UDC 004.021

DESIGNING THE GRAPHIC INTERFACE OF THE SYSTEM FOR COVERING INFORMATION BASED ON DISCRETE TRANSFORMATIONS BY MEANS OF KOH AND ZHAO ALGORITHM

KLAUDZIYA STANKEVICH, DMITRY PASTUKHOV
Polotsk State University, Belarus

This article discusses the design of a graphical interface system for hiding information based on discrete transformations using the Koch and Zhao algorithm. The degree of suitability of the container for modification, modeling attacks and determining resistance to them have been analyzed.

The development of computer technology in the last decade has given a new impetus to the development of computer steganography. There are many new applications. Messages are now embedded in digital data, usually having an analog nature.

The program interface must have a number of properties: naturalness, consistency, friendliness, the principle of 'feedback', simplicity, flexibility, aesthetic appeal.

Any application should be properly designed and divided into separate modules, which should be relatively independent of each other. This separation greatly facilitates not only the implementation of the application, but also its possible modifications. This is the principle of object-oriented programming modularity.

The application "KochZhao" is an application to hide information in images. To hide the message, you will need to select the container (supported formats: bmp and png), select the hidden file and specify the settings: P and the size of the segments (blocks).

For further extraction of the message it is necessary to remember the key, which will be displayed in the corresponding field, and the size of segments (blocks).

To determine the optimal container, we will use different images with predominance of one RGB color component.

As a result, it was found that the most suitable for the container are images with the predominance of blue and green components.

To determine the stability of the steganosystem, several types of attacks (passive intruder, active intruder) have been carried out.

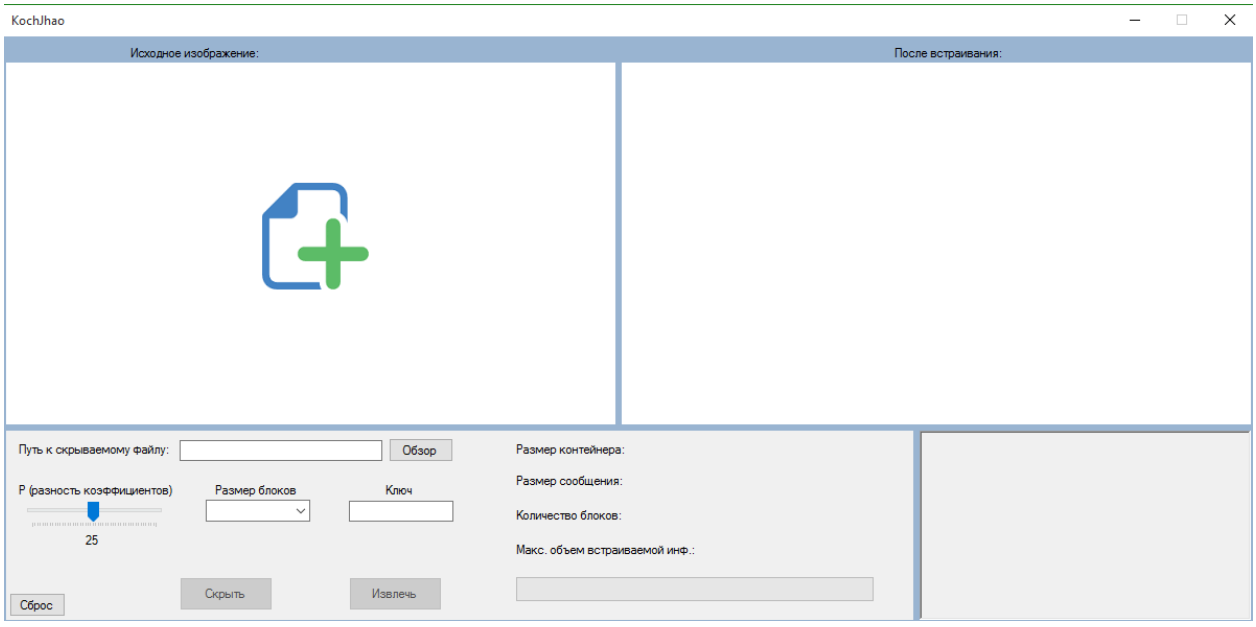

Figure 1. – Program interface

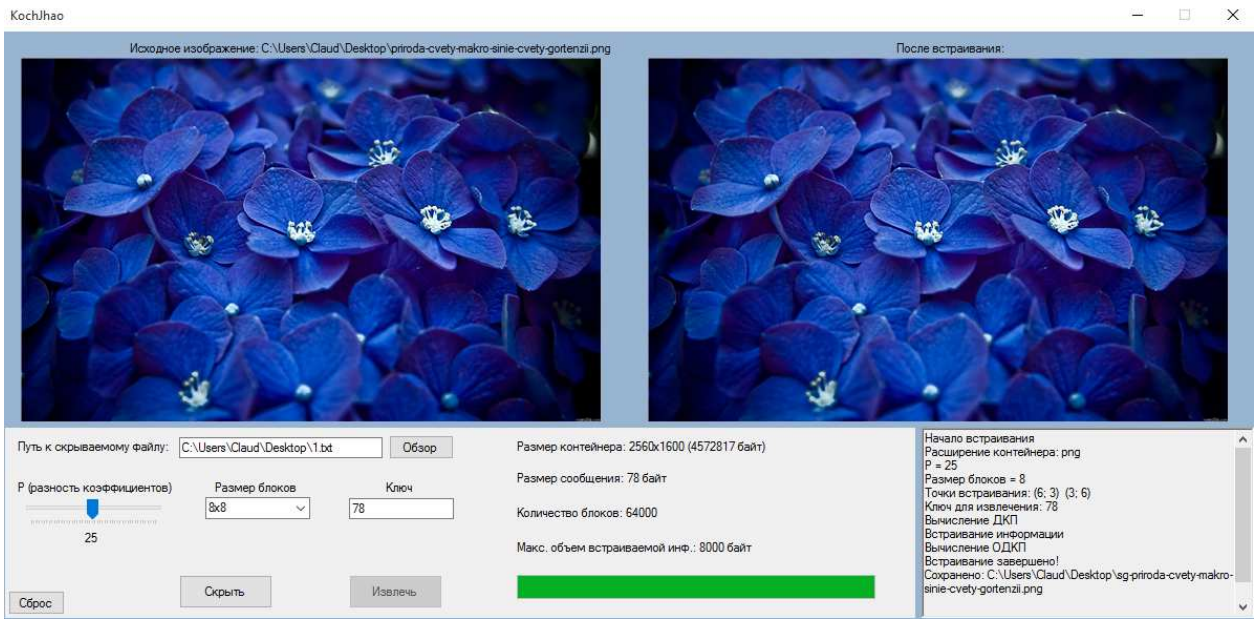

Figure 2. – Encryption interface

A passive attack is an attack when the enemy is not able to modify the transmitted messages and insert its messages into the information channel between the sender and the recipient. The purpose of a passive attack can only be listening to the transmitted messages and traffic analysis.

An active attack is an attack when the enemy has the ability to modify the transmitted messages and insert its messages. There are the following types of active attacks:

– denial of service DoS-attack (Denial of Service);
– modification of the data stream;
– the creation of a false stream (falsification);
– reusability.

When trying to determine the presence of a hidden message in the container, using the function of Adobe Photoshop channel levels, it was noticed that some pixels had a blue channel, which indicates the presence of a hidden message.

During active attacks it was revealed that the algorithm is resistant to most known steganacin, including attack, compression, affine transformation, geometric attacks.

As a result, the tests found out the following:

– change the color of the model before the DKT has significantly worsened the result of the ratio signal/noise;
– embedding in the high frequency region of the spectrum slightly improved the result;
– embedding in the low-frequency region of the spectrum has significantly worsened the result, reduced resistance to compression;
– reducing the block to the 4x4 dimension slightly improved the result, reducing the compression resistance;
– embedding 2 bits per unit in midrange and high-frequency region improved result.

REFERENCES

1. Матюшик, В.Н. Методы и средства стеганографии для защиты графических образов / В.Н. Матюшик. – Минск : БГУиР. – Минск, 2004. – 169 с.
2. Грибунин, В.Г. Цифровая Стеганография / В.Г. Грибунин. – М., 2003. – 15 с.
3. Конахович, Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – Киев : МК-Пресс, 2006. – 207 с.