Studying of Stability of the Information Hiding Methods in Still Images

Andriy Astrakhantsev, Oleksiy Doroghan, Oleksandr Poponin, Nataliya Shostak

Abstract – **In this paper, the comparative analysis of the two information hiding methods (LSB and Kutter) characteristics is presented. We analyzed the resistance to intentional attacks and noise in the communication channel.**

Keywords – **Steganography, Hiding information, LSB, Kutter method.**

I. Introduction

Steganography – hiding (by embedding) messages in the digital data, such as speech, image, audio or video, text files. The advantage of steganography to cryptographically protect information is provided that hides the very existence of your confidential information during transmission, storage or processing. From a practical point of view, using steganography in audio and images is most interesting. The most widely used methods of embedding the digital watermark to verify the copyright.

II. Basic Methods Hiding Information

Now widely used method of replacing the least significant bit, because it is simple to implement, allows to hide large amounts of information with little changes in image quality container [1]. The method consists in replacing the bits in the RGB-encoded bits to hide sensitive messages. The disadvantage of this method is very low resistance to the effects of the image container.

To change the method of least significant bit (LSB) investigated the characteristics of stegosystem as for embedding information in the LSB, and for embedding in the second, third, fourth and fifth bits. The results show that the image quality and signal/noise ratio (SNR) did not change significantly when embedding in two least significant bits, which allows you to duplicate the second bit of embedded information, and improve stability of the method to attack.

Also, for the method was evaluated by LSB probability of erroneous reception stego on the background of additive noise in the communication channel.

At second researched the method Kutter, announced good results in resistance. Embedding is performed in the blue channel, since the blue color of human visual system is the least sensitive. Secret bits (s_i) embedded in the blue channel by modifying the brightness:

$$l(p) = 0{,}299r(p) + 0{,}587g(p) + 0{,}114b(p), \quad \ldots\ldots\ldots \quad (1)$$

$$b'(p) = \begin{cases} b(p) - ql(p), & \text{if } s_i = 0, \\ b(p) + ql(p), & \text{if } s_i = 1. \end{cases} \quad \ldots\ldots\ldots \quad (2)$$

where q – ratio of energy embedded information.

We obtained the characteristics of stegosystem depending on coefficient of embedding energy. A plot of normalized average absolute difference (NAD) (3) on the energy of embedding is shown in Fig. 1.

Andriy Astrakhantsev, Oleksiy Doroghan, Oleksandr Poponin, Nataliya Shostak – Kharkiv National University of Radioelectronics, Lenina Av., 14, Kharkiv, 61166, UKRAINE, E-mail: astrahkture@mail.ru

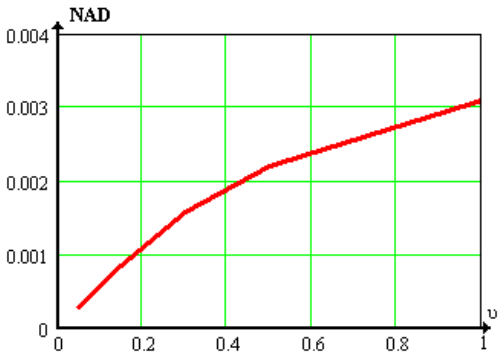

Fig.1 The dependence of the NAD from the energy of embedding

$$NAD = \sum_{x,y} \left| C_{x,y} - S_{x,y} \right| \Big/ \sum_{x,y} \left| C_{x,y} \right|. \quad (3)$$

The presented ratios through $C_{x,y}$ denotes pixel empty container with coordinates (x,y), and by $S_{x,y}$ – the pixel-filled container.

In the method for increasing the stability Kutter can be used to hide the concealed information rote. After analyzing Fig. 2 can be determined that up to 5 repetitions of embedded bits slightly decrease the signal/noise ratio (SNR), with more repetitions SNR noticeably worse.

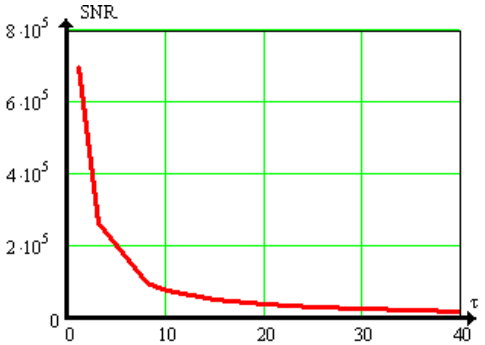

Fig.2 The dependence of the SNR from the number of re-embedding

III. Conclusion

In this paper, the comparative analysis of the two information hiding methods (LSB and Kutter) characteristics is presented. Also we obtained values SNR depending on the number of re-embedding and embedding energy; analyzed the resistance to intentional attacks and noise in the communication channel.

References

[1] V.F. Konahovich, A.J. Puzyrenko, "Computer steganography. Theory and Practice" – *Kiev: MC Press*, 2006. – 288.