Mathematical Problems of Computer Science 24, 2005, 89–103.

On Information Hiding System With Multiple Messages*

Mariam E. Haroutunian and Smbat A. Tonoyan

Institue for Informatics and Automation Problems of NAS of RA
e-mail armar@ipia.sci.am, smbatt@ipia.sci.am

Abstract

Many algorithms and schemes of multiple watermarking, fingerprinting and multimedia data creation are implementing to hide more than one watermark. Information theoretical analysis of information hiding system with multiple messages is considered in this paper. The rate-reliability-distortion function (which we call *the information hiding E-capacity* [5, 9]) for this system, in case of two messages (watermarks) is investigated. The inner bounds for information hiding E-capacity and for information hiding capacity [1] regions are constructed.

1 Introduction

Various applications and technical problems, such as multimedia data creation, copyright protection, digital watermarking and fingerprinting generate necessity to explore many complex configurations of information hiding systems. Each model of information hiding system presents the mechanism where an original data is modified in order to embed some extra information (watermark, fingerprint, etc.) before the public distribution [5, 1, 10, 11].

Many algorithms and protocols of digital watermarking are implemented to hide more than one watermark within a single object. Such schemes are applied in the multiple watermarking [6]. In fingerprinting different watermarks are embedded in a single object for identification of one of many users.

Without loss of generality, we explore the model of information hiding system with two messages, which is drawn on fig. 1.

Two independent messages, generated by the corresponding message sources (1 and 2 on fig. 1) are embedded within the same host data block, which is the output of host data source (3 on fig. 1). The data blocks, with the embedded messages (marked blocks) are publicly transmitted to the corresponding receivers via different channels (6 and 7 on fig. 1), which can be attacked by different independent attackers. These attacks are directed to changing, removing or spoiling the hidden information to make it unrestorable from the marked blocks. Each user decodes (8 and 9 on fig. 1) the message designated for him. The side information blocks are shared between a single information hider and two opposite different users (the side information can consist of the features of the host data or of the cryptographic keys).

*The work was partially supported by 04.10.31 Target Program of RA.

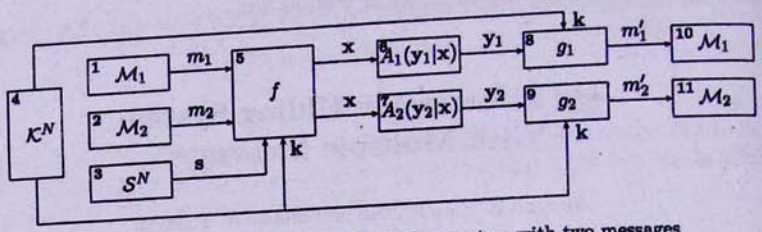

Fig. 1. The model of information hiding system with two messages

The attackers are assumed to be aware about the information hiding strategy but their attack algorithms are unknown to the users and information hider. The side information is not available to the attackers.

The information hiding process must be *transparent*. It means that the marked data blocks must be similar to host data blocks, or the distortion, introduced during information hiding process must not exceed some fixed allowed distortion level. And the system must be *robust* - the distortion, introduced by any attacker also must not exceed the allowable distortion level, defined for him.

The notion of E-capacity [4] (rate-reliability-distortion function) for this system is investigated, which we call *the information hiding E-capacity*. It expresses the dependences between the *information hiding rates, reliability* and the distortion levels, defined for information hider and for attackers. The random coding bound for information hiding E-capacity and the inner bound for information hiding capacity region are constructed.

Certain similar results for the various cases of information hiding systems with single message are obtained by P. Moulin and J. O'Sullivan [1], M. Haroutunian and S. Tonoyan [5, 9], N. Merhav [10], N. Merhav and A. Somekh-Baruch [11].

Theoretical analysis of studied information hiding system is related to the analysis of broadcast channels [12, 13, 14].

2 Statement of the Problem

We use the following notation: the discrete finite sets are denoted by the calligraphic letters (e.g. $\mathcal{X}$), the random variables (RV) by the upper case letters (e.g. X), their individual values by the lower case letters (e.g. x). The probability distribution of RV X on $\mathcal{X}$ we denote by $P(x) = \{P(x), x \in \mathcal{X}\}$. The N-length vector of RVs with the identically independently distributed components is denoted by $X^N = (X_1, ..., X_N)$, which takes its values $\mathbf{x} = (x_1, ..., x_N)$ within the set $\mathcal{X}^N$. By $I_P(X \wedge Y)$ the mutual information of RVs X, Y and by $I_P(X \wedge Y|Z)$ the conditional mutual information of RVs X, Y, under condition of Z is denoted ($P = \{P(x, y, z), x \in \mathcal{X}, y \in \mathcal{Y}, z \in \mathcal{Z}\}$). The informational divergence of PDs $Q(s)$ and $Q'(s)$ we denote by $D(Q'\|Q)$ and the conditional divergence of PDs $Q(s)$ and $Q'(s)$ under the condition of $P(x)$ we denote $D(Q'\|Q|P)$. The entropy of RV X we denote by $H_P(X)$. And we denote by $\mathcal{T}_Q^N(S)$ the set of N-length vectors $(\mathbf{s})$ of the type Q, and by $\mathcal{T}_{Q,P}^N(X|\mathbf{s})$ the set of N-length vectors $\mathbf{x}$ of conditional type P, for given $\mathbf{s} \in \mathcal{T}_Q^N(S)$. All logarithms and exponents in the paper are of the base 2.

Now we pass to the mathematical description of the system, presented in fig. 1. Two independent messages m_1 and m_2 which are independently and identically distributed on

the message sets $\mathcal{M}_1$, $\mathcal{M}_2$ are embedded within the same host data block $\mathbf{s} \in \mathcal{S}^N$. Marked data blocks $\mathbf{x} \in \mathcal{X}^N$ are transmitted to the two independent users via different channels. The channels are untrusted and can be attacked. In the result of possible attacks the users receive transformed data blocks $\mathbf{y}_1 \in \mathcal{Y}_1^N$ and $\mathbf{y}_2 \in \mathcal{Y}_2^N$, instead of $\mathbf{x}$. Each of users restores the messages designated for it. The side information, in the form of data blocks $\mathbf{k} \in \mathcal{K}^N$ is shared between the information hider (encoder) and users (decoders). The RV's S and K, describing the host data and side information sources are distributed jointly, with the given PD $Q = \{Q(s,k), s \in \mathcal{S}, k \in \mathcal{K}\}$. Depending on the various cases the RVs S and K also can be distributed independently, for example when the side information blocks $\mathbf{k} \in \mathcal{K}^N$ are the cryptographic keys. It is assumed that the attackers are aware about the encoding and decoding strategies, know the PDs of all RVs, but they don't learn the side information. The strategies of the attackers are unknown to the encoder and the decoders.

For the mathematical description of the transparency and robustness we define the following notions: the distortion functions are the mappings $d_0 : \mathcal{S} \times \mathcal{X} \to [0, \infty)$, $d_1 : \mathcal{X} \times \mathcal{Y}_1 \to [0, \infty)$, $d_2 : \mathcal{X} \times \mathcal{Y}_2 \to [0, \infty)$ and allowed distortion levels for the information hider and for the attackers are positive numbers $\Delta_0, \Delta_1, \Delta_2$ respectively. Denote by $\mathbf{\Delta} = (\Delta_0, \Delta_1, \Delta_2)$ the vector of distortion levels of the system. The distortion functions are supposed to be symmetric:

$$d_0(s,x) = d_0(x,s), \; d_i(x,y_i) = d_i(y_i,x) \; i = 1,2.$$

and

$$d_0(s,x) = 0 \text{ if } s = x, \; d_i(x,y_i) = 0 \text{ if } x = y_i, \; i = 1,2.$$

Distortion functions for N-length vectors are:

$$d_0^N(\mathbf{s},\mathbf{x}) = \frac{1}{N}\sum_{n=1}^{N} d_0(s_n,x_n), \; d_i^N(\mathbf{x},\mathbf{y}_i) = \frac{1}{N}\sum_{n=1}^{N} d_i(x_n,y_{i,n}), \; i = 1,2.$$

We use auxiliary RVs U_1 and U_2 taking values in the discrete finite sets $\mathcal{U}_1$ and $\mathcal{U}_2$ and forming the Markov chain $(U_1, U_2, S, K) \to X \to (Y_1, Y_2)$, with the RVs S, K, X, Y_1, Y_2.

The information hiding N-length code (f, g_1, g_2) is a triple of mappings $f : \mathcal{M}_1 \times \mathcal{M}_2 \times \mathcal{S}^N \times \mathcal{K}^N \to \mathcal{X}^N$, $g_1 : \mathcal{Y}_1^N \times \mathcal{K}^N \to \mathcal{M}_1$ and $g_2 : \mathcal{Y}_2^N \times \mathcal{K}^N \to \mathcal{M}_2$, where f is the encoding and g_1, g_2 are the decoding functions.

A discrete memoryless covert channel P, designed by information hider, subject to distortion level Δ_0, is a probability distribution $P = \{P(u_1,u_2,x|s,k), \; u_1 \in \mathcal{U}_1, \; u_2 \in \mathcal{U}_2 \; x \in \mathcal{X}, \; s \in \mathcal{S}, \; k \in \mathcal{K}\}$ such, that

$$\sum_{u_1,u_2,x,s,k} d_0(s,x) P(u_1,u_2,x|s,k) Q(s,k) \le \Delta_0.$$

Denote by $\mathcal{P}(Q,\Delta_0)$ the set of all covert channels, subject to distortion level Δ_0. The N-length memoryless expression for the covert channel P is:

$$P^N(\mathbf{u}_1,\mathbf{u}_2,\mathbf{x}|\mathbf{s},\mathbf{k}) = \prod_{n=1}^{N} P(u_{1n},u_{2n},x_n|s_n,k_n).$$

Discrete memoryless attack channels A_i, $i = 1,2$, designed by two independent attackers, subject to distortion levels Δ_i, $i = 1,2$, under the condition of covert channel $P \in \mathcal{P}(Q,\Delta_0)$,

are defined by a probability distributions $A_i = \{A_i(y_i|x),\ y_i \in \mathcal{Y}_i,\ x \in \mathcal{X}\},\ i = 1,2$ such, that

$$\sum_{u_1,u_2,x,y,s,k} d_i(x,y_i)A_i(y_i|x)P(u_1,u_2,x|s,k)Q(s,k) \le \Delta_i,\ i = 1,2.$$

Denote by $\mathcal{A}_i(Q,P,\Delta_i),\ i = 1,2$ the sets of all attack channels, under the condition of covert channel $P \in \mathcal{P}(Q,\Delta_0)$ and subject to distortion levels $\Delta_i,\ i = 1,2$.

The N-length memoryless expressions for the attack channels $A_i,\ i = 1,2$ are:

$$A_i^N(\mathbf{y}_i|\mathbf{x}) = \prod_{n=1}^{N} A(y_{in}|x_n),\ i = 1,2.$$

Probabilities of erroneous reconstructions of messages $m_i \in \mathcal{M}_i,\ i = 1,2$ for $(\mathbf{s},\mathbf{k}) \in \mathcal{S}\times\mathcal{K}$ via channel $A_i,\ i = 1,2$ are:

$$e_i(f,g_i,N,m_1,m_2,\mathbf{s},\mathbf{k},A_i) = A_i^N\{\mathcal{Y}_i^N - g_i^{-1}(m_i|\mathbf{k})|f(m_1,m_2,\mathbf{s},\mathbf{k})\},i = 1,2. \quad (1)$$

Error probabilities of messages $m_i \in \mathcal{M}_i,\ i = 1,2$ averaged over all $(\mathbf{s},\mathbf{k}) \in \mathcal{S}\times\mathcal{K}$, equal to

$$e_i(f,g_i,N,m_1,m_2,Q,A_i) = \sum_{(\mathbf{s},\mathbf{k})\in\mathcal{S}^N\times\mathcal{K}^N} Q^N(\mathbf{s},\mathbf{k})e_i(f,g_i,N,m_1,m_2,\mathbf{s},\mathbf{k},A_i).$$

Error probabilities of the code, for any messages $m_i \in \mathcal{M}_i,\ i = 1,2$, maximal over all attack channels $\mathcal{A}_i(Q,P,\Delta_i),\ i = 1,2$ is denoted by:

$$e_i(f,g_i,N,m_1,m_2,Q,P,\Delta_i) = \max_{A_i\in\mathcal{A}_i(Q,P,\Delta_i)} e_i(f,g_i,N,m_1,m_2,Q,A_i),\ i = 1,2.$$

Maximal error probabilities of the code, maximal over all attack channels from $\mathcal{A}_i(Q,P,\Delta_i),\ i = 1,2$, equals to:

$$e_i(f,g_i,N,Q,P,\Delta_i) = \max_{m_1\in\mathcal{M}_1,m_2\in\mathcal{M}_2} e_i(f,g_i,N,m_1,m_2,P,Q,\Delta_i),i = 1,2,$$

and average error probabilities of the code, maximal over all attack channels from $\mathcal{A}_i(Q,P,\Delta_i),\ i = 1,2$, equals to:

$$\overline{e_i}(f,g_i,N,Q,P,\Delta_i) = \frac{1}{M_1M_2}\sum_{m_1\in\mathcal{M}_1,m_2\in\mathcal{M}_2} e_i(f,g_i,N,m_1,m_2,P,Q,\Delta_i),i = 1,2, \quad (2)$$

Nonnegative numbers (R_1,R_2) are called E-achievable information hiding rates pair for the system with two messages, if for any $\delta_i > 0,\ i = 1,2$, for sufficiently large N there exists a code that

$$\frac{1}{N}\log M_i \ge R_i - \delta_i,\ i = 1,2,$$

and

$$e_i(f,g_i,N,Q,P,\Delta_i) \le \exp\{-NE\},\ i = 1,2, \quad (3)$$

where $E > 0$ is called *the reliability*.

The region of all E-achievable information hiding rate pairs (R_1,R_2) is called *information hiding E-capacity* and denoted $\mathcal{R}(Q,E,\Delta) = \mathcal{C}(Q,E,\Delta)$. We also consider the E-capacity region $\overline{\mathcal{C}}(Q,E,\Delta)$ for the case of average error probabilities in (3). The region of maximum rates of reliable transmission is called *information hiding capacity* $\mathcal{C}(Q,\Delta)$ [1, 5, 9].

Main Result

Consider the following functions:

$$\mathcal{R}_\tau(Q,P,E,\Delta)=\bigcup_{i=1,2}\{(R_1,R_2):$$

$$0\le R_i\le \min_{A_i\in\mathcal{A}_i(Q,P,\Delta_i)}\min_{Q',V_i:D(Q'\circ P\circ V_i\|Q\circ P\circ A_i)\le E}|I_{Q',P,V_i}(Y_i\wedge U_i|K)-$$
$$-I_{Q',P}(S\wedge U_i|K)+D(Q'\circ P\circ V_i\|Q\circ P\circ A_i)-E|^+,$$
$$0\le R_{3-i}\le \min_{A_{3-i}\in\mathcal{A}_{3-i}(Q,P,\Delta_{3-i})}\min_{Q',V_{3-i}:D(Q'\circ P\circ V_{3-i}\|Q\circ P\circ A_{3-i})\le E}|I_{Q',P,V_{3-i}}(Y_{3-i}\wedge U_{3-i}|K)-$$
$$-I_{Q',P}(U_2\wedge U_1,S|K)+D(Q'\circ P\circ V_{3-i}\|Q\circ P\circ A_{3-i})-E|^+\}. \qquad (4)$$

$$\mathcal{R}_\tau(Q,E,\Delta)=\bigcup_{P\in\mathcal{P}(Q,\Delta_0)}\mathcal{R}_\tau(Q,P,E,\Delta).$$

Theorem. *For all $E>0$ and for the system with the vector of distortion levels Δ, the random coding bound $\mathcal{R}_\tau(Q,E,\Delta)$ is the inner bound of information hiding E-capacity region for maximal and average error probabilities:*

$$\mathcal{R}_\tau(Q,E,\Delta)\subseteq C(Q,E,\Delta)\subseteq\overline{C}(Q,E,\Delta).$$

Corollary. *From the (4), when $E\to 0$, using time sharing arguments [12, 13], we obtain the inner bound of information hiding capacity region.*

$$C(Q,\Delta)\supseteq\mathcal{R}_\tau(Q,\Delta)=\bigcup_{P\in\mathcal{P}(Q,\Delta_0)}\{(R_1,R_2):$$

$$0\le R_i\le\min_{A_i\in\mathcal{A}_i(Q,P,\Delta_i)}[I_{Q,P,A_i}(Y_i\wedge U_i|K)-I_{Q,P}(S\wedge U_i|K)],\ i=1,2,$$
$$\le R_1+R_2\le\sum_{i=1,2}\min_{A_i\in\mathcal{A}_i(Q,P,\Delta_i)}[I_{Q,P,A_i}(Y_i\wedge U_i|K)-I_{Q,P}(S\wedge U_i|K)]-I_{Q,P}(U_1\wedge U_2|S,K)\}.$$

Similar results for E-capacity for the broadcast channel is obtained by M. Haroutunian [14] and for the information hiding system by M. Haroutunian and S. Tonoyan [5, 9].

Proof of the Theorem

The theorem is proved by the Shannon's random coding arguments and the method of types [18, 19, 16].

Denote by $\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1,m_2,\mathbf{s},\mathbf{k})$ the triple of vectors $\mathbf{u}_1(m_1,\mathbf{s},\mathbf{k})\mathbf{u}_2(m_1,m_2,\mathbf{s},\mathbf{k})\mathbf{x}(m_1,m_2,\mathbf{s},\mathbf{k})$ from the $\mathcal{T}^N_{Q,P}(U_1,U_2,X|\mathbf{s},\mathbf{k})$, and denote by $\mathcal{Z}(\mathcal{M}_1,\mathcal{M}_2,\mathcal{T}^N_Q(S,K))$ the family of all 3D matrices $\mathbf{Z}=\{\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1,m_2,\mathbf{s},\mathbf{k})\}^{(\mathbf{s},\mathbf{k})\in\mathcal{T}^N_Q(S,K)}_{m_1\in\mathcal{M}_1,\ m_2\in\mathcal{M}_2}$, the planes

$$\mathbf{Z}(\mathbf{s},\mathbf{k})=\begin{pmatrix}\mathbf{u}_1\mathbf{u}_2\mathbf{x}(1,1,\mathbf{s},\mathbf{k}) & \dots & \mathbf{u}_1\mathbf{u}_2\mathbf{x}(1,M_2,\mathbf{s},\mathbf{k})\\ \mathbf{u}_1\mathbf{u}_2\mathbf{x}(2,1,\mathbf{s},\mathbf{k}) & \dots & \mathbf{u}_1\mathbf{u}_2\mathbf{x}(2,M_2,\mathbf{s},\mathbf{k})\\ \dots & & \\ \mathbf{u}_1\mathbf{u}_2\mathbf{x}(M_1,1,\mathbf{s},\mathbf{k}) & \dots & \mathbf{u}_1\mathbf{u}_2\mathbf{x}(M_1,M_2,\mathbf{s},\mathbf{k})\end{pmatrix}$$

of which are collections of not necessarily distinct vector triples.

Denote by $\beta_{Q,P}(m_1, m_2, \mathbf{s}, \mathbf{k})$ for any $m_1 \in \mathcal{M}_1, m_2 \in \mathcal{M}_2$ and $(\mathbf{s}, \mathbf{k}) \in \mathcal{T}_Q^N(S, K)$ the random event

$$\beta_{Q,P}(m_1, m_2, \mathbf{s}, \mathbf{k}) = \{\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1, m_2, \mathbf{s}, \mathbf{k}) \in \mathcal{T}_{Q,P}^N(U_1, U_2, X|\mathbf{s}, \mathbf{k})\},$$

and consider the following sets:

$$\mathcal{SK}(m_1, m_2, Q, P) = \{(\mathbf{s}, \mathbf{k}) \in \mathcal{T}_Q^N(S, K) : \text{for which } \beta_{Q,P}(m_1, m_2, \mathbf{s}, \mathbf{k}) \text{ takes place}\},$$

$$m_1 \in \mathcal{M}_1,\ m_2 \in \mathcal{M}_2,$$

$$\mathcal{M}_i(m_{3-i}, \mathbf{s}, \mathbf{k}, Q, P) = \{m_i \in \mathcal{M}_i : \text{for which } \beta_{Q,P}(m_1, m_2, \mathbf{s}, \mathbf{k}) \text{ takes place}\},$$

$$m_{3-i} \in \mathcal{M}_{3-i},\ (\mathbf{s}, \mathbf{k}) \in \mathcal{T}_Q^N(S, K), i = 1, 2.$$

$$\mathcal{M}_1\mathcal{M}_2(\mathbf{s}, \mathbf{k}, Q, P) = \{m_1 \in \mathcal{M}_1,\ m_2 \in \mathcal{M}_2 : \text{for which } \beta_{Q,P}(m_1, m_2, \mathbf{s}, \mathbf{k}) \text{ takes place}\},$$

$$\mathcal{M}_1\mathcal{M}_2\mathcal{SK}(Q, P) = \{(m_1, m_2, \mathbf{s}, \mathbf{k}), m_1 \in \mathcal{M}_1, m_2 \in \mathcal{M}_2, (\mathbf{s}, \mathbf{k}) \in \mathcal{T}_Q^N(S, K) : \text{for which}$$

$$\beta_{Q,P}(m_1, m_2, \mathbf{s}, \mathbf{k}) \text{ takes place}\}.$$

Lemma 1. *For all $E > 2\delta \geq 0$, $i = 1, 2$, type Q, covert channel $P \in \mathcal{P}(Q, \Delta_0)$ and the sets of attack channels $\mathcal{A}_i(Q, P, \Delta_i)$, $i = 1, 2$ there exists a matrix $\mathbf{Z} = \{\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1, m_2, \mathbf{s}, \mathbf{k})\}_{m_1=\overline{1,M_1},\ m_2=\overline{1,M_2}}^{(\mathbf{s},\mathbf{k})\in\mathcal{T}_Q^N(S,K)}$, with*

$$M_1 = \exp\left\{N \min_{A_1 \in \mathcal{A}_1(Q,P,\Delta_1)} \min_{V_1 : D(V_1\|A_1|Q,P) \leq E} |I_{Q,P,V_1}(Y_1 \wedge U_1|K) - \right.$$

$$\left. - I_{Q,P}(S \wedge U_1|K) + D(V_1\|A_1|Q, P) - E + 2\delta|^+\right\}, \tag{5}$$

$$M_2 = \exp\left\{N \min_{A_2 \in \mathcal{A}_2(Q,P,\Delta_2)} \min_{V_2 : D(V_2\|A_2|Q,P) \leq E} |I_{Q,P,V_2}(Y_2 \wedge U_2|K) - \right.$$

$$\left. - I_{Q,P}(U_2 \wedge U_1, S|K) + D(V_2\|A_2|Q, P) - E + 2\delta|^+\right\}, \tag{6}$$

such that for each vector pair $(\mathbf{s}, \mathbf{k}) \in \mathcal{T}_Q^N(S, K)$ vectors $\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1, m_2, \mathbf{s}, \mathbf{k})$ for different $m_i \in \mathcal{M}_i(m_{3-i}, \mathbf{s}, \mathbf{k}, Q, P)$, $i = 1, 2$ are distinct and

$$\Pr\{\overline{\beta}_{Q,P}(m_1, m_2, \mathbf{s}, \mathbf{k})\} \leq \exp\{-\exp\{N\delta/2\}\}, \tag{7}$$

and for any $(m_1, m_2, \mathbf{s}, \mathbf{k}) \in \mathcal{M}_1\mathcal{M}_2\mathcal{SK}(Q, P)$, conditional types $V_i, \hat{V}_i : \mathcal{X} \to \mathcal{Y}_i$, $i = 1, 2$ for sufficiently large N, the following inequalities hold:

$$\left|\mathcal{T}_{Q,P,V_i}^N(Y_i|\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1, m_2, \mathbf{s}, \mathbf{k}), \mathbf{s}, \mathbf{k}) \bigcap \right.$$

$$\left. \bigcap \bigcup_{m_i' \neq m_i} \bigcup_{\mathbf{s}' : (\mathbf{s}', \mathbf{k}) \in \mathcal{SK}(m_1', m_2', Q, P)} \bigcup_{m_{3-i}' \in \mathcal{M}_{3-i}(m_i', \mathbf{s}', \mathbf{k}, Q, P)} \mathcal{T}_{Q,P,\hat{V}_i}^N(Y_i|\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1', m_2', \mathbf{s}', \mathbf{k}), \mathbf{s}', \mathbf{k})\right| \leq$$

$$\leq |\mathcal{T}_{Q,P,V_i}^N(Y_i|\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1, m_2, \mathbf{s}, \mathbf{k}), \mathbf{s}, \mathbf{k})| \exp\left\{-N\left|E - \min_{A_i \in \mathcal{A}_i(Q,P,\Delta_i)} D(\hat{V}_i\|A_i|Q, P)\right|^+\right\}, \tag{8}$$

$$i = 1, 2.$$

The proof of lemma 1 is given in the next section. Lemma 2 follows from lemma 1.

Lemma 2. *For all $E > 2\delta \geq 0$, $i = 1, 2$, type Q', such that $D(Q'\|Q) \leq E$, covert channel $P \in \mathcal{P}(Q, \Delta_0)$ and the sets of attack channels $\mathcal{A}_i(Q, P, \Delta_i)$, $i = 1, 2$ there exists a matrix $\mathbf{Z} = \{\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1, m_2, \mathbf{s}, \mathbf{k})\}_{m_1=\overline{1,M_1},\ m_2=\overline{1,M_2}}^{(\mathbf{s},\mathbf{k})\in\mathcal{T}_{Q'}^N(S,K)}$, with*

$$M_1 = \exp\left\{N \min_{A_1\in\mathcal{A}_1(Q,P,\Delta_1)} \min_{V_1: D(Q'\circ P\circ V_1\|Q\circ P\circ A_1)\leq E} |I_{Q',P,V_1}(Y_1 \wedge U_1|K) - \right.$$

$$\left. - I_{Q',P}(S \wedge U_1|K) + D(Q'\circ P\circ V_1\|Q\circ P\circ A_1) - E + 2\delta|^+\right\},$$

$$M_2 = \exp\left\{N \min_{A_2\in\mathcal{A}_2(Q,P,\Delta_2)} \min_{V_2: D(Q'\circ P\circ V_2\|Q\circ P\circ A_2)\leq E} |I_{Q',P,V_2}(Y_2 \wedge U_2|K) - \right.$$

$$\left. - I_{Q',P}(U_2 \wedge U_1, S|K) + D(Q'\circ P\circ V_2\|Q\circ P\circ A_2) - E + 2\delta|^+\right\},$$

such that for each vector pair $(\mathbf{s}, \mathbf{k}) \in \mathcal{T}_{Q'}^N(S, K)$ vectors $\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1, m_2, \mathbf{s}, \mathbf{k})$ for different $m_i \in \mathcal{M}_i(m_{3-i}, \mathbf{s}, \mathbf{k}, Q', P)$ are distinct and

$$\Pr\{\overline{\beta}_{Q',P}(m_1, m_2, \mathbf{s}, \mathbf{k})\} \leq \exp\{-\exp\{N\delta/2\}\}, \tag{9}$$

and for any $(m_1, m_2, \mathbf{s}, \mathbf{k}) \in \mathcal{M}_1\mathcal{M}_2\mathcal{SK}(Q', P)$, conditional types $V_i, \hat{V}_i : \mathcal{X} \to \mathcal{Y}_i$, $i = 1, 2$, for sufficiently large N the following inequalities hold:

$$\left|\mathcal{T}_{Q',P,V_i}^N(Y_i|\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1, m_2, \mathbf{s}, \mathbf{k}), \mathbf{s}, \mathbf{k}) \bigcap \right.$$

$$\left. \bigcap \bigcup_{m_i'\neq m_i\ \mathbf{s}':(\mathbf{s}',\mathbf{k})\in\mathcal{SK}(m_1',m_2',Q,P)} \bigcup_{m_{3-i}'\in\mathcal{M}_{3-i}(m_i',\mathbf{s}',\mathbf{k},Q',P)} \mathcal{T}_{Q',P,\hat{V}_i}^N(Y_i|\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1', m_2', \mathbf{s}', \mathbf{k}), \mathbf{s}', \mathbf{k})\right| \leq$$

$$\leq |\mathcal{T}_{Q',P,V_i}^N(Y_i|\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1, m_2, \mathbf{s}, \mathbf{k}), \mathbf{s}, \mathbf{k})| \times$$

$$\times \exp\left\{-N\left|E - \min_{A_i\in\mathcal{A}_i(Q,P,\Delta_i)} D(Q'\circ P\circ \hat{V}_i\|Q\circ P\circ A_i)\right|^+\right\},$$

$$i = 1, 2.$$

To prove the theorem 1 we shall use the lemma 3, which follow from lemma 2. Denote by

$$\mathcal{T}_Q^E(S, K) = \bigcup_{Q': D(Q'\|Q)\leq E} \mathcal{T}_{Q'}^N(S, K).$$

Lemma 3. *For all $E > 2\delta \geq 0$ $i = 1, 2$, covert channel $P \in \mathcal{P}(Q, \Delta_0)$ and the sets of attack channels $\mathcal{A}_i(Q, P, \Delta_i)$ $i = 1, 2$ there exists a matrix $\mathbf{Z} = \{\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1, m_2, \mathbf{s}, \mathbf{k})\}_{m_1=\overline{1,M_1},\ m_1=\overline{1,M_2}}^{(\mathbf{s},\mathbf{k})\in\mathcal{T}_Q^E(S,K)}$, with*

$$M_1 = \exp\left\{N \min_{A_1\in\mathcal{A}_1(Q,P,\Delta_1)} \min_{Q',V_1: D(Q'\circ P\circ V_1\|Q\circ P\circ A_1)\leq E} |I_{Q',P,V_1}(Y_2 \wedge U_1|K) - \right.$$

$$\left. - I_{Q',P}(S \wedge U_1|K) + D(Q'\circ P\circ V_1\|Q\circ P\circ A_1) - E + 2\delta|^+\right\}, \tag{10}$$

$$M_2 = \exp\Big\{N \min_{A_2 \in \mathcal{A}_2(Q,P,\Delta_2)} \min_{Q',V_2: D(Q'\circ P\circ V_2\|Q\circ P\circ A_2)\le E} |I_{Q',P,V_2}(Y_2 \wedge U_2|K) -$$

$$-I_{Q',P}(U_2 \wedge U_1, S|K) + D(Q'\circ P\circ V_2\|Q\circ P\circ A_2) - E + 2\delta|^+\Big\}, \qquad (11)$$

such that for each $Q' : D(Q'\|Q) \le E$, *vector pairs* $(\mathbf{s},\mathbf{k}) \in \mathcal{T}^N_{Q'}(S,K)$ *vectors* $\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1,m_2,\mathbf{s},\mathbf{k})$ *for different* $m_i \in \mathcal{M}_i(m_{3-i},\mathbf{s},\mathbf{k},Q',P)$ *are distinct and (9) is true and for any* $(m_1,m_2,\mathbf{s},\mathbf{k}) \in \mathcal{M}_1\mathcal{M}_2\mathcal{SK}(Q',P)$, *conditional types* $V_1,\hat{V}_1 : \mathcal{X}\to\mathcal{Y}_1$, *type* $\hat{Q}$, *such that* $D(\hat{Q}\|Q) \le E$, *for sufficiently large* N *the following inequality holds:*

$$|\mathcal{B}_i(Q,Q',\hat{Q},P,V_i,\hat{V}_i,m_1,m_2,\mathbf{s},\mathbf{k})| \le |\mathcal{T}^N_{Q',P,V_i}(Y_i|\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1,m_2,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k})|\times$$

$$\times \exp\left\{-N\left|E - \min_{A_i\in\mathcal{A}_i(Q,P,\Delta_i)} D(\hat{Q}\circ P\circ\hat{V}_i\|Q\circ P\circ A_i)\right|^+\right\},\ i=1,2, \qquad (12)$$

where

$$\mathcal{B}_i(Q,Q',\hat{Q},P,V_i,\hat{V}_i,m_1,m_2,\mathbf{s},\mathbf{k}) = \mathcal{T}^N_{Q',P,V_i}(Y_i|\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1,m_2,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k}) \bigcap$$

$$\bigcap \bigcup_{m_i'\ne m_i} \bigcup_{\mathbf{s}':(\mathbf{s}',\mathbf{k})\in\mathcal{SK}(m',\hat{Q},P)} \bigcup_{m_{3-i}'\in\mathcal{M}_{3-i}(m_i',\mathbf{s}',\mathbf{k},\hat{Q},P)} \mathcal{T}^N_{\hat{Q},P,\hat{V}_i}(Y_i|\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1',m_2',\mathbf{s}',\mathbf{k}),\mathbf{s}',\mathbf{k}).$$

Lemma 1,2 and 3 can be similarly written for M_1, M_2 replaced with roles.

Now to prove the theorem 1, we must show the existence of a code with $\mathcal{M}_1, \mathcal{M}_2$ satisfying (10), (11), such that for any $0<\varepsilon<E$, $i=1,2$, the following inequalities take place

$$e_i(f,g_i,N,Q,P,\Delta_1) \le \exp\{-N(E-\varepsilon)\},\ i=1,2.$$

We construct the code only for $(\mathbf{s},\mathbf{k})$ from $\mathcal{T}^E_Q(S,K)$, because for sufficiently large N,

$$Q^N\{(\mathbf{s},\mathbf{k}) \notin \mathcal{T}^E_Q(S,K)\} = Q^N\left\{(\mathbf{s},\mathbf{k}) \in \bigcup_{Q':D(Q'\|Q)>E} \mathcal{T}^N_{Q'}(S,K)\right\} \le$$

$$\le \sum_{Q':D(Q'\|Q)>E} Q^N\{(\mathbf{s},\mathbf{k}) \in \mathcal{T}^N_{Q'}(S,K)\} \le \sum_{Q':D(Q'\|Q)>E} \exp\{-ND(Q'\|Q)\} <$$

$$< (N+1)^{|\mathcal{S}||\mathcal{K}|}\exp\{-NE\} \le \exp\{-N(E-\varepsilon)\}. \qquad (13)$$

The existence of a matrix $\mathbf{Z} = \{\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1,m_2,\mathbf{s},\mathbf{k})\}^{(\mathbf{s},\mathbf{k})\in\mathcal{T}^E_Q(S,K)}_{m_1=\overline{1,M_1}\ m_2=\overline{1,M_2}}$, satisfying (7), (10), (11) and (12) is guaranteed by lemma 3.

Consider

$$\mathcal{SK}^E_Q(m_1,m_2,P) = \bigcup_{Q':D(Q'\|Q)\le E} \mathcal{SK}(m_1,m_2,Q',P).$$

Now apply the decoding rule for the decoder g_1 (similar decoding rule can be applied for decoder g_2): each $\mathbf{y}_2$ and $\mathbf{k}$ are decoded to such m_1 that for some m_2, $\mathbf{y}_1 \in \mathcal{T}^N_{Q',P,V}(Y_1|\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1,m_2,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k})$, where Q',P,V are such that $\min\limits_{A_1\in\mathcal{A}_1(Q,P,\Delta_1)} D(Q'\circ P\circ V\|Q\circ P\circ A_1)$ is minimal.

The decoder can make an error if the messages m_1 and m_2 are transmitted and $\overline{\beta}_{Q',P}(m_1,m_2,\mathbf{s},\mathbf{k})$ takes place or if $\beta_{Q',P}(m_1,m_2,\mathbf{s},\mathbf{k})$ takes place, $(\mathbf{s},\mathbf{k}) \in \mathcal{SK}^E_Q(m_1,m_2,P)$,

but there exist $m_1' \neq m_1$, type $\hat{Q}$ (such that $D(\hat{Q}\|Q) \leq E$), $\hat{V}_1$, m_2', vector pair $(\mathbf{s}', \mathbf{k}) \in \mathcal{SK}(m_1', m_2, \hat{Q}, P)$, such that

$$\mathbf{y}_1 \in \mathcal{T}^N_{Q',P,V_1}(Y_1|\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1, m_2, \mathbf{s}, \mathbf{k}), \mathbf{s}, \mathbf{k}) \bigcap \mathcal{T}_{\hat{Q},P,\hat{V}_1}(Y|\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1', m_2', \mathbf{s}', \mathbf{k}), \mathbf{s}', \mathbf{k})$$

and

$$\min_{A_1 \in \mathcal{A}_1(Q,P,\Delta_1)} D(\hat{Q} \circ P \circ \hat{V}_1 \| Q \circ P \circ A_1) \leq \min_{A_1 \in \mathcal{A}_1(Q,P,\Delta_1)} D(Q' \circ P \circ V_1 \| Q \circ P \circ A_1). \quad (14)$$

Denote

$$\mathcal{D}_1 = \left\{V_1, \hat{V}_1 : (14) \text{ is valid}\right\}$$

The error probability of message $m_1 \in \mathcal{M}_1$, maximal over all attack channels $A_1 \in \mathcal{A}_1(Q, P, \Delta_1)$ can be written in the following form:

$$e_1(f, g_1, N, m_1, m_2, Q, P, \Delta_1) = \max_{A_1 \in \mathcal{A}_1(Q,P,\Delta_1)} \sum_{(\mathbf{s},\mathbf{k}) \in \mathcal{S}^N \times \mathcal{K}^N} Q^N(\mathbf{s}, \mathbf{k}) e_1(f, g_1, N, m_1, m_2, \mathbf{s}, \mathbf{k}, A_1) =$$

$$= \max_{A_1 \in \mathcal{A}_1(Q,P,\Delta_1)} \left[\sum_{(\mathbf{s},\mathbf{k}) \in \mathcal{T}^E_Q(S,K)} Q^N(\mathbf{s}, \mathbf{k}) e_1(f, g_1, N, m_1, m_2, \mathbf{s}, \mathbf{k}, A_1) + \right.$$

$$\left. + \sum_{(\mathbf{s},\mathbf{k}) \notin \mathcal{T}^E_Q(S,K)} Q^N(\mathbf{s}, \mathbf{k}) e_1(f, g_1, N, m_1, m_2, \mathbf{s}, \mathbf{k}, A_1) \right].$$

Using the inequality (13) the error probabiltity can be upper bounded in the following way:

$$e_1(f, g_1, N, m_1, m_2, Q, P, \Delta_1) \leq \max_{A_1 \in \mathcal{A}_1(Q,P,\Delta_1)} \sum_{(\mathbf{s},\mathbf{k}) \in \mathcal{T}^E_Q(S,K)} Q^N(\mathbf{s}, \mathbf{k}) e_1(f, g_1, N, m_1, m_2, \mathbf{s}, \mathbf{k}, A_1) +$$

$$+ \exp\{-N(E-\varepsilon)\} \leq \sum_{(\mathbf{s},\mathbf{k}) \in \mathcal{T}^E_Q(S,K) \setminus \mathcal{SK}^E_Q(m_1,m_2,P)} Q^N(\mathbf{s}, \mathbf{k}) \Pr\{\overline{\beta}_{Q',P}(m_1, m_2, \mathbf{s}, \mathbf{k})\} +$$

$$+ \max_{A_1 \in \mathcal{A}_1(Q,P,\Delta_1)} \sum_{(\mathbf{s},\mathbf{k}) \in \mathcal{SK}^E_Q(m_1,m_2,P)} Q^N(\mathbf{s}, \mathbf{k}) \times$$

$$A_1^N \left\{ \bigcup_{\mathcal{D}_1} B_1(Q, Q', \hat{Q}, P, V_1, \hat{V}_1, m_1, m_2, \mathbf{s}, \mathbf{k}) | \mathbf{x}(m_1, m_2, \mathbf{s}, \mathbf{k}) \right\} + \exp\{-N(E-\varepsilon)\} \leq$$

$$\leq \sum_{(\mathbf{s},\mathbf{k}) \in \mathcal{T}^E_Q(S,K) \setminus \mathcal{SK}^E_Q(m_1,m_2,P)} Q^N(\mathbf{s}, \mathbf{k}) \exp\{-\exp\{N\delta/2\}\} +$$

$$+ \sum_{\mathcal{D}_1} \left| B_1(Q, Q', \hat{Q}, P, V_1, \hat{V}_1, m_1, m_2, \mathbf{s}, \mathbf{k}) \right| \times$$

$$\times \max_{A_1 \in \mathcal{A}_1(Q,P,\Delta_1)} \sum_{(\mathbf{s},\mathbf{k}) \in \mathcal{SK}^E_Q(m_1,m_2,P)} Q^N(\mathbf{s}, \mathbf{k}) A_1^N(\mathbf{y}_1|\mathbf{x}) + \exp\{-N(E-\varepsilon)\}.$$

Taking into account (12) and the following combinatorial expressions [18, 19]

$$|\mathcal{T}^N_{Q',P,V}(Y|\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1, m_2, \mathbf{s}, \mathbf{k}), \mathbf{s}, \mathbf{k})| \leq \exp\{N H_{Q',P,V}(Y|U_1, U_2, X, S, K)\} \leq$$

$$\leq \exp\{N H_{Q',P,V}(Y|X)\},$$

for $(\mathbf{s},\mathbf{k}) \in \mathcal{T}^N_{Q'}(S,K)$, $\mathbf{x} \in \mathcal{T}^N_{Q',P}(X)$, $\mathbf{y} \in \mathcal{T}^N_{Q',P,V}(Y|\mathbf{x})$

$$Q^N(\mathbf{s},\mathbf{k}) = \exp\{-N(H_{Q'}(S,K) + D(Q'\|Q))\}, \tag{15}$$

$$A^N(\mathbf{y}|\mathbf{x}) = \exp\{-N(H_{Q',P,V}(Y|X) + D(V\|A|Q',P))\}, \tag{16}$$

$$D(Q'\|Q) + D(V\|A|Q',P) = D(Q'\circ P\circ V\|Q\circ P\circ A), \tag{17}$$

the error probability can be bounded in the following way:

$$e_1(f,g_1,N,m_1,m_2,Q,P,\Delta_1) \le (N+1)^{|\mathcal{S}||\mathcal{K}|}\exp\{-\exp\{N\delta/2\}\} + \exp\{-N(E-\varepsilon)\}+$$

$$+\sum_{\mathcal{D}_1}\exp\{NH_{Q',P,V_1}(Y_1|X)\}\exp\{-N(E - \min_{A_1\in\mathcal{A}_1(Q,P,\Delta_1)} D(\hat{Q}\circ P\circ\hat{V}_1\|Q\circ P\circ A_1))\}\times$$

$$\times \max_{A_1\in\mathcal{A}_1(Q,P,\Delta_1)}[\exp\{-N(H_{Q',P,V_1}(Y_1|X) + D(Q'\|Q) + D(V_1\|A_1|Q',P))\}] =$$

$$= \exp\{-\exp\{N\delta/2\} + N\delta_1\} + \exp\{-N(E-\varepsilon)\}+$$

$$+\sum_{\mathcal{D}_1}\exp\{N(H_{Q',P,V_1}(Y_1|X) - E - H_{Q',P,V_1}(Y_1|X)-$$

$$-\min_{A_1\in\mathcal{A}_1(Q,P,\Delta_1)} D(Q'\circ P\circ V_1\|Q\circ P\circ A_1) - \min_{A_1\in\mathcal{A}_1(Q,P,\Delta_1)} D(\hat{Q}\circ P\circ\hat{V}_1\|Q\circ P\circ A_1)\Big)\Big\},$$

and taking into account (14) we can write

$$e_1(f,g_1,N,m_1,m_2,Q,P,\Delta_1) \le \exp\{-\exp\{N\delta/2\} + N\delta_1\} + \exp\{-N(E-\varepsilon)\}+$$

$$+(N+1)^{|\mathcal{S}||\mathcal{K}|+|\mathcal{A}_1||\mathcal{A}_2||\mathcal{X}|+2|\mathcal{A}_1||\mathcal{A}_2||\mathcal{X}||\mathcal{Y}_1|}\exp\{-NE\} \le \exp\{-N(E-\varepsilon)\}.$$

Therefore, for N large enough $e_i(f,g_1,N,Q,P,\Delta_1) \le \exp\{-N(E-\varepsilon)\}$, $i=1,2$, for all $A_i \in \mathcal{A}_i(Q,P,\Delta_i)$, $i=1,2$.

Theorem 1 is proved.

5 Proof of the Lemma 1

We shall construct a random matrix $\mathbf{Z} = \{\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1,m_2,\mathbf{s},\mathbf{k})\}^{(\mathbf{s},\mathbf{k})\in\mathcal{T}^N_Q(S,K)}_{m_1\in\mathcal{M}_1,\ m_2\in\mathcal{M}_2}$ in the following way.

For each $\mathbf{k}\in\mathcal{T}^N_Q(K)$ we choose at random, according to uniform distribution M_1 collections $\mathcal{L}(m_1)$ from $\mathcal{T}^N_{Q,P}(U_1|\mathbf{k})$, each of

$$L = \exp\{N(I_{Q,P}(U_1\wedge S|K) + \delta/2)\} \tag{18}$$

vectors $\mathbf{u}_{1l}(m_1)$, $l=\overline{1,L}$, $m_1=\overline{1,M_1}$. For each $m_1\in\mathcal{M}_1$ and $\mathbf{s}\in\mathcal{T}^N_Q(S|\mathbf{k})$ we choose such $\mathbf{u}_{1l}(m_1)$ from $\mathcal{L}(m_1)$, that $\mathbf{u}_{1l}(m_1)\in\mathcal{T}^N_{Q,P}(U_1|\mathbf{s},\mathbf{k})$. We denote this vector by $\mathbf{u}_1(m_1,\mathbf{s},\mathbf{k})$. If there is no such vector, let $\mathbf{u}_1(m_1,\mathbf{s},\mathbf{k}) = \mathbf{u}_{1L}(m_1)$.

Then for each $\mathbf{k}\in\mathcal{T}^N_Q(K)$ we choose at random, according to uniform distribution M_2 collections $\mathcal{J}(m_2)$ from $\mathcal{T}^N_{Q,P}(U_2|\mathbf{k})$, each of

$$J = \exp\{N(I_{Q,P}(U_2\wedge U_1,S|K) + \delta/2)\} \tag{19}$$

vectors $\mathbf{u}_{2j}(m_2)$, $j=\overline{1,J}$, $m_2=\overline{1,M_2}$. For each $m_2\in\mathcal{M}_2$, $\mathbf{s}\in\mathcal{T}^N_Q(S|\mathbf{k})$ and $\mathbf{u}_1(m_1,\mathbf{s},\mathbf{k})\in\mathcal{T}^N_{Q,P}(U_1|\mathbf{s},\mathbf{k})$ we choose such $\mathbf{u}_{2j}(m_2)$ form $\mathcal{J}(m_2)$, that $\mathbf{u}_{2j}(m_2)\in\mathcal{T}^N_{Q,P}(U_2|\mathbf{u}_1(m_1,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k})$.

We denote this vector by $\mathbf{u}_2(m_1, m_2, \mathbf{s}, \mathbf{k})$. If there is no such vector, let $\mathbf{u}_2(m_1, m_2, \mathbf{s}, \mathbf{k}) = \mathbf{u}_{2J}(m_2)$. Denote by $\mathbf{u}_1\mathbf{u}_2(m_1, m_2, \mathbf{s}, \mathbf{k})$ vector pairs $\mathbf{u}_1(m_1, \mathbf{s}, \mathbf{k})\mathbf{u}_2(m_1, m_2, \mathbf{s}, \mathbf{k})$ from $\mathcal{T}^N_{Q,P}(U_1, U_2|\mathbf{s}, \mathbf{k})$.

For each $m_1 \in \mathcal{M}_1$, $m_2 \in \mathcal{M}_2$ and $(\mathbf{s}, \mathbf{k}) \in \mathcal{T}^N_Q(S, K)$ we choose at random a vector $\mathbf{x}(m_1, m_2, \mathbf{s}, \mathbf{k})$ from $\mathcal{T}^N_{Q,P}(X|\mathbf{u}_1\mathbf{u}_2(m_1, m_2, \mathbf{s}, \mathbf{k}), \mathbf{s}, \mathbf{k})$ if $\mathbf{u}_1\mathbf{u}_2(m_1, m_2, \mathbf{s}, \mathbf{k}) \in \mathcal{T}^N_{Q,P}(U_1, U_2|\mathbf{s}, \mathbf{k})$, or from $\mathcal{T}^N_{Q,P}(X|\mathbf{s}, \mathbf{k})$, when $\mathbf{u}_1\mathbf{u}_2(m_1, m_2, \mathbf{s}, \mathbf{k}) \notin \mathcal{T}^N_{Q,P}(U_1, U_2|\mathbf{s}, \mathbf{k})$. Denote by $\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1, m_2, \mathbf{s}, \mathbf{k}) \in \mathcal{T}^N_{Q,P}(U_1, U_2, X|\mathbf{s}, \mathbf{k})$ the triple of vectors $\mathbf{u}_1(m_1, \mathbf{s}, \mathbf{k})\mathbf{u}_2(m_1, m_2, \mathbf{s}, \mathbf{k})\mathbf{x}(m_1, m_2, \mathbf{s}, \mathbf{k})$.

$$\Pr\{\overline{\beta}_{Q,P}(m_1, m_2, \mathbf{s}, \mathbf{k})\} = \Pr\{\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1, m_2, \mathbf{s}, \mathbf{k}) \notin \mathcal{T}^N_{Q,P}(U_1, U_2, X|\mathbf{s}, \mathbf{k})\} \le$$

$$\le \Pr\left\{\bigcup_{l=1}^{L} \mathbf{u}_{1l}(m_1) \notin \mathcal{T}^N_{Q,P}(U_1|\mathbf{s}, \mathbf{k}) \quad \bigcup \quad \bigcup_{j=1}^{J} \mathbf{u}_{2j}(m_2) \notin \mathcal{T}^N_{Q,P}(U_2|\mathbf{u}_1(m_1, \mathbf{s}, \mathbf{k}), \mathbf{s}, \mathbf{k})\right\} \le$$

$$\le \prod_{\substack{l=\overline{1,L} \\ j=\overline{1,J}}} [1 - \Pr\{\mathbf{u}_{1l}(m_1) \in \mathcal{T}^N_{Q,P}(U_1|\mathbf{s}, \mathbf{k})\} \times \Pr\{\mathbf{u}_{2j}(m_2) \in \mathcal{T}^N_{Q,P}(U_2|\mathbf{u}_1(m_1, \mathbf{s}, \mathbf{k}), \mathbf{s}, \mathbf{k})\}] \le$$

$$\le \left[1 - \frac{|\mathcal{T}^N_{Q,P}(U_1|\mathbf{s}, \mathbf{k})|}{|\mathcal{T}^N_{Q,P}(U_1|\mathbf{k})|} \times \frac{|\mathcal{T}^N_{Q,P}(U_2|\mathbf{u}_1(m_1, \mathbf{s}, \mathbf{k}), \mathbf{s}, \mathbf{k})|}{|\mathcal{T}^N_{Q,P}(U_2|\mathbf{k})|}\right]^{LJ} \le$$

$$\le [1 - \exp\{N(I_{Q,P}(U_1 \wedge S|K) + I_{Q,P}(U_2 \wedge U_1, S|K) + \delta/2)\}]^{LJ}.$$

Using the inequality $(1-t)^n \le \exp\{-nt\}$, which is true for any n and $t \in (0,1)$ and (18), (19) we can see that

$$\Pr\{\overline{\beta}_{Q,P}(m_1, m_2, \mathbf{s}, \mathbf{k})\} \le \exp\{-\exp\{N\delta/2\}\}.$$

If the matrix $\mathbf{Z} = \{\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1, m_2, \mathbf{s}, \mathbf{k})\}^{(\mathbf{s},\mathbf{k}) \in \mathcal{T}^N_Q(S,K)}_{m_1 \in \mathcal{M}_1,\ m_2 \in \mathcal{M}_2}$ satisfyies (8) for any $V_i, \hat{V}_i$, $i = 1, 2$, then $\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1, m_2, \mathbf{s}, \mathbf{k}) \ne \mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1', m_2', \mathbf{s}, \mathbf{k})$, for $(m_1', m_2') \ne (m_1, m_2)$. To prove that, it is enough to chose $V_i = \hat{V}_i$ and $\min\limits_{A_i \in \mathcal{A}_i(Q,P,\Delta_i)} D(\hat{V}_i \| A_i|Q, P) < E$, $i = 1, 2$.

If $\hat{V}_i$, $i = 1, 2$ are such that $\min\limits_{A_i \in \mathcal{A}_i(Q,P,\Delta_i)} D(\hat{V}_i \| A_i|Q, P) \ge E$, $i = 1, 2$, then

$$\exp\left\{-N\left|E - \min_{A_i \in \mathcal{A}_i(Q,P,\Delta_i)} D(\hat{V}_i \| A_i|Q, P)\right|^+\right\} = 1, \ i = 1, 2$$

and (8) is valid for any M_1, M_2.

So to prove lemma 1 it remains to prove the inequality (8) for

$$\hat{\mathcal{V}}_i(Q, P, E) = \{\hat{V}_i : \min_{A_i \in \mathcal{A}_i(Q,P,\Delta_i)} D(\hat{V}_i \| A_i|Q, P) < E\}, i = 1, 2.$$

Denote by

$$\mathcal{B}_i(Q, P, V_i, \hat{V}_i, m_1, m_2, \mathbf{s}, \mathbf{k}) = \mathcal{T}^N_{Q,P,V_i}(Y_i|\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1, m_2, \mathbf{s}, \mathbf{k}), \mathbf{s}, \mathbf{k}) \bigcap$$

$$\bigcap \bigcup_{m_1' \ne m_i} \bigcup_{\mathbf{s}':(\mathbf{s}',\mathbf{k}) \in S\mathcal{K}(m_1', m_2', Q, P)} \bigcup_{m_{3-i}' \in \mathcal{M}_{3-i}(m_i' \mathbf{s}', \mathbf{k}, Q, P)} \mathcal{T}^N_{Q,P,\hat{V}_i}(Y_i|\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1', m_2', \mathbf{s}', \mathbf{k}), \mathbf{s}', \mathbf{k}), i = 1, 2.$$

It is sufficient to show that for N large enough

$$(N+1)^{|\mathcal{U}_1||\mathcal{U}_2||\mathcal{S}||\mathcal{K}||\mathcal{X}||\mathcal{Y}_1||\mathcal{Y}_2|} \times$$

$$\times \sum_{i=1,2} \sum_{V_i} \sum_{\hat{V}_i \in \hat{\mathcal{V}}_i(Q,P,E)} \exp\left\{N\left(E - \min_{A_i \in \mathcal{A}_i(Q,P,\Delta_i)} D(\hat{V}_i \| A_i | Q,P) - H_{Q,P,V_i}(Y_i|X,S,K)\right)\right\} \times$$

$$\times \max_{(\mathbf{s},\mathbf{k}) \in \mathcal{SK}(m_1,m_2,Q,P)} \mathbf{E}\left|\mathcal{B}_i(Q,P,V_i\hat{V}_i,m_i,\mathbf{s},\mathbf{k})\right| \le 1. \tag{20}$$

Notice that

$$\mathbf{E}|\mathcal{B}_i(Q,P,V_i,\hat{V}_i,m_i,\mathbf{s},\mathbf{k})| \le \sum_{\mathbf{y}_i \in \mathcal{Y}_i^N} \Pr\{\mathbf{y}_i \in \mathcal{T}^N_{Q,P,V_i}(Y_i|\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1,m_2,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k})\} \times$$

$$\times \Pr\left\{\mathbf{y}_i \in \bigcup_{m_i' \ne m_i} \bigcup_{\mathbf{s}':(\mathbf{s}',\mathbf{k}) \in \mathcal{SK}(m_1',m_2',Q,P)} \bigcup_{m_{3-i}' \in \mathcal{M}_{3-i}(m_i,\mathbf{s}',\mathbf{k},Q,P)} \mathcal{T}^N_{Q,P,\hat{V}_i}(Y_i|\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1',m_2',\mathbf{s}',\mathbf{k}),\mathbf{s}',\mathbf{k})\right\},$$

$$i = 1,2,$$

as the selected events are independent.

The first probability, for $i = 1,2$ is different from zero if and only if $\mathbf{y}_i \in \mathcal{T}^N_{Q,P,V_i}(Y_i|\mathbf{s},\mathbf{k})$, $i = 1,2$. In this case for sufficiently large N we have

$$\Pr\{\mathbf{y}_i \in \mathcal{T}^N_{Q,P,V_i}(Y_i|\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1,m_2,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k})\} = \frac{|\mathcal{T}^N_{Q,P,V_i}(U_1,U_2,X|\mathbf{y}_i,\mathbf{s},\mathbf{k})|}{|\mathcal{T}^N_{Q,P}(U_1,U_2,X|\mathbf{s},\mathbf{k})|} \le$$

$$\le (N+1)^{|\mathcal{U}_1||\mathcal{U}_2||\mathcal{X}||\mathcal{S}||\mathcal{K}|} \exp\{-NI_{Q,P,V}(Y \wedge U_1,U_2,X|S,K)\} \le$$

$$\le (N+1)^{|\mathcal{U}_1||\mathcal{U}_2||\mathcal{X}||\mathcal{S}||\mathcal{K}|} \exp\{-NI_{Q,P,V_i}(Y_i \wedge X|S,K)\},\ i = 1,2.$$

The second probability for $i = 1$ can be upper bounded in the following way

$$\Pr\left\{\mathbf{y}_1 \in \bigcup_{m_1' \ne m_1} \bigcup_{\mathbf{s}':(\mathbf{s}',\mathbf{k}) \in \mathcal{SK}(m_1',m_2',Q,P)} \bigcup_{m_2' \in \mathcal{M}_2(m_1',\mathbf{s}',\mathbf{k},Q,P)} \mathcal{T}^N_{Q,P,\hat{V}_1}(Y_1|\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1',m_2',\mathbf{s}',\mathbf{k}),\mathbf{s}',\mathbf{k})\right\} \le$$

$$\le \Pr\left\{\mathbf{y}_1 \in \bigcup_{\mathbf{u}_{1l}(m_1') \in \mathcal{L}(m_1')} \bigcup_{\mathbf{s}':(\mathbf{s}',\mathbf{k}) \in \mathcal{T}^N_{Q,P}(S,K|\mathbf{u}_{1l}(m_1'))} \mathcal{T}^N_{Q,P,\hat{V}_1}(Y_1|\mathbf{u}_{1l}(m_1'),\mathbf{s}',\mathbf{k})\right\} \le$$

$$\le \sum_{\mathbf{u}_{1l}(m_1') \in \mathcal{L}(m_1')} \Pr\{\mathbf{y}_1 \in \mathcal{T}^N_{Q,P,\hat{V}_1}(Y_1|\mathbf{u}_{1l}(m_1'),\mathbf{k})\} \le L\frac{|\mathcal{T}^N_{Q,P,\hat{V}_1}(U_1|\mathbf{y}_1,\mathbf{k})|}{|\mathcal{T}^N_{Q,P}(U_1|\mathbf{k})|} \le$$

$$\le (N+1)^{|\mathcal{U}_1||\mathcal{K}|} \exp\{-N(I_{Q,P,\hat{V}_1}(Y_1 \wedge U_1|K) - I_{Q,P}(S \wedge U_1|K) - \delta/2)\}.$$

And the second probability for $i = 2$ we upper bound in the following way

$$\Pr\left\{\mathbf{y}_2 \in \bigcup_{m_2' \ne m_2} \bigcup_{\mathbf{s}':(\mathbf{s}',\mathbf{k}) \in \mathcal{SK}(m_1',m_2',Q,P)} \bigcup_{m_1' \in \mathcal{M}_1(m_2',\mathbf{s}',\mathbf{k},Q,P)} \mathcal{T}^N_{Q,P,\hat{V}_2}(Y_2|\mathbf{u}_1\mathbf{u}_2\mathbf{x}(m_1',m_2',\mathbf{s}',\mathbf{k}),\mathbf{s}',\mathbf{k})\right\} \le$$

$$\le \Pr\left\{\mathbf{y}_2 \in \bigcup_{\mathbf{u}_{2j}(m_2') \in \mathcal{J}(m_2')} \bigcup_{\mathbf{s}':(\mathbf{s}',\mathbf{k}) \in \mathcal{T}^N_{Q,P}(S,K|\mathbf{u}_{2j}(m_2'))} \mathcal{T}^N_{Q,P,\hat{V}_2}(Y_2|\mathbf{u}_{2j}(m_2'),\mathbf{s}',\mathbf{k})\right\} \le$$

$$\leq \sum_{u_{2j}(m_2')\in\mathcal{J}(m_2')} \Pr\{\mathbf{y}_2 \in \mathcal{T}^N_{Q,P,\hat{V}_2}(Y_2|\mathbf{u}_{2j}(m_2'),\mathbf{k})\} \leq J\frac{|\mathcal{T}^N_{Q,P,\hat{V}_2}(U_2|\mathbf{y}_2,\mathbf{k})|}{|\mathcal{T}^N_{Q,P}(U_2|\mathbf{k})|} \leq$$

$$\leq (N+1)^{|\mathcal{U}_2||\mathcal{K}|}\exp\{-N(I_{Q,P,\hat{V}_2}(Y_2\wedge U_2|K) - I_{Q,P}(U_2\wedge U_1,S|K) - \delta/2)\}.$$

Finally we obtain

$$\mathrm{E}|\mathcal{B}_1(Q,P,V_1,\hat{V}_1,m_1,\mathbf{s},\mathbf{k})| \leq (N+1)^{|\mathcal{U}_2||\mathcal{K}|(1+|\mathcal{U}_1||\mathcal{X}||\mathcal{S}|)}(M_1-1)|\mathcal{T}_{Q,P,V_1}(Y_1|\mathbf{s},\mathbf{k})|\times$$
$$\times\exp\{-N(I_{Q,P,V_1}(Y_1\wedge X|S,K) + I_{Q,P,\hat{V}_2}(Y_2\wedge U_2|K) - I_{Q,P}(U_2\wedge U_1,S|K) - \delta/2)\}.$$

where, from (5)

$$M_1 - 1 \leq \exp\Big\{N\Big(I_{Q,P,V_1}(Y_1\wedge U_1|K) -$$
$$-I_{Q,P}(S\wedge U_1|K) + \min_{A_1\in\mathcal{A}_1(Q,P,\Delta_1)} D(\hat{V}_1\|A_1|Q,P) - E + \delta\Big)\Big\}.$$

We obtain

$$\mathrm{E}|\mathcal{B}_1(Q,P,V_1,\hat{V}_1,m_1,\mathbf{s},\mathbf{k})| \leq (N+1)^{|\mathcal{U}_2||\mathcal{K}|(1+|\mathcal{U}_1||\mathcal{X}||\mathcal{S}|)}\exp\{N(H_{Q,P,V_1}(Y_1|S,K))\}\times$$
$$\times\exp\{-N(I_{Q,P,V}(Y_1\wedge X|S,K) + I_{Q,P,\hat{V}_1}(Y_1\wedge U_1|K) - I_{Q,P}(S\wedge U_1|K) - \delta/2)\}\times$$
$$\times\exp\Big\{N\Big(I_{Q,P,V_1}(Y_1\wedge U_1|K) - I_{Q,P}(S\wedge U_1|K) + \min_{A_1\in\mathcal{A}_1(Q,P,\Delta_1)} D(\hat{V}_1\|A_1|Q,P) - E + \delta\Big)\Big\},$$

$$\mathrm{E}|\mathcal{B}_1(Q,P,V_1,\hat{V}_1,m_1,\mathbf{s},\mathbf{k})| \leq (N+1)^{|\mathcal{U}_2||\mathcal{K}|(1+|\mathcal{U}_1||\mathcal{X}||\mathcal{S}|)}\times$$
$$\times\exp\Big\{-N\Big(E - \min_{A_1\in\mathcal{A}_1(Q,P,\Delta_1)} D(\hat{V}_1\|A_1|Q,P - H_{Q,P,V_1}(Y_1|X,S,K) - \delta/2)\Big)\Big\} \qquad (21)$$

Similarly

$$\mathrm{E}|\mathcal{B}_2(Q,P,V_2,\hat{V}_2,m_2,\mathbf{s},\mathbf{k})| \leq (N+1)^{|\mathcal{U}_2||\mathcal{K}|(1+|\mathcal{U}_1||\mathcal{X}||\mathcal{S}|)}(M_2-1)|\mathcal{T}_{Q,P,V_2}(Y_2|\mathbf{s},\mathbf{k})|\times$$
$$\times\exp\{-N(I_{Q,P,V_2}(Y_2\wedge X|S,K) + I_{Q,P,\hat{V}_2}(Y_2\wedge U_2|K) - I_{Q,P}(U_2\wedge U_2,S|K) - \delta/2)\}.$$

where, from (6)

$$M_2 - 1 \leq \exp\Big\{N\Big(I_{Q,P,V_2}(Y_2\wedge U_2|K) -$$
$$-I_{Q,P}(U_2\wedge U_1,S|K) + \min_{A_2\in\mathcal{A}_2(Q,P,\Delta_2)} D(\hat{V}_2\|A_2|Q,P) - E + \delta\Big)\Big\}.$$

We obtain

$$\mathrm{E}|\mathcal{B}_2(Q,P,V_2,\hat{V}_2,m_2,\mathbf{s},\mathbf{k})| \leq (N+1)^{|\mathcal{U}_2||\mathcal{K}|(1+|\mathcal{U}_1||\mathcal{X}||\mathcal{S}|)}\exp\{N(H_{Q,P,V_2}(Y_2|S,K))\}\times$$
$$\times\exp\{-N(I_{Q,P,V}(Y_2\wedge X|S,K) + I_{Q,P,\hat{V}_2}(Y_2\wedge U_2|K) - I_{Q,P}(U_2\wedge U_1,S|K) - \delta/2)\}\times$$
$$\times\exp\Big\{N\Big(I_{Q,P,V_2}(Y_2\wedge U_2|K) - I_{Q,P}(U_2\wedge U_1,S|K) + \min_{A_2\in\mathcal{A}_2(Q,P,\Delta_2)} D(\hat{V}_2\|A_2|Q,P) - E + \delta\Big)\Big\},$$

$$\mathrm{E}|\mathcal{B}_2(Q,P,V_2,\hat{V}_2,m_2,\mathbf{s},\mathbf{k})| \leq (N+1)^{|\mathcal{U}_2||\mathcal{K}|(1+|\mathcal{U}_1||\mathcal{X}||\mathcal{S}|)}\times$$
$$\times\exp\Big\{-N\Big(E - \min_{A_2\in\mathcal{A}_2(Q,P,\Delta_2)} D(\hat{V}_2\|A_2|Q,P) - H_{Q,P,V_2}(Y_2|X,S,K) - \delta/2)\Big)\Big\} \qquad (22)$$

Taking into account (21, 22), and that the number of all $V_i, \hat{V}_i$ $i = 1,2$ does not exceed $(N+1)^{|\mathcal{X}|(|\mathcal{Y}_1|+|\mathcal{Y}_2|)}$ we obtain that (20) is true for N large enough.

Lemma 1 is proved.

References

[1] P. Moulin and J. A. O'Sullivan, "Information-theoretic analysis of information hiding", *IEEE Trans. Inform. Theory*, vol. 49, no. 3, pp. 563-593, Mar. 2003.

[2] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding–A Survey," *Proc. IEEE (Special Issue on Identification and Protection of Multimedia Information)*, vol. 87, pp. 1062-1078, July 1999.

[3] P. Moulin, "The role of information theory in watermarking and its application to image watermarking," *Signal Processing*, vol. 81, pp. 1121-1139, 2001.

[4] E. A. Haroutunian, "Upper estimate of transmission rate for memoryless channel with countable number of output signals under given error probability exponent", (in Russian), *3rd All-Union Conf. on Theory of Information Transmission and Coding, Uzhgorod, Publication house of Uzbek Academy of Sciences, Tashkent*, pp. 83–86, 1967.

[5] M. E. Haroutunian and S. A. Tonoyan, "Random coding bound of information hiding E-capacity", *Proc. of IEEE Intern. Symp. Infrom. Theory*, p. 536, USA, Chicago, 2004.

[6] N. P. Sheppard, R. Safavi-Naini and P. Ogunbona, "On multiple watermarking", *ACM Multimedia Conference, ACM Multimedia*, pp 3-6, 2001.

[7] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon. "A secure, robust watermark for multimedia", *Information Hiding: First International Workshop*, pp. 185-206, Springer, Berlin, Germany, 1996.

[8] F. Mintzer and G. W. Braudaway, "If one watermark is good, are more better?", *IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 2067-2069, 1999.

[9] M. E. Haroutunian and S. A. Tonoyan, "Bounds of information hiding E-capacity", Submitted to *IEEE Trans. Inform. Theory*, (15 pages), 2004.

[10] N. Merhav, "On random coding error exponents of watermarking systems", *IEEE Trans. Inform. Theory*, vol. 46, no. 2, pp. 420-430, Mar. 2000.

[11] N. Merhav and A. Somekh-Baruch, "On the error exponent and capacity games of private watermarking systems", *IEEE Trans. Inform. Theory*, vol. 49, no. 3, pp. 537-562, Mar. 2003.

[12] T. M. Cover, " Broadcast channels", *IEEE Trans. Inform. Theory*, vol. IT-18, no. 1, pp. 2–14, 1972.

[13] T. M. Cover, "An achievable rate region for the broadcast channel," *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 399–404, 1975.

[14] M. E. Haroutunian, "Random coding bound for E-capacity region of the broadcast channel", Transactions of the Institute for Informatics and Automation Problems of the NAS of RA and of YSU, *Mathematical Problems of Computer Science*,vol. 21, pp. 50–60, 2000.

[15] S. I. Gel'fand and M. S. Pinsker, "Coding for channel with random parameters," *Problems of Control and Information Theory*, vol. 9, no. 1, pp. 19-31, 1980.

[16] M. E. Haroutunian, "New bounds for E-capacities of arbitrarily varying channel and channel with random parameter" *Trans. IIAP NAS RA and YSU, Mathematical Problems of Computer sciences*, vol. 22, p. 44-59, 2001.

[17] M. E. Haroutunian, "Bounds of E-capacity for multiple-access channel with random parameter", special book issued in the framework of research project "General Theory of Information Transfer and Combinatorics" at ZiF, Bilefeld University, Germany, 2004.

[18] I. Csiszár and J. Körner, *Information Theory: Coding theorems for discrete memoryless systems*, Academic Press, New York, 1981.

[19] I. Csiszár, "The method of types", *IEEE Trans. Inform. Theory*, vol. 44, no. 6, pp. 2505–2523, 1998.

[20] A. Somekh-Baruch and N. Merhav, On the random coding error exponents of the Single-User and the Multiple-Access Gelfand-Pinsker Channels, *Proc. of IEEE Intern. Symp. Infrom. Theory*, p. 448, USA, Chicago, 2004.

Բազմակի հաղորդագրություններով տվյալներ թաքցնող համակարգի մասին

Մ. Ե. Հարությունյան, Ս. Ա. Տոնոյան

Ամփոփում

Բազմակի ջրանշման, ինչպես նաև մուլտիմեդիայի ստեղծման մի շարք ալգորիթմներ և սխեմաներ նախատեսում են թաքցնել մեկից ավելի հաղորդագրություններ: Աշխատանքում դիտարկված է բազմակի հաղորդագրություններով տվյալներ թաքցնող համակարգերի տեղեկատվատեսական-տեսական հետազոտություն: Երկու հաղորդագրությունների դեպքի համար ներմուծվել և հետազոտվել է համակարգի արագություն-հուսալիություն-շեղում (E-ունակություն) ֆունկցիան: Կառուցվել են ներքին գնահատականներ համակարգի E-ունակության և ունակության տիրույթների համար: