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.
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.
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.

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]

\[
M = \left\{ c \in \mathbb{C} | \lim_{n \to \infty} Z_n \neq \infty \right\} 
\]  

(1)

\[
Z_0 = c \\
Z_{n+1} = Z_n^2 + c 
\]  

(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 \( Z_n \) 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 odkazu. shows parameters for
construction of fractal set. Parameters \( X_1, X_2, Y_1 \) and \( Y_2 \)
specify the coordinates of fractal field. Parameters were found
by experimental generating process.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>( X ) - part of the operating quadrant</td>
<td>-0.903046875</td>
</tr>
<tr>
<td>( Y ) - part of the operating quadrant</td>
<td>0.2501171875</td>
</tr>
<tr>
<td>Range</td>
<td>0.00390625</td>
</tr>
<tr>
<td>Number of iterations</td>
<td>250</td>
</tr>
</tbody>
</table>

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 odkazu.
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>
<thead>
<tr>
<th>Table 2 Mandelbrot set</th>
<th>200 x 200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolution</td>
<td>200 x 200</td>
</tr>
<tr>
<td>Type of Data</td>
<td>Alpha-numeric Numeric</td>
</tr>
<tr>
<td>Transits</td>
<td>12 10</td>
</tr>
<tr>
<td>Border</td>
<td>125 50</td>
</tr>
<tr>
<td>Iterations</td>
<td>145 56</td>
</tr>
<tr>
<td>Average speed of generating</td>
<td>1,74s 0,52s</td>
</tr>
<tr>
<td>Average maximal length of message</td>
<td>310 989</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 3 Julia Sets</th>
<th>200 x 200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolution</td>
<td>200 x 200</td>
</tr>
<tr>
<td>Type of Data</td>
<td>Alpha-numeric Numeric</td>
</tr>
<tr>
<td>Transits</td>
<td>9 10</td>
</tr>
<tr>
<td>Border</td>
<td>55 115</td>
</tr>
<tr>
<td>Iterations</td>
<td>295 315</td>
</tr>
<tr>
<td>Range</td>
<td>4 4</td>
</tr>
<tr>
<td>Average speed of generating</td>
<td>1,87s 2,09s</td>
</tr>
<tr>
<td>Average maximal length of message</td>
<td>281 779</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 4 Burning Ship</th>
<th>200 x 200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolution</td>
<td>200 x 200</td>
</tr>
<tr>
<td>Type of Data</td>
<td>Alpha-numeric Numeric</td>
</tr>
<tr>
<td>Transits</td>
<td>15 17</td>
</tr>
<tr>
<td>Border</td>
<td>130 130</td>
</tr>
<tr>
<td>Iterations</td>
<td>235 215</td>
</tr>
<tr>
<td>Range</td>
<td>4 4</td>
</tr>
<tr>
<td>Average speed of generating</td>
<td>3,07s 3,18s</td>
</tr>
<tr>
<td>Average maximal length of message</td>
<td>362 894</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 5 Bird of Prey</th>
<th>200 x 200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolution</td>
<td>200 x 200</td>
</tr>
<tr>
<td>Type of Data</td>
<td>Alpha-numeric Numeric</td>
</tr>
<tr>
<td>Transits</td>
<td>16 15</td>
</tr>
</tbody>
</table>
Table 6 Water Plane

<table>
<thead>
<tr>
<th>Resolution</th>
<th>200 x 200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of Data</td>
<td>Alpha-numeric</td>
</tr>
<tr>
<td>Transits</td>
<td>19</td>
</tr>
<tr>
<td>Border</td>
<td>90</td>
</tr>
<tr>
<td>Iterations</td>
<td>150</td>
</tr>
<tr>
<td>Range</td>
<td>4</td>
</tr>
<tr>
<td>Average speed of generating</td>
<td>6,75s</td>
</tr>
<tr>
<td>Average maximal length of message</td>
<td>203</td>
</tr>
</tbody>
</table>

Table 7 4th Degree Multibrot

<table>
<thead>
<tr>
<th>Resolution</th>
<th>200 x 200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of Data</td>
<td>Alpha-numeric</td>
</tr>
<tr>
<td>Transits</td>
<td>18</td>
</tr>
<tr>
<td>Border</td>
<td>115</td>
</tr>
<tr>
<td>Iterations</td>
<td>135</td>
</tr>
<tr>
<td>Range</td>
<td>4</td>
</tr>
<tr>
<td>Average speed of generating</td>
<td>3,52s</td>
</tr>
<tr>
<td>Average maximal length of message</td>
<td>268</td>
</tr>
</tbody>
</table>

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

\[ M = \left\{ c \in \mathbb{C} \mid \lim_{{n \to \infty}} Z_n \neq \infty \right\} \]

(3)

\[ Z_0 = c \]
\[ Z_{n+1} = Z_n^2 + c \]

(4)
B. Fractal structures used along the research – Julia sets

\[ J = \left\{ c \in \mathbb{C} | \lim_{n \to \infty} Z_n \neq \infty \right\} \]

\[ Z_0 = c \]
\[ Z_{n+1} = Z_n^2 + K \]

C. Fractal structures used along the research – Burning Ship

\[ B = \left\{ c \in \mathbb{C} | \lim_{n \to \infty} Z_n \neq \infty \right\} \]

\[ Z_0 = c \]
\[ Z_{n+1} = [\|Re(Z_n)\| + i|Im(Z_n)|]^2 + c \]
D. Fractal structures used along the research – Bird of Prey

\[ P = \left\{ c \in \mathbb{C} \mid \lim_{n \to \infty} Z_n \neq \infty \right\} \]  

(9)

\[ Z_0 = c \]

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

(10)

E. Fractal structures used along the research – Water Plane

\[ W = \left\{ c \in \mathbb{C} \mid \lim_{n \to \infty} Z_n \neq \infty \right\} \]  

(11)

\[ Z_0 = c \]

\[ Z_{n+1} = Z_n^3 + \text{Sin}(Z_n) + c \]  

(12)
F. Fractal structures used along the research – 4th Degree Multibrot

\[ D = \{ c \in \mathbb{C} | \lim_{n \to \infty} Z_n \neq \infty \} \]

(13)

\[ Z_0 = c \]

\[ Z_{n+1} = Z_n^4 + c \]

(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

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 Zlín, 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.