Analysis of the Fractal Structures for the Information Encrypting Process

Ivo Motýl, Roman Jašek, Pavel Vařacha

***Abstract*—** This article is focused on the analysis of the fractal structures for purpose of encrypting information. For this purpose were used principles of fractal orbits on the fractal structures. The algorithm here uses a wide range of the fractal sets and the speed of its generation. The system is based on polynomial fractal sets, specifically on the Mandelbrot set. In the research were used also Bird of Prey fractal, Julia sets, 4Th Degree Multibrot, Burning Ship and Water plane fractals.

***Keywords*—**Fractal, fractal geometry, information system, security, information security, authentication, protection, fractal set

I. Introduction

Information systems are undoubtedly indispensable entity in modern society. [7]

There are many definitions and methods for their separation and classification. These systems are located in almost all areas of human activity, such as education, health, industry, defense and many others. Close links with the life of our information systems brings greater efficiency of human endeavor, which allows cooperation of man and machine. [3] This connection may also represent a certain danger in the event of a failure as a man or a "machine", which can lead to information loss, disruption or misuse of the operating state of the system against the will for which it was deployed.

This article describes the new ways of using fractal geometry for secure storage of information, which is a different view of the traditional methods of encryption mechanisms. The process of transformation into a secure form of news lies in the basic idea of the concept of fractal geometry - the endless fractal structures [5] inside the set. Fractal geometry is a representative group of complex geometric objects, which present the scientific community, knows. Fractal geometry provides great promise for the future to find solutions too many issues that would have been difficult to apply the methods used. [2]

The aim of this study was describe to using fractal geometry structures for securing information inside of the information system.

II. Problem Solution

Using of fractal geometry for the encryption is an alternative to commonly solutions based on classical mathematical principles. For proper function of the process is necessary to ensure the following points:

- Generate fractal structure with appropriate parameters for a given application
- Analyze the fractal structure and determine the ability to handle a specific amount of information
- use of fractal orbits to alphabet mapping

A. Principle of the Fractal Analysis in the Encryption Process

Fig. 1 shows the principle the fractal structure analysis for determining of the maximum message length.

After generating the fractal visualization is displayed on the main program window. Fractal structure is stored in two-dimensional array, called the fractal structure [2], where each rendered pixel is represented by its coordinates and the number of iterations. In the next step, this field is analysed and calculated the frequency of iterations of all the various elements it contains. This creates a data field called field of frequency where these frequencies recorded. In the first field of the index indicates the number of points that meet the structural conditions of the first fractal iteration, the second index are included frequency points that these conditions are fulfilled in the second iteration, etc. The maximum number of indexes of this field is related to the parameter set number of iterations.

The input alphabet contains alphabetic characters AZ, digits 0-9 and the other characters, what are the decimal points, minus sign or a space character or a special delimiter character keys. This information is stored in one-dimensional array, called the input alphabet characters, where each index contains one character from the input alphabet. After surgery, the descending sort field and frequency shift of the total number of indices that has a field input alphabet characters can specify the maximum length of information that can be encrypted.

Ivo Motýl is with the Department of Informatics and Artificial Intelligence, Faculty of Applied Informatics, Tomas Bata University in Zlín, nám. T. G. Masaryka 5555, 76001 Zlín, CZECH REPUBLIC; e-mail: motyl@fai.utb.cz

Roman Jašek is with the Department of Informatics and Artificial Intelligence, Faculty of Applied Informatics, Tomas Bata University in Zlín, nám. T. G. Masaryka 5555, 76001 Zlín, CZECH REPUBLIC; e-mail: jasek@fai.utb.cz.

Pavel Vařacha is with the Department of Informatics and Artificial Intelligence, Faculty of Applied Informatics, Tomas Bata University in Zlín, nám. T. G. Masaryka 5555, 76001 Zlín, CZECH REPUBLIC; e-mail: varacha@fai.utb.cz.

Fig. 1 Maximal length message on the basis of fractal structure

Fig. 2 shows the automatic generating process. The process begins by reading the input parameters. These parameters contain values: The number of passages, Threshold orbit, initial size and number of iterations. Before starting the process of generating the coordinates of the coordinate system is in its infancy. The initial parameter range is determined by the area Cartesian coordinates, which will be started generating fractal. After this operation is generated the first iteration of fractal sets. In nested cycles are investigated coordinate system single points and tested for conditions that correspond to the fractal structure. In case of the Mandelbrot set, this condition is expressed by equation (2). At the end of this step is to create two-dimensional field that carries information about each sample point. This information says that the fractal iteration equation left the investigated point boundary conditions defined fractal structure. A number of these iterations given input variable number of iterations, which can be modified and significantly change the shape of the resulting fractal. The parameter number represents the number of passes of simulated clicks the mouse on the desktop fractal. Selection fractal view of the new center is executed via a random number generator. This selection is further influenced by the threshold parameter s orbit. This value gives the minimum number of iterations, which must contain a point randomly selected to be included in the selection of a new center of the display. This finding provides parameter structure that contains a wide range of points on orbits of different sizes, which is convenient for the problem. After finding a new point is the next iteration of the process. The number of iterations is given by the number of iterations. After the final iteration is generated fractal structure.

Fig. 2 Auto generating process Fig. 1 shows the principle the fractal structure analysis for determining of the maximum message length.

After generating the fractal visualization is displayed on the main program window. Fractal structure is stored in two-dimensional array, called the fractal structure [2], where each rendered pixel is represented by its coordinates and the number of iterations. In the next step, this field is analyzed and calculated the frequency of iterations of all the various elements it contains. This creates a data field called field of frequency where these frequencies recorded. In the first field of the index indicates the number of points that meet the structural conditions of the first fractal iteration, the second index are included frequency points that these conditions are fulfilled in the second iteration, etc. The maximum number of indexes of this field is related to the parameter set number of iterations.

The input alphabet contains alphabetic characters AZ, digits 0-9 and the other characters, what are the decimal points, minus sign or a space character or a special delimiter character keys. This information is stored in one-dimensional array, called the input alphabet characters, where each index contains one character from the input alphabet. After surgery, the descending sort field and frequency shift of the total number of indices that has a field input alphabet characters can specify the maximum length of information that can be encrypted.

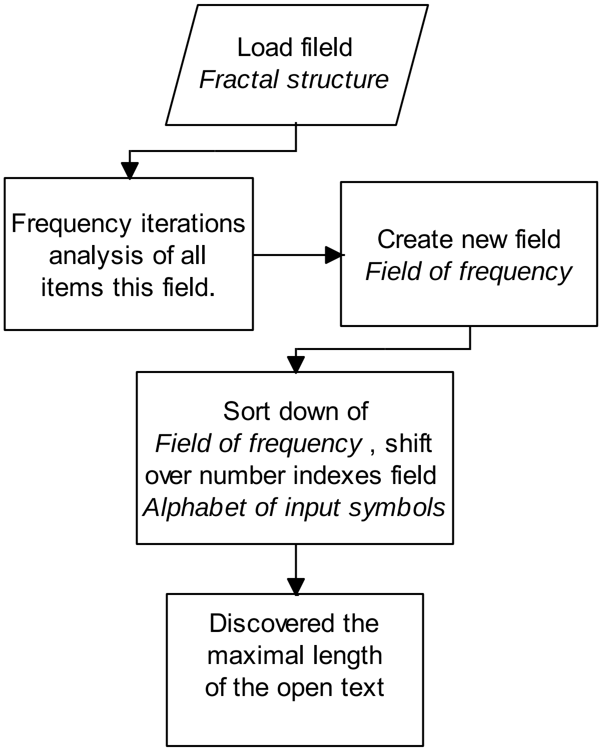
Load fileld
Fractal structure
Frequency iterations analysis of all items this field.
Create new field
Field of frequency
Sort down of
Field of frequency , shift over number indexes field
Alphabet of input symbols
Discovered the maximal length of the open text

Fig. 1 Maximal length message on the basis of fractal structure

Fig. 2 shows the automatic generating process. The process begins by reading the input parameters. These parameters contain values: The number of passages, Threshold orbit, initial size and number of iterations. Before starting the process of generating the coordinates of the coordinate system is in its infancy. The initial parameter range is determined by the area Cartesian coordinates, which will be started generating fractal. After this operation is generated the first iteration of fractal sets. In nested cycles are investigated coordinate system single points and tested for conditions that correspond to the fractal structure. In case of the Mandelbrot set, this condition is expressed by equation (2). At the end of this step is to create two-dimensional field that carries information about each sample point. This information says that the fractal iteration equation left the investigated point boundary conditions defined fractal structure. A number of these iterations given input variable number of iterations, which can be modified and significantly change the shape of the resulting fractal. The parameter number represents the number of passes of simulated clicks the mouse on the desktop fractal. Selection fractal view of the new centre is executed via a random number generator. This selection is further influenced by the threshold parameter s orbit. This value gives the minimum number of iterations, which must contain a point

randomly selected to be included in the selection of a new centre of the display. This finding provides parameter structure that contains a wide range of points on orbits of different sizes, which is convenient for the problem. After finding a new point is the next iteration of the process. The number of iterations is given by the number of iterations. After the final iteration is generated fractal structure.

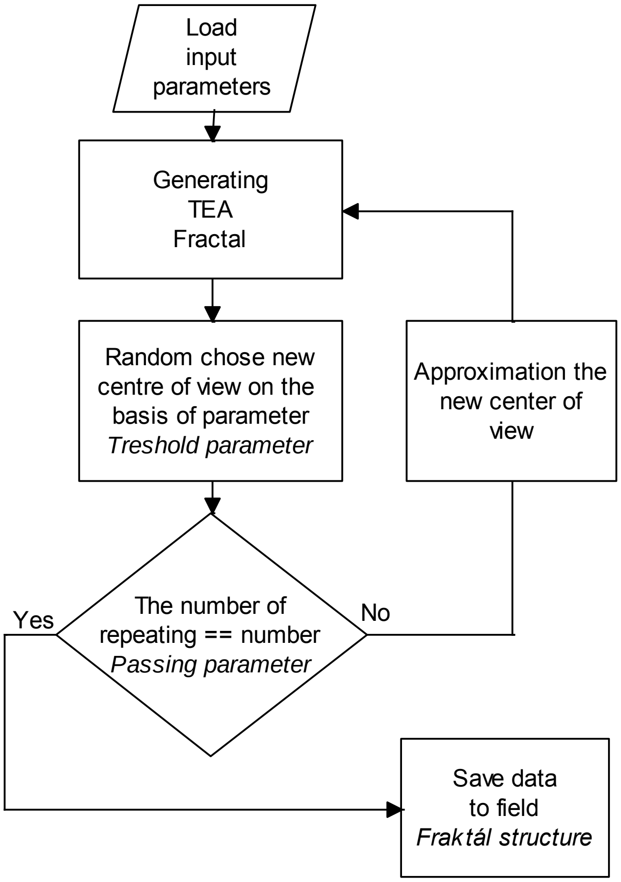
Load input parameters
Generating TEA Fractal
Random chose new centre of view on the basis of parameter *Treshold parameter*
Approximation the new center of view
The number of repeating == number *Passing parameter*
Yes
No
Save data to field *Fraktál structure*

Fig. 2 Auto generating process

III. Problem Solution

Polynomial fractals are between the most popular. Their design takes advantage of the attractiveness of areas for various solutions of nonlinear systems. The coordinate system is tested at points belonging to it, whether the rule meet the specified condition. Evaluation of equations, which are based on polynomial fractals, happens iteratively. Iterative cycle can be terminated either after a specified number of iterations, or after the evaluation of test conditions. After the process is the appropriate point in the coordinate system indicated by the ink. Here, depending on the specific application of fractal, if required by the resulting fractal monochrome to colour, such as shade or equal to the number of iterations performed in the evaluation algorithm. [4]

A. Principles of TEA Fractal Generating in the Information Encryption Process

For the purpose of the information encryption was used polynomial fractal. After the generating of this fractal was obtained parameters represent a password. For this experiment was used Mandelbrot set. The Mandelbrot set is a set of complex numbers defined in the following way: [5]

$$M = \left\{ c \in \mathbb{C} \mid \lim_{n \to \infty} Z_n \neq \infty \right\} \tag{1}$$

$$Z_0 = c$$
$$Z_{n+1} = Z_n^2 + c \tag{2}$$

The Mandelbrot set is the set of all complex numbers which fulfilled the condition described above, that is, if the value of the (recursive) function Zn for the value c is not infinite when n approaches infinity, then c belongs to the set. Attractors are related to the "orbit" of the function. This orbit is defined by the path formed by the values of Z at each step n. The orbit of Z for a certain value c either tends towards the attractor or not. In this type of fractals a value c causing the orbit of Z to go to the attractor point is considered to be outside the set. [5]

B. Parameters for Fractal Construction

Key factor for the construction of the fractal structures are necessary to set the initial conditions which symbolise key. **Chyba! Nenalezen zdroj odkazů.** shows parameters for construction of fractal set. Parameters X1, X2, Y1 and Y2 specify the coordinates of fractal field. Parameters were found by experimental generating process.

Table 1 Fractal parameters

X - part of the operating quadrant	*-0,903046875*
Y- part of the operating quadrant	0,2501171875
Range	*0,00390625*
Number of iterations	*250*

Fig. 3 shows the output of the fractal structure used in the algorithm for encryption process. It is part of the Mandelbrot set. The coordinates for generating this picture was used from **Chyba! Nenalezen zdroj odkazů.**.

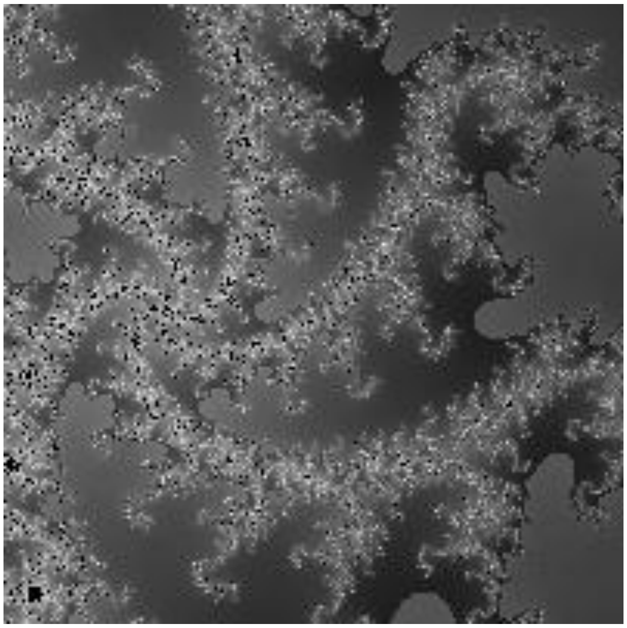

Fig. 3 fractal structure for encrypting information

C. Fractal Cipher Process in the Alphabet Mapping

In the process of mapping a character is determined by what value the orbit of the fractal structure will represent a specific character input alphabet. For this you created a new field, called the index field. The cycle is crawled field frequency. If the content index is greater or equal than the specified maximum message size, it is assigned a number that corresponds to the index in the input alphabet characters. In the next iteration of the loop index is incremented pointer field. Subject to the conditions described above to the index field is again assigned to the index entry corresponding letter alphabet. This operation is performed once for each index entry contains an array of alphabetic characters. The process of mapping determines the character of the orbit, which can be used to encrypt information using the fractal structure.

D. Comparison of Used Parameters in Generating Process

In the following tables are the parameters of fractal generator which each showed the best properties of fractal structure for the purpose of encryption.

Table 2 Mandelbrot set

Resolution	200 x 200	
Type of Data	Alpha-numeric	Numeric
Transits	12	10
Border	125	50
Iterations	145	55
Range	4	4
Average speed of generating	1,74s	0,52s
Average maximal length of message	310	989

Table 3 Julia Sets

Resolution	200 x 200	
Type of Data	Alpha-numeric	Numeric
Transits	9	10
Border	55	115
Iterations	295	315
Range	4	4
Average speed of generating	1,87s	2,09s
Average maximal length of message	281	779

Table 4 Burning Ship

Resolution	200 x 200	
Type of Data	Alpha-numeric	Numeric
Transits	15	17
Border	130	130
Iterations	235	215
Range	4	4
Average speed of generating	3,07s	3,18s
Average maximal length of message	362	894

Table 5 Bird of Prey

Resolution	200 x 200	
Type of Data	Alpha-numeric	Numeric
Transits	16	15

Border	130	90
Iterations	240	240
Range	4	4
Average speed of generating	3,46s	2,72s
Average maximal length of message	368	947

Table 6 Water Plane

Resolution	200 x 200	
Type of Data	Alpha-numeric	Numeric
Transits	19	8
Border	90	90
Iterations	150	210
Range	4	4
Average speed of generating	6,75s	3,63s
Average maximal length of message	203	334

Table 7 4th Degree Multibrot

Resolution	200 x 200	
Type of Data	Alpha-numeric	Numeric
Transits	18	15
Border	115	115
Iterations	135	295
Range	4	4
Average speed of generating	3,52s	5,91s
Average maximal length of message	268	768

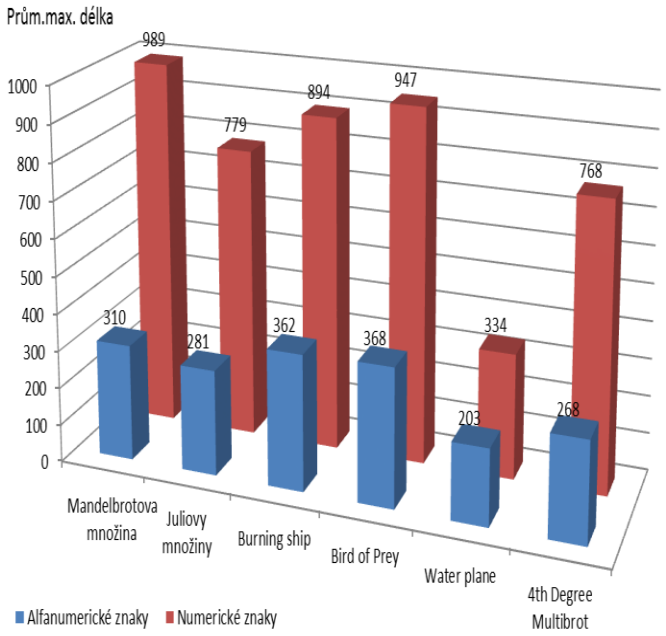

Fig. 4 Average - max length separates fractal structures

The best parameters of alphanumeric reached fractals Bird of Prey, and Burning Ship Mandelbrot set. In the numerical part of it was a Mandelbrot fractal set, Bird of Prey and Burning Ship. With the increasing number of passes grew and time-consuming generation of fractal structures.

IV. Conclusion

This article was focused on the possible use of fractal geometry for encrypting information. This process is an alternative for the now widely used encrypting functions. The process meets the requirements spoken in the second chapter. The process of generating and its principles are described in chapter three. The size of fractal object can be selected by modifying the function generating the initial conditions for the creation of fractals. The system uses the advantages of fractal geometry, in particular the wide range of fractal sets and the speed of its generation.

Appendix

A. Fractal structures used along the research – Mandelbrot set

$$M = \left\{ c \in \mathbb{C} \mid \lim_{n \to \infty} Z_n \neq \infty \right\} \tag{3}$$

$$Z_0 = c$$
$$Z_{n+1} = Z_n^2 + c \tag{4}$$

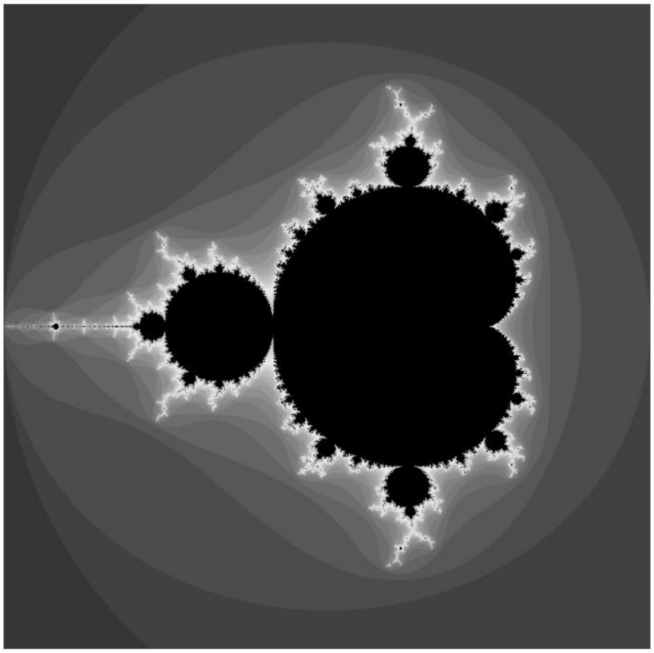

Fig. 5 Mandelbrot set

B. *Fractal structures used along the research – Julia sets*

$$J = \left\{ c \in \mathbb{C} \,\middle|\, \lim_{n \to \infty} Z_n \neq \infty \right\} \tag{5}$$

$$\begin{aligned} Z_0 &= c \\ Z_{n+1} &= Z_n^2 + K \end{aligned} \tag{6}$$

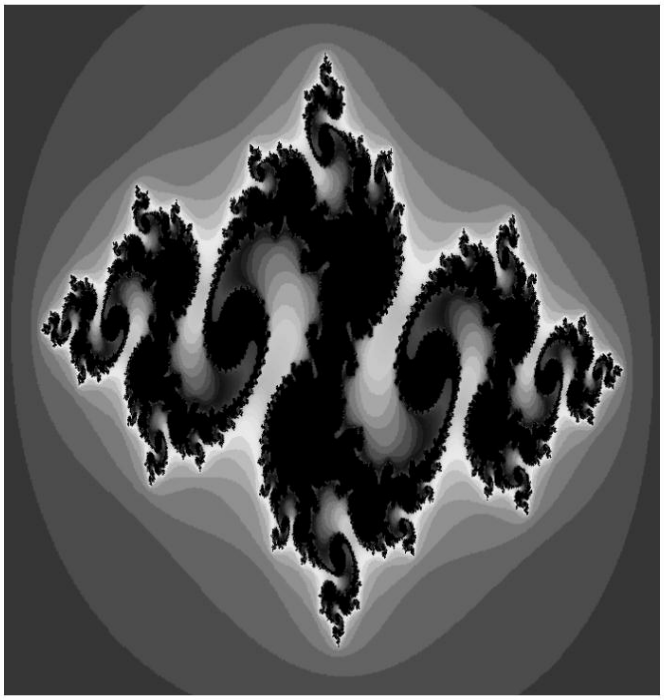

Fig. 6 Julia sets

C. *Fractal structures used along the research – Burning Ship*

$$B = \left\{ c \in \mathbb{C} \,\middle|\, \lim_{n \to \infty} Z_n \neq \infty \right\} \tag{7}$$

$$\begin{aligned} Z_0 &= c \\ Z_{n+1} &= [|Re(Z_n)| + i|Im(Z_n)|]^2 + c \end{aligned} \tag{8}$$

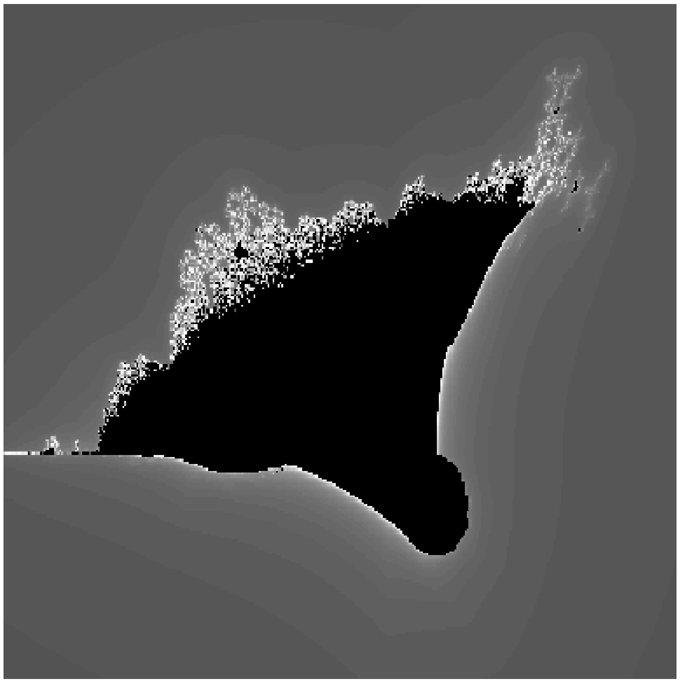

Fig. 7 Burning Ship

D. Fractal structures used along the research – Bird of Prey

$$P = \left\{ c \in \mathbb{C} \middle| \lim_{n\to\infty} Z_n \neq \infty \right\} \tag{9}$$

$$Z_0 = c$$

$$Z_0 = c[|Re(Z_n)| + i|Im(Z_n)|]^3 + c \tag{10}$$

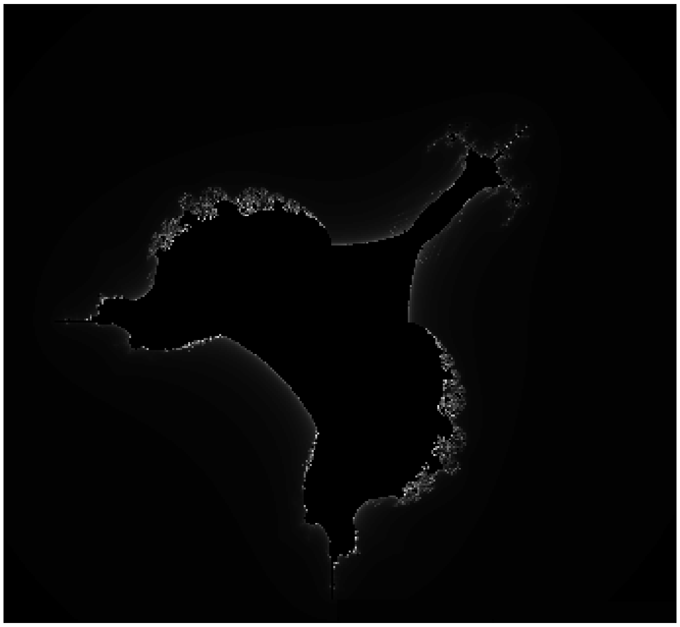

Fig. 8 Bird of Prey

E. Fractal structures used along the research – Water Plane

$$W = \left\{ c \in \mathbb{C} \middle| \lim_{n\to\infty} Z_n \neq \infty \right\} \tag{11}$$

$$Z_0 = c$$

$$Z_{n+1} = Z_n^3 + Sin(Z_n) + c \tag{12}$$

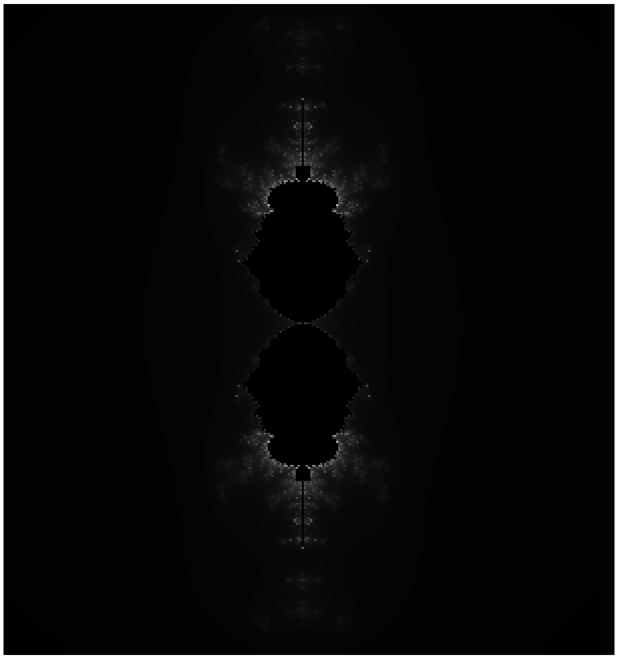

Fig. 9 Water Plane

F. Fractal structures used along the research – 4th Degree Multibrot

$$D = \left\{ c \in \mathbb{C} \mid \lim_{n \to \infty} Z_n \neq \infty \right\} \tag{13}$$

$$Z_0 = c$$

$$Z_{n+1} = Z_n^4 + c \tag{14}$$

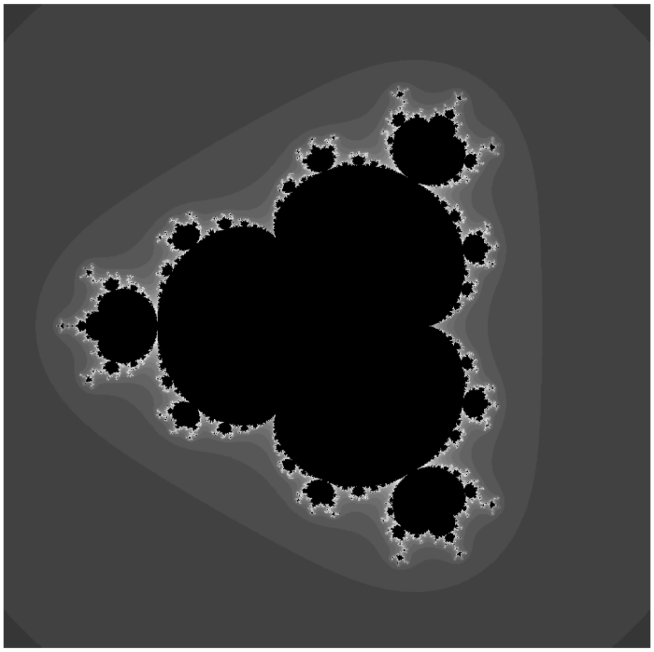

Fig. 10 4th Degree Multibrot

Acknowledgment

This article was supported by the European Regional Development Fund under the Project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089 and Internal grant agency (IGA/FAI/2012/019).

References

[1] PILLER, I., Hashovací funkce a jejich využití při autentizaci, Vysoké učení technické v Brně, 2009

[2] TŘÍSKA, D., Kryptografická ochrana, Univerzita Tomáše Bati ve Zlíně, 2009.

[3] MANDELBROT, B. B., Fractals nad chaos: the Mandelbrot set and beyond. New York: Springer, 2004. 308 s. ISBN 0-387-20158-0.

[4] ZELINKA, I. Fraktální geometrie – principy a aplikace, BEN Praha 2006.

[5] The Mandelbrot set, available from: <http://warp.povusers.org/Mandelbrot/>

[6] LOFSTEDT, T. Fractal Geometry, Graph and Tree Constructions, Umea University, Sweden 2008.

[7] PIPER, F., MURPHY, S. Kryptografie – průvodce pro každého. 1. vyd. Praha:Dokořán, 2006. 157s. ISBN: 80-7363-074-5.

[8] BOSE, S. Information theory, coding and cryptography. Tata McGraw-Hill Education, 2008. 326s. ISBN: 0070669015.

[9] SPROTT, J. C., Chaos and time-series analysis aplikace. Oxford University Press, 2003. 507 s. ISBN:978-0198508403.

[10] STAIR, R. M., REYNOLDS, G. W. Principles of Information systems. 7. vyd. Course Technology, 2005. 808 s. ISBN-10: 9780619215613.

[11] MOTÝL, I., PÁLKA, J., JAŠEK, R.: Application of hash function to increase security level of the information system. In Int. 2010. Internet, bezpečnost a konkurenceschopnost organizací. Zlin 17-18. 3. 2010. ISBN 978-83-61645-16-0.

[12] *CAREY, J., M.* Human Factors in Information Systems: *The Relationship Between User Interface Design and Human Performance. 1. vyd. USA: Intellect Books, 1996. 254 s. ISBN: 9781567502862.*

[13] *FEIL, T., SINKOV, A.* Elementary Cryptanalysis. *2. vyd. USA: Michigan university, 2009. 226 s. ISBN: 9780883856475.*

[14] *GALBRAITH, S. Blockwise – Adaptive Chosen – Plaintext Attack and Online Modes of Encryption.* American Journal of Applied Sciences 4. *1^{st} ed. Heidelberg: Springer, 2007, vol. 23 , p. 129-151.*

[15] KAHATE, A. Cryptography in the database. 2. vyd. New York: Tata McGraw-Hill Education, 2008. 792 s. ISBN: 9780070648234.

[16] KIZZA, J., M. Computer Network Security. 1. vyd. USA: Springer, 2005. 534 s. ISBN: 9780387204734.

[17] LESMOIR-GORDON, N., ROOD, W., EDNEY, R. Introducing Fractal Geometry. 3. vyd. United Kingdom: Icon Books, 2002. 176 s. ISBN: 9781840467130.

[18] LU, N. Fractal Imaging. 1. vyd. London: Academic Press, 1997. 412 s. ISBN: 0124580106.

[19] NAGEL, CH., EVJEN, B., GLYNN, J. Professional C# 2008. 1. vyd. USA: John Wiley & Sons, 2011. 1848 s. ISBN: 9781118059463.

[20] POUR, J. Informační systémy a technologie. 1. vyd. Praha: VSEM, 2006. 492 s. ISBN: 9788086730035.

[21] SCHNEIDER, B. Applied cryptography: Protocols, algorithms, and source code in C. 2. vyd. USA: Michigan university, 1996. 758 s. ISBN: 9780471128458.

[22] STAIR, R., M., REYNOLDS, G., REYNOLDS, G., W. Fundamentals of Information Systems. 5. vyd. USA: Cengage Learning, 2006. 457 s. ISBN: 9781423925811.

[23] SUTTON, R., J. Secure Communications: Applications and Management. 1. vyd. USA: J. Wiley & Sons, 2002. 322 s. ISBN: 9780471499046.

[24] WHITMAN, M., MATTORD, H., J. Principles of Information Security. 4. vyd. USA: Cengage Learning, 2011. 617 s. ISBN: 9781111138219.

[25] LONG, J., MITNICK, D. No Tech Hacking: A guide to social engineering, dumpster diving, and shoulder surfing. Syngress, 2008. 285 s. ISBN 1597492159.

[26] GODBOLE, N. Information systems security: Security management, metrics, frameworks and best practices. 1. vyd. India: Wiley India Pvt. Limited, 2008. 1020 s. ISBN: 9788126516926.

Ivo Motyl is a member of doctoral study program on the Department of Informatics and Artificial Intelligence, Faculty of Applied Informatics. He was born in Zlin, Czech Republic on 11.3.1984. He received his bachelor's degree in Faculty of Applied Informatics in Zlín in the year 2006. Later, he was awarded master's degree in the same place in the year 2008. He started doctoral study programe in 2008. He was on the short term attachment in the University in Vigo in 2010. He made degree examination in 2011. He has published 24 technical papers in international journals and conferences.