FOLIA 180

Annales Universitatis Paedagogicae Cracoviensis

Studia Technica VIII (2015)

Olesia Afanasieva

Information support of steganography messages hiding

According to possible definitions of a common information model, the main components, being converted by (MI)[1] model, are:

- data structure S(D),
- interpretational extension of the data structure J[S(D)].

In the case of implementation of the simplest functions of the connection between S(D) and J[S(D)] within the framework of MI, S(D) and J[S(D)] are transformed independently, J[S(D)] is an interpretational extension of the structure S(D). Within the framework of MI function F, describing the process of functioning of MI, it consists of the following parts:

- S(D),
- J[S(D)],
- S(D) and J[S(D)].

In this case, a possible way of implementation of the MI functioning process can be described by the following correlations:

$$\left\{\left[J(x_i)\,\&\,j_C(x_i)\right] \to J\left[S_i^*(d_{i1},...,d_{ik})\right]\right\} \Rightarrow \left\{\left[S_i(d_{i1},...,d_{ik})\,\&\,j\left[S_i^*(d_{i1},...,d_{ik})\right]\right]\right\} \to$$
$$\to S_i^*(d_{i1},...,d_{ik}) \qquad (1)$$

$j(x_i)$ – interpretational extension of the structure of the initial data for a task the purpose of which is described by $j_C(x_i)$;

$J\left[S_i^*(d_{i1},...,d_{ik})\right]$ – interpretational description of the task $S_i(d_{i1},...,d_{ik})$, which must be solved;

$S\ (d_i\ ,...,d_{ik})$ – the data structure of the solved problem the purpose of which is described by: $j_C(x_i)$.

Correlation (1) corresponds to the case, when interpretation of the solution of the problem on the basis of initial data $j(x_i) = S_i(d_{i1},...,d_{ik})$ and description of a goal $j(x_i)$ is first formed in MI. Then, basing on the initial data $S_i(d_{i1},...,d_{ik})$ and the interpretation of the solution $j\left[S_i^*\left(d_{i1},...,d_{ik}\right)\right]$, solution to the $S_i^*\left(d_{i1},...,d_{ik}\right)$ problem is formed.

For a more detailed analysis of the process of solution of the problem in the MI model, let us have a closer look at different ways of presentation of the task and with respect to those ways consider possible methods of formation of interpretation of the problem solution. At a qualitative level such a distribution of the overall process of functioning of MI consists of the following fragments. Solution of the problem consists of finding or forming through some transformations, which are determined by the algorithm for solving the problem, a certain initial structure with new quantitative values of the parameters that describe the relevant data. It is possible to say, that the solution is in looking for new data values even under the old structure on the basis of initial data using the initial $S_i\left(d_{i1},...,d_{ik}\right)$ structure. In this case, let us describe the solved task as $S_i\left(d_{i1}^*,...,d_{ik}^*\right)$. Output or formation of interpretive extension of the task solving is in building the description, which by its nature is a comment to results of the task solving in subject area, to which the relevant task belongs.

In case when description of targets of the task $j_C\left(x_i\right)$ is an incomplete description or comment to task solution, the procedure of output of complete interpretation $j\left[S_i^*\left(d_{i1},...,d_{ik}\right)\right]$ is very simple. It is reduced to a search of separate components from $J\left[S\left(D\right)\right]$ which relates to the whole W_i area and the most suitable or the most coordinated with fragments $j_C\left(x_i\right)$ of the $j_K\left(x_k\right)$ elements. As a result of such extension, a description of interpretation of the task solution is formed. Formally, this process can be described by the following correlation:

$$\left\{\left[j\left(x_{C1}\right)*...*j\left(x_{cv}\right)\right]\&\left[j\left(x_{ik}\right),j\left(x_?\right),...,\mathrm{j}\left(\mathrm{x}_{\mathrm{if}}\right)\right]\right\}\rightarrow j\left[S_i^*\left(d_{i1},...,d_{ik}\right)\right]$$

If the target represents itself as a description of requirements for results of the task solution, then output of interpretational description of the solution is in the following. Structure of the text representation of interpretational extension, especially when it relates to natural language, is linear. This means that separate elements $j\left(S_i^*\left(d_{i1},...,d_{ik}\right)\right)$ are placed sequentially and between them there exists or is established a hierarchy of their sequence. Value of the hierarchy of separate requirements and conditions, related to description of the task is closely tied with hierarchy of components, defined by structure of description of the subject area. It is obvious that task solution or its results must correlate with general structure of W_i. To evaluate the relevant level of coordination, let us review possible relations of the general description of W_i with results of task solution. Such relations or dependencies can be in following:

- results of solution of Z_i task, which can be sent as separate fragments of S_i^* or $S_{i1}^*,S_{i2}^*,...,S_{i3}^*$ structure, in W_i or $S\left(W_i\right)$ structure they can cause change of some d_{ij} data values, which allows its own interpretation as parameters of the subject area,

- results of solution of Z_i task can lead to modification of some separate fragments of W_i structure,
- result of solution of Z_i task $S(x_i)$ can lead to extension of structure of the W_i subject area.

In the first case, implementation of conditions and requirements, formed in $j_C\left[S(d)\right]$ is performed in accordance to hierarchy of parameters, used in W_i. Such hierarchy is defined by the structure of semantic dictionary S_C. In S_C each parameter, identified by attribute x_i has interpretational extension $j\left(x_j\right)$. Description of such extension is selected as in fragment for $j\left[S^*\left(x_i\right)\right]$. In that case, output process of $j\left[S^*\left(d_{i1},...,d_{ik}\right)\right]$ results in coordination of separate fragments $j\left[S_{i1}^*\left(d_{i1},...,d_{iN}\right)\right]$ which form the ψ_i phrase and $\psi_{i1},...,\psi_{i2}$ sentence of interpretational extension $j\left[S_i^*\left(d_{i1},...,d_{ik}\right)\right]$ according to the grammar rules Γ, which are used in language $M(\Gamma,R)$, forming $J\left[S(D)\right]$ in W_i.

If requirements, formed in $j_C\left(x_i\right)$, expect modification of W_i structure, output procedure of $j\left[S_i^*\left(d_{i1},...,d_{ik}\right)\right]$, like in the first case, defines priorities of fragments, which are subject for modification. Those priorities are defined by S_C, because in dictionary, fragments of the structure are described as separate elements. As far as fragments $S_{il},...,S_{im}$ from W_i are coordinated and connected with each other in framework of W_i, modification of one S_{ij} can result in conflict in W_i. So, the procedure of $V_i\left[j\left(S\left(d_i\right)\right)\right]$ output performs conflict check in relevant set of descriptions $j\left(S_i\right)$, and is preconditioned by requirements $j_C\left(x_i\right)$ at each step of the output. If at one separate step of the output conflict S^K is not detected, then $V_i\left[j\left(S\left(d_i\right)\right)\right]$ moves to the next step of the output $j\left[S_i^*\left(d_{i1},...,d_{ik}\right)\right]$. Formally, such procedure is described by the following correlation:

$$V_i\left[j\left[S^*(D)\right]\right]=F_P\left[\left[j\left(S_{i1}^*\right),...,j\left(S_{ik}^*\right)\right],S_C,\left[j_C\left(x_i\right)=\left[U_{il}\left(S_{il}\right),...,U_{ir}\left(S_{ir}\right)\right]\right]\rightarrow$$

$$\rightarrow\left[\forall j\left(S_{ij}\right)\neg\exists j\left(S_{ig}\right)\left(j\left(S_{ij}=j\left(S_{ig}\right)\right)\right)\right]\right]\rightarrow\left\{j\left[S_i^*(D)\right]=j\left[S_{i1}^*\left(d_{il}^l,...,d_{ir}\right)\right.\right.$$

$$\left.\left.*S_{i2}^2\left(d_{sl}^2,...,d_{ik}^2\right)*...*S_{ik}^*\left(d_{il}^m,...,d_{if}^m\right)\right]\right\}$$

If description of the target $j_C\left(x_i\right)$ represents itself as conditions $U_1\left(S_{i1}\right),...,U_k\left(S_{ik}\right)$ which suppose extension of the structure W_i or extension of the structure of separate fragments, then the output procedure V_i of interpretational extension $j\left[S^*(D)\right]$ differs from the last one by the step of checking the coordination between two neighbour elements – instead of semantic conflict, semantic controversy is being checked. This fragment of output process $j\left[S^*(D)\right]$ is formally described by the following correlation, corresponding to conditions of definition of S^C:

$$\forall j\left(S_{ij}\right)\neg\exists j\left(S_{ig}\right)\left\{\sigma^{S}\left[j\left(S_{ij}\right),j\left(S_{ig}\right)\right]\right\}\leq\beta_i^S$$

Where β_i^S is given value of semantic controversy σ^S between sequent fragments $j\left(S_{ij}\right)$ and $j\left(S_{ig}\right)$ in interpretational extension $j\left[S^*(D)\right]$.

Another way to solve the problem within the framework of the MI model can be formally described by the following correlations:

$$\left\{\left[S_i\left(d_{i1},...,d_{ik}\right)\&\ j_C\left(x_i\right)\right]\to S_i^*\left(d_{i1},...,d_{ik}\right)\right\}\Rightarrow$$

$$\Rightarrow\left\{\left[S_i^*\left(d_{i1},...,d_{ik}\right)\&\ j_C\left(x_i\right)\right]\to j\left[S_i^*\left(d_{i1},...,d_{ik}\right)\right]\right\} \tag{2}$$

In this case, the process of transformation in the MI consists of the following. Basing on the initial data $S_i\left(d_{i1},...,d_{ik}\right)$ and task of the problem $j_C\left(x_i\right)$, solution to the problem $S_i^*\left(d_{i1},...,d_{ik}\right)$ is formed. After that, basing on the solution of the problem $S_i^*\left(d_{i1},...,d_{ik}\right)$ and description of the task $j_C\left(x_i\right)$, interpretation of the solution to the problem $j\left[S_i^*\left(d_{i1},...,d_{ik}\right)\right]$ is formed.

Thus, in both cases, the process of functioning of the information model is completed with the formation of the solution of the problem $S_i^*\left(d_{i1},...,d_{ik}\right)$ and interpretative extension of this solution $j\left[S_i^*\left(d_{i1},...,d_{ik}\right)\right]$. Formally, this is described by the following correlation:

$$MI=F\left\{S(D),I\left[S(D)\right]\right\}\to\left\{S_i^*\left(d_{i1},...,d_{ik}\right)\&\ j\left[S_i^*\left(d_{i1},...,d_{ik}\right)\right]\right\}$$

An important type of representation of target of solution of the task $Z\left[S(D)\right]$ is the description $j_C\left(x_i\right)$ in shape of some approximation of solution algorithm, or in shape of system of requirements to the task solution algorithm. In that case, $j_C\left(x_i\right)$ is formally written as:

$$j_C\left(x_i\right)=\left[j_i\left(a_1\right),...,j_k\left(a_k\right)\right]\vee\left[j\left[U_1\left(a_1\right)\right],...,j\left[U_k\left(a_k\right)\right]\right],$$

where a_i is a fragment of algorithm, described by interpretational extension $j_i\left(a_i\right)$ or condition, to which fragment a_i must correspond, represented as $U_i\left(a_i\right)$ in a shape of interpretational extension $j\left[U_i\left(a_i\right)\right]$. In that case, procedure of $V_i\left[j\left[S^*(D)\right]\right]$ output will represent itself as the following sequence of actions. Algorithm, according to its definition [2], represents some sequence of actions or transformations of initial data aimed on receiving the defined data at the output. Interpretational extension of approximated description of such algorithm can represent itself as a description of separate fragments of algorithms, ordered or not with each other. A fragment of algorithm, related to fragments of other objects, is defined by presence of the following elements:

- one or a sequence of transformations, described by some functions of calculation of discrete or uninterrupted variables,
- description of requirements to a form of representation of initial data, expected in the framework of relevant fragment of transformation,
- type of transformations, reflecting peculiarities of the data transformation process, i.e. complexity of their implementation, method of transformation completion of one option of the initial data.

So, fragment of algorithm a_{ij} can be represented as the following formal description:

$$a_{ij} = S_i\left(y_i\right) \to \left\{ f_{ij}\left[S_i^j\left(y_i^j\right)\right] * ... * f_{im}\left[S_i^m\left(y_i^m\right)\right]\right\} \to S_i^*\left(y_i^*\right),$$

where $S_i\left(y_i\right)$ – structure of initial data y_i of fragment a_{ij}, $S_i^*\left(y_i^*\right)$ – structure of output data of fragment a_{ij}, f_{ij} – separate elementary transformations, used in fragment $a_{ij} \in A_i$. In proposed correlation is not shown the last element, defining character of the whole process of functioning, or transformations, implemented by algorithm a_{ij}. This is conditioned by the fact, that this component describes one or another condition or limitations, describing the character of transformations. In explicit mode, such limitations or conditions are related first of all to initial variables and parameters of fragment a_{ij} in which they define functioning mode of a_{ij} or influence of one or another peculiarity $S_i\left(y_i\right)$ on a_{ij}. In most cases, the character of functioning of a_{ij} is tightly connected to $S_i\left(y_i\right)$ or $S_i^*\left(y_i^*\right)$. Relevant conditions, defining the character of functioning of a_{ij}, are described in the middle of the fragment, if the last one consists of the sequence of elementary transformations f_{ij}, or if conditions are related to the whole fragment, then they are written before the fragment, for example as:

$$\forall\left(y_i\right)\left[\left(y_i^l > \beta_j\right) \& \left(y_i^l \leq \beta_j\right)\right]$$

The mentioned condition describes the allowed interval of initial data, transformed by the fragment a_{ij}. Relevant conditions can also relate to the structure of initial data, as far as $j_C\left(x_i\right)$ represents it the interpretational description of algorithm, reflecting the last one with some approximation, then such approximations can relate to the following elements of the relevant fragments of the algorithm, or the algorithm in general:

- some level of indetermination of requirements to initial and output data, transformed by relevant fragment a_{ij},
- indetermination related to specific transformations f_{ij}, used in a_{ij},
- indetermination in general character of functioning of algorithm's fragment,
- indetermination related to the use of fragment a_{ij} in framework of the whole algorithm $A_i\left(Z_i\right)$ of the task solution.

Obviously, in framework of descriptions $j_C(x_i) = j_l(a_{il} * ... * a_{ik})$, such indeterminations are represented quite constructively, i.e. representation of such indeterminations in framework of $j_C(x_i) = j\left[A_i^*\right]$ can be implemented in the following forms of description of the task solution targets:

- absence in description $j\left(A_i^*\right) = j\left(a_{i1},...,a_{ik}\right)$ of separate fragments a_{ij}, and in descriptions $j\left(a_{ij}\right)$ of separate functions f_{ij},
- incompleteness of description of functions f_{ij}, that can lead to indetermination of its selection during forming of a_{ij},
- absence of the baseline characteristic a_{ij}, that does not allow to formulate requirements of the specific fragment functioning, or determine its abilities.

The output procedure, with such form of usage of the task target, will represent itself the following. Taking into account that $J\left[S_i^*(D)\right]$ is a structure, described by semantic parameters, and the last ones are defined in framework of some intervals of allowed values, then $J\left[S_i^*(D)\right]$ must not completely eliminate indeterminations, represented in $j_C\left[a_{i1},...,a_{ij}\right]$, but define allowed ranges, in which undetermined components are absent, parameters or values must be specified. Expediency of such approach is conditioned by the fact, that in framework of $J(W_i)$ there can be an incomplete set of attributes components, describing allowed transformations f_{ij}, or some variables x_{ij}, characterized by ranges of values and metrics, in which such values are defined. Then, in framework of the relevant description $j_C\left(A_i^*\right)$, in process of forming of the necessary algorithm, which is the solution of the task, we can select from $J(W_i)$ attributes, close to the given ones, and their inconformity to one or another condition can be compensated by forming one or another requirements to the initial data, or to the method of implementation of separate fragments of the algorithm of task solving. Formally, such procedure of $j\left[S_i^*\left(d_{i1},...,d_{ik}\right)\right] = j\left(A_i^*\right)$ output can be presented as the following correlation:

$$\left\{\left[S_i\left(d_{ik},..,d_{ik}\right)\right] \& \, j_C\left[u_1\left(a_{i1}\right),...,u_m\left(a_{im}\right)\right]\right\} \rightarrow$$

$$\rightarrow \left\{\left[j\left[u_i\left(d_{i1},...,d_{ik}\right)\right] \& \, j\left(a_{i1} * .... * a_{im}\right)\right]\right\} \Rightarrow J\left[S_i^*\left(d_{i1},...,d_{ik}\right)\right]$$

where $u_i\left(a_{ij}\right)$ – requirements to fragment of algorithm a_{ij}, described in $j_C(x_i)$, $j\left[u_i\left(d_{i1},...,d_{ik}\right)\right]$ – interpretation of conditions, related to initial data, formed basing on $S_i\left(d_{i1},...,d_{ik}\right)$ and separate conditions $u_i\left(a_{ij}\right)$, $j\left(a_{i1},...,a_{im}\right)$ – interpretation of ordered fragments a_{ij}, implemented basing on $u_i\left(d_{i1},...,d_{ik}\right)$ interpretation, as the algorithm in general, in the part of transformations where it defines conditions for initial data and vice versa, the required modifications of fragments a_{ij}, if they are allowed, are conditioned by fragments of structures of the relevant initial data $S_i\left(d_{ij}\right)$.

The above analysis of the method of implementation of information process in information MI model illustrates efficiency of using MI and quite wide possibilities in use of interpretational extensions of the main components of the applied system, described in the framework of the subject area of interpretation W_i [3,4]. In relation to this, there arises the task of proving that in the framework of MI the process of output $J\left[S_i^*(D)\right]$ will not lead to forming of such interpretational extension, which would be incorrect or controversy related the process of solving the task, presented in framework of MI as output of task solving $S_i^*(d_{i1},...,d_{ik})$ which we understand as forming the solution $A_i\left[S_i(d_{i1},...,d_{ik})\right]\rightarrow S_i^*(d_{i1},...,d_{ik})$ and calculation of the output data of algorithm A_i. Let us review the following assertion for solving the task.

Assertion 1. The process of forming interpretational extension of task solution $j\left[S_i^*(d_{i1},...,d_{ik})\right]$ is not a controversy and causes no conflicts with the process of task solution, described by the following correlation:

$$\left[S_i(d_{i1},...,d_{ik})\,\&\,j\left[S_i^*(d_{i1},...,d_{ik})\right]\right]\rightarrow\left[S_i^*(d_{i1},...,d_{ik})\right]. \tag{3}$$

As far as there exists some functional dependency between semantic controversy and semantic conflict, which we will write down as $\sigma^K\rightarrow\sigma^S$, which means that having the appropriate conditions, first appears σ^K and only after it appears σ^S, in most cases as a development of σ^K, so, let us first review the possibility of appearance of σ^S between $j\left[S_i^*(d_{i1},...,d_{ik})\right]$ and the process of solution of (3). As far as σ^S can be detected in local networks in framework of separate phrases or sentences, we can show, that as a result of forming, or output of $j\left[S_i^*(d_{i1},...,d_{ik})\right]$ in framework of interpretational extension of solution, semantic controversy σ^S will not appear. Let us suppose that in $j\left[S_i^*(d_{i1},...,d_{ik})\right]$ σ^S is absent. Such supposition is valid, as all $j_C(x_i)$ are formed as output data, or like the initial description of the model MI. Then the following takes place:

$$\left[S_i(d_{i1},...,d_{ik})\,\&\,j_C(x_i)\right]\rightarrow j\left[S_i^*(d_{i1},...,d_{ik})\right].$$

It means that basing on initial data and basing on interpretational description of the target of task description Z_i we can output the interpretational extension of the task solution.

Let us review a case, when $j_C(x_i)=j\left[S_i^{**}(d_{i1},...,d_{im})\right]$, where $m<k$ and S_i^{**} – incomplete description of structure of data of the output task solution. Then, the procedure of $j\left[S^*(x_i)\right]$ output is in supplement of $j\left[S^{**}(x_i)\right]$ with missing data. If in $j_C(x_i)$ data is missing, then $j_C(x_i)$ contains description of this fact. Description $j\left[S_i^*(d_{i1},...,d_{ik})\right]$ contains not only data with description of the own structure of S_i^*, but also elements of algorithm, with which the relevant output data is received, as data represent some parameters, identified by attributes x_i together with their current values. In framework of S_C all attributes, which are not elementary in W_i are described in functional part of S_C or in $S_{cf}\subset S_c$. This means that elementary fragment a_{ij} from A_i exists in S_C. Then we can write down the sequence $A_i^*=a_{i1}*...*a_{im}$, in which some separate fragments could be absent. In $j_C(x_i)$ the

absence of initial data means that the value of corresponding parameter is missing. For supplement of A_i^* with required parameters a_{ij}^* in dictionary S_{cf}, we will select functional attributes, corresponding to attribute parameters, preset in $j_C(x_i)$. As the set of initial parameters of the task Z_i is complete, then we will use them in S_{cf} as arguments for the required x_j from $j\left[S^*(x_i)\right]$. So, out of S_{cf} we will receive a_{ij}^*, formed out of attribute , corresponding to $S_j^*\left(d_{j1},...,d_{iz}\right)$.

Interpretational description $j\left[S_i^*(d_{i1},...,d_{ik})\right]$ is formed basing on syntax rules of grammar [2] and so, the relevant parameter $j\left(a_{ij}\right)$ has correct syntax and does not create σ^S in its $j\left[S_i^*(d_{i1},...,d_{ik})\right]$ neighbourhood. Let us show, that relevant construction does not lead to appearance of σ^K. By definition of σ^K, the last one means presence in $j\left[S_i^*(d_{i1},...,d_{ik})\right]$ of two functionally identical fragments. As there are no such elements in $j_C(x_i)$, then it is necessary to show that they appear on output of $j\left[S_i^*(d_{i1},...,d_{ik})\right]$. This is provided by extension of the mentioned above procedure of validation of the selected fragment $j\left(a_{ij}\right)$ for its repeats. If in the procedure of selection from S_{cf} for each sequentially selected $j\left(a_{ij}\right)$ we will not check, if it was not selected before in framework of the current output, then it guaranties that σ^K in $j\left[S_i^*(d_{i1},...,d_{ik})\right]$ will be absent.

Let us review a case, when $j_C(x_i)$ is set as a set of some conditions and limitations [3]. Then the following correlation takes place:

$$j_C(x_i) = j_i\left[u_1(d_{i1},...,d_{ik}),...,u_i\left(d_{ij},...,d_{i(j+k)}\right),...,u_m(d_{im})\right].$$

Each condition has some elementary function of validation of attribute x_i parameter. As A_i consists of a number of fragments, this means that in A_i there are used a_{ij}, which implement basic functions of analysis of current values of data d_{ij}. As in $j_C(x_i)$ are described $u_i\left(d_{ij},d_{ik}\right)$, then those conditions are implemented in different fragments of A_i. In a contrary case they would not be mentioned in $j_C(x_i)$. So, there are no logical contradictions in A_i, implementing $j_C(x_i)$. As σ^S is a contradiction to values in the interval [0,1], then it also accepts values at the boundaries of this interval, which interpret values of controversy in logical expressions. Therefore, if there is no logical controversy in A_i at the level of logic of its functioning, then with forming of $j\left[S_i^*(d_{i1},...,d_{ik})\right]$ there will be no σ^S if $\Delta\sigma^S \le \delta$, where δ – allowed deviation of the value of semantic controversy. As in the previous case, output of interpretation $j\left[S_i^*(d_{i1},...,d_{ik})\right]$ is implemented in framework of syntax rules Γ and output system Ξ, which reflect semantics of its separate fragments. Therefore, with providing logical consistency of fragments of interpretation $j\left[S_i^*(d_{i1},...,d_{ik})\right]$, consistency σ^S will also be provided.

In the case when the target of the task $j_C(x_i)$ is described as some fragments of algorithm of task solution [4], then we can write down:

$$j_C(x_i) = \psi_C\left[j_C(a_{i1}) * ... * j_C\left(a_{ij}\right) * j_C\left(a_{i,(j+k)}\right) * j\left(a_{im}\right)\right],$$

where ψ_C – some grammar function, reflecting descriptions of separate $a_{ij} \in A_i$ in the form of interpretational representation of separate fragment of algorithm A_i. In that case, to implement output:

$$j_C\left[S^*\left(d_{i1},...,d_{ik}\right)\right]=\psi_C\left[j_C\left(a_{i1}\right)*...*j_C\left(a_{ij}\right)*j_C\left(a_{i,(j+k)}\right)*...*j_C\left(a_{im}\right)\right],$$

It is necessary to reconstruct descriptions of fragments a_{ij}, missing in $j_C\left(x_i\right)$.

If some a_{ij} fragment is missing in $j_C\left(x_i\right)$, it is not described in S_{cf} as it represents itself derivative fragment or some structure of elementary fragments a_{ij} from S_{cf}, then it is formed basing on the usage of output system Ξ, describing semantically allowed in W_i transformations. So, in this case, there is an output interpretation of solution $j\left[S_i^*\left(d_{i1},...,d_{ik}\right)\right]$, which accomplishes proving of the given assertion. Other variants of the description of the target are brought to the variants, reviewed in the assertion.

References

[1] Markov A.A., Nagorny N.M., *Algorithm theory*, Fazist, Moscow 1996.
[2] Arno A., Nikol P., *Logics or Art of thinking*, Nauka, Moscow 1991.
[3] Akimov O.E., *Discrete mathematics: logics, groups, graphs, fractals*, Akimova, Moscow 2005.
[4] Dazhone M.T., *Programming artificial intellect in applications*, DMK Press, Moscow 2006.

Abstract

Hiding information with steganography means an actual and complicated task from the point of view of modern achievements and data transfer possibilities. So, modeling of information processes of messages hiding with steganography is a necessary, continuously developing and improving process.

This work is a review of theoretical implementation of two methods of information model functioning process. Methods of implementation of transformation of input and output data, used in steganography systems, together with their text description were researched in this work. Use of such description enables implementation of semantic analysis of input and output data transformations which itself enables evaluation of adequacy between the aim of the task and received result. A lot of aspects of the aim of steganography transformations are described as a text, so the methods, reviews in the work, are specialized on work with text fragments.

Key words: information model, steganography system, text description of data interpretation, semantic analysis.

Olesia Afanasieva
Pedagogical University of Cracow
Institute of Technology
ul. Podchorążych 2
30-084 Kraków, Poland