Scientific Journals
of the Maritime University of Szczecin

Zeszyty Naukowe
Akademii Morskiej w Szczecinie

2016, 48 (120), 161–170
ISSN 1733-8670 (Printed)
ISSN 2392-0378 (Online)
DOI: 10.17402/190

Received: *29.04.2016*
Accepted: *07.11.2016*
Published: *15.12.2016*

Development and research of additional parameters of steganographic systems

Olesya Afanasyeva

Technical Institute in Kraków
e-mail: olesya@afanasyev.kiev.ua

Key words: steganosystem, digital environment, hiding messages, parameter of data concealing, steganogram

Abstract

This paper contains research on and methods of determining values for basic parameters of steganographic systems. In particular, a parameter of concealing the presence of information in a digital environment is researched. Using this particular parameter increases the degree of protection of a message introduced into a digital environment. This parameter is one of the fundamental ones in case of implementation of a steganalysis system. Besides that, this paper contains a review of parameters of redundancy of a digital environment and the parameter of steganogram resistance to technological transformations in digital environments.

Introduction

Steganography methods, such as those to hide messages from unauthorized use, are effective and can be widely used in naval information systems for various purposes. For example, in naval applications, it is used to protect information being communicated between ships or between ships and ports and can be implemented via satellite-communication channels. Another example is protection of limited-access information, like electronic logs and other tasks, related to use of naval-information systems. For successful use of steganography systems in graphical, digital environments it is necessary to conduct analysis of parameters, characterizing the steganography systems, with the aim to select optimal parameters of the information-hiding task.

In this work, new parameters are introduced that characterize steganography systems and methods of evaluating their values and the aim of use of each parameter are reviewed.

One of the new parameters introduced in this work is the parameter of secrecy, which charactersizes the level of hiding of the existence of the hidden message in the digital environment. With that parameter, it becomes possible to increase the level of protection of the hidden messages from steganography-analysis (steganalysis) systems, used for detection of such messages in any environments, including digital ones.

Basic tasks

When creating steganographic systems, several requirements for this kind of system have to be taken into account. These requirements are defined, firstly, by providing given values of fundamental parameters that characterize a steganographic system. Thus, several tasks are necessary that are related to defining basic parameters which characterize a steganosystem: tasks of determining values of the corresponding parameters, tasks of extending parameters representing certain possibilities of such system, and some other tasks related to the problems of creating a steganographic system.

Interpretation of parameters of a steganosystem

Steganographic methods of concealing information in a digital environment can be divided into the following ways of implementing the corresponding concealment: a technical way of placing information in the environment that leads to its distortion within acceptable limits; a method of using semantic analysis of information with the purpose of determining changes that would save the information with semantics intact; a method of placing a hidden image by hidden components, implemented so that it would not distort the main image; a method of using the plot analysis in order to modify the image without changing the plot of the main image; and a method of generating new images oriented towards placing hidden information within them.

To create more-effective steganography systems, it is necessary to:

- add additional parameters that better reflect the requirements of providing the invisibility of messages, injected into the digital media; or
- develop the determination methods of the values of the input parameters.

Since the algorithm of hiding messages in steganography systems is aimed at providing the invisibility of the messages, adding the new parameters and development of methods of their values' calculation are actual tasks for steganography.

One of the key parameters characterizing the concealment of stenographic information is the degree of invisibility, which is subjective because this parameter is correlated with subjective characteristics of a human. A development in informatics leads to creating a great variety of different information converters, among which may be found some that make invisible-data fragments reveal themselves. From the point of view of conceptions of objective invisibility, the latter has to be defined while considering those kinds of converters that are not oriented towards revealing hidden information. We can introduce the following definitions of information invisibility in a digital environment.

Definition 1. Subjective invisibility of information is a property of a digital environment (DE) that contains the information, which is not visible under an ordinary examination of the corresponding environment by a user. Such invisibility is personalized. Obviously, steganographic methods of information concealment have to ensure objective invisibility.

Definition 2. Objective invisibility of information is a property of a DE that ensures information concealment when using various standard tools for analysis of a DE that are not designed for detecting steganographically-hidden information.

Another important characteristic of a stegano-system is absence of information regarding hidden information being present in the DE. We will call this parameter the parameter of information concealment. A parameter of concealment of hidden information in the DE defines the capability of DE elements that carry hidden information to be interpreted as DE elements that do not carry hidden information. To ensure constructiveness and unambiguity of interpretation of this parameter, let us review the following definition.

Definition 3. The parameter of concealment of hidden information characterizes a degree of deviation of parameter values of DE fragments that contain the hidden information from the parameter values that characterize components that do not contain hidden information and are surrounded by them.

This definition is constructive because with it we can discuss the signs of presence of hidden information. Based on the invisibility definition, criteria of invisibility of hidden information can be discussed (Afanasyeva, 2006; 2009). The invisibility parameter is written as η, and the concealment parameter is written as $\Im$. Definitions of the parameter of objective invisibility η and the parameter of concealment $\Im$ allow creation of algorithms of their definition.

Any environment that displays some information must have a certain interpretation. For example, if we have some symbols $x_1,\dots,x_n$, that can be used to display certain information, then each symbol and its chosen combinations must have an interpretation that is independent of a specific steganogram. Suppose that symbol interpretation is written as $J(x_i)$, and interpretation of symbol combinations is written as $J(x_{i1},\dots,x_{ij})$. Information will be such a set of symbols and their combinations, each one of which has an interpretation. Formally, this can be represented as the following relation:

$$U(x_{i1},\dots,x_{ijn}) = [J_1(x_{i1}),\dots,J_m(x_{ij}*x_{ik}*\dots*x_{ir})],\dots,J_n(x_{im})] \tag{1}$$

where "*" is a symbol that describes correlation between x_{ij} and x_{ik} within the scope of their semantic interpretation. Interpretation of $J(x_1,\dots,x_n)$ will be called an interpretational extension of the corresponding data set or symbols $(x_1,\dots,x_n)$. Because each interpretational extension is different from another one, if it relates to different symbols or their combinations (thanks to determining a single element $J(x_i)$) it becomes possible to introduce a way to describe interpretational extensions by numeric values. Given definitions of η and $\Im$ parameters in this case, they can be defined not only qualitatively but quantitatively as well. The latter allows for an introduction of numeric criteria to define the invisibility measure or the concealment measure of information in the DE. In information systems, converters and analyzers of DE are widely used that are not oriented towards the tasks related to steganography. Examples of these known converters of DE are compression systems widely used in data transfer systems and such (Katzenbeisser & Petitcolas, 2000; Provos & Honeyman, 2003). These tools and other tools of examination of DE will be considered technological tools of DE conversion and analysis. Thus, from the point of view of steganographic systems, we should review one more parameter that characterizes a steganogram, which is a capability of the latter to withstand technological tools of conversion and modification of elements that contain the hidden information.

Definition 4. The resistance of a steganosystem (SS) to technological transformations $\varkappa$ ensures impossibility to destroy elements of hidden information in the DE or to detect their interpretational extensions with the help of technological tools and DE transformations.

It is incorrect to claim that certain converters or analyzers of DE cannot detect components that carry hidden information in the DE. Thus, we have to assume that methods that are not related to steganalysis tasks exist that can reveal elements which carry hidden information and which will be called steganoelements (SE). A set of SE will be called a steganogram (SG). Because steganography is not so much about concealing the information carriers as about concealing the that there are hidden data in the DE, a certain steganosystem has to solve, at least, the following tasks: a task of concealing the carriers of hidden information, or carriers of steganoelements; and the task of concealing interpretational extensions of the corresponding SE carriers. A degree of information concealment, defined by the invisibility and concealment parameters, is implemented by concealing SE carriers and concealing SE interpretation. In most graphic DEs that are representations of versatile and rich information there are semantic redundancies. This means that in some DEs that represent information with a certain richness, regardless of whether a SE set is introduced into this environment, there always are components interpretation of which can be, with various degree of coherence, related to the interpretation of the whole DE. This is caused by the following factors: information generated without special limitations of its way of representation always has redundancies that do not essentially affect the content of key information stored in this DE; when generating information in the DE, components can be introduced in this DE resulting from technological tools of generating the corresponding information; and there is a whole set of random factors that cause generation in the DE of non-basic elements represented in the DE. All of these factors influence the parameters that characterize an informational image and information concealed in it, generated in the DE.

In cases with η and $\Im$ parameters, it is valuable to review possible approaches to determining the value of the $\varkappa$ parameter. Resistance of SGs against technological conversions is closely related to DE properties. Technological processes acting on the DE can lead to the following consequences: destroying certain SE and, respectively, the modification of the hidden information; revealing the hidden information; and distorting the main information in the DE, which can be its radical change or its destruction. We will not consider the last case because it is not so much related to SG as to the image stored in the DE. Let us assume that influences of technological tools on the SG are not related to steganalysis tasks. The main danger that can arise when using technological tools is the destruction of SE components as a result of conversions of the corresponding DE by these tools.

Revealing hidden information by technological tools is only possible when information is concealed not only by placing symbols defining certain information elements but by placing the interpretation itself of these elements, as well. An example of this situation can be a case when alphabet-letter codes, describing the corresponding interpretation, are used to display information stored in the DE. In this case, texts that describe the corresponding interpretation on the users' native language are the corresponding description as interpretational extensions. This situation is typical for those technological tools that use interpreters of symbols in some alphabets. Among these technological tools are various editors that could be used for converting elements detected in the description environment of a certain image. It should be noted that such an informational image could be a text image stored in the DE.

Generally, steganography never uses direct placement of concealed information as a description of its interpretation. A way to separate carriers of concealed information, or separate symbols embedded in the DE from their interpretational extensions, is performed by the following methods: on the basis of using transformations of interpretation description; on the basis of space distribution of symbols used to describe the information introduced in the DE and to describe interpretational extension of these symbols; and on the basis of using the rules of forming interpretational extensions for a certain set of symbols, using a known interpretation of certain used symbols to describe concealed information in the digital environment.

The first way lies in using various cryptographic algorithms to encrypt the texts that describe the corresponding interpretations or the concealed information itself in the user language (Doubechies, 1990; Babash & Shangin, 2002).

A space distribution of symbols used to describe information and the description of their interpretational extensions that describe the corresponding symbol in the user language is based on using vocabularies for symbols used when coding the information embedded in the DE. This method is rather cumbersome, but when considering the specifics of the subject of steganographic information concealment, using personal vocabularies by two subscribers that use steganography to exchange information is quite well founded. Essentially, using vocabularies is quite popular in the branch of message encryption.

A third way is a modification of a method based on using vocabularies. The point is that personal vocabularies can grow in time, requiring a large amount of memory, and in time these vocabularies can be accessed by third parties, which can lead to compromising the corresponding steganosystems. Thus, in the third approach, it is proposed to shorten this vocabulary to a degree necessary for defining a certain symbol. On the basis of interpretations that are single-text descriptions in the user language, rules are formed to generate phrases and sentences that could describe information that has to be embedded in the DE for the transfer to a subscriber. These rules are the secret part of a steganosystem, or a part that is personalized for users of the corresponding steganosystem. These rules can be represented in a compact way and do not require big amounts of memory and vocabularies for a certain symbol set that can be available to all.

Reasoning from the above, the main threat from technological processes is unforeseen destruction of information embedded in the DE. Let us determine possible approaches to calculate the values of the corresponding parameter, which lie in the following: based on the detected fact of destruction of information, to determine the number of SE elements that were distorted or removed from the DE by the corresponding tools; to determine the DE parameters that could be used to predict the amount of distortion of hidden information, which could allow an estimate of the possible resistance of the steganosystem as a value opposite to the amount of distortions; and based on an analysis of basic characteristics of technological tools of DE transformation, parameters are defined that allow an estimate of distortions in the DE that could be caused by using technological tools.

Parameter-evaluation methods of steganography system based on a usage example of graphical, digital media

Parameters that characterize a steganosystem (SS) have to be described qualitatively in order to obtain estimates for characterizing SS and SG (Yhang & Ping, 2003; Noda, Niimi & Kawaguchi, 2006). Let us review the possible methods of measurement of parameters, among which are: a degree of invisibility (η) of information introduced in the DE and its varieties: a subjective degree of invisibility η_s, an objective degree of invisibility η_b, and a technological degree of invisibility η_t; a degree of redundancy of DE (μ), which has the following varieties: semantic redundancy μ_s, technical redundancy μ_t, technological redundancy μ_p, and natural redundancy μ_n; and a degree of carrying capacity of a steganographic channel π. Let us examine the possible ways of measuring the parameters that are their basic sort.

The invisibility degree has to be measured within the limits of psychophysiological invisibility. A value of these limits is determined on the basis of psychovisual research that lie in generating experimental dependencies, displayed as curves or data tables where a value of change of brightness ΔJ_i is measured in one of selected colors on the distance between the two dots where two values of brightness are measured, which is formally written as the following expression:

$$\eta^{+} = \frac{\left(\alpha(\Delta J)\right)^{J}}{\left|l_1(J_1) - l_2(J_2)\right|} \tag{2}$$

Let us assume that the upper limit of invisibility η is set on the basis of experimental data corresponding to the relation (2). Let us review the definition of the lower limit of invisibility for changes in the image caused by introducing information in the digital environment. A graphical image can be represented in the following forms: as brightness of pixels creating the image field; as codes of value of single pixels depending on the color model; or as an image semantic description. Choosing these three forms of image representation is based on the fundamental difference in the methods of these representations and different possibilities to interpret the conceptions of information concealing. On the level of a semantic-image representation, certain heterogeneities within its placement, if they do not distort codes and symbols that are semantic-image elements, are not factors that are taken into consideration when reviewing the corresponding image. The upper limit of the invisibility value, described by the expression (2), is placed below the level of semantic invisibility that is defined by the degree of semantic distortion of the image where the concealed information is introduced. Within this degree, visual heterogeneities, that could be visible, are acceptable. Semantic invisibility is mostly used in text environments. The upper limit of invisibility values η^+ is defined on the basis of analysis of psychophysiological features of visual perception of graphical images. The lower invisibility limit η^- has to be defined on the level of codes representing the brightness values and color values of the corresponding dots. Although different models of generating colors exist, as well as vector methods of generating an image, a method of representing the lower limit of visibility η^- will be added up to representations that use conceptions of pixel codes. We will define the lower limit of η^- value as a degree of change of code values describing the corresponding pixels.

The role of the lower limit of the invisibility value of the introduced element of a hidden-information code could be taken by a single change of the least-significant bit. But in practice, depending on the purpose of using the steganographic method of information concealing, the digital environment is affected by factors of a various nature that could lead to unforeseen changes in the corresponding environment. These changes are normally called noise. The main characteristic that represents the degree of noise in the signal is the signal-to-noise ratio. Because of this, there is no sense in talking about η^- values that are less than the noise. Thus, the lower limit of the invisibility value of the concealed information in the digital environment will be defined on the basis of the following relation:

$$\eta^+ \geq \alpha_p \beta \sum_{i=1}^{n} \frac{\Delta d_{si} - \Delta d_{szi}}{\Delta d_s} \tag{3}$$

where Δd_s is the value of the signal change caused by introducing the hidden information, Δd_{sz} is a noise value within the signal, α_p is a factor of a usage mode of a steganogram, and β is a factor that represents description features of certain image dots or fragments. In this case, the source of noise can be technological transformations, compression, decompression, and so on. In order to get η^+ and η^- to a common-measurement unit, let us transform the relation (2) to the form that has the same unit as the relation (3). Transforming the unit $\eta^+ \rightarrow \eta^-$ (not vice-versa $\eta^- \rightarrow \eta^+$, although it is possible) is caused by the fact that the process of embedding the element of concealed information lies in modifying codes by introducing bits or codes of information elements. When introducing information codes causes modification of the components that describe the image not in the coordinate space (such as the (x, y) system, but in the time-frequency system, for instance, (ω, t)), the degree of invisibility of information embedded in the image is defined after the reverse transformation of the image representing space from (ω, t) space to (x, y) space.

Let us review transforming $\eta^+ \rightarrow \eta^-$ to a common measurement unit. Brightness values J_1 and J_2, as well as ΔJ, are brightness values of certain pixels. A value of the code d_i, which defines the brightness value, is related to the brightness degree at least in the visibility range of the user, which can be written as:

$$J_i = f(d_i) \tag{4}$$

where J_i is the brightness of the pixel i and d_i is a value of the code written in the register corresponding to the pixel i. If we assume that brightness in the visible range can be directly proportional to the value of the code written in the corresponding register, the relation (3) can be written as:

$$\eta^+ = \frac{\alpha(a\Delta d + b)}{\left| l_1(a_1 d_1 + b_1) - l_2(a_2 d_2 + b_2) \right|}$$

where $J_1 = a_1 d_1 + b_1$, a is a factor of proportionality that adjusts the value of code change with the value of brightness change of a certain pixel, and b is a constant in the linear dependence $\Delta J = a\Delta d + b$.

Let us review methods of measurement of redundancy parameter value SG, or redundancy of a container where hidden information is stored. In this case, the analysis is conducted on the level of technical implementation of a method when introducing a message in the DE, so we will review the technical redundancy μ_t, which will be written as μ. Practical redundancy μ_P is a parameter that ensures the possibility to implement a required invisibility degree of other types, such as η_S. If redundancy $\mu = 0$, it means that every register that stores the brightness code d_i (J_i) can be used to store an element of information being concealed. However, because the function f_i in the expression (4) is not linear, it means that on the level of displaying an image fragment, due to optical laws, various effects can take place, especially in the fragments that carry semantic load where brightness or colors change. This is illustrated in cases that create an effect of tridimensionality of an image (Katzenbeisser & Petitcolas, 2000; Provos & Honeyman, 2002). This leads to the necessity to use not only η parameters of various types, but μ parameter as well. It can be asserted that redundancy of a parameter that characterizes DE is closely related to SS. Moreover, a parameter μ can be interpreted as the one that is necessary in order to make it possible to implement processes of concealing information by a SS system. For steganography, only DEs with redundancy are used. Because DE redundancy is closely related to the invisibility level, methods of measuring redundancy μ have to be compatible with methods of measuring the invisibility parameter. Within a single DE redundancy can be several levels: redundant number of places that can be selected for storing the introduced information; redundant coding of single-image pixels; redundant number of image elements from the point of view of their semantic significance; etc. These redundancies are closely related to redundancies μ_s, μ_p, μ_t, and μ_n. Because redundancies μ and the invisibility degree η are related to each other, to define μ we will use the η parameter that is already transformed to the unit defined by a numeric value. The value of μ can be determined from the following relation:

$$\mu^1 = \alpha \frac{\eta^+ - \eta^-}{\Delta d_{\mathrm{SG}}} - 1$$

where Δd_{SG} is a value of modification of a single environment element that is necessary for, at least, introducing the minimal element of concealed information, α is a proportionality factor and μ^1 is redundancy of DE within a single element that can be modified. Redundancy of a DE in general is composed of the following components: a redundancy component μ^1, a redundancy component μ^2 that determines this value regarding all environment elements where, based on technical requirements, and an information element that can be introduced. Redundancy μ^2 depends on the size of the information code that has to be introduced, and will be written as R. If we define N(SG) as the number of elements in a DE suitable for storing information elements, and N(R) as the number of information-elements embedded in the DE, we can write the following relation:

$$\mu^2 = N(\mathrm{SG}) - N(\mathrm{R}).$$

In this case, redundancy due to unused environment elements for storing information codes within them will be defined by the relation:

$$\mu^3 = \mu^2 \alpha \frac{\eta^+ - \eta^-}{\Delta d_{\mathrm{SG}}}$$

Full redundancy of the DE environment with introduced information of the size N(R) equals to: $\mu = \mu^3 + \mu^1 \cdot \mu^2$. This relation can be written in the form reduced to the common measurement units:

$$\mu = \left(N(\mathrm{CS}) - N(\mathrm{R})\right)\left(2\alpha \frac{\eta^+ - \eta^-}{\Delta d_{\mathrm{SG}}} - 1\right).$$

Let us examine the parameter of carrying capacity of a steganochannel π.

Definition 5. A steganochannel (SCh) is a name of a system that consists of a DE, where the DE and steganosystems SS are planned to be placed, and that performs this placement, formally written as:

$$\mathrm{SCh} = F(\mathrm{DE}, \mathrm{SS}) \qquad (5)$$

In most cases, the idea of an SK is limited by its comparison to the possibilities of a digital environment where some information can be stored secretly (Katok & Hasselblat, 1999). These possibilities mostly depend on the steganosystem type. In the known approaches, determining the carrier capacity SK depends on the possibility to transfer data without errors during the counter-actions from an opponent. In this case, only such properties of SS are indirectly accounted for as the ability of the latter to generate an SG that is resistant to the attacks, although it is reasonable to be estimated using a separate parameter.

Within the scope of this approach, function F from the expression (5) describes the fusion of an SS with a DE so that, on the basis of this fusion-solving task of optimizing the process of using SCh, it would be possible. In this case, the carrying capability is examined independently from the parameter that defines resistance of an SG related to the attacks. Thus, the π parameter for SCh has to be defined not only on the basis of DE, but also on the basis of analysis of functional abilities of SS. Let us assume that the function F from the expression (5) is linear. This means that the two components DE and SS can be reviewed independently, if we accept the conditions for SS that will represent limitations regarding the functioning way of SS. The redundancy parameter μ of the DE environment is a key one to determine the carrying capability SCh. So, the carrying capability of a channel π has to be directly proportional to the redundancy degree of DE, which can be written as follows: $\pi_m = \beta f(\mu)$, where β is a proportionality factor.

Definition 6. A momentary carrying capability of a steganochannel π_m characterizes the maximal amount of information hidden in the DE that could be stored in the SG while saving the given level of invisibility of hidden data, or $\pi_{\mathrm{CS}} = \beta\mu$.

Analysis of a concealment parameter

Known parameters that characterize not only steganographic systems (SSs), but the principle of steganographic concealment, is a parameter of invisibility degree of information embedded in the digital environment η and a parameter of concealing degree of presence of information $\Im$ hidden in the DE. Parameter $\Im$, as well as parameter η, have subjective nature regarding the user who is not authorized (NAU to detect the steganographically-hidden information. In general, in this case we can assume that parameter $\Im$ mostly represents subjective properties of certain NAU, because one NAU$_i$ can think that there is a steganographically-hidden element of an information image (IO$_i$) in some environment, while another NAU$_j$ can think that there is none. In order to evade such subjectivity when determining the value of $\Im$ parameter, let us assume the following. We will examine a certain DE where single fragments of DE$_i$ can be distinguished where information intended to be concealed will be stored. These fragments DE$_i$ from DE will be called steganographic containers (SC). In this case, we will review the parameter $\Im$ within the following conditions.

Condition 1. The NAU knows that there is no SC in the DE where concealed information could be stored, or there is no SG in the DE.

Then, subjective factors that could distinguish NAU$_i$ from NAU$_j$ from the point of view of parameter $\Im$, and will be eliminated by the next condition that needs to be accepted because of the introduction of parameter $\Im$.

Condition 2. The DE, in general, does not have to be divided into fragments DE$_i$ that, from the point of view of NAU, can be used for concealing information.

Qualitatively, the given conditions lie in the following. A subjective decision of a single NAU$_i$ regarding possibility of existence of concealed information in the given DE$_i$ is considered a random event regarding all fragments of information images present in the DE. This event depends on a random event of appearance of an NAU$_i$ among all possible NAU. Besides, in a certain DE there is always some set DE$_i$ that is suitable for placing a DE in it, which can also add to the randomness factor that could be used to compensate the subjectivity factor from the side of NAU$_i$. Obviously, the *Condition 2* does not mean that absolutely all fragments DE$_i$ from the DE can be suitable for embedding IO$_i$. There must be algorithms within the SS that, corresponding to certain criteria, select some DE$_i$ for their usage as containers. Let us assume that the selection of DE$_i$ from DE is performed according to this relation: DE$_i$ = SKl(DE), where SKl is a steganographic key for the container selection. Thus, the properties of SKl can affect the value of the parameter $\Im$. Because the value of the parameter $\Im$ is determined by different factors that characterize the degree of suitability of certain SC elements for invisible concealing of information image elements (EIO) in the selected container or a certain DE$_i$ that is directly related to the concealment degree, it is reasonable within the scope of the algorithm of SC selection and, respectively, within SKl to foresee the features and criteria which would not lead to a decrease of invisibility degree and, respectively, concealment when placing the corresponding IO in the selected SC. There are the following possible ways to solve this problem: using integral parameters, similar to the parameters used in the SS when placing IO in SG that are generated on the basis of analysis of parameters used on the level of SG analysis by the SS system; defining the parameters that characterize DE, in general, and can be related to technical aspects connected to embedding information in the DE; and defining the parameters that characterize DE from the point of view of external features related to the corresponding environment.

The first approach looks the most natural, because defining the concealment parameter can be considered a development of invisibility parameter that is researched quite intensively and has a commonly-accepted interpretation. Let us review the second approach in more detail. One of the basic conditions of using DE for selecting a container within it is a condition corresponding to the size of the DE, which has to be bigger than the foreseen container: $\{[\mathrm{CS} = k(\mathrm{SKO})\ \&\ (k \geq 1)\}$. For the parameter $\Im$, within the scope of this relation, it is natural to assume that $\Im$ increases together with k. If $\Im = 0$ and $k = 1$, then DE = SC and a place for storing IO is unambiguously determined by the size of SC. In order to be able to use the given starting condition, $\Im$ has to be related to k by a logarithmic dependency, which will be written as:

$$\Im = A \ln k \qquad (6)$$

where *A* is a certain expression that describes the dependency of $\Im$ from other parameters of DE that could characterize $\Im$. The next parameter closely related to the parameters that characterize SS is a noise pollution in the DE. Let us assume that any DE environment, especially if it is transferred in the space of an electronic network, suffers from noise pollution. Introducing information in the selected fragments of DE or in the SG can also be considered as some sort of noise pollution. In this case, there can be heterogeneous noise pollution throughout all DE environments. Let us assume that noise pollution of the DE throughout the entire environment is uniform from the point of view of noise-spectral power because it can be assumed that during the transfer of DE through the same channel along all the length of this channel DE is affected by the same reasons of noise pollution. So, one of DE parameters that could be considered as independent, from the point of view of methods of introducing information in DE, from the parameter $\Im$, if the latter ensures the given concealment degree, is a spectral thickness of a noise pollution signal. In this case, the spectral thickness of noise in the DE is examined at the input and the output of DE channel. Channel input and output will be identified with the source where the SG is generated and the users among which there is a recipient whom SG is addressed to. The spectral thickness of noise is calculated at the channel input and is defined as D_{xx} and is determined by the embedded message, while spectral thickness of noise at the channel output, which is also determined by the channel noise pollution, is defined as D_{yy}. For noise analysis in DE, the mutual-spectral thickness D_{xy} is examined. Then, a coherence function can be used for analysis (Kharin, Bernik & Matveev, 1999; Popov, 2000) that is described by the following relation:

$$\gamma_{xy}^2(f) = \frac{\left|D_{xy}(f)\right|^2}{[D_{xx}(f), D_{yy}(t)]}.$$

Substantial essence of γ^2_{xy} (*f*) allows the following interpretation within the range of $\Im$. If, in the DE environment, a value of γ^2_{xy} (*f*) for the noise existing in the DE is changed heterogeneously, it could mean that there is a SG in the DE with an embedded IO that leads to a change in uniformity of value of γ^2_{xy} (*f*) in the corresponding DE fragment. Because the embedded IO is implemented at the channel input of SS, in order to determine the value of γ^2_{xy} (*f*) we will differentiate it by the *x* variable, and then the following relation can be written:

$$\delta_x[\gamma_{xy}^2(f_{sz})] = d[\gamma_{xy}^2(f_{sz})]/d[x(t_{sz})]$$

where f_{sz} is a frequency of a noise component of the information signal described in DE. Regarding the size of the DE that is defined by the value of *k*, the frequency component can be considered, with respect to *k*, an additive variable. So, the relation (6) can be written as follows:

$$\Im = A_1\{\delta_x[\gamma_{x,y}^2(f_{sz})] + \ln k\} \qquad (7)$$

where A_1 is a possible extension of the dependency (7).

External characteristics that characterize DE are firstly related to semantic features. Among these features, the following can be mentioned: different DE types; informational uniformity of DE, parameters of DE that characterize semantic properties of information in IO; and functional orientation of information placed in the corresponding environment.

Informational uniformity is determined by the degree of integrity of information stored in the DE environment. Informational uniformity has different degrees depending on the DE type. This is caused by the possibility of recreating one or another plot in different environments.

Semantic parameters of information in IO are important parameters because any user, including one not authorized to receive concealed information, first uses semantic content of the corresponding IO. Different IO types have different measures of semantic representation as interpretational descriptions. Text types of DE are the ones most covered by interpretational descriptions of IO. The next one, based on its interpretational abilities, is the graphical type of DE. The ones with the least interpretational abilities are musical images. In this case, their musical essence is emphasized, because sound images can be represented in the symbolic form.

Within the scope of problems related to determining the $\Im$, an important task is to determine the value of $\Im$ for each single case of steganographic information concealment in the DE. At the same time, the $\Im$ value must not be affected by the modification of the IO implemented by technological tools. So, let us formulate a definition.

Definition 7. A technical modification of DE takes place when the latter does not lead to change of IO semantics.

The change of IO in DE will be understood not only as changes regarding the output IO, but also changes that could extend semantics of the modified IO. For example, if, as a result of modification of a DE fragment containing IO, elements of an image appear that do not directly affect the semantics of the main IO and are dots, spots, etc., these elements can lead to a change in semantics of the IO.

Definition 8. A semantic modification of DE takes place in a case when, as a result of embedding information in DE, changes are introduced in the IO that lead to change of IO semantics.

An example of these modifications can be a color change of certain elements of an IO image and others. Let us assume that an arbitrary IO has a standard IO, or IO^E, if there is an interpretational description of the corresponding image. Obviously, in most cases the following relation takes place:

$$\forall(\mathrm{IO}_i)[\Delta\mathrm{IO}_i = [\mathrm{IO} - \mathrm{IO}^E]] \qquad (8)$$

This means that IO^E is a standard only in case when there is a certain set of such IO that the following relation is true:

$$\{[\mathrm{IO}^k = \{\mathrm{IO}_1^k,\ldots,\mathrm{IO}_n^k\}] \,\&\, \forall(\mathrm{IO}_i^k)[\Delta I_i \neq 0]\} \rightarrow \forall(\mathrm{IO}_i^k)\,\exists\,(\mathrm{IO}^{Ek}) \qquad (9)$$

The accuracy of image descriptions and their deviations from standards in the relations (8) and (9) is determined by the accuracy of interpretational descriptions of the corresponding images, which will be written as $j(\mathrm{IO}_i)$. Let us assume that an interpretational description of $j(\mathrm{IO}^k{}_i)$ is represented in the user's native language in the normalized form that is ordered corresponding to semantic accents of importance of certain IO elements (Sayood, 2002; Vatolin et al., 2002). Normalization of the description lies in using only determined words in the text descriptions and excluding redundancies, additional grammatical expressions and words. The ordering accent is understood as such placement of text of interpretation description when at the beginning of the $j(\mathrm{IO}_i)$ description those elements of $j_i\,(\mathrm{IO}_i)$ are placed that within this IO$_i$ have the biggest semantic significance from the point of view of information transferred through IO$_i$. In the next element $j_{i+1}(\mathrm{IO}_i)$, a fragment of IO$_i$ description is placed that has the next value of semantic significance that is determined from IO$_i$ interpretation, etc. Let us assume that $j(\mathrm{IO}_i)$ is a single phrase of a text $\varphi_i\,(\mathrm{IO}_i)$. One of the basic functions of the standard IO^E of an image IO$_i$ is determining the ordering accents of description $j_i\,(\mathrm{IO}_i)$ for images IO^K of a certain class K. Let us assume that IO^E for the image class K contains the full semantic representation of the corresponding IO$^K{}_i$. We will assume that $j_i\,(\mathrm{IO}_i)$ can be represented as a description of IO$_i$ semantics that has a varying value of significance depending on the number of components $j_i\,(\mathrm{IO}_i)$ included in $j(\mathrm{IO}_i)$. With regards to the conception of accented ordering of $j(\mathrm{IO}_i)$ let us assume that the measure of semantic significance of $j_i\,(\mathrm{IO}_i)$ for description of IO$_i$ semantics is determined by the value of the accent assigned to phrases $\varphi_i[j_i\,(\mathrm{IO}_i)]$ that compose a text description of $j(\mathrm{IO}_i)$ and a number of place of φ_i storage in $j(\mathrm{IO}_i)$. With respect to the normalization of $j(\mathrm{IO}_i)$ description, let us assume that φ_i with the highest accents are placed at the beginning of $j(\mathrm{IO}_i)$ description. We can represent $j(\mathrm{IO}_i)$ as series of phrases φ_i, or $j(\mathrm{IO}_i) = \varphi'^i{}_1 * \varphi'^i{}_2 * \ldots * \varphi'^i{}_m$, where each $\varphi'^i{}_j$ has a value of accent ξ_j, and also, $(g < k) \rightarrow (\xi_g > \xi_k)$. To step aside from the absolute values of ξ_j, let us assume that $(\Sigma^m{}_{j=1}\xi_j) = 100\%$ for IO$_i$. In graphical images a situation can take place when IO$_i$ in DE corresponds to the standard image only at α%. This, in turn, means that such semantic modification of IO$_i$ from DE can be performed, that:

$$[(\mathrm{IO}_i) + (\Delta(\mathrm{IO}_i))] \rightarrow [\,j(\mathrm{IO}_i + \Delta I_i) \leq j(\mathrm{IO}^E)].$$

In order to move to the qualitative estimation of value of semantic modification that will be a next component of parameter $\Im$, let us assume the next conditions and definitions.

Definition 9. An IO$_i$ image will be represented in an incomplete semantic form, if the value of sum of its accents is less than sum of accents of its full standard, or:

$$\sum\nolimits_{i=1}^{k} \xi_i(\mathrm{IO}^k) < \sum\nolimits_{i=1}^{m} \xi_i[P(j(\mathrm{IO}^{kE}))],$$

where $P(j(\mathrm{IO}^{kE}))$ is a full-interpretation description of an IO^k image of K class that is a standard for IO^k.

When introducing a message V_i in DE, it is impossible to adjust, throughout the whole DE or all the elements IO^k, the modification of their semantics so that the corresponding modification would be the same for all IO^k components, so the following is true:

$$\lambda_i(\mathrm{IO}_i) = \left|\sum\nolimits_{i=1}^{k(i)} \xi_i(\mathrm{IO}_j) - \xi_p(\mathrm{IO}_P^E)\,\right|.$$

A component for $\Im$ that represents the semantic modification in IO$_i$ with DE will be written as s_i. To define it, let us use the following relation:

$$\{[[\lambda_i(\mathrm{IO}_i) - \delta] \geq 0] \rightarrow (s_i = s_i + 1)\} \,\&$$
$$\{[[\lambda_i(\mathrm{IO}_i) - \delta] < 0] \rightarrow (s_i = s_i)\}$$

where δ is a threshold value of difference of sums ξ_i between images IO$_i$ and IO$^E{}_P$. This relation can be extended like following:

$$\Im = s_i(\mathrm{CS}) + \delta_x\left[\gamma_{xy}^2(f_{sz})\right] + \ln k \qquad (10)$$

Let us assume the following condition of using certain components of EIO$_i$ from IO$_i$.

Condition 3. If in IO_i from DE a component EIO_i from IO_i is used that has its own semantic meaning that causes the presence of the corresponding standard IO^E_i, and EIO_i has incomplete semantic interpretation, then $j(EIO_i) = \varphi_1 * ... * \varphi_k$ has to have the highest value of acceptance from the complete interpretational description of $j(IO_i)$.

The given condition means that in cases when in graphic or any other symbolic images IO_i there are no components of interpretational description, the corresponding φ_i that describe single fragments of interpretational representation correspond to the elements of such representation in IO^E_i that have the highest values of ξ_i. At the qualitative level the given condition means that, when a graphical image is generated so that it represents a certain object or a certain entity with some semantic approximation, such elements of the corresponding image are used that are the most informative for this IO_i. This means that these components have greater values of ξ_i regarding the elements that are used during the implementation of IO_i.

Conclusions

In this paper, several basic parameters are developed and researched that characterize steganographic systems, regardless of the type of digital environment the steganographic system is oriented towards.

Along with the invisibility parameter of a message embedded in the DE, a parameter of concealment of a hidden message is researched. Thanks to using this parameter, it became possible to estimate the degree of detection of environment elements where the message elements can be stored. In many cases, this can be sufficient because, on the basis of estimation of this parameter, the detected DE can be eliminated from the whole environment in order to withstand the possibility to transfer a hidden message to a recipient. In this case, the invisibility parameter characterizes the degree of possibility to detect, based on the selected DE elements, when using the concealment parameter, the elements of the message itself.

Introducing the concealment parameter allows a division of the steganographic concealing of a message in the DE into two stages:

- a stage of selecting such DE fragments, to place a message within them, that would be hard to distinguish among the surrounding DE fragments;
- a stage of implementing such a way to introduce, in the selected DE fragments, the message elements that would make it hard to recognize certain elements of the concealed message.

The researched parameter of concealing the message placement in the DE is a description of a certain aspect of invisibility degree of a hidden message that increases the safety level of a message hidden in the DE.

The paper contains analysis of other parameters of a steganosystem and research of methods to calculate their values. Such parameters are the redundancy parameter of DE and the parameter of steganogram resistance regarding technological transformations of DE, foreseen by standard methods used in the digital information systems.

The results obtained in the paper allow the constructive approach to solving tasks that lie in creating new steganosystems.

References

1. Afanasyeva, O.Y. (2006) *Parameter of invisibility in steganosystems*. Science and techniDE conference of young scientists and engineers of modeling. Kyiv, Institute of modeling problems in energetiDE of NAS of Ukraine.
2. Afanasyeva, O.Y. (2009) *Analysis of parameters of steganosystems oriented towards using graphical digital environments.* Modeling and information technologies: collected articles (IMPE of NAS of Ukraine). Kyiv, Issue 50.
3. Babash, A.V. & Shankin, G.P. (2002) *The history of cryptography*. Moscow: SOLON-R.
4. Doubechies, I. (1990) The wavelet transform, time-frequency localization and signal analysis. *IEEE Transactions on Information Theory* 36, pp. 961–1005.
5. Katok, A. & Hasselblat, B. (1999) *Introduction to the modern theory of dynamical systems*. Moscow: Factorial.
6. Katzenbeisser, S. & Petitcolas, F.A.P. (Eds) (2000) *Information hiding techniques for steganography and digital watermarking*. Boston – London: Artech House.
7. Kharin, Y.S., Bernik, V.I. & Matveev, G.V. (1999) Mathematical basiDE of cryptology. Minsk: BSU.
8. Noda, H., Niimi, M. & Kawaguchi, E. (2006) High-performance JPEG steganography using quantization index modulation in DCT domain. *Pattern Recognition Letters* 27(5), pp. 455–461.
9. Popov, S.N. (2000) *PC video system*. St. Petersburg: BHV-Peterburg, Arlit.
10. Provos, N. & Honeyman, P. (2002) *Detecting Steganographic Content on the Internet*. Proc. 2002 Network and Distributed System Security Symp., Internet Soc.
11. Provos, N. & Honeyman, P. (2003) *Hide and Seek: An introduction to steganography*. University of Michigan. IEEE Security & Privacy.
12. Sayood, H. (2002) *Kompresja danych. Wprowadzenie*. Warszawa: RM.
13. Vatolin, D., Ratushnyak, A., Smirnov, M. & Yukin, V. (2002) *Methods of data compression. Structure of archivers, image and video compression*. Moscow: DIALOG-MIFI.
14. Yhang, T. & Ping, X. (2003) *A Fast and Effective Steganalytic Technique Against JSteg-like Algorithms*. Pric. 8th ACM Sym. Applied Computing, ACM.