UDC 004.56.5 DOI: 10.18372/2073-4751.69.16808

Gasimov V.A.,
orcid.org/0000-0003-3192-4225,
Mammadov J.I.,
orcid.org/0000-0003-3939-4708,
Mustaphayeva E.A.,
orcid.org/0000-0002-5300-2830

INTERSYMBOL INTERVAL METHOD FOR HIDING SECRET INFORMATION BASED ON PSEUDO-RANDOM NUMBER SEQUENCES

Azerbaijan Technical University

gasumov@yahoo.com
mustafayevaesmira@yahoo.com

Introduction

Although graphic, audio and video files are used as containers in most modern steganographic methods, the method of using texts for this purpose to hide secret information has not lost its importance. The direction of steganography which deals with methods of hiding information in texts is called text steganography or linguistic steganography. In turn, methods of hiding of secret information in texts, are divided into several groups, and one of them is the method of intervals [1-5]. The intervals method includes letter case, lines, intervals between words and paragraphs, kerning, tabulation, line and paragraph marks, and other usage-based methods [1-4]. In one of our research works conducted in this direction, a new method has been suggested using the possibility of changing the inter-symbol intervals in a relatively wide range, and this method ensures the concealment of a larger amount of information [6]. The essence of the method is based on increasing or decreasing the intervals between the symbols of the words in the text below the limit visible to the human eye, thereby making it difficult to detect the fact that secret information is hidden in the container. According to the viewed method, in order to place the hidden secret information in the intervals between the symbols of the text, first, a table is to be drawn up by giving certain values to the interval parameters. Here, since the starting value is 0 and the increment-decrement step is 0.05, it is possible to create 10 encoding options when the inter-symbol interval (considering both dense and sparse intervals) varies from 0 to 0.25. This gives an opportunity to hide more information in the document (table 1). It should also be noted that when the inter-symbol interval is less or more than -0.3 (dense) and +0.3 (sparse), the human eye may be capable to determine these intervals.

Table 1. Binary bit sequences and suggested inter-symbol intervals to encode them.

Encoded bits	Inter-symbol intervals	
	Sparse	Dense
000	0,05	-
001	-	0,05
010	0,1	-
011	-	0,1
100	0,15	-
101	-	0,15
110	0,2	-
111	-	0,2
0	0,25	-
1	-	0,25

In addition to all this, it can be noted that it is possible to further increase the durability of the viewed method to stegoanalysis through the initial encryption of the hidden information. In this research work we conducted, the problem of increasing the reliability of the inter-symbol interval method has been considered by pseudo-randomly selecting the position in the container where the symbols that make up the concealed text will be placed.

Defining a pseudo-random sequence for hiding text symbols

By placing hidden secret information in texts in a random sequence, the stegoanalysis durability of the inter-symbol interval method of information hiding can be significantly increased. For this, efficient algorithms for selecting the positions where symbols will be placed in the container should be used. The combined use of pseudo-random number generators is suggested here, as such an algorithm.

There is extensive information about the methods of generating a sequence of pseudo-random numbers in the technical literature [7-11]. The analysis of the viewed methods shows that the efficiency of the methods based on different algorithms mainly depends on the areas where they are applied. In more serious matters such as information protection, the joint use of several methods is considered appropriate [7, 12-17].

In this research work of ours, to place the hidden secret information in a text-type container in a random sequence, we used a sequence of pseudo-random numbers obtained by the joint application of the linear congruent method and Feigenbaum's quadratic function.

Generation of pseudo-random numbers by linear congruent method

The algorithm of the linear congruent method was suggested by D.X. Lemer in 1948, and it is one of the algorithms created for the generation of regularly distributed random numbers. The basis of the algorithm constitutes the expression

$$x_{n+1} = (ax_n + c)\, mod\, m, n \geq 0 \qquad (1)$$

Here, x_0 – is a starting value ($x_0 \geq 0$), a – is a multiplier ($a \geq 0$), c – is a fixed number ($c \geq 0$), and m is a module ($m > x_0, m > a, m > c$) [7]. The sequence x_0 obtained as a result of implementation of the algorithm depends on the selection of the starting value, and for different values of this, different sequences of random numbers are obtained. Periodic repetitions happen in the sequence of numbers obtained at certain values of the quantities x_0, a, c and m, and it means that, these quantities cannot be chosen arbitrarily. The period of a linear sequence is equal to m- only if it meets the following conditions:

1. c and m are mutually simple numbers;
2. for each simple $p$divisor of m, the number $b = a - 1$ equals to the muitiple of p;
3. while $m$is equal to a multiple of 4, the number b is equal to a multiple of 4.

Choosing the constant a by meeting the above conditions ensures the obtaining of a good enough result, of course, the condition m>a imposed on the numbers a and m should also be taken into consideration here. The constant c does not play a significant role in determining the value of a, and the main requirement here is that c is a single (odd) number. For example, based on the viewed requirements if we take $m = 1024, a = 397$ and $c = 11$, based on the expression

$$x_{i+1} = (397x_i + 11)\, mod\, 1024 \qquad (2)$$

We can generate a sequence of random numbers up to 1024. A visual image of the sequence of generated pseudo-random numbers is shown in fig.1.

However, it should be noted that, in this method, like most Pseudo-Random Sequence Generations (PTAG), there is a certain dependence between consecutive elements, and if several consecutive numbers are known from this dependence, they can be used to calculate others. Taking this into account, by weakening the connection at certain points of the sequence of numbers, it is possible to make significantly complex the process of calculating others according to the known elements of the sequence. For this purpose, in our research work, we suggest to use Feigenbaum's quadratic function.

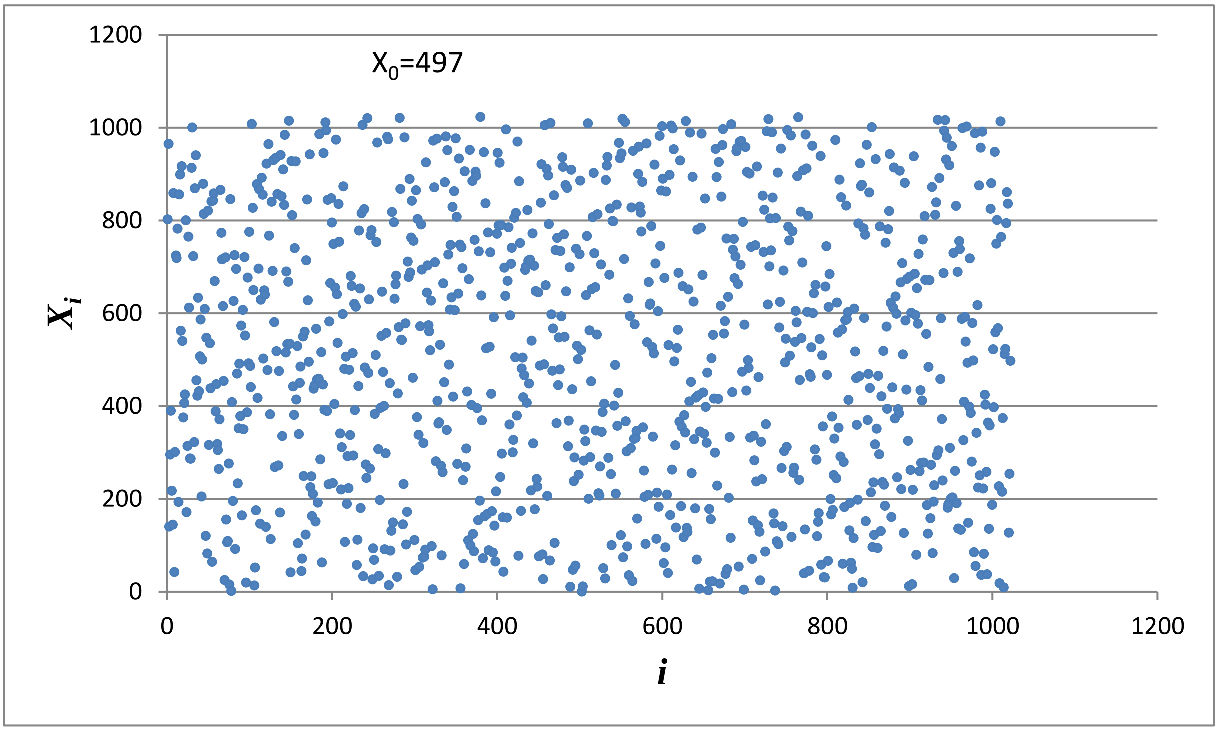


Fig. 1. A sequence of pseudorandom numbers obtained by the linear congruent method

Generation of pseudo-random numbers based on Fiegenbaum's quadratic function

Feigenbaum's quadratic function is one of the functions reflecting deterministic chaos processes and is expressed by the following iterative formula:

$$y_{n+1} = ry_n(1 - y_n) \qquad (3).$$

The quadratic function (3) allows to generate a sequence of numbers changing chaotically between 0 and 1 of y_i at values of parameter r from 3.57 to 4. Using this chaotic feature, a new sequence is created by selectively removing a part of the sequence of numbers obtained on the basis of expression (2).

Calculation of pseudo-random numbers by the combined method

The process of obtaining a new sequence is carried out in the following steps:

a) A sequence consisting of a number of pseudo-random numbers is generated based on expression (2);

b) The sequence of generated numbers each consisting of 10 numbers, is divided into m number (m=n/10) qk (k=1.. m) groups;

c) Based on expression (3), a sequence of m/10 elements is generated (here the length of the fractional part of each bi element in the form of a decimal fraction of sequence B should not be less than 10 digits);

d) Corresponding to the 1st digit after the comma of the b1 element of the B sequence, the first elements of the q1 group of the A sequence are taken and accepted as the first elements of the new C sequence;

e) The first elements of the q2 group of the A sequence corresponding to the 2nd digit after the comma of the b1 element of B sequence is taken and added to the new C sequence. This process, we mean the process of selecting the appropriate number of elements from the q2 group according to the 2nd digit of the b1 element, and adding them to the C sequence, is continued until the 10th digit after the comma of the b1 element is used;

f) Corresponding to the numbers of all elements of sequence B in the fractional part, the process of selecting elements from sequence A in a similar way to point e) and adding them to sequence C is completed by selecting elements from group qm.

In the obtained new sequence, the statistical correlation between the elements is weakened enough, and this complicates the task of calculating others according to the known elements of the sequence.

A visual representation of the sequence of pseudo-random numbers generated according to the linear congruent method and Feigenbaum's quadratic function is shown in fig.2. The elements of this sequence are used to determine the positions in which hidden secret text characters are to be placed within the container.

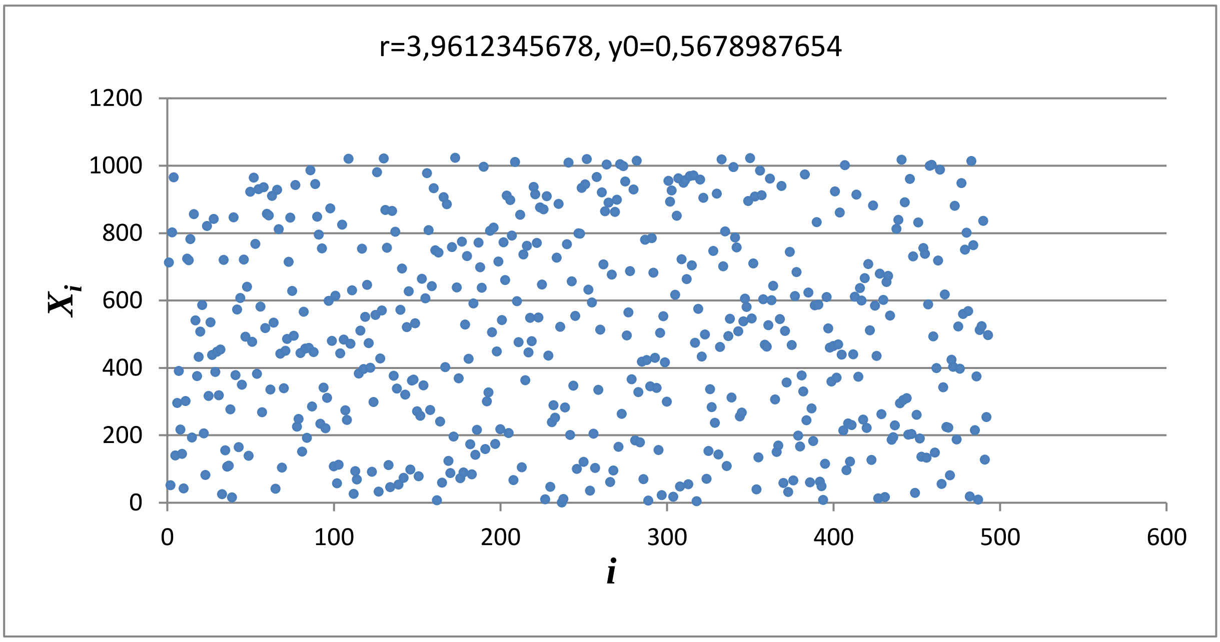


Fig. 2. A sequence of pseudo-random numbers obtained according to the Linear congruent method and Feigenbaum's quadratic function

Proposed steganographic hiding algorithm

Generated according to previous section, the algorithm of the inter-symbol interval method of hiding secret information in texts using pseudo-random numbers will be as follows:

1. the hidden secret information is changed into a binary code;

2. the information contained in the binary code is consecutively divided into groups consisting of 3 bits;

3. for hiding information a text-type container is selected;

4. A sequence of pseudo-random numbers is generated according to the order specified in section 2;

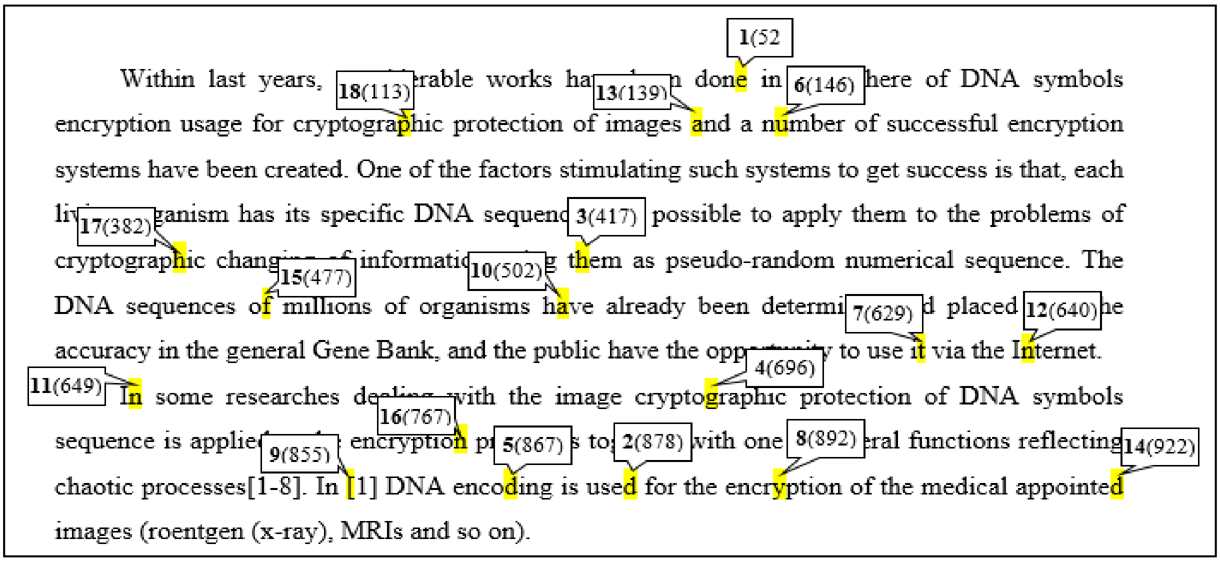
5. corresponding to the 1st element of the pseudo-random sequence the position of the symbol of the container is determined. The intermediate interval of that symbol is changed according to the interval selected from table 1 of group 1 of code 2 of hidden text;

6. operations according to section 6 are performed on all groups of code 2 of hidden secret text.

It should be noted that the information in table 1, as well as the values of the quantities x_0, r and y_0, are delivered in advance to the parts that send and receive the information and are kept confidential.

An example. The suggested algorithm has been realised in the C# software development on various text samples. Here, the pseudo-random sequence obtained in the values of x_0=497, r=3,9612345678, y_0=0,5678987654 with expressions (2) and (3) has been used. The result of the process is given as a visual image in fig.3.

The process of removing the hidden secret information from the stegocontainer is carried out in a similar way. In this case, intermediate intervals of symbols are selected from the stegocontainer according to the specified positions, the sequence of bits of secret information hidden according to the intervals is obtained from table 1, and this sequence is grouped by bytes to restore the original text.



Within last years, erable works ha n done in here of DNA symbols encryption usage for cryptographic protection of images and a number of successful encryption systems have been created. One of the factors stimulating such systems to get success is that, each li ganism has its specific DNA sequenc possible to apply them to the problems of cryptographic chang informati g them as pseudo-random numerical sequence. The DNA sequences of millions of organisms have already been determi d placed he accuracy in the general Gene Bank, and the public have the opp y to use it via the Internet.

In some researches de with the image cryptographic protection of DNA symbols sequence is applie encryption p s to with one eral functions reflecting chaotic processes[1-8]. In [1] DNA encoding is used for the encryption of the medical appointed images (roentgen (x-ray), MRIs and so on).

Fig. 3. A visual representation of secret information hiding process

Conclusion

The suggested secret information hiding method is more durable to stegoanalysis than similar methods. This is obtained by selecting positions in the container for hiding in a sequence defined by pseudorandom numbers. Linear congruent method and Feigenbaum's quadratic function were used in conbined form in the suggested algorithm to make it difficult to calculate the sequence of pseudorandom numbers by undesirable people. The effectiveness of the suggested method was checked by realizing it in the C# software development.

References

1. *Gasimov V.A.* Fundamentals of information security. – Baku: Publishing-polygraphy center of the MNS, 2009. – 340 p.

2. *Bender W., Gruhl D., Morimoto N., Lu A.* "Techniques for data hiding". IBM Systems Journal. – Vol. 35. – Issues 3&4. – 1996. – P. 313-336.

3. *Konakhovich G.F., Puzyrenko A.Yu.* Computer steganography. Theory and practice // MK-Press, 2006. – 288 p.

4. *Tekin V.* Text steganography // World of PC – 2004. – № 11. – 63 p.

5. *Gasimov V.A., Mammadov J.I., Javadov A.F.* “About one method of steganographic information hiding in text-type containers”, Integration of Education, Science and Business in Modern Environment: Winter Debates: abstracts of the 2nd International Scientific and Practical Internet Conference, February 4-5, 2021. – Dnipro, Ukraine.

6. *Gasimov V.A., Mustafayeva E.A.* Intercharacter intervals method of hiding information in Word documents // Baku: News of ANAS, 2014. – № 6. – P. 124-129.

7. *Knut D.* The Art of Computer Programming. – M. 1977. – V. 2. – 724 p.

8. *Sidorenko A.V., Shakinko I.V., Sidorenko Yu.V.* Image Encryption Algorithm Using Two-Dimensional Chaotic Mappings / System Analysis and Applied Informatics. – 2016. – № 2. – P. 44-49.

9. *Ptitsyn N.* Application of the theory of deterministic chaos in cryptography. – M.: MSTU named after N.E. Bauman, 2002. – 81 p.

10. *Schneier B.* Practical Cryptography, 2nd Edition. – 610 p.

11. *Mammadov J.I., Namazov F.H.* Development of the image encryption algorithm with the use of chaotic sequences and fractals // – Baku: ASOIU, AHTS News, 2018. – № 2. – P. 85-94.

12. *Mammadov J.I., Gasimova N.N., Isganderova G.J.* Increasing the efficiency of applying pseudorandom number sequences based on deterministic chaos // Scientific works of AHMA. – 2018. – № 1. – P. 67-71.

13. *Dovgal V.M., Gordienko V.V., Nikitin M.O.* A method of hierarchical cryptography based on discrete mappings // El.

scientific journal of Kursk State University. – 2014. – №1.

14. *Politansky R.L., Shpatar P.M., Gres A.V., and Veriga A.D.* Data transmission system with encryption by chaotic sequences // Technology and design in electronic equipment. – 2014. – No. 2-3. – P. 28-32.

15. *Gasimov V.A., Mammadov J.I.* "Method of encryption of text information based on LFSR." Problems of informatization and management. – 2020. – № 64. – P. 35-40.

16. *Gasimov V.A. and Mammadov J.I.* “DNA-based image encryption algorithm” / IOP Conf. Series: Materials Science and Engineering 734 012162 IOP Publishing.

17. *Gasimov V.A. and Mammadov J.I.* "Image encryption algorithm using DNA pseudo-symbols and chaotic map," 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). – 2021. – P. 1-5.

Gasimov V.A., Mammadov J.I., Mustaphayeva E.A.

INTERSYMBOL INTERVAL METHOD FOR HIDING SECRET INFORMATION BASED ON PSEUDO-RANDOM NUMBER SEQUENCES

In the article, an efficient method of hiding secret information in text-type containers based on changing inter-symbol intervals is suggested. Here, the hiding process is performed by selecting the symbols of the container in a pseudo-random sequence to increase reliability. To obtain a pseudo-random sequence the linear congruent method and Feigenbaum's quadratic function were used.

Keywords: *steganography, container, inter-symbol interval method, sequence of pseudo-random numbers, linear congruent method, Feigenbaum's quadratic function.*

Касумов В.А., Маммадов Дж.І., Мустафаєва Е.А.

МІЖСИМВОЛЬНИЙ ІНТЕРВАЛЬНИЙ МЕТОД ПРИХОВУВАННЯ СЕКРЕТНОЇ ІНФОРМАЦІЇ НА ОСНОВІ ПСЕВДОВИПАДКОВИХ ЧИСЛОВИХ ПОСЛІДОВНОСТЕЙ

У статті запропоновано ефективний спосіб приховування секретної інформації в текстових контейнерах на основі зміни міжсимвольних інтервалів. Тут процес приховування виконується шляхом вибору символів контейнера в псевдовипадковій послідовності для підвищення надійності. Для отримання псевдовипадкової послідовності використано лінійний конгруентний метод і квадратичну функцію Фейгенбаума.

Ключові слова: *стеганографія, контейнер, метод міжсимвольних інтервалів, послідовність псевдовипадкових чисел, лінійний конгруентний метод, квадратична функція Фейгенбаума.*