Advanced user authentication process based on the principles of fractal geometry

IVO MOTÝL, ROMAN JAŠEK
Department of Informatics and Artificial Intelligence
Thomas Bata University
Faculty of Applied Informatics nám. T.G.Masaryka 5555
Czech Republic
motyl@fai.utb.cz, jasek@fai.utb.cz

Abstract: This article is focused on authentication of users inside and outside the information systems. For this purpose is widely used hash function. The proposed process is based on the elements of the fractal geometry. 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. The system meets all the conditions for the construction of hash functions.

Key-Words: HASH, hash function, fractal geometry, information system, security, information security, authentication, protection, fractal set

1 Introduction

Hash functions have in the world of information technology an important role. They are represented in many areas of the information system. Hash functions can be used for example in password section of information system, data identification, integrity control, database comparing and many others solutions.

Hash functions are one-way functions, which must meet defined conditions. A hash function maps string of arbitrary length string of constant length (from a given large amounts of data returns a much smaller amount of data, but it clearly shows the contents of the document). The resulting impression is dependent on all bits of the string. [2] Hashing is the process of taking any input and transforming it into a fixed length string. This output which is obtained is called the hash value/message digest. In informal terms, a hash is a sort of signature/identification for some stream of data which represents the value of the data. It is a one way transformation. [3]

The aim of this study was describe how to using fractal geometry generates hash function for secure authentication inside of the information system.

2 Problem Formulation

Using of fractal geometry for the authentication process is an alternative to authentication process using the hash function. For proper function of the process is necessary to ensure the following parameters:

- One-way function – For a given message M is very simple compute $h = H(M)$, but the h is computationally impossible to calculate M. This characteristic is very desirable and is used for example for storing passwords. We do not store password, but only stored hash code. When authentication is the point of direct comparison entered and saved passwords compare their hash codes.
- Non-collision function – impossibility to find a variety of M and M', then the $M \neq M'$ so that $h(M) = h(M')$. Two input strings are not allowed to apply the same hash.
- Random oracle – Output of the hash function must be as random.[1]

2.1 Principle of the classical HASH function in the authentication process

Fig. 1 shows the basic principle of the HASH function in password processing. This is only basic illustration case of the HASH process. In the modern information systems are items for more sophisticated solutions. One of them is for example Salting process. This is one of many possibilities how to increase the password security. The password processing in this case is very simple. The password is extended by the several random characters. All string is converted by the hash function to HASH. This HASH string is stored to database.

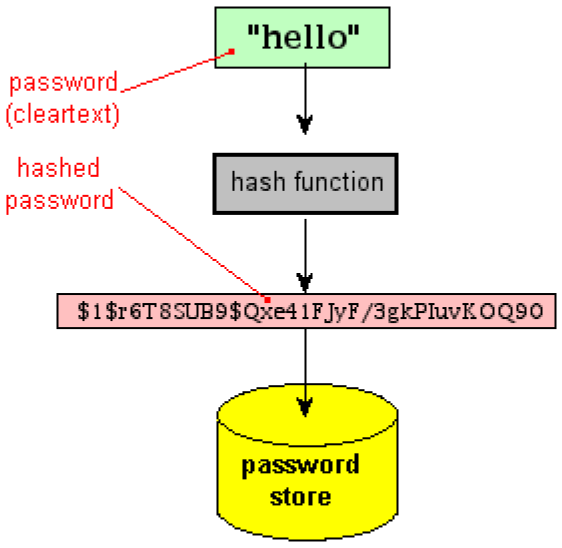

Fig. 1 Password hashing [3]

Fig. 2 shows the login process with the hashed password. The information system contain database with users password. In the first step user enter his secret password into the login form. The entered password is converted by the hash process to hash string. This string is compared with the record in database. If the entered password is correct, the user is successfully logged.

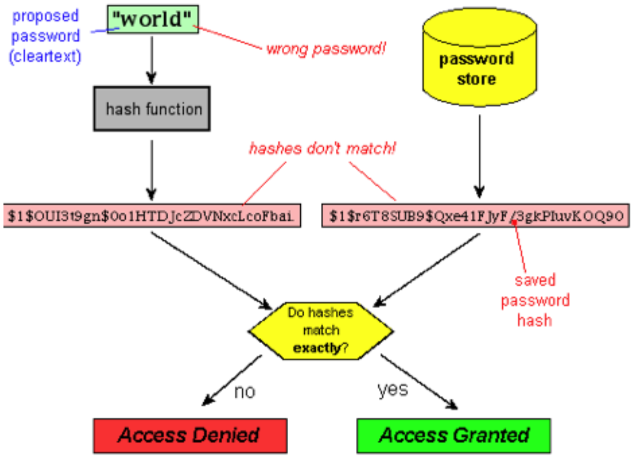

Fig. 2 Login process [3]

3 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]

3.1 Principles of fractal geometry for HASH generating

To generate fractal impressions of password can be used polynomial fractals described in section 3. For this experiment was used Mandelbrot set. The Mandelbrot set is a set of complex numbers defined in the following way: [5]

$$M = \left\{ c \in \mathbb{C} \middle| \lim_{n \to \infty} Z_n \neq \infty \right\} \quad (1)$$

$$Z_0 = c$$
$$Z_{n+1} = Z_n^2 + c \quad (2)$$

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]

3.2 Parameters for fractal construction

For the construction of fractal hash is necessary to set the initial conditions. Table 1 shows parameters for construction of fractal set. Parameters X1, X2, Y1 and Y2 specify the coordinates of fractal field. Parameters were found by experimental process. The experimentally determined parameters are used as the basis for creating new parameters for the user password. User password is converted to ASCII characters arranged in a row and increment to rest of the value on the fifth place behind the decimal point.

This border is optimal for the purpose of this process. In the case that the value of place was less could to be stuck in a place where he reached the full number of iterations in the creation of fractal.

X1- real part of the operating quadrant	*0,371447488729618*
Y1- imaginary part of the operating quadrant	*0,37149495542098*
X2 - real part of the operating quadrant	*0,585327310008748*
Y2 - imaginary part of the operating quadrant	*0,58537477670011*
Number of iterations	*640*

Table 1 Fractal parameters

Fig. 3 shows the output of the fractal structure used in the algorithm for advanced user authentication. It is part of the Mandelbrot set. The coordinates for generating this picture was used from Table 1.

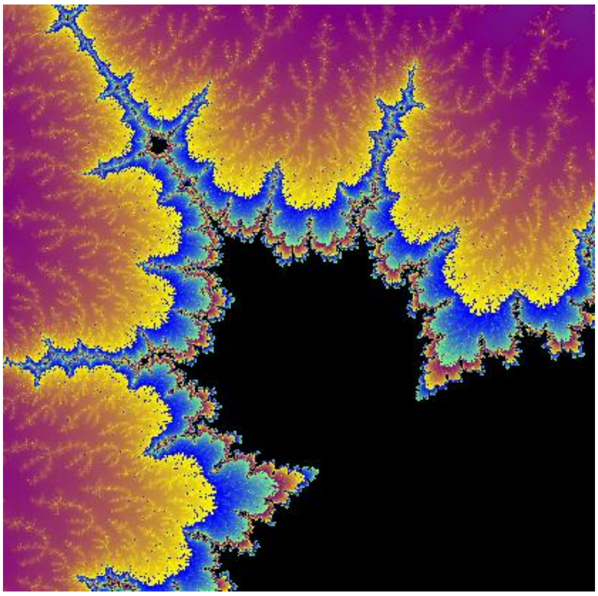

Fig. 3 fractal structure for advanced user authentication

3.3 Fractal HASH functions in the authentication process

Fig. 4 shows the login process with the fractal hashed password. The information system contain database with users password in the form of fractal.

In the first step user enter his secret password into the login form. The entered password is converted to parameters for fractal algorithm. The fractal algorithm produces fractal images in agreement by the initial conditions. This image is compared with the record in database. If the entered password is correct, the user is successfully logged. This is caused by the conformity of the fractal images.

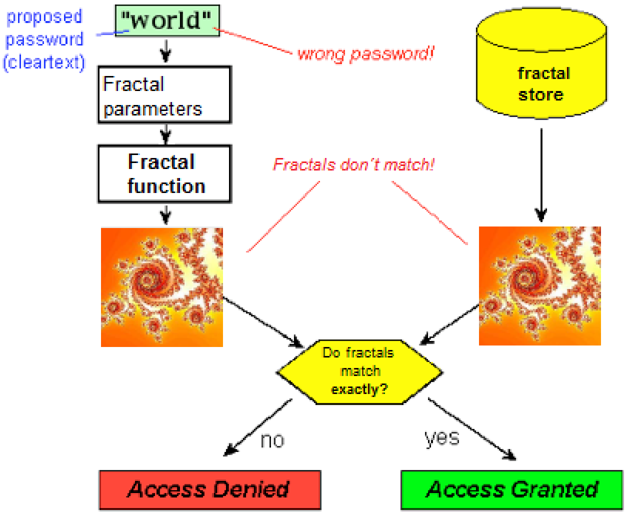

Fig. 4 Fractal authentication process

4 Conclusion

This article was focused on the possible use of fractal geometry for secure authentication of users. This process is an alternative for the now widely used hash function. The process meets the requirements spoken in the second chapter. The process of authentication and its principles are described in chapter three. If we compare the authentication process using hash function and fractal geometry, we find that in many ways are similar. 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.

Acknowledgement: 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/29/FAI/11/D).

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] Oracle ThinQuest, available from: <http://library.thinkquest.org/07aug/01676/relevance_cryp tog raphi ctec hnologies_authe ntication_ hashcodes.html>.
[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.