Block Diagram and Formal Mathematical Definition of Steganographic System

Alexey Smirnov
Associate Professor in the Department of Software, Kirovohrad National Technical University, Kirovohrad, Ukraine

Abstract

This paper studies a formal mathematical description and the block diagram of the secret system and, by analogy with the theory of secret systems, introduces the basic elements and mathematical operators, abstractly describing steganographic information protection system.

Keywords: secret systems, steganographic system, formal mathematical definition

1. Introduction

Mathematical foundations of modern cryptography are laid by the famous American scientist C. Shannon [1-3], who, for the first time, using information-theoretic approach, introduced abstract mathematical definition of a secret system and formalized the procedures for data cryptographic transformation of data. These studies gave a significant boost to the development of the individual methods of the theory of information security, cryptography and authentication, digital steganography, and digital signal processing techniques and error-correcting coding [4-12].

This paper studies a formal mathematical description (in terms of C. Shannon) and the block diagram of the secret system and, by analogy with the theory of secret systems, introduces the basic elements and mathematical operators, abstractly describing steganographic information protection system.

2. Block diagram and a formal mathematical definition of cryptographic (secret) system

Abstract secret system is defined as some set of mappings from one space (the set of possible messages) to a different space (the set of possible cryptograms) [1-3].

Let's fix a set of possible messages $M = \{M_1, M_2, \ldots, M_m\}$ and a set of cryptograms $E = \{E_1, E_2, \ldots, E_n\}$. We will also fix a set of mappings:

$$\varphi = \{\varphi_1, \varphi_2, \ldots, \varphi_k\},$$

where:

$$\varphi_i: M \to E,\ i = 1, 2, \ldots, k.$$

If the sets M and E are equivalent, i.e., n = m, then there is an inverse mapping $\varphi_i^{-1}: E \to M$, which assigns each element of the set E to an element of M. Obviously, φ_i and φ_i^{-1} are given reciprocally the same mapping of the sets M and E.

Let's now fix a set of keys $K = \{K_1, K_2, \ldots, K_k\}$, so that for all $i = 1, 2, \ldots, k$ mapping $\varphi_i \in \varphi$ is uniquely specified by the key K_i, that is:

$$\varphi_i : M \xrightarrow{K_i} E .$$

Each specific mapping of φ_i from the set φ corresponds to the way of encryption with a specific key K_i.

Let's fix a set of keys $K^* = \{K_1^*, K_2^*, \ldots, K_k^*\}$, in general to $K \neq K^*$. All the elements of the inverse mappings:

$$\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, \ldots, \varphi_k^{-1}\}$$

are given the appropriate key:

$$\varphi_i^{-1} : E \xrightarrow{K_i^*} M .$$

Each specific mapping φ_i^{-1} of the set φ^{-1} corresponds to the way of decryption using the key K_i^*. If the key K_i^* is known, then the only one answer is possible as the result of decryption – an element of the set M.

Thus, an abstract definition of a secret system includes the following sets of M, E, φ, φ^{-1}, K and K^* (the sets of open texts and cryptograms, sets of direct and inverse mappings, sets of keys). If, in addition, $K \neq K^*$, then the system is asymmetric. On the contrary, if $K = K^*$ – the system is symmetric. Fig. 1 represents a block diagram of a secret system.

A message source generates the flow of messages from the set M. Each message is a specific implementation of some random process describing the work of a message source. Each message $M_j \in M = \{M_1, M_2, \ldots, M_m\}$ corresponds to the probability $P(M_j)$. A distribution of the random process probability is given by set of probability distribution of random variables, i.e. by a set of probabilities:

$$P_M = \{P(M_1), P(M_2), \ldots, P(M_m)\}. \quad (1)$$

Keys' source generates a flow of keys from the set K and/or K^*. Each key $K_i \in K = \{K_1, K_2, \ldots, K_k\}$ corresponds to some probability $P(K_i)$, and each $K_i^* \in K^* = \{K_1^*, K_2^*, \ldots, K_k^*\}$ corresponds to the probability $P(K_i^*)$. Random process of keys' generation is defined by the sets of probabilities:

$$P_K = \{P(K_1), P(K_2), \ldots, P(K_k)\} \quad (2)$$

and

$$P_{K^*} = \{P(K_1^*), P(K_2^*), \ldots, P(K_k^*)\}. \quad (3)$$

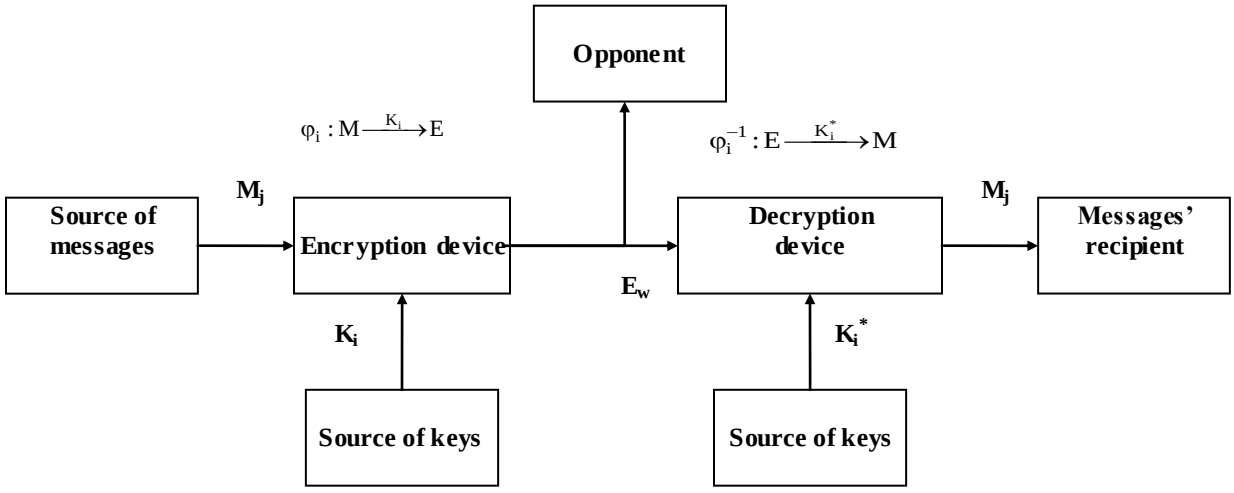

Fig. 1. The block diagram the secret system

Sets of values of a priori probabilities (1 - 3) form a priori knowledge of the opponent about the source of messages and the source of keys, respectively. In fact, these sets characterize the a priori knowledge of the opponent of the possible "weakness" of the secret system.

Selection of K_i determines specific mapping φ_i of the set of mappings φ. With the help of the mapping φ_I which corresponds to the selected key K_i, the cryptogram M_j is formed according to a received message:

$$E_w = \varphi_i(K_i, M_j),$$

$$i \in [1,2,\ldots,k], \; j \in [1,2,\ldots,m], \; w \in [1,2,\ldots,n], \; n \geq m.$$

E_w cryptogram is transmitted to the point of taking on some of the channels and can be intercepted by the opponent. At the receiving end, the original message is restored of cryptogram E_w using reverse mapping φ_i^{-1} (given by the key K_i^*):

$$M_j = \varphi_i^{-1}(K_i, E_w).$$

If the opponent takes over the cryptogram E_l, he can use it to try to calculate the a posteriori probabilities of various possible messages:

$$P_{M|E_w} = \{P(M_1|E_w), P(M_2|E_w), \ldots, P(M_m|E_w)\}, \quad (4)$$

and a variety of possible keys:

$$P_{K|E_w} = \{P(K_1|E_w), P(K_2|E_w), \ldots, P(K_k|E_w)\}, \quad (5)$$

that could be used in the formation of cryptogram E_w.

Sets of a posteriori probabilities (4 – 5) form a posteriori knowledge of the opponent about the keys $K = \{K_1, K_2, \ldots, K_k\}$ and messages $M = \{M_1, M_2, \ldots, M_m\}$ after intercepting a cryptogram E_l. In fact, the sets $P_{K|E_w}$ and $P_{M|E_w}$ are the sets of assumptions, which the corresponding probabilities are assigned to.

3. Block diagram and a formal mathematical definition of steganographic system

By analogy with the theory of secret systems let's consider the basic functional elements and mathematical operators abstractly describing steganographic information protection system.

Let's fix a set of possible messages $M = \{M_1, M_2, \ldots, M_m\}$, the set of possible container $L = \{L_1, L_2, \ldots, L_l\}$, and the set of possible filled containers (steganograms) $E = \{E_1, E_2, \ldots, E_n\}$. Let's also fix a set of mappings:

$$\varphi = \{\varphi_1, \varphi_2, \ldots, \varphi_k\},$$

where:

$$\varphi_i: (M, L) \to E,\ i = 1, 2, \ldots, k.$$

We will define the inverse mapping:

$$\varphi_i^{-1}: E \to (M, L),$$

which each element of the set E assigns to an element of the set M and an element of the set L.

Let's fix a set of keys $K = \{K_1, K_2, \ldots, K_k\}$, so that for all $i = 1, 2, \ldots, k$ mapping $\varphi_i \in \varphi$ is uniquely specified by the key K_i, that is:

$$\varphi_i : (M, L) \xrightarrow{K_i} E.$$

Each specific mapping of φ_i of the set φ corresponds to the way of the message embedding from the set M in the container of the set L with the help of the specific key K_i.

Let's fix the set of keys $K^* = \{K_1^*, K_2^*, \ldots, K_k^*\}$, in general, to $K \neq K^*$. All the elements of the inverse mappings' set:

$$\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, \ldots, \varphi_k^{-1}\}$$

are given the appropriate key:

$$\varphi_i^{-1} : E \xrightarrow{K_i^*} (M, L).$$

Each specific mapping φ_i^{-1} of the set φ^{-1} corresponds to a process of recovering messages from the filled container (and the formation of empty container) with the key K_i^*. If the key K_i^* is known, there is only one possible answer as a result of the extraction operation – an element of the set M and an element of the set L:

$$(M_j, L_l) = \varphi_i^{-1}(E_w, K_i^*).$$

For robust systems the following equality is correct:

$$(M_j, L_l) = \varphi_i^{-1}(E_w + \varepsilon, K_i^*),$$

i.e. slight change of the filled container (for the value ε) will not lead to an incorrect message retrieval.

Fragile steganosystems are characterized with the performance of inequality:

$$(M_j, L_l) \neq \varphi_i^{-1}(E_w + \varepsilon, K_i^*)$$

for an arbitrarily small value ε.

Thus, an abstract definition of steganographic system includes the following sets of M, L, E, φ, φ^{-1}, K and K^* (the sets of open texts, empty containers and steganograms (filled containers), sets of forward and backward mappings, and sets of the corresponding keys).

Fig. 2 represents a block diagram of a steganographic system.

A message source generates a flow of information from a variety of information messages I_j from the set $I = \{I_1, I_2, \ldots, I_m\}$, which, after preliminary converting in a precoder is formed as a message M_j from the set M. A precoder performs a function of preliminary preparation of the informational message to embedding in a container (such as converting an informational message in an array of specially formatted digital data).

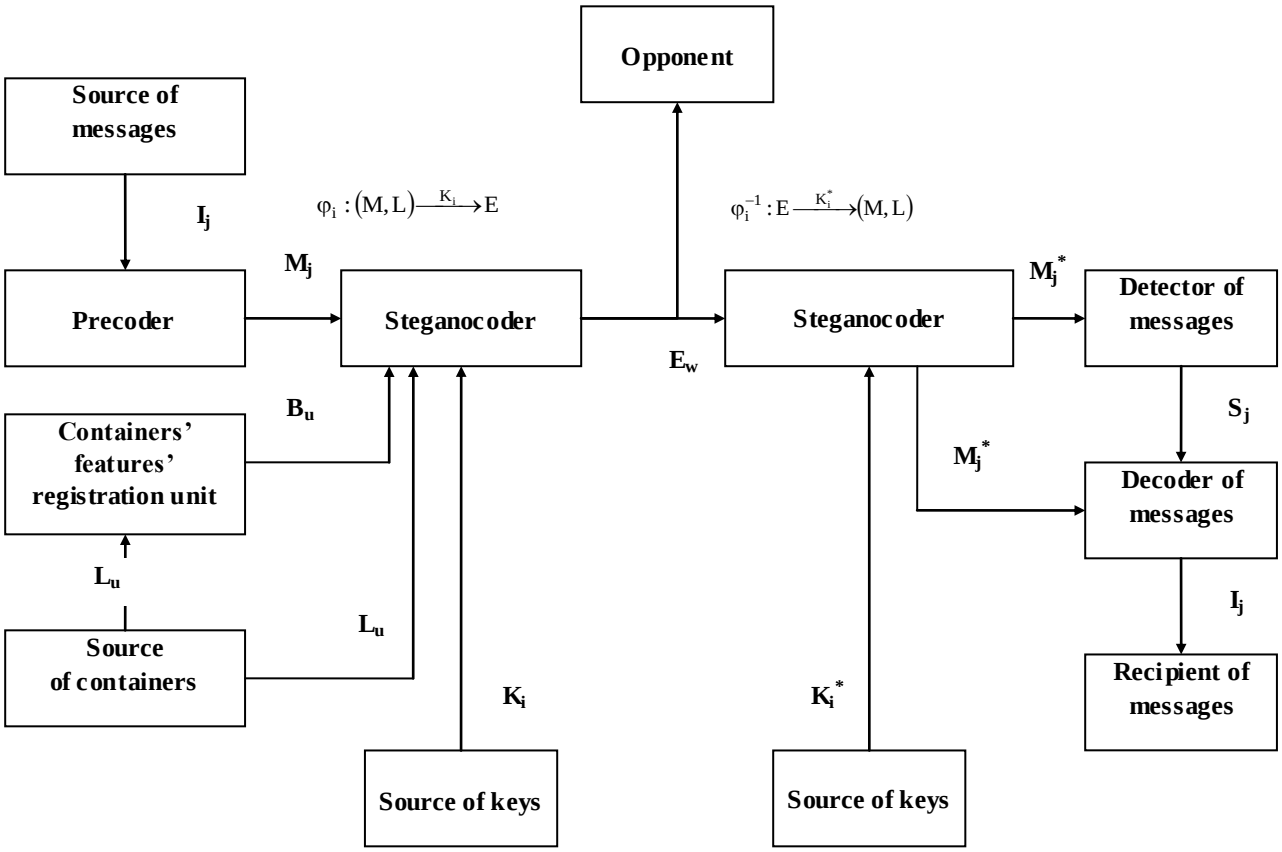

Fig. 2. Block diagram of steganographic system

Each message $M_j \in M = \{M_1, M_2, \ldots, M_m\}$ corresponds to the probability $P(M_j)$. The probability distribution of a random process is given by a cumulative distribution of probability distribution sets of random variables, i.e. the set of probabilities:

$$P_M = \{P(M_1), P(M_2), \ldots, P(M_m)\}. \quad (6)$$

Source of containers generates a flow of empty containers L_u from the set $L = \{L_1, L_2, \ldots, L_l\}$. Work of the source of containers can also be described by some random process, the specific realization of which is the container L_u. In this case we deal with random containers that can be attributed to the corresponding probabilities:

$$P_L = \{P(L_1), P(L_2), \ldots, P(L_l)\}.$$

Much more often, in practice, a different type of containers is used, the formation of which is impossible to describe by a random process. In this case, the source container works on a deterministic rule, asked or authorized (e.g., transmitting) side, or the opponent. In the first case, a so-called selected container, i.e. the container used is not formed by chance, but is chosen by the party responsible for some non-stochastic characteristics. In the second case, the source container is managed by the opponent, and the containers themselves are generated by an attacker and imposed the transmitting side by a deterministic rule. Thus, we have the so-called imposed-on container.

In the simplest case, a lot of empty containers contain only one element, which is used by the transmitting side to embed message and secretly pass it through a communication channel.

L_u shaped container is processed by the containers' features' registration unit. The main function of the containers' features' registration unit is the selection of attributes (features) B_u of incoming container L_u, which will be used for embedding the message to M_j.

A source of keys in steganographic system generates a flow of the set of keys K and/or K^*. Each key $K_i \in K = \{K_1, K_2, \ldots, K_k\}$ corresponds to some probability $P(K_i)$, and each $K_i^* \in K^* = \{K_1^*, K_2^*, \ldots, K_k^*\}$ corresponds to the probability $P(K_i^*)$. Random key generation process is given by the sets of probabilities:

$$P_K = \{P(K_1), P(K_2), ..., P(K_k)\} \quad (7)$$

and:

$$P_{K^*} = \{P(K_1^*), P(K_2^*), ..., P(K_k^*)\}. \quad (8)$$

Sets of values of a priori probabilities (6 - 8) form a priori knowledge of the opponent about the source of messages and the source of keys, respectively. In fact, these sets characterize the a priori knowledge of the opponent on the possible "weakness" of steganographic system.

Key selection K_i determines specific mapping φ_i of the set of mappings φ. With the help of mapping φ_i corresponding to the selected key K_i, following received message M_j and the received container L_u based on identified characteristics B_u of the container L_u, a steganogram (full container) is formed:

$$E_w = \varphi_i(K_i, M_j, L_u),$$

$$i \in [1,2,...,k],\ j \in [1,2,...,m],\ u \in [1,2,...,l],\ w \in [1,2,...,n],\ n \geq m.$$

A steganogram E_w is transferred to the receiving point by a certain channel and may be intercepted by the opponent. At the receiving end with the help of the reverse mapping φ_i^{-1} (given by the key K_i^*) of the steganogram E_w restored the original message and the empty container is restored:

$$(M_j, L_u) = \varphi_i^{-1}(K_i, E_w).$$

When transferring the steganogram E_w through a communication channel and because of the opponent's possible impact on E_w, a transmitted steganogram may become distorted. In this case, the receiving side will get a mixture of a delivered filled container and of a feedback to the container during the transmission through the communication channel: $E_w+\varepsilon$. Performing the operation of a reverse mapping φ_i^{-1} (given by the key K_i^*) will lead, in this case, to a certain evaluation of a transferred message and give an empty container, i.e. we get:

$$(M_j^*, L_u^*) = \varphi_i^{-1}(K_i, E_w + \varepsilon).$$

For fragile steganographic systems, an inequality $M_j^* \neq M_j$ should lead to a message rejection, i.e. at the slightest distortion of the container ($\varepsilon \neq 0$), an extracted assessment M_j^* should not lead to the reading of embedded message (the message M_j is destroyed when $\varepsilon \neq 0$).

Robust steganographic systems are resistant to the impact on a filled container. In the above notations, this means that when $\varepsilon \neq 0$, an extracted assessment M_j^* should be compared to one of the possible messages (ideally, with the message M_j). At the same time, the derived from a communication channel container E_w can contain no embedded message at all, i.e. the extracted from the container assessment M_j^* should not be compared to any of the possible messages. A built-in message detection functions at a receiving side are assigned to messages' detector, which by the received assessment M_j^* decide on the presence or absence of an internal message in the received container E_w. Thus, the estimate of the detector S_j can be interpreted as a binary (yes/no) decision of an error-correcting decoder on the presence or absence of uncorrectable errors. The decoding itself is performed at a messages decoder, the main functions of which are to compare the extracted assessment M_j^* with one of the possible messages M_j and to transform the latter to the informational message I_j provided to the recipients of information.

The opponent may capture the steganogram E_w. In this case, he can use it to try to calculate posteriori probabilities of various possible messages:

$$P_{M|E_w} = \{P(M_1|E_w), P(M_2|E_w), ..., P(M_m|E_w)\} \quad (9)$$

and of a variety of possible keys:

$$P_{K|E_w} = \{P(K_1|E_w), P(K_2|E_w), ..., P(K_k|E_w)\}, \quad (10)$$

that could be used in the formation of the steganogram E_w.

The sets of posterior probabilities (9 - 10) form a posteriori knowledge of the opponent about the keys $K = \{K_1, K_2, ..., K_k\}$ and the messages $M = \{M_1, M_2, ..., M_m\}$ after the interception of the steganogram E_w. In fact, the sets $P_{K|E_w}$ and $P_{M|E_w}$ are sets of assumptions, which are assigned the corresponding probabilities.

4. Conclusions

In this paper we have analyzed and studied the formal mathematical description and a block diagram of a secret system. By analogy with the examined formalization of the theory of secret systems the basic elements and mathematical operators, abstractly describing steganographic information protection system, are introduced. In the introduces formalization a definition of fragile and robust steganosystems has been received, as well as probabilistic indicators characterizing a posteriori knowledge of the opponent on the secret keys and embedded messages. A promising direction for further research is the analysis and theoretical basis of criteria and performance indicators of steganographic security systems, the study of the properties of the known examples of steganosystems by entering the show-makers and the criteria of performance evaluation.

References

[1] C. Shannon, A Mathematical Theory of Information and Cybernetics. – M: FL, 1963. – 829 p.
[2] C. Shannon, Communication in the Presence of Noise. // Information Theory and its Applications. Collection of translations. – Moscow: FIZMATGIZ, 1959. – P. 82-12.
[3] C. Shannon, Communication Theory of Secret Systems // C. Shannon, A Mathematical Theory of Information and Cybernetics. – Moscow: Publishing House of Foreign Literature, 1963. – P.333-402.
[4] Dolgov V. I., Statistical Theory of Receiving Digital Signals. – Kh.: KhHMCSMF, 1989. – 448 p.
[5] Stasev Y. V., Basic Theory of Building Signals. - Kh.: KhMU, 1999. – 87 p.
[6] MacWilliams F. J., Sloane N. J. A., The Theory of Error-Correcting Codes. –M.: Sviaz, 1979. – 744 p.
[7] Naumenko M. I., Stasev Y. V., Kuznetsov O. O., Theoretical Basis and Methods of Algebraic Block Codes. Monography. – Kh.: KhAFU, 2005. – 267 p.
[8] Moldovyan N. A., Moldovyan A. A., Eremeev M.A., Cryptography: From Primitive to the Synthesis of Algorithms. – St.: BHV-Petersburg, 2004. – 448p.
[9] V.M. Sidelnikov, Cryptography and Coding Theory. Materials of the conference "Moscow University and the Development of Cryptography in Russia", Moscow State University. – 2002. – 22 p.
[10] Salomaa A., Public-key Cryptography: Trans. from English, – M.: Mir, 1995. – 318 p.
[11] Konahovich G. F., Puzyrenko A. Y., Computer Steganography. Theory and Practice. – K.: "MK-Press"b 2006. – 288 p., Ill.
[12] Sklar B., Digital Communication. Theoretical Basis and Practical Application. – M. Williams, 2003. – 1104 p.

Author Name

Alexey Smirnov was born in 1977. Graduated from Kharkiv Military University with a degree in "Automated Control Systems" in 1999. Candidate of Technical Sciences. Associate Professor of Department of Software of Kirovohrad National Technical University, Ukraine. Field of interest: information security and routing issues.