UDC 004.056

Bekirov A. E, Dumansky M. V., Triphonenko K.Y., Kutya N.V.

THE WAYS OF AN ENCREASING OF SAFETY OF INFORMATION RESOURCES IN APPLICATION-SPECIFIC SYSTEMS

Paper discusses ways for the improvement of the information security of the information resources in video conferencing systems of automated control systems for special purposes of the Ministry of Defence. The groups of indicators of the quality of steganographic techniques are determined. On the basis of formulated requirements, existing steganographic algorithm of embedding information in an image container was analyzed.

Keywords: *steganography, quality indicators, resistance, algorithm of embedding.*

Introduction

Wide dissemination and development of telecommunication networks on-going application in various fields of human activity. There is also the question of introduction of modern telecommunication systems in special purpose automated control systems for the Ministry of Defense. One of the possible implementation of the rapid exchange of information in the Ministry of Defence is Xia videoconference. Use of this type of connection has the advantages of reduced time exchange of information between the abonents, as close as it is possible to the actual modalities for the exchange of information, thus enabling the transfer of additional information in the channels of transmission of video data and a reduction in the time required for management and decision making.

Despite the fact that on behalf of the Ministry of Defence is a closed video conferencing, there is a need to enhance the security of information resources management. This need as the advent of the opponent has a large amount of information and technical means for carrying out the attacks, and the use of foreign technologies for the processing and transmission of data. One of the possible

means of the resistance is the use of digital steganography. These methods allow you to simultaneously transmit with video data transparent private information.

Thus, a chance to improve the information-security consulting, namely the use of stenographic method of embedding information into an image-container. This method applies the Xia in addition to cryptographic protection method and requires no additional costs.

The main part

For comparison and evaluation of the existing steganosystem to the distinction of an adequate system of indicators to evaluate the quality of their functioning. Such an evaluation should provide a complete picture of the success of their use to hide data [1]. Indicators of quality of steganographic algorithms can be divided into the following groups-characteristics:

I. Group indicators steganoalgorythm stealth position, i.e. steganoalgorythm resistance to revealing the existence of a hidden message in the image and its cure. The components of it are: 1. The probability of establishing the existence of an attacker a secret message in the image.

If you have the original image container resistance stegano-algorythm can be assessed by using quantitative difference and correlation of indicators [2]: 1) maximum difference between MD: where are the pixels in the image container, with coordinates x, y, is peak-sat steganograms at coordinates x, y. .

2) average absolute difference AD:

$$AD = \frac{1}{XY} \cdot \sum_{x,y} | C_{x,y} - S_{x,y} | . \quad (1)$$

3) image quality IF. Then, the closer the resulting ISO-objects is turned on it is the closer to the original. .

$$IF = 1 - \frac{\sum_{x,y} (C_{x,y} - S_{x,y})^2}{\sum_{x,y} (C_{x,y})^2} . \quad (2)$$

4) Signal-to-noise ratio SNR.

$$SNR = \frac{\sum_{x,y} (C_{x,y})^2}{\sum_{x,y} (C_{x,y} - S_{x,y})^2}. \quad (3)$$

5) Normalized mutual correlation NCC. When high-like images.

$$NCC = \frac{\sum_{x,y} C_{x,y} \cdot S_{x,y}}{\sum_{x,y} (S_{x,y})^2}. \quad (4)$$

5) Normalized mutual correlation NCC. A probability of the existence of an attacker secret messages in picture can be determined with the help of expert assessments.

A probability of the existence of an attacker-Licia secret messages in picture can be determined with the help of expert assessments.

2. The likelihood of correctly identifying the block images with embedded information.

3. The probability of a correct removal of embedded messages from steganograms.

II. Group of indicators of steganoalgorythm from the perspective of embedded data.

1. Standard coefficient of steganotransformation, i.e. the maximum required amount of mini image or parts of it, in which, in accordance with the specified may embed the message volume.

$$\tau = \frac{w_{встр}}{W_{исх}}, \quad (5)$$

where w is the volume of the embedded information is measured in bits.

2. Steganographic bitrate, that highlights the number of pixels on the average you should embed one bit of information. It is measured in bits per pixel bits/pixel.

$$p_b = \frac{w_{встр}}{z_{строк} z_{столб}}, \quad (6)$$

where: steganographic, bits/pixel; minimum desired size of the image, but enough to embed steganographical algorithm information.

III. Indicators of steganoalgorithm from the perspective of time for processing. 1. The time of injection, i.e. time necessary to embed the information volume. 2. Time, i.e. the time of steganogram information, volume.

IV. Indicators of steganoalgorithm from a position of strength to attack. The main index is likely to modify the built-in messages. The probability can evaluate different algorythms to resistance-type attacks.

V. Indicators of the deterioration of its position with steganoalgorythm compression views. Due to the use of modern telecommunication systems compressed images that you need to take into account the effects of the embedded information on compression performance steganograms. Therefore, it is proposed to introduce the following indicators to measure the impact of change on the steganographic performance of the compression view image-container:

1. The coefficient of reduction of the amount of compression (8) where is the volume of a container compressed image without embedding;

$$\Delta k = \frac{W_{сж}}{W'_{сж}} (7)$$

2. The degree of change peak signal-to-noise ratio

$$\Delta h = | h - h' |, \qquad (8)$$

where is the peak signal-to-noise ratio of the container-pictures, DB; peak signal-to-noise images with embedded information, DB.

3. The degree of increase in the total processing time Δt.

$$\Delta t = \frac{t'_{обр} - t_{обр}}{t_{обр}} \cdot 100\%, \qquad (9)$$

VI. Indicators of steganoalgorythm from the perspective of sustainability. Sustainability indicators embedded messages to errors in the communication channel and packet loss when it is sent in the information: 1. the probability of encountering a built-in message; 2. the possibility of losing the inline message.

After reviewing the principles of construction and organization of the closed video conferencing systems, you can define requirements for the clothing-method of embedding stikam.

1. Possibility of blind retrieval, i.e. without a source container and any information about the embedded message. 2. Steganosystems. Resistance to distortion of the container, and messages are sent over the lossy channels and packages. 3. Steganosystems. Resistance to passive and active attacks. Probability of modifications that will ensure delivery of embedded communication management in conditions of active and passive attacks.

4. Ability to embed messages in real time. At that time, embedding and seizures tend to 0. 5. Ability to embed data. When implementing the algorithm of embedded data. 6. Install the secret message must not increase the size of their container. 7. The algorithm must be resistant to the compression. At the same time $\Delta k \to 0$ и $\Delta t \to 0$..

The Ministry of Defence information you want to embed in the videopo-current, is the arbitrary nature. Thus, the algorithms used in videoconferencing, to extract the embedded community-without the receiving party of any information on the tejnere and the original message. The least significant bit substitution method. Physics method is to replace the little significant bit bit s-particular posts [1]. Among the modifications of this method there are the random distribution of bits of secret messages in the tejnere and the pseudorandom permutation. Block-encoding method is an implementation of the algorithm replace the image in one of the blocks is hiding a secret. Method for Palette-Mena. In this method to embed secret messages-use container-color palette of the image. With the implementation of the algorithm, there are N different ways to reposition N-color palette, which is enough to build a small message [2]. Method of modification of brightness (the Cutter-Jordan-Bossen). Embedding a message occurs in channel blue RGB images [4]. The Darmstedtera-Delejgla-Kviskvotera-Mack. The algorithm is a variaty of modification of brightness at which the container is split into blocks of 8 * 8 pixel, commensurate with the building blocks for the JPEG compression [5]. Method of

relative replacement values of the discrete cosine transform (method of Koha and Zhao). The method implemented modification coefficients of the DCT blocks, which creates a relationship that allows you to embed a "0" or "1" the secret message. Method Bengam-Ee-Jung Memon. Method is an optimized version of the CSA values and substitution method uses to build three of the OST of the MF area.

Method of embedding in the least significant bit and its modifications does not provide additional data in the image, and only replaces the redundant data. The advantages of these methods is their simplicity and sufficiently large amounts of data that may be embedded within a relatively-large files. Embedding algorithm is implemented without prior to developing the images and this has a positive effect on the time. The main disadvantage of the methods are highly sensitive to the slightest distortions of the container.

This method has a low steganographic resistance, and it is not resistant to attack by compression.

Maximum difference. Average absolute difference, MD AD Quality images tion, IF the signal-to-noise ratio. Pro-countries-spatial-area method to replace the least significant bits (LSB GSZ method) 1 0.494 0.99998 4975 0.999439

Method of pseudo-random interval 1 7.690 * 10-3 ~ 1 3.193 * 106 0.999992

Method of pseudo-random permutation 1 5.920 * 10-3 ~ 1 4.148 * 106 0.999998

Method of block-1 coding 6.165 * 103 ~ 1 3.983 * 106 0.999988

Method to replace the palette 3 9.827 * 10-3 1.142 0.999999 * 106 0.999942

Quantization method of ISO-images 3 7.141 * 10-3 ~ 1 2.596 * 106 1.000001

Method of modifying a style (method of Cutter-Jordan-Bossen) 0.994799 192.271 0.988343 4.588 38. Spectral AP Method of relative-value exchange OST (method of Kokh and Zhao) 45 11.392 0.992737 137.690 0.986178

Method of Bengam-Ee-Jung Memon

951 3.042 0.998721 781.605 0.994154

Method to replace the palette is quite high. Dan-method also does not put additional information in the container, and the redundancy in the color palette. One of the advantages of the IU is the availability of a variety of ways to improve implementation, not visas-the image distortion. Among the deficiencies of this algorithm is the limited number of embedded information, as well as the lack of resistance to attacks with the change of palette images and attacks. Method of modification of brightness (the Cutter-Jordan-Bossen) takes into account the redundancy of the RGB color components, namely blue. Despite the resistance to a variety of attacks (LF filter, JPEG compression, cropping the edges), this algorithm introduces distortions in the container [4], which in turn is displayed on its visual signature and statistical characteristics.

The spectral conversion of IP-steganographic image is the compression of algorithms, so most Speck-delivery methods are resistant to compression attack [3]. The amount of embedded data is limited by the resolution of the image and the number of units conversion factors selected for installation. Among the disadvantages of spectral methods, you can highlight the selectivity of the protected. A container of smooth areas of the process on frequency rates of change. Smooth the ISO-images contain large amounts of LF coefficients and structural-HF ratios. The limited use of HF patients-due to their load factor of zeroing when quantization. Using heavily distorts the source container and appears in the led-endorsed by the difference and correlation. In some of the sources are the methods of embedding in the mid-range rates change. The fact that such rates may block specific changes, but not for all blocks or other images. Such a definition is arbitrary, and under certain conditions (quantization) mid-range coefficients will be characteristic of treble and bass. Also steganographic algorithms are, because of their complexity, require enough time.

Thus, there is no algorithm that would be resistant to all kinds of attacks. Some steganoalgorithms are making a significant distortion in the image container, resulting in reduced resistance. The major shortcoming of the most current to the

methods is the loss of built-in data processing algorhythms, such as JPEG compression.

CONCLUSIONS

This article contains a list of indicators of the quality of steganographic systems, allowing reporters to give an adequate assessment of the success of utilization systems for embedding data. Requirements for embedding data stream algorithm in process control are outlined. The review and analysis of existing methods of embedding reports into an image are carried out. The existing algorithms do not entirely meet the requirements of secrecy and time requirements of embedding and extraction. The effectiveness of these methods depends on the specific conditions of use.

LIST OF USED SOURCES

1. *Грибунин В.Г.* Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М. : Солон-Пресс, 2002 .– 272 с
2. *Конахович Г.Ф.* Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – К. : « МК-Пресс», 2006. – 288 с.
3. *Тарасов Д.О.* Класифікація та аналіз безкоштовних програмних засобів стеганографії / Д.О. Тарасов, А.С. Мельник, М.М. Голобородько // Інформаційні системи та мережі. Вісник НУ “Львівська політехніка”. – 2010. – № 673. – С. 365–374.
4. *Kutter* M. Digital Signature Of Color Images Using Amplitude Modulation / M. Kutter, F. Jordan, F. Bossen // Proc.Of the SPIE Storage and Retrieval for Image and Video Databases V. – 1997. – Vol. 3022. – Pp. 518–526.
5. *Darmstaedter V.* Low Cost Spatial Watermarking / *V. Darmstaedter, J.-F. Delaigle, J.J. Quisquater, B. Macq* // Computers and Graphics. – 1998. – Vol. 5. – P. 417–423.