International Journal of Engineering & Technology, 7 (3.13) (2018) 14-16

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Virtual Immediate Coding

V.V. Kotenko[1]*, A.I. Polyakov[2]

[1] *Southern Federal University, Rostov-on-Don, Russia, virtsecurity@mail.ru*
[2] *Southern Federal University, Rostov-on-Don, Russia, rp_rec@mail.ru*
**Corresponding author E-mail: virtsecurity@mail.ru*

Abstract

A distinctive feature of virtualization of noise-immune encoding is the realized possibility of complex solution of problems of noise immunity, protection against information intrusions and imitating resistance. This, with relatively low economic costs, will significantly expand the capabilities of telecommunications systems in terms of information security. The effectiveness of the complex solution of information protection tasks from the positions of virtualization of the noise-immune encoding processes is experimentally proved in the work. The effectiveness of protection from information intrusions provided by virtual noise-immune codes and the effect of virtualization on the efficiency of the original noise-immune code were experimentally investigated. The obtained results show that virtual noise-resistant coding provides the effectiveness of protection from information intrusions, comparable with the efficiency of modern standards of cryptographic protection, with significantly lower complexity of practical implementation. In general, the results of experimental studies show that the virtualization of the process of noise-immune encoding from the perspective of the approach proposed in [1] opens an additional possibility of protecting information in the part of ensuring information security.

Keywords: *information security, coding, noise immunity, encryption, virtualization, optimization, information flow, information security*.

1. Introduction

Creation of laser communication systems with spacecrafts The complex solution of the problems of noise immunity and information security in telecommunications from the standpoint of known approaches seems impossible in view of the antagonism of the strategic goals of information transformation: ensuring information security requires reducing redundancy, ensuring noise immunity - increasing redundancy. The possibility of solving the problem opens with the approach from the standpoint of the theory of virtualization, proposed in [1]. The purpose of the study is to develop and substantiate a strategy for the complex solution of information protection tasks from the point of view of virtualization of the processes of noise-immune coding.

2. Theoretical Justification

According to [1], the transfer of information from the source to the receiver can be represented as an information stream that initially represents the message flow $\mathrm{I}[\mathrm{X}]$ the form of which during the transfer is subject to change by branching out or adding new information flows. In this case, virtualization involves optimizing these flows relative to the set value Q by specifying virtualization conditions. With regard to noise-resistant encoding, the set of virtualization conditions is defined as:

Condition1. The form of the information flow is optimal for $\mathrm{I}\left[\mathrm{X}^{*};\mathrm{Y}^{*}\right]=\mathrm{Q}.$•

Condition2. Average conditional mutual information $\mathrm{I}[\mathrm{X}/\mathrm{Y}]$ unambiguously characterizes the direct transformation of the coding Φ of the ensemble elements X in the elements of the ensemble Y

Condition3. Average conditional mutual information $\mathrm{I}[\mathrm{X}/\mathrm{Y}]$ unambiguously characterizes the direct transformation of the coding Φ^{-1} of the ensemble elements X in the elements of the ensemble Y

Condition4. Sum of conditional mutual information $\mathrm{I}[\mathrm{Y}/\mathrm{X}]+\mathrm{I}[\mathrm{X}/\mathrm{Y}]$ characterizes a direct encoding transformation Φ from inverse coding transformation Φ^{-1}

Then the virtualization, defined by condition 1, consists in the injective mapping of the joint ensemble XY in a joint virtual ensemble $\mathrm{X}^{*}\mathrm{Y}^{*}$

$$vir(\mathrm{I}[\mathrm{X};\mathrm{Y}]):\mathrm{XY}\rightarrow\mathrm{X}^{*}\mathrm{Y}^{*}, \tag{1}$$

Where the overall view of the virtualization process is characterized as

$$\mathrm{I}\left[\mathrm{X};\mathrm{Y}\right]+\Psi\left[\mathrm{I};\mathrm{I}^{*}\right]=\mathrm{I}\left[\mathrm{X}^{*};\mathrm{Y}^{*}\right]. \tag{2}$$

It follows from (2) that the fulfillment of condition 1 requires a change in the characteristic of the transformation of the form of the information flow into quantity $\Psi\left[I;I^*\right]$ defined as a virtualization functional. Functional $\Psi\left[I;I^*\right]$ - Is a numerical function defined on the vector space formed by $I[X;Y]$ and $I[X^*;Y^*]$ over the sample space of the joint ensemble XYX^*Y^* The functional takes as an argument the element of this vector space (vector) and returns the scalar as the result. From the standpoint of mathematics, the simplest functional is a projection.

The virtualization functional that optimizes the information flow relative to condition 1 is defined as

$$\Psi\left[I;I^*\right]=Q-I\left[X\right]+I\left[X/Y\right]=Q-I\left[Y\right]+I\left[Y/X\right]. \qquad (3)$$

The virtualization functional in (3), on the basis of Theorems 1.2.4-1.2.9 in [1], forms the projection onto the region of absolutely optimal solutions given by the virtualization condition 1. The optimization task of information flows is reduced to optimizing the form of the information flow representation $\mathbf{I[Y]}$ at the output of the encoding transformation, i.e. to the definition $\mathbf{I[Y^*]}$ Information flow presentation form $\mathbf{I[Y^*]}$ can be obtained by transforming the expression derived from (3)

$$I\left[Y\right]-I\left[Y/X\right]+Q-I\left[X\right]+I\left[X/Y\right]=I\left[Y^*\right]-I\left[Y^*/X^*\right], \qquad (4)$$

To mind

$$I\left[Y^*\right]=I\left[Y\right]+\left((I\left[Y^*/X^*\right]-I\left[Y/X\right])+(Q-I\left[X\right])\right)+I\left[X/Y\right]. \qquad (5)$$

It should be noted that expressions (4) and (5) represent the forms of information flows, which does not allow the possibility of an arbitrary reduction of identical and derived elements of the left and right sides of the equations. Admissibility of these statements is convincingly supported by the results of experimental studies.

Expression (5) reflects the general form of the solution of the problem of optimizing the form of the transformation of the information flow relative to condition 1. From these positions $I[Y^*]$ can be considered as a projection of the logical form of the information flow [2] at the output of the encoding transformation to the region of absolutely optimal solutions, given by the condition 1. The transition from (5) to the material form of the information stream presentation is provided by virtualization conditions 2-4. The application of these conditions makes it possible to obtain a virtual coding algorithm

$$y_i^*=y_i+\Phi_{i-l}\left(\left(\Phi_{i-r}^{-1}\left(y_{i-r}^*\right)-\Phi_{i-n}^{-1}\left(y_{i-n}\right)\right)+\left(x^*_{i-p}-x_{i-j}\right)\right). \qquad (6)$$

And the virtual decoding algorithm

$$x_i=\Phi_i^{-1}\left(y_i^*-\Phi_{i-l}\left(\left(\Phi_{i-r}^{-1}\left(y_{i-r}^*\right)-\Phi_{i-n}^{-1}\left(y_{i-n}\right)\right)+\left(x^*_{i-p}-x_{i-j}\right)\right)\right). \qquad (7)$$

The analysis of the algorithms shows that virtualization is realized by including the encoding transformation at the output and at the input of the decoding conversion of the information flow virtualization module (MVP) decoding the codograms of the source and virtual information streams, encoding the decoding results and time delays of the codograms and messages. This provides optimization of the initial encoding and decoding transformations

An experimental estimation of the efficiency of the solutions obtained was carried out on the basis of computer simulation of the obtained algorithms in the form of a software complex (Fig. 1).

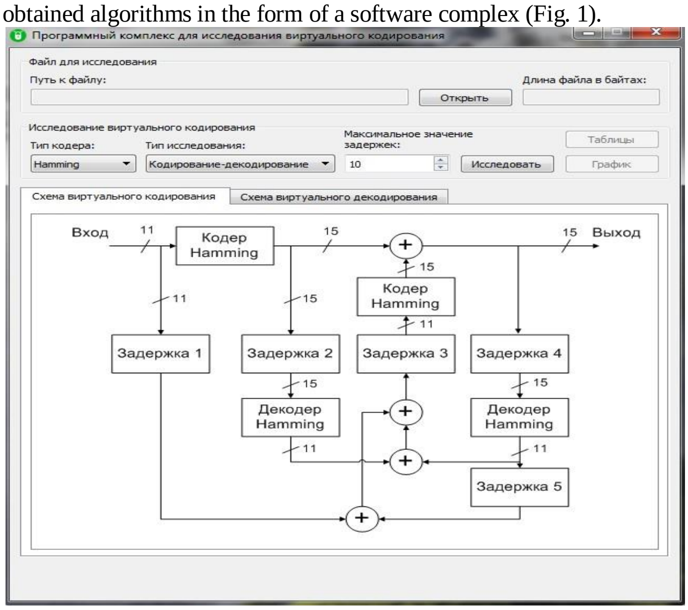

Figure 1. The interface of the software complex for studying virtual noise-immune coding

3. Experimental Study of the Effectiveness of Protection against Information Intrusions

The main tool currently used to evaluate the effectiveness of cryptographic algorithms is a set of NIST STS tests. Using the NIST STS package, three virtualization modes were tested:

1. Virtual noise-immune encoding HAMMING (15, 11).
2. Virtual noise-immune encoding CRC32, polynomial $x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{5}+x^{4}+x^{2}+x+1$.
3. Virtual noise immunity coding REED-SOLOMON.

Testing was carried out on various file formats: 1) text data (txt); 2) audio data (mp3) video data (mp4).

For the purpose of comparative analysis on identical files testing of the US encryption standard AES (algorithm aes256-cbc).

For testing purposes, the following parameters are selected: length of the test sequence n = 106 bits; number of test sequences m = 100; the volume of the test sample N = 108 bits; significance level $a = 0.01$ number of tests $q = 189$

Thus, the statistical portrait of the generator contains 18,900 probability values P.

Ideally, when $m = 100$ and $a = 0.01$ only one sequence of one hundred can be rejected, i.e., the transmission coefficient of each test should be 99%. But this is too rigid a rule. Therefore, a rule based on the confidence interval for r_j The lower limit in this case is $r_{min} = 0.96015$

The NIST STS package includes 16 statistical tests, which are designed to test the hypothesis of randomness of binary sequences of arbitrary length. All tests are aimed at the appearance of various randomness defects.

The decision on whether a given sequence of zeros and ones is random or not, is taken on the totality of the results of all tests. The results of the cryptographic evaluation of the effectiveness of information protection are given in Table 1.

Table 1; Results of Cryptographic Evaluation of Information Security Effectiveness

Virtual noise-immune coding, protection algorithm		**The number of tests in which more than 99% of the sequences have been tested**	**The number of tests in which more than 96% of the sequences have been tested**

HAMMING (15,11)	txt	129(68%) - 147(77%)	183(96%) - 185(97%)
HAMMING (15,11)	mp3	124(65%) - 150(79%)	182(96%) - 185(97%)
HAMMING (15,11)	mp4	122(64%) - 151(79%)	183(96%) - 185(97%)
CRC32	txt	129(68%) - 151(79%)	185(97%) - 189(100%)
CRC32	mp3	135(71%) - 153(80%)	188(99%) - 189(100%)
CRC32	mp4	134(70%) - 148(78%)	187(98%) - 189(100%)
Algorithm aes256-cbc	txt	131(69%) - 152(80%)	186(98%) - 189(100%)
Algorithm aes256-cbc	mp3	129(68%) - 151(79%)	187(98%) - 189(100%)
Algorithm aes256-cbc	mp4	128(67%) - 147(77%)	184(97%) - 189(100%)

4. Conclusion

The analysis of the obtained results shows that virtual noise-immune coding ensures the effectiveness of protection from information intrusions, comparable with the effectiveness of modern protection standards. In general, the results of experimental studies show that the virtualization of the process of noise-immune encoding from the perspective of the approach proposed in [1] opens an additional possibility of protecting information in the part of ensuring information security. This determines the feasibility of further research in this direction.

Acknowledgement

The work was prepared with the support of the Russian Foundation for Basic Research, projects number 16-08-00752.

References

[1] V.V. Kotenko, The theory of virtualization and protection of telecommunications: monograph - Taganrog: Publishing house of the TTI SFU, 2011. P. 244.
[2] V.V. Kotenko, The effectiveness of virtual noise-immune coding . News of SFedU. Technical science. – 2016. – № 9 (182). – P.15-27.
[3] V.V. Kotenko, K.E Rumyantsev, Theory of Information and Protection of telecommunications: Monograph. - Rostov-on-Don: Southern Federal University Publishing House, 2009.- P. 369.
[4] V.V. Kotenko, Virtualization continuous data protection process with respect to the theoretical conditions undecipherability. Information counter the threats of terrorism. 2013. № 20. P. 140-147.
[5] V.V. Kotenko, S.V. Kotenko, Identification analysis of cryptographic algorithms from the point of virtualization IDs / Proceedings of the SFU. Technical science. 2015. Number 8 (169). P 32-46.
[6] V.V. Kotenko, A.R. Kertiev, Model of crypto algorithm with the virtualization of estimations / the International magazine of experimental education. 2015. № 8-3. P. 411-412.
[7] V.V. Kotenko Virtualization continuous data protection process with respect to the theoretical conditions undecipherability / Information counter the threats of terrorism. 2013. № 20. P. 140-147.
[8] V.V. Kotenko, S.V. Polikarpov, The strategy of forming virtual sample spaces ensembles key in solving the problems of information security. Problems of information security. - 2002. - №2. - P. 47-51.
[9] V.V. Kotenko, K.E. Rumyantsev, S.V. Polikarpov A new approach to assessing the effectiveness of encryption methods from the standpoint of information theory . Questions of information security. - 2004. - №1.- P.16-22.
[10] J. Irvine, D. Harle Types of coding. Data Communications and Networks. John Wiley & Sons, 2002. – P 268.
[11] V.V. Kotenko, K.E. Rumyantsev, Y.V. Yukhanov, A.S. Evseev, Virtualization technologies of information security processes in computer networks // Herald of computer and information technologies: scientific and practical. Zh., Moscow. - 2007. - №9 (39). - P. 46-56.
[12] V.V. Kotenko The strategy of applying the theory of the virtualization of information flows for solving information security. Proceedings of the IX International scientific-practical conference "Information Security". - Taganrog - 2007. - P. 68-73.
[13] V.V. Kotenko, K.E. Rumyantsev, S.V. Polikarpov, A method of encrypting binary data // The patent for the invention № 2260916 Russian Federation. Published: 20.09.2005 Bull. №26. P. 1-3
[14] V.V. Kotenko Evaluation of the information of the image of the object from the point of virtual knowledge theory. News TSURE. - Taganrog: - 2006. - №4 (48). - P. 42-48.
[15] V.V. Kotenko Virtualization is the process of continuous protection of information concerning the conditions of theoretical undecipherability. Information counter terrorist threats. Scientific-practical zhurnal.- 2013.-№20- P. 140-147.
[16] V.V. Kotenko Information resources protection in position of information protection process virtualization with absolute uncertainty of the source // Technical and natural sciences: Theory and practice. Proceedings of materials of international scientific e-Symposium. Russia, Moscow, 27 – 28 March 2015. – Kirov, 2015. – P. 73 – 90.
[17] S.V. Kotenko, V.V. Kotenko, K.E. Rumyantsev, Evaluation of auricular-diagnostic identification topology effectiveness // Technical and natural sciences: Theory and practice. Proceedings of materials of international scientific e-Symposium. Russia, Moscow, 27 – 28 March 2015. – Kirov, 2015. – P. 91 – 107.
[18] S.A. Khovanskov, O.R. Norkin, S.S. Parfenov, V.S. Khovanskova, Algorithmic support distributed computing using hierarchical computing structure // Informatization and Communication. - 2014. - № 2 (156). – P. 71-75.
[19] V.V. Kotenko, I.M. Pershin, S.V. Kotenko, Features of the analysis based on the identification information of virtualization image the location of objects in the GIS // Proceedings of SFU. Technical science. - 2014. - №8 (157). - P. 212-219.
[20] V.V. Kotenko, K.E. Rumyantsev, S.V. Kotenko, Methodology of identification analysis of communication systems: monograph. - Rostov-on-Don: Southern Federal University Publishing House, 2014. P 226.
[21] R. Gallagher Information theory and reliable communication. - Moscow: Soviet radio, 1974. - 720.
[22] S.V. Kotenko, Virtualization is the process of continuous protection of information concerning the conditions of theoretical nedeshifruemosti. / Information counter terrorism threats. Scientific-practical zhurnal.- 2013.-№20- P. 152 -158.
[23] V.V. Kotenko , K.E. Rumjantsev , S.V. Kotenko . New Approach to Evaluate the Effectiveness of the Audio Information Protection for Determining the Identity of Virtual Speech Images // Proceeding of the Second International Conference on Security of Information and Networks. The Association for Computing Machinery. New York, 2009. – P. 235 –239.
[24] W.Peterson, E. Weldon Codes correcting mistakes / W. Peterson, E. Weldon / / M .: Mir, 1976. – P 223.
[25] K. Shannon, Works on the theory of information and cybernetics / K. Shannon - M .: Izd-vo inostr. lit., 1963. – P. 829.
[26] R.J. McEliece. A Public-Key Criptosystem Based on Algebraic Theory. // DGN Progress Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January – February, 1978. – P. 114-116.
[27] H. Niederreiter. Knapsack-Type Cryptosystems and Algebraic Coding Theory. // Probl. Control and Inform. Theory. – 1986. – V.15. – P. 19-34.
[28] D. Kimura. Functional asymmetry of the brain in dichotic listening //Cortex, 1967. —№ 3. —P. 163-178.
[29] R. Morelos-Zaragoza, The art of noise-immune coding / Morelos-Zaragoza R. Methods, algorithms, application: Trans. with English. - Moscow: Technosphere, 2006. – P. 320.
[30] V.V. Kotenko Theory of virtualization and protection of telecommunications: monograph / Kotenko VV- Taganrog: Publishing house of TIT SFedU, 2011. – P. 236.
[31] A.I. Velichkin Transmission of analog messages over digital channels. - Moscow: Radio and Communication, 1983. – P. 284.
[32] V.V. Kotenko, K.E. Rumyantsev. Information Theory and Protection of Telecommunications: Monograph. - Rostov-on-Don: SFU Publishing House, 2009. – P. 369.
[33] R.M. Akert, A.T. Panter. Extraversion and the ability to decode nonverbal communication // Per. and individual. Differ. 1988, 9. — l 6. — P. 965-972