UDC 004.056
DOI: 10.15587/1729-4061.2024.313471

DETERMINING OPTIMAL PARAMETERS OF ALGEBRAIC FRACTALS IN ZERO-KNOWLEDGE AUTHENTICATION PROTOCOLS

Denys Samoilenko
PhD, Associate Professor
Department of Information Technologies
and Fundamental Study
Odesa Technological University "STEP"
Sadova str., 3, Odesa, Ukraine, 65023
E-mail: denniksam@gmail.com

Most information systems, especially on the Internet, have a distributed architecture with remote access and an insecure communication channel. In such systems, the tasks of permanent authorization mean implementing time intervals of user work without re-authentication are especially actual. The problem is that repeatedly sending a password increases the likelihood of it corruption. One solution is to use zero-knowledge protocols. In these protocols, passwords are not transmitted over the channel but are included in the algorithms as parameters. However, the computational complexity, as well as the finite number of passwords, limit their use, ensuring the relevance of further research. Focusing on object of the exchange protocols security, the use of algebraic fractal sets has been proposed as a potentially infinite source of data for passwords. In this work, algorithms were developed, implemented, and tested, which proved the higher reliability of fractal protocols in comparison with the reference generator of random bits (with an error probability of 0.5). It was also noted that the calculation operations have an insignificant influence on the overall time complexity of the exchange protocol as a whole. Practical recommendations for the use of fractals with a Hausdorff dimensionally of about 1.6 on the boundary of the Mandelbrot set are given. The paper also highlights the advantages of including color information in fractal sets, which gives about 3 times improving of confidential security indicators of communication protocol. The proposed algorithms do not require specialized software and can be implemented in the majority of network information systems as an additional module

Keywords: information security, network technologies, confidence, authentication, zero knowledge protocol, fractal

Received date 05.08.2024
Accepted date 15.10.2024
Published date 23.10.2024

How to Cite: *Samoilenko, D. (2024). Determining optimal parameters of algebraic fractals in zero-knowledge authentication protocols. Eastern-European Journal of Enterprise Technologies, 5 (9 (131)), 79–87. https://doi.org/10.15587/1729-4061.2024.313471*

1. Introduction

The principles of self-similar symmetry, the use of reduced copies of a large object within the same object, known as fractal principles, have been used by humankind in architecture and household art since ancient times. It should be emphasized that fractals are often found in nature, and in its various manifestations. However, the scientific study of fractals as independent objects began relatively recently, from the middle of the 20th century, due to the relative complexity of the mathematical apparatus for their description, the need to operate with fractional dimensionalities of figures. Moreover, it began precisely with the description of natural objects – calculating the length of countries' coastlines.

With the development of the computing power of electronic devices, mathematical complexity ceased to be an obstacle for the generation of fractals, their visualization and practical analysis or research. Manifestation of fractal features was found in less noticeable natural phenomena – signals, processes, etc. Fractal mathematics has shown multiple advantages of its algorithms in many areas of science and technology.

The complexity of fractals played a positive role in information security tasks. If one imagines protection as a certain digital "seal", then the complexity of its forgery will be greater, the more complex the structure of this seal. And here fractals show themselves as best as possible. Having potentially infinite detail, they provide high reliability, which does not lose its relevance with the development of technology. The deeper one can penetrate owing to new technologies, the smaller details one is able to study, the more the fractal details will reveal their infinity. Instead of switching to new protection technologies, one can simply calculate in more detail those that one already has. This proves the promise of introducing fractal objects into various information security tasks and a long period of their use, as well as the relevance of researching the security tasks themselves for the possibility of using fractals in them.

One of the tasks that require large sets of unique data for their work is the task of providing a security service "privacy in exchange". According to the regulatory documentation, this service is responsible for ensuring that requests are processed only if they come from administrators or users who have been granted the appropriate authority. The corresponding confirmation should preferably be updated with each request in order to prevent interception and reuse of previous data. Moreover, for the purpose of confirming the user's activity, requests can be forcibly sent with a certain frequency. At the same time, confirmation of confidentiality should have a single source – the user's password. This additionally testifies to the relevance of searching for sources with a large, potentially infinite capacity at constant values of the structural parameters.

On the other hand, repeated use of the same parameters can worsen the resistance of protocols to direct cryptanalytic attacks with the accumulation of long sequences of intercepted data. A reverse engineering resistance requirement is added to the sources of this data. The potential infinity of fractals in this problem can become a sufficient solution, once again confirming the promise of researching the possibility of using fractals in security tasks related to exchange protocols.

2. Literature review and problem statement

In [1], a detailed analysis of the possibility of general synchronization of systems with chaotic behavior using cryptographic transformations was carried out. It is shown that the transfer of personal data has a significant limitation, in particular, conclusions have been drawn regarding the refusal to transfer data in the form of audio recordings or signals. The work focuses on the predominance of the text type of data transmitted by the protocol, these conclusions are taken into account in the present paper. But the issues related to the user authentication itself, which precedes the issues of data transfer and synchronization, as well as the influence of the parameters of the fractal transformation on the reliability of the protocol, remained unresolved. The reason for this may be the adoption of the authentication process itself as a one-time, rather than a permanent, process similar to signaling.

Analysis of transformation parameters was considered in [2], in particular, conclusions were drawn regarding the optimal correlation at the level of 0.0511 for the used spherical fractal transformation when transmitting color images. Cryptographic transformations were also used during transmission. At the same time, the work is focused on images and issues of data transmission of other types were not considered. This may be related to the fundamentally different way of representing textual and graphic data and the difficulties in devising a unified approach to their description. However, the conclusion about the low data correlation coefficient is the basis for finding "sparse" fractal sets for protocol security problems.

Attempts to generalize approaches to fundamentally different processes and the data accompanying them are reported in [3, 4] in different ways. In particular, analogies were made between neural and network structures [3], and natural and anthropogenic factors [4]. Generalizations are based on bi-orthogonal decompositions of signals and also lead to conclusions about low correlation or fractional dimensionality of fractals. The results show the success of extrapolation of data obtained in one field of knowledge to another while preserving the fractal nature of their description. But at the same time, issues regarding security indicators during the transfer of relevant data between different consumers remained unresolved.

Work [5] focuses on solving the issue of safety and reliability. A mechanism for generating fragile digital watermarks (DWAs) for images using fractals was shown, with additional emphasis on self-similarity properties. The fragility of fractals is noted as the main sign of reliability. This conclusion can be easily transferred to arbitrary exchange protocols. Nevertheless, methods for introducing such "fragile" information into systems other than images were not considered in the work. The reason for this may be the low storage capacity of other containers, in particular, text containers.

Also, the promise of using fractal transformations is disclosed in [6]. The possibility of generating long numerical sequences for information security problems was shown. A long sequence length is a very similar characteristic to a set of password parameters. The results of the work can be adapted to exchange protocols with a large number of communications; however, such adaptation is not given in the work itself. The work also uses fields of integers, which have a lower power than fractional numbers.

Paper [7] shows the potential of using fractal sets as part of exchange protocols in order to improve the security of authorization data. The technology is based on the high sensitivity of the image of the fractal set to minor changes in the numerical parameters of the iterative transformation function. However, the work did not affect the reliability of color information of fractals, as well as their dimensionalities.

ISO 24165 standards provide for the use of digital token identifiers (DTI – Digital token identifier). According to the Internet standard RFC 8693, they are recommended for implementation in protocols in the form of digital media (Bearer) or in the form of JSON web tokens (JWT). However, the requirement to verify tokens for uniqueness (clause 6.2 of ISO 24165-1) significantly complicates their use for tasks of permanent authorization, which requires a large number of intermediate requests. Also, the need to store a large number of tokens, especially in JWT format, which will be received in the background, can become a complication.

All this gives reason to assert that it is expedient to conduct a study aimed at defining optimal parameters of fractal transformations for the task of maintaining permanent authorization in network exchange protocols.

3. The aim and objectives of the study

The aim of this study is to improve exchange network protocols with zero-knowledge by implementing algorithms based on algebraic fractals in order to determine the optimal parameters of these algorithms. This will provide an opportunity to implement permanent user authorization during a network session, resistant to intercepted data reuse attacks common in networks with an open data link.

To achieve the goal, the following tasks were set:

– to implement mechanisms for generating fractals (in the sense of algebraic fractal sets), to implement tools for comparing fractals;

– to introduce the color of the fractal point as a parameter, investigate the effect of color information on the general characteristics of the protocols, evaluate the effectiveness of its implementation with an obvious increase in the total number of parameters of the mathematical transformation;

– to investigate the influence of accuracy of parameters of fractal transformations on the magnitude of changes they cause in fractal sets and, as a result, on the assessment of the reliability of network protocols;

– to estimate the time complexity of the algorithms and the possibility of their implementation for typical performers such as personal computer browsers.

4. The study materials and methods

The object of this study is the security service "confidentiality during exchange" for communication processes taking place in computer networks with an unsecured communication channel. Algorithms based on protocols without disclosure are chosen as the subject of research.

The main hypothesis assumes that algebraic fractal sets in the complex number plane can be chosen for the source of confidential data of protocols that should not be repeated. The potential infinity of fractal detail is expected to resolve the conflict between multiple data generation and the success of direct cryptanalysis attacks. This hypothesis requires verification, as it can be assumed that slight differences of infinitely close points can lead to slight changes in the results of the fractal transformation. This can formally nullify the advantages of infinite detail, making the sets discrete within the permissible error of localization of their points.

Outlining the subject of the research, I note that protocols without disclosure (protocols with zero-knowledge, zero-knowledge protocol, PNR) are widely used in the tasks of authorization and authentication [8]. In accordance with PNR, the participant who authorizes themselves must prove that they have certain knowledge (password), while the knowledge itself is not disclosed – it is not transmitted in the communication channel either in an open or in a transformed form.

The authentication process involves performing a question-answer operation several times, based on the results of which a decision is made regarding the presence of knowledge of the participant of the protocol, that is, its authenticity. Externally, the process of implementing the protocol resembles the process of knowledge assessment, which is carried out by an automated distance learning system.

PNRs make it possible to balance the inconvenience that will arise when constantly asking the user for a password, and the potential vulnerability that occurs when providing long-term access with a single password entry. This is especially relevant for remote systems (web technologies), where there is no alternative control of operator change through video surveillance or physical access control.

PNRs are built on mathematical problems in a complicated inverse solution, that is, with the absence of fast algorithms for setting initial parameters based on a known problem solution. Such problems include, for example, the problem of factorization [9] or isomorphism of graphs [10].

Fractal mathematics problems can be an alternative to the common problems used in PNR. The circumstance that makes it possible to verify the correctness of the knowledge (password) in the object of authorization will look like checking whether the point with the given coordinates belongs to the fractal. It is obvious that without information about the parameters of the fractal construction, it is impossible to guarantee the results and check them.

Mathematical algorithms that allow unambiguously restoring the initial parameters of the fractal transformation based on several known points of the fractal image do not exist at present. At the same time, the complexity of the mathematical analysis of fractals requires additional research to assess the reliability of PNRs built on fractal transformations.

The general scheme of user interaction with the network information resource (NIR) can be simplified by the following scheme (Fig. 1).

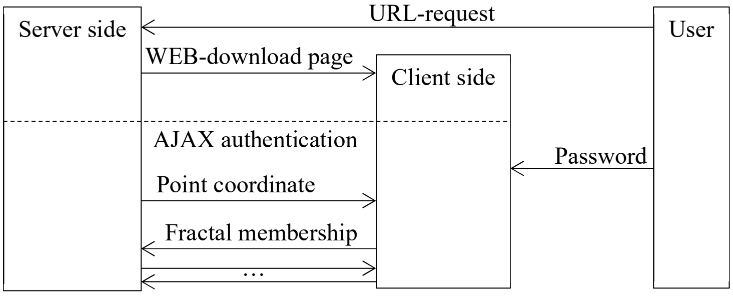

Fig. 1. Scheme of user interaction with a network information resource

The user enters the network address (URL) of the resource, the server generates a response in the form of a WEB page, which forms the client part of NIR, which is displayed by the browser. The provision of the confidentiality service during the exchange is offered in the form of a separate, self-sufficient part, outlined in Fig. 1 line "AJAX authentication". The following principle of its operation is proposed:

– user enters password information. This information is not transferred to the server, remaining exclusively on the client's side. After that, a periodic exchange process is launched;

– the server generates a random point of the complex space from the area of existence of the fractal and transmits its coordinates to the client;

– active codes of the client part calculate the membership of the point to the fractal set taking into account the entered password information, the calculation results are sent to the server as a response;

– the process is repeated with the necessary time interval until the communication channel is closed;

– if during the exchange of data it turns out that the client provided an incorrect calculation result, the exchange is terminated, a security incident is recorded, further work is regulated by the internal security policy, the purpose of the protocol is to detect privacy violations.

In the given form, the privacy algorithm can be implemented as a software module that does not require coordination with other communication processes. It also does not envisage an impact on the data transmitted by the channel during the main work of NIR. Therefore, it has a universal character and can be integrated into arbitrary network systems.

The described scheme was implemented experimentally. Apache HTTP Server version 2.4, server programming language PHP version 7 was used as the server. The client part is implemented in JavaScript without using additional frameworks or libraries. AJAX technology is implemented using the "window.fetch()" method, the implementation of "XMLHttpRequest" was not investigated separately since the basis of the algorithm is a mathematical calculation, and not a data transmission technique.

Experiments were conducted under two modes: local and network. Under the local mode, the server and client sides were deployed on the same physical computer, which made it possible to achieve a higher density of requests per unit of time. Under a network mode, the sides were spread over different computers on a local computer network. Measurements were repeated both within one local domain and in different local domains. It is assumed that the quantitative results obtained in different schemes will be averaged.

5. Results of research on the optimality of fractal parameters

5. 1. Generation and comparison of fractals

It should be noted that the term "fractal" does not have a single, generally accepted, clear definition. As a rule, fractals are a figure that has the properties of self-similarity or non-triviality or has a fractional dimensionality [11]. On the other hand, fractals can be algebraic sets with properties similar to those listed. Their typical representatives are the Mandelbrot set or the Julia set.

The fractional dimensionality of a fractal, the self-similarity of parts and the whole, as well as the non-triviality of its structure are related properties. It should be remembered that the Hausdorff dimensionality, which is used in this context, is the power of a function that characterizes the filling of a certain space by an object. It represents the asymptote of the ratio of the number of grid cells crossed (filled) by the object, depending on the inverse size of this grid. Accordingly, the smaller the grid cell, the larger the number of cells the object fills, and the extent of this growth (within the limit) is the dimensionality of the object.

It is obvious that a finite (in terms of shape) object cannot have a fractional dimensionality. At a certain level of detail (grid size), the object will be described completely, that is, it will occupy a fixed volume (area or length). After that, its dimensionality will stop changing, settling on the whole value. Typical dimensionalities for objects are 1, 2, or 3, depending on whether the object is a line, plane, or solid figure. So, the form of an object of fractional dimensionality requires infinite detailing, the disclosure of smaller and smaller details of the structure upon "closer" examination, which, in fact, means the non-triviality of the structure.

Infinite detailing of the object is possible under two conditions: either an infinite amount of information is embedded in the object, or some information block is repeated an infinite number of times, possibly undergoing transformation during repetitions. It is clear that objects with an infinite content of information cannot be built in a finite time. Therefore, in order to fulfill the requirement of non-triviality, the same structure with a finite amount of information must be endlessly repeated in the object. The latter makes the object self-similar – each of its parts contains many similar parts.

The only thing that should be noted is the possibility of an entire dimensionality even for objects of a non-trivial shape. A typical example is a "thread ball" in which a one-dimensional thread creates a three-dimensional structure. The dimensionality of such a tangle is exactly 2. To account for such exceptions, the requirement of differences in the topological and fractal (Hausdorff) dimensionalities of objects is added.

The infinity of the fractal form can serve as a source of a large number of non-repeating numerical (vector, matrix, etc.) values. If the coordinates of the point of the fractal are given with high accuracy, the question of belonging (or not belonging) of the point to the fractal requires establishing its boundary with no worse accuracy. At the same time, two points that are very close in distance can have different belonging to the fractal.

The reliability of authentication protocols is determined by the probability of successful intrusion or tampering attacks, which are carried out randomly or from the analysis of intercepted data. Accurate determination of the specified probabilities for fractal objects is complicated due to the peculiarities of their structure. Nevertheless, separate estimates based on general approaches can be given.

An intrusion attack, from the point of view of images, can be imagined as the probability of a point falling into the area of intersection of figures built on exact and approximate password information. As an estimate, I shall use information about the fractal dimensionality of Julia sets, which form the basis of protocols under consideration.

It can be argued that the area of intersection (the number of common points) of fractal sets is greater, the greater their fractal dimensionality. In analogy with the Euclidean dimensionality, an example can be given – the area of intersection of two lines versus the area of intersection of flat figures. Lines with arbitrarily close parameters of their equations still have one point of intersection (the case of parallel lines is an exception). At the same time, the intersection of plane figures is also a figure, that is, a set of points commensurate with the figure itself. In other words, the smaller the fractal dimensionality, the more robust it is to intrusion attacks.

On the other hand, objects with small dimensionalities are less resistant to substitution attacks based on the analysis of several intercepted messages. If it is known that the dimensionality of the figure is one, then it is enough to intercept N messages to completely restore the line, which is a polynomial of power N–1. In this sense, the restoration of a flat figure requires the interception of a much larger number of messages.

Fractals, as objects of fractional dimensionalities, make it possible to reach a certain balance for security indicators, which additionally proves in favor of their use as protective solutions. The study of various Julia sets made it possible to establish the limits of changing their dimensionalities from 1.2 to 2 [11] (for a quadratic form) and the possibility of obtaining intermediate values in the specified range.

From a practical point of view, monochrome fractals provide for checking whether a point of the complex space (re$X$, im$X$) belongs to its own set according to a single criterion – the absence of divergence of the iterative sequence during a given number of iterations. Classically, the following sequence is used for Julia sets:

$$z_{k+1} = z_k^N + C, \tag{1}$$

where C is a certain complex constant, N is the degree of transformation. The specific values of C and N determine the form of a specific set and play the role of a numerical password in information security problems.

The mathematical apparatus of the study is the generalization of Julia sets, which assumes an arbitrary complex function in the form of a polynomial power N in the right-hand side of expression (1):

$$z_{k+1} = \sum_{n=0}^{N} C_n z_k^n. \tag{2}$$

The coefficients C_n in these polynomials, as well as the value of N, form the set of password information of users. In other words, the password is a set of values $\{N, C_N, C_{N\text{-}1}, \ldots C_0\}$, which can be more powerful in a limited bitwise representation of numbers than the classic set $\{N, C\}$ in expression (1). From a practical point of view, the increased set of parameters provides wider opportunities for studying their influence on the overall efficiency of the algorithm.

One should also note the practical possibility of evaluating the divergence of sequence (2). Obviously, it is impossible to calculate an infinite number of iterations, and the search for periodicity does not guarantee its detection on a fixed length of the sequence. However, this situation is solved by introducing the concept of "color" of the fractal.

By the color of a point on the $\{N, C_N, C_{N\text{-}1}, \ldots C_0\}$ plane, I mean the number of iterations during which the sequence does not diverge. A practical criterion for divergence at a finite number of iterations $k_{\max}$ is a certain limiting value for the modulus of a complex number:

$$|z_k| > R_{\max}, \tag{3}$$

where $R_{\max}$ is a real number that guarantees further divergence of the sequence (greater than $\sqrt{2}$). Since the practical calculation of the modulus of a complex number requires a relatively complex calculation of the square root, the discrepancy condition can be replaced by a simpler one from the point of view of software implementation:

$$\left|\mathrm{Re}\, z_k\right| + \left|\mathrm{Im}\, z_k\right| = \left|x\right| + \left|y\right| > r_{\max}, \qquad (4)$$

where $r_{\max}$ is a number at least twice than $R_{\max}$. The specific values of $k_{\max}$ and $r_{\max}$ can also be attributed to the algorithm implementation parameters.

The specified features make it possible to specify the broad term "fractal" for a narrower use in this work. Hereafter, the fractal is understood as the set of all points $z=(x, y)$ of the complex plane for which the numerical value of "color" equal to the number of transformations k, during which transformation (2) remains within the limits of condition (3) or (4) in depending on the specific implementation.

If the sequence does not diverge in $k_{\max}$ steps, then the color of the point is considered "black" and is equal to the $k_{\max}$ value, which can be considered the "depth" of the color for the fractal. Monochrome fractals shall be understood as fractals whose color belongs to the set {0, 1} depending on whether transformation (2) converges or diverges during $k_{\max}$ iterations.

For the practical generation of fractals in the above sense, the following JavaScript code was used:

```
    n=0;
    while(n<255 && Math.abs(reX)+Math.abs(imX) <3) {
    x=reX*reX-imX*imX+reC; // Opening the square in
complex numbers
    y=2*reX*imX+imC; // reC and imC – components of
constant C
    reX=x;
    imX=y;
    n++;
    }
    if(n==255){
    Point (reX, imX) belongs to a fractal
    }.
```

The given code generates a monochrome fractal according to transformation (1) and illustrates the general approach to their generation. The parameters of the algorithm are N=2, $k_{\max}$=255, $r_{\max}$=3. For fractals with other parameters, the corresponding numbers should be changed, as well as the rules for transforming the variables x and y. For example, for N=5, the expression will take the following form:

```
    x=reZ**5–10*reZ**3*imZ**2+5*reZ*imZ**4+reC;

    y=5*reZ**4*imZ–10*reZ**2*imZ**3+imZ**5+imC.
```

Monochrome fractals are useful in cases where the data involved in the exchange should be minimized, since the result is a single bit. For example, this is relevant in the case of using steganographic means to hide authentication data among other information transmitted in the protocol.

It is the monochrome images that make it possible to determine the dimensionality of the fractal set since the belonging of the point to the image is established unambiguously. At the stage of choosing the optimal fractal set in terms of safety indicators, one should start with monochrome fractals (Fig. 2).

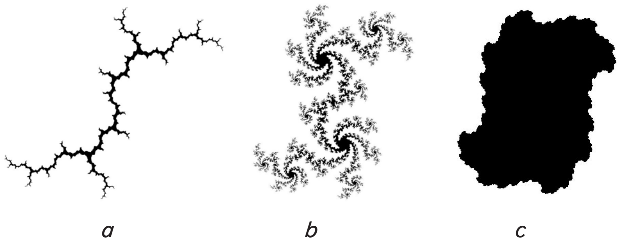

Fig. 2. Images from the Julia set with the following dimensionalities: *a* — 1.2, *C*=(0, 1); *b* — 1.6, *C*=(0.37, 0.37); *c* — 2.0, *C*=(0.25, 0.25)

Fractals with dimensionality 2 are obtained for constants C, which are the interior points of the Mandelbrot set. As C approaches the boundary of the Mandelbrot set, the fractal acquires "sparseness", which is accompanied by a decrease in its dimensionality. Also, at the same time, there is an increased sensitivity of the fractal to the selection of the maximum number of iterations.

From the images shown in Fig. 2, several conclusions can be drawn regarding the suitability of fractals for the given privacy problems:

– fractals with a dimensionality close to 1 (Fig. 2, *a*) contain a small number of points, occupying a small percentage of the total definition space. This is not acceptable for practical use;

– with dimensionality 2 (Fig. 2, *c*), the area of the fractal is close to half of the total definition space, which is positive. But such fractals are very predictable: the probability that points adjacent to a fractal point also belong to the fractal is very high. Ambiguous conclusion only for the border points of the fractal. It also makes practical use of such sets impossible.

Choosing an intermediate dimensionality (between 1 and 2) is a balance between the number of points and the predictability of its neighboring points. The best results were observed for dimensionality 1.6, the image of which is shown in Fig. 2, *b*.

5. 2. Influence of color information on the general characteristics of protocols

Additional security enhancements provide information about the color of the fractal points. To obtain them, they store information about the number of iterations after which the sequence diverges. This number of iterations is translated into a color gamut and applied to the drawing, forming a color image of a fractal.

Information about color complicates the understanding of the dimensionality of the set since in fact all points of space are formally related to the fractal. As already noted, in order to assess the dimensionality, which is conjugated with safety indicators, a monochrome image of the set should be constructed.

At the same time, color information complicates the process of discrediting the authentication protocol by increasing the set of possible answer values for a particular point. The probability of a random guess is the smaller, the greater the discreteness of the color information.

The conclusions obtained for monochrome fractals are also valid for colored ones. The maximum sensitivity to changing password parameters is observed for the limit points of the Mandelbrot set (Fig. 3).

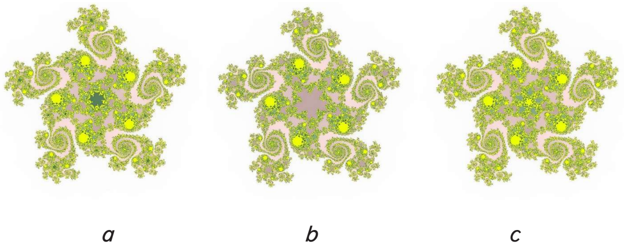

Fig. 3. Images of colored fractals for power *N*=5 and the following values of constants: *a* – C=(0.24493, 0.69915); *b* – *C*=(0.24494, 0.69915); *c* – *C*=(0.24493, 0.69916)

The following conversion of the color gamut was used when constructing the drawing:

```
if(n<20){r=g=b=255–n;}
else if(n<100){r=255-n+20;g=b=255–n–5;}
else if(n<200){g=255-n+20;r=b=255–n–5;}
else{b=255–n–3;g=r=255;},
```

where *r*, *g*, and *b* are the red, green, and blue components of the fractal color; *n* is the number of iterations until the divergence of the sequence from the code listing in chapter 5. 1.

As can be seen in Fig. 3, the difference of components *C* in the fifth sign after the comma leads to changes noticeable even "to the eye". At the same time, it should be noted that the central part of the fractal undergoes the greatest metamorphosis, while the changes on the periphery are less noticeable (less detailed). This testifies to the expediency of using a limited space containing the most sensitive to changes in the parameters of the fractal area in security tasks. Depending on other parameters of the fractal, these may not only be central areas.

Moreover, the general symmetry observed due to the peripheral areas of the image, as well as the direction of its "twisting" can provide information about the password data. Thus, the presence of five symmetrical branches indicates the power of transformation (*N*=5), their complete similarity indicates the absence of other powers in the transformation, and the direction of spiral rotation (counter-clockwise) determines the positive value of the imaginary part of the constant *C*.

In order to complicate such an analysis of fractal images, one should, firstly, avoid involving areas with obvious symmetry in the area of consideration and, secondly, use iterative transformations with combined powers (2) and, as a result, without clearly expressed symmetry of images.

Fig. 4 shows the fractal image by transformation (2) with the following coefficients:

$$z_{k+1} = z_k^4 + 0.3z_k + 0.523 + 0.411i.$$

As can be seen from Fig. 4, the axial symmetry of the fractal image is not observed. However, there remains a certain possibility to establish the greatest degree of transformation due to the presence of four peripheral branches. In order to hide this information, only the central part of the fractal space can be used.

The view of the central part (Fig. 4, *b*), at the same time, does not provide unambiguous information about symmetry. Moreover, the clearly visible pole of the fractal in the lower left part of the figure has 8-ray symmetry, which can be mistakenly interpreted as the power of transformation *N*=8.

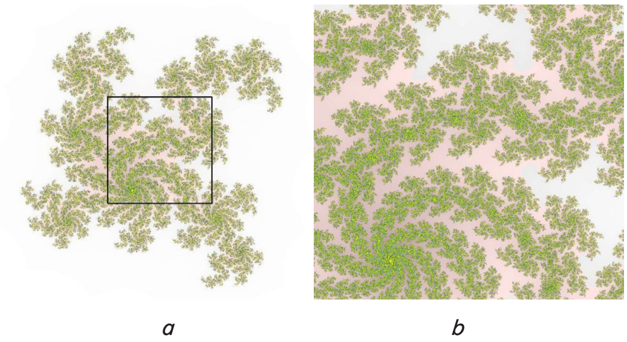

Fig. 4. The image of a fractal with the transformation formula $z_{k+1} = z_k^4 + 0.3z_k + 0.523 + 0.411i$: *a* – full space; *b* – central part

Differences in the color scheme between Fig. 3, 4 correspond to different values of iterations that occur before sequence divergence.

It should be noted that reducing the size of the space does not reduce the potential of using fractals in authentication protocols. On the one hand, the fractal detail is infinite for any area. On the other hand, data representation in computer technology involves the separation of the mantissa of a number and its exponent, that is, operation with numbers of a smaller range does not lead to loss of accuracy or discretization.

5. 3. Assessment of protocol reliability

A local information resource was compiled for the practical determination of the potential of permanent background authentication based on a protocol with zero-knowledge and using fractal sets. The server side is implemented in the PHP language, the client side is implemented in HTML/JavaScript.

The interaction algorithm implements Fig. 1. The sequence iteration program codes of both parts are completely identical. On the server side, the password data is entered as program constants, on the client side fields are provided for entering the corresponding values. The authorization process is repeated 10,000 times for each entry. As a result, the number of correct and incorrect answers of the client regarding the belonging of the point with the coordinates transmitted by the server to the given fractal and the frequency of errors are determined. The results of the tests of the authentication protocol are summarized in Table 1.

To form Table 1, fractals were used, the images of which are shown above in Fig. 2–4. To take into account the central part of the fractal, in some cases, the range of random numbers used in the server protocol was limited. Information about the range, if it was limited, is indicated in Table 1 separately. The color of the fractal (in the corresponding protocol) was set in the range [0, 255].

It should also be noted that the experiments conducted under different communication schemes (the same and different network nodes) showed absolutely identical results regarding the specific number of errors. The difference was only in the speed of movement of requests and responses, but this was not among the characteristics under investigation. The data in Table 1 correspond to all schemes of experiments.

The specific number of authorization errors *p* with differences in password data better characterizes the protocol, the greater its value. Accordingly, preference should be given to those data from the table for which the maximum *p* is observed.

Table 1

Specific number of authorization errors (p) of the client-server authentication protocol using monochrome (M) and color (K) fractals with different password data on the client and server

No.	Server: C_0, N	Client: C_0, N	p, %	
			M	K
1	(0, 1), 2	(0, 1.001), 2	<0.01	2
		(0.001, 1), 2	<0.01	2
2	(0.37, 0.37), 2	(0.3701, 0.37), 2	0.02	14
		(0.37, 0.3701), 2	0.04	17
		(0.37001, 0.37), 2	0.04	7
		(0.37, 0.37001), 2	0.04	8
3	(0.25, 0.25), 2	(0.2501, 0.25), 2	0.02	0.2
		(0.25, 0.2501), 2	0.02	0.2
4	(0.24493, 0.69915), 5	(0.24494, 0.69915), 5	12	33
		(0.24493, 0.69916), 5	14	34
5	(0.532, 0.419), 4	(0.53201, 0.419), 4	0.01	15
		(0.532, 0.41901), 4	0.01	14
6	(0.24493, 0.69915), 5 range of random numbers [0,1/3]	(0.24494, 0.69915), 5	27	75
		(0.24493, 0.69916), 5	27	76
7	(0.532, 0.419), 4 range of random numbers [0.1/3]	(0.53201, 0.419), 4	0.03	22
		(0.532, 0.41901), 4	0.03	24
8	(0.24493, 0.69915), 5 range of random numbers [0.1/4]	(0.24494, 0.69915), 5	26	84
		(0.24493, 0.69916), 5	32	84
9	(0.532, 0.419), 4 range of random numbers [0.1/4]	(0.53201, 0.419), 4	0.03	28
		(0.532, 0.41901), 4	0.03	28

From analysis of the data in Table 1, the following conclusions can be drawn.

Color fractals show significantly better performance (p_K) than monochrome ones (p_M). The difference is determined by the ratio (p_K/p_M) from about 3 times (for rows of Tables 4, 6, 8) to about 1000 (for rows 5, 9).

The higher the power of conversion (2), the better the indicators that protocol demonstrates. The average values of errors in a series of powers N=2, 4, and 5 (throughout the table) are 5, 17, and 65, respectively. At the same time, for N=5, the average error probability exceeds 0.5 (specific value – 50 %), which makes this option the first better than the random bit generator. It can be argued that the choice of power N=5 is optimal as a balance between the number of calculations of a polynomial of power N and the reliability of the protocol it provides.

Limiting the area to the central part of the fractal also shows better performance. Thus, in a series with a space reduction factor of 1, 1/3, 1/4 at N=5 and the constancy of the rest of the parameters (lines 4, 6, 8 of the table), p runs through values of 33, 75, 84, respectively. Similarly, for N=4, it is 14, 23, 28 (rows 5, 7, 9, respectively). This proves greater sensitivity to changes in the parameters of the central part of the fractals, and the improvement in the given series is no less than 2 times.

From the received data on the specific number of errors, it is possible to calculate the probability of success of an attack on a common protocol. A numerical estimate of the probability of a privacy attack can be represented by the formula for the probability of independent events:

$$P_R = (1-p)^R, \qquad (5)$$

where R is the number of repeated authorization rounds, p is the probability of authorization rejection, the value of which corresponds to the frequency of errors indicated in Table 1. Expression (1–p) corresponds to the probability of a successful attack for one round of authentication. Assuming constant password data used for all rounds, this probability will characterize each round, remaining constant and forming the end result (5).

The inverse problem of determining the number of authentication rounds will have a solution in the form of:

$$R = \log_{1-p} P_R = \frac{\ln P_R}{\ln(1-p)}. \qquad (6)$$

Table 2 gives results from calculating the number of authorization rounds R required to achieve a typical value of the probability of a successful authentication attack at the P_R=2^{-128} level, depending on the probability of a single authorization error p.

Table 2

Number of authorization rounds R with the probability of errors p

p	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
R	843	398	249	174	128	97	74	56	39

From the analysis of the results in Table 2, a number of conclusions can also be drawn.

Changes in the number of rounds are non-linear. Although it is obvious from formula (5), the table makes it possible to give a numerical estimate. On the range [0.1, 0.9], when the error probability changes by 9 times, the number of rounds changes by almost 22 times (inversely proportional). This indicates the expediency of measures to influence the frequency of single errors in comparison with an increase in the number of rounds.

For better estimates of the values of the specific errors given in Table 1 (about 70–80 %) the number of rounds can be estimated in the range of 56–74. The gain in the number of repetitions compared to the random bit generator (probability 0.5, number of rounds 128) will be about 2 times. This also proves the greater efficiency of algorithms with fractal sets.

The findings inform further research on increasing the probability of error for a single round of the protocol. In particular, this can be achieved by choosing the power of fractal transformation, the dimensionality of the fractal set, the localization of the random coordinates generation area, as well as the depth of the color information of fractal points.

5. 4. Estimating the time complexity of the algorithm

In order to assess the possibility of implementing the developed algorithms in standard devices (personal computers, smartphones, tablets, etc.), I shall calculate their computational complexity. For better safety indicators, from Table 1 (row No. 8), the percentage of errors with colored fractals is 84 %, which corresponds to p=0.84. The number of authorization rounds R needed to ensure this probability was determined from formula (6). For practical use, the result was rounded to a larger integer:

$$R = \frac{\ln 2^{-128}}{\ln(1-0.84)} = 48.41 \approx 49.$$

The resulting value R=49 makes it possible to estimate the average number of iterations of sequence (1) at the level N_c=128. This corresponds to half of the built-in color limit of 255 different values. At each iteration, $2N(N+1)$ multiplication operations are performed (expansion of binomial power N in complex space). Accordingly, for N=5, which corresponds to the selected fractal, the total number of multiplication operations for the entire authorization protocol will be $2RN_cN(N+1)$=376320. At a typical computer speed of 1 GFLOPS (10^9 floating-point operations per second), the time spent on the authorization protocol will be approximately 0.38 ms.

The following factors may affect the assessment. Interpreted languages such as JavaScript, typical of browsers, may not fully utilize the computing power of the processor. This will overestimate the time. On the other hand, most modern computers are faster than 1 GFLOPS. This factor, on the contrary, will reduce the time estimate. Limiting oneself to the fact that it is enough to note the order of magnitude for the evaluation, one can round off the given numerical value to 1 ms. At the same time, one can be guided by the fact that this is an upper estimate of the time and the real values of the execution time of the algorithm would be somewhat less than the given value.

6. Discussion of results regarding the optimality of fractal parameters

Having chosen the security service "confidentiality during exchange" as the main characteristic of the protocol, it should be noted that the overall evaluation of the protocol will be the better, the more authentication errors will occur with small deviations of password data among exchange participants. In other words, if the password (password parameters) are selected, but not with absolute accuracy, then this will lead to the fact that some point color calculations will coincide, even with different parameters. The reason for this is the limited number of iterations of expression (2) and the finite set of values for the point color. But some points will show differences in results. And the more such points there are at random selection of their coordinates, the better one shall consider the fractal transformation (2) for the given problem.

From the analysis of results summarized in Tables 1, 2, a number of statements can be made. Owing to the introduction of color information into fractals, the protocols began to demonstrate better reliability indicators, compared to monochrome ones. The ratio of the number of rejected requests varies from about 3 (with high error probabilities) to 1000 (with small ones) in favor of color schemes. Accordingly, the implementation of protocols on monochrome fractals is not recommended if there are no fundamental restrictions for the implementation of color ones.

As expected, fractals with a marginal dimensionality close to 1 (No. 1 in Table 1, Fig. 2, *a*) and close to 2 (No. 3 in Table 1, Fig. 2, *c*) demonstrate worse reliability indicators than fractals with an intermediate dimensionality – close to 1.6. This testifies to the expediency of preliminary analysis of password data for the corresponding Hausdorff dimensionality of the fractal image. Using randomly generated password data without additional verification is not recommended.

Fractals with intermediate dimensionalities correspond to the limit points of the Mandelbrot set. When moving away from its boundary, the fractals "thin out" and lose large values for colors (the divergence of the sequence (2) is observed at small k). As a result, the monochrome image of the fractal becomes inconspicuous since all colors smaller than the threshold are considered "white". This corresponds to a significant loss of protocol reliability when switching to monochrome mode (No. 5 in Table 1). This additionally proves the advantages of color schemes and the need for preliminary analysis of password data for reliability indicators.

Limiting the range of random coordinates of a point in the fractal space in order to use only the central part of the fractal improves reliability indicators by 1.5–2.5 times (series No. 4-6-8 and No. 5-7-9 in Table 1). For practical use, the specified limitation should be applied.

The value of the power of fractal transformation (2) also affects the quality indicators of the protocol. The higher the power, the more sensitive the z_k sequence is to password data changes and the better the reliability of the protocol. This conclusion can be confirmed by evaluating the binomial expansion $(1+x)^N \approx 1+Nx$ for small x. In this case, x is responsible for the deviation of the password parameters, and the estimate shows an approximately linear dependence of the sensitivity to changes on the power of the polynomial.

Individual values of the specific number of authorization errors are greater than that of the random bit generator with a probability of 0.5 (No. 6 and No. 8 in Table 1). This indicates better security properties of the protocol than the one with an ideal source of random binary sequence. The specified frequencies are observed for transformations with power N=5, for smaller degrees the indicators are worse. This observation makes it possible to formulate a recommendation for the use of transformations of type (2) with powers not less than 5.

At the same time, the evaluation of the protocol's operating time with the specified parameters for a typical performer (at a level of no more than 1 ms) allows me to assert that it is sufficiently effective. This time is comparable to the typical client-server connection establishment time (triple handshake) of 1 ms, that is, it will not affect the noticeable increase in the time of information exchange. For full-fledged computers and, even more so, servers, the time estimation result can be reduced by 2–3 orders of magnitude, which significantly strengthens the conclusion.

It should be noted that the above calculations of computational complexity were carried out under the condition of deviation of the password data in the fifth digit for one of the components of a complex number when the parameters (power) of the iterative transformation (1) match. For a situation with a worse initial approximation, the reliability measures will show better results.

However, it is possible to point out certain shortcomings of the developed implementation of the algorithm. It uses basic representations of fractional numbers with a dimensionality of 64 bits. This is quite sufficient for human user authorization tasks but may not be enough for fully automated work. The mathematical statement of the algorithm does not contain restrictions, which allows the use of numbers of arbitrary size. However, there were no practical tests for them.

As prospects for further research, it is possible to indicate its practical adaptation to work with numbers of increased dimensionality (more than 64 bits). This could significantly increase the set of password parameters and make the protocol cryptographically reliable. Studies of various polynomials (2) with different powers and coefficients are also considered promising. Potentially, this could produce practical sets of best parameters or algorithms for generating them.

7. Conclusions

1. Authentication protocols with zero-knowledge have been successfully tested using algebraic fractal sets in their composition. An authentication algorithm based on polynomial fractal transformation has been proposed and implemented. It is shown that sufficient safety indicators are achieved for polynomials of power 4–5. At power 5, the indicators exceed the random bit generator. It is recommended to use asymmetric transformation formulas with a choice for practical use of the central part of the fractal with a power of polynomial not lower than 5.

2. Taking into account color information makes it possible to improve the reliability of protocols by at least 3 times compared to monochrome ones. The use of the latter is appropriate only if it is impossible to transmit color data as part of the protocol. Nevertheless, achieving high reliability of protocols requires preliminary testing of password parameters. It is highly not recommended to choose them at random. The greatest reliability is demonstrated by fractals belonging to the boundary points of the Mandelbrot set with a Hausdorff dimensionality close to 1.6.

3. It has been confirmed that the infinite detailing of the fractal set structure allows password data to be used for a long time without updating. The revealed high sensitivity to changes in password parameters, as well as their variable number, provide high reliability indicators against intrusion attacks. Reliability can be set at an arbitrary level; this is achieved by repeating the algorithm several times.

4. The estimated time complexity of the implemented algorithm with the limitation of the probability of an intrusion attack at the level of 2^{-128} does not exceed the value of 1 ms for the speed inherent in typical mobile devices and is comparable to the time of establishing a client-server connection using the HTTP protocol. This indicates the insignificant impact of the protocol on the total time of the communication session and the possibility of its free practical implementation in the form of an independent additional module.

Conflicts of interest

The author declares that he has no conflicts of interest in relation to the current study, including financial, personal, authorship, or any other, that could affect the study, as well as the results reported in this paper.

Funding

The study was conducted without financial support.

Data availability

All data are available, either in numerical or graphical form, in the main text of the manuscript.

Use of artificial intelligence

The author confirms that he did not use artificial intelligence technologies when creating the current work.

The images were built by authentic algorithms, without AI involvement.

References

1. Nail, B., Atoussi, M. A., Saadi, S., Tibermacine, I. E., Napoli, C. (2024). Real-Time Synchronisation of Multiple Fractional-Order Chaotic Systems: An Application Study in Secure Communication. Fractal and Fractional, 8 (2), 104. https://doi.org/10.3390/fractalfract8020104
2. Adeyemi, V.-A., Tlelo-Cuautle, E., Sandoval-Ibarra, Y., Nuñez-Perez, J.-C. (2023). FPGA Implementation of Parameter-Switching Scheme to Stabilize Chaos in Fractional Spherical Systems and Usage in Secure Image Transmission. Fractal and Fractional, 7 (6), 440. https://doi.org/10.3390/fractalfract7060440
3. Jansen, B. H. (2000). Nonlinear methods for evoked potential analysis and modeling. Chaos in Brain?, 173–193. https://doi.org/10.1142/9789812793782_0014
4. Bildirici, M. E., Ersin, Ö. Ö., Uçan, Y. (2024). Bitcoin, Fintech, Energy Consumption, and Environmental Pollution Nexus: Chaotic Dynamics with Threshold Effects in Tail Dependence, Contagion, and Causality. Fractal and Fractional, 8 (9), 540. https://doi.org/10.3390/fractalfract8090540
5. Sulaiman, A. H., Baji, F. S. (2009). Fractal Based Fragile Watermark. 2009 Second International Conference on Computer and Electrical Engineering, 1, 139–143. https://doi.org/10.1109/iccee.2009.35
6. Lock, A. J. J., Loh, C. H., Juhari, S. H., Samsudin, A. (2010). Compression-Encryption Based on Fractal Geometric. 2010 Second International Conference on Computer Research and Development, 3, 213–217. https://doi.org/10.1109/iccrd.2010.40
7. Samoilenko, D. N. (2014). Authentication scheme on fractal sets. Ukrainian Information Security Research Journal, 16 (1). https://doi.org/10.18372/2410-7840.16.5396
8. Schneier, B. (1996). Applied Cryptography. Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 784. Available at: https://www.schneier.com/books/applied-cryptography/
9. Giani, A. (2001). Identification with Zero Knowledge Protocols. SANS Institute. Available at: https://www.sans.org/reading-room/whitepapers/vpns/identification-zero-knowledge-protocols-719
10. Gerardo, I. (2002). A Primer on Zero Knowledge Protocols. Universidad Nacional del Sur. Available at: http://cs.uns.edu.ar/~gis/publications/zkp-simari2002.pdf
11. Feder, J. (1988). Fractals. Springer New York, 284. https://doi.org/10.1007/978-1-4899-2124-6