Development of a video data protection system using the solution of the problem of verifying of graph isomorphism

R.T. Faizullin[1], G.S. Rzhanitsyn[1]
[1]Dostoevsky Omsk State University

Abstract

The article addresses the use of various approaches to the protection of video data. A study of the security of approaches associated with the rearrangement of rows and columns of video frames is provided. A structure of a cryptosystem is proposed that uses the connection with the solution of the problem of verifying of graph isomorphism.

Keywords:

Citation: Faizullin RT, Rzhanitsyn GS. Development of a video data protection system using the solution of the problem of verifying of graph isomorphism. Computer Optics 2006; 29: 127-134.

Access full text (in Russian)

References:

[1] Volodin AA, Mitjko VG, Spinko EN. Video processing in television surveillance systems [In Russian]. Voprosy Zaschity Informacii 2002; 4(59): 34-47.
[2] Alferov AP, Zubov AYu, Kuzmin AS, Cheremushkin AV. Basics of cryptography [In Russian]. Moscow: "Gelios ARV" Publisher, 2001. ISBN: 5-85438-025-0.
[3] Faizullin R, Prolubnikov A. An algorithm of the spectral splitting for the double permutation cipher. Pattern Recognit Image Anal 2002; 12(4): 365-375.
[4] Prolubnikov AV, Faizullin RT. The class of graphs whose isomorphism check problem is solvable in polynomial time by the spectral splitting algorithm [In Russian]. Mathematical Structures and Modeling 2003; 12: 28-57.
[5] Burmester M, Piper F, Desmedt Y, Walker M. A general zero-knowledge scheme. In Book: De Santis A, ed. Advances in cryptology – EUROCRYPT'94. Berlin, Heidelberg, New York: Springer-Verlag; 1994: 275-286. DOI: 10.1007/BFb0053443.
[6] TV signal secrecy [In Russian]. Source: http://www.smolsat.com/secret.html.
[7] A basic intro to VideoCrypt. Source: http://www.heyrick.co.uk/willow/vcrypt.html.
[8] Protection of TV channels and the possibility of its overcoming [In Russian]. Source: http://www.computerra.ru/offline/2002/469/21579/print.html.
[9] Satellite coding systems [In Russian]. Source: http://sat-tv.infonet.by/kod.htm.
[10] Geljnikov V. Cryptographic from notebook to computer [In Russian]. Moscow: "ABF" Publisher; 1996.
[11] Brassard G. Modern cryptology. Berlin, Heidelberg: Springer-Verlag; 1988. ISBN: 0-387-96842-3.
[12] Petrakov AV, Lagutin VS. Tele protection [In Russian]. Moscow: "Energoatomizdat" Publisher; 1998: 245-257.
[13] Qiao L, Nahrstedt K. Comparison of MPEG ecryption algorithms. Comput Graph 1998; 22(4): 437-448. DOI: 10.1016/S0097-8493(98)00033-8.
[14] Wu Ch-P, Jay Kuo C. Efficient multimedia encryption via entropy codec design. Proc SPIE 2001; 4314: 128-138. DOI: 10.1117/12.435392.