https://doi.org/10.31891/csit-2023-2-6
UDC 004.91

Liudmyla NECHVOLODA, Kateryna KRYKUNENKO, Katerina PARAMONOVA
Donbas State Engineering Academy

APPLICATION OF A MATHEMATICAL MODEL FOR THE GENERATION OF SEPARATE ELEMENTS OF A STEGANOGRAPHIC SYSTEM IN A HIGHER EDUCATION INSTITUTION

Information protection is extremely important not only in the commercial, but also in the state sphere. The Law of Ukraine "On the National Security of Ukraine" among the threats to the national interests and security of Ukraine in the information sphere indicates: computer terrorism and crime; disclosure of secret or confidential information that is the property of the state or is aimed at ensuring the needs and national interests of society and the state; manipulation of public consciousness, in particular, by spreading false information. There is a need to protect various information systems, in particular local networks of state and commercial institutions, from the threat of information leakage and copyright infringement.

The article presents the method of generating separate elements of the steganographic system based on the combination of cryptography and steganography methods, which makes it possible to increase the level of information protection and develop more effective new non-traditional methods of ensuring information security in the global network. Considering the constant development and improvement of computer cryptography and steganography methods, the study of this particular area of steganoanalysis is the most relevant.

It is proposed to apply the method of replacing the least significant bits (LSB method), because it, in combination with the RSA cryptographic algorithm, allows to ensure a high level of information security and the speed of embedding and extraction of a large amount of information.

The practical value lies in the ability to quickly generate steganographic containers and ensure reliable encryption and decryption of hidden information in them. At the stage of experimental research, the proposed method of replacing the younger bits was compared with other methods that could be used to generate individual elements of the steganographic system. According to research results, the LSB method has clearly confirmed its effectiveness. The results of the experiment showed the high stability and quality of the received data encryption and decryption method when sending it through an open communication channel (e-mail).

Keywords: steganographic system, cryptography, encryption, decryption, steganoanalysis, fractals, RSA, LSB

Людмила НЕЧВОЛОДА, Катерина КРИКУНЕНКО, Катерина ПАРАМОНОВА
Донбаська державна машинобудівна академія

ЗАСТОСУВАННЯ МАТЕМАТИЧНОЇ МОДЕЛІ ДЛЯ ГЕНЕРАЦІЇ ОКРЕМИХ ЕЛЕМЕНТІВ СТЕГАНОГРАФІЧНОЇ СИСТЕМИ У ЗАКЛАДІ ВИЩОЇ ОСВІТИ

Захист інформації є надзвичайно важливим не тільки в комерційній, але й у державній сфері. Закон України "Про національну безпеку України" серед загроз національним інтересам і безпеці України в інформаційній сфері зазначає: комп'ютерний тероризм та злочинність; розголошення таємної або конфіденційної інформації, яка є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; маніпулювання суспільною свідомістю, зокрема, шляхом поширення неправдивої інформації. Існує необхідність захисту різних інформаційних систем, зокрема, локальних мереж державних і комерційних установ, від загрози витоку інформації та порушення авторських прав.

У статті представлено методику генерації окремих елементів стеганографічної системи на базі об'єднанні методів криптографії та стеганографії, що дає змогу підвищити рівень захисту інформації та розробити більш ефективні нові нетрадиційні методи забезпечення інформаційної безпеки у глобальній мережі. Зважаючи на невпинний розвиток та вдосконалення методів комп'ютерної криптографії та стеганографії дослідження саме цього напрямку стеганоаналізу є найбільш актуальним.

Запропоновано застосувати метод заміни молодших біт (LSB- метод), оскільки він, у комбінації з криптографічним алгоритмом RSA, дає змогу забезпечини високий рівень інформаційної безпеки та швидкість вбудовування і вилучення великого об'єму інформації.

Практична цінність полягає в можливості швидкої генерації стеганографічних контейнерів та забезпеченні надійного шифрування і дешифрування прихованої інформації в них. На етапі експериментальних досліджень запропонований метод заміни молодших біт був порівняний з іншими методами, що могли б використовуватись для генерації окремих елементів стеганографічної системи. За результатами досліджень метод LSB підтвердив наочно свою ефективність. Результати експерименту показали високу стійкість та якість отриманої методики шифрування та дешифрування даних при пересиланні їх відкритим каналом зв'язку (електронною поштою).

Ключові слова: стеганографічна система, криптографія, шифрування, дешифрування, стеганоаналіз, фрактали, RSA, LSB

Introduction

Information protection is extremely important not only in the commercial, but also in the state sphere. The Law of Ukraine "On the National Security of Ukraine" [1] among the threats to the national interests and security of Ukraine in the information sphere indicates: computer terrorism and crime; disclosure of secret or confidential information that is the property of the state or is aimed at ensuring the needs and national interests of society and the state; manipulation of public consciousness, in particular, by spreading false information. There is a need to protect various information systems, in particular local networks of state and commercial institutions, from the threat of information leakage and copyright infringement.

The methods of criminals are diverse, therefore the information security service must conduct a constant search for information leakage channels, monitor the goals and actions of criminals [2].

Two methods of software protection are traditionally used to preserve the confidentiality of information when it is sent over open communication channels: cryptographic and steganographic protection methods.

The essence of cryptographic protection is that information is encrypted by a certain algorithm into an unreadable format. In turn, steganographic protection is the concealment of the very fact of the existence of information by embedding it in digital objects (containers), which causes some distortion of these objects. The most common types of such containers are text, images, audio data, video sequences.

Today, methods of probability theory and mathematical statistics, theory of fast orthogonal transformations, theory of approximation, theory of coding, theory of complexity, theory of errors, digital processing of signals and images, etc. are widely used as tools for the development of this field.

Both cryptographic and steganographic approaches have their advantages and disadvantages. A promising direction of software information protection is the combination of cryptography and steganography methods. Considering the continuous development and improvement of computer cryptography and steganography methods, the study of this direction of steganoanalysis is the most relevant [3].

Quantitative assessment of the resistance of a steganographic system to external influences is a rather difficult task, which is usually implemented by methods of system analysis, mathematical modeling, or experimental research.

A reliable steganosystem solves two main tasks: hiding the very fact of the message's existence (the first level of protection); preventing unauthorized access to information by choosing an appropriate method of hiding information (second level of protection). The existence of a third level of protection is possible - preliminary cryptographic protection of the message (encryption).

Related works

A significant part of research in the field of steganography is devoted to methods of hiding confidential messages and digital watermarks in still images. Currently, there are a large number of methods of hiding information in graphic files.

A classic example of replacement methods in the spatial domain is the method of replacing the least significant bits (LSB method), which is based on the fact that the least significant bits of graphic, audio and video formats carry little information and their change practically does not affect the quality of the transmitted image or sound. This makes it possible to use them to encode confidential information [4].

In work [5], the main advantage of this method is the simplicity of implementation, the high speed of message embedding and extraction, and the possibility of secret transmission of a large amount of information. However, due to the introduction of additional information, the statistical characteristics of the container file are distorted, and the hidden message is in some cases easy to detect using statistical attacks, such as entropy estimation and correlation coefficients. To reduce compromising features, correction of statistical characteristics is required.

In the scientific publication [6] Taranchuk A.A. the methods operating in the frequency domain are considered, and the data is hidden in the coefficients of the frequency representation of the container. For this, transformations are most often used, which are used in modern lossy compression algorithms (discrete cosine transformation in the JPEG standard and wavelet transformation in JPEG2000). Information can be hidden both in the initial image and simultaneously with the compression of the container image. It is important that stegosystems, which take into account the features of the compression algorithm, are insensitive to further compression of the container.

The essence of broadband methods is to expand the frequency band of the signal to a spectrum width much greater than is necessary for the transmission of real information. There are two ways to expand the range: the method of direct spectrum expansion, using a pseudo-random sequence, and the method of frequency hopping. At the same time, useful information is distributed over the entire range, so when a signal is lost in some frequency bands, there is enough information in other bands to restore it. The principle of operation of broadband methods is related to the tasks solved by stegosystems: to try to "dissolve" a secret message in a container and make it impossible to detect it [7]. Also, in recent years, methods based on image processing have begun to be used for signal detection. In [8], a method for estimating the parameters of transmission from the HFRC based on the spectrogram is proposed. The application of image processing methods to the obtained spectrogram allows you to suppress noise and highlight the necessary parameters.

Statistical methods hide information by changing some statistical properties of the image. In [9], the idea of the Patchwork algorithm is considered, which is based on the assumption that the pixel values are independent and equally distributed. At the same time, a secret key is generated to initialize the generator of pseudo-random numbers, which indicate the place in the image where the watermark bits are entered. This method provides high resistance to digital processing operations, and the difficulty of detecting hidden data without a corresponding secret key.

Thus, the research results show that the reliability of replacement methods in the spatial domain depends on the level of frequency distortions of the container. At the same time, they provide high speed and a significant amount of embedded data, so it is advisable to use them when transmitting hidden messages. Methods operating in the frequency domain are more resistant to distortions and digital processing operations, but can hide a smaller amount of data. The presence of a secret key in broadband and statistical methods using pseudo-random coding increases their reliability.

Proposed mathematical model for the generation of separate elements of a steganographic system in a higher education institution

One of the tasks of information security of every educational institution is to ensure reliable transmission of information between its units. In particular, it can be used to protect students' personal data.

Reliability of data transmission through an open communication channel can be ensured using a steganographic system.

The stegosystem should have the following components:

- message;
- container;
- steganographic channel;
- public and private keys.

The method of secure data transfer through an open communication channel involves the implementation of eight stages.

1. Formation of the student base.
2. Selection of students from the established base.
3. Generation of logins and passwords.
4. Construction of "Plasma" stochastic fractals.
5. Data encryption with the RSA algorithm.
6. Hiding an encrypted message in the lower bits of fractal images using the LSB method.
7. Emailing images to users/students.
8. Decoding and extracting the login and password from the "Plasma" fractal.

For example, generated data: login and password are sent to users of the information system of a higher education institution as an e-mail message. To simplify the work, it is advisable to use email distribution of messages with the help of a previously formed database of students.

The random stochastic fractal "Plasma" can be used as a stegocontainer in this case. The Diamond Square algorithm is most suitable for constructing the "Plasma" stochastic fractal. First, the four corners of the square are assigned random values. After the boundaries of the square are set, it is divided into four equal squares, in each of which the value of one of the angles is known. The value of the height of the central point is the sum of the averaging of the heights of all four corner points and a random value (noise). In practice, the noise should not be completely random, but a function that depends on the distance between neighboring points, because the smaller the distance, the smaller the average value of the noise should be [10].

To ensure greater reliability, along with hiding data, it is advisable to apply data encryption, for example, using the RSA method. The RSA algorithm consists of 4 stages: key generation, encryption, decryption, and key distribution. The security of the RSA algorithm is built on the principle of the complexity of the factorization of integers. The algorithm uses two keys - public and private, together the open and corresponding private keys form key pairs. The public key does not need to be kept secret, it is used to encrypt data. If the message was encrypted with a public key, it can only be decrypted with the corresponding private key.

In order for the Sender to be able to send his secret messages, he transmits his public key (n,e) to the Receiver through a secure, but not necessarily secret, route. The private key d is never distributed. In order to generate key pairs, the following actions are performed:

1. Selecting from two large prime numbers p and q are approximately 512 bits long each.
2. Calculation of their product $n = pq$.
3. Calculation of the Euler function $\varphi(n)=(p-1)(q-1)$.
4. Choosing an integer e such that $1<e< \varphi(n)$ and e is reciprocally prime to $\varphi(n)$.
5. Finding a number d such that $d\equiv1(\mathrm{mod}\ \varphi(n))$ using the extended Euclid algorithm.

The number n is called the modulus, and the numbers e and d are called open and closed exponents. Number pairs (n,e) are the public part of the key, and (n,d) are the secret part. The numbers p i q after the generation of the key pair can be destroyed, but must not be revealed in any case.

Algorithm for finding prime numbers:

1. N is an odd number. Finding s and t satisfying the equation: N - 1 = 2s t.
2. Random selection of the number a,1 <a <N.
3. If N is divisible by a, go to point 6.
4. If the condition at = 1 (mod N) is fulfilled, go to point 2.
5. If k,0 <= k <s such that a_2k t = -1 (mod N) is found, go to point 2.
6. The number N is composite: choosing another odd number N, going to point 1.

It is important that the number s cannot be greater than the number of bits in the number. The numbers s and t are found using a binary shift of the number N – 1, until the lower digit becomes 1. As a result, s is the number of shifts, t is the number N – 1 after the shift.

Suppose that the Sender would like to send a message M to the Receiver. First, it transforms M into an integer m such that $0 \leq m < n$ using a consistent reversible protocol known as a complement scheme. It then calculates the ciphertext c using the public key of the recipient e, using the equation:

$$c = m^e \ (mod\ n). \tag{1}$$

This is done quite quickly, even for 500-bit numbers, using modular exponentiation. The Sender then forwards c to the Receiver.

To decipher the message of the Sender m, the Receiver needs to calculate the following equality [11]:

$$m = c^d \ (mod\ n). \tag{2}$$

After encrypting the message, it needs to be hidden in an image. In our case, the encrypted message is hidden in the lower bits of the fractal image (LSB method). The essence of the method of replacing the least significant bit (Least Significant Bits - LSB) is to hide information by changing the last bits of the image, which encode the color, to the bits of the hidden message.

In the BMP format, the image is stored as a matrix of color shade values for each point of the image.

Diamond Square Algorithm:

1. Setting the height at the corner points A, B, C, D (Fig. 1 (a)).
2. Calculation of values at the central point of the square (Fig. 1 (b)):

$$E = \frac{A+B+C+D}{4} + rand_1. \tag{3}$$

3. Calculation of values at the midpoints of the sides (Fig. 1 (c)):

$$F = \frac{A+B}{2} + rand_2. \tag{4}$$

$$G = \frac{A+C}{2} + rand_3. \tag{5}$$

$$H = \frac{B+D}{2} + rand_4. \tag{6}$$

$$I = \frac{C+D}{2} + rand_5. \tag{7}$$

4. Smaller squares AFEG, BFEH, CGEI, DHEI are considered. For them, the steps of the algorithm are repeated until the squares become the required size [12].

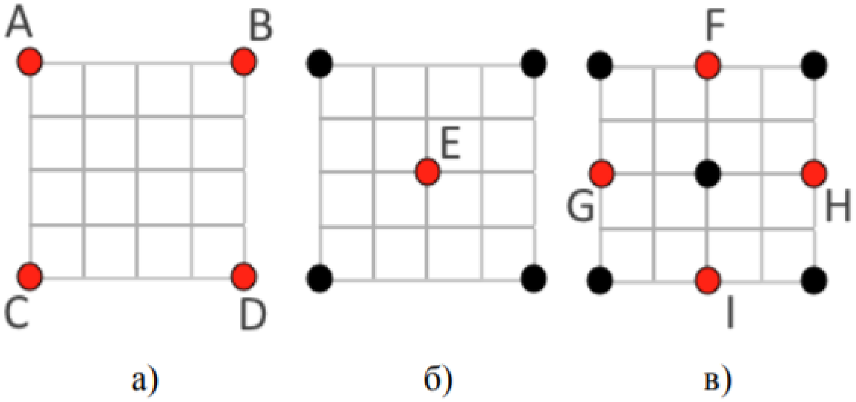


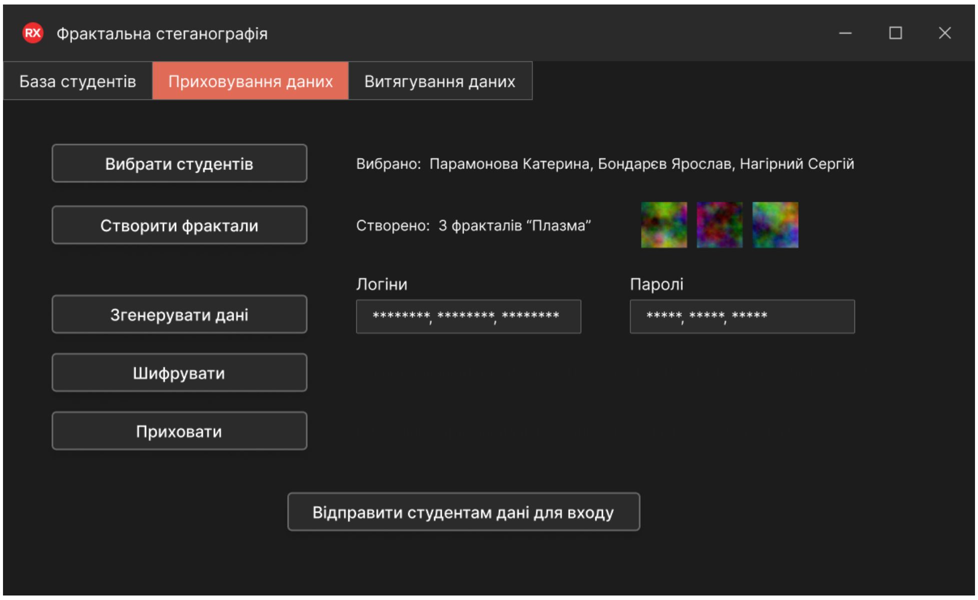
Fig. 1. Diamond Square Algorithm:
a – height in corner points; b – value at the central point;
c is the value at the middle of the sides

The use of the method of replacing the least significant bits (LSB method) in combination with the RSA cryptographic algorithm makes it possible to ensure a high level of information security and the speed of embedding and extraction of a large amount of information.

Experiments

Let's consider the program implementation of the above method using the example of pre-processing of student data for further authorization in the information system of a higher educational institution. The software module for generating individual elements of the steganographic system was developed in Embarcadero RAD Studio 10.2. The program has a user interface in Ukrainian and is divided into three parts: the student database, hiding and data extraction. On the "Data Hiding" tab, the full cycle of actions to obtain a ready-made image with encrypted data for the "Sender" role is performed. Students are selected from the database and will be sent data for entering the personal account [13,14].

The next step in data hiding is to generate the Plasma stochastic fractals using the Generate Fractals button. After displaying the fractals on the form to generate logins and passwords, you need to click the "Generate data" button. Data is invisible to the sender, protected by stars (Figure 2).



Вибрано: Парамонова Катерина, Бондарєв Ярослав, Нагірний Сергій

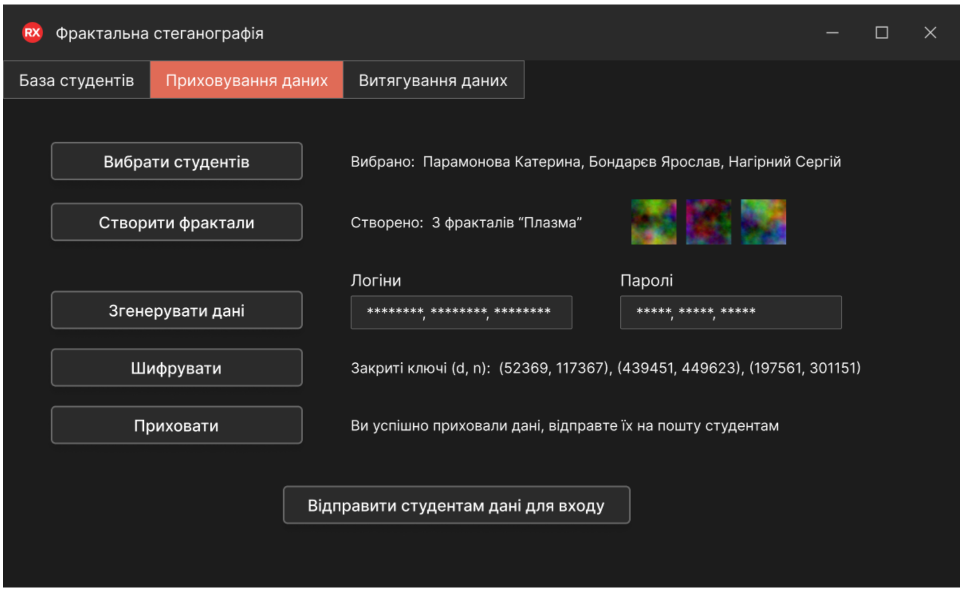
Створено: 3 фракталів "Плазма"

Логіни: ********, ********, ********

Паролі: *****, *****, *****

Fig. 2. Generation of logins/passwords and stochastic fractal "Plasma"

To receive ready-made images with encrypted data (data hiding), logins and passwords will be encrypted using the RSA method. To do this, click on the "Encrypt" button. After this action, private keys appear. The private key is important, it is transmitted to the respective student through a secure communication channel. Then data is hidden in the last bits of previously generated fractals using the LSB method, rasterization and image storage (Figure 3).



Вибрано: Парамонова Катерина, Бондарєв Ярослав, Нагірний Сергій

Створено: 3 фракталів "Плазма"

Логіни: ********, ********, ********

Паролі: *****, *****, *****

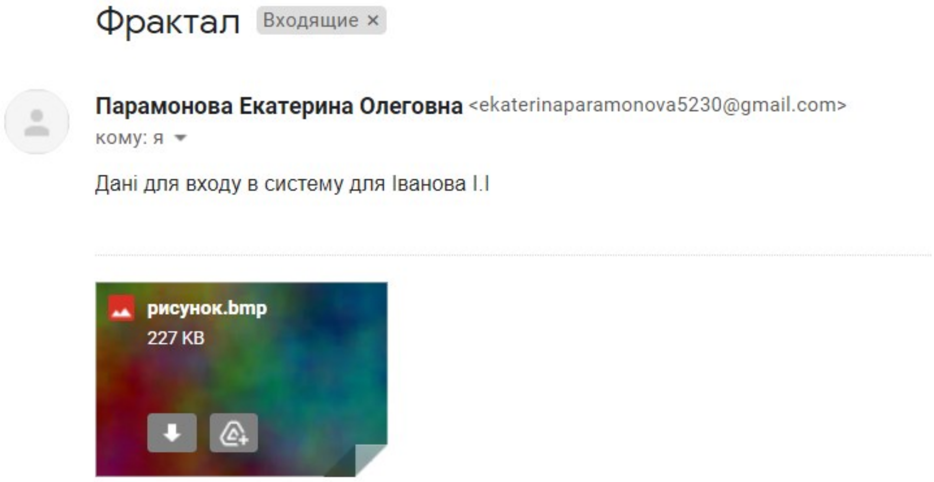
Закриті ключі (d, n): (52369, 117367), (439451, 449623), (197561, 301151)

Ви успішно приховали дані, відправте їх на пошту студентам

Fig. 3. Hiding data in fractals

To send saved images to selected students by e-mail, click on the "Send login data to students" button. This completes the action cycle for the "Sender" role.

On the "Data extraction" tab, the complete cycle of actions to obtain the login and password for the "Recipient" role is performed. A corresponding message will be sent to the e-mail with an attached image (Figure 4). The message should have: the subject "Fractal", the text of the message: "Login data for "Surname and First name of the student", as well as the attached picture of the stochastic fractal "Plasma".



Фрактал

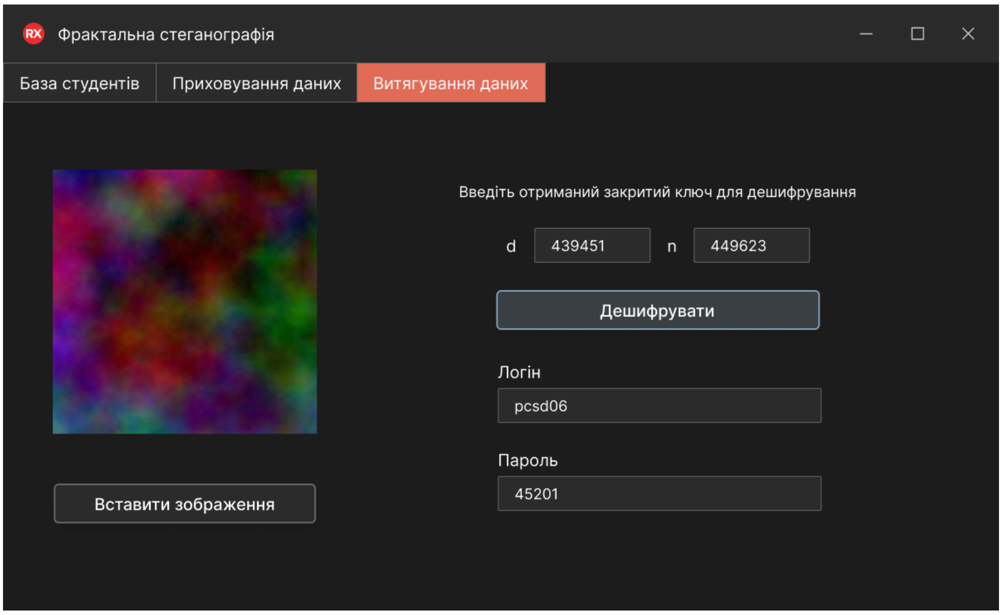
Параменова Екатерина Олеговна <ekaterinaparamonova5230@gmail.com>
кому: я

Дані для входу в систему для Іванова І.І

рисунок.bmp
227 KB

Fig. 4. The message that came to the recipient's e-mail

The next step in extracting data is to enter a private key that is transmitted over a secure communication channel and decrypt the data using that key. After the actions described above, the required initial data will appear in the "Login" and "Password" fields (Fig. 5).



Фрактальна стеганографія

Введіть отриманий закритий ключ для дешифрування

d 439451 n 449623

Логін
pcsd06

Пароль
45201

Fig. 5. Data decryption

The given example demonstrates the option of using a steganographic system to protect students' personal data.

Conclusions

In the process of analyzing the quality of the proposed model, it was found that to create a system for generating individual elements of the steganographic system, it is advisable to use the method of replacing the least significant bits (the LSB method), since it, in combination with the RSA cryptographic algorithm, makes it possible to ensure a high level of information security and embedding speed and extracting a large amount of information. In particular, it will make it possible to transmit data over an open channel more securely with minimal risks of errors occurring when transmitting and extracting data from encrypted messages.

The capabilities of the presented algorithm can be used by dean's offices, personnel and practice departments, and other units of the higher education institution to transmit information containing personal data of students. This is especially relevant in the conditions of information warfare.

References

1. Pro natsionalnu bezpeku Ukrainy: zakon Ukrainy vid 2018r № 31, st.241 URL:https://www.mil.gov.ua/diyalnist/reformi-ta-planuvannya-u-sferi-oboroni/zakon-ukraini-pro-naczionalnu-bezpeku-ukraini.html

2. Sorokivska O. A., Hevko V.L. Informatsiina bezpeka pidpryiemstva: novi zahrozy ta perspektyvy [Tekst]: Visn. Khmelnyts. nats. un-tu. Ser.: Ekon. nauky. 2010. № 2. T. 2.

3. Tarnavskyi Yu.A. Tekhnolohii zakhystu informatsii [Elektronnyi resurs] : pidruchnyk dlia stud. spetsialnosti 122 «Kompiuterni nauky», spetsializatsii «Informatsiini tekhnolohii monitorynhu dovkillia», «Heometrychne modeliuvannia v informatsiinykh systemakh». KPI im. Ihoria Sikorskoho. Elektronni tekstovi dani (1 fail: 2,04 Mbait). Kyiv : KPI im. Ihoria Sikorskoho, 2018. 162 s.

4. Khoroshko V. A., Chekatov A.A. Metody y zasoby zakhystu informatsii. K.: Yunior, 2003. 504 s.

5. Kuznetsov O. O., Yevseiev S.P., Korol O.H. Stehanohrafiia : navchalnyi posibnyk. Kh. : Vyd. KhNEU, 2011. 232 s. (ukr. mov.)

6. Taranchuk A. A., Halper L.H. Stehanohrafichnyi metod prykhovuvannia danykh v oblasti chastotnykh peretvoren zobrazhen. Visnyk Khmelnytskoho natsionalnoho Universytetu. Khmelnytskyi, 2009. № 2 «Tekhnichni nauky» C.197-201.

7. Iudin O. K., Konakhovych H.F., Korchenko O.H. Zakhyst informatsii v merezhakh peredachi danykh: Pidruchnyk K.: Vydavnytstvo TOV NVP «INTERSERVIS»,2009. 352 s.

8. Chevva L., Sagar G. V. R. FH Signal Interception Based on the Time-Frequency Spectrogram by Image Enhancement Techniques // International Journal of Engineering Research and Applications, 2012. Vol. 2, Issue 2. R. 687−692.

9. O.B. Polusyn. Metody zabezpechennia zakhystu multymediinykh danykh nanesenniam tsyfrovoho vodianoho znaku Naukovo-tekhnichna konferentsiia profesorsko-vykladatskoho skladu, naukovykh pratsivnykiv i aspirantiv (u rezhymi onlain) (07 liutoho – 11 liutoho 2022 r.). Tezy dopovidei, Lviv. Ukr. akad. drukarstva, 2022. 193 s.

10. Fraktaly [Elektronnyi resurs]. – URL: http://www.kpi.kharkov.ua/archive/microcad/2011/%95%D0%A0%D0%95%D0%94%D0%9E%D0%92%D0%98%D0%A9.pdf.

11. Metody stehanohrafii [Elektronnyi resurs]. – URL: http://masters.donntu.org/2013/fknt/ippolitov/library/article2.htm.

12. Alhorytm Diamond Square [Elektronnyi resurs]. – URL: https://habr.com/ru/post/111538/.

13. Shevchenko N.Iu., Paramonova K.O. Fraktalni konteinery v stehanohrafii. Informatyka, upravlinnia ta shtuchnyi intelekt. Tezy deviatoi mizhnarodnoi naukovo-tekhnichnoi konferentsii. Kharkiv: NTU "KhPI", 2022. 160 s. ukrainskoiu, anhliiskoiu movamy. S. 141.

14. Shevchenko N.Iu., Paramonova K.O. Heneratsiia stehokonteineriv dlia pidvyshchennia informatsiinoi bezpeky kanaliv peredachi danykh. «TAK»: telekomunikatsii, avtomatyka, kompiuterno-intehrovani tekhnolohii: zb. dopovidei Vseukr. nauk.-prakt. konf. molodykh vchenykh, 1-2 hrudnia 2021 r. DVNZ «DonNTU; vidp. red. M.V. Stupak. Pokrovsk: DVNZ «DonNTU», 2021. S. 4–6.

Liudmyla Nechvoloda **Людмила Нечволода**	PhD, Associate Professor of the Department of Intelligent Systems of Decision Making, Donbas State Engineering Academy, Ternopil, Ukraine e-mail: lylyne4v@gmail.com https://orcid.org/0000-0002-7584-6735 ResearcherID: HPB-8625-2023	кандидат технічних наук, доцент кафедри інтелектуальних систем прийняття рішень, Донбаська державна машинобудівна академія, Тернопіль, Україна.
Kateryna Krykunenko **Катерина Крикуненко**	Assistant of the Department of Intelligent Systems of Decision Making, Donbas State Engineering Academy, Ternopil, Ukraine e-mail: ladybabenko87@ukr.net https://orcid.org/0000-0003-1530-216X	асистент кафедри інтелектуальних систем прийняття рішень, Донбаська державна машинобудівна академія, Тернопіль, Україна.
Katerina Paramonova **Катерина Парамонова**	Master of specialty «Information systems and technologies», Donbas State Engineering Academy, Ternopil, Ukraine e-mail: ekaterinaparamonova5230@gmail.com	магістр спеціальності «Інформаційні системи та технології», Донбаська державна машинобудівна академія, Тернопіль, Україна.