Algorithm of data enciphering and decoding with use of dynamic chaos

Andreev V.V., Sapozhnikova Ju.V.
Chuvash State University, Cheboksary, Russia
E-mail: andreev_vsevolod@mail.ru

1. Introduction

Now a great attention is devoted to development of the enciphering algorithms based on determined chaos [1- 3]. In this paper as the chaos generator it is used Lorentz attractor, described by system of the differential equations (1).

$$dX/dt = -\sigma X + \sigma Y,$$
$$dY/dt = -XZ + rX - Y, \qquad (1)$$
$$dZ/dt = XY - bZ.$$

Here $r = 28$, $\sigma = 10$, $b = 8/3$, t is the time.

2. The description of coding algorithm

In this paper the following algorithm of signal enciphering is developed. Let us consider it on an example of the text information enciphering.

1. Each symbol of a text file is represented in the form of the ASCII-codes. As a result we receive a numerical file **ascii** (see fig.1) containing N numbers. Here N is the symbols quantity in the initial text. Then the file **ascii** is sorted by increase. Thus, if among file elements meets a some identical, we leave only one of them. As a result let us receive a file **u** (see fig.2).

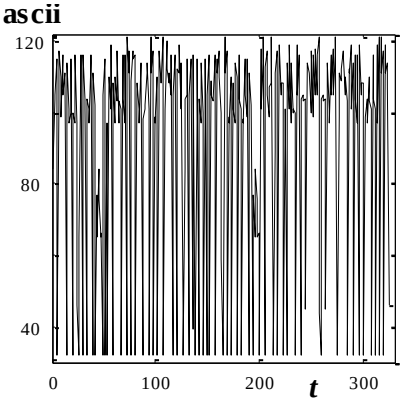

Fig. 1. A graphic representation of the ASCII- codes file

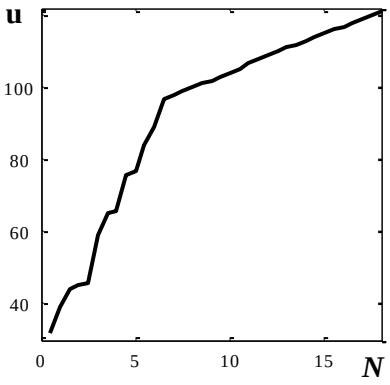

Fig. 2. The file **u** containing sorted by increase and taken in the single copy symbols

2. In the file $\mathbf{n}_1$ let us remember numbers of the file **ascii** elements coinciding on value with each of elements of a file **u** (see fig.3). Thus, dimension of a file $\mathbf{n}_1$ is equal to dimension of a file **ascii** .

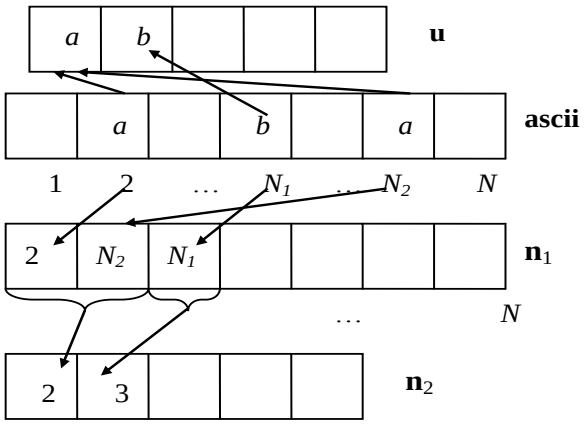

Fig. 3. To the explanatory of files $\mathbf{u}$, $\mathbf{n}_1$, $\mathbf{n}_2$ creation

3. In the file $\mathbf{n}_2$ let us remember quantity of repetitions in an initial signal of each of the values which have been written down in a file $\mathbf{u}$ (see fig. 3). Hence, the files $\mathbf{u}$ and $\mathbf{n}_2$ also have identical dimension.

4. Here let us consider two different variants.

- Let us multiply each element of the file $\mathbf{u}$ on constant k, i.e. it is calculated $k\mathbf{u}$. Further to the end of file $k\mathbf{u}$ let us add the file $2k\mathbf{u}$. Then turned out file let us will designate as $k\mathbf{u}$. Further to the end of file $k\mathbf{u}$ let us add a file $3k\mathbf{u}$. Again let us will designate it as $k\mathbf{u}$. So it is continued until the length of the file will not be bigger than $\dim(\mathbf{n}_1+\mathbf{n}_2)$. In the points of a time axis t, coinciding with elements of a file $k\mathbf{u}$, let us find solutions of Lorentz attractor (1). Thus solutions of the differential equations system (1) can be both positive, and negative.
- Let us receive solutions of the Lorentz attractor (1) on an interval, which length is more than length of the file $\mathbf{n}_1+\mathbf{n}_2$. For further let us take values from the randomness area of the received solutions. The quantity of the chosen values should be equal to quantity of elements of the file $\mathbf{n}_1+\mathbf{n}_2$. How these values get out it should be known to the transmitter and the receiver.

5. Let us carry out shift of Lorentz attractor solutions, for example, $X(t)$ to area of positive values $X(t)+\Delta$. Here the constant Δ is selected from a condition $X(t)+\Delta \geq 0$ for $\forall t$. Let us normalise the values $X(t)+\Delta$ so that maximum from them was equal to dimension of a file $\mathbf{n}_1+\mathbf{n}_2$. So we will receive a file $\mathbf{X}_1$.

6. Let us approximate file elements.

7. Let us create the file $\mathbf{n}_3$ with length $\dim(\mathbf{n}_1+\mathbf{n}_2)$ and consisting of conditional symbols, for example -1. Let us touch one after another the file $\mathbf{X}_1$ elements. We will admit, that the next element M_1 with value a (see fig.4). Then to the file $\mathbf{n}_3$ after an element with number $a-1$ it is added an empty cell, shifting thus elements, since the number a, on one unit to the right. In the added cell let us write an element with number M_1 from the file

$\mathbf{n}_1$. When thus we will pass all file $\mathbf{n}_1$, let us start to distribute elements of the file $\mathbf{n}_2$ (see fig.5). As a result we will receive a new file $\mathbf{n}_3$ with length $2\dim(\mathbf{n}_1+\mathbf{n}_2)$. Dimension of the file $\mathbf{n}_3$ can be reduced. For example, it is possible if in case of consistently standing values -1 to transfer only number of such elements.

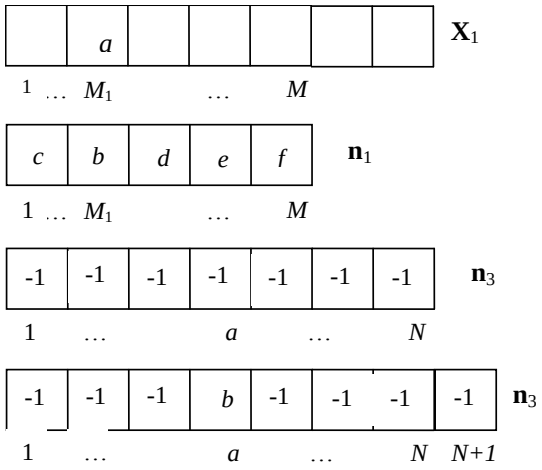

Fig. 4. To the explanatory of file $\mathbf{n}_3$ creation

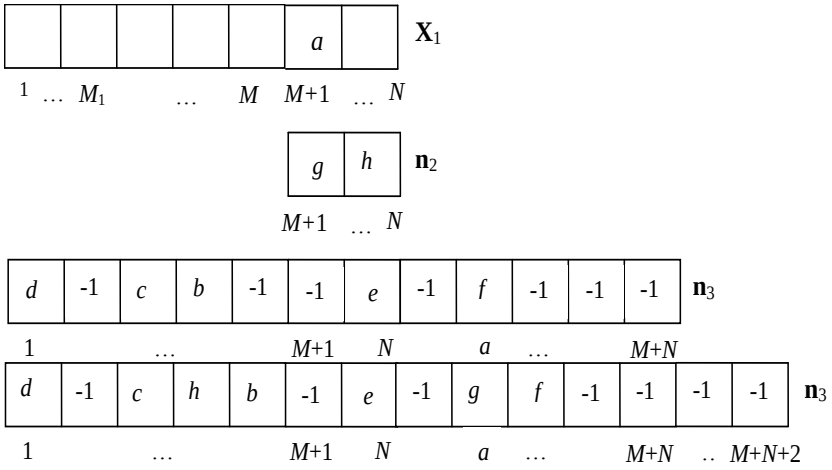

Fig. 5. To the explanatory of file $\mathbf{n}_3$ creation

On the communication channel are transferred the files $\mathbf{u}$, $\mathbf{n}_3$, and also coefficient k, if the file $X(t)$ has been formed in the first variant.

3. The description of decoding algorithm

Decoding in the receiver occurs in a following order.

1. We have coefficient k in case of first variant, of Lorentz attractor parameters, and also files $\mathbf{u}$ and $\mathbf{n}_3$.

2. Let us start Lorentz attractor (1). In result we receive its solutions

a) during the moments of time corresponding to elements of the file $k\mathbf{u}$ in case of first variant (see point 4 in the previous section);

b) under the arrangement in case of second variant.

3. Let us normalise values $X(t)$ in the same order, as at enciphering. As a result we will receive the file $\mathbf{X}_1$.

4. Let us approximate the file $\mathbf{X}_1$ elements as at enciphering.

5. Knowing the elements of file $\mathbf{X}_1$, let us allocate from the file $\mathbf{n}_3$ files $\mathbf{n}_1$ and $\mathbf{n}_2$.

6. Knowing files $\mathbf{n}_1$, $\mathbf{n}_2$ and $\mathbf{u}$ we restore the file **ascii**. In result the initial text is received.

4. Conclusion

It is considered, that in modern code numbers the algorithm of enciphering is known. Cryptographic firmness of the code number is completely defined by privacy of a key. Parameters and initial conditions of Lorentz attractor (1) are the key of algorithm. The algorithm is symmetric. The infinite space of keys is advantage of algorithm.

5. Literature

1. Lepsoy S., Oien G.E., Ramstad T.A. Attractor image compression with a fast non-iterative decoding algorithm. In book: Acoustics, Speech, and Signal Processing: 1993 IEEE International Conference. 1993. V.5. P. 337-340.

2. Kal'yanov G.N., Kal'yanov E.V. Coding Digital Information with the Use of Generators with Chaotic Dynamics // Journal of communications technologies and electronics. – 2008. №4. Pp. 434–442.

3. Andreev V.V., Sapozhnikova Ju..V., Fomichev A.I. The Determined chaos and information coding// Applied computer science. – 2009. №6 (24). Pp. 80–85 (in Russian).