International Journal of
Science and Engineering Investigations
vol. 10, issue 113, June 2021
Received on May 25, 2021
ISSN: 2251-8843

Development of a Model for Detecting Means of Covert Information Retrieval Using Topological Threat Identification

Asadi Hrebennikov[1], Serhii Laptiev[2], Tetiana Laptieva[3], Mykhailo Lutsenko[4], Anton Naumenko[5], German Shuklin[6]
[1,2,3,4,5,6]State University of Telecommunications, Kyiv, Ukraine
([1]g_as_b@ukr.net, [2]mordorec@i.ua, [3]tetiana1986@ukr.net, [4]mikhaillutsenko1@gmail.com, [5]lectorpcau@gmail.com, [6]mathacadem-kiev@ukr.net)

***Abstract*-**The article considers the model of detection of means of secret information retrieval using topological identification of threats. The partial task of developing a model for detecting means of covert information retrieval and identifying threats of information leakage has been solved. Using the results of application of the developed model and characteristics of fractal geometry, it is possible to divide any object of information activity into fractals - areas of self-similarity. The criteria by which these areas are determined is determined by the physical principles of operation of embedded devices. By setting the appropriate reference values of the corresponding parameters, you can determine the fractal dimensions through the Hearst index, and depending on the obtained dimension value, you can identify the type of embedded device that is hidden in the object of information activities. The peculiarity of the developed model is that in addition to the fractal dimension, in order to significantly increase the probability of detection of means of covert retrieval of information, it is necessary to introduce appropriate fractal measures as identification. This additionally allows you to identify areas covered by dangerous signals.

Keywords*-Signal, Fractal, Distribution Density, Threat, Identification, Fractal Dimension, Information Leakage Channel*

I. Introduction

Mankind has entered an era of information value. At the same time, information becomes a more important resource than material or energy resources, so gaining access to information, especially information that is confidential and contains the main competitive advantages, is a priority of competition. Obtaining such information is usually associated with a violation of the law and the use of special technical means of secretly obtaining information. It is now possible to solve complex information leakage problems at a faster pace, but technical intelligence professionals can use new ways to infiltrate your system in order to steal valuable information and cause irreparable damage. The quality of the information used allows to obtain the corresponding economic or moral effect. According to analysts, 76% of international companies and government agencies have faced industrial intelligence. With the help of technical means 80-90% of the necessary information is extracted. In this regard, the secrecy of commercially important information allows us to compete successfully in the market of production and sale of goods and services. In accordance with the goal set for the seeker of confidential information from the object of information activities, the appropriate channel of information leakage is used. There are many models that make it possible to identify individual channels through which confidential information is leaked. This requires certain actions aimed at protecting confidential information. Therefore, the construction of a mathematical model by which it would be possible to identify the channel of leakage of confidential information on the object of information activities is very relevant today.

Setting objectives. The main tasks of information protection at the objects of information activity are the identification of threats of information leakage and detection of means of covert receipt of information. Various methods and models of identification are used for this purpose. There are currently many different methods of identification, but there is currently no universal model for detecting information leakage channels. Therefore, the development of models for the identification of threats and the detection of secret means of obtaining information for the objects of information activities is relevant today.

II. ANALYSIS OF LITERARY SOURCES

A significant number of publications are devoted to the issues of information protection, development of models for detecting information leakage channels and means of secret information retrieval. Thus, in [1] different methods of biometric identification by their characteristics and which are divided into two groups, namely static and dynamic. These methods are based on the physiological characteristics of man. On the basis of these features it is possible to build various mathematical models of identification which can be applied at creation of various technologies of protection of the information with limited access.

In [2] defines a tuple of parameters for the identification of cyberattacks on information systems, which makes it possible to increase the level of information protection, but they are defined only for a narrow class of objects for which it is necessary. Therefore, the problem is not fully solved.

In [3] the peculiarities of identification in corporate information and telecommunication systems are revealed. Modern means of identification are considered. However, no mathematical model has been proposed that can be used to create threat detection technology.

In [4] the technological solution for identification of objects of information activity at creation of technical systems of protection is offered. However, this solution is not specific to every system, most systems remain outside the developed method.

In [5], the fractal dimension method is used for identification only for optical systems. Which significantly reduces the list of systems in which it is possible to use fractal analysis. Therefore, the development of fractal theory requires further dissemination, dissemination to various systems and objects of information activities.

There are many models that make it possible to identify individual channels through which confidential information is leaked, but there is currently no universal model by which information leakage can be detected.

Based on the above, the development of models for identifying threats and identifying means of covert retrieval of information for objects of information activities is relevant.

The purpose of this article is to develop a mathematical model for detecting means of covert retrieval of information through topological identification of threats to the object of information activities.

III. PRESENTING OF THE MAIN MATERIAL

When studying the objects of information activities for the presence of embedded devices, there is a need to divide the room into zones in which most likely concentrated the device of covert removal of information. Modern topological analysis is used in the implementation of various topological effects associated with the analysis of audio information, image analysis [4]. When studying geometric objects in many cases there is a task to find out how geometric images are related. In other words, it is necessary to understand whether it is possible to obtain another from one geometric image. The branch of mathematics that studies these questions is fractal theory, part of which is the topology of the system.

Since a fractal is a geometric figure that has the property of self-identity, the study of dimension *D* of this object can be used when searching for embedded devices on the object of information activities. This is due to the fact that signals and fields have features of fractal structure. If the fractal dimension of the signal propagation region *D=1*, it means that the signal is continuously propagated through the wire without interference. If *D=2*, then the polarized signal propagates in the flat region and at *D=3* the signal propagates in three-dimensional space. In other words, the fractal dimension gives an accurate description of the signal propagation.

However, in the presence of interference, the area of signal propagation cannot be considered as continuous and in this case there are special zones in which the signal is not propagated. In these cases, the fractal dimension already takes a fractional value. Therefore, depending on the area of signal propagation, the fractal dimension of this area can generally be written as follows

$$D = k - H\ , \qquad k = \overline{1,3} \tag{1}$$

where *H* is the Hirst index. The Hirst index is determined as follows.

Let $\{\Delta_i, i = 1,..,n\}$ be a sequence of levels of thresholds for exceeding the signals from the copy file (previously removed radio signal file), which are determined in the room, which is examined for the presence of embedded devices. Picture 1 shows schematically how the threshold of excess is determined.

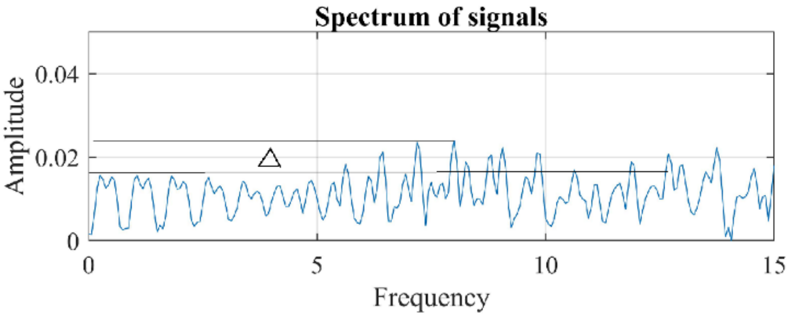

Figure 1. Determination of thresholds for exceeding a given threshold signal amplitude

Figure 1 shows that to detect the presence of the embedded device, the threshold amplitude A_n is set and in a given frequency range from f_1 to f_2 using a scanning device determines the i -th amplitude of the signal that is available on the OIA. Then,

$$\Delta_i = A_i - A_n$$

Let R be the range between the maximum and minimum values of these thresholds. Then

$$R = \max \Delta_i - \min \Delta_i \tag{2}$$

In this case, the average value of the threshold Δ is defined as the arithmetic mean of all threshold values, i.e.

$$\Delta = \frac{1}{n} \sum_{i=1}^{n} \Delta_i \tag{3}$$

and the standard deviation has the form

$$\sigma = \sqrt{\frac{1}{n} \sum_{i=1}^{n} \Delta_i^2 - \Delta^2} \tag{4}$$

Then, taking into account (2) - (4), the Hirst index will be determined as follows

$$H = \frac{\ln\left(\frac{R}{\sigma}\right)}{\ln\left(\frac{n}{2}\right)} \tag{5}$$

Substituting (5) into (1) we have three possible values of the fractal dimension, namely

$$D_1 = 1 - H, \; D_2 = 2 - H, \; D_3 = 3 - H. \tag{6}$$

When conducting research on OIA, it was found that if the fractal dimension has a value of $D_1 > 0.6$, it is likely that the OIA under study has a network embedded device.

If the fractal dimension takes the value of $1 < D_2 < 1.35$, then the OIA is capturing information using UHF pumping. The embedded device transmits the directional signal.

If the fractal dimension takes the value $D_3 > 2$, then the OIA is hidden digital means of obtaining information.

The developed model of detection of means of secret receipt of information by means of topological identification of threats which uses characteristics of fractal geometry allows to break any object of information activity into fractals - areas of self-similarity. Allows you to detect means of covert information with a high probability.

But the criterion by which these areas are determined is determined by the physical principles of operation of embedded devices. It depends on the intuition of a specialist who understands in which part of the object may be a particular type of means of obtaining information secretly. Therefore, the probability of detecting means of covert information also depends on the specialist.

A. Practical application of the developed model

In order to practically confirm the adequacy of the developed model, full-scale modeling was performed. DigScan software and hardware were used as a search tool for secret information retrieval in field modeling. As a threshold value was set, the value of the amplitude of 50 dB. The frequency range did not matter because we only needed to get a deviation from the threshold. That is, in full-scale modeling we were interested only in the deviation from the established threshold value. In a real search process, when searching and blocking means of secretly obtaining information, the threshold value is set for a specific object. In various methods, this value may be called a «sample file». In this file, the threshold will be different for different scan frequency values. Therefore, we will assume that in our case at a given frequency range, the threshold value of the amplitude will be 50 DB. Which is quite favorable. The scan results in the specified range are shown in table 1.

Using the data in table 1, we find that $\Delta_{\min} = -10$, $\Delta_{\max} = 3$ and according to (2) $R = 13$. Using formula (3) we have that $\Delta = -2{,}84$, then the standard deviation of the level of the threshold of excess according to formula (4) $\sigma = 3{,}3$ DB. Then, the Hirst index according to (5) is calculated as follows

$$H = \ln(3.94) / \ln(12.5) = 0.54$$

TABLE I. SCAN RESULTS IN THE SPECIFIED RANGE

i- sequence number of the signal amplitude	Δ_i in (DB)
1	-6
2	-6.5
3	-4
4	1
5	0,5
6	-2
7	-5
8	2
9	-4
10	-4,5
11	-8
12	-10
13	-5
14	-1.5
15	-3,5
16	-5
17	3
18	1
19	2
20	-1,5
21	-1
22	-4,5
23	-5
24	-6
25	-5,5

Then, the fractal dimensions are respectively $D_1 = 0.46$, $D_2 = 1.46$, $D_3 = 2.46$. The obtained values of fractal dimensions show that the largest region of propagation of the dangerous signal corresponds to the fractal dimension D_3, which in turn makes it possible to say that on OIA, the signal propagates in three-dimensional space, that with high probability it is possible to state existence of digital means of secret reception of the information on object of information activity.

IV. CONCLUSION

As a result of development of the model of detection of means of secret reception of the information by means of topological identification of threats the partial problem of protection of the information on objects of information activity is solved. This is the task of identifying threats of information leakage and identifying means of obtaining secret information.

Using the results of application of the developed model and characteristics of fractal geometry, it is possible to divide any object of information activity into fractals -areas of self-similarity.

The criteria by which these areas are determined is determined by the physical principles of operation of embedded devices. By setting the appropriate reference values of the corresponding parameters, you can determine the fractal dimensions through the Hearst index, and depending on the obtained dimension value, you can identify the type of embedded device that is hidden in the object of information activities. The peculiarity of the developed model is that in addition to the fractal dimension, in order to significantly increase the probability of detection of means of covert receipt of information, it is necessary to introduce appropriate fractal measures as identification. This additionally allows you to identify areas covered by dangerous signals. Which makes it possible not only to detect means of covert receipt of information, but also to determine the location of the means of receiving information.

REFERENCES

[1] Petro Bidiuk, Volodymyr Bondarchuk. Modern methods of biometric identification. Legal, regulatory and metrological support of the information protection system in Ukraine 1(18) issue, pp. 137-146, 2009.

[2] Andrii Hizun, Vladyslava Volianska, Viktoriia Ryndiuk, Serhii Hnatiuk. Basic parameters for identification of information security violator. Information protection. Volume 15, №1, January-March, pp. 66-74, 2013.

[3] V. Kozachok. Features of identification and authorization in modern corporate information and telecommunication systems. Modern information protection, №2 (30), pp. 42-48, 2017.

[4] Y. Kurskoi. Topological identification of optical systems. Radio engineering, Issue 196, pp. 51-54, 2019.

[5] S. Solomonova. Technological solution for identification of objects of information activity in the technical system of protection. Modern information protection, №1 (41), pp. 49-53, 2020.

[6] V. Pichkur, O. Kapustian, V. Sobchuk. Theory of dynamical systems. Tutorial. Lutsk: Vezha-Druk, 2020. - 348 p.

[7] Sobchuk V.V., Samoilenko A.M., Samoilenko V.G.On periodic solutions of the equation of a nonlinear oscillator with pulse influence. Ukrainian Mathematical Journal, 1999 (51), 6 Springer New York – pp. 926-933

[8] Sobchuk V. , Капустян О. Approximate Homogenized Synthesis for Distributed Optimal Control Problem with Superposition Type Cost Functional. Statistics Opt. Inform. Comput., Vol. 6, June 2018, pp 233–239.

[9] Sobchuk V. Oleg Barabash, Oleg Kopiika, Iryna Zamrii, Andrey Musienko. Fraktal and Differential Properties of the Inversor of Digits of Q_s -Representation of Real Number. Modern Mathematics and Mechanics: Fundamentals, Problems and Challenges, 2019. Springer. P. 79-95.

[10] Mashkov O.A., Sobchuk V.V., Barabash O.V., Dakhno N.B., Shevchenko H.V., Maisak T.V. Improvement of variational-gradient method in dynamical systems of automated control for integro-differential models. Mathematical Modeling and Computing, 2019, Vol. 6, No 2, pp. 344 – 357.

[11] Barabash, O., Lukova-Chuiko, N., Sobchuk, V., Musienko, A. Application of petri networks for support of functional stability of information systems. 2018 IEEE 1st International Conference on System Analysis and Intelligent Computing, SAIC 2018 – Proceedings, 2018, DOI: 10.1109/SAIC.2018.8516747

[12] O. Barabash, N. Dakhno, H. Shevchenko, V. Sobchuk. Integro-Differential Models of Decision Support Systems for Controlling Unmanned Aerial Vehicles on the Basis of Modified Gradient Method. IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC) – Ukraine, Kyiv, 16 October 2018. P. 94 – 97.

[13] Danchuk V. D., Svatko V.V. Optimization of the search for paths by graph in logistics problems by the method of a modified ant algorithm. Bulletin of the National Transport University. 2010. № 20. Page 109 – 114.

[14] Lukova-Chuyko N.V. Modeling of optimal information protection systems. Scientific and technical conference "Information Security of the State": Scientific reports of the participants of the scientific and technical conference, March 12-13, Kiev, Taras Shevchenko KNU, 2015. S. 119 - 120.

[15] Maksimenko G.A., Khoroshko V.A. Methods of detection, processing and identification of signals of radio display devices. K: Polygraph Consal-ting, 2004. 317 p.

[16] Samoilenko A. M., Perestyuk N. A. Differential equations with pulsed influence. K.: Visch., Shock. 1987. – 252 p.

[17] Laptiev O.A. Barabash O.V., Savchenko V.V., Savchenko V.A., Sobchuk V.V. The method of searching for digital means of illegal reception of information in information systems in the working range of Wi-Fi // International Journal of Advanced Research in Science, Engineering and Technology. India. Vol. 6, Issue 7 2019, ISSN: 2350-0328, P. 10101-10105

[18] Kolmogorov A.N. On the representation of continuous functions of several variables in the form of a superposition of continuous functions of one variable. Dokl. AN SSr-1957.-T.114, No. 5. Page 953-956.

[19] Samoylenko A.M., Samoylenko V. G., Sobchuk V. V. On periodic denouements of the equation of a nonlinear oscillator with impulse action. Ukr. mat. magazine.. 51, №6. 1999. S. 827 - 834.

[20] Petrov Y.P. How to obtain reliable systems of equations/Y.P. Petrov - SPb: BHV-Petersburg, 2009-176 p.

[21] Samoilenko V. G., Sobchuk V. V. Periodic denouements of the Lienar equation with impulse action. Nonlinear oscillations. T. 3, No. 2. 2000. Page. 256 – 265.

[22] Laptev A. A., Polovinkin I.M, Musienko A.P., D.V. Klyukovsky. Using the Prony method to analyze random radio monitoring signals //East European Scientific Journal, Poland, № 9 (49), 2019 part 3, P.41-46.

[23] Laptiev Oleksandr, Shuklin German, Savchenko Vitalii, Barabash Oleg, Musienko Andrii and Haidur Halyna, The Method of Hidden Transmitters Detection based on the Differential Transformation Model. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 8 No. 6 (November - December 2019) Scopus Indexed - ISSN 2278 – 3091

[24] Mashkov O.A., Sobchuk V.V., Barabash O.V., Dakhno N.B., Shevchenko H.V., Maisak T.V. Improvement of variational-gradient method in dynamical systems of automated control for integro-differential models. // Mathematical Modeling and Computing, 2019, Vol. 6, No 2, pp. 344 – 357.

[25] Barabash, O., Lukova-Chuiko, N., Sobchuk, V., Musienko, A. Application of petri networks for support of functional stability of information systems// 2018 IEEE 1st International Conference on

System Analysis and Intelligent Computing, SAIC 2018 – Proceedings, 2018, DOI: 10.1109/SAIC.2018.8516747

[26] O. Barabash, N. Dakhno, H. Shevchenko, V. Sobchuk. Integro-Differential Models of Decision Support Systems for Controlling Unmanned Aerial Vehicles on the Basis of Modified Gradient Method. // IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC) – Ukraine, Kyiv, 16 October 2018. P. 94 – 97.

[27] Danik Y. Synergistic effects of information and cybernetic interaction in civil aviation / Y. Danik, R. Hryschuk, S. Gnatyuk // Aviation. – 2016. – Vol. 20(3). – P. 137–144. (Scopus).

[28] Hryshchuk R. Verification Classifier Cyberattacks / R. Hryshchuk, V. Mamarev, V. Okhrimchuk, M. Kachniarz, I. Korobiichuk // Advanced Solutions in Diagnostics and Fault Tolerant Control : Spring-er International Publishing AG, 2017. – № 635. – P. 402–411. (Scopus)

[29] Stasiuk A.I. A mathematical model of cyber security computer network control in power supply of traction substations / A.I. Stasiuk, R.V. Hryshchuk, L.L. Goncharova // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 3. P. 170–179. (Scopus).

[30] Hryshchuk, R. The Throughput of Technical Channels as an Indicator of Protection Discrete Sources from Information Leakage / R. Hryshchuk, I. Korobiichuk, S. Ivanchenk, O. Roma, A. Golishevsky // Computer Modeling and Intelligent Systems – 2019. – Vol. 2353. p. 523–532. (Scopus).

How to Cite this Article:

Hrebennikov, A., Laptiev, S., Laptieva, T., Lutsenko, M., Naumenko, A. & Shuklin, G. (2021). Development of a Model for Detecting Means of Covert Information Retrieval Using Topological Threat Identification. International Journal of Science and Engineering Investigations (IJSEI), 10(113), 1-5. http://www.ijsei.com/papers/ijsei-1011321-01.pdf