this, it is possible to map each binary record (or equivalent Ballot record) of length $2n$ to the corresponding permutation of the length n by applying a stack.

Consider an example of encrypting one of the 3D coordinates (x, y, z) using Stack Permutations. The x coordinate is $x = 1430$, its binary record is $1430_{10} = 10110010110_2$ with $n = 11$ bits. The value of the Catalan number (below the key) is $K = 2816098$. His binary record is $2816098_{10} = 1010101111100001100010_2$, consisting of $2n = 22$ bits. Figure 2.1 describes the details.

The decryption process is analogous to the corresponding encryption. The key and the code in the decryption are read in the reverse order. The *Balanced Parentheses* method is equivalent to a stack permutation [4]. Figure 2.2 represents the encoding process.

3. Voronoi diagram and Delaunay triangulation of 3D plane

The goal of Delaunay triangulation is the decomposition of a certain surface into non-crossing triangular elements. The angular points of the triangles are main points of the surface, and each anchor represents the corner of the least one triangle. Triangulation is a procedure that is used to process points that have a random

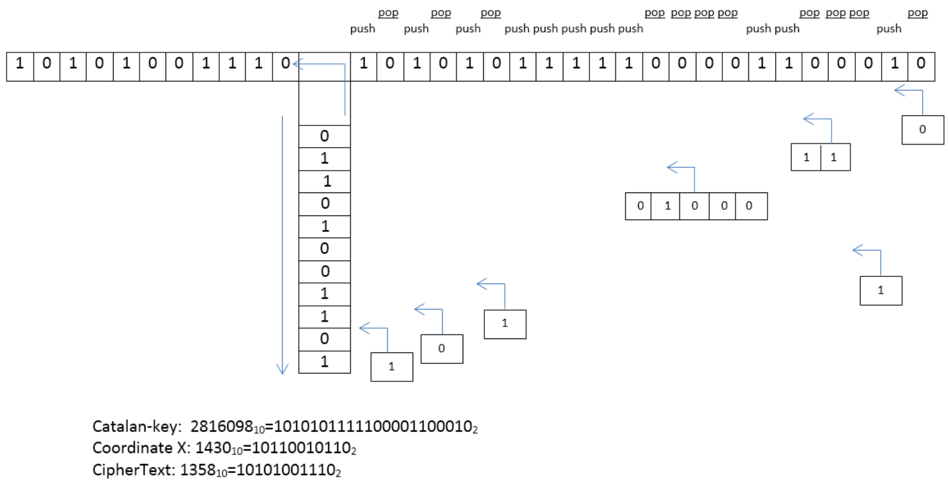

Fig. 2.1: Coordinates encryption example based on Stack Permutation principle

Key	1	0	1	0	1	0	1	1	1	1	1	0	0	0	0	1	1	0	0	0	1	0
Balanced Parentheses	(	)	(	)	(	)	(	(	(	(	(	)	)	)	)	(	(	)	)	)	(	)
Coordinate X	1		0		1		1	0	0	1	0					1	1				0	
Cipher Text		1		0		1						0	1	0	0			1	1	1		0

Fig. 2.2: Coordinates encryption example based on Balanced Parentheses

distribution [10]. *Voronoi polygon* is the geometric place of the closest points of one particular point in the finite set of points. Union of all Voronoi polygons in the set of points in the plane defines the *Voronoi diagram*.

Essentially, the Voronoi diagram as a geometric structure is used for determining the distance between points and the closest points. The Voronoi polygon points separate any point from their nearest neighboring points. The sides of a Voronoi polygon consist the bisectors of the segment line obtained by connecting a point with adjacent points, where each point is combined with adjacent points in order to obtain the Delaunay triangulation. Each cell of the Voronoi diagram presented in Figure 3.1 possesses its own center.

Some of useful properties of an arbitrary Delaunay triangulation are listed bellow:

- Uniqueness and independence from the starting point.
- Formed triangles are in the form of equilateral triangles.

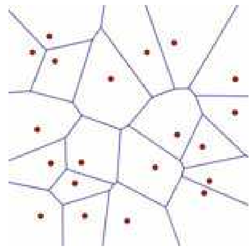

Fig. 3.1: Voronoi diagram - partitions of the plane in the cells

- There is no other point in the circumcircles of the triangles (property of the circumcircle).
- The convex hull is triangulated.
- A line segment that is obtained from the closest pairs of points is in the triangulation.
- A line segment obtained from the point and its nearest point is the side of the triangle in the triangulation

4. Spatial Data Structure in GIS

Spatial data are most important in each GIS. They are geo-referenced by their location on the surface of the earth. Geo-referencing implies a precisely recorded location in a particular coordinate system. Since the GPS system is the backbone of locating and monitoring targets on the surface of the earth, the security or protection of GPS signals sent to earth stations is of great importance in the process of creating business navigation applications. In that sense, 3D level encryption using Catalan numbers and Delaunay triangulation is just one of the geographic data protection models.

4.1. Remote Detection - Global positioning GPS system

The method for collecting and interpreting information about remote objects without physical contact with any of them is termed as *remote sensing*. Common platforms for observations in remote sensing are planes, space probes, and satellites. This method will most often focus on two narrow areas: teledetections and photogrammetry. *Teledetective* is a remote sensing in which information about the earth's surface is collected with the help of the devices located in satellites. *Photogrammetry* means a technique of measurement by which the shape, size, and position of the recorded object are performed on the basis of photographic images.

Basically, GPS satellites send signals to their receivers about their latitude, length, and height, i.e., they send signals for three coordinates (x, y, z). The procedure for obtaining these coordinates is based on the principle of intersection (*trilateration*) of the spheres emitting three satellites. GPS application is multiple [5]. First, it was developed for military purposes, and later in the 1980s, it began to be used for civilian purposes. Navigation of planes, boats, cars without GPS is inconceivable. In the process of signal protection, it is required to have a mechanism (algorithm) for the encryption of coordinates of the points (receiver positions) in the satellite.

So, the a cryptographic signal and an encryption key are sent by a receiver. On the other hand, the receiver should have a decryption mechanism (algorithm) that is capable of returning the received signal (encrypted with the key) to its original value. This algorithm will be explained with more details in the next section.

4.2. Modeling of 3D plane - TIN model

The standard way to represent the terrain surface in digital form is done via *Digital Modeling of Terrain* (DMT). The representation of the surface of the plane is enabled by a mathematical model based on the correct height network (*GRID*) or on the *Triangulated Irregular Network* (TIN). The TIN is formed on the basis of known positions of points and their heights, i.e, coordinates (x, y, z) of given points. The incremental algorithm of Delaunay triangulation is used in the process of network formation.

Based on the TIN model, all the desired calculations can be performed: the value of the inclination at a given point, the height for the given position in the horizontal sense, the direction of the maximum inclination, the curvature of the surfaces at the given point, the visualization of the terrain model, geostatistic analysis and others. Today, TIN models are used in designing traffic, hydraulic engineering, underground facilities, military geographic analysis, etc [6].

Given the wide use of the TIN model, it is necessary to allow encryption of coordinates of points in the moment of electronic transmission as well during storing the model on a certain medium. In general, the algorithm presented in the next section gives the TIN model in conjunction with other (encrypted) coordinate values.

5. Implementation of the 3D plane encryption algorithm in the Java-Net Beans environment

The process of encrypting the coordinate begins by generating a sequence of the total number of randomly selected triangles of the TIN model. After that, the incremental Delaunay triangulation algorithm is applied. In the second step, each decimal value of the vertices coordinate (x, y, z) of the formed triangulation is remembered in the integer string. Then their conversion from decimal to binary form is done because the Catalan key is assigned in binary form. By using the *Stack Permutation* method, the obtained binary coordinate format is converted to another text encoded by the principle *LIFO*, which, after re-conversion to decimal form, is actually *ENCRYPT*, i.e., the result of Algorithm 1.

Algorithm 1 LegalizeEdge $(p_r, \overline{p_i p_j}, \mathcal{T})$

Require: P is set of n points in a plane.
Let p_{-1}, p_{-2} i p_{-3} three points in triangle which consists all other points from set P .
Initial triangulation $\mathcal{T}$ consist the triangle p_{-1}, p_{-2} i p_{-3}
for $r = 1$ to n **do** (Put in p_r u $\mathcal{T}$)
Find the triangle $p_i p_j p_k \in \mathcal{T}$, which consist p_r.
put the p_r integer array K.
return $\mathcal{T}$
for $r = 1$ to n **do** (Access p_r in the array K)
Convert p_r in binary record
Put in the **Stack permutation (LIFO)** method on basis of **Catalan key** from C_n
Convert p_s in decimal record (after permutaton bit p_r it become p_s)
Put the p_s in array K_s
for $s = 1$ to n **do** (Put p_s in $\mathcal{T}_s$)
Find the triangle $p_i p_j p_k \in \mathcal{T}_s$, which consists p_s.
return $\mathcal{T}_s$.
Output : Encrypted n points from set P (encrypted TIN model in plane)

The encoding of the plane points is clearly explained in Algorithm 1. However, this encoding of points implies encryption of their coordinates (x, y, z). In addition to the Delaunay triangulation method, the following methods are used for the implementation of the above steps in the algorithm:

Convert_in_Binary_Record, *Binary_Encoding_Coordinate*,

Convert_Binary_in_Integer and class *DelaunayAp.ja-va*.

Since the application is done in the *NetBeans* environment, it is possible to present the plane only in 2D form. However, the way of the encryption of the third coordinate z is the same as for x, y. Below we present this algorithm in more details.

5.1. Structure of Java source code

Java GUI application starts by the execution of the executable method `main()` class *DelaunayAp.java*. It is necessary to enter the n (number of points in the plane) from the set P. After that, the random coordinates (x, y) are assigned by clicking on the level panel in the large initial triangle $p_i p_j p_k$. The position of the point p_r in the level is determined in this way. The incremental Delaunay triangulation algorithm lies in the background of the constructed method such that all points in the plane are in separated positions. After that, the TIN network of the triangles to be encrypted is created. The decimal values of the coordinates (x, y) are presented in Figure 5.1.

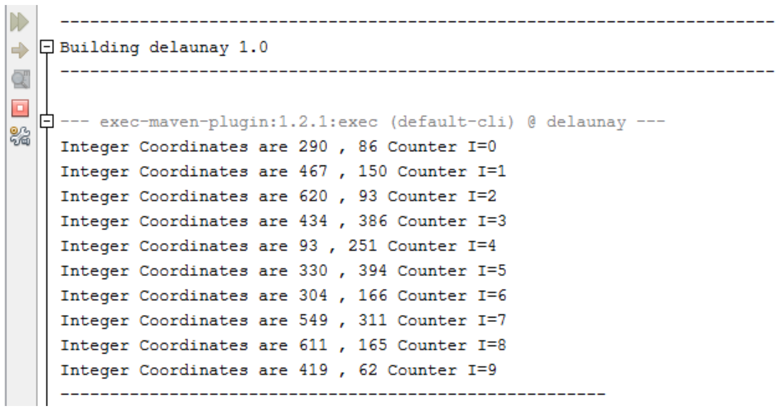

FIG. 5.1: (x, y)coordinate values of triangles

A TIN model of the level with introduced points (triangles) of the triangles given in decimal form is presented in Figure 5.2. Previously described events correspond to Algorithm 1 up to step 6, where we get a series of K with the coordinate inputs of x, y points."Encrypt the TIN model" are called the methods $Encoding\_X\_Y\_Coordinates()$. Within this method, the first one is the $Convert\_U\_Binary\_Entry()$, where each dot coordinate in the K sequence is accessed and its conversion from decimal to binary form is executed (step 8 in the algorithm). The method $Binary\_Encoding\_Coordinate()$ is started after the conversion.

Application of this method is explained in more detail in Section 2. The result of the application of this method is the implementation of steps from 9 to 14 in Algorithm 1. It should be noted that the resolution of the monitor in such an environment is a limiting factor. The number of coordinate bits is the exponent of 2 and must always be within the range relative to the resolution of the monitor. For example, in the case of resolution of 1440 x 900 pixels, the number 1440 exceeds the value of 1024 (2^{10}=1024) and due to this in the representation of coordinate values larger than 1024, the exponent must be 11. Also, the Catalan key length always is $2n$, where n is the number of the bits from the coordinates. In our case, the length is of 22 bits. When it comes to 3D modeling and coordinate values which GPS satellites send to Earth stations, this condition is not true. In this case, after the conversion of the decimal value of the coordinates into the binary value, the Catalan key is chosen according to the model $2n$. The result of this method is given in Figure 5.3. Figure 5.4 shows the encrypted TIN level model.

The encoding process is similar to the decoding process, only the encoded and original coordinates change the place. The Catalan key keeps the same value, and

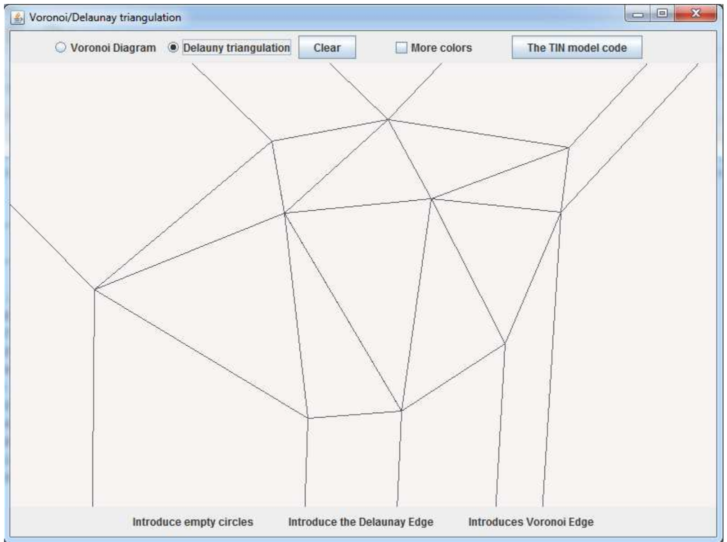

FIG. 5.2: TIN network of irregular triangles

```
--------------------------------------------------------------------------------
Integer Cooordinate: X = 611, Y =165
Catalan Key for N=11: 1010101111100001100010
Binary Coordinate: X = 01001100011 ,Y = 00010100101
Encrypted Binary Coordinates: X = 01000111001 Y = 00000100111
Encrypted Binary Coordinates: X = 569 Y = 39
--------------------------------------------------------------------------------
Integer Cooordinate: X = 419, Y =62
Catalan Key for N=11: 1010101111100001100010
Binary Coordinate: X = 00110100011 ,Y = 00000111110
Encrypted Binary Coordinates: X = 00100101011 Y = 00011101100
Encrypted Binary Coordinates: X = 299 Y = 236
--------------------------------------------------------------------------------
End of Encryption Coordinates---------------------------------------------------
 Encrypted Coordinates X = 296 Y= 92
 Encrypted Coordinates X = 347 Y= 78
 Encrypted Coordinates X = 692 Y= 213
 Encrypted Coordinates X = 362 Y= 266
 Encrypted Coordinates X = 213 Y= 251
 Encrypted Coordinates X = 408 Y= 394
 Encrypted Coordinates X = 352 Y= 46
 Encrypted Coordinates X = 549 Y= 365
 Encrypted Coordinates X = 569 Y= 39
 Encrypted Coordinates X = 299 Y= 236
Execution time: 20 millisecond
```

FIG. 5.3: Values of binary coordinates and their encryptions

reading of the key length and the cipher is done from right to left, ie, in reverse order of encryption. Figure 5.5 shows the descriptive coordinates corresponding to

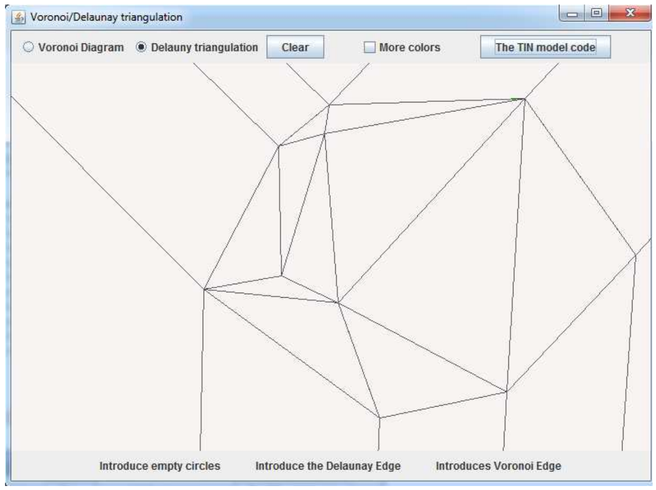

Fig. 5.4: Encrypted TIN model

the original values of the coordinates in Figure 5.3.

```
Decryption Binary Coordinates: X = 01000100101 Y = 00100110111
Described - Original Integer Coordinates: X = 549 Y = 311
--------------------------------------------------------------------------------
Encrypted Coordinates: X = 569, Y =39
Catalan Key for N=11: 1010101111100001100010
Encrypted Binary Coordinates: X = 01000111001 ,Y = 00000100111
Decryption Binary Coordinates: X = 01001100011 Y = 00010100101
Described - Original Integer Coordinates: X = 611 Y = 165
--------------------------------------------------------------------------------
Encrypted Coordinates: X = 299, Y =236
Catalan Key for N=11: 1010101111100001100010
Encrypted Binary Coordinates: X = 00100101011 ,Y = 00011101100
Decryption Binary Coordinates: X = 00110100011 Y = 00000111110
Described - Original Integer Coordinates: X = 419 Y = 62
--------------------------------------------------------------------------------
End of Deciphering Coordinate------------------------------------------------------
Described Coordinates X= 290 Y= 86
Described Coordinates X= 467 Y= 150
Described Coordinates X= 620 Y= 93
Described Coordinates X= 434 Y= 386
Described Coordinates X= 93 Y= 251
Described Coordinates X= 330 Y= 394
Described Coordinates X= 304 Y= 166
Described Coordinates X= 549 Y= 311
Described Coordinates X= 611 Y= 165
Described Coordinates X= 419 Y= 62
```

Fig. 5.5: Values of decrypted coordinates

FIG. 5.6: Encryption time of coordinate (x, y, z)

5.2. Experimental results - Encryption time

The encryption time was tested on the vertices $N = \{5,10,20,40,100,200,400\}$. Since *JavaNetBeans* compiles and interprets simultaneously, the capabilities of our algorithm were examined in this environment.

N Vertex	*Time execution of Algoritms in "ms"*
5	1
10	2
20	4
40	549
100	628
200	2137
400	1332

Table1: Encription time

If we also present this data graphically, it can be noticed that the encryption time is not in direct proportion to the number of vertices of the triangles. This fact is a good indicator, because the encryption time does not grow on the basis of increasing the number of vertices. Corresponding results are presented in Figure 5.6.

Considering this low time for encryption, encrypted coordinates can be stored in a database, which will further increase the efficiency of this algorithm. The numerical testing was done on a computer with the next performances: *Intel Core i5-CPU 2.6 GHz, RAM -4 GigaBytes, Operating system: Windows 7 Microsoft -64 bits.*

6. Conclusion and further works

The proposed method is a combination of the computational geometry, geographic information systems and cryptography. A new method for encoding coordinates is based on the Catalan-key. If an integer n is a basis for generated keys, then C_n is total space of different keys, i.e, the number of different binary records. For a 64-bit key, there exist a huge number of total valid values which fulfil the bit-balance property (for base $n = 32$, the space of 64-bit Catalan keys is $C_{32} = 55534064877048198$). In order to provide all Catalan numbers and store them on a disk, it is required a memory space of 44 427 251 901 MB or about 42 369 TB. So, this procedure is very demanding with respect to memory requirements. Further, if it is necessary to find all 64-bit Catalan numbers, and if $1ms$ is necessary to access each element in the set of all C_n, then the CPU time would spend about 176097 years. Average time will be $176097/2 = 88048$ years. Our strategy is usage of some larger bases to generate Catalan-key spaces to prove that the Catalan-key space drastically increases even after a small increase in the base.

In fact, the construction of a large space of Catalan keys assures the security of the presented cryptosystem. The proposed methods of encryption may have wide applications. GIS is the most promising information technology today, due to wide spectrum of possibilities and the scope of its applications. It is almost impossible to efficiently conduct a geographic analysis of the terrain without GIS. Especially, its application in the military analysis of the field is expressed, i.e. in the creation of digital modeling of terrain (DMT). The TIN model is one of the most common methods for presenting DMT, i.e., a network of irregular triangles with vertices in the points with known heights on the terrain [6]. In addition to the application of GIS or DMT for military purposes and in monitoring and navigation devices, it is applied in other areas, such as construction, hydro-engineering, generating maps for flood risks, etc. Lately, there is an increasingly important role in hydraulic modeling. Given this wide application of DMT, the TIN modeling is of great importance. Cryptography is a very dynamic domain and in this paper, only some of its basic mathematical concepts are covered.

REFERENCES

1. Heywood I., Cornelius S., Carver S., *An Introduction to Geographical Information Systems*, Pearson Education: Prentice-Hall, 2012.
2. Koshy T., *Catalan Numbers with Applications*, Oxford University Press, New York 2009.
3. Saračević, M., Stanimirović, P., Krtolica, P., Mašović, S., Construction and Notation of Convex Polygon Triangulation based on ballot problem, *ROMJIST - Journal of Information Science and Technology*, 17(3), pp. 237-251, 2014.
4. Geary, F.R., Rahman, N., Raman, R., A Simple Optimal Representation for Balanced Parentheses, *Theoretical Computer Science*, 368 (3), pp. 231-246, 2006.
5. Berg M., Cheong O., Kreveld M., Overmars M., *Computational Geometry: Algorithms and Applications (3rd Edition)*, Springer 2008.

6. Sisti A. F., Farr S. D., Modeling and simulation enabling technologies for military applications, *Proceedings Winter Simulation Conference*, California, USA, pp. 877-883, 1996.
7. Saračević M., Aybeyan S., Selimovic F., Generation of cryptographic keys with algorithm of polygon triangulation and Catalan numbers, *Computer Science - AGH*, 19(3), pp. 243–256, 2018.
8. Saračević M., Koricanin E., Bisevac E., Encryption based on Ballot, Stack permutations and Balanced Parentheses using Catalan-keys, *Journal of Information Technology and Applications*, 7(2), pp. 69–77, 2017.
9. Saračević M., Adamovic S., Bisevac E., Application of Catalan Numbers and the Lattice Path Combinatorial Problem in Cryptography, *Acta Polytechnica Hungarica - Journal of applied sciences*, 15(7), pp. 91–110, 2018.
10. Lee D.T., Preparata F.P., Computational Geometry - A Survey, *IEEE Transactions On Computers*, Vol c-33 (12), 1984.

Faruk B. Selimšović
Faculty of Sciences and Mathematics
Department of Computer Sciences
Višegradska 33
18000 Niš, Serbia
faruk.selimovic@pmf.edu.rs

Predrag S. Stanimirović
Faculty of Sciences and Mathematics
Department of Computer Sciences
Višegradska 33
18000 Niš, Serbia
pecko@pmf.ni.ac.rs

Muzafer H. Saračević
Faculty of Sciences and Mathematics
Department of Computer Sciences
Višegradska 33
18000 Niš, Serbia
muzafers@gmail.com

Selver Pepić
Higher Technical Machine School of professional studies
Inforamtion tehnology
Radoja Krstića 19
37240 Trstenik
selverp@gmail.com