dated December 17, 2010 no. 1897 “On approval of the federal state educational standard of basic general education”]. Available at: http://www.edu.ru/db-mon/mo/Data/d_10/m1897.html (accessed 28.03.2019).

10. *Prikaz Minobrnauki Rossii ot 29 dekabrya 2014 g. № 1644 «O vnesenii izmeneniy v federalnyy gosudarstvennyy obrazovatelnyy standart osnovnogo obshchego obrazovaniya, utverzhdyonnyy prikazom Ministerstva obrazovaniya i nauki Rossiyskoy Federatsii ot 17 dekabrya 2010 g. № 1897»* [Order of the Ministry of Education and Science of Russia of December 29, 2014 No. 1644 “On Amendments to the Federal State Educational Standard of Basic General Education, approved by Order of the Ministry of Education and Science of the Russian Federation of December 17, 2010 no. 1897]. Available at: http://minobrnauki.rf/dokumenty/543 (accessed 28.03.2019).

11. Semakin I. G. *Avtorskaya masterskaya* [The Author's online-workshop]. Available at: http://lbz.ru/metodist/authors/informatika/2/ (accessed 27.02.2019).

12. Smirnova M. O., Kuznetsova V. Yu. Proektnaya deyatelnost pri izuchenii kriptografii v sredney shkole [The project activity at the studing of cryptography in the second school]. *Proektnaya deyatelnost: novyy vzglyad na obrazovanie : sbornik trudov Vserossiyskoy nauchno-prakticheskoy konferentsii* [Project activity: a new look at education: a collection of works of the All-Russian scientific-practical conference]. Astrakhan, Astrakhan State University, Publishing House “Astrakhan University”], 2018, pp. 212–216.

13. Tanova E. V. *Formirovanie kompetentnosti v oblasti zashchity informatsii u shkolnikov v processe obucheniya informatike* [Formation of competence in the field of information security among schoolchildren in the process of teaching computer science]. Chelyabinsk, Chelyabinsk State Pedagogical University, 2005.

14. Tanova E. V. *Vvedenie v kriptografiyu: kak zashchitit svoe pismo ot lyubopytnykh: uchebnoe posobie* [Introduction to cryptography: how to protect your letter from the curious: study guide]. Moscow, Binom. Laboratoriya znaniy Publ., 2007. 173 p.

15. *Federalnyy gosudarstvennyy obrazovatelnyy standart osnovnogo obshchego obrazovaniya (5–9 kl.)* [Federal State Educational Standard of Basic General Education (5–9 cl.)]. Available at: http://www.edu.ru/db-mon/mo/Data/d_10/prm1897-1.pdf (accessed 05.05.2019).

16. Maykulov Zh. Zh. Prestupleniya protiv detey s ispolzovaniem Interneta [The crimes against children using the Internet]. *Kontsept : nauchno-metodicheskiy elektronnyy zhurnal* [Concept : scientific-methodical electronic journal], 2017, vol. 39, pp. 2636–2640. Available at: http://e-koncept.ru/2017/970854.htm.

УДК 004.422

IDENTIFICATION OF PERSONALITY BASED ON ELECTRONIC DOCUMENTS WITH INCREASED SECURITY LEVEL

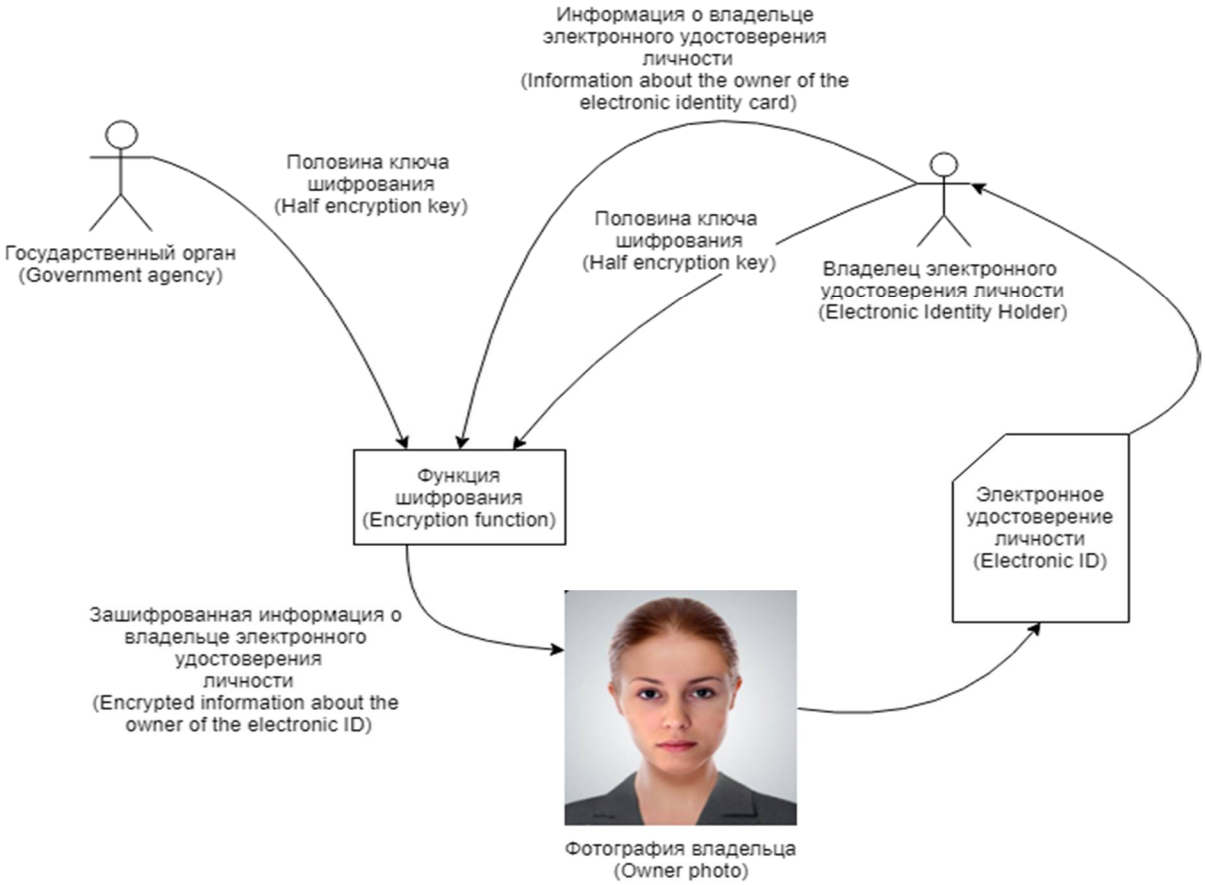
The article was received by editorial board on 22.03.2019, in the final version – 31.05.2019.

Azhmukhamedov Iskandar M., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
Doct. Sci. (Engineering), Professor, e-mail: iskander_agm@mail.ru
Poletayev Nikita S., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
student, e-mail: npoletaev97@gmail.com
Stanishevskaya Alina V., Astrakhan State Technical University, 16 Tatishchev St., Astrakhan, 414056, Russian Federation,
undergraduate student, e-mail: a.stanishevskaia@gmail.com

Identity documents play a big role in ensuring personal and public safety. However, the most widely used paper documents today have significant drawbacks. To eliminate them, a technique has been proposed that involves the combined use of steganographic and cryptographic algorithms. This paper describes approaches to the implementation of software that allows in practice to implement this technique. There are three main modules in the software: data encryption module; steganographic data embedding module in the image; a module for recording generated data on a smart card. Using the developed software allows you to get an identity document with a high level of protection from attacks on its integrity and the inability to use third parties, because without knowing the key, part of which is known only to the owner, and the other part is stored in the database of the public authority, it is impossible to decipher the embedded information.

Keywords: electronic identification card, robust steganography algorithm, data flow diagram, cryptography, steganography

Graphical annotation (Графическая аннотация)



УДОСТОВЕРЕНИЕ ЛИЧНОСТИ НА ОСНОВЕ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ С ПОВЫШЕННЫМ УРОВНЕМ ЗАЩИЩЁННОСТИ

Статья поступила в редакцию 22.03.2019, в окончательной варианте – 31.05.2019.

Ажмухамедов Искандар Маратович, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
доктор технических наук, профессор, e-mail: iskander_agm@mail.ru
Полетаев Никита Сергеевич, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
студент, e-mail: npoletaev97@gmail.com
Станишевская Алина Владимировна, Астраханский государственный технический университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 16,
магистрант, e-mail: a.stanishevskaia@gmail.com

Документы, удостоверяющие личность, играют большую роль в обеспечении личной и общественной безопасности. Однако наиболее широко используемые в настоящее время бумажные документы обладают рядом существенных недостатков. Для их устранения ранее была предложена методика, предусматривающая совместное использование стеганографических и криптографических алгоритмов. В данной работе описываются подходы к реализации программного обеспечения, позволяющего на практике реализовать указанную методику. В программном обеспечении присутствует три основных модуля: модуль шифрования данных; модуль стеганографического внедрения данных в изображение; модуль записи сформированных данных на смарт-карту. Использование разработанного программного обеспечения позволяет получить документ, удостоверяющий личность, с повышенным уровнем защищённости от атак на его целостность и невозможностью использования третьими лицами, так как без знания ключа, часть которого известна лишь владельцу, а другая часть хранится в базе данных государственного органа, невозможно расшифровать внедрённую информацию.

Ключевые слова: электронное удостоверение личности, робастный стеганографический алгоритм, диаграмма потоков данных, криптография, стеганография

Introduction. Identity documents of the owner have always played a big role in the public and private security provision [6]. Such documents are also given to employees in enterprises for the organization of access control. Now paper versions of such documents are still widely used. However, they have a number of significant drawbacks:

- such certificates are more subject to mechanical stress than electronic documents (for example, even short-term contact with water may result the information contained on the paper in an unreadable state);
- paper document can be forged, passed on intruder;
- it is impossible to ensure the safe storage of the document holder's personal data (PD), because they are stored in open form;
- difficulties in tracking the movement of a document at all stages of its life cycle;
- duration of the document's preparation and approval;
- paper archive has no possibility of access rights to documents flexible management, etc.

The development of technology for the production of identity documents is continuously. Currently, their development is associated with biotechnology [8]. State structures of different countries monitor the development of biometric systems and documents based on them. The result is the creation of the electronic identity documents. In addition to the owner's photo, they contain a microprocessor with its own memory, into which additional information, including biometric parameters, can be recorded. Such documents are introduced by the USA, Germany, Great Britain, Japan, etc. Russia is also developing a similar project [14].

Based on this, the purpose of this work was the development of technology for constructing an electronic identity card (EIC), which would eliminate the shortcomings of the paper identity documents, described above.

Method development. The main task in the creating of any identity document is to ensure the cumulative integrity of the person's identifiable features and personal data specified in the document and the impossibility of counterfeiting or unauthorized alteration after the document is produced. It is also necessary to minimize the possibility of using someone else's document, that could have been lost or stolen by an intruder.

To solve the problem in the creating of electronic identity documents, it seems appropriate to use cryptographic methods and algorithms based on steganography.

The cryptographic and steganographic transformations used in the aggregate make it possible to provide the necessary qualities of identity documents.

The main idea when creating an EIC is as follows: some information is selected (last name, first name, patronymic, date of birth, etc.) that needs to be embedded in the owner's photo, and the owner's photo itself, which will be a container for embedded information. After determining the input data, the information is encrypted, and the encryption key is divided into two parts. One of which belongs to the owner of the document, and the other – to the public authority. The figure 1 below shows schematically the main idea of creating an EIC by embedding information in a person's photo.

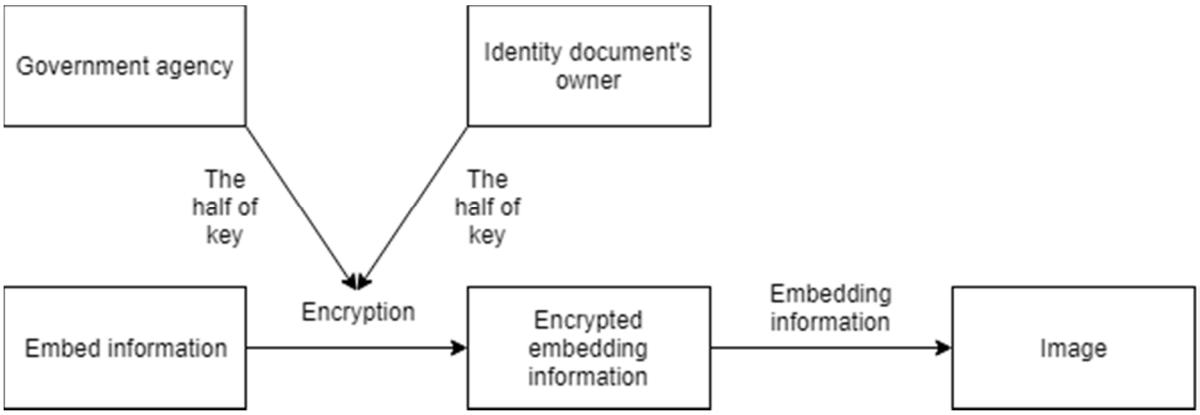


Figure 1 – The scheme of creating EIC

The EIC test takes place in several stages. First, we need to extract information from the image. We need to decrypt the received information because the information is encrypted. To do this, we need to connect the two halves of the encryption key and perform the decryption. The scheme of verification of EIC is shown in the figure 2.

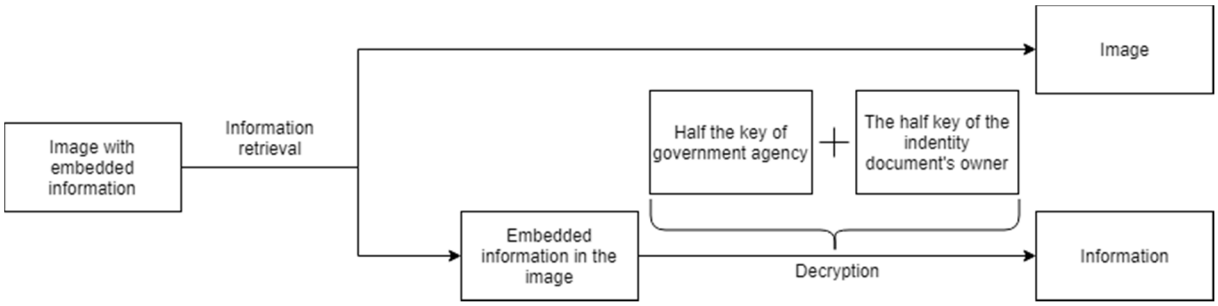


Figure 2 – The scheme of EIC test

A scheme to produce an autonomous electronic identity card (EIC) based on steganographic and cryptographic algorithms, which makes it possible to create a qualitatively new identification system with an elevated level of security was proposed in [3]. An algorithm of digital steganography with data encryption [2], which allows solving the main task in the manufacture of an identity document - ensuring the cumulative integrity of the person's identifying features and personal data specified in the document was also developed.

The proposed algorithm allows to embed data into a graphic file, including those was compressed with the JPEG standard. During embedding data, the algorithm works with images whose color depth is 24 bits. Embedding is performed in the blue channel, because the human vision system is least sensitive to it. Let message «M» be a bits sequence of length «N», the number of pixels in the transform domain is «C». Embedded pixels are evenly distributed throughout the image in a pseudo-random manner.

The image or its part bounded by the transformation region is divided into two types of blocks r1 and r2, with r1 = r2 + 1. The blocks number of length r1 and r2 is equal to n1 and n2, respectively. Provided that n1 + n2 = N и (r1 · n1) + (r2 · n2) = C, the values of r1, r2, n1, и n2 are calculated by the following formulas:

(1)

(2)

(3)

(4)

Blocks alternate pseudo-randomly based on the key. Each message bit has its own block in which a pixel is selected that undergoes a change in accordance with the key from key sequence.

Consider the procedure for the formation of a key sequence. The password entered by the user is converted to a 16-byte word using any hashing algorithm. Then three more such words are formed by cyclic permutation. The result is an array of numbers of dimension [128 bits, 4 bits], the columns of which are a pseudo-random sequence of numbers of 128 bits long. Getting the remainder of dividing these numbers by the block length, we calculate the position of the pixel change inside this block.

Each pixel component is described by 8 bits with a color depth of 24 bits. 8 bits are according to one of three color channels - by the number of main colors. Bits with position 4, 5 and 6 are subject to change. The deviation of the color intensity in this case does not exceed 6.3 %, and the total change in pixel brightness does not exceed 1 % [1].

Consider embedding information in an image. The pixel number is selected in which the embedding is performed in accordance with the key in the pixel block. The bit number is determined based on the values of the same block's other pixels. For example, if all the fourth bits from this block are 0 or 1, then the algorithm leaves the fourth bit of this pixel unchanged and proceeds to consider all the fifth bits of this block, etc. If all the fourth, fifth and sixth bits of all pixels from this block are 0 or 1, then 4 bits are given preference. After finding the bit number to be modified, the embedding of secret information occurs. Figure 3 shows a block diagram of a digital steganography algorithm with data encryption.

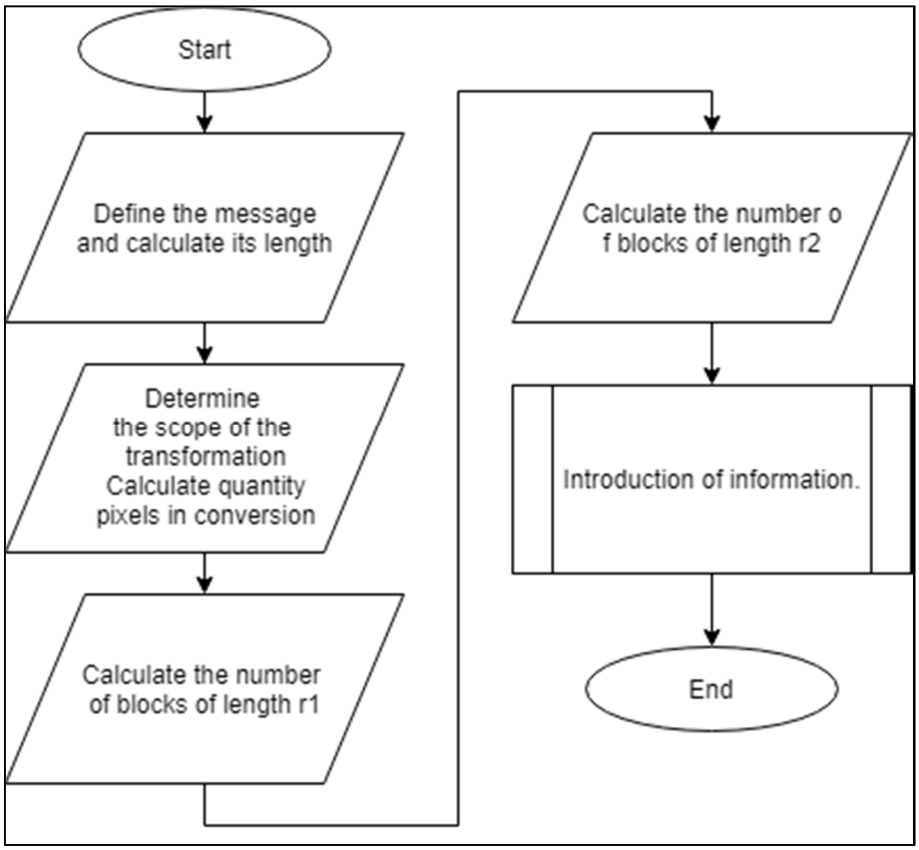


Figure 3 – Block diagram of digital steganography algorithm with data encryption.

As an example, consider the modification of a single image block. Let the block consist of five pixels (fig. 4).

$$
\begin{aligned}
b_1 &= 1\,1\,1\,1\,0\,1\,1\,0\\
b_2 &= 1\,1\,0\,1\,0\,1\,1\,1\\
b_3 &= 1\,0\,1\,1\,0\,0\,0\,0\\
b_4 &= 1\,0\,1\,1\,0\,0\,0\,1\\
b_5 &= 1\,0\,0\,1\,0\,1\,0\,1
\end{aligned}
$$

Figure 4 – Bit representation of the blue channel of one block's pixels

As can be seen from the figure 3, the fourth and fifth bits (in red rectangles) do not satisfy the non-uniformity condition. According to the algorithm, only the sixth bit (in green rectangle) can be modified.

Results. Charts and flowcharts were developed, reflecting the general principles of the program. Below, as an example, is presented the Use Case diagram (fig. 5), which describes the possible behavior of the system during interacting with the administrator. The administrator can select the image to be modified, the data to be recorded. He also chooses an algorithm for encryption. After the administrator has entered the first half of the key and the owner has entered the second half, the data is encrypted. Finally, the administrator writes to the smart card the prepared image with the embedded stego, containing the user's encrypted personal data.

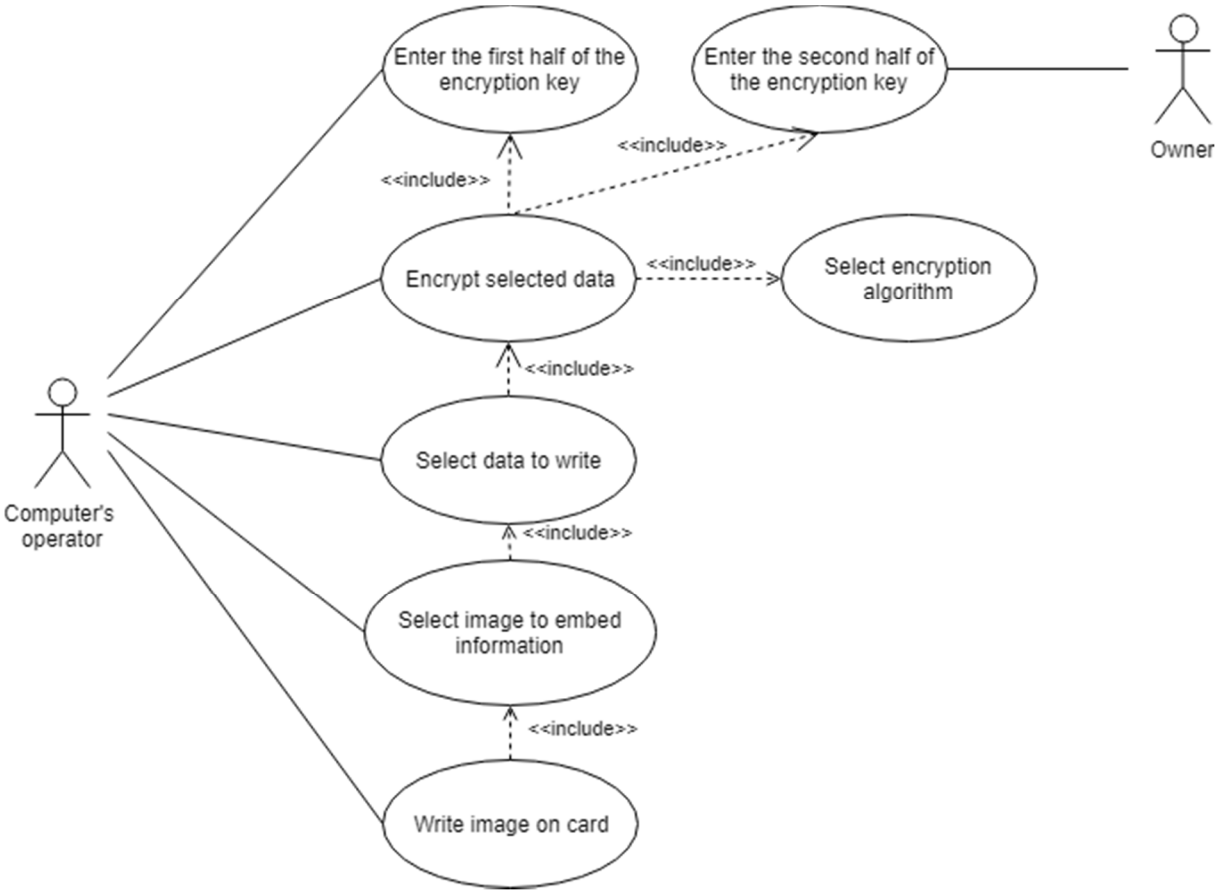


Figure 5 – The Use Case diagram of software to create EIC

Figure 6 shows the data flow diagram. Three modules are involved in the software: data encryption, steganographic embedding of data into an image, and data recording on a smart card.

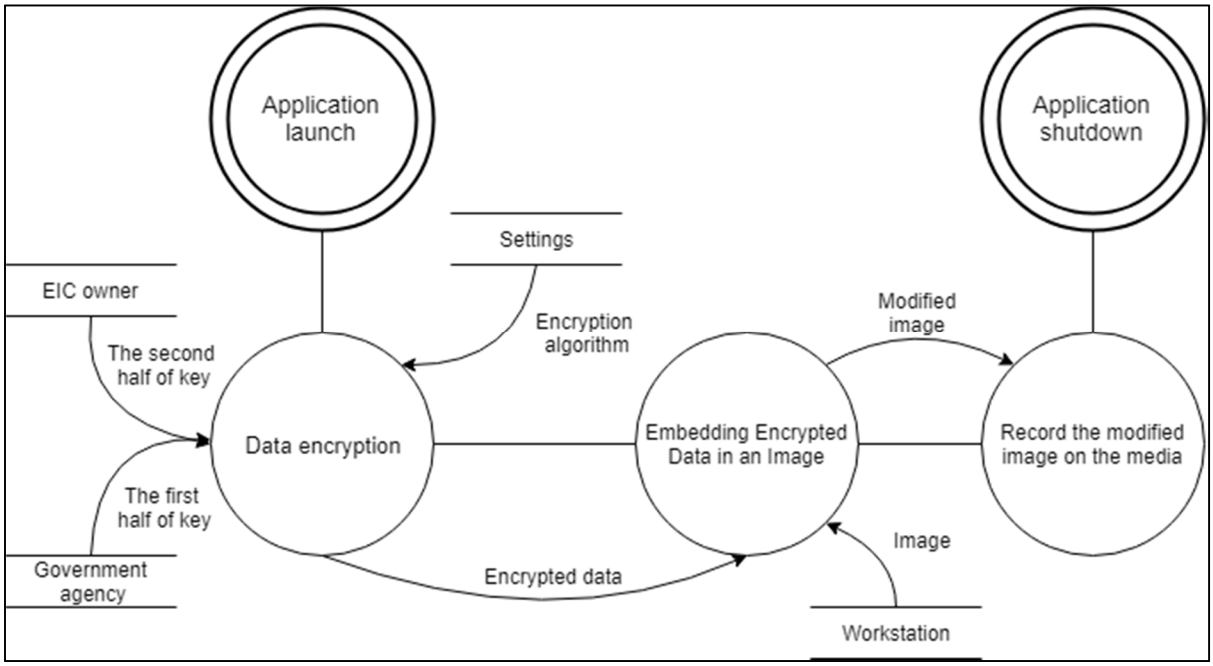


Figure 6 – The software data flow diagram in Yourdon-DeMarco notation for creating an EIC

The block diagram (fig. 7) shows the work of the algorithm for creating an EIC. At the beginning of the program, PlainText, Password, Image, Algorithm variables are declared, in which the data for encryption, the password entered by the user, the image being modified and information about the selected encryption algorithm are written.

The developed software implements the following encryption algorithms: GOST 28147-89 [6], GOST R 34.12-2015 [7], AES [4]. Next, a function is called that performs data encryption. This function has three "overloads" for each encryption algorithm. After performing cryptographic transformations, the program determines the area for stego implementation. Then, the encrypted information is embedded in the image based on the above algorithm, after the data is written to the smart card.

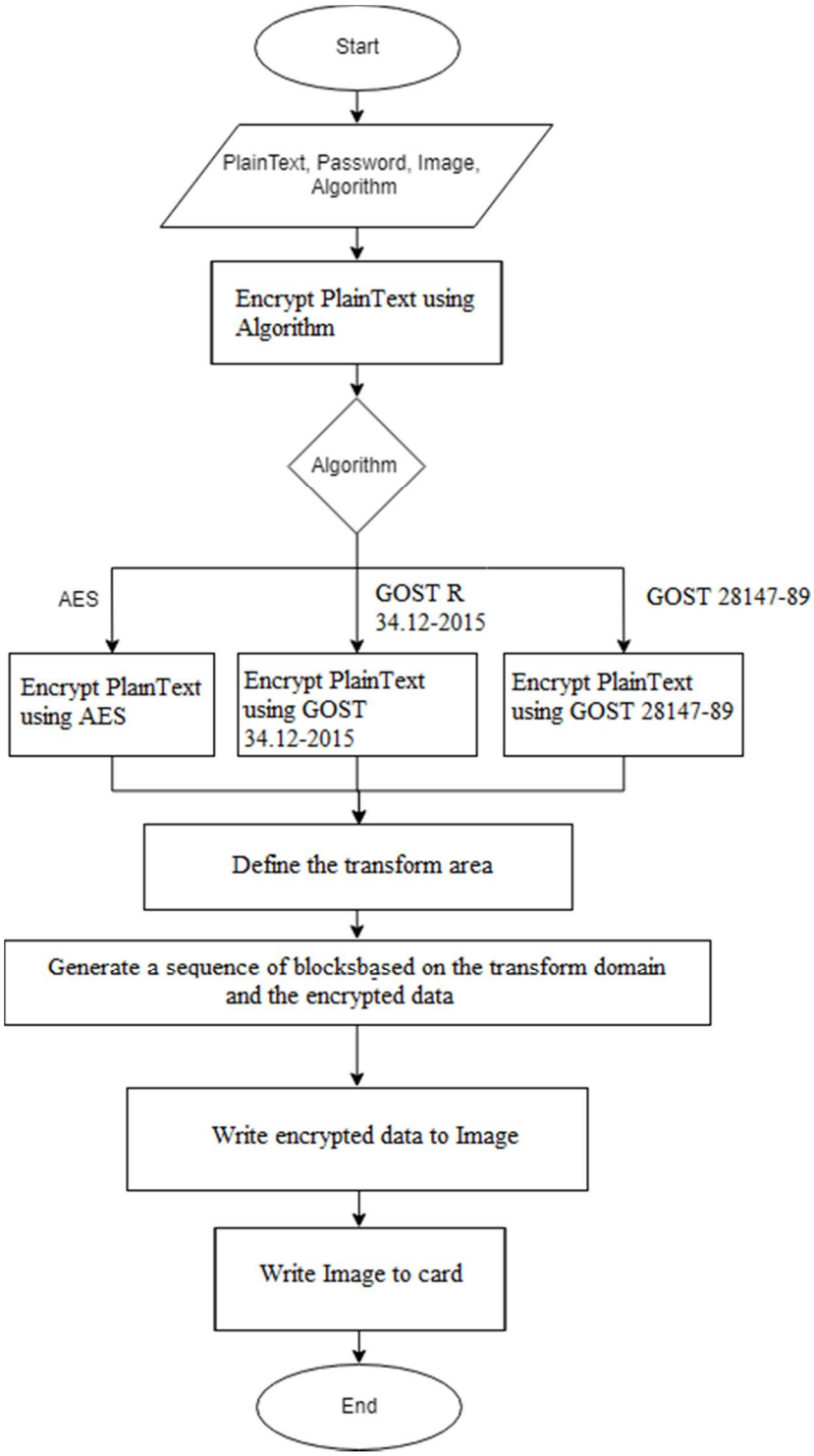


Figure 7 – A block diagram of the software's work to create an electronic identity card [5]

The described software is developed in a high-level programming language - C # because it provides intuitive and convenient desktop development tools.

Figure 8 shows the code for generating a sequence of blocks.

```
public class BlockCreator
{
    public Point StartPoint { get; set; }
    public Point EndPoint { get; set; }

    public BlockCreator(Point startPoint, Point endPoint) {
        StartPoint = startPoint; //Стартовая точка области преобразования
        EndPoint = endPoint; //Конечная точка области преобразования
    }

    public List<int> GenerateBlockList(string encText) {
        int M = (EndPoint.X - StartPoint.X) * (EndPoint.Y - StartPoint.Y); // Область преобразования

        int encTextLength = encText.Length; // Длина сообщения

        int r2 = (M / encTextLength); // Длина блоков 2 типа
        int r1 = r2 + 1; // Длина блоков 1 типа

        int n2 = (r2 + 1) * encTextLength - M; // Количество блоков 2 типа
        int n1 = encTextLength - n2; // Количество блоков 1 типа

        List<int> Blocks = new List<int>();
        for (int i = 0; i < n2; i++) {
            Blocks.Add(r2);
        }
        for (int i = 0; i < n1; i++) {
            Blocks.Add(r1);
        }

        return Blocks;
    }
}
```

Figure 8 – The program code of the class, responsible for generating the sequence of blocks

Consider an example of the information introduction in the photo (PNG format). It is necessary to analyze the numerical representation of the pixels row's the blue channel because the human eye will not be able to see the insignificant changes in the image. A 10x10 pixel transform area and a string to embed were selected – 1110010000011001111010011010000101001111010010100 1. Figure 9 shows the result of the work of program.

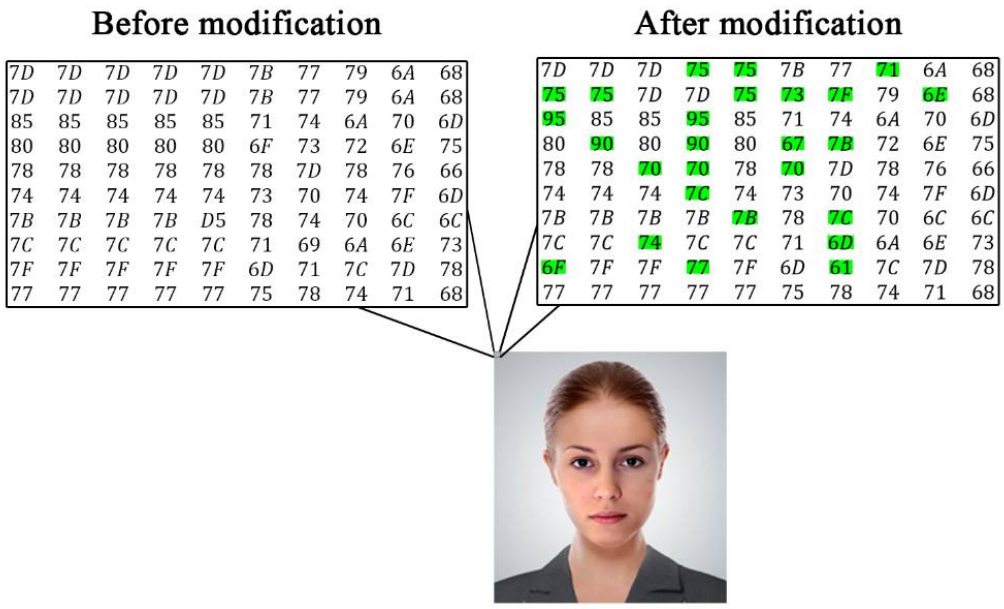


Figure 9 – The results of program work in the fragment of the image

In image 9, the pixels, which have green background, have been changed. The information capacity of the container (image) depends on the image resolution. The size of the transformation area (a place for embedding information) is determined based on the length of the data.

Conclusion. The declared approach to the production of electronic documents allows us to minimize the described shortcomings of paper identity documents. Such a document is protected from attacks on its integrity, since photography and personal data are a single entity. The possibility of using the document by third parties is also minimized, since without knowing the key, part of which is known only to the owner, and the other part is stored in the database of government agency, it is impossible to decrypt the embedded information.

Библиографический список

1. Ажбаев Т. Г. Анализ стойкости современных стеганографических алгоритмов/ Т. Г. Ажбаев, И. М. Ажмухамедов // Вестн. Астраханского гос. техн. ун-та. – 2008. – № 1. – Режим доступа: https://cyberleninka.ru/article/n/analiz-stoykosti-sovremennyh-steganograficheskih-algoritmov, свободный. – Заглавие с экрана. – Яз. рус.

2. Ажбаев Т. Г. Алгоритм цифровой стеганографии с шифрованием данных / Т. Г. Ажбаев, И. М. Ажмухамедов // Вестн. Астраханского гос. техн. ун-та. – 2008. – № 1 (42). – С. 50–55.

3. Ажмухамедов И. М. Электронные удостоверения личности на основе стеганографических и криптографических алгоритмов / И. М. Ажмухамедов // Вестн. Астраханского гос. техн. ун-та. – 2009. – № 2. – С. 49–52.

4. Federal Information Processing Standards Publication 197, AES (Advanced Encryption Standard). – Режим доступа: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf, свободный. – Заглавие с экрана. – Яз. рус.

5. ГОСТ 19.701-90. Единая система программной документации. Схемы алгоритмов, программ, данных и систем. Условные обозначения и правила выполнения. – Режим доступа: http://cert.obninsk.ru/gost/282/282.html, свободный. – Заглавие с экрана. – Яз. рус.

6. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – Режим доступа: http://docs.cntd.ru/document/gost-28147-89, свободный. – Заглавие с экрана. – Яз. рус.

7. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. – Режим доступа: http://wwwold.tc26.ru/standard/gost/GOST_R_3412-2015.pdf, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения 15.05.2019).

8. Гуриев В. Восход Европы: электронные паспорта в России / В. Гуриев. – Режим доступа: http://www.kongord.ru/Index/BigBrother07/e-pass-in-russ.html, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения 15.05.2019).

9. Кириченко Ю. Н. Значение взаимодействия государственных служб Российской Федерации в предупреждении преступлений и правонарушений. Значение перехода на новое удостоверения личности / Ю. Н. Кириченко, А. В. Медведев. – Режим доступа: https://cyberleninka.ru/article/v/znachenie-vzaimodeystviya-gosudarstvennyh-sluzhb-rossiyskoy-federatsii-v-preduprezhdenii-prestupleniy-i-pravonarusheniy-znachenie, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения 15.05.2019).

10. Клак Н. Н. Проблема идентификации человека / Н. Н. Клак. – Режим доступа: https://cyberleninka.ru/article/v/problema-identifikatsii-cheloveka, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения 15.05.2019).

11. Skiena S. Steven. The Algorithm Design Manual / Skiena S. Steven. – Режим доступа: http://mimoza.marmara.edu.tr/~msakalli/cse706_12/SkienaTheAlgorithmDesignManual.pdf, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения 15.05.2019).

12. Stephen Cleary. Concurrency in C# Cookbook: Asynchronous, Parallel, and Multithreaded Programming 1st / Stephen Cleary. – Режим доступа: http://cdn.oreillystatic.com/oreilly/booksamplers/9781449367565_sampler.pdf, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения 15.05.2019).

13. Andrew Troelsen. C# 6.0 and the .NET 4.6 Framework (7th Edition) / Andrew Troelsen, Philip Japikse. – Режим доступа: https://vk.com/doc2036633_459501322?hash=3cd572dcf4edcaf039&dl=3e1d4845790a76d3e7, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения 15.05.2019).

14. Указ Президента Российской Федерации от 29 декабря 2012 № 1709 «Об основных документах, удостоверяющих личность гражданина РоссийскойФедерации за пределами территории Российской Федерации, содержащих электронные носители информации».

References

1. Azhbaev T. G., Azhmukhamedov I. M. Analiz stoykosti sovremennykh steganograficheskikh algoritmov [Analysis of the persistence of modern steganographic algorithms]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta* [Bulletin of Astrakhan State Technical University], 2008, no. 1. Available at: https://cyberleninka.ru/article/n/analiz-stoykosti-sovremennyh-steganograficheskih-algoritmov

2. Azhbaev T. G., Azhmukhamedov I. M. Algoritm tsifrovoy steganografii s shifrovaniyem dannykh [Digital steganography algorithm with data encryption]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta* [Bulletin of Astrakhan State Technical University], 2008, no. 1 (42), pp. 50–55.

3. Azhmukhamedov I. M. Elektronnyye udostovereniya lichnosti na osnove steganograficheskikh i kriptograficheskikh algoritmov [Electronic identity cards based on steganographic and cryptographic algorithms]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta* [Bulletin of Astrakhan State Technical University], 2009, no. 2, pp. 49–52.

4. *Federal Information Processing Standards Publication 197, AES (Advanced Encryption Standard).* Available at: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf

5. *GOST 19.701-90. Yedinaya sistema programmnoy dokumentatsii. Skhemy algoritmov, programm, dannykh i sistem. Uslovnye oboznacheniya i pravila vypolneniya* [GOST 19.701-90. Unified system for program documentation. Data, program and system flowcharts, program network charts and system resources charts. Documentation symbols and conventions for flowcharting]. Available at: http://cert.obninsk.ru/gost/282/282.html

6. *GOST 28147-89. Sistemy obrabotki informatsii. Zashchita kriptograficheskaya. Algoritm kriptograficheskogo preobrazovaniya* [Information processing systems. Cryptographic protection. Algorithm of cryptographic transformation]. Available at: http://docs.cntd.ru/document/gost-28147-89

7. *GOST R 34.12-2015. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Blochnyye shifry* [Information technology. Cryptographic protection of information. Block ciphers]. Available at: http://wwwold.tc26.ru/standard/gost/GOST_R_3412-2015.pdf (accessed 15.05.2019).

8. Guriyev V. Voskhod Yevropy: elektronnyye pasporta v Rossii [The Rise of Europe: Electronic Passports in Russia]. Available at: http://www.kongord.ru/Index/BigBrother07/e-pass-in-russ.html (accessed 15.05.2019).

9. Kirichenko Yu. N., Medvedev A. V. *Znacheniye vzaimodeystviya gosudarstvennykh sluzhb Rossiyskoy Federatsii v preduprezhdenii prestupleniy i pravonarusheniy. Znacheniye perekhoda na novoye udostovereniye lichnosti* [The value of the interaction of public services of the Russian Federation in the prevention of crimes and offenses. The value of the transition to a new identity card]. Available at: https://cyberleninka.ru/article/v/znachenie-vzaimodeystviya-gosudarstvennyh-sluzhb-rossiyskoy-federatsii-v-preduprezhdenii-prestupleniy-i-pravonarusheniy-znachenie (accessed 15.05.2019).

10. Klak N. N. *Problema identifikatsii cheloveka* [Problem of human identification]. Available at: https://cyberleninka.ru/article/v/problema-identifikatsii-cheloveka (accessed 15.05.2019).

11. Skiena S Steven. *The Algorithm Design Manual.* Available at: http://mimoza.marmara.edu.tr/~msakalli/cse706_12/SkienaTheAlgorithmDesignManual.pdf (accessed 15.05.2019).

12. Stephen Cleary. *Concurrency in C# Cookbook: Asynchronous, Parallel, and Multithreaded Programming 1st.* Available at: http://cdn.oreillystatic.com/oreilly/booksamplers/9781449367565_sampler.pdf (accessed 15.05.2019).

13. Andrew Troelsen, Philip Japikse. *C# 6.0 and the .NET 4.6 Framework (7th Edition).* Available at: https://vk.com/doc2036633_459501322?hash=3cd572dcf4edcaf039&dl=3e1d4845790a76d3e7 (accessed 15.05.2019).

14. *Ukaz Prezidenta Rossiyskoy Federatsii ot 29 dekabrya 2012 № 1709 «Ob osnovnykh dokumentakh, udostoveryayushchikh lichnost' grazhdanina Rossiyskoy Federatsii za predelami territorii Rossiyskoy Federatsii, soderzhashchikh elektronnyye nositeli informatsii»* [Decree of the President of the Russian Federation of December 29, 2012 no. 1709 "On the main documents proving the identity of a citizen of the Russian Federation outside the territory of the Russian Federation, containing electronic media"]. Available at: http://www.consultant.ru/document/cons_doc_LAW_140171/ (accessed 15.05.2019).