DOI: 10.2507/31th.daaam.proceedings.085

UTILIZATION OF FRACTAL GEOMETRY POSSIBILITIES FOR INFORMATION SYSTEMS SECURITY

Marta Blahová, Michaela Mikuličová & Martin Hromada

This Publication has to be referred as: Blahova, M[arta]; Mikulicova, M[ichaela] & Hromada, M[artin] (2020). Utilization of Fractal Geometry Possibilities for Information Systems Security, Proceedings of the 31st DAAAM International Symposium, pp.0619-0625, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-29-7, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/31st.daaam.proceedings.085

Abstract

This article deals with the use of the principles of fractal geometry applicable in the field of cryptographic security of communication within information systems. The theory of the proposed solution is based on the field of iterative fractals created using the TEA (Time Escape Algorithm) algorithm. The acquired knowledge proved the usability of the proposed solution for the selected area of its use. Aim of this research is to design a suitable design for a diagnostic device that will periodically monitor and record selected quantities in the device. The diagnostic equipment must be as flexible as possible, as the design will be applicable to all output electronic equipment of this project. This means that the diagnostic design can be applied to all control units, add-on modules or turnstile controllers. Each checked element contains different quantities that are valid for correct diagnostics. Therefore, there is a desire for a uniform design that can be customized based on the device. The main benefit is finding a way to secure data against unwanted retrieval of its content. The involvement of the branch of fractal geometry in the field of information security opens up new possibilities, given the different conception of fractals, in contrast to the objects of classical Euclidean or other geometry. The proposed system works with complex fractal structures, which can be described by relatively trivial equations, which allows using this system with high speed both for encoding the message and for its retrospective reconstruction. This fact opens the way to the use of the proposed system for information security even in devices with limited computing capacity. The system emphasizes resistance to cryptanalytic methods, such as brute force attack, statistical methods, or analytical methods. The objectives are summarized in the following points: Find a suitable category of fractals, usable in the field of information systems security, Design and verify a method suitable for fractal information security, Determine the resistance of the proposed solution to cryptanalytic methods.

Keywords: Fractals; fractal geometry; cryptography; encryption; encrypted information.

1. Introduction

Fractal geometry examines objects called fractals. Her presence in the field of serious science dates back to the 1970s, when a mathematician, Bernoit Mandelbrot, defined the term fractal, from the Latin word fractus, or broken. However, the first tremors of what we call fractals today arose earlier. As early as the 19th century, mathematics at the time found strange patterns and structures of a fractal character, but they were not given sufficient attention.

There is still no mathematical definition of a fractal. The definition of a fractal is best approached by Mandelbrot's statement, which defines a fractal as such a formation whose Hausdorf dimension is larger than the topological dimension [1]. Fractal objects do not only exist in the world of mathematics. Fractal structures can be found in the surrounding world, for example in the form of clouds, trees, leaves, rocks, terrain, and many other natural objects.The principles of fractal geometry enable its use especially in the areas of compression algorithms, artware, studies of dynamic systems, modeling of chemical and physical processes, or in the field of security technologies. Ensuring the security of the information transmitted from the sender to the recipient and trying to prevent the unwanted person from obtaining the confidential content they carry has been a task that has accompanied man since ancient times. With the development of human knowledge and technical progress, encryption methods are gradually being improved and replaced by new ones that meet the demands and requirements of security at the time of their deployment [1].

At the time of the expansion of computer technology, the development of cryptography is growing to unprecedented proportions. It is no longer just an instrument of statesmen, spies, and a small circle of interested people who used it in the past, but it is now becoming a common tool of a man of our time. There are many ways to protect information from unwanted third-party eyesight [1]. The article proposes and processes a method of encrypting information based on the principles of fractal geometry, specifically on one of their groups - iterative fractals created using the TEA(Time Escape Algorithm) algorithm. Fractal geometry extends in its scope to many fields of human activity. In this case, this relatively young scientific discipline lends its potential in the field of information security. The introductory part of the article describes the area of the problem, sets out the goals, and then the methods of securing information used at present [2].

One of the chapters deals with the principles of fractal geometry and further analyzes the individual groups of fractals according to the method of their construction. The next section describes the process of securing information using an iterative fractal created using the TEA (Time Escape Algorithm) algorithm. Following these points, processes extending the proposed algorithm to encrypt long messages are described and the proposed process of using a unique key, which increases the resistance of the proposed solution to cryptanalytic methods, is described.

The next part of the article describes the solution to the problem of generating a suitable fractal structure for individual types of fractals. Following the next section, variants of encryption and decryption processes are demonstrated and their properties and parameters are described. The knowledge gained by cryptanalysis of the proposed solution and formulates the basis for determining its resistance to cryptanalytic methods. Furthermore, the article deals with the description of the programmed interface in C # language used to demonstrate encryption and decryption processes and test the proposed solution. Furthermore, the hardware and software resources used in the research are summarized here. In the final part of the article are the possibilities of using the acquired knowledge for science and practice [2].

2. Cryptography

Today, computer networks and the Internet are being set up, where transmission channels of information are transmitted from the sender to the recipient. This raises the need to protect this information from eavesdropping. Other interception techniques do not hide much complexity and the attack on the information does not represent a large financial means. Currently, two basic types of cryptographic methods are widespread for information security [3].

The first is Symmetric cryptography, the second Asymmetric cryptography. Every one who causes their pros and cons is deployed where its strength is available. We come across their combinations, which they call hybrid cryptography. The advantages of symmetric cryptography, are in its speed compared to asymmetric. Significant computing speed is not required for its deployment. The same key is used to encrypt and decrypt the message. Before initiating communication, the sending and receiving parties must agree on a common key [3].

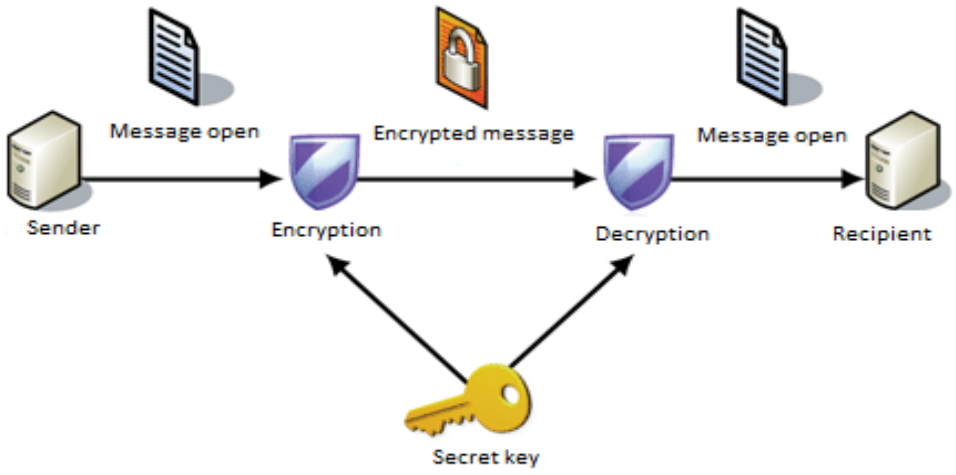

Fig. 1. Symmetric cryptography

Asymmetric encryption, is characterized by different keys for encrypting and decrypting the message. The so-called public key is used to encrypt the message, and the private key is used to decrypt it. The user's public key is known to each participant in the communication. The private key is unique for each participant. Encryption is done by the sender encrypting the message with the recipient's public key. The recipient receives the message, uses his private key, and reads the message. During the key pairing process, the rule of non-derivation of a private key from a public key applies [3].

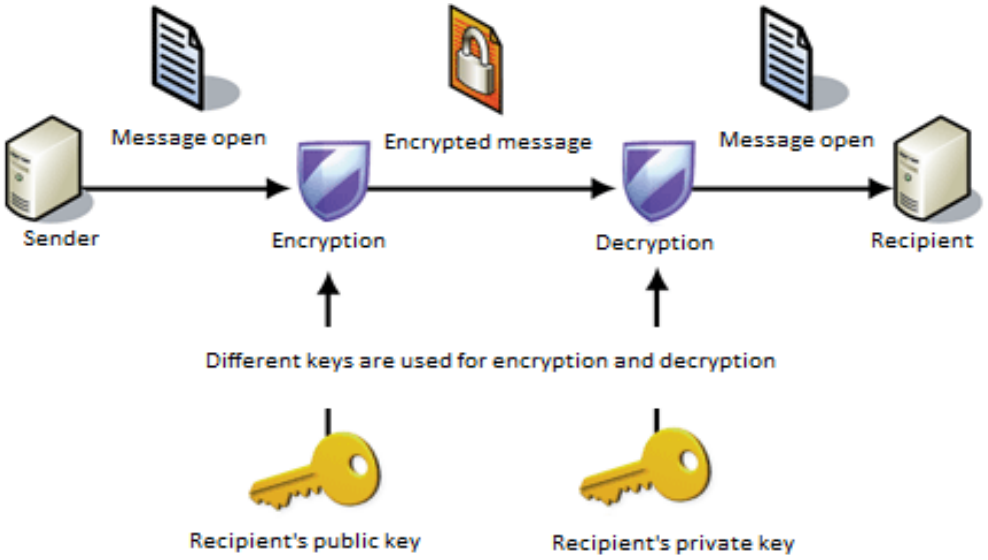

Fig. 2. Asymmetric cryptography

Hybrid encryption takes advantage of both of the above encryption methods. It takes over from symmetric encryption, from asymmetric usability and the existence of key pairs. The cryptographic cycle takes place by encrypting the message with a symmetric key, the symmetric key is then encrypted with the recipient's public key and is sent with the message. The recipient receives the message, uses the private key to find the symmetric key, and uses it to decrypt the message [4].

3. Fractal geometry

Fractal geometry examines objects called fractals. The principles of fractal geometry enable its use especially in the areas of compression algorithms, hardware, the study of dynamic systems, modeling of chemical and physical processes, or in the field of security technologies [4].

The group of fractals created using the TEA algorithm is one of the most widespread. The corresponding fractal of this group is defined by its equation and initial conditions. The equation is performed iteratively according to the set conditions. The conditions can be interrelated and the process of generating a fractal thus depends on their mutual combinations. One of the cases may be, for example, the determination of a given number of iterations and at the same time the value of the relevant parameter of the equation, which must not be exceeded. Parameters that figured in solving targets in this group of fractals, a point on a surface or in space is investigated. At the end of the process, the relevant point is drawn in a shade proportional to the number of iterations performed that had to be performed to leave the selected boundary. The best-known representatives of fractals where the TEA algorithm can be used include Julius sets, Mandelbrot sets, and fractals based on it [5].

4. The process of using the points of a fractal structure to encrypt information

The research of fractal geometry directed the progress in the work to the area of using the category of fractals created using the TEA algorithm. These fractals, as it turned out, allowed their principles to be applied to the solution of goals [6]. The process begins with the generation of one of the fractals by the TEA algorithm. The process of generating a fractal takes place on the basis of predetermined conditions related to both the design properties of the fractal and the purpose of using the output fractal structure. After the fractal generation operation, the message encryption process can be started. The visualized points that represent the generated fractal have different shades of color. Each shade of color is represented by a number. This number represents the number of iterations performed by the algorithm when calculating a given point of a fractal set. For each point drawn in this way, we know information about its x-coordinate, about they-coordinate, and information about the hue. Based on these values, we can encode the message into a so-called vector. This vector can be stored or securely transferred via an insecure channel to the recipient.

The message encoding process is performed so that the hue number defines the value of the character. Letters can be understood as letters, numbers, and other special characters [6]. Thus, it can be said that, as with other encryption mechanisms, the strength of encryption does not lie in not knowing what transformations were used, but in a wide range of possible solutions and therefore considerable computational complexity for decrypting and subsequent analysis of data structures. This principle describes the so-called Kerckhoff assumption. The entire encryption and decryption procedure described is shown in the block diagram in Figure 3.

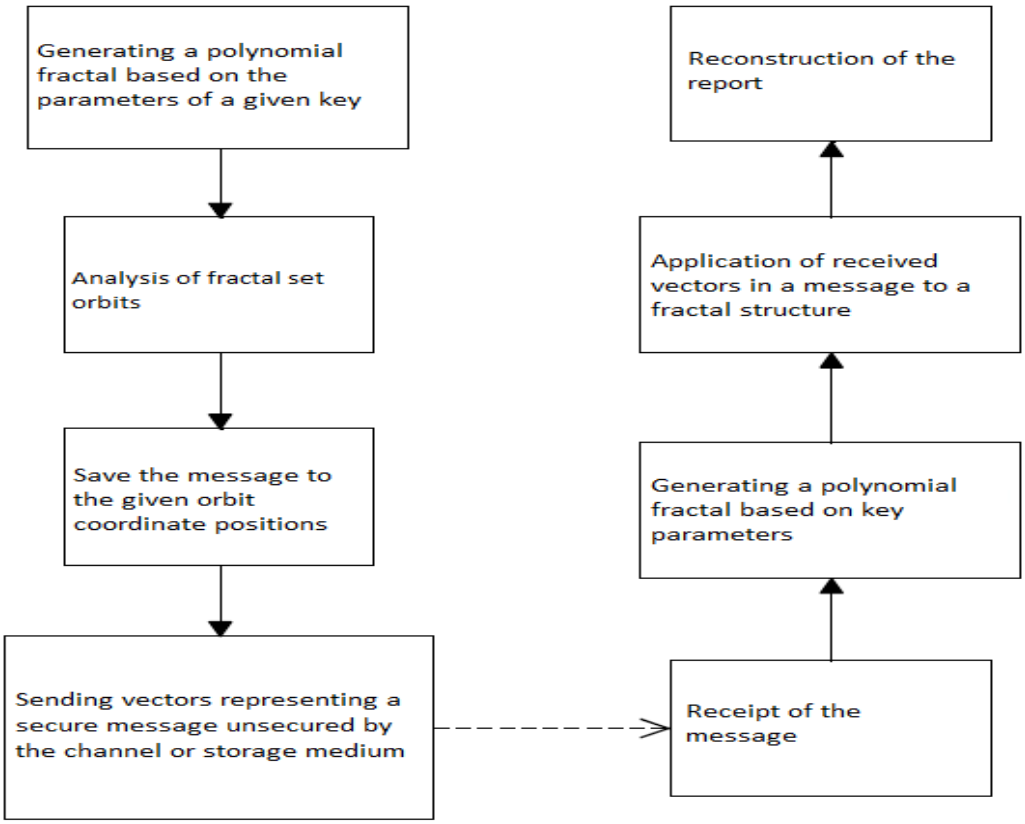

Fig. 3. Asymmetric cryptography

5. Description of the implemented algorithm for encrypting information

For the purposes of testing and development of the algorithm, a program was created in the development environment Microsoft Visual Studio 2010. The process of encrypting information based on the principles of fractal geometry consists of three consecutive operations. These operations were called: Fractal Generation, Fractal Analysis, and Information Encryption. Fractal generation was implemented in the test program manually and automatically. As part of the automatic fractal generation, detailed settings of the generating process were implemented [7].

There are two ways to manually generate a fractal. Using the mouse or entering its parameters in the appropriate text fields in the program. The second way is to enter the display center parameters x and y, Initial range, and Number of iterations. After pressing the generate button, a fractal structure with the given parameters will be generated. This procedure can be applied during the encryption process but is mainly used during decryption. It can be performed manually or automated [7].

6. Encrypting information

After the successful operation of fractal generation and analysis, the process of information encryption can be started. The input information is read from a text box on the tab called Encrypt Message, located on the main program window. From the generated fractal, the maximum possible length of the input information is calculated and the Index field is determined, which determines the points of the fractal structure, the future representatives of the used characters [8].

During the development of the writing method, the resistance to cryptanalytic methods was taken into account. The message is divided into individual characters. In each cycle, each character is processed separately. In the first phase, the character index is determined in the Input alphabet of characters field based on the currently processed character. Subsequently, a pair of numbers in the range of the Fractal field is generated. Because this field is two-dimensional, a pair of values must be generated. These values serve as indexes for its crawl.

If by this random generation a value corresponding to the index of a given letter in the Index field is found in the Fractal field and this cell is not used yet, this pair of generated values are recorded in the output vector [8]. This pair represents encrypted information. If these values are already used, the process is repeated until they are unique. This cycle runs for all characters of the input information. The process is terminated by processing the last character of the message [8].

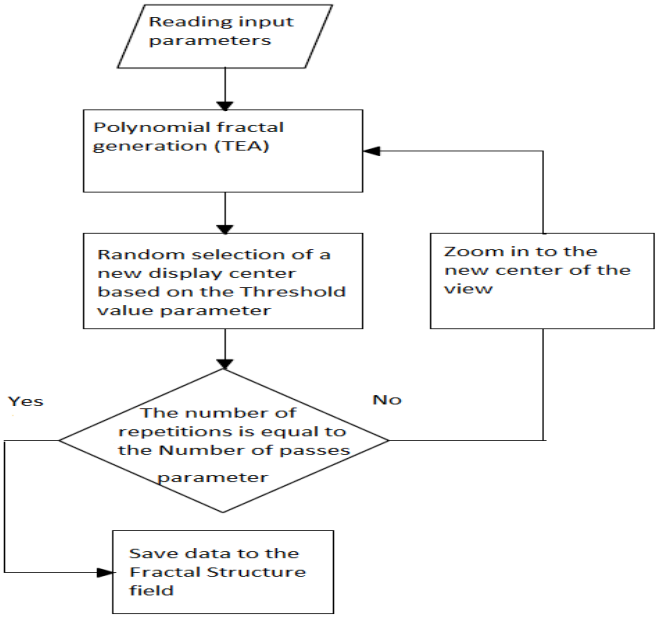

Fig. 4. The process of encrypting information

7. Description of the implemented algorithm for decrypting information

Fractal generation

Before the actual reconstruction of the encrypted message, it is necessary to first perform the process of generating a fractal, which was used to encrypt the information. Generation is done by a key. A fractal structure is generated using the parameters carried by the key [9].

Fractal analysis

Similar to the process of encrypting information, there is also the process of fractal analysis when decrypting information. The main reason for this step is to determine the frequency of iterations of the points of the fractal structure, stored in a two-dimensional Fractal field, and then to determine the maximum length of the decrypted message. This information is then used to map the Index Field and thus determine the point of the fractal structure that will represent the particular decrypted character. Information about the number and number of iterations of fractal structure points on a fractal is stored in a one-dimensional field called Frequency Field [10].

Decryption of information

After successfully performing the fractal generation and analysis operations, the step of reconstructing the encrypted information can be started. The encrypted message has the form of a vector of numbers, which contains coordinates pointing to specific points of the fractal structure. The fractal analysis performed in the previous step determined in the Index field which letter represents a particular value of a fractal structure point [11].

The vector containing the encrypted information is read sequentially and at the corresponding coordinates in the fractal, points with numbers corresponding to the value of the point of the fractal structure are found. This value is found in the Index field, and the index of this field corresponds to an encrypted character. This process is completed by processing the last character of the encrypted message. When finished, the decrypted information is displayed in the appropriate text box on the Decrypt Message tab in the main program interface [11].

8. The process of multiple generations when encrypting a message

The message encryption process itself begins with the generation of a key-based fractal. In the next step, the fractal structure is analyzed. The analysis primarily determines how many characters of open text a given fractal structure can hold. Based on the performed analysis, the next step determines whether the fractal parameters allow the encryption of the entire open text at once, or whether it will be necessary to use the method of multiple generations [12].

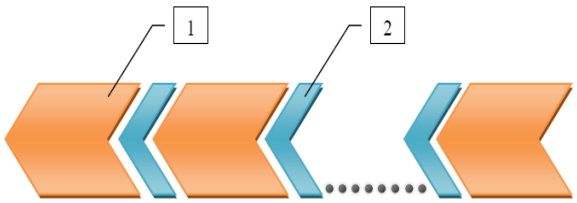

Fig. 5. Message scheme after performing the multiple generation process (1-data, 2-keys)

9. The process of applying a unique key when encrypting information

The use of a unique key process increases the security of the proposed information encryption algorithm using fractal geometry methods. The absence of this process would not make the algorithm unusable. The way the encryption system uses the same key for a long time is not uncommon. However, the implementation increases the resistance of the algorithm to cryptanalytic methods. The following paragraphs describe and compare ways to use a non-unique and unique key for a given algorithm [13].

10. Generating a fractal structure

Generating a fractal structure is one of the important steps in the process of encrypting and decrypting information. By suitable setting of the generator parameters, it is possible to achieve that the fragmentation of the fractal structure will be at a high level. The following subchapters document the research carried out in this area. The results were achieved using a test environment implemented in the interface of a program created to research the processes of generation, encryption, and decryption [14].

11. Comparison of individual fractal structures

Suitable parameters for generating fractal structures were determined. The values were determined after ten measurements. The obtained parameters are summarized. In Figure 6, these comparisons are made graphically. Blue characteristics indicate the alphanumeric character set, red numeric character set. The fractal resolution was 200 x 200 pixels for all types. Higher values significantly prolonged the generation process, using computer technology [15].

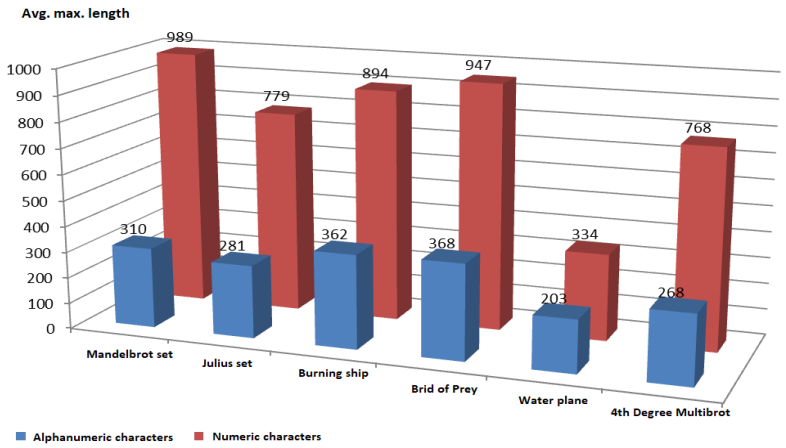

Fig. 6. Comparison of average max. Message lengths for individual fractals

12. Conclusion

The proposed method of encryption, based on the principles of fractal geometry, offers a wide range of possibilities for its application in the field of cryptographic security of communication inside and outside information systems. Research points to the possibility of using fractals in the field of cryptography. The encryption and decryption processes of a given algorithm can be used in human-human, human-machine, and machine-machine links. The human-to-human link can be used in situations where it is appropriate to ensure a high degree of confidentiality between the sender and recipient. The given process, implemented in the human-machine connection, includes securing the user's communication with the elements of the information systems with which he works. Based on embedded user requests, these systems provide the required output, process requests for further use, or simply store the necessary data in a database.

Similarly, it is also in the machine-machine connection, where the proposed method ensures the security of mutual communication of elements of information systems, between which information of a confidential nature takes place. I see a possible area of use of the proposed solution in the environment of electronic banking systems, in communication applications with a high level of confidentiality, in public administration, private institutions, registration systems of persons and property, as well as in health information systems inpatient records, storage and archiving. laboratory results and patient diagnoses. The interface using the proposed solution can be implemented both in the field of desktop applications and in the future on mobile devices and further extend its use to various platforms. The first important step in the research was to ensure the generation of a fractal structure with suitable parameters for the message encryption process. The tests performed using the Fractal software determined the appropriate generator settings for the selected types of fractals. In the next part, a part devoted to the analysis of fractal structures was processed, the outputs of which are used to determine the maximum number of characters that can be encrypted using the structure. Based on this analysis, an encryption mode was determined, which is based on the length of the plaintext. In the case of a longer length of open text than the given fractal structure can process, it is encrypted by the Long Message mode, when additional fractal structures are generated to process all the open text. As shown by the performed tests, for the proposed purpose it is more advantageous from time-consuming to generate new fractals than, for example, to increase the resolution of the fractal beyond the selected parameters. Based on the ongoing cryptanalysis during development, the encryption method was extended by the so-called encryption with a unique key. It turned out that the implementation of this solution increased the security of the algorithm, especially against statistical methods of cryptanalysis.

The proposed solution was continuously, but also in the end subjected to cryptanalytic research. The purpose of the performed analyzes was to reveal and treat the weak points of the algorithm and to meet the expected requirements for its functionality and the meaning of the effort. The cryptanalysis was conducted from several perspectives based on different approaches to the problem. The resistance of the developed algorithm to cryptanalytic methods was proved here. The purpose was to find a way to cryptographically secure information, including the principles of a relatively young scientific discipline - fractal geometry. The topic for further research is in the involvement of artificial intelligence methods in the process of generating fractal structures with suitable parameters for encryption processes and further development of activities in the field of key distribution before the initial use of the proposed solution.

13. Acknowledgments

This research was based on the support of the Internal Grant Agency of Tomas Bata University in Zlín, the IGA / FAI / 2020/003 project and the Institute of Safety Engineering, Faculty of Applied Informatics.

14. References

[1] Champlain, J. J. (2003). Auditing Information systems. New York: John Wiley and sons, 430 s. ISBN 0-471-28117-4.
[2] Stinson, D. R. (2006). Cryptography: theoryand practice, Chapman and Hall/CRC, 593 s. ISBN 1584885084.
[3] Stallings, W. (2010). Cryptography and Network Security: Principles and Practice. USA: Prentice Hall, 719 s. ISBN: 9780136097044.
[4] Stamp, M. (2011). Information Security: Principles and Practice. John Wiley & Sons, 606 s. ISBN: 0470626399.
[5] Mandelbrot, B. B. (2004). Fractals and chaos: the Mandelbrot set and beyond. New York: Springer, 308 s. ISBN 0-387-20158-0.
[6] Piper, F. & Murphy, S. (2006). Cryptography - A Guide for Everyone. Prague, 157 pp. ISBN 80-7363-074-5.
[7] Kenan, K. (2006). Cryptography in the database: The last line of defense. USA: Michigan university, 277 s. ISBN: 0321320735.
[8] Kahate, A. (2011). Cryptography in the database. New York: Tata McGraw-Hill Education, 792 s. ISBN: 9780070648234.
[9] Feiů, T. & Sinkov, A. (2009). Elementary Cryptanalysis, USA: Michigan university, 2009. 226 s. ISBN: 9780883856475.
[10] Bunatová, P. (2006). Asymmetric cryptography [online], [cit. 2011-05-17]. Available on the World Wide Web: <http://volny.cz/tbu/asym_sifra.html>.
[11] Bunatová, P. (2006). Symmetric cryptography [online], [cit. 2011-05-17]. Available on the World Wide Web: <http://volny.cz/tbu/sym_sifra.html>.
[12] Zelinka, I. (2005). Applied Informatics, or, Introduction to fractal geometry, cellular automata. 2nd edition Zlín: Tomas Bata University - Faculty of Technology, 183 pp. ISBN: 8073182750.
[13] Mach, V., Adamek, M., Valouch, J. & Tomasek, P. (2018). Software Extension for Advanced Technology Zone. Proceedings of the 29th DAAAM International Symposium, 2018, DAAAM International, ISBN 978-3-902734-20-4, ISSN 1726-9679, Vienna, Austria DOI: 10.2507/29th.daaam.proceedings.105.
[14] Meyers, M. (2002). Certification Passport. 1. vyd. California: McGraw- Hill/Osborne, Inc., 2002. 425 s. ISBN 0-07-222578-5.
[15] Zelinka, I., Včelař, F. & Čandík, M. (2006). Fractal geometry principles and applications. 1st ed. Prague: BEN, 2006. 160 pp ISBN 80-7300-191-8.