UDC 62-50:519.7(045)

V. Kirichenko, PhD
(National Aviation University, Ukraine)

Features information UAV control system

The paper discusses the features of the information channel UAV is considered a way to encrypt data, using direct and inverse dynamic systems. With encryption program - the decryption carried out a series of experiments to transform the data, which showed some features of algorithms based on the above-mentioned systems.

Today, there are a number of technical issues hindering the UAV development. The overarching task is to ensure information transmission between an aerial vehicle also called, for brevity's sake, the 'Board' and a ground control station (GCS) that we further designate using the term the 'Ground' to the volume required, at the given rate and without noise. This task can be solved by increasing the capacity and noise resistance of the information transmission channels.

Topical issues of classified information in communication channels with ground control UAV investigated in many recent papers, for example [1], [2]. However, analysis of recent research and publications shows that these issues are not completely addressed in the literature.

The most important information kinds exchanged by the Board and the Ground include the command-line, telemetric and video information.

ON-board video cameras are needed to give the panorama in sight of UAV to detect various objects afield and determine their coordinates, to explore areas of forest and peat-bog fires, major man-induced disasters, to perform environmental monitoring, etc. Particular tactical tasks carried out using the aircraft-borne video cameras are confidential and protected from unauthorized disclosure. The use of stream ciphers offers a simple solution for cryptographic information security in broadband video transmission system.

The problem of vulnerability of the channels used to transmit information between UAV and the ground control station more often being a tablet computer or a laptop, can be solved by using one of the following methods:

– the use of autonomous UAV;

– the use of satellite repeaters;

– closure of communication lines by using cryptographic means.

In most applications, the last of the above mentioned methods turns to be the most appropriate and cost-effective one.

In evaluating the requirements applicable to channel protection system using cryptographic means, the following aspects can be distinguished: speed-of-response, encryption reliability, weight and overall dimensions of the on-board system part. These factors are in conflict with each other, especially with increasing channel carrying capacity and low weight of UAV.

Several factors determine the choice of the encryption algorithm, such as organizational (including certification issues) and technical ones, of which an important moment is feasibility on the available component basis.

The aim of this paper is to develop of software and modeling cypher algorithm that ensures high-speed streamed cryptographic conversion of signals transmitted from the UAV board.

In recent years, a new direction in cryptology is being developed, which is associated with the use of dynamical systems with chaotic behavior [3]. One of the basic approaches in this direction is based on the use of inverse control systems for developing cryptographic algorithms [4].

Dynamical systems with chaotic behavior are being widely used now and are used in various fields, in particular for ensuring cryptographic protection of information. Such systems can serve as the basis for pseudorandom sequence generators that are further used to encrypt plaintext data. On the other hand, every dynamical system of the input-output structure can be directly used for conversion of information. On the basis of such systems an encoder is developed. The log-in is a digitized message, while the log-out is an encrypted signal directed to the telecommunications network. A necessary condition for unique decrypting is availability of the feedback system.

The cheapest of the UAV does not provide cryptographic protection of the communication channel. That is, the same commands coming from the ground to the board and from board to the ground correspond to the same signals. This allows an attacker to take control of the UAV.

Any information processed by different discrete calculators can eventually be represented by a sequence of bits (0 or 1). This representation, in fact, is used in its conversion using a variety of dynamical chaotic systems. However, in computing systems to represent different types of data they use larger units that is to say 88 bytes (bit), and machine words from 16 to 64, usually depending on the machine digit capacity. Most commonly byte representation of information is used. Thus, the code tables in computing systems for representing textual information indicate correspondence between 256 bytes and characters of different scripts.

In many cases, the use of the byte information representation also simplifies algorithms of its processing by computing systems. Therefore, we will further consider the byte to be a unit of digital information, and the information processed in computer environment, will be represented as a sequence of different bytes.

The method of data encryption will be the method of direct information conversion by a dynamical chaotic system using forward and backward systems.

The encryption algorithm used in this work is based on the use of discrete analogue of the Chua dynamical chaotic system [4].

The final Chua machine is described by the system of equations:

Direct system

$$\begin{aligned}\dot{x}_1 &= A_1(A_2(x_2 - x_1) - (x_1 + 1)) \\ \dot{x}_2 &= A_3(A_2(x_1 - x_2) - x_3 + Av_{in}) \\ \dot{x}_3 &= A_4(x_2 - A_5 x_3)\end{aligned}$$

Inverse system

$$\dot{x}_1 = A_1(A_2(x_2' - x_1') - (x_1' + 1)$$

$$V_{out} = \frac{1}{A}(\frac{1}{A_3}\dot{x}_2 - A_2(x_1' - x_2') + x_3'$$

$$\dot{x}_3' = A_4(x_2' - A_5 x_3')$$

Here v_{in} and v_{out} – inputs direct and inverse systems respectively. A set of input and output symbols, components $x_i\,(t)$, $i = 1, 2, 3$ are understood as the elements of the Galois field $GF\,(q)$ or the ring $Z\,(q)$, and operations of addition or multiplication are relative operations in this field or ring. This allows the use of inexpensive signal processing controller is not great AC.

For digital information conversion, the fields and rings of characteristic 2 are usually used, that is to say $q = 2n,\ \ n \in N$. Given the nature of information representation in the computer memory, the program uses the fields $GF\,(2^{8k})$ or the rings $Z\,(2^{8k})$, $k = 1, 2, 3, 4$. This is due to the fact that the information file is stored in the computer memory as a sequence of bytes. There are several types of the Galois field representation. The program uses two of them: integer representation, and vector representation. Implicitly, polynomial representation is also applied in developing calculation algorithms in the fields.

The key of the decryption system are system coefficients and initial state for the machine. Sampled differential equations with step 1, we get:

Direct system:

$$\begin{cases} x_1(t+1) = x_1(t) + A_1\left[A_2(x_2(t) - x_1(t)) - (x_1(t) + 1)\right], \\ x_2(t+1) = x_2(t) + A_3\left[A_2\left[x_1(t) - x_2(t)\right] - x_3(t) + Av_{in}(t)\right], \\ x_3(t+1) = x_3(t) + A_4\left[x_2(t) - A_5 x_3(t)\right]. \end{cases}$$

Here output of system $v_{out}\,(t) = x_2(t)$.

Inverse system:

$$\begin{cases} x_1(t+1) = x_1(t) + A_1\left[A_2(x_2(t) - x_1(t)) - (x_1(t) + 1)\right], \\ v_{out}(t+1) = \dfrac{1}{A}\left(\dfrac{x_2(t+1) - x_2(t)}{A_3} - A_2\left[x_1(t) - x_2(t)\right] + x_3(t)\right), \\ x_3(t+1) = x_3(t) + A_4\left[x_2(t) - A_5 x_3(t)\right]. \end{cases}$$

Re-calculation of coefficients of the reverse machine occurs during system setup for file decryption. As a result of encoder output will be a sequence, which should have the properties of a pseudo-random one. To study the pseudo-random sequence of numbers, there are two groups of tests.

Graphic tests. Statistical properties of sequences are displayed as curves, the form of which is used to make conclusions about the properties of the sequence under test.

Evaluation tests. Statistical properties of sequences are defined by numerical characteristics.

Based on evaluation criteria, conclusions about the proximity degree for characteristics of the sequence under test and a true random sequence are made.

Figs 1-4 show the results of the encryption and continuous periodic signals using Chua machine in the final ring $Z(2^8)$ of the following conditions $A_1=9$, $A_2=99$, $A_3=113$, $x_{10}=116$, $x_{20}=47$, $x_{30}=38$.

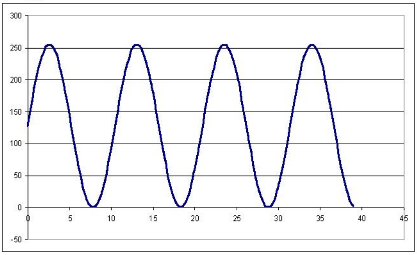

Fig. 1. The periodic signal

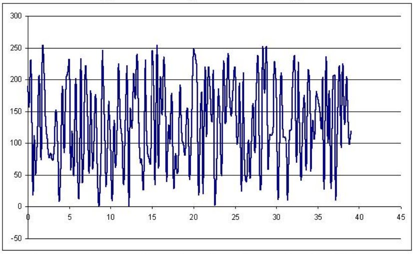

Fig. 2. Transformed periodic signal via Chua system

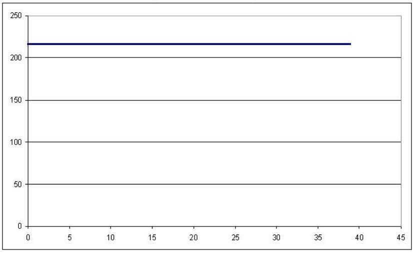

Fig. 3. The permanent signal

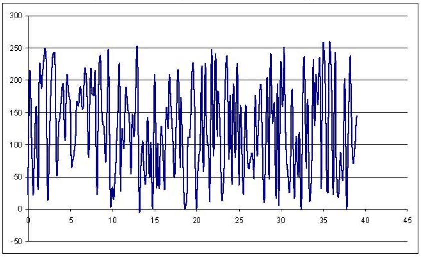

Fig. 4. The converted DC signal by Chua system

To estimate the pseudo random sequence of numbers generated using the Chua system, a package of statistical NIST tests was applied.

For encryption, the Chua system was used in finite rings (2^p) and fields $GF(2^p)$ $8 \leq p \leq 128$.

Test 1. Analysis of algorithms using graphical visualization. For this test 10 various incoming sequences of 320 000 length were used. Each sequence was ciphered by each algorithm 20 times with different, randomly chosen parameters. As a result of the tests performed, the following conclusions were made:

– When the ring output increases, the 'blurring' improves.

– When non-linearity is added in the first equation of the Lorentz system, the picture 'improves' slightly.

– In the fields $GF(2^8)$, $GF(2^{16})$, the modified Chua system has a uniform blurred image.

Test 2. Using the package of NIST statistical tests to assess the quality of pseudo-random sequence generators. In this test, a sequence of units of length 1,000,000 is encrypted 125 times. Each parameter moves in increments of $2^p/5$, and all possible combinations are considered. Thus, we obtained 125 sequences. A battery of NIST tests in applied to them.

The NIST tests show that encryption by the Chua system in the ring $Z(2^8)$ produces an unsatisfactory result. With the increasing ring output the result improves while the test time reduces. When adding a predicate to the system a slight improvement of the result is observed. Performing all operations in the fields $GF(2^{\mathrm{p}})$ significantly improves the results.

Conclusions

The researches carried out and their evaluation allow us suggest that we obtained new results that extend the theoretical basis of the modern cryptology and seem to be efficient for developing efficient cryptographic algorithms. At the same time, there is a number of open issues related to the impact of dynamic parameters on the stability of cryptographic algorithms to attacks, resistance to information distortion, and appearance of invariant varieties.

References

12. V. M. Ilyushka and T.M. Narytnik, The data transmission system based on high-altitude unmanned aerial vehicle (SPD "Phaeton"). Communication, 2004, no. 7. pp. 38–39.

13. Kirichenko V. V. Information security of communication channel with UAV // Electronics and control systems. – N 3(45), 2015. – P. 23-27.

14. A. M. Kovalev, V. A. Kozlovsky and V. F. Scsherbak, Generalized Inverse dynamical systems in problems of encryption: Applied Discrete Mathematics, 2009, no. 1, pp. 20–21.

15. M. J. Sobhy and A. Shehata, Secure computer communication using haotic algorithms. Int. J. of Bifurcation and Chaos. vol. 10, no. 12, 2000, pp. 2831–2839.