# Fractal Theory Based on the Pseudo-Attacks on Encryption Model

**MA Ji**

*Shenyang University, Shenyang, China*

*e-mail*: *mjllmjt*@163.*com*

**Abstract:** From the angle of improving data encryption in the information domain, we put forward an arithmetic that applies the fractal geometry characteristic and spatial alternation to data encryption technology, and simultaneously uses the method that spoils the data to achieve the purpose which protects the data. Turn an ordered and significant data into several out-of-order and insignificant data, and then combine the data which is gotten by pseudo-attacking with the rules which are brought by the attacking and augment the additive data. The experiments show that the arithmetic can make the fractal transformation be focused on any details of encryption, and make the scale of fractal achieve the operation of bit. Simultaneously, the arithmetic has certain safety, and it can be used with the existing data encryption technology to increase the safety of the existing encryption technology. The arithmetic can also be applied to logic circuit, namely, to encrypt the digital signal which is transmitted on medium.

**Keywords:** fractal technology; spatial alternation; data encryption technology; pseudo-atman attack

## 1. Introduction

The information in the crisis-ridden society, as people for information confidentiality, integrity and authenticity has become increasingly demanding, encryption algorithms and more complex. In the encryption process, in order to clear as the encrypted data, processed through the logic, to make it not clearly stated intention. Despite this, we can also consider the hidden ciphertext plaintext of all the data. Many encryption key management and encryption in order to achieve the balance of speed, will adopt the European-style two-dimensional space of some classical linear or discrete mathematics as a theoretical basis for key management. But because the European space integral dimension of the limit, generate the key, if the law ignores some features, would produce some weak keys and semi-weak keys.

For these reasons, the use of a new theory to establish a viable new algorithm for the graphical information

## 2. Design Idea

If the “approximate the integral values may have different geometric significance” [1]. This feature and fractal theory, designed to join together with the encryption algorithm, may make a more secure encryption algorithm, based on the idea to make the following algorithm:

For any document stored in a computer a simple operation, so that it can be seen as a variable x as a column to the variable y as the line of two-dimensional plane, that is, xOy; the rules of cutting processing; the start of each district where the behavior of data axis, so that partition the data in the rollover to the xOz plane parallel to the axis and contains the corresponding plane (see Figure 1, the number of axis and the vertical with the original plane cutting the number of related).

After such transformation, which the concept can be a body to manipulate the data, the body has the following characteristics:

1) At the end of the original graph can be considered the amount of data of all axes;

2) The boundaries of the different time-cut produce, so it is not all vertices belong to the same plane, but according to the rules generated by splitting surface;

3) The parallel to the longitudinal distance between the first-order infinitesimal Δ.

After such an operation, it can be considered to be a three-dimensional space after the irregular body. Such

Received Date: 2009-Fund Project: Liaoning Provincial Department of Education Science and Technology Program A Class (04D091), Shenyang Science and Technology Program (2007KY1032, 1091178-1-00) Funding Author：Ma Ji (1953－) man Professors，Master Tutor, Engaged in communication engineering automatic control theory and applications.



978-1-935068-06-8 

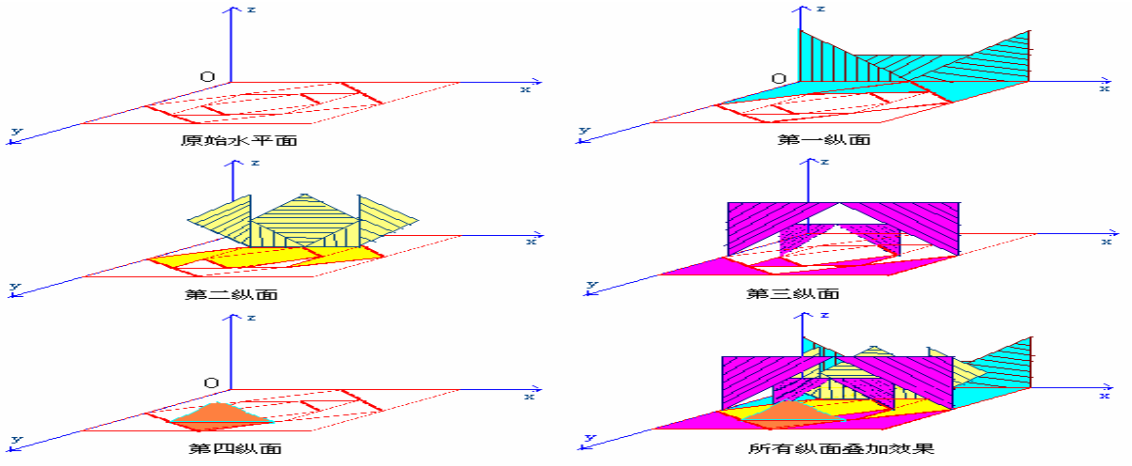


**Figure 1. Explanation of the algorithm**

rules can be proved through the following methods:

$$\text{Set } F(x) = \iint f(x)dxdy, G(x)$$

$$= \iiint g(x)dxdydz, \text{ And } F(x) = G(x)$$

Clearly $F(x)$ and $G(x)$, the geometric meaning is different, $F(x)$ is a two-dimensional space in the graphics area, $G(x)$ is a three-dimensional space the size of graphics, but the relationship between algebraic values are equal.

$$\iint f(x)dxdy = \iiint g(x)dxdydz$$

That we are asking for from the plane to the body of the derivation formula. These are just a simple change, but because the space dimension increases, making traversal is no longer simple, or is obviously difficult to change before. If we continue to use this method, for each vertical have adopted such a transformation, that is all the area is similar to the independent existence of any parallel to the plane yOz get the body shape will be more complex. Reuse of a pseudo-random way to engage in distortions of space for each flat, we can get a four-dimensional space objects.

Although we can conduct a space conversion, for confidentiality of the data, it is not enough. Because of space though distorted, there are still some continuous, meaningful data. It is necessary in order to break this relationship. To do this, select the one that can traverse the path all the data objects so that the overall spatial distortion along this path again.

To do this, select the one that can traverse the path all the data objects so that the overall spatial distortion along this path again. Also, the object surface and a cube of space between the border so that the new two-dimensional plane, there are many airspace, the airspace to increase the randomness of the data traversal and data analysis more difficult.

After two years of the new space conversion was flat, with its formation process, the four-dimensional space objects, all points within the characteristics and values. Operation of this plane to complete the original four-dimensional space objects, all points of operation. And the regularity of two-dimensional space can cause the object in the path of the corresponding complex changes in the path. Therefore, we chose a well-established law, but also with differences in the path of its own to change the location of the new plane of data. At the same time, creating a new set of mobile data plane is not validation data as additional data. When the operation is completed, the four-dimensional space objects in accordance with this point in the path of the corresponding two-dimensional space complete the data path of movement. After such pre-set operation, the original data has been fragmented, that is, pseudo-attack operation is complete. At this point, we get a distorted four-dimensional space. All air space filled with additional data, which is to be a standard European-style three-dimensional space in the cube contains a four-dimensional space, objects cutting room. Distortion due to space and the additional data interference, making this method even more detrimental to differential cryptanalysis, that is not easy to crack [2-4].

Based on the above design ideas, obtain the following modules:

The preparation phase: the original document is adjusted to facilitate the operation of the data process is called normalization;

Pseudo-attack first phase: the data segmentation process is called packet, while grouping module needs to be done after two transform two-dimensional plane formed by the proportion of the new two-dimensional space and add distortion to the true separation of data by region operations completed by the disintegration of the module.

Also in the decryption, each module corresponds to the method exists, but the encryption process is called decryption process and the corresponding module interfaces in reverse order.

In the module design process, in order to make interface design simple and easy to understand, all modules are symmetrical design.

## 3. Fractal Encryption Converter Detailed Module Design

### 3.1 Describe the Idea as a Whole

Algorithm is designed to crack encryption algorithms in order to allow all lost their versatility, that is, apply a different algorithm embedded in the module, making algorithms even if they are cracked, can not be judged is clear that this module is called converters. This is not changing the existing encryption technology, but to add some mechanism to make the security of the existing encryption technology can be improved significantly. Converter is a devastating real meaning of the algorithm, using a four-dimensional pseudo-self-attack mechanism to increase data security.

If you want to without changing the existing algorithms, then select an appropriate time to join the module as encryption key. Analysis of the data transfer process, assuming that encryption and transmission process is transparent; you can get the following model:

Data <-> terminal <-> Data Encryption <-> Network Transmission

Analysis concludes that there are three stages of the best stage to join the module. Namely: 1) Data <-> terminal; 2) terminal <-> Data Encryption; 3) Data Encryption <-> Network Transmission.

Because the data the algorithm to achieve a design must be pinned on one device as the medium, but also required for all encryption algorithm has no effect, so the data-to-end process to achieve the best stage of the algorithm.

### 3.2 Algorithm is the Basic Description of the Overall Process

Will be transmitted or the sender encrypted the original document as a clear reading, the use of a formatting mechanism, rendering the module can identify and deal with the formatting of data, followed by graphical boundaries correspond to the relative address of the method of formatting data division and made the following requirements:

1) For the design of the content is concerned, must be reversible based on the data division, and directly from the normalized data, the amount of data to determine the choice of graphics.

2) The complexity of the selected graphics should have, there are differences.

Conventional encryption algorithm for the characteristics, which is applied as the algorithm is an improvement in the idea of a good idea of fractal geometry confirmed this idea of existence and can be implemented.

3) After the split with the diversity of data.

The data is in the early stages of pseudo-attack with the uncertainty and therefore is more difficult to decipher and more secure.

The data generated will be divided into blocks of a pseudo-attack for the second phase of the data, broken data block by block in the first relative address from left to right, top-down order to fill in the corresponding row of new data and, based on the amount of data together with the relative address to confirm its position, and each line shows the specified location in the bank in the beginning and end location of the original data. The transformation of the block to the line of the process, generate information on-line verification. Derived rules derived based on additional data. After the end of the process into the pseudo-self-attacks, the second stage, namely, phase out of order. Can not repeat and can choose a bit-of-order data on all people wishing to traverse the path, as the base path of transformation. In the traversal, the generated data is valid data address there is a list of traversal step after the end of a specified


978-1-935068-06-8 © 2009 SciRes.

list of moving valid data address data stored in the corresponding bit to change the location of the data in the original data [5-8].

These are the basic algorithms described in the overall process. The analysis was informed that both the sender and the receiver have two main phases: the transmitter pseudo-attack phase and the receiver pseudo-attack to restore the stage.

### 3.3 Module

#### 3.3.1 Sender

When the sender to the receiver to send a document, the sender will transfer to send the process to read the document ready to be sent will be read into the document sent to the child in the process to normalize normalized. According to the rules laid down in advance of the specification data for the first phase of pseudo-self-attack operations, making it scattered fragments, these fragments according to a certain rule generation want out of order data.

#### 3.3.2 Receiver

When the receiver receives the sender of the document, the receiver transferred to receiving process to determine whether the document has to be restored group [2] to receive the full. If the document is missing, call the error-handling process to the sender to send control to recover the lost document issued, otherwise the document will receive the incoming group of fit process.

These are the ideas for the algorithm to achieve the overall design of each functional module derived from the design process.

## 4. Case Analysis to Prove

### 4.1 The Stability of the Calculation Algorithm

1) Bit code group and the law of transformation. The amount of data bits when the code group and the proportion of operations can be based on the actual document encoding format may be. When the encoding format to determine, this proportion would uniquely determined. Suppose an instance of the data in the calculation of the amount of code group and the bit conversion formula for 1B=8b.

2) Segmentation graphic dimension and measure. Pseudo-attack on the first phase of the selected laws of the fractal graphics is: each time cutting the original square area will be to add four isosceles triangle, the triangle will no longer be cutting operation, according to the description of such a graph derived from the triangle to know with the original graphics side of the proportion of right-angle triangle, that is similar to the ratio of

$$\gamma = \frac{\sqrt{2}}{4}, N = 4,$$

The dimension

$$\dim_s A_1 = -\frac{\log_a N}{\log_a \gamma} = -\frac{\log_a 4}{\log_a \frac{\sqrt{2}}{4}} = \frac{4}{3},$$

measure the amount of data corresponding to the reciprocal of normalized. That is, if the specification data for n, then the measure

$$\mu_1 = \frac{1}{n}$$

3) The chaotic sequence dimension and measure the graph Pseudo-attacks on the second phase of the selected laws of the fractal graphics is: each time to cut the original square area is divided into four equal size squares, and each resulting square regions to attend the next cutting operation, according to the above graphic descriptions that square with the original graphics in the proportion of square edges, That is similar to the ratio of

$$\gamma = \frac{1}{2}, N = 4,$$

The dimension

$$\dim_s A_2 = -\frac{\log_a N}{\log_a \gamma} = -\frac{\log_a 4}{\log_a \frac{1}{2}} = 2,$$

To measure corresponds to the reciprocal of the amount of data out of order. That is, if the normalized number of n, the first phase of cutting the number of k, then the measure

$$\mu_2 = \begin{cases} \dfrac{1}{\left[96 + \left(\frac{1}{2}\right)^{k-3} n\right](4k+1)}, & k < 3 \\ \dfrac{1}{(96+n)(4k+1)}, & k \geq 3 \end{cases}$$

4) Variation of the amount of additional data based on the above instructions may be added that the amount of data.

$$x' = \begin{cases} (\frac{1}{2})^{k-3}(4k+1)n - 8n, k < 3 \\ (4k+1)n - 8n, k \geq 3 \end{cases}$$

5) Subject to the transfer document focused on the

amount of data on each line changes of

$$S = \begin{cases} 96 + (\frac{1}{2})^{k-3} n, k < 3 \\ 96 + n, k \geq 3 \end{cases}$$

It is not difficult to see from the above laws of the fractal dimension of the graph can be recognized in the graphics recognition; measure and cut the number of relevant, namely the amount of data n-related; and all operations of the data are determined as the amount of data n, determined. Therefore, this process is considered to be stable. Because $A_1, A_2$ Owned a collection of mutually independent, the overall mathematical expectation:

$$E(A_1, A_2) = E(A_1)E(A_2) = \int \mu_1 dn \int \mu_2 dn$$

It can be simple that the two independent events identified by the safety factor for the two dimensions of the product graph [4].

### 4.2 Test Case Analysis

Assume that the paper we use the amount of data is 100kB, assume that the number of cut points 50 times, you can get:

$$\because k \geq 3, \quad n = 102400 + 16 = 102416$$
$$S = (96 + 102416) \times 50 = 5125600$$

The overall safety factor

$$\phi = \frac{8}{3}\omega > 1$$

$$E = \omega * 11.537 \cdot \omega * \frac{1}{201} \int \frac{1}{19296 + 201n} d(19296 + 201n) + c$$
$$= \omega * 11.537 \cdot \omega * \frac{1}{201} \times \ln|19296 + 201n| + c$$
$$= \omega * 11.537 \cdot \omega * \frac{1}{201} \times 16.841 + c$$
$$= \omega * 0.967 + 1$$

## 5. Conclusions

The algorithm mentioned in this article itself has some security, but also, and existing data encryption techniques used in combination to enhance the security of the existing encryption technology. Data encryption security and encryption algorithm cracked degree of difficulty levels have a direct relationship. The more difficult to crack encryption algorithms, security, the higher; generated more redundant data to increase the more the interference factors.

It is easy to implement because of the binary fractal program, and the calculation of a small amount of engineering applications can guarantee the confidentiality of data, therefore, this article focuses on the design of encryption algorithms. In practical applications, as needed, choose a different fractal function to break it down, as to what kind of fractal graphics better suited to this algorithm, the need to accumulate experience in practice. Algorithm itself is both and can be used alone, and other algorithms used in conjunction with the encryption algorithm, so if not for the network information transmission, also have a certain practicality. If the application logic circuit design ideas and other hardware to achieve, can be directly targeted at the media for information dissemination of the digital signal confidential.

In addition, data encryption process, if you want to focus to the fractal transformation can be encrypted in any detail; the need to scale up the fractal can be bit operation level. Fractal technology in information security technology is still in its infancy, I believe that with the gradual improvement of fractal theory to study the further development of the fractal technology information security technology will play a greater role.

## References


[1] Shi-Da Liu. Fractal Theory and fractal dimension [M]. Beijing: China Meteorological Press, 1993(9), 46-59.

[2] Keneth Falconer Fractal Geometry-Mathematics and Its Applications [M]. Shenyang: Northeastern University Press, 1991(8), 120-131.

[3] Dong-Xu Qi Computer-generated fractal [M]. Beijing: Science Press, 1994(11), 73-76.

[4] Wen-Qu Zheng, Xiang-Yang Wang waiting. Fractal theory and fractal computer simulation [M]. Shenyang: Northeastern University Press, 1993(9), 62-79.

[5] Falcone Qu–Wen Zheng Transtar Mathematical basis of fractal geometry and its applications (2nd edition) Beijing: Posts & Telecom Press, 2007(10), 83-97.

[6] Bo-wen Sun. Fractal design of algorithms and procedures-Visual Basic realization of [M]. Beijing: Science Press, 2004(11), 107-122.

[7] Bo-wen Sun. Fractal design of algorithms and procedures-Java realization of [M]. Beijing: Science Press, 2004(11), 132-146.

[8] Shu-Chun Du Single-chip C language and assembly language programming examples explain the mixed [M]. Beijing: Beijing University of Aeronautics and Astronautics Press, 2006(6), 36-69.