Journal of Universal Computer Science, vol. 29, no. 11 (2023), 1254-1273
submitted: 19/5/2023, accepted: 30/9/2023, appeared: 28/11/2023 CC BY-ND 4.0

Two-Stage Optimal Hypotheses Testing for a Model of Stegosystem with an Active Adversary

Mariam Haroutunian
(Institute for Informatics and Automation Problems of NAS of RA, Yerevan, Armenia
https://orcid.org/0000-0002-9262-4173, armar@sci.am)

Parandzem Hakobyan
(Institute for Informatics and Automation Problems of NAS of RA, Yerevan, Armenia
https://orcid.org/0000-0002-5056-9591, par_h@iiap.sci.am)

Arman Avetisyan
(Institute for Informatics and Automation Problems of NAS of RA, Yerevan, Armenia
https://orcid.org/0000-0002-0434-2767, armanavetisyan1997@gmail.com)

Abstract: We study the information-theoretic model of stegosystem with an active adversary, where unlike a passive adversary he can not only read but also write. The legitimate sender as well as the adversary can embed or not a message in the sending data. The receiver's first task is to decide whether the communication is a covertext, data with no hidden message, or a stegotext, modified data with a hidden secret message. In case of stegotext, the receiver's second task is to decide whether the message was sent by a legitimate sender or from an adversary. For this purpose an authenticated encryption from the legitimate sender is considered.

In this paper we suggest two-stage statistical hypothesis testing approach from the receivers point of view. We propose the logarithmically asymptotically optimal testing for this model. As a result the functional dependence of reliabilities of the first and second kind of errors in both stages is constructed. A comparison of overall error probabilities with the situation of one stage hypotheses testing is discussed and the behaviour of functional dependences of reliabilities are illustrated.

Keywords: Security, Hypotheses testing, Authentication.
Categories: E.4
DOI: 10.3897/jucs.112913

1 Introduction

The aim of steganography is communicating messages by hiding them within other data thereby creating a covert channel. By standard terminology of information hiding [Pfitzmann 1996] the legitimate users are Alice and Bob, who wishes to communicate over a public channel, such that the presence of hidden message must be unnoticed to an adversary (Eve).

Various models with various tasks have been studied [Katzenbeisser et al. 2002], [Hopper et al. 2002], [Von Ahn and Hopper 2004], [Backes and Cachin 2005], [Dedic et al. 2009], [Liśkiewicz et al. 2011], [Augot et al. 2011]. We are interested in information-theoretic investigations studied in many papers including [O'Sullivan et al. 1998], [Moulin and O'Sullivan 2003], [Cachin 2004], [Mittelholzer 2000], [Wang and Moulin 2008], [Shikata and Matsumoto 2008], [Balado and Haughton 2018].

In [Cachin et al. 1998], [Cachin 2004] Cachin first proposed an information-theoretic model of steganography with passive adversary (who has read-only access to the public channel) (Fig. 1). Alice can be inactive and send a covertext C without hidden information or be active and send stegotext S. Bob has the exctracting algorithm, but Eve does not know if Alice was active or not. Hence, Eve must solve the problem of Hypothesis testing.

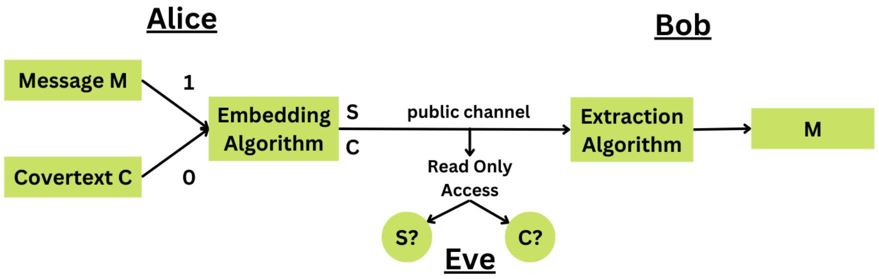

Figure 1: The model of stegosystem with passive attacks.

An extended information-theoretic model for steganography with active attacks (where adversary can read and write a message over an insecure channel) was proposed and studied in [Shikata and Matsumoto 2008]. More specifically, the authors showed a generic construction of secure stegosystems by using almost unbiased functions and secure authenticated encryption with random ciphertexts in the model with active adversaries in unconditional setting. The problem of information-theoretically secure authenticated encryption is addressed in [Alomair and Poovendran 2009].

In this paper we consider an information-theoretic model of a stegosystem with active attacks (Fig. 2), we propose and study the problem of optimal hypothesis testing, which will be described later in this section.

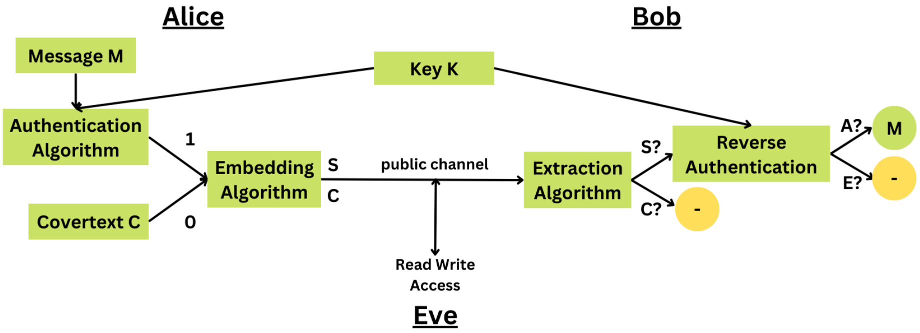

Figure 2: The model of stegosystem with active adversary.

Adversary has an access to a read and write public channel and is able to analyze and modify data. Alice as well as Eve can be either active or passive, i.e. can embed or not a message in the sending data. Bob's first task is to decide whether the received data X is a covertext C, data with no hidden message, or stegotext S, modified data with a hidden secret message M. In case of deciding that the obtained data is stegotext, Bob has the extraction function, and the second task for Bob is to decide whether the extracted message was sent by Alice or Eve. For this purpose an authenticated encryption of message M with secret key K is considered. Depending on applications this encryption except authentication can include also secrecy requirements of hidden message.

Covertext is generated by a source according to a distribution P_C, stegotext has a distribution P_S according to a certain embedding function. The distribution of secret key we denote by P_K. We assume that Eve knows all these distributions. For the authenticated encryption Alice generates the encrypted message according to P_{MK} and Eve can generate a message with distribution $P_M P_K$.

We suggest two-stage statistical hypotheses testing approach from receivers point of view. On the first stage Bob has to decide if the data was generated according to P_C or P_S. In the case when Bob decides that stegotext is obtained, after extracting the secret message, on the second stage Bob has to decide if the message was generated according to P_{MK} or $P_M P_K$. Further, we substantiate the advantages of our approach.

The paper is organized as follows. In the next section the considered problem and the related art are presented. The main notations and definitions are given in the section 3 and the results are formulated in section 4. Some discussions on partial cases and reccomendations are provided in section 5. In section 6 some illustrations of the functional behaviour is presented. The conclusion remarks are in section 7. The detailed proofs of the theorems are placed in the appendix.

2 Problem Statement

In classical statistical hypothesis testing problem a statistician makes decision on which of the two proposed hypotheses H_1 and H_2 must be accepted based on data samples. This decision is made on the certain procedure which is called test. Due to randomness of the data the result of this decision may lead to two types of errors: the fist type is called the error for accepting H_2 when H_1 is true and the second type error for accepting H_1 when H_2 is true. In such problems the aim is to find such a test, that reduces both types of errors as much as possible. The complexity of the task is that the two types of errors are interconnected, when the one is reduced the other one can get increased.

Another problem related with information theory is the case of a tests sequence, where the error probabilities are decreasing exponentially as 2^{-NE}, when the number of observations N is increasing. The exponent of error probability E is called *reliability*. In the case with two hypotheses both reliabilities corresponding to two possible error probabilities could not increase simultaneously. It is an accepted way to fix the value of one of the reliabilities and try to make the tests sequence get the greatest value of the remaining reliability. Such a test is called *logarithmically asymptotically optimal* (LAO). The publications [Hoeffding 1965], [Csiszár and Longo 1971] , [Blahut 1974], [Tusnady 1977], [Longo and Sgarro 1980], [Birgé 1981],[Haroutunian 1989], [Haroutunian 1990] and [Haroutunian et al. 2008] are devoted to this problem, particularly, the problem of multiple hypotheses LAO testing was investigated in [Haroutunian 1989], [Haroutunian 1990], [Haroutunian et al. 2008]. Multiple hypotheses testing was proposed in many studies as an effective framework for analyzing problems in various domains, such as performance evaluation of biometric systems (see [Willems et al 2003], [Harutyunyan et al. 2011], [Yagi and Hirasawa 2022]. This framework enables looking into the underlying problems from the information-theoretic perspectives and optimal achievability bounds of error probability trade-offs while treating observations data emitted from classical models of information sources like Discrete Memoryless Source or Arbitrarily Varying Source (AVS) [Harutyunyan and Han Vinck 2006], [Grigoryan and Harutyunyan 2015], [Grigoryan et al. 2011].

The problem of LAO testing of statistical hypotheses for the steganography model with a passive adversary (Fig. 1) was solved in [Haroutunian et al. 2018]. In that model the adversary's task was to distinguish the covertext from stegotext. The functional dependence of the reliabilities of the first and the second kind errors was given.

In this paper we suggest two stage logarithmically asymptotically optimal testing of the legal receiver for the steganographic model with active adversary. At the first stage Bob decides whether a covertext or a stegotext is received. If at the first stage Bob decides that the data is a stegotext, then he uses the extraction algorithm to get the hidden message and using the key at the second stage he decides whether Eve or Alice was active.

We study the functional dependence of reliabilities of the first and second kind of errors of optimal tests in both stages. The proof of the result for first stage is similar to the result suggested in [Haroutunian et al. 2018], where the problem of LAO testing of statistical hypotheses for the steganography model with a passive adversary is solved by the method of types [Csiszár 1998]. For the second stage the approach studied in [Maurer 2000] was useful.

The results of this paper partially were reported at the CODASSCA Workshop [Haroutunian et al. 2022]. Here we introduce the full version, i.e with added proofs, discussions on advantages of our approach and illustrations of the theoretical dependences.

3 Notations and Definitions

Here we present some necessary characteristics and results of information theory [Blahut 1987], [Cover and Thomas 2006]. We denote finite sets by script capitals. The cardinality of a set $\mathcal{X}$ is denoted as $|\mathcal{X}|$. We denote random variables (RV) by X, S, C, K, M. Probability distributions (PD) are denoted by P, P_C, P_S, P_M, P_K, Q and P_{MK}.

Let PD of RV K and M be

$$P_K \stackrel{\triangle}{=} \{P_K(k), \quad k \in \mathcal{K}\},$$

$$P_M \stackrel{\triangle}{=} \{P_M(m), \quad m \in \mathcal{M}\},$$

and the joint PD of RVs M and K be

$$P_{MK} \stackrel{\triangle}{=} \{P_{MK}(m,k), \ m \in \mathcal{M}, \ k \in \mathcal{K}\}.$$

The Shannon entropy $H_P(X)$ of RV X with PD $P \stackrel{\triangle}{=} \{P = P(x), \ x \in \mathcal{X}\}$ is:

$$H_P(X) \stackrel{\triangle}{=} -\sum_{x \in \mathcal{X}} P(x) \log P(x).$$

The mutual information of RV M and K equals:

$$I_{P_{MK}}(M;K) \stackrel{\triangle}{=} \sum_{m\in\mathcal{M},\ k\in\mathcal{K}} P_{MK}(m,k)\log\frac{P_{MK}(m,k)}{P_M(m)P_K(k)}.$$

It is important to note that

$$P_M(m) = \sum_{k\in\mathcal{K}} P_{MK}(m,k),$$

$$P_K(k) = \sum_{m\in\mathcal{M}} P_{MK}(m,k).$$

The joint entropy of RVs M and K is the following:

$$H_{P_{MK}}(M,K) \stackrel{\triangle}{=} -\sum_{m\in\mathcal{M},\ k\in\mathcal{K}} P_{MK}(m,k)\log P_{MK}(m,k).$$

We use the notion of divergence (Kullback-Leibler information or "distance") defined on two PDs, say P_C and P_S, on $\mathcal{X}$ as:

$$D(P_C||P_S) \stackrel{\triangle}{=} \sum_{x\in\mathcal{X}} P_C(x)\log\frac{P_C(x)}{P_S(x)}.$$

The divergence of joint PDs $Q \stackrel{\triangle}{=} \{Q = Q(m,k),\ \ m\in\mathcal{M},\ k\in\mathcal{K}\}$ and P_{MK} on $(\mathcal{M}\times\mathcal{K})$ is:

$$D(Q||P_{MK}) \stackrel{\triangle}{=} \sum_{m\in\mathcal{M},k\in\mathcal{K}} Q(m,k)\log\frac{Q(m,k)}{P_{MK}(m,k)}.$$

The space of all joint PDs on finite set $\mathcal{M}\times\mathcal{K}$ we denote by

$$\mathcal{Q}(\mathcal{M}\times\mathcal{K}) \stackrel{\triangle}{=} \{Q : Q = Q(m,k), m\in\mathcal{M},\ \ k\in\mathcal{K}\}.$$

When RV M and K are independent, then

$$\begin{aligned} D(Q||P_{MK}) &= D(Q||P_M P_K) \\ &= \sum_{m\in\mathcal{M},k\in\mathcal{K}} Q(m,k)\log\frac{Q(m,k)}{P_M(m)P_K(k)}. \end{aligned}$$

In particular, the divergence of PDs P_{MK} and $P_M P_K$ is the mutual information:

$$\begin{aligned} D(P_{MK}||P_M P_K) &\stackrel{\triangle}{=} \sum_{m\in\mathcal{M},k\in\mathcal{K}} P_{MK}(m,k)\log\frac{P_{MK}(m,k)}{P_M(m)P_K(k)} \\ &= I_{P_{MK}}(M;K). \end{aligned}$$

For our investigations we use the method of types, [Haroutunian et al. 2008], [Csiszár 1998], [Csiszár and Körner 1981], the essence of which is to partition the set of all same length vectors into classes according to their empirical distributions.

The type $P_{\mathbf{x}}$ of a vector $\mathbf{x} = (x_1, ..., x_L) \in \mathcal{X}^L$ is a PD (the empirical distribution)

$$P_{\mathbf{x}} = \left\{ P_{\mathbf{x}}(x) = \frac{N(x|\mathbf{x})}{L}, x \in \mathcal{X} \right\},$$

where $N(x|\mathbf{x})$ is the number of repetitions of symbol x in vector $\mathbf{x}$. We denote by $\mathcal{P}^L(\mathcal{X})$ the set of all types of vectors in $\mathcal{X}^L$ for given L and the set of vectors $\mathbf{x}$ of type $P_{\mathbf{x}}$ is denoted by $\mathcal{T}^L_{P_{\mathbf{x}}}(X)$.

The joint type of vectors $\mathbf{m} = (x_1, ..., x_N) \in \mathcal{M}^N$ and $\mathbf{k} = (k_1, ..., k_N) \in \mathcal{K}^N$ $Q_{\mathbf{m},\mathbf{k}}$ a PD (the empirical distribution)

$$Q_{\mathbf{m},\mathbf{k}} = \left\{ Q_{\mathbf{m},\mathbf{k}} = \frac{N(m,k|\mathbf{m},\mathbf{k})}{N}, m \in \mathcal{M},\ \ k \in \mathcal{K} \right\},$$

where N(m,k|**m, k**) is the number of repetitions of symbols pair (m, k) in the pair of vectors $(\mathbf{m}, \mathbf{k})$. The set of all joint types of vector pairs $(\mathbf{m}, \mathbf{k})$ in $(\mathcal{M} \times \mathcal{K})^N$ for given N is denoted by $\mathcal{Q}^N(\mathcal{M} \times \mathcal{K})$ and the set of vector pairs $(\mathbf{m}, \mathbf{k})$ of type $Q_{\mathbf{m},\mathbf{k}}$ is denoted by $\mathcal{T}^N_{Q_{\mathbf{m},\mathbf{k}}}(M, K)$.

The following well known inequalities [Csiszár and Körner 1981] we use in the proofs of our results :

$$| \mathcal{P}^L(\mathcal{X}) | \leq (L+1)^{|\mathcal{X}|}, \tag{1}$$

$$| \mathcal{Q}^N(\mathcal{M} \times \mathcal{K}) | \leq (N+1)^{|\mathcal{M}||\mathcal{K}|}, \tag{2}$$

for any type $P \in \mathcal{P}^L(\mathcal{X})$

$$(L+1)^{-|\mathcal{X}|} \exp\{LH_P(X)\} \leq | \mathcal{T}^L_P(X) | \leq \exp\{LH_P(X)\}, \tag{3}$$

for any type $Q \in \mathcal{Q}^N(\mathcal{M} \times \mathcal{K})$

$$(N+1)^{-|\mathcal{M}||\mathcal{K}|} \exp\{NH_Q(M,K)\} \leq | \mathcal{T}^N_Q(M,K) | \leq \exp\{NH_Q(M,K)\}. \tag{4}$$

The method of types is one of the important technical tools in Information Theory.

4 Formulation of Results

First stage. At the first stage, from the received data $\mathbf{x} = (x_1, ..., x_L)$, $\mathbf{x} \in \mathcal{X}^L$, Bob must decide whether it is a covertext or a stegotext. Hence, Bob must accept one of the two hypotheses

$$H_1 : P = P_S \quad \{\text{data is a stegotext}\}$$

$$H_2 : P = P_C \quad \{\text{data is a covertext}\}.$$

The procedure of decision making is a non-randomized test φ_L, which can be defined by partition of the set of possible messages $\mathcal{X}^L$ on two disjoint subsets $\mathcal{A}^L_i$, $i = \overline{1,2}$. The set $\mathcal{A}^L_i$, $i = \overline{1,2}$ contains all data $\mathbf{x}$ for which the hypothesis H_i is adopted.

The first kind error probability, which is the probability of the rejection of the correct hypothesis H_1 is the following:

$$\alpha_{2|1}(\varphi_L) = P_S^L(\mathcal{A}_2^L).$$

The second kind error probability, which is the probability of the erroneous acceptance of hypothesis H_1 is defined as follows:

$$\alpha_{1|2}(\varphi_L) = P_C^L(\mathcal{A}_1^L).$$

The error probability exponents, called “reliabilities” of the infinite sequence of tests φ, are defined respectively as follows:

$$E_{2|1}^I(\varphi) \triangleq \varliminf_{L\to\infty} -\frac{1}{L}\log\alpha_{2|1}(\varphi_L),$$

$$E_{1|2}^I(\varphi) \triangleq \varliminf_{L\to\infty} -\frac{1}{L}\log\alpha_{1|2}(\varphi_L).$$

As defined in [Birgé 1981] the sequence of tests φ^* is called **logarithmically asymptotically optimal** (LAO) if for given positive value of $E_{2|1}^I$ the maximum possible value is provided for $E_{1|2}^I$.

The procedure for creating an optimal decision rule is similar to [Haroutunian et al. 2018]. Our first result, that is the functional dependence of the reliabilities of the first and second kind of errors is given by the following theorem.

Theorem 1. *For given*

$$0 < E_{2|1}^I < D(P_C||P_S) \tag{5}$$

there exists a LAO sequence of tests, the reliability $E_{1|2}^{*,I}$ of which is defined as follows:

$$E_{1|2}^{*,I} = E_{1|2}^{*,I}(E_{2|1}^I) = \inf_{P:\ D(P||P_S)\leq E_{2|1}^I} D(P||P_C). \tag{6}$$

When $E_{2|1}^I \geq D(P_C||P_S)$, then $E_{1|2}^{*,I}$ is equal to 0 .

Thus, for a given reliability of incorrectly rejecting the stegotext, we get the maximal reliability of wrongly accepting the stegotext.

Comment 1: Unlike model considered in [Cachin 2004], [Haroutunian et al. 2018], here Bob has no additional information about whether Alice is active or passive. Therefore, considered stegosystem should not be *perfectly secure*, because otherwise Bob cannot find out that he has received a covertext or a stegotext. Hence, we assume that for distributions P_C and P_S, $D(P_C||P_S) > 0$.

Comment 2. For given $E_{2|1}^I \in (0, D(P_C||P_S))$ the following holds:

$$E_{1|2}^{*,I} < D(P_S||P_C).$$

If at the first stage Bob accepts the hypothesis H_1, which means that he decides that the data is a stegotext, then he uses the extraction algorithm to get the hidden message

$\mathbf{m} = (m_1, m_2, ..., m_N)$.

Second stage. After the extraction using key sequence $\mathbf{k} = (k_1, k_2, ..., k_N)$ Bob has to decide whether Eve or Alice sent him that message. So he moves on to the second stage of hypothesis testing:

$$H_1 : \quad Q = P_{MK}(m, k) \qquad \{\text{there was no attack}\}$$

$$H_2 : \quad Q = P_M(m)P_K(k) \qquad \{\text{there was attack}\}.$$

In this case the test Φ_N is defined by partition of the set $(\mathcal{M} \times \mathcal{K})^N$ on two disjoint subsets $\mathcal{B}_l^N$, $l = \overline{1,2}$. The set $\mathcal{B}_1^N$ contains all data pairs $(\mathbf{m}, \mathbf{k})$ for which the hypothesis H_1 is adopted, which in our context means that message $\mathbf{m}$ is sent from Alice. Correspondingly, the set $\mathcal{B}_2^N$ contains all pairs $(\mathbf{m}, \mathbf{k})$ for which the hypothesis H_2 is adopted, i.e. Bob decides that message is sent from Eve.

The probabilities of errors of the first and second kind by analogy to the case of the first stage are defined as follows:

$$\alpha_{2|1}^{II}(\Phi_N) = P_{MK}^N(\mathcal{B}_2^N), \ \ \text{(the first kind error probability)}$$

$$\alpha_{1|2}^{II}(\Phi_N) = (P_M P_K)^N(\mathcal{B}_1^N), \ \ \text{(the second kind error probability).}$$

The error probability exponents of the infinite sequence of tests Φ, are defined respectively as follows:

$$E_{i|j}^{II}(\Phi) \stackrel{\triangle}{=} \varlimsup_{N\to\infty} -\frac{1}{N}\log \alpha_{i|j}^{II}(\Phi_N), \ \ i \neq j, \ \ i, j = \overline{1,2}.$$

The second kind error probability in Bob's decision essentially coincides with the probability of Eve's succeeding. Hence, the maximum value of $E_{1|2}^{II}$ guarantees that the attacker will fail.

As in the First Stage, for given positive value $E_{2|1}^{II}$ we constructed the LAO sequence of tests Φ^* and the dependence of maximal value $E_{1|2}^{II}$ from $E_{2|1}^{II}$ is provided in the following theorem.

Theorem 2. *For given*

$$0 < E_{2|1}^{II} < D(P_M P_K || P_{MK}) \tag{7}$$

there exists a LAO sequence of tests, the reliability $E_{1|2}^{*,II}$ of which is defined as follows:

$$E_{1|2}^{*,II}\left(E_{2|1}^{II}\right) = \inf_{Q:\ D(Q||P_{MK}) \leq E_{2|1}^{II}} D(Q||P_M P_K). \tag{8}$$

When $E_{2|1}^{II} \geq D(P_M P_K||P_{MK})$, then $E_{1|2}^{*,II}$ is equal to 0 .

Comment 3. For given $E_{2|1}^{II} \in (0, D(P_M P_K||P_{MK}))$ the following holds:

$$E_{1|2}^{*,II} < D(P_{MK}||P_M P_K) = I_{P_{MK}}(M; K).$$

The proofs of the theorems are given in the appendix, the brief outline of which is the following. Decision regions of the first and second stages, which are the disjoint subsets of the corresponding sample spaces, are constructed by comparing the divergance of the sample type and the distribution of the first hypothesis with the given reliability of the first error. When divergance is less than or equal to the given reliability, the first hypothesis is accepted, otherwise, the second hypothesis is accepted. According to the properties of types, the optimality of such sample space divisions is substantiated and the dependence of reliabilities is established.

5 Discussions

Obviously, by skipping the first stage of hypotheses testing, that is, using the extraction algorithm for all the data received, Bob can gain in error probability of the first stage at loss in time. Two questions arise.

- How much does the total error probability of the two-stage model differ from the one-stage case?

- Is it possible to propose situations, where the total error probability of the two-stage model is equal to the one-stage case, therefore, the gain will be in time without loss in the error probabilities?

Let us consider the total error probabilities and exponents in two-stage approach. First notice that $\alpha^{I}_{1|2}$ is not a principal error, because deciding that the data is a stegotext, while it is a covertext, will be discovered on extracting phase and hence, this error can be ignored.

If we denote by $\alpha_{2|1}$ the probability of Alice's failure, i.e. that Bob erroneously rejects the useful information sent by Alice, then

$$\alpha_{2|1} = \alpha^{II}_{2|1} + \alpha^{I}_{C|S\&Alice} \leq \alpha^{II}_{2|1} + \alpha^{I}_{2|1} \leq 2\max(\alpha^{II}_{2|1}, \alpha^{I}_{2|1}),$$

where $\alpha^{I}_{C|S\&Alice}$ is the error probability when data includes message sent by Alice, but Bob rejects it in the first stage deciding it as covertext.

For the corresponding reliability $E_{2|1}$ in one-stage scenario the following inequality takes place

$$E_{2|1} \geq \min(E^{II}_{2|1}, E^{I}_{2|1}).$$

On the other hand

$$\alpha_{2|1} = \alpha^{II}_{2|1} + \alpha^{I}_{C|S\&Alice} \geq \alpha^{II}_{2|1}.$$

There is also one principal error probability $\alpha_{1|2}$, when accepting fake message sent by Eve.

$$\alpha_{1|2} = \alpha^{II}_{1|2} + \alpha^{I}_{1|2} = \alpha^{II}_{1|2},$$

because as it was mentioned above we can ignore $\alpha^{I}_{1|2}$ as a not principal error.

Therefore, the overall reliability $E_{1|2}$ is equal to $E^{II}_{1|2}$.

Thus, for $E_{2|1}$ and $E_{1|2}$ we have the following:

$$\min(E^{II}_{2|1}, E^{I}_{2|1}) \leq E_{2|1} \leq E^{II}_{2|1}, \tag{9}$$

$$E_{1|2} = E^{II}_{1|2}. \tag{10}$$

Now through a pair $(E^{I}_{2|1}, E^{II}_{2|1})$ of given reliabilities of the first and second stages, we can make a judgement about the total reliabilities $(E_{2|1}, E_{1|2})$.

The pair of total reliabilities $(E_{2|1}, E_{1|2})$ can be also obtained by one-stage testing. In this approach, Bob uses the extraction algorithm to get the hidden message $\mathbf{m} = (m_1, m_2, ..., m_N)$. Obviously the data which are covertexts, are not taken into account during this process. This means that the error probability of the $\alpha^{I}_{C|S\&Alice}$ discussed in the previous scenario is equal to zero. After that he performs hypotheses testing in similar way at the second stage:

$$H_1 : \quad Q = P_{MK}(m,k) \qquad \{\text{there was no attack}\}$$

$$H_2 : \quad Q = P_M(m)P_K(k) \qquad \{\text{there was attack}\}$$

For optimal testing we have

$$0 < E_{2|1} < D(P_M P_K || P_{MK}) \tag{11}$$

and find optimal $E^{*}_{1|2}$:

$$E^{*}_{1|2}\left(E_{2|1}\right) = \inf_{Q:\ D(Q||P_{MK}) \leq E_{2|1}} D(Q||P_M P_K). \tag{12}$$

We are interested in the situations where for the indicated reliabilities we will get the same result with a two-stage approach as with the one-stage case. We shall show that such cases exist.

According to (9), for $E^{I}_{2|1} \geq E^{II}_{2|1}$ the reliability $E_{2|1}$ is equal to $E^{II}_{2|1}$. Thus, according to (9),(10), (8) and (12), the results of two and one stage approaches are the same. More specifically:

1. When
$$D(P_M P_K || P_{MK}) \geq D(P_C || P_S),$$
then for each
$$0 < E^{I}_{2|1} < D(P_C || P_S)$$
Bob can choose the reliability $E^{II}_{2|1}$, such that $E^{II}_{2|1} \leq E^{I}_{2|1}$, satisfying this condition:
$$0 < E^{II}_{2|1} \leq D(P_C || P_S).$$
In this case the results of two-stage and one-stage approaches are the same for $E_{2|1} \in \Big(0, D(P_C||P_S)\Big)$.

   Under the condition $D(P_M P_K || P_{MK}) \geq D(P_C || P_S)$ for each
$$D(P_C || P_S) < E^{II}_{2|1} < D(P_M P_K || P_{MK})$$
the reliability $E^{II}_{2|1}$ is greater than $E^{I}_{2|1}$, hence the total reliability of the two-stage test $E_{2|1}$ is less than the corresponding one-stage reliability (see (9)).

   In this case the results of two-stage and one-stage approaches are not the same.

2. When

$$D(P_M P_K||P_{MK}) \leq D(P_C||P_S),$$

then for each

$$0 < E^I_{2|1} < D(P_C||P_S)$$

Bob can choose the reliability $E^{II}_{2|1}$, such that

$$0 < E^{II}_{2|1} < D(P_M P_K||P_{MK}), \quad E^{II}_{2|1} \leq E^I_{2|1}.$$

For this case the results of two and one stage approaches are the same always, because the reliability of $E_{2|1}$ for two-stage and one-stage testing stays the same (it is true for all situations discussed above). Moreover, unlike the case 1, the changing ranges of the corresponding reliabilities $E_{2|1}$ for one-stage and two-stage testing are the same.

For all situations discussed above, the reliabilities $E^I_{1|2}$ of two-stage and one-stage testing are equal. This claim is justified by considering (9), (10), (8), (11) and (12).

6 Illustration of Results

To see the behaviour of the functions obtained in Theorem 1 and Theorem 2, here we consider simple examples with illustrations.

Consider the binary set $\mathcal{X}$ and the following distorions are given on $\mathcal{X}$:

$$P_C = \{0.2, 0.8\}, \; P_S = \{0.35, 0.65\}.$$

The values of the following divergences are:

$$D(P_C||P_S) \approx 0.005419, \; D(P_S||P_C) \approx 0.00609.$$

On Fig. 3 the function $E^{*,I}_{1|2}(E^I_{2|1})$ (6) is presented. Here (see (5)),

$$0 < E^I_{2|1} < 0.005419.$$

For the values $E^I_{2|1} \geq 0.005419$ the reliability $E^{*,I}_{1|2}$ equals 0.

Now let the distribution P_{MK} on the set $\mathcal{M} \times \mathcal{K}$ is given by the following matrix

$$P_{MK} = \begin{pmatrix} 0.1, & 0.2 \\ 0.3 & 0.4 \end{pmatrix}.$$

Then from the joint distribution P_{MK} we find

$$P_M = (0.3, 0.7), \; P_K = (0.4, 0.6).$$

The values of the divergences are:

$$D(P_M P_K||P_{MK}) \approx 0.004088, \; D(P_{MK}||P_M P_K) \approx 0.004022.$$

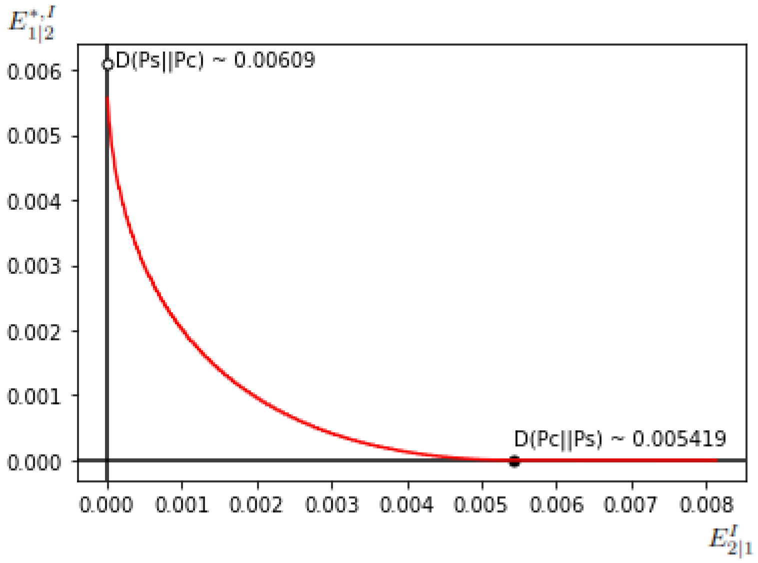

Figure 3: The dependence of reliabilities for the first stage of LAO test.

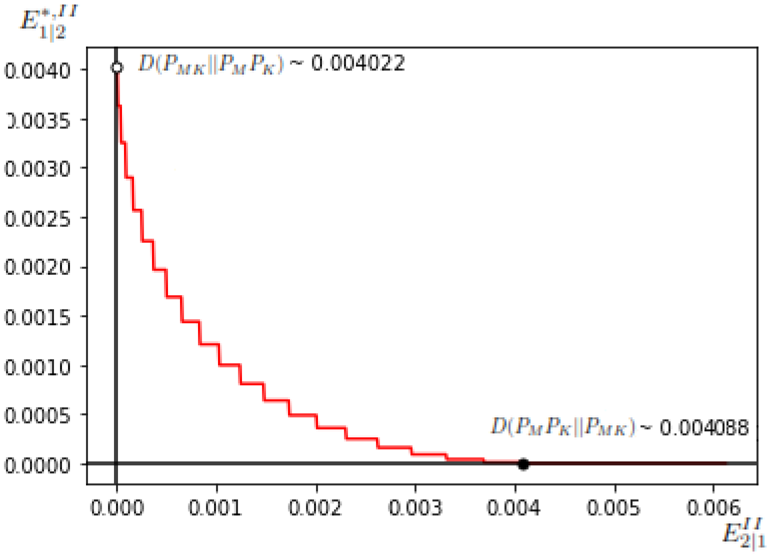

Figure 4: The dependence of reliabilities for the second stage of LAO test.

On Fig. 4 the dependence of reliabilities $E^{*,II}_{1|2}(E^{II}_{2|1})$ of the second stage obtained in

Theorem 2 (see (8), (7)) is presented. As we see, when

$$0 < E_{2|1}^{II} < 0.004088$$

then

$$0 < E_{1|2}^{*,II}(E_{2|1}^{II}) < 0.004022.$$

In the case of one-stage approach the illustration of dependence of the reliabilities $E_{2|1}$ and $E_{1|2}^{*}$ is similar to Fig. 4.

From two-stage testing we can get the same result for total reliabilities $E_{2|1}$ and $E_{1|2}$, if for every $E_{2|1}^{I} \in \big(0,\ 0.005419\big)$ Bob will choose $E_{2|1}^{II} \in \big(0,\ 0.004088\big)$, such that $E_{2|1}^{II} \leq E_{2|1}^{I}$, and vice versa, for every $E_{2|1}^{II} \in \big(0,\ 0.004088\big)$ Bob can find $E_{2|1}^{I} \in \big(0,\ 0.005419\big)$, such that $E_{2|1}^{II} \leq E_{2|1}^{I}$. According to case 2, the scatter plot of all pairs $(E_{2|1}, E_{1|2})$ will have an image like Fig. 4.

7 Conclusions

Two-stage statistical hypothesis testing approach from the receivers point of view in the stegosystem with active adversary is considered. The logarithmically asymptotically optimal testing for this model is analyzed. As a result the functional dependence of reliabilities of the first and second kind of errors in both stages is constructed. The advantages of the two-stage approach are discussed. The elaboration on behavior of derived exponents justifies the theoretical viability of the proposed framework.

In our future work, we will consider using this research to create an e-voting model with added security.

APPENDIX

The proof of Theorem 1.

The proof of the theorem is carried out in the following steps. First we show that for a given number $E_{2|1}^{I}$ we can construct a test. And at the second part, we prove that the constructed test is LAO. Let us consider the following subsets of $\mathcal{X}^L$:

$$\mathcal{B}_1^L = \bigcup_{P_{\mathbf{x}}:\ D(P_{\mathbf{x}}||P_S) \leq E_{2|1}^{I}} \mathcal{T}_{P_{\mathbf{x}}}^L(X),$$

$$\mathcal{B}_2^L = \bigcup_{P_{\mathbf{x}}:\ D(P_{\mathbf{x}}||P_S) > E_{2|1}^{I}} \mathcal{T}_{P_{\mathbf{x}}}^L(X).$$

We want to prove, that this division for given $E_{2|1}^{I}$ determines a test φ_L^*. Thus, we are going to validate, that

1. $\mathcal{X}^L = \mathcal{B}_1^L \cup \mathcal{B}_2^L$;
2. $\mathcal{B}_1^L \cap \mathcal{B}_2^L = \emptyset$;

3. $\alpha_{2|1}(\varphi^*_L) \approx 2^{-LE^I_{2|1}}$

The proof of the fist and the second claims are obvious.

Let us prove the third claim, i.e. given $E^I_{2|1}$ is the reliability of error probability $\alpha_{2|1}(\varphi^*_L)$ of tests φ^*_L.

For the proofs we use the known properties of types [Csiszár 1998]:

if $\mathbf{x} \in \mathcal{T}^L_{P_\mathbf{x}}(X)$, then

$$P^L(\mathbf{x}) = \exp\{-L(H_{P_\mathbf{x}}(X) + D(P_\mathbf{x}||P))\}. \tag{13}$$

$$(L+1)^{-|\mathcal{X}|} \exp\{-LD(P_\mathbf{x}||P)\} \leq P^L(\mathcal{T}^L_{P_\mathbf{x}}(X)) \leq \exp\{-LD(P_\mathbf{x}||P)\}. \tag{14}$$

According to (1), (3) and (14), we can estimate $\alpha^I_{2|1}(\varphi^*_L)$ by the following way:

$$\begin{aligned}
\alpha_{2|1}(\varphi^*_L) &= P^L_S\left(\mathcal{B}^L_2\right) \\
&= P^L_S\left(\bigcup_{P_\mathbf{x}: D(P_\mathbf{x}||P_S) > E^I_{2|1}} \mathcal{T}^L_{P_\mathbf{x}}(X)\right) \\
&\leq (L+1)^{|\mathcal{X}|} \sup_{P_\mathbf{x}: D(P_\mathbf{x}||P_S) > E^I_{2|1}} P^L_S\left(\mathcal{T}^L_{P_\mathbf{x}}(X)\right) \\
&\leq (L+1)^{|\mathcal{X}|} \sup_{P_\mathbf{x}: D(P_\mathbf{x}||P_S) > E^I_{2|1}} \exp\{-LD(P_\mathbf{x}||P_S)\} \\
&\leq \exp\left\{-L\left[E_{2|1} - o_L(1)\right]\right\},
\end{aligned}$$

where $o_L(1) \to 0$ when $L \to \infty$. From the definition of the reliability we get the claim 3.

Now let us prove (6), for which the first we need to estimate second error probability $\alpha_{1|2}(\varphi^*_L)$.

Using (1), (2) and (14) for this case we obtain:

$$\begin{aligned}
\alpha_{1|2}(\varphi^*_L) &= P^L_C\left(\mathcal{B}^L_1\right) \\
&= P^L_C\left(\bigcup_{P_\mathbf{x}: D(P_\mathbf{x}||P_S) \leq E^I_{2|1}} \mathcal{T}^L_{P_\mathbf{x}}(X)\right) \\
&\leq (L+1)^{|\mathcal{X}|} \sup_{P_\mathbf{x}: D(P_\mathbf{x}||P_S) \leq E^I_{2|1}} P^L_C\left(\mathcal{T}^L_{P_\mathbf{x}}(X)\right) \qquad (15) \\
&\leq (L+1)^{|\mathcal{X}|} \sup_{P_\mathbf{x}: D(P_\mathbf{x}||P_S) \leq E^I_{2|1}} \exp\{-LD(P_\mathbf{x}||P_C)\}
\end{aligned}$$

$$= \exp\left\{-L\left(\inf_{P_{\mathbf{x}}:D(P_{\mathbf{x}}||P_S)\le E^I_{2|1}} D(P_{\mathbf{x}}||P_C) - o_L(1)\right)\right\}.$$

Moreover, we can prove the inverse inequality:

$$\begin{aligned}\alpha_{1|2}(\varphi^*_L) &= P^L_C\left(\mathcal{B}^L_1\right)\\ &= P^L_C\left(\bigcup_{P_{\mathbf{x}}:D(P_{\mathbf{x}}||P_S)\le E^I_{2|1}} \mathcal{T}^L_{P_{\mathbf{x}}}(X)\right)\\ &\ge \sup_{P_{\mathbf{x}}:D(P_{\mathbf{x}}||P_S)\le E^I_{2|1}} P^L_C(\mathcal{T}^L_{P_{\mathbf{x}}}(X)) \qquad (16)\\ &\ge (L+1)^{-|\mathcal{X}|}\sup_{P_{\mathbf{x}}:D(P_{\mathbf{x}}||P_S)\le E^I_{2|1}} \exp\{-LD(P_{\mathbf{x}}||P_C)\}\\ &= \exp\left\{-L\left(\inf_{P_{\mathbf{x}}:D(P_{\mathbf{x}}||P_S)\le E^I_{2|1}} D(P_{\mathbf{x}}||P_C) + o_L(1)\right)\right\}.\end{aligned}$$

Taking into account (15), (16), and the continuity of the functions $D(P_{\mathbf{x}}||P_C)$ and $D(P_{\mathbf{x}}||P_S)$ we get that $\lim\limits_{L\to\infty} -L^{-1}\log\alpha_{1|2}(\varphi^*_L)$ exists:

$$\lim_{L\to\infty} -\frac{1}{L}\log\alpha_{1|2}(\varphi^*_L) = \inf_{P:D(P||P_S)\le E^I_{2|1}} D(P||P_C).$$

On the other hand,

$$\lim_{L\to\infty} -\frac{1}{L}\log\alpha_{1|2}(\varphi^*_L) = E^I_{1|2}(\varphi^*) \overset{\triangle}{=} E^{*,I}_{1|2}.$$

This means that for given $E^I_{1|2}$ there exists φ^* test, for which

$$E^{*,I}_{1|2} = E^{*,I}_{1|2}(E^I_{2|1}) = \inf_{P:D(P||P_S)\le E^I_{2|1}} D(P||P_C).$$

The proof of the first part of Theorem 1 will be accomplished if we demonstrate that the sequence of the test φ^* is LAO, that is for given $E^I_{2|1}$ and every sequence of tests φ $E^I_{1|2}(\varphi) \le E^{*,I}_{1|2}$ takes place.

Let us consider any other sequence φ^{**} of tests which for given $E^I_{2|1}$ is defined by partition of $\mathcal{X}^L$ to disjoint subsets $\mathcal{D}^L_1$ and $\mathcal{D}^L_2$ such that $E_{1|2}(\varphi^{**}) \ge E^{*,I}_{1|2}$. This condition is equivalent to the inequality

$$\alpha_{1|2}(\varphi^{**}_L) \le \alpha_{1|2}(\varphi^*_L) \qquad (17)$$

for L large enough.

Let us show that $\mathcal{D}_2^L \bigcap \mathcal{B}_1^L = \emptyset$. If $\mathcal{D}_2^L \bigcap \mathcal{B}_1^L \neq \emptyset$, then there exists $P'_{\mathbf{x}}$ such that $D(P'_{\mathbf{x}}||P_S) \leq E_{2|1}^I$ and $\mathcal{T}_{P'_{\mathbf{x}}}^L(X) \in \mathcal{D}_2^L$ from which it follows that

$$\alpha_{2|1}(\varphi_L^{**}) = P_S^N(\mathcal{D}_2^L) \geq P_S^L(\mathcal{T}_{P'_{\mathbf{x}}}^N(X)) \geq \exp\left\{-L\left[E_{2|1}^I + o_L(1)\right]\right\}.$$

From $\mathcal{D}_1^L \bigcup \mathcal{D}_2^L = \mathcal{X}^L$, $\mathcal{D}_1^L \bigcap \mathcal{D}_2^L = \emptyset$ and $\mathcal{D}_2^L \bigcap \mathcal{B}_1^L = \emptyset$, follows that $\mathcal{B}_1^L \subseteq \mathcal{D}_1^L$. If $\mathcal{B}_1^L \subset \mathcal{D}_1^L$, then we have that $\alpha_{1|2}(\varphi_L^{**}) \geq \alpha_{1|2}(\varphi_L^*)$, which contradicts to (17). Hence $\mathcal{D}_1^L = B_1^L$, as well as $\mathcal{D}_2^L = B_2^L$. It is the same that $\varphi^{**} = \varphi^*$.

The proof of the second part of the Theorem 1 is simple. Really, if $E_{2|1} \geq D(P_C||P_S)$, then from (6) follows that $E_{1|2}^{*,I}$ is equal to 0.

The theorem is proved.

The Proof of Theorem 2.

The optimal division of the set $(\mathcal{M} \times \mathcal{K})^N$ is constructed in the following way.

$$\mathcal{B}_1^N = \bigcup_{Q_{\mathbf{m},\mathbf{k}}:\ D(Q_{\mathbf{m},\mathbf{k}}||P_{MK}) \leq E_{2|1}^{II}} \mathcal{T}_{Q_{\mathbf{m},\mathbf{k}}}^N(M,K),$$

$$\mathcal{B}_2^N = \bigcup_{Q_{\mathbf{m},\mathbf{k}}:\ D(Q_{\mathbf{m},\mathbf{k}}||P_S) > E_{2|1}^{II}} \mathcal{T}_{Q_{\mathbf{m},\mathbf{k}}}^N(M,K).$$

We must prove, that this division for given $E_{2|1}^{II}$ determines a test Φ_N^*.

The following equalities take place for $(\mathbf{m},\mathbf{k}) = [(m_1,k_1),(m_2,k_2),...,(m_N,k_N)]$, $(\mathbf{m},\mathbf{k}) \in \mathcal{T}_{Q_{\mathbf{m},\mathbf{k}}}^N(M,K)$

$$P_M^N P_K^N(\mathbf{m},\mathbf{k}) = \exp\Big\{-N\Big[D(Q_{\mathbf{m},\mathbf{k}}||P_M P_K) + H_{Q_{\mathbf{m},\mathbf{k}}}(M,K)\Big]\Big\}, \tag{18}$$

and

$$P_{MK}^N(\mathbf{m},\mathbf{k}) = \exp\Big\{-N\Big[D(Q_{\mathbf{m},\mathbf{k}}||P_{MK}) + H_{Q_{\mathbf{m},\mathbf{k}}}(M,K)\Big]\Big\}. \tag{19}$$

Using (2), (4) and (19) we will get the estimation of the first kind error probability $\alpha_{2|1}^I(\varphi_L^*)$:

$$\begin{aligned}\alpha_{2|1}(\Phi_N^*) &= P_{MK}^N\left(\mathcal{B}_2^N\right)\\ &= P_{MK}^N\left(\bigcup_{Q_{\mathbf{m},\mathbf{k}}:D(Q_{\mathbf{m},\mathbf{k}}||P_{MK})>E_{2|1}^{II}} \mathcal{T}_{Q_{\mathbf{m},\mathbf{k}}}^N(M,K)\right)\end{aligned}$$

$$\begin{aligned}
&\leq (N+1)^{|\mathcal{M}||\mathcal{K}|} \sup_{Q_{\mathbf{m},\mathbf{k}}:D(Q_{\mathbf{m},\mathbf{k}}||P_{MK})>E^{II}_{2|1}} P^N_{MK}\left(\mathcal{T}^N_{Q_{\mathbf{m},\mathbf{k}}}(M,K)\right)\\
&= (N+1)^{|\mathcal{M}||\mathcal{K}|} \sup_{Q_{\mathbf{m},\mathbf{k}}:D(Q_{\mathbf{m},\mathbf{k}}||P_{MK})>E^{II}_{2|1}} \exp\Big\{-ND(Q_{\mathbf{m},\mathbf{k}}||P_{MK})\Big\}\\
&\leq \exp\left\{-N\left[E^{II}_{2|1}-o_N(1)\right]\right\},
\end{aligned}$$

where $o_N(1) \to 0$ when $N \to \infty$.

Now let us consider the second kind error probability. Using (2), (4) and (18) we can find the lower and the upper bounds of the second kind error probability $\alpha_{1|2}(\Phi^*_N)$.

The following inequality gives the upper bound:

$$\begin{aligned}
\alpha_{1|2}(\Phi^*_N) &= P^N_M P^N_K\left(\mathcal{B}^N_1\right)\\
&= P_M P_K\left(\bigcup_{Q_{\mathbf{m},\mathbf{k}}:D(Q_{\mathbf{m},\mathbf{k}}||P_{MK})\leq E^{II}_{2|1}} \mathcal{T}^N_{Q_{\mathbf{m},\mathbf{k}}}(M,K)\right)\\
&\leq (N+1)^{|\mathcal{M}||\mathcal{K}|} \sup_{Q_{\mathbf{m},\mathbf{k}}:D(Q_{\mathbf{m},\mathbf{k}}||P_{MK})\leq E^{II}_{2|1}} P_M P_K\left(\mathcal{T}^N_{Q_{\mathbf{m},\mathbf{k}}}(M,K)\right) \qquad (20)\\
&\leq \exp\left\{-N\left[\inf_{Q_{\mathbf{m},\mathbf{k}}:\ D(Q_{\mathbf{m},\mathbf{k}}||P_{MK})\leq E^{II}_{2|1}} D(Q_{\mathbf{m},\mathbf{k}}||P_M P_K)-o_N(1)\right]\right\}.
\end{aligned}$$

The lower bound is:

$$\begin{aligned}
\alpha_{1|2}(\Phi^*_N) &= P^N_{MK}\left(\mathcal{B}^N_1\right)\\
&= P_M P_K\left(\bigcup_{Q_{\mathbf{m},\mathbf{k}}:D(Q_{\mathbf{m},\mathbf{k}}||P_{MK})\leq E^{II}_{2|1}} \mathcal{T}^N_{Q_{\mathbf{m},\mathbf{k}}}(M,K)\right)\\
&\geq \sup_{Q_{\mathbf{m},\mathbf{k}}:D(Q_{\mathbf{m},\mathbf{k}}||P_{MK})\leq E^{II}_{2|1}} P_M P_K\left(\mathcal{T}^N_{Q_{\mathbf{m},\mathbf{k}}}(M,K)\right) \qquad (21)\\
&\geq (N+1)^{-|\mathcal{M}||\mathcal{K}|} \sup_{Q_{\mathbf{m},\mathbf{k}}:D(Q_{\mathbf{m},\mathbf{k}}||P_{MK})\leq E_{2|1}} \exp\{-ND(Q_{\mathbf{m},\mathbf{k}}||P_{MK})\\
&\geq \exp\left\{-N\left[\inf_{Q_{\mathbf{m},\mathbf{k}}:\ D(Q_{\mathbf{m},\mathbf{k}}||P_{MK})\leq E^{II}_{2|1}} D(Q_{\mathbf{m},\mathbf{k}}||P_M P_K)+o_N(1)\right]\right\}.
\end{aligned}$$

According to (20), (21), the definition of reliability and the continuity of the divergence function we get

$$E_{1|2}^{II}(\Phi_N^*) \overset{\triangle}{=} E_{1|2}^{*,II} = \inf_{Q:\ D(Q||P_{MK}) \leq E_{2|1}^{II}} D(Q||P_M P_K).$$

The proof of the optimality of the test Φ^* is similar to the proof of Theorem 1. The theorem is proved.

Acknowledgements

The work was supported by the Science Committee of RA, in the frames of the research project № 21T-1B151.

References

[Alomair and Poovendran 2009] Alomair, B, Poovendran, R: "Information theoretically secure encryption with almost free authentication"; JUCS - Journal of Universal Computer Science, 15, 15 (2009), 2937-2956. https://doi.org/10.3217/jucs-015-15-2937

[Augot et al. 2011] Augot, D., Barbier, M., Fontaine, C.: "Ensuring message embedding in wet paper steganography"; Cryptography and Coding, IMACC 2011, Lecture Notes in Computer Science, 7089, Springer, Berlin, Heidelberg, (2011), 244-258. https://doi.org/10.1007/978-3-642-25516-8_15

[Backes and Cachin 2005] Backes, M., Cachin, C.: "Public-key steganography with active attacks"; Lecture Notes in Computer Science, 3378, Springer-Verlag, (2005), 210-226. https://doi.org/10.1007/978-3-540-30576-7_12

[Balado and Haughton 2018] Balado, F., Haughton, D.: "Asymptotically optimum perfect universal steganography of finite memoryless sources"; IEEE Transactions on Information Theory, 64, 2 (2018), 1199-1216. https://doi.org/10.1109/TIT.2017.2783539

[Blahut 1974] Blahut, R,: "Hypothesis testing and information theory"; IEEE Transactions on Information Theory, 20, 4 (1974), 405–417. https://doi.org/10.1109/TIT.1974.1055254

[Blahut 1987] Blahut, R.: "Principles and Practice of Information Theory"; Addison-Wesley, Reading, MA (1987).

[Birgé 1981] Birgé, L.: "Vitesses maximales de décroissance des erreurs et tests optimaux associés"; Z. Wahrsch. verw. Gebiete, 55, (1981), 261–273.

[Cachin et al. 1998] Cachin, C.: "An information-theoretic model for steganography"; Proc. Workshop on Information Hiding, Lecture Notes in Computer Science, 1525, Springer-Verlag, (1998), 306-318. https://doi.org/10.1007/3-540-49380-8_21

[Cachin 2004] Cachin, C.: "An information-theoretic model for steganography"; Information and Computation, 192, (2004), 41–56. https://doi.org/10.1016/j.ic.2004.02.003

[Csiszár 1998] Csiszár, I.: "Method of types"; IEEE Transactions on Information Theory, 44, 6 (1998), 2505–-2523. https://doi.org/10.1109/18.720546

[Csiszár and Körner 1981] Csiszár, I., Körner, J.: "Information Theory: Coding Theorems for Discrete Memoryless Systems"; Academic Press, New York (1981).

[Csiszár and Longo 1971] Csiszár, I., Longo, G.: "On the error exponent for source coding and for testing simple statistical hypotheses"; Studia Sc. Math. Hungarica, 6, (1971), 181–191.

[Cover and Thomas 2006] Cover, T., Thomas, J.: "Elements of Information Theory"; Second Edition, Wiley, New York (2006).

[Dedic et al. 2009] Dedic, N., Itkis, G., Reyzin, L., Russell, S.: "Upper and lower bounds on black box steganography"; Journal of Cryptology, 22, 3 (2009), 365-394. https://doi.org/10.1007/s00145-008-9020-3

[Grigoryan and Harutyunyan 2015] Grigoryan, N., Harutyunyan, A.: "Multiple hypothesis testing for arbitrarily varying sources"; Communications in Information and Systems, 15, 3 (2015), 309–330. https://doi.org/10.4310/CIS.2015.v15.n3.a1

[Grigoryan et al. 2011] Grigoryan, N., Harutyunyan, A., Voloshynovskiy, S., Koval, O.: "On multiple hypothesis testing with rejection option"; Proc. IEEE Information Theory Workshop, Paraty, Brazil, (Oct 2011). doi: 10.1109/ITW.2011.6089531.

[Haroutunian 1989] Haroutunian, E.: "On asymptotically optimal criteria for Markov chains"; The First World Congress of Bernoulli Society, (in Russian) 2, 3 (1989), 153–156.

[Haroutunian 1990] Haroutunian, E.: "Logarithmically asymptotically optimal testing of multiple statistical hypotheses"; Problems of Control and Information Theory, 19, 5-6 (1990), 413–421.

[Harutyunyan et al. 2011] Harutyunyan, A., Grigoryan, N., Voloshynovskiy, S., Koval, O.: "A new biometric identification model and the multiple hypothesis testing for arbitrarily varying objects"; Proc. Special Interest Group on Biometrics and Electronic Signatures (BIOSIG2011), Darmstadt, Germany, (Sep 2011), 305–312.

[Haroutunian et al. 2008] Haroutunian, E., Haroutunian, M., Harutyunyan, A.:"Reliability Criteria in Information Theory and in Statistical Hypothesis Testing"; Foundations and Trends in Communications and Information Theory, 4, 2-3 (2008). doi: 10.1561/0100000008

[Haroutunian et al. 2022] Haroutunian, M., Hakobyan, P., Harutyunyan, A., Avetisyan, A.: "Information-theoretic investigation of authenticated steganographic Model in the presence of active adversary"; CODASSCA Intern. Workshop, (2022), 1-7. https://doi.org/10.30819/5520

[Haroutunian et al. 2018] Haroutunian, M., Haroutunian, E., Hakobyan, P., Mikayelyan, H.: "Logarithmically asymptotically optimal testing of statistical hypotheses in steganography applications"; CODASSCA Intern. Workshop, (2018), 157–163.

[Harutyunyan and Han Vinck 2006] Harutyunyan, A., Han Vinck, A. J.: "Error exponent in AVS coding"; Proc. IEEE International Symposium on Information Theory, Seattle, WA, 2 (July 2006), 166-2170. doi:10.1109/ISIT.2006.261934

[Hoeffding 1965] Hoeffding, W.: "Asymptotically optimal tests for multinomial distributions"; The Annals of Mathematical Statistics, 36, (1965), 369–401. doi: 10.1214/aoms/1177700150

[Hopper et al. 2002] Hopper, N., Langford, J., von Ahn, L.: "Provably secure steganography"; Lecture Notes in Computer Science, 2442, Springer-Verlag, (2002), 18-22. https://doi.org/10.1007/3-540-45708-9_6

[Katzenbeisser et al. 2002] Katzenbeisser, S., Petitcolas, F. A. P.: "Defining security in steganographic systems"; Security and Watermarking of Multimedia Contents IV, 4675, (2002), 50-56. https://doi.org/10.1117/12.465313

[Liśkiewicz et al. 2011] Liśkiewicz, M., Reischuk, R., Wölfel, U.: "Grey-box steganography"; Theory and Applications of Models of Computation. TAMC 2011. Lecture Notes in Computer Science, 6648, Springer, Berlin, Heidelberg (2011), 390-402. https://doi.org/10.1007/978-3-642-20877-5_38

[Longo and Sgarro 1980] Longo, G., Sgarro, A.: "The error exponent for the testing of simple statistical hypotheses: A combinatorial approach"; Journal of Combinatorics, Information and System Sciences, 5, 1 (1980), 58-67.

[Maurer 2000] Maurer, U.: "Authentication theory and hypothesis testing"; IEEE Transactions on Information Theory, 46, 4 (2000), 1350–1356. doi: 10.1109/18.850674.

[Mittelholzer 2000] Mittelholzer, T.: "An information-theoretic approach to steganography and watermarking"; Proc. Workshop on Information Hiding, Lecture Notes in Computer Science, 1768, Springer-Verlag (2000), 1-16. https://doi.org/10.1007/10719724_1

[Moulin and O'Sullivan 2003] Moulin, P., O'Sullivan, J. A.: "Information theoretic analysis of information hiding"; IEEE Transactions on Information Theory, 49, 3 (2003), 563-593. doi: 10.1109/TIT.2002.808134.

[O'Sullivan et al. 1998] O'Sullivan, J. A., Moulin, P., Ettinger, J. M.: "Information theoretic analysis of steganography"; Proc. IEEE Intern. Symposium on Information Theory, 297 (1998). doi: 10.1109/ISIT.1998.708902.

[Pfitzmann 1996] Pfitzmann, B.: "Information hiding terminology"; Information Hiding, First International Workshop, Lecture Notes in Computer Science 1174, Springer (1996), 347–350. https://doi.org/10.1007/3-540-61996-8_52

[Shikata and Matsumoto 2008] Shikata, J., Matsumoto, T.: "Unconditionally secure steganography against active attacks"; IEEE Transactions on Information Theory, 54, 6 (June 2008), 2690–2705. doi: 10.1109/TIT.2008.921884.

[Tusnady 1977] Tusnady, G.: "On asymptotically optimal tests"; Ann. of Statist, 5, 2 (1977), 385-393. https://doi.org/10.1214/aos/1176343804

[Von Ahn and Hopper 2004] Von Ahn, L., Hopper, N.: "Public-key steganography"; Lecture Notes in Computer Science 3027, Springer-Verlag (2004), 323-341. https://doi.org/10.1007/978-3-540-24676-3_20

[Wang and Moulin 2008] Wang, Y., Moulin, P.: "Perfectly secure steganography: capacity, error exponents, and code constructions"; IEEE Transactions on Information Theory, 54, 6 (2008), 2706-2722. https://doi.org/10.1109/TIT.2008.921684

[Willems et al 2003] Willems, F., Kalker, T., Goseling, J., and Linnartz, J.-P.: "On the capacity of a biometrical identification system"; Proc. IEEE International Symposium on Information Theory, Yokohama, Japan (July 2003). doi: 10.1109/ISIT.2003.1228096.

[Yagi and Hirasawa 2022] Yagi, H., Hirasawa, Sh.: "Performance analysis for biometric identification systems with nonlegitimate users"; Proc. 2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Prague, Check Republic (Oct 2022), 3060-3065. doi: 10.1109/SMC53654.2022.9945401.