A formal description of a multi-key steganographic systems

Pavel Urbanovich[1,2], Nadzeya Shutko[2], August Zapala[1]
1 - Catholic University of Lublin, Poland; 2 - Belarusian State Technological University;
e-mail: pav.urb@yandex.by

The steganographic system (steganosystem) – a set of tools and techniques that are used to form a secret channel of information transfer [1] or to protect copyrights for the electronic digital documents. The last thing is most relevant for text documents [2].

The embedding of secret message (M) in the protected document (container, C) can be performed using the key (K) and without using it. Message M can be used to prove ownership. To increase the steganographic resistance of the system, a key can be used as a verification tool. It can also have an impact on the distribution of message bits within the container during the generation of embedded bits of the message M.

An important distinctive feature of the mathematical model of the considered steganosystem is the identification of the stenographic method used for embedding/ extracting of the message M. For an unauthorized user this information must be secret.

Let $\boldsymbol{M}$ be a finite set of messages that can be hidden in the container: $\boldsymbol{M} = \{M_1, M_2, \ldots, M_n\}$; $\boldsymbol{C}$ – is the finite set of all admissible container (cache files or text cache documents): $\boldsymbol{C} = \{C_1, C_2, \ldots, C_p\}$, p>n; $\boldsymbol{K}$ – is the finite set of keys, generally we will understand methods and deposition message algorithms in container or other operations preliminary transformed embedded message M_i or selecting elements in container for such a deposition: $\boldsymbol{K} = \{K_1, K_2, \ldots, K_z\}$. An arbitrary hidden message M_i can be hidden in the container C_j using key K_m. The result of this type of transformation is a full container (or steganomessage) S_q, pertaining to a set of full container or steganoomessages $\boldsymbol{S}$: $\boldsymbol{S} = \{S_1, S_2, \ldots, S_r\}$.

Thus, an important feature of the analyzed systems is the multiple meaning of key information. Such systems will be classified as the multi-key systems.

A suitable transformation $\boldsymbol{F}$ defined on $\boldsymbol{M} \times \boldsymbol{C} \times \boldsymbol{K}$ with the values in $\boldsymbol{S}$, will be identified with deposition or insertion of messages M_i from the set $\boldsymbol{M}$ in container C_j (from the set $\boldsymbol{C}$) on the basis of key K_m of set $\boldsymbol{K}$, which demands the using of an appropriate algorithm concerning deposition and space (geometric or other) parameters of container C_j:

$$\boldsymbol{F}: \boldsymbol{M} \times \boldsymbol{C} \times \boldsymbol{K} \rightarrow \boldsymbol{S}; \quad \boldsymbol{F} = \{F_1, F_2, \ldots, F_l\}. \tag{1}$$

The transformation $\boldsymbol{F^*}$:

$$\boldsymbol{F^*}: \boldsymbol{S} \times \boldsymbol{K^*} \rightarrow \boldsymbol{M} \times \boldsymbol{C}; \quad \boldsymbol{F^*} = \{F^*_1, F^*_2, \ldots, F^*_l\}, \tag{2}$$

where each specific mapping backward transformation F^*_w ($w = 1, 2, \ldots, l$) corresponds to a fixed key K^*_w from $\boldsymbol{K^*}$ (formally, we separate the keys for embedding and the keys for extracting of the message).

Thus, the expression (2) defines the inverse to (1) mapping, where each element S_q of set $\boldsymbol{S}$ and a fixed element of the set $\boldsymbol{K^*}$ assigns the element M_i of the set $\boldsymbol{M}$ and element C_j of the set $\boldsymbol{C}$. The multi-key steganosystem $\boldsymbol{\Sigma}$ in an ordered structure, consisting of 6 connected elements, formally describes as $\boldsymbol{\Sigma} = \{\boldsymbol{M}, \boldsymbol{C}, \mathbf{K}, \boldsymbol{S}, \boldsymbol{F}, \boldsymbol{F^*}\}$.

References

[1] Urbanovich P., Shutko N.: Theoretical Model of a Multi-Key Steganography System, in: Recent Developments in Mathematics and Informatics, Contemporary Mathematics and Comput. Science Vol. 2, Ed. A. Zapała, Wyd. KUL, Lublin ,2016, Part II, Chapter 11, pp. 181-202.

[2] Shutko N. The use of aprosh and kerning in text steganography, Przeglad Elektrotechniczny, 2016, N10, p. 222-225.