УДК 004.056.55

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ МЕТОДОМ СТЕГАНОГРАФИИ

Головченко О. Н.

магистрант

Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова

Новочеркасск, Россия

Оганян Р. Г.

аспирант

Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова

Новочеркасск, Россия

Аннотация

В данной статье осуществлена программная разработка метода криптографической защиты с помощью стеганографии. Описываются основные понятия стенографии, а также принцип работы.

Ключевые слова: криптографическая защита, стенография, шифрование, криптография.

SOFTWARE IMPLEMENTATION OF CRYPTOGRAPHIC PROTECTION BY THE STEGANOGRAPHY METHOD

Golovchenko O.N.

master student

South-Russian State Polytechnic University (NPI)

Novocherkassk, Russia

Oganyan R.G.
graduate student
South-Russian State Polytechnic University (NPI)
Novocherkassk, Russia

Abstract
This article carried out the software development of a method of cryptographic protection using steganography. It describes the basic concepts of shorthand, as well as the principle of operation.
Key words: cryptographic protection, shorthand, encryption, cryptography.

Shorthand is a cryptographic add-on that protects information. Steganographic system (stegosystem) - the combination of methods and tools used to create a hidden channel for transmitting information.

The principle of shorthand is to scatter the secret text in the main message array, which can even be excellent in meaning. In this case, it will be possible to extract it, only knowing the principle by which the breakdown and dispersion was made.

The following is the software development of shorthand.

This program demonstrates the implementation of the LSB method for encrypting / decrypting the bmp file. The program interface is shown in Figure 1, which will encode the text into a picture. In the upper left corner there is a button for calling the file selection window (in this case, a picture) and an area for displaying the selected picture. Below, below it, is the area for entering the key-string, to protect the encrypted information from unauthorized access. The user clicks the "Browse" button and opens the image selected to encode the information.

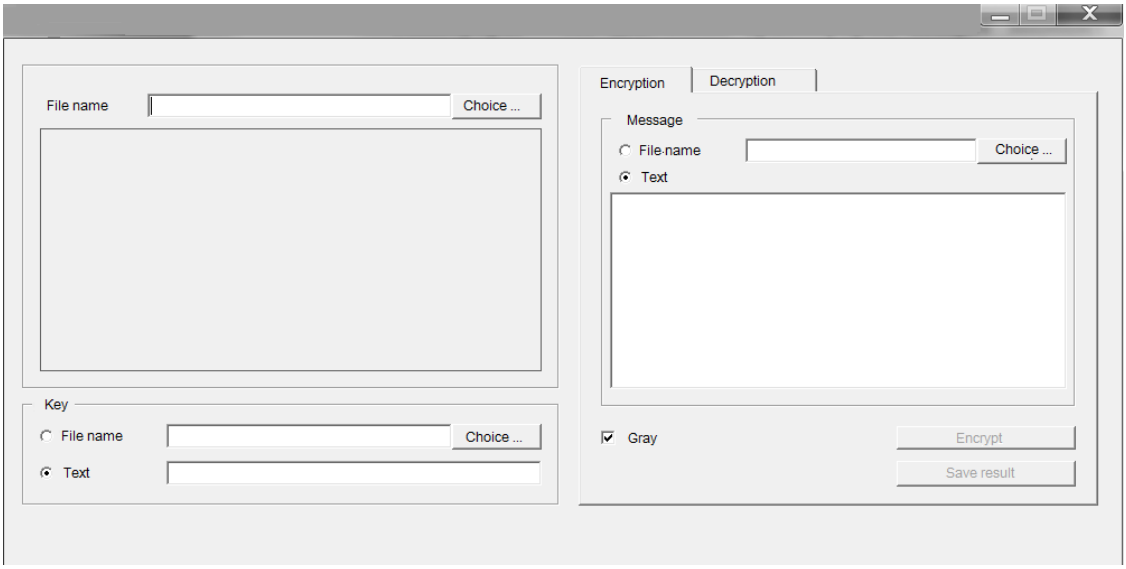

Fig.1 - Main window

The user enters (or downloads from the text file) the key-text that will be requested when decrypting, i.e. only knowing that key can decipher the picture.

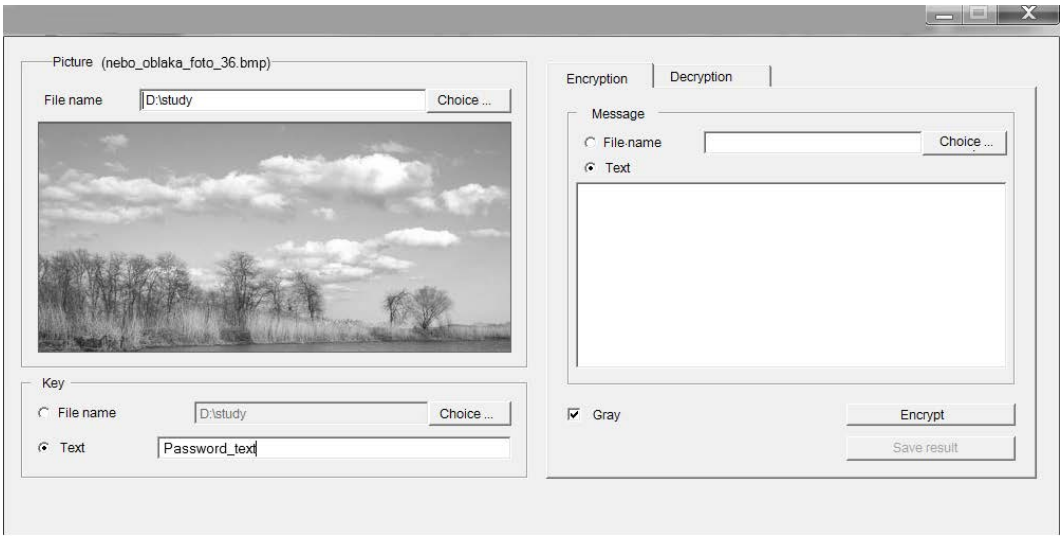

Fig.2 - Picture selection and key-text input

The next area of the user window is located on the right side of the window and consists of two tabs. The first tab is used to enter a message (or download from a text file) that needs to be encrypted into a picture (Figure 3).

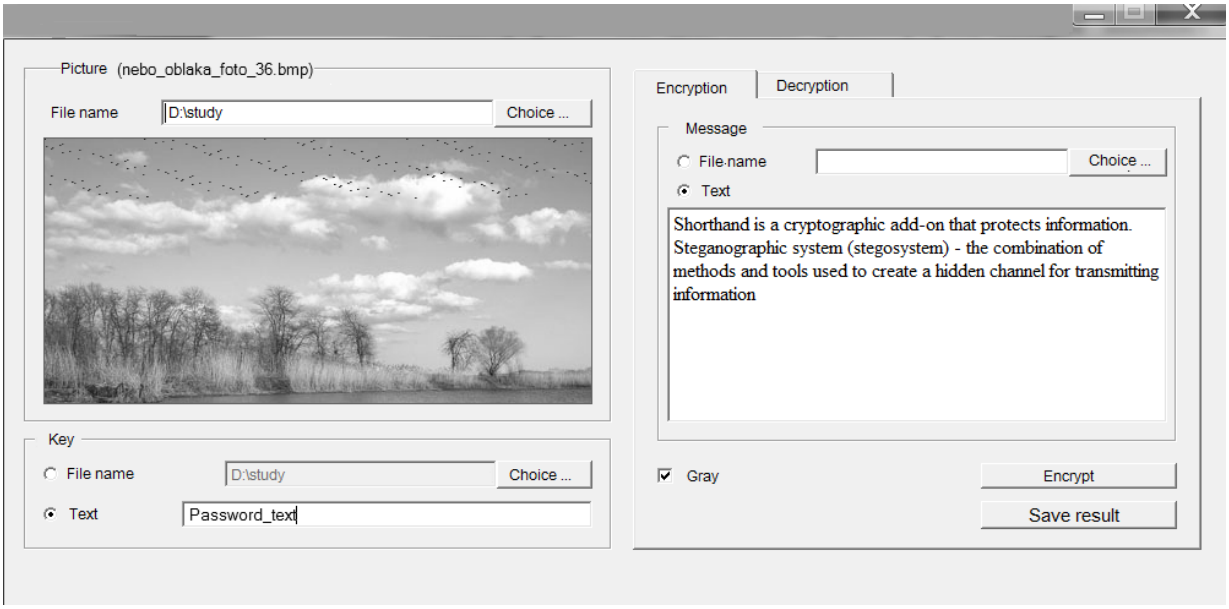

Fig.3 - Text Encryption

Then follows the opposite action. By clicking the "Decrypt" button, the user receives the original message (you can also save the message received when decrypting it to a text file) This process is shown in Figure 4.

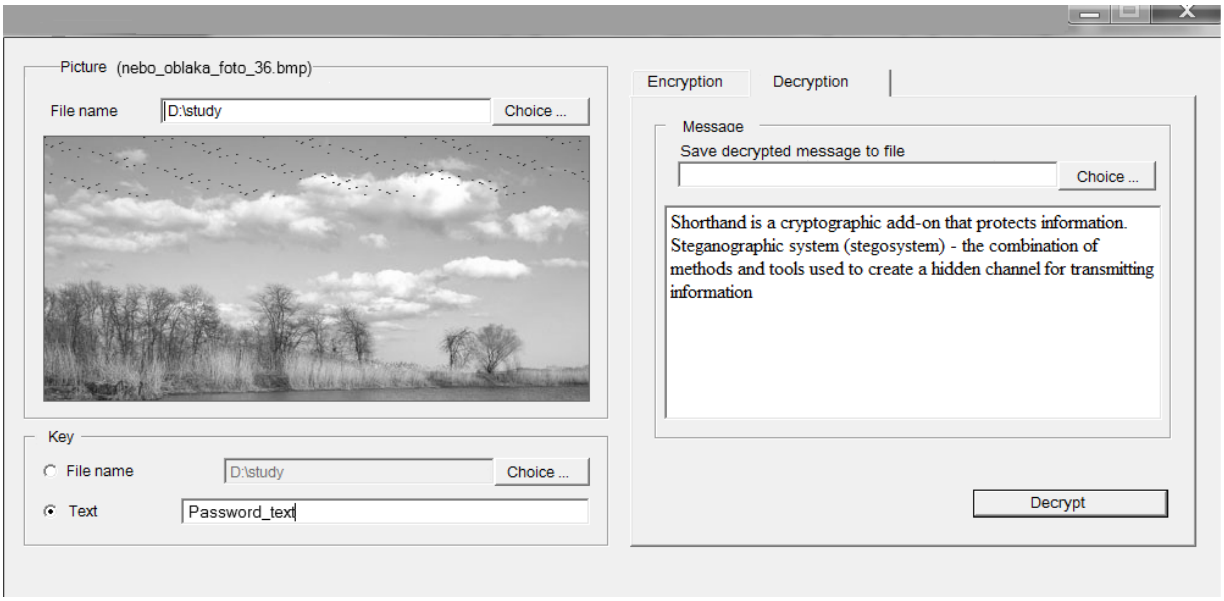

Fig.4 - Text Decryption

Thus, information was added to the selected picture, as well as the removal of previously hidden information from the selected picture. Information hidden by shorthand has less chance of revealing the fact that the content of the message has been transferred. And message encryption provides additional protection.

References

1. Steganography [Electronic resource]. - Access Mode: https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B5%D0%B3%D0%B0%D0%B3% D0% B0% D0% B3% D1 % 80% D0% B0% D1% 84% D0% B8% D1% 8F (circulation date 12/20/2018).

Оригинальность 90%