Mathematical Problems of Computer Science 23, 2004, 20–31.

On Estimates of Rate-reliability-distortion Function for Information Hiding System*

Mariam E. Haroutunian and Smbat A. Tonoyan

Institute for Informatics and Automation Problems of NAS of RA
e-mails: armar@ipia.sci.am, smbatt@ipia.sci.am

Abstract

The model of information hiding system, introduced and studied by P. Moulin and J. A. O'Sullivan [1] is explored. The rate-reliability-distortion function for this system is investigated. Upper and lower estimates of rate-reliability-distortion function, called the random coding and the sphere packing bounds are constructed. The limit of random coding bound, when $E \to 0$, coincides with the information hiding capacity stated by P. Moulin and J. A. O'Sullivan.

1 Introduction

Many application areas, such as the copyright protection for digital media, watermarking, fingerprinting, steganography and data embedding have a certain generality, which can be formulated as information hiding problem [2, 3]. We explore the generic information hiding system, introduced and studied by P. Moulin and J. A. O'Sullivan [1].

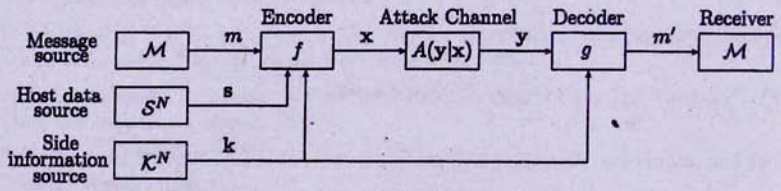

Fig. 1. The generic model of information hiding system

The message (watermark, fingerprint, etc.) needs to be embedded in the host data set (which can be the blocks from the audio, image and video data) and to be reliably transmitted to a receiver via unknown channel, called the *attack channel* as it can be subject to random attacks of *attacker*. Side information, which can be cryptographic keys, properties of the host data, features of audio, image or video data or locations of watermarks, is available both to encoder and decoder. The encoding and decoding functions are known to the attacker, the side information is not.

*The work was partially supported by INTAS Grant 00-738 and by 04.10.31 Target Program of RA.

The information hider introduces certain distortion in the host data set for the data embedding. The attacker trying to change or remove this hidden information, introduces some other distortion. The information hiding system must satisfy two main requirements, which are called *transparency* (the distortion introduced by information hider must not exceed the allowable level) and *robustness* (the distortion introduced by the attacker should be restricted by corresponding level).

Here we investigate the rate-reliability-distortion function, called information hiding E-capacity, which is the generalization of the notions of rate-distortion function, introduced by P. Moulin and J. A. O'Sullivan [1] and E-capacity introduced by E. A. Haroutunian [4]. The information hiding E-capacity expresses the dependence of the information hiding rate from reliability and distortion levels for information hider and attacker. The lower bound of information hiding E-capacity [5], called the random coding bound, and the upper bound, called the sphere packing bound are derived. The limit of random coding bound, when $E \to 0$, coincides with the information hiding capacity stated by P. Moulin and J. A. O'Sullivan [5].

2 Statement of the Problem

In description of the system and for definition of principal notions we follow formulations of [1]. Host data source (fig. 1) is described by the random variable S, which takes values in the discrete finite set $\mathcal{S}$, according to the probability distribution $Q_0 = \{Q(s),\ s \in \mathcal{S}\}$ and generates N-length data blocks $\mathbf{s} = (s_1, s_2, ..., s_N) \in \mathcal{S}^N$ of independent and identically distributed components. The message source creates equiprobable and independent messages m, from the message set $\mathcal{M}$, which must be transmitted to the receiver. The side information source is described by the random variable K, which takes values in the discrete finite set $\mathcal{K}$, and in the most general case has the given joint probability distribution $Q = \{Q(s,k),\ s \in \mathcal{S},\ k \in \mathcal{K}\}$ with the random variable S. In particular case, when the side information is a cryptographic key, S and K are distributed independently. The side information in the form of N-length sequences $\mathbf{k} = (k_1, k_2, ..., k_N) \in \mathcal{K}^N$ of independent and identically distributed components is available to the encoder and decoder.

The *information hider* (encoder) embeds the message $m \in \mathcal{M}$ in the host data blocks $\mathbf{s} \in \mathcal{S}^N$ using the side information $\mathbf{k} \in \mathcal{K}^N$. The resulting codeword $\mathbf{x} \in \mathcal{X}^N$ is transmitted via attack channel with the finite input and output alphabets $\mathcal{X}$ and $\mathcal{Y}$. The *attacker* trying to change or remove the message m, transforms the data blocks $\mathbf{x} \in \mathcal{X}^N$ into corrupted blocks $\mathbf{y} \in \mathcal{Y}^N$. The decoder, which knows the side information, decodes the data block $\mathbf{y} \in \mathcal{Y}^N$, deriving the message m. We assume, that the attacker knows the distributions of all random variables but not the side information.

Let the mappings $d_1 : \mathcal{S} \times \mathcal{X} \to [0, \infty)$, $d_2 : \mathcal{X} \times \mathcal{Y} \to [0, \infty)$ are distortion functions and positive numbers Δ_1, Δ_2 are allowed distortion levels for the information hider and the attacker, respectively. The distortion functions are supposed to be symmetric: $d_1(s,x) = d_1(x,s), d_2(x,y) = d_2(y,x)$ and $d_1(s,x) = 0$, if $s = x, d_2(x,y) = 0$, if $x = y$. Distortion functions for the N-length vectors are

$$d_1^N(\mathbf{s},\mathbf{x}) = \frac{1}{N}\sum_{n=1}^{N} d_1(s_n, x_n),\ d_2^N(\mathbf{x},\mathbf{y}) = \frac{1}{N}\sum_{n=1}^{N} d_2(x_n, y_n).$$

Consider an auxiliary random variable U, taking values in the discrete finite set $\mathcal{U}$ and forming the Markov chain $(U, S, K) \to X \to Y$ with random variables S, K, X, Y.

Definition 1. *The information hiding N-length code (f, g) is a pair of mappings $f: \mathcal{M} \times \mathcal{S}^N \times \mathcal{K}^N \to \mathcal{X}^N$ and $g: \mathcal{Y}^N \times \mathcal{K}^N \to \mathcal{M}$, where f is the encoding and g is the decoding.*

Definition 2. *A memoryless covert channel P, designed by information hider, subject to distortion level Δ_1, is a fancy name for probability distribution $P = \{P(u, x|s, k),\ u \in \mathcal{U},\ x \in \mathcal{X},\ s \in \mathcal{S},\ k \in \mathcal{K}\}$ such, that*

$$\sum_{u,x,s,k} d_1(s, x) P(u, x|s, k) Q(s, k) \le \Delta_1.$$

Denote by $\mathcal{P}(Q, \Delta_1)$ the set of all covert channels, subject to distortion level Δ_1. The N-length memoryless expression for the covert channel P is:

$$P^N(\mathrm{u}, \mathrm{x}|\mathrm{s}, \mathrm{k}) = \prod_{n=1}^{N} P(u_n, x_n|s_n, k_n).$$

Definition 3. *A memoryless attack channel A, designed by attacker, subject to distortion level Δ_2, under the condition of covert channel $P \in \mathcal{P}(Q, \Delta_1)$, is defined by a probability distribution $A = \{A(y|x),\ y \in \mathcal{Y},\ x \in \mathcal{X}\}$ such, that*

$$\sum_{u,x,y,s,k} d_2(x, y) A(y|x) P(u, x|s, k) Q(s, k) \le \Delta_2.$$

Denote by $\mathcal{A}(Q, P, \Delta_2)$ the set of all attack channels, under the condition of covert channel $P \in \mathcal{P}(Q, \Delta_1)$ and subject to distortion level Δ_2.

The N-length memoryless expression for the attack channel A is:

$$A^N(\mathrm{y}|\mathrm{x}) = \prod_{n=1}^{N} A(y_n|x_n).$$

The nonnegative number

$$R = \frac{1}{N} \log M$$

is called *the information hiding code rate*, where M is the cardinality of the set $\mathcal{M}$.

The probability of erroneous reconstruction of the message $m \in \mathcal{M}$ for $(\mathrm{s}, \mathrm{k}) \in \mathcal{S} \times \mathcal{K}$ via channel A is:

$$e(f, g, N, m, \mathrm{s}, \mathrm{k}, A) = A^N\{\mathcal{Y}^N - g^{-1}(m|\mathrm{k})|f(m, \mathrm{s}, \mathrm{k})\}. \tag{1}$$

The error probability of the message m averaged over all $(\mathrm{s}, \mathrm{k}) \in \mathcal{S} \times \mathcal{K}$ equals to

$$e(f, g, N, m, Q, A) = \sum_{(\mathrm{s},\mathrm{k}) \in \mathcal{S}^N \times \mathcal{K}^N} Q^N(\mathrm{s}, \mathrm{k}) e(f, g, N, m, \mathrm{s}, \mathrm{k}, A).$$

The error probability of the code, for any message $m \in \mathcal{M}$, maximal over all attack channels $\mathcal{A}(Q, P, \Delta_2)$ is denoted by:

$$e(f, g, N, m, Q, P, \Delta_2) = \max_{A \in \mathcal{A}(Q,P,\Delta_2)} e(f, g, N, m, Q, A).$$

The maximal error probability of the code, maximal over all attack channels from $\mathcal{A}(Q, P, \Delta_2)$ equals to:

$$e(f, g, N, Q, P, \Delta_2) = \max_{m \in \mathcal{M}} \max_{A \in \mathcal{A}(Q,P,\Delta_2)} e(f, g, N, m, Q, A),$$

and the average error probability of the code, maximal over all attack channels from $\mathcal{A}(P,\Delta_2)$ equals to:

$$\overline{e}(f,g,N,Q,P,\Delta_2)=\frac{1}{M}\sum_{m\in\mathcal{M}}\max_{A\in\mathcal{A}(Q,P,\Delta_2)}e(f,g,N,m,Q,A). \tag{2}$$

Consider the codes, the maximal error probability of which exponentially decreases with the given exponent $E>0$, (called *the reliability*)

$$e(f,g,N,Q,P,\Delta_2)\le\exp\{-NE\}. \tag{3}$$

Denote by $M(Q,E,N,\Delta_1,\Delta_2)$ the highest volume of the code, satisfying the condition (3) for the given reliability E and the distortion levels $\Delta_1,\ \Delta_2$.

The rate-reliability-distortion function, which we call information hiding E-capacity by analogy with the information hiding capacity [1] and with E-capacity of ordinary channel [4], is defined as:

$$R(Q,E,\Delta_1,\Delta_2)=C(Q,E,\Delta_1,\Delta_2)\triangleq\varlimsup_{N\to\infty}\frac{1}{N}\log M(Q,E,N,\Delta_1,\Delta_2).$$

By $C(Q,E,\Delta_1,\Delta_2)$ and $\overline{C}(Q,E,\Delta_1,\Delta_2)$ we denote the information hiding E-capacity for maximal and average error probabilities respectively.

In this paper the lower and upper bounds of information hiding E-capacity for maximal and average error probabilities are constructed. It must be noted, that the solution of the problem has certain analogy with the construction of the lower and upper bounds of E-capacity for channel with random parameter [6, 7, 8].

In [9] the lower bound of the error exponent for the situation, when the decoder is informed of the attack strategy and host data realization, was performed. The results of [9] were extended in [10].

3 Formulation of Results

For the formulation of our results we use notations from [11, 12, 7] of the well known in information theory notions of conditional mutual informations $I_{Q,P}(S\wedge U|K)$, $I_{Q,P,V}(X\wedge Y|S,K)$, informational divergences $D(Q\|Q')$, $D(V\|A|Q,P)$, and the notion of type, where $V=\{V(y|x),\ y\in\mathcal{Y},\ x\in\mathcal{X}\}$. We denote by $\mathcal{T}_Q^N(S,K)$ the set of N-length vectors $(\mathbf{s},\mathbf{k})$ of the type Q, and by $\mathcal{T}_{Q,P}^N(U|\mathbf{s},\mathbf{k})$ the set of N-length vectors $\mathbf{u}$ of conditional type P, for given $(\mathbf{s},\mathbf{k})\in\mathcal{T}_Q^N(S,K)$. All logarithms and exponents in the paper are of the base 2.

Consider the following function, which we call *random coding bound*

$$R_r(Q,E,\Delta_1,\Delta_2)=\max_{P\in\mathcal{P}(Q,\Delta_1)}\min_{A\in\mathcal{A}(Q,P,\Delta_2)}\min_{Q',V:D(Q'\circ P\circ V\|Q\circ P\circ A)\le E}|I_{Q',P,V}(Y\wedge U|K)-$$

$$-I_{Q',P}(S\wedge U|K)+D(Q'\circ P\circ V\|Q\circ P\circ A)-E|^+,$$

and the function, called *the sphere packing bound*

$$R_{sp}(Q,E,\Delta_1,\Delta_2)=\max_{P\in\mathcal{P}(Q,\Delta_1)}\min_{A\in\mathcal{A}(Q,P,\Delta_2)}\min_{Q',V:D(Q'\circ P\circ V\|Q\circ P\circ A)\le E}I_{Q',P,V}(X\wedge Y|S,K).$$

Note that in the last function

$$P=\{P(x|s,k)=\sum_{u\in\mathcal{U}}P(u,x|s,k):\ P(u,x|s,k)\in\mathcal{P}(\Delta_1),\ u\in\mathcal{U},\ x\in\mathcal{X},\ s\in\mathcal{S},\ k\in\mathcal{K}\}. \tag{4}$$

Theorem 1. *For all $E > 0$, for information hiding system with distortion levels Δ_1, Δ_2, the random coding bound $R_r(Q, E, \Delta_1, \Delta_2)$ is the lower bound and the sphere packing bound $R_{sp}(Q, E, \Delta_1, \Delta_2)$ is the upper bound of information hiding E-capacity for maximal and average error probabilities:*

$$R_r(Q, E, \Delta_1, \Delta_2) \le C(Q, E, \Delta_1, \Delta_2) \le \overline{C}(Q, E, \Delta_1, \Delta_2) \le R_{sp}(Q, E, \Delta_1, \Delta_2).$$

In [1] it was stated that the cardinality of the set $\mathcal{U}$ can be restricted to $|\mathcal{U}| = |\mathcal{X}||\mathcal{Q}|+1$, where $\mathcal{Q} = \{(s,k) \in \mathcal{S} \times \mathcal{K} : \ Q(s,k) \neq 0\}$.

Corollary 1. *When $E \to 0$ we obtain the lower and upper bounds of information hiding capacity:*

$$R_r(Q, \Delta_1, \Delta_2) = \max_{P \in \mathcal{P}(Q,\Delta_1)} \min_{A \in \mathcal{A}(Q,P,\Delta_2)} \{I_{Q,P,A}(Y \wedge U|K) - I_{Q,P}(S \wedge U|K)\}, \qquad (5)$$

$$R_{sp}(Q, \Delta_1, \Delta_2) = \max_{P \in \mathcal{P}(Q,\Delta_1)} \min_{A \in \mathcal{A}(Q,P,\Delta_2)} I_{Q,P,A}(X \wedge Y|S, K),$$

where the lower bound (5) coincides with the information hiding capacity, obtained by P. Moulin and J. A. O'Sullivan [1].

4 Proof of the Lower Bound

The lower bound in theorem 1 is proved by the Shannon's random coding arguments, using the method of types and demonstration of a generalization of packing lemma [11, 12, 7].

Denote by $\mathcal{L}(\mathcal{T}_Q^N(S,K))$ the family of all matrices

$$\mathbf{L} = \{\mathbf{ux}(m, \mathbf{s}, \mathbf{k})\}_{m=\overline{1,M}}^{(\mathbf{s},\mathbf{k}) \in \mathcal{T}_Q^N(S,K)},$$

where $\mathbf{ux}(m, \mathbf{s}, \mathbf{k}) = \mathbf{u}(m, \mathbf{s}, \mathbf{k})\mathbf{x}(m, \mathbf{s}, \mathbf{k})$, such that the rows

$$\mathbf{L}(\mathbf{s}, \mathbf{k}) = (\mathbf{ux}(1, \mathbf{s}, \mathbf{k}), \mathbf{ux}\{2, \mathbf{s}, \mathbf{k}), \ldots, \mathbf{ux}(M, \mathbf{s}, \mathbf{k}))$$

are collections of not necessarily distinct vector pairs, the majority of which are from $\mathcal{T}_{Q,P}^N(U, X|\mathbf{s}, \mathbf{k})$.

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

$$\beta_{Q,P}(m, \mathbf{s}, \mathbf{k}) \triangleq \{\mathbf{ux}(m, \mathbf{s}, \mathbf{k}) \in \mathcal{T}_{Q,P}^N(U, X|\mathbf{s}, \mathbf{k})\},$$

and consider the following sets:

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

$$\mathcal{M}(\mathbf{s}, \mathbf{k}, Q, P) \triangleq \{m \in \mathcal{M} : \text{for which } \beta_{Q,P}(m, \mathbf{s}, \mathbf{k}) \text{ takes place}\}, \ (\mathbf{s}, \mathbf{k}) \in \mathcal{T}_Q^N(S,K),$$

$$\mathcal{MSK}(Q, P) \triangleq \{(m, \mathbf{s}, \mathbf{k}), m \in \mathcal{M}, (\mathbf{s}, \mathbf{k}) \in \mathcal{T}_Q^N(S,K) : \text{for which } \beta_{Q,P}(m, \mathbf{s}, \mathbf{k}) \text{ takes place}\}.$$

Lemma 1. *For all $E > 2\delta \ge 0$, type Q, covert channel $P \in \mathcal{P}(Q, \Delta_1)$ and the set of attack channels $\mathcal{A}(Q, P, \Delta_2)$ there exists a matrix $\mathbf{L} = \{\mathbf{ux}(m, \mathbf{s}, \mathbf{k})\}_{m=\overline{1,M}}^{(\mathbf{s},\mathbf{k}) \in \mathcal{T}_Q^N(S,K)}$, with*

$$M = \exp\Big\{N \min_{A \in \mathcal{A}(Q,P,\Delta_2)} \min_{V : D(V\|A|Q,P) \le E} |I_{Q,P,V}(Y \wedge U|K) -$$

$$-I_{Q,P}(S \wedge U|K) + D(V\|A|Q,P) - E + 2\delta|^+\Big\},$$

such that for each vector pair $(\mathbf{s},\mathbf{k}) \in \mathcal{T}_Q^N(S,K)$ *vectors* $\mathbf{ux}(m,\mathbf{s},\mathbf{k})$ *for different* $m \in \mathcal{M}(\mathbf{s},\mathbf{k},Q,P)$ *are distinct and*

$$\Pr\{\overline{\beta}_{Q,P}(m,\mathbf{s},\mathbf{k})\} \le \exp\{-\exp\{N\delta/4\}\}, \tag{6}$$

and for any triple $(m,\mathbf{s},\mathbf{k}) \in \mathcal{MSK}(Q,P)$, *conditional types* $V,\hat{V}: \mathcal{X} \to \mathcal{Y}$ *for sufficiently large* N, *the following inequality holds:*

$$\left|\mathcal{T}^N_{Q,P,V}(Y|\mathbf{ux}(m,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k}) \bigcap \bigcup_{m'\ne m\, \mathbf{s}':(\mathbf{s}',\mathbf{k})\in\mathcal{SK}(m',Q,P)} \bigcup \mathcal{T}^N_{Q,P,\hat{V}}(Y|\mathbf{ux}(m',\mathbf{s}',\mathbf{k}),\mathbf{s}',\mathbf{k})\right| \le$$

$$\le |\mathcal{T}^N_{Q,P,V}(Y|\mathbf{ux}(m,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k})| \exp\left\{-N\left|E - \min_{A\in\mathcal{A}(Q,P,\Delta_2)} D(\hat{V}\|A|Q,P)\right|^+\right\}. \tag{7}$$

Lemma 1 is the generalization of packing lemma [11, 7], and proved by the method of types [12]. Lemma 2 follows from lemma 1.

Lemma 2. *For all* $E > 2\delta \ge 0$, *type* Q', *such that* $D(Q'\|Q) \le E$, *covert channel* $P \in \mathcal{P}(Q,\Delta_1)$ *and the set of attack channels* $\mathcal{A}(Q,P,\Delta_2)$ *there exists a matrix* $\mathrm{L} = \{\mathbf{ux}(m,\mathbf{s},\mathbf{k})\}_{m=\overline{1,M}}^{(\mathbf{s},\mathbf{k})\in\mathcal{T}^N_{Q'}(S,K)}$, *with*

$$M = \exp\left\{N \min_{A\in\mathcal{A}(Q,P,\Delta_2)} \min_{V:D(Q'\circ P\circ V\|Q\circ P\circ A)\le E} |I_{Q',P,V}(Y\wedge U|K) -\right.$$

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

such that for each vector pair $(\mathbf{s},\mathbf{k}) \in \mathcal{T}^N_{Q'}(S,K)$ *vectors* $\mathbf{ux}(m,\mathbf{s},\mathbf{k})$ *for different* $m \in \mathcal{M}(\mathbf{s},\mathbf{k},Q',P)$ *are distinct and*

$$\Pr\{\overline{\beta}_{Q',P}(m,\mathbf{s},\mathbf{k})\} \le \exp\{-\exp\{N\delta/4\}\}, \tag{8}$$

and for any triple $(m,\mathbf{s},\mathbf{k}) \in \mathcal{MSK}(Q',P)$, *conditional types* $V,\hat{V}: \mathcal{X} \to \mathcal{Y}$ *for sufficiently large* N *the following inequality holds:*

$$\left|\mathcal{T}^N_{Q',P,V}(Y|\mathbf{ux}(m,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k}) \bigcap \bigcup_{m'\ne m\, \mathbf{s}':(\mathbf{s}',\mathbf{k})\in\mathcal{SK}(m',Q',P)} \bigcup \mathcal{T}^N_{Q',P,\hat{V}}(Y|\mathbf{ux}(m',\mathbf{s}',\mathbf{k}),\mathbf{s}',\mathbf{k})\right| \le$$

$$\le |\mathcal{T}^N_{Q',P,V}(Y|\mathbf{ux}(m,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k})| \exp\left\{-N\left|E - \min_{A\in\mathcal{A}(Q,P,\Delta_2)} D(Q'\circ P\circ V\|Q\circ P\circ A)\right|^+\right\}:$$

In the proof of theorem 1 we use the statement of lemma 3, which follow from lemma 2. Let us denote

$$\mathcal{T}^E_Q(S,K) = \bigcup_{Q':D(Q'\|Q)\le E} \mathcal{T}^N_{Q'}(S,K).$$

Lemma 3. *For all $E > 2\delta \geq 0$, covert channel $P \in \mathcal{P}(Q, \Delta_1)$ and the set of attack channels $\mathcal{A}(Q, P, \Delta_2)$ there exists a matrix $\mathrm{L} = \{\mathbf{ux}(m, \mathbf{s}, \mathbf{k})\}_{m=\overline{1,M}}^{(\mathbf{s},\mathbf{k})\in\mathcal{T}_Q^E(S,K)}$, with*

$$M = \exp\left\{N \min_{A\in\mathcal{A}(Q,P,\Delta_2)} \min_{Q',V:D(Q'\circ P\circ V\|Q\circ P\circ A)\leq E} |I_{Q',P,V}(Y\wedge U|K) - \right.$$

$$\left. - I_{Q',P}(S\wedge U|K) + D(Q'\circ P\circ V\|Q\circ P\circ A) - E + 2\delta|^+\right\}, \tag{9}$$

such that for each $Q' : D(Q'\|Q) \leq E$, vector pairs $(\mathbf{s}, \mathbf{k}) \in \mathcal{T}_Q^N(S, K)$ vectors $\mathbf{ux}(m, \mathbf{s}, \mathbf{k})$ for different $m \in \mathcal{M}(\mathbf{s}, \mathbf{k}, Q', P)$ are distinct and (8) is true and for any triple $(m, \mathbf{s}, \mathbf{k}) \in \mathcal{MSK}(Q', P)$, conditional types $V, \hat{V} : \mathcal{X} \to \mathcal{Y}$, type $\hat{Q}$, such that $D(\hat{Q}\|Q) \leq E$, for sufficiently large N the following inequality holds:

$$\left|\mathcal{T}^N_{Q',P,V}(Y|\mathbf{ux}(m,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k}) \bigcap \bigcup_{m'\neq m}\bigcup_{\mathbf{s}':(\mathbf{s}',\mathbf{k})\in\mathcal{SK}(m',\hat{Q},P)} \mathcal{T}^N_{\hat{Q},P,\hat{V}}(Y|\mathbf{ux}(m',\mathbf{s}',\mathbf{k}),\mathbf{s}',\mathbf{k})\right| \leq$$

$$\leq |\mathcal{T}^N_{Q',P,V}(Y|\mathbf{ux}(m,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k})| \exp\left\{-N\left|E - \min_{A\in\mathcal{A}(Q,P,\Delta_2)} D(\hat{Q}\circ P\circ\hat{V}\|Q\circ P\circ A)\right|^+\right\}. \tag{10}$$

Now to prove the random coding bound, we must show the existence of a code, that for any $0 < e < E$, the following inequality takes place

$$e(f, g, N, m, Q, P, \Delta_2) \leq \exp\{-N(E - e)\}.$$

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

$$\Pr\{(\mathbf{s}, \mathbf{k}) \notin \mathcal{T}_Q^E(S, K)\} \leq \exp\{-ND(Q'\|Q)\} < \exp\{-N(E - e)\} \tag{11}$$

(we consider only such types Q', for which $D(Q'\|Q) \leq E$).

The existence of a matrix $\mathrm{L} = \{\mathbf{ux}(m, \mathbf{s}, \mathbf{k})\}_{m=\overline{1,M}}^{(\mathbf{s},\mathbf{k})\in\mathcal{T}_Q^E(S,K)}$, satisfying (6), (9) and (10) is guaranteed by lemma 3.

Consider

$$\mathcal{SK}_Q^E(m, P) = \bigcup_{Q':D(Q'\|Q)\leq E} \mathcal{SK}(m, Q', P).$$

We apply the following decoding rule for the decoder g: each $\mathbf{y}$ and $\mathbf{k}$ are decoded to such m, for which $\mathbf{y} \in \mathcal{T}^N_{Q',P,V}(Y|\mathbf{ux}(m, \mathbf{s}, \mathbf{k}), \mathbf{s}, \mathbf{k})$, where Q', P, V are such that $\min\limits_{A\in\mathcal{A}(Q,P,\Delta_2)} D(Q'\circ P\circ V\|\hat{Q}\circ P\circ A)$ is minimal.

The decoder g can make an error when the message m is transmitted if $\overline{\beta}_{Q',P}(m, \mathbf{s}, \mathbf{k})$ takes place or if $(\mathbf{s}, \mathbf{k}) \in \mathcal{SK}_Q^E(m, P)$, but there exist $m' \neq m$, type $\hat{Q}$ (such that $D(\hat{Q}\|Q) \leq E$), $\hat{V}$, vector pair $(\mathbf{s}', \mathbf{k}) \in \mathcal{SK}(m', \hat{Q}, P)$ such that

$$\mathbf{y} \in \mathcal{T}^N_{Q',P,V}(Y|\mathbf{ux}(m,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k}) \bigcap \mathcal{T}_{\hat{Q},P,\hat{V}}(Y|\mathbf{ux}(m',\mathbf{s}',\mathbf{k}),\mathbf{s}',\mathbf{k})$$

and

$$\min_{A\in\mathcal{A}(Q,P,\Delta_2)} D(\hat{Q}\circ P\circ\hat{V}\|Q\circ P\circ A) \leq \min_{A\in\mathcal{A}(Q,P,\Delta_2)} D(Q'\circ P\circ V\|Q\circ P\circ A). \tag{12}$$

Denote

$$\mathcal{D} = \left\{\hat{Q}, V, \hat{V} : (12) \text{ is valid}\right\}.$$

The error probability of the code for any message $m \in \mathcal{M}$, maximal over all attack channels $A \in \mathcal{A}(Q, P, \Delta_2)$ can be upper bounded in the following way:

$$e(f, g, N, m, Q, P, \Delta_2) \le \max_{A \in \mathcal{A}(Q,P,\Delta_2)} \sum_{(\mathbf{s},\mathbf{k}) \in \mathcal{T}^E_Q(S,K)} Q^N(\mathbf{s},\mathbf{k}) e(f, g, N, m, \mathbf{s}, \mathbf{k}, A) + \exp\{-N(E-e)\},$$

which follows from (11). Then from (8) we have

$$\max_{A \in \mathcal{A}(Q,P,\Delta_2)} \sum_{(\mathbf{s},\mathbf{k}) \in \mathcal{T}^E_Q(S,K)} Q^N(\mathbf{s},\mathbf{k}) e(f, g, N, m, \mathbf{s}, \mathbf{k}, A) \le$$

$$\le \sum_{(\mathbf{s},\mathbf{k}) \in \mathcal{T}^E_Q(S,K) \setminus \mathcal{SK}^E_Q(m,P)} Q^N(\mathbf{s},\mathbf{k}) \Pr\{\overline{\beta}_{Q',P}(m,\mathbf{s},\mathbf{k})\} +$$

$$+ \max_{A \in \mathcal{A}(Q,P,\Delta_2)} \sum_{(\mathbf{s},\mathbf{k}) \in \mathcal{SK}^E_Q(m,P)} Q^N(\mathbf{s},\mathbf{k}) \times A^N \left\{ \bigcup_{\mathcal{D}} \mathcal{T}^N_{Q',P,V}(Y|\mathbf{ux}(m,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k}) \bigcap \right.$$

$$\left. \bigcap \bigcup_{m' \ne m} \bigcup_{\mathbf{s}':(\mathbf{s}',\mathbf{k}) \in \mathcal{SK}(m',\hat{Q},P)} \mathcal{T}^N_{\hat{Q},P,\hat{V}}(Y|\mathbf{ux}(m',\mathbf{s}',\mathbf{k}),\mathbf{s}',\mathbf{k}) \middle| \mathbf{x}(m,\mathbf{s},\mathbf{k}) \right\} \le$$

$$\le \sum_{(\mathbf{s},\mathbf{k}) \in \mathcal{T}^E_Q(S,K) \setminus \mathcal{SK}^E_Q(m,P)} Q^N(\mathbf{s},\mathbf{k}) \exp\{-\exp\{N\delta/4\}\} +$$

$$+ \sum_{\mathcal{D}} \left| \mathcal{T}^N_{Q',P,V}(Y|\mathbf{ux}(m,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k}) \bigcap \bigcup_{m' \ne m} \bigcup_{\mathbf{s}':(\mathbf{s}',\mathbf{k}) \in \mathcal{SK}(m',\hat{Q},P)} \mathcal{T}^N_{\hat{Q},P,\hat{V}}(Y|\mathbf{ux}(m',\mathbf{s}',\mathbf{k}),\mathbf{s}',\mathbf{k}) \right| \times$$

$$\times \max_{A \in \mathcal{A}(Q,P,\Delta_2)} \sum_{(\mathbf{s},\mathbf{k}) \in \mathcal{SK}^E_Q(m,P)} Q^N(\mathbf{s},\mathbf{k}) A^N(\mathbf{y}|\mathbf{x}).$$

Taking into account the inequality (10) and the following combinatorial expressions [11, 12]

$$|\mathcal{T}^N_{Q',P,V}(Y|\mathbf{ux}(m,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k}| \le \exp\{N H_{Q',P,V}(Y|U,X,S,K)\} \le \exp\{N H_{Q',P,V}(Y|X)\},$$

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

$$Q^N(\mathbf{s},\mathbf{k}) = \exp\{-N(H_{Q'}(S,K) + D(Q'\|Q))\}, \tag{13}$$

$$A^N(\mathbf{y}|\mathbf{x}) = \exp\{-N(H_{Q',P,V}(Y|X) + D(V\|A|Q',P))\}, \tag{14}$$

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

we can bound error probability from above by

$$e(f, g, N, m, Q, P, \Delta_2) \le (N+1)^{|\mathcal{S}||\mathcal{K}|} \exp\{-\exp\{N\delta/4\}\} + \exp\{-N(E-e_1)\} +$$

$$+ \sum_{\mathcal{D}} \exp\{N H_{Q',P,V}(Y|X)\} \exp\{-N(E - \min_{A \in \mathcal{A}(Q,P,\Delta_2)} D(\hat{Q} \circ P \circ \hat{V} \| Q \circ P \circ A))\} \times$$

$$\times \max_{A\in\mathcal{A}(Q,P,\Delta_2)} [\exp\{-N(H_{Q',P}(Y|X)+D(Q'\|Q)+D(V\|A|Q',P)\}] \le$$
$$\le \exp\{-\exp\{N\delta/4\}+N\delta_1\}+\exp\{-N(E-e_1)\}+$$
$$+\sum_{\mathcal{D}} \exp\{N(H_{Q',P,V}(Y|X)-E-H_{Q',P,V}(Y|X)-$$
$$-\min_{A\in\mathcal{A}(Q,P,\Delta_2)} D(Q'\circ P\circ V\|Q\circ P\circ A)-\min_{A\in\mathcal{A}(Q,P,\Delta_2)} D(\hat{Q}\circ P\circ \hat{V}\|Q\circ P\circ A)\Big)\Big\} \le$$
$$\le \exp\{-\exp\{N\delta/4\}+N\delta_1\}+\exp\{-N(E-e_1)\}+(N+1)^{|\mathcal{S}||\mathcal{K}|+|\mathcal{A}||\mathcal{X}|+2|\mathcal{A}||\mathcal{X}||\mathcal{Y}|}\exp\{-NE\} \le$$
$$\le \exp\{-N(E-e)\}.$$

Therefore, for N large enough $e(f,g,N,Q,P,\Delta_2) \le \exp\{-N(E-e)\}$, for all $A \in \mathcal{A}(Q,P,\Delta_2)$.

The lower bound in theorem 1 is proved.

5 Proof of the Upper Bound

Let $0 < e < E$ is any positive number and $P \in \mathcal{P}(Q,\Delta_1)$ is any fixed covert channel (defined in (4)).

Consider the given code (f,g), average error probability of which over all attack channels $\mathcal{A}(Q,P,\Delta_2)$ satisfies the condition

$$\bar{e}(f,g,N,Q,P,\Delta_2) \le \exp\{-N(E-e)\}.$$

According to (1) and (2), it means that

$$\frac{1}{M}\max_{A\in\mathcal{A}(Q,P,\Delta_2)}\sum_{m\in\mathcal{M}}\sum_{(\mathbf{s},\mathbf{k})\in\mathcal{S}^N\times\mathcal{K}^N} Q^N(\mathbf{s},\mathbf{k})A^N\{\mathcal{Y}^N-g^{-1}(m|\mathbf{k})|f(m,\mathbf{s},\mathbf{k})\} \le \exp\{-N(E-e)\}.$$

The left part of this inequality can only decrease, if we take the sum by vector pairs $(\mathbf{s},\mathbf{k})$ of any fixed type Q'.

$$\max_{A\in\mathcal{A}(Q,P,\Delta_2)}\sum_{(\mathbf{s},\mathbf{k})\in T^N_{Q'}(S,K)}\sum_{\mathbf{x}(m,\mathbf{s},\mathbf{k})\in f(\mathcal{M},\mathbf{s},\mathbf{k})} Q^N(\mathbf{s},\mathbf{k})A^N\{\mathcal{Y}^N-g^{-1}(m|\mathbf{k})|f(m,\mathbf{s},\mathbf{k})\} \le$$
$$\le M\exp\{-N(E-e)\},$$

where $f(\mathcal{M},\mathbf{s},\mathbf{k})$ is the set of all codewords, used for the vector pair $(\mathbf{s},\mathbf{k}) \in T^N_{Q'}(S,K)$. Fix the conditional type P and consider the vectors $\mathbf{x}(m,\mathbf{s},\mathbf{k})$ from $T^N_{Q',P}(X|\mathbf{s},\mathbf{k})$ for each vector pair $(\mathbf{s},\mathbf{k}) \in T^N_{Q'}(S,K)$. Then

$$M = \sum_P |f(\mathcal{M},\mathbf{s},\mathbf{k})\bigcap T^N_{Q',P}(X|\mathbf{s},\mathbf{k})|$$

and

$$M = \frac{1}{|T^N_{Q'}(S,K)|}\sum_{(\mathbf{s},\mathbf{k})\in T^N_{Q'}(S,K)}\sum_P |f(\mathcal{M},\mathbf{s},\mathbf{k})\bigcap T^N_{Q',P}(X|\mathbf{s},\mathbf{k})|.$$

Taking into account that the number of types P is not greater than $(N+1)^{|\mathcal{S}||\mathcal{K}||\mathcal{X}|}$ [11, 12], we have

$$M \le (N+1)^{|\mathcal{S}||\mathcal{K}||\mathcal{X}|} \frac{1}{|\mathcal{T}^N_{Q'}(S,K)|} \sum_{(\mathbf{s},\mathbf{k})\in\mathcal{T}^N_{Q'}(S,K)} \max_P |f(\mathcal{M},\mathbf{s},\mathbf{k}) \bigcap \mathcal{T}^N_{Q',P}(X|\mathbf{s},\mathbf{k})|.$$

Then there exists at least one type P, such that

$$M|\mathcal{T}^N_{Q'}(S,K)|(N+1)^{-|\mathcal{S}||\mathcal{K}||\mathcal{X}|} \le \sum_{(\mathbf{s},\mathbf{k})\in\mathcal{T}^N_{Q'}(S,K)} |f(\mathcal{M},\mathbf{s},\mathbf{k})) \bigcap \mathcal{T}^N_{Q',P}(X|\mathbf{s},\mathbf{k})|. \qquad (15)$$

For any conditional type V we have

$$\max_{A\in\mathcal{A}(Q,P,\Delta_2)} \sum_{(\mathbf{s},\mathbf{k})\in\mathcal{T}^N_{Q'}(S,K)} \sum_{\mathbf{x}(m,\mathbf{s},\mathbf{k})\in f(\mathcal{M},\mathbf{s},\mathbf{k})\bigcap\mathcal{T}^N_{Q',P}(X|\mathbf{s},\mathbf{k})} Q^N(\mathbf{s},\mathbf{k})A^N\{\mathcal{T}^N_{Q',P,V}(Y|\mathbf{x}(m,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k}) -$$

$$-g^{-1}(m|\mathbf{k})|\mathbf{x}(m,\mathbf{s},\mathbf{k})\} \le M\exp\{-N(E-e)\}.$$

As $A^N(\mathbf{y}|\mathbf{x})$ and $Q^N(\mathbf{s},\mathbf{k})$ are constant for all $(\mathbf{s},\mathbf{k}) \in \mathcal{T}^N_{Q'}(\mathbf{s},\mathbf{k})$, $\mathbf{x} \in \mathcal{T}^N_{Q',P}(X|\mathbf{s},\mathbf{k})$, $\mathbf{y} \in \mathcal{T}^N_{Q',P,V}(Y|\mathbf{x},\mathbf{s},\mathbf{k})$, we obtain

$$\max_{A\in\mathcal{A}(Q,P,\Delta_2)} \sum_{(\mathbf{s},\mathbf{k})\in\mathcal{T}^N_{Q'}(S,K)} \sum_{\mathbf{x}(m,\mathbf{s},\mathbf{k})\in f(\mathcal{M},\mathbf{s},\mathbf{k})\bigcap\mathcal{T}^N_{Q',P}(X|\mathbf{s},\mathbf{k})} Q^N(\mathbf{s},\mathbf{k})A^N(\mathbf{y}|\mathbf{x})\times$$

$$\times\{|\mathcal{T}^N_{Q',P,V}(Y|\mathbf{x}(m,\mathbf{s},\mathbf{k}))| - |g^{-1}(m|\mathbf{k})\bigcap\mathcal{T}^N_{Q',P,V}(Y|\mathbf{x}(m,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k})|\} \le M\exp\{-N(E-e)\},$$

or

$$\sum_{(\mathbf{s},\mathbf{k})\in\mathcal{T}^N_{Q'}(S,K)} \sum_{\mathbf{x}(m,\mathbf{s},\mathbf{k})\in f(\mathcal{M},\mathbf{s},\mathbf{k})\bigcap\mathcal{T}^N_{Q',P}(X|\mathbf{s},\mathbf{k})} \{|\mathcal{T}^N_{Q',P,V}(Y|\mathbf{x}(m,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k})| -$$

$$-|g^{-1}(m|\mathbf{k})\bigcap\mathcal{T}^N_{Q',P,V}(Y|\mathbf{x}(m,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k})|\} \le \frac{M\exp\{-N(E-e)\}}{Q^N(\mathbf{s},\mathbf{k})\max\limits_{A\in\mathcal{A}(Q,P,\Delta_2)} A^N(\mathbf{y}|\mathbf{x})}.$$

Taking into account (13) and (14) we obtain

$$\sum_{(\mathbf{s},\mathbf{k})\in\mathcal{T}^N_{Q'}(S,K)} \sum_{\mathbf{x}(m,\mathbf{s},\mathbf{k})\in f(\mathcal{M},\mathbf{s},\mathbf{k})\bigcap\mathcal{T}^N_{Q',P,V}(X|\mathbf{s},\mathbf{k})} \{|\mathcal{T}^N_{Q',P,V}(Y|\mathbf{x}(m,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k})| -$$

$$-\frac{M\exp\{-N(E-e)\}}{\exp\{-N(H_{Q'}(S,K)+D(Q'\|Q)+H_{Q',P,V}(Y|X)+\min\limits_{A\in\mathcal{A}(Q,P,\Delta_2)} D(V\|A|Q',P))\}} \le$$

$$\le \sum_{(\mathbf{s},\mathbf{k})\in\mathcal{T}^N_{Q'}(S,K)} \sum_{\mathbf{x}(m,\mathbf{s},\mathbf{k})\in f(\mathcal{M},\mathbf{s},\mathbf{k})\bigcap\mathcal{T}^N_{Q',P}(X|\mathbf{s},\mathbf{k})} |g^{-1}(m|\mathbf{k})\bigcap\mathcal{T}^N_{Q',P,V}(Y|\mathbf{x}(m,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k})|\}.$$

The right part of the last inequality can be upper bounded by

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

as the sets $g^{-1}(m|\mathbf{k})$, are disjoint for different $m \in \mathcal{M}$.

Taking into account the following properties of types [11, 12]

$$(N+1)^{-|\mathcal{Y}||\mathcal{X}||\mathcal{S}||\mathcal{K}|}\exp\{NH_{Q',P,V}(Y|X,S,K)\} \le |\mathcal{T}^N_{Q',P,V}(Y|\mathbf{x}(m,\mathbf{s},\mathbf{k}),\mathbf{s},\mathbf{k})|$$

and (11) we have

$$\sum_{(\mathbf{s},\mathbf{k})\in\mathcal{T}^N_{Q'}(S,K)} |f(\mathcal{M},\mathbf{s},\mathbf{k})\bigcap\mathcal{T}^N_{Q',P}(X|\mathbf{s},\mathbf{k})|(N+1)^{-|\mathcal{X}||\mathcal{Y}||\mathcal{S}||\mathcal{K}|}\times$$

$$\times\exp\{NH_{Q',P,V}(Y|X,S,K)\} - M\exp\{N(H_{Q'}(S,K)+H_{Q',P,V}(Y|X)+$$

$$+\min_{A\in\mathcal{A}(Q,P,\Delta_2)} D(Q'\circ P\circ V||Q\circ P\circ A) - E + e)\} \le \sum_{(\mathbf{s},\mathbf{k})\in\mathcal{T}^N_{Q'}(S,K)} \exp\{NH_{Q',P,V}(Y|S,K)\}.$$

As the random variables X, Y, S, K form the following Markov chain $(S,K)\to X\to Y$, then $H_{Q',P,V}(Y|X) = H_{Q',P,V}(Y|X,S,K)$. Then, taking into account (15) we obtain

$$M\exp\{N(H_{Q'}(S,K)+H_{Q',P,V}(Y|X,S,K))\}\left[(N+1)^{-|\mathcal{X}|(|\mathcal{Y}|+|\mathcal{S}||\mathcal{K}|)} - \right.$$

$$\left. -\exp\left\{N\left(\min_{A\in\mathcal{A}(Q,P,\Delta_2)} D(Q'\circ P\circ V||Q\circ P\circ A) - E + e\right)\right\}\right] \le$$

$$\le \exp\{N(H_{Q'}(S,K)+H_{Q',P,V}(Y|S,K))\},$$

or

$$M \le \frac{\exp\{N(H_{Q',P,V}(Y|S,K) - H_{Q',P,V}(Y|X,S,K))\}}{(N+1)^{-|\mathcal{X}|(|\mathcal{Y}|+|\mathcal{S}||\mathcal{K}|)} - \exp\left\{N\left(\min_{A\in\mathcal{A}(Q,P,\Delta_2)} D(Q'\circ P\circ V||Q\circ P\circ A) - E + e\right)\right\}} =$$

$$= \min_{A\in\mathcal{A}(Q,P,\Delta_2)} \frac{\exp\{N(H_{Q',P,V}(Y|S,K) - H_{Q',P,V}(Y|X,S,K))\}}{(N+1)^{-|\mathcal{X}|(|\mathcal{Y}|+|\mathcal{S}||\mathcal{K}|)} - \exp\{N\left(D(Q'\circ P\circ V||Q\circ P\circ A) - E + e\right)\}}.$$

For each $A\in\mathcal{A}(Q,P,\Delta_2)$ the function in the right part of this inequality can be minimized by the choice of types Q', V, keeping positive the denominator, for which the following inequality must be satisfied

$$D(Q'\circ P\circ V||Q\circ P\circ A) \le E.$$

Taking into account the continuity of all expressions we can minimize not only by types, but also by any conditional probability distributions V and Q'. Then it can be maximized by the choice of the covert channel $P\in\mathcal{P}(Q,\Delta_1)$.

It remains to notice that $H_{Q',P,V}(Y|S,K) - H_{Q',P,V}(Y|X,S,K) = I_{Q',P,V}(Y\wedge X|S,K)$. The upper bound 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] 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.

[7] 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.

[8] 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.

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

[10] 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.

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

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

Տվյալներ թաքցնող համակարգերի համար արագություն-հուսալիություն-շեղում ֆունկցիայի գնահատականների մասին

Մ. Ե. Հարությունյան և Ս. Ա. Տոնոյան

Ամփոփում

Աշխատանքում ուսումնասիրված է Պ. Մուլինի և Ջ. Օ'Սուլիվանի կողմից դիտարկված տվյալներ թաքցնող համակարգի ընդհանուր մոդելը: Այդ համակարգի համար ներմուծված է արագություն-հուսալիություն-շեղում ֆունկցիայի գաղափարը, որի համար կառուցված են ստորին և վերին գնահատականներ, որոնք համապատասխանաբար կոչվում են պատահական կողավորման և սֆերաների փաթեթավորման սահմաններ: Ստորին գնահատականը սահմանային դեպքում, երբ $E \to 0$, համընկնում է համակարգի ունակության հետ: