Yuriy S. Kharin and Egor V. Vecherko

Detection of embeddings in binary Markov chains

DOI: 10.1515/dma-2016-0002
Received March 31, 2015

Abstract: The paper is concerned with problems in steganography on the detection of embeddings and statistical estimation of positions at which message bits are embedded. Binary stationary Markov chains with known or unknown matrices of transition probabilities are used as mathematical models of cover sequences (container files). Based on the runs statistics and the likelihood ratio statistic, statistical tests are constructed for detecting the presence of embeddings. For a family of contiguous alternatives, the asymptotic power of statistical tests based on the runs statistics is found. An algorithm of polynomial complexity is developed for the statistical estimation of positions with embedded bits. Results of computer experiments are presented.

Keywords: steganography, model of embeddings, Markov chain, statistical test, power, total number of runs

Note: Originally published in *Diskretnaya Matematika* (2015) **27**, №3, 123–144 (in Russian).

1 Introduction

The paper is concerned with a topical problem in steganographic information security—this is the problem of embedding detection, that is of the construction of statistical tests for the existence of embeddings and of statistical estimates of positions (points) of embeddings.

The problem of detection of embeddings was studied in [1, 2, 3, 4] under the assumption that the probabilistic model of a cover sequence is completely known. So, in [1] statistical tests were constructed for the embedding existence in the case when the initial (cover) sequence is modeled by a Bernoulli scheme of independent trials; it was also shown that the embedding detection is impossible if the fraction of the embeddings tends to 0 as the length of the initial sequence tends to ∞. A similar fact was proved in [3]. In [2] a most powerful statistical test for the embedding existence was constructed for the model based on a Bernoulli scheme of independent trials, and statistical estimates of the fraction of embeddings were put forward. Statistical estimates of the model parameters of the embedding in a binary Markov chain were constructed and examined in [5]; they allow to make preliminary conclusions on the fraction of embeddings. It is worth mentioning that the majority of studies on the detection of embeddings are based on empirical characteristics of sequences, which involve methods of discriminant analysis for testing the embedding existence. We also note that the above problems of recognition of embeddings are close to those on the detection of deviations of output sequences of cryptographic generators from uniformly distributed random sequences [6].

Our purpose in this paper is to continue the studies initiated in [5]: we construct and analyse statistical tests for the embedding existence, and to develop algorithms for the statistical estimation of embeddings points.

The paper is organized as follows. In § 2 we describe the mathematical (q, r)-block model of embedding in a binary Markov chain. In § 3 we construct statistical tests for the embedding existence based on the runs statistics and on the short runs statistics, and in § 4 we consider tests based on the likelihood ratio statistics. In § 5, we put forward an algorithm of polynomial complexity for statistical estimation. The results of numerical experiments are given in § 6.

Yuriy S. Kharin: Belarusian State University, e-mail: kharin@bsu.by
Egor V. Vecherko: Belarusian State University, e-mail: vecherko@bsu.by

2 Mathematical model of embedding

We define the generalized (q, r)-block model of embedding, a particular case of which was proposed by the authors of the present paper in [5]. Throughout, $(\Omega, F, \mathbf{P})$ is the underlying probability space, $V = \{0, 1\}$ is the binary alphabet, V_T is the space of binary T-dimensional vectors, $\mathcal{O}(\cdot)$ is the 'big O' notation introduced by Landau, $\mathbb{N}$ is the set of natural numbers, $I\{A\}$ is the indicator of an event A, $u_{t_1}^{t_2} = (u_{t_1}, \dots, u_{t_2}) \in V_{t_2-t_1+1}$ $(t_1, t_2 \in \mathbb{N}, t_1 \le t_2)$ is a binary string of $t_2 - t_1 + 1$ successive symbols of some sequence $\{u_t : t \in \mathbb{N}\}$, $w(\cdot)$ is the Hamming weight, $\mathfrak{L}\{\xi\}$ is the probability distribution of a random variable ξ, $\mathfrak{B}(\theta)$ denotes the Bernoulli distribution with parameter $\theta \in [0, 1]$: $\mathbf{P}\{\xi = 1\} = 1 - \mathbf{P}\{\xi = 0\} = \theta$, $\Phi(\cdot)$ is the distribution function for the standard normal law $\mathcal{N}(0, 1)$.

According to [5], an adequate model of the cover sequence for embedding a message is a binary sequence $x_1^T = (x_1, x_2, \dots, x_T) \in V_T$, $x_t \in V$, $t = 1, \dots, T$, of length T, which is a homogeneous first-order binary Markov chain with symmetric matrix of one-step transition probabilities P:

$$P = P(\varepsilon) = \frac{1}{2}\begin{pmatrix} 1+\varepsilon & 1-\varepsilon \\ 1-\varepsilon & 1+\varepsilon \end{pmatrix}, \ \mathbf{P}\{x_t \oplus x_{t+1}\} = \frac{1}{2}(1-\varepsilon), \ |\varepsilon| < 1. \tag{1}$$

Here, ε is the parameter of the model: the case $\varepsilon = 0$ corresponds to a scheme of independent trials which was examined in [1]. The case $\varepsilon > 0$ takes into account an attraction-type dependence, and the $\varepsilon < 0$, a repulsion-type dependence. We note that the Markov chain (1) satisfies the ergodicity conditions [7] and has the uniform stationary distribution $(1/2, 1/2)$. In what follows, we shall assume that the Markov chain (1) is stationary, and so its initial probability distribution agrees with the uniform distribution.

In practical applications [5] a message is subject to a cryptographic transformation before being embedded in the cover sequence, and hence we assume in what follows that a message $\xi_1^M = (\xi_1, \dots, \xi_M) \in V_M$, $M \le T$, is a sequence of M independent Bernoulli random variables:

$$\mathfrak{L}\{\xi_t\} = \mathfrak{B}(\theta_1), \ \mathbf{P}\{\xi_t = j\} = \theta_j, \ j \in V, \ \theta_1 = 1 - \theta_0, \ t = 1, \dots, M. \tag{2}$$

The stego-key $\gamma_1^T = (\gamma_1, \dots, \gamma_T) \in V_T$ specifies the points (time instants) at which the message bits ξ_1^M are embedded in the sequence x_1^T. We introduce a special (q, r)-block model of the stego-key γ_1^T $(q, r \in \mathbb{N}$, $r \le q)$, assuming that the length of the sequence x_1^T is a multiple of q: $T = Kq$.

Let $\zeta_k \in V$, $\mathfrak{L}\{\zeta_k\} = \mathfrak{B}(\delta)$, $k = 1, \dots, K$, be auxiliary independent random variables, which govern the choice of the blocks $\{x_{(k)} = x_{(k-1)q+1}^{kq}\}$ for embedding the message ξ_1^M: if $\zeta_k = 1$, then r successive bits of the message are embedded in r randomly chosen bits of the block $x_{(k)}$; if $\zeta_k = 0$ then no embedding in the block $x_{(k)}$ is performed; $G^{(q,r)} = \{g_1^{(q,r)}, \dots, g_{C_q^r}^{(q,r)}\} = \{u_1^q \in V_q : w(u_1^q) = r\}$ is the set consisting of C_q^r lexicographically ordered binary vectors of length q equipped with the Hamming weight r; $g_1, g_2, \dots$ are independent random variables, g_k has uniform probability distribution on the set $\{1, \dots, C_q^r\}$,

$$\mathbf{P}\{\gamma_{(k)} = g_i^{(q,r)} | \zeta_k = 1\} = \mathbf{P}\{g_k = i\} = \frac{1}{C_q^r}.$$

In the (q, r)-block model of embedding, the sequence γ_1^T consists of blocks of length q: $\gamma_{(1)} = \gamma_1^q, \gamma_{(2)} = \gamma_{q+1}^{2q}, \dots, \gamma_{(K)} = \gamma_{(K-1)q+1}^{Kq}$,

$$\gamma_{(k)} = \begin{cases} (\underbrace{0, \dots, 0}_{q}), & \zeta_k = 0, \\ g_i^{(q,r)} \in G^{(q,r)}, & \zeta_k = 1, \ g_k = i, \end{cases} \quad k = 1, \dots, T/q, \tag{3}$$

the parameter δ characterizes the fraction of embeddings. We note that for the (q, r)-block model of embedding the maximum capacity for the stego system is Tr/q bits, while the cardinality of the set of all possible stego-keys

$$I^{(q,r)} = \{G^{(q,r)} \cup \{(0, \dots, 0)\}\}^{T/q}$$

is $|\Gamma^{(q,r)}| = (1 + C_q^r)^{T/q}$. In the case $q = r = 1$, we have the classical model [5] of a bit-wise embedding, $|\Gamma^{(1,1)}| = 2^T$.

For the most commonly encountered in steganography methods of embedding (the 'LSB replacement' and the '± embedding' [8]) the random stego-sequence $Y_1^T = (Y_1, \dots, Y_T)$ is generated by the sequences $\{x_t\}$, $\{\xi_t\}$, $\{\gamma_t\}$ via the function transform

$$Y_t = x_t \oplus \gamma_t x_t \oplus \gamma_t \xi_{\tau_t} = \begin{cases} x_t, & \gamma_t = 0, \\ \xi_{\tau_t}, & \gamma_t = 1, \end{cases} \tag{4}$$

where $\tau_t = \sum_{j=1}^t \gamma_j$. The sequences $\{x_t\}$, $\{\xi_t\}$, $\{\gamma_t\}$ are assumed to be jointly independent.

We note that for $r = 1$ the model presented here coincides with the q-block model considered in [5].

From the practical point of view, the case with $\theta_0 = \theta_1 = 1/2$ in (2), which presents the greatest challenge for embedding detection, is the most noteworthy in the framework of the Markov model of embedding (1)–(4). In this case the one-dimensional distribution of probabilities is not distorted for an embedding in (4),

$$\mathbf{P}\{Y_t = 1\} = \mathbf{P}\{Y_t = 0\} = \mathbf{P}\{x_t = 1\} = \mathbf{P}\{x_t = 0\} = 1/2, \quad t = 1, 2, \dots, T. \tag{5}$$

Another justification of the relevance of the case considered in the present paper is the practical utilization of preliminary cryptographic transformation of a message that removes the nonuniformity in the probability distribution of symbols.

3 Embedding detection based on the runs statistics

3.1 Using the total number of runs statistics

We introduce two hypotheses concerning the fraction $\delta \in [0, 1]$ of embeddings:

$$H_0 : \{\delta = 0\}, \; H_1 : \{\delta > 0\}. \tag{6}$$

The hypothesis H_0 means that there are no embeddings and the stego-sequence Y_1^T agrees with the cover sequence x_1^T. The composite alternative H_1 means there exist embeddings with some unknown fraction $\delta > 0$. If the parameter of the cover sequence ε is known, then the null hypothesis, which will be denoted by $H_{0,\varepsilon}$, is simple; otherwise, H_0 is also a composite hypothesis. If the hypothesis H_0 holds, then the probability measure $\mathbf{P}$ will be denoted by $\mathbf{P}_0$, otherwise, by $\mathbf{P}_\delta$. One similarly denotes the moments of random variables. The distributions $\mathbf{P}_0$ and $\mathbf{P}_\delta$ were found in [5].

Lemma 1. *Under the hypothesis $H_{0,\varepsilon}$, the probability distribution of the stego-sequence Y_1^T is as follows*

$$\mathbf{P}_0\{Y_1^T = y_1^T\} = \mathbf{P}_0\{x_1^T = y_1^T\} = 2^{-T}(1 - \varepsilon)^{B_T - 1}(1 + \varepsilon)^{T - B_T},$$

where

$$B_T = B_T(y_1^T) = 1 + \sum_{t=1}^{T-1} y_t \oplus y_{t+1}$$

is the minimal sufficient statistics with $H_{0,\varepsilon}$.

The statistics B_T is called the 'runs test' in [9] (it means the total number of runs). By virtue of (1), under the hypothesis H_0 the sequence of indicators $I\{Y_t \oplus Y_{t+1} = 1\}$ consists of independent random variables with Bernoulli distribution $\mathfrak{B}(2^{-1}(1 - \varepsilon))$. Using the exact binomial probability distribution of the statistics B_T with the known value of ε, one may construct a randomized statistical test for the embedding existence with the given probability of the first kind error α,. However, for practical purposes, it is more convenient to use its asymptotic variant as $T \to \infty$, which is given by the critical region

$$\begin{aligned} \mathscr{X}_{1\alpha}^{B+} &= \{y_1^T : B_T \geq 1 + \tfrac{1}{2}T(1 - \varepsilon) - \tfrac{1}{2}t_\alpha\sqrt{T(1 - \varepsilon^2)}\} \quad \text{for } \varepsilon > 0, \\ \mathscr{X}_{1\alpha}^{B-} &= \{y_1^T : B_T \leq 1 + \tfrac{1}{2}T(1 - \varepsilon) + \tfrac{1}{2}t_\alpha\sqrt{T(1 - \varepsilon^2)}\} \quad \text{for } \varepsilon < 0, \end{aligned} \tag{7}$$

where t_α is the α-quantile of the standard normal distribution: $\Phi(t_\alpha) = \alpha$.

Theorem 1. *Let the model of embedding* (4) *hold. Then as* $T \to \infty$ *the asymptotic size of test* (7) *for the hypotheses* $H_{0,\varepsilon}$, H_1 *based on the total number of runs statistics* B_T *coincides with a preassigned significance level* $\alpha \in (0,1)$. *The asymptotic expression for the power of this test in the case of the* $(1,1)$*-model of embedding and of the family of simple contiguous alternatives* $H_{1,\delta}: \{\delta = \dfrac{\rho}{T^\beta}\}$, $\beta > 0$, *is as follows:*

$$W_1^{B+} = W_1^{B-} \to \begin{cases} 1, & 0 < \beta < 1/2, \\ \Phi\left(t_\alpha + 2\rho\dfrac{|\varepsilon|}{\sqrt{1-\varepsilon^2}}\right), & \beta = 1/2, \\ \alpha, & \beta > 1/2. \end{cases} \tag{8}$$

Proof. Under the hypothesis H_0, the De Moivre–Laplace limit theorem implies that

$$\mathfrak{L}_0\left\{\frac{B_T - 1 - \frac{1}{2}T(1-\varepsilon)}{\frac{1}{2}\sqrt{T(1-\varepsilon^2)}}\right\} \to \mathcal{N}(0,1) \quad \text{as} \quad T \to \infty. \tag{9}$$

Hence, using (9) we have, as $T \to \infty$,

$$\mathbf{P}_0\{\mathscr{X}_{1\alpha}^{B+}\} \to \alpha, \qquad \mathbf{P}_0\{\mathscr{X}_{1\alpha}^{B-}\} \to \alpha.$$

In the case $q = r = 1$, under the alternative H_1, it follows from (1), (2), (4), (5) that the initial first moment of the random variable B_T is equal to

$$\mathbf{E}_\delta\{B_T\} = 1 + \sum_{t=1}^{T-1} \mathbf{E}_\delta\{Y_t \oplus Y_{t+1}\} = 1 + 2^{-1}(T-1)(1-(1-\delta)^2\varepsilon).$$

Using similar arguments, we calculate the initial second moment under the alternative H_1. We have

$$\begin{aligned}
\mathbf{E}_\delta\{B_T^2\} &= \mathbf{E}_\delta\left\{(1 + \sum_{t_1=1}^{T-1} Y_{t_1} \oplus Y_{t_1+1})(1 + \sum_{t_2=1}^{T-1} Y_{t_2} \oplus Y_{t_2+1})\right\} = \\
&= \mathbf{E}_\delta\left\{\sum_{t_1,t_2=1}^{T-1} (Y_{t_1} \oplus Y_{t_1+1})(Y_{t_2} \oplus Y_{t_2+1})\right\} + 2\mathbf{E}_\delta\{B_T\} - 1 = \\
&= 3\mathbf{E}_\delta\{B_T\} - 2 + 2\sum_{t=1}^{T-2}\sum_{h\in V} \mathbf{P}_\delta\{Y_t = h, Y_{t+1} = 1-h, Y_{t+2} = h\} + \\
&+ 2\sum_{\tau=2}^{T-2}\sum_{t=1}^{T-\tau-1}\sum_{h_1,h_2\in V} \mathbf{P}_\delta\{Y_t = h_1, Y_{t+1} = 1-h_1, Y_{t+\tau} = h_2, Y_{t+\tau} = 1-h_2\} = \\
&= 3\mathbf{E}_\delta\{B_T\} - 2 + 2^{-1}(T-2)(1+\varepsilon(\varepsilon-2)(1-\delta)^2) + \\
&+ 4\sum_{\tau=2}^{T-2}(T-\tau-1)\big(\mathbf{P}_\delta\{Y_t = 0, Y_{t+1} = 1, Y_{t+\tau} = 0, Y_{t+\tau+1} = 1\} + \\
&+ \mathbf{P}_\delta\{Y_t = 0, Y_{t+1} = 1, Y_{t+\tau} = 1, Y_{t+\tau+1} = 0\}\big) = \\
&= 1 + 2^{-1}3(T-1)(1-\varepsilon(1-\delta)^2) + 2^{-1}(T-2)(1+\varepsilon(\varepsilon-2)(1-\delta)^2) + \\
&+ 2^{-2}(T-2)(T-3)(1+\varepsilon(\varepsilon\delta^2 - 2\varepsilon\delta - 2 + \varepsilon)(1-\delta)^2).
\end{aligned}$$

For the variance, we have

$$\begin{aligned}
\mathbf{D}_\delta\{B_T\} &= \tfrac{1}{4}T(1-(1-\delta)^2\varepsilon^2(1-6\delta+3\delta^2)) - \tfrac{1}{4}(1-(1-\delta)^2\varepsilon^2(1-10\delta+5\delta^2)) = \\
&= T(\tfrac{1}{4}(1-(1-\delta)^2\varepsilon^2(1-6\delta+3\delta^2)))(1+o(1)), \qquad T \to \infty.
\end{aligned}$$

By the construction (4) the random sequence $\{Y_t\}$ satisfies the strong mixing property [10, 11], and hence the central limit theorem for weakly dependent random variables holds,

$$\mathfrak{L}_\delta\left\{\frac{B_T - 1 - \frac{1}{2}T(1-(1-\delta)^2\varepsilon)}{\sqrt{\mathbf{D}_\delta\{B_T\}}}\right\} \to \mathcal{N}(0,1). \tag{10}$$

In the case $\varepsilon > 0$, we take into account (10) and substitute $\delta = \dfrac{\rho}{T^\beta}$ as $T \to \infty$ into the expression for the power. As a result, we have

$$\begin{aligned}\lim W_1^{B+} &= \lim \mathbf{P}_\delta\{\mathscr{X}_{1\alpha}^{B+}\} = \lim \mathbf{P}_\delta\{B_T \geq 1 + \tfrac{1}{2}T(1-\varepsilon) - \tfrac{1}{2}t_\alpha\sqrt{T(1-\varepsilon^2)}\} = \\ &= \lim \mathbf{P}_\delta\left\{\frac{B_T - \mathbf{E}_\delta\{B_T\}}{\sqrt{\mathbf{D}_\delta\{B_T\}}} \geq \frac{1 + \frac{1}{2}T(1-\varepsilon) - \mathbf{E}_\delta\{B_T\} - \frac{1}{2}t_\alpha\sqrt{T(1-\varepsilon^2)}}{\sqrt{\mathbf{D}_\delta\{B_T\}}}\right\} = \\ &= \Phi\left(\lim \frac{T\varepsilon\delta(2-\delta) + t_\alpha\sqrt{T(1-\varepsilon^2)}}{\sqrt{T(1-(1-\delta)^2\varepsilon^2(1-6\delta+3\delta^2))}}\right).\end{aligned}$$

Analyzing various values of β in this expression, we arrive at (8). The case $\varepsilon < 0$ is dealt with similarly. □

3.2 Using the short runs statistics

Let us construct the sequence of indicators of sign changes in the sequence $Y_1, \ldots, Y_T \in V_T$:

$$z_t = Y_t \oplus Y_{t+1} \in V,\ t = 1, \ldots, T-1. \tag{11}$$

Next, we define the set of patterns in sequence (11):

$$\{\mathfrak{b}_1, \mathfrak{b}_2, \ldots\},\ \mathfrak{b}_\tau = (1, \underbrace{0, \ldots, 0}_{\tau}, 1),\ \tau \in \mathbb{N} \cup \{0\};$$

here $\mathfrak{b}_\tau$ is the chain of τ successive 0's bounded from the left and right by 1's. Such patterns specify series of 0's and 1's of length $\tau + 1$ in the stego-sequence $\{Y_t\}$. Further, we consider the disjoint random events $\mathfrak{C}_\tau$, $\tau \in \mathbb{N} \cup \{0\}$:

$$\mathfrak{C}_\tau = \{(z_t, z_{t+1}, \ldots, z_{t+\tau+1}) = \mathfrak{b}_\tau\}.$$

Lemma 2. *Let the model of embedding* (4) *hold,* $q = r = 1$. *Then under the alternative* H_1 *the probability distribution of the random events* $\mathfrak{C}_\tau$ *is given by*

$$\mathbf{P}_\delta\{\mathfrak{C}_\tau\} = \mathbf{P}_0\{\mathfrak{C}_\tau\} + \mathfrak{a}_\tau(\delta,\varepsilon) = 2^{-(\tau+2)}(1+\varepsilon)^\tau(1-\varepsilon)^2 + \mathfrak{a}_\tau(\delta,\varepsilon), \tag{12}$$

where $\mathfrak{a}_\tau(\delta,\varepsilon) \to 0$ *as* $\delta \to 0$, $|\varepsilon| < 1$.

Proof. Using the law of total probability for the model of embedding under consideration we find that

$$\begin{aligned}\mathbf{P}_\delta\{\mathfrak{C}_\tau\} &= \sum_{u_1^{\tau+2} \in V_{\tau+2}} \mathbf{P}_\delta\{\gamma_t^{t+\tau+1} = u_1^{\tau+2}\}\mathbf{P}_\delta\{(z_t, z_{t+1}, \ldots, z_{t+\tau+1}) = \mathfrak{b}_\tau | \gamma_t^{t+\tau+1} = u_1^{\tau+2}\} = \\ &= (1-\delta)^{\tau+2}\mathbf{P}_0\{\mathfrak{C}_\tau\} + \delta \sum_{u_1^{\tau+2} \in V_{\tau+2}:\ w(u_1^{\tau+2})>0} \delta^{w(u_1^{\tau+2})-1}(1-\delta)^{\tau+2-w(u_1^{\tau+2})} \times \\ &\times \mathbf{P}_\delta\{(z_t, z_{t+1}, \ldots, z_{t+\tau+1}) = \mathfrak{b}_\tau | \gamma_t^{t+\tau+1} = u_1^{\tau+2}\} \xrightarrow[\delta\to 0]{} 2^{-(\tau+2)}(1+\varepsilon)^\tau(1-\varepsilon)^2.\end{aligned}$$

□

Theorem 2. *Under the hypotheses of Lemma 2, the function* $\mathfrak{a}_\tau(\delta,\varepsilon)$ *has the asymptotic expansion*

$$\begin{gathered}\mathfrak{a}_\tau = \delta\mathfrak{a}_\tau^{(1)}(\varepsilon) + \mathcal{O}\left(\delta^2\right), \\ \mathfrak{a}_\tau^{(1)}(\varepsilon) = \begin{cases} 2^{-1}\varepsilon(2-\varepsilon), & \tau = 0, \\ 2^{-2}\varepsilon(1-\varepsilon)(1+\varepsilon), & \tau = 1, \\ 2^{-\tau-1}\varepsilon(1-\varepsilon)(1+\varepsilon)^{\tau-2}(\varepsilon^2 + (\tau+1)\varepsilon - \tau + 2), & \tau \geq 2. \end{cases}\end{gathered} \tag{13}$$

Proof. We partition the set $\mathfrak{U}_{\tau+2,1} = \{u_1^{\tau+2} = (u_1, \dots, u_{\tau+2}) \in V_{\tau+2}\colon w(u_1^{\tau+2}) = 1\}$, $|\mathfrak{U}| = \tau + 2$, of binary vectors of length $\tau + 2$, $\tau \geq 3$, with unit Hamming weight into three disjoint subsets:

$$\begin{aligned}
\mathfrak{U}_{\tau+2,1} =& \mathfrak{U}^{(0)}_{\tau+2,1} \cup \mathfrak{U}^{(1)}_{\tau+2,1} \cup \mathfrak{U}^{(2)}_{\tau+2,1},\\
\mathfrak{U}^{(j)}_{\tau+2,1} =& \{u_1^{\tau+2} \in \mathfrak{U}_{\tau+2,1} : \ u_{j+1} + u_{\tau+2-j} = 1\}, \ j \in \{0,1\},\\
\mathfrak{U}^{(2)}_{\tau+2,1} =& \{u_1^{\tau+2} \in \mathfrak{U}_{\tau+2,1} : \ \sum\nolimits_{j=3}^{\tau} u_j = 1\}.
\end{aligned}$$

Arguing as in the proof of Lemma 2, we have

$$\begin{aligned}
&\mathbf{P}_\delta\{\mathfrak{C}_\tau\} = \mathbf{P}_0\{\mathfrak{C}_\tau\} - \delta(\tau+2)\mathbf{P}_0\{\mathfrak{C}_\tau\} +\\
&+\delta \sum_{j\in\{0,1,2\}} \sum_{u_1^{\tau+2}\in\mathfrak{U}^{(j)}_{\tau+2,1}} \mathbf{P}_\delta\{(z_t, z_{t+1}, \dots, z_{t+\tau+1}) = \mathfrak{b}_\tau | \gamma_t^{t+\tau+1} = u_1^{\tau+2}\} + \mathcal{O}\left(\delta^2\right).
\end{aligned} \tag{14}$$

Let us consider the case $\tau \geq 2$. The subset $\mathfrak{U}^{(j)}_{\tau+2,1}$, $j \in \{0,1,2\}$, contains sequences $u_1^{\tau+2} \in \mathfrak{U}_{\tau+2,1}$ such that the events $\mathfrak{C}_\tau \cap \{\gamma_t^{t+\tau+1} = u_1^{\tau+2}\}$ are equiprobable under the alternative H_1:

$$\begin{aligned}
&\mathbf{P}_\delta\{\mathfrak{C}_\tau \cap \{\gamma_t^{t+\tau+1} = u_1^{\tau+2}\}\} =\\
&= \begin{cases}
\delta(1-\delta)^{\tau+2}2^{-\tau-3}(1-\varepsilon)(1+\varepsilon)^\tau, & u_1^{\tau+2} \in \mathfrak{U}^{(0)}_{\tau+2,1},\\
\delta(1-\delta)^{\tau+2}2^{-\tau-3}(1-\varepsilon)^2(1+\varepsilon)^\tau, & u_1^{\tau+2} \in \mathfrak{U}^{(1)}_{\tau+2,1},\\
\delta(1-\delta)^{\tau+2}2^{-\tau-3}(1-\varepsilon)^2(1+\varepsilon^2)(1+\varepsilon)^{\tau-2}, & u_1^{\tau+2} \in \mathfrak{U}^{(2)}_{\tau+2,1}.
\end{cases}
\end{aligned} \tag{15}$$

Now (13) with $\tau \geq 2$ follows by substitution of (15) into (14). The case $\tau < 2$ in (13) is considered similarly. □

Theorem 3. *Under the hypotheses of Lemma 2, the function $\mathfrak{a}_\tau(\delta, \varepsilon)$ has the second-order asymptotic expansion*

$$\mathfrak{a}_\tau = \delta\mathfrak{a}^{(1)}_\tau(\varepsilon) + \delta^2\mathfrak{a}^{(2)}_\tau(\varepsilon) + \mathcal{O}\left(\delta^3\right),$$

where

$$\begin{aligned}
&\mathfrak{a}^{(2)}_0(\varepsilon) = 2^{-2}\varepsilon(-2+\varepsilon), \ \mathfrak{a}^{(2)}_1(\varepsilon) = 2^{-3}\varepsilon(-1+4\varepsilon+\varepsilon^2),\\
&\mathfrak{a}^{(2)}_2(\varepsilon) = 2^{-4}\varepsilon^2(-7+10\varepsilon+\varepsilon^2), \ \mathfrak{a}^{(2)}_3(\varepsilon) = 2^{-5}\varepsilon(1-12\varepsilon+2\varepsilon^2+16\varepsilon^3+\varepsilon^4),\\
&\mathfrak{a}^{(2)}_\tau(\varepsilon) = 2^{-\tau-2}\varepsilon(1+\varepsilon)^{\tau-4}(\tau-2+\varepsilon(2\tau^2-14\tau+13)+2\varepsilon^2(-2\tau^2+7\tau-8)+\\
&\qquad + 2\varepsilon^3(\tau^2-3\tau+9) + \varepsilon^4(5\tau+2) + \varepsilon^5), \ \tau \geq 4.
\end{aligned} \tag{16}$$

The proof is similar to that of Theorem 2, the set of stego-keys $\mathfrak{U}_{\tau+2,2}$ being split into classes of equiprobable events.

From Theorems 2, 3 it follows that under the alternative H_1 (existence of embeddings) the probability distribution of the total number of runs of a given length differs from that distribution under the hypothesis H_0. In particular, for $\varepsilon > 0$ the probabilities of the events $\mathfrak{C}_0, \mathfrak{C}_1, \mathfrak{C}_2$ increase as δ increases from 0 to 1, whereas for $\tau > \tau_\varepsilon = 2 + \varepsilon(3+\varepsilon)(1-\varepsilon)^{-1}$ the probability $\mathbf{P}_\delta\{\mathfrak{C}_\tau\}$ decreases with the increasing of δ. This being so, we consider the statistics

$$\mathcal{B}_{T,1} = \sum_{t=1}^{T-2} z_t, \ \mathcal{B}_{T,2} = \sum_{t=1}^{T-2} z_t z_{t+1}, \tag{17}$$

where the statistics $\mathcal{B}_{T,2}$ is the total number of series of 0's and of 1's of length 1 in the sequence $\{y_t\}$, and the statistics $\mathcal{B}_{T,1}$ is related to the total number of runs statistics B_T by the relation $\mathcal{B}_{T,1} = B_T - z_{T-1} - 1$.

Using Theorem 1 from [5] one may show that under the alternative H_1 the initial first-order moments of the bivariate statistics $(\mathcal{B}_{T,1}, \mathcal{B}_{T,2})$, as given by (17), read as

$$\begin{aligned}
\mathbf{E}_\delta\{\mathcal{B}_{T,1}\} &= (T-2)\tfrac{1}{2}(1-(1-\delta)^2\varepsilon) = \mathbf{E}_0\{\mathcal{B}_{T,1}\} + T\tfrac{1}{2}\delta(2-\delta)\varepsilon + o(T), \ T \to \infty,\\
\mathbf{E}_\delta\{\mathcal{B}_{T,2}\} &= (T-2)\tfrac{1}{4}(1-(1-\delta)^2\varepsilon(2-\varepsilon)) = \mathbf{E}_0\{\mathcal{B}_{T,2}\} + T\tfrac{1}{4}\delta(2-\delta)\varepsilon(2-\varepsilon) + o(T), \ T \to \infty.
\end{aligned} \tag{18}$$

From (18) it is seen that for $\varepsilon > 0$ the mean number of sign changes or of two neighbouring sign changes is larger when the embeddings exist than in the opposite case.

Theorem 4. *Let the model of embedding* (4) *holds. Then, as* $T \to \infty$, *the statistical test for the hypotheses* $H_{0,\varepsilon}$, H_1 *of the asymptotic significance level* $\alpha \in (0,1)$ *based on the bivariate statistics (17) is given by the critical region*

$$\mathscr{X}_{1\alpha}^{\mathcal{B}_{1,2}} = \{y_1^T : (\mathcal{B}_{T,1}, \mathcal{B}_{T,2}) \in \mathcal{D}_{1,2}\}, \tag{19}$$

where the region $\mathcal{D}_{1,2}$ *is as follows*

$$\begin{gathered}\mathcal{D}_{1,2} = \left\{(\mathcal{B}_{T,1}, \mathcal{B}_{T,2}) : (\mathcal{B}_{T,1} - T\mu_{0,1})\varepsilon \geq 0,\ (\mathcal{B}_{T,2} - T\mu_{0,1}^2)\varepsilon \geq 0,\right. \\ \left.\begin{pmatrix} \mathcal{B}_{T,1} - \mu_{0,1} \\ \mathcal{B}_{T,2} - \mu_{0,1}^2 \end{pmatrix}' \begin{pmatrix} \frac{(5-3\varepsilon)(1-\varepsilon)}{16} & -\frac{1-\varepsilon}{4} \\ -\frac{1-\varepsilon}{4} & \frac{1}{4} \end{pmatrix} \begin{pmatrix} \mathcal{B}_{T,1} - \mu_{0,1} \\ \mathcal{B}_{T,2} - \mu_{0,1}^2 \end{pmatrix} \geq Tc_{1,2}\right\}, \\ \mu_{0,1} = \tfrac{1}{2}(1-\varepsilon),\ c_{1,2} = 2^{-5}(1-\varepsilon^2)^2 \ln \frac{\pi - \arccos\left(2\sqrt{\frac{1-\varepsilon}{5-3\varepsilon}}\right)}{2\pi\alpha},\end{gathered} \tag{20}$$

that is,

$$\mathbf{P}_0\{\mathscr{X}_{1\alpha}^{\mathcal{B}_{1,2}}\} = \mathbf{P}_0\{(\mathcal{B}_{T,1}, \mathcal{B}_{T,2}) \in \mathcal{D}_{1,2}\} \to \alpha.$$

Proof. Using the fact that under the hypothesis $H_{0,\varepsilon}$ the random variables $\{z_t\}$ are independent and have the Bernoulli distribution $\mathfrak{B}(2^{-1}(1-\varepsilon))$, and since the random variables $z_t z_{t+1}$ and $z_s z_{s+1}$ are independent if $|t-s| > 1$, we find that

$$\begin{gathered}\mathbf{E}_0\{\mathcal{B}_{T,1}\} = T\tfrac{1}{2}(1-\varepsilon)(1+o(1)),\ \mathbf{E}_0\{\mathcal{B}_{T,2}\} = T\tfrac{1}{4}(1-\varepsilon)^2(1+o(1)), \\ \mathbf{D}_0\{\mathcal{B}_{T,1}\} = (T-2)\mathbf{D}_0\{z_t\} = T\tfrac{1}{4}(1-\varepsilon^2)(1+o(1)), \\ \mathbf{D}_0\{\mathcal{B}_{T,2}\} = (T-2)\mathbf{D}_0\{z_t z_{t+1}\} + 2\sum_{1\leq t<s\leq T-2} \operatorname{cov}_0\{z_t z_{t+1}, z_s z_{s+1}\} = \\ = (T-2)\mathbf{D}_0\{z_t z_{t+1}\} + 2(T-3)\operatorname{cov}_0\{z_t z_{t+1}, z_{t+1} z_{t+2}\} = \\ = (T-2)(\tfrac{1}{4}(1-\varepsilon)^2 - \tfrac{1}{16}(1-\varepsilon)^4) + 2(T-3)(\tfrac{1}{8}(1-\varepsilon)^3 - \tfrac{1}{16}(1-\varepsilon)^4) = \\ = T\tfrac{1}{16}(1-\varepsilon^2)(1-\varepsilon)(5-3\varepsilon)(1+o(1)), \\ \operatorname{cov}_0\{\mathcal{B}_{T,1}, \mathcal{B}_{T,2}\} = \sum_{t,s=1}^{T-2} \operatorname{cov}_0\{z_t, z_s z_{s+1}\} = \\ = (T-2)\operatorname{cov}_0\{z_t, z_t z_{t+1}\} + (T-3)\operatorname{cov}_0\{z_{t+1}, z_t z_{t+1}\} = \\ = (2T-6)(\tfrac{1}{4}(1-\varepsilon)^2 - \tfrac{1}{8}(1-\varepsilon)^3) = T\tfrac{1}{4}(1-\varepsilon^2)(1-\varepsilon) - \tfrac{3}{4}(1-\varepsilon^2)(1-\varepsilon) = \\ = T\tfrac{1}{4}(1-\varepsilon^2)(1-\varepsilon)(1+o(1)).\end{gathered}$$

Next, since the sequence of pairs $(z_t, z_t z_{t+1}) \in V_2$ is 1-dependent, it follows that as $T \to \infty$ the random vector $\frac{1}{\sqrt{T}}\left(\mathcal{B}_{T,1} - \frac{1}{2}T(1-\varepsilon), \mathcal{B}_{T,2} - \frac{1}{4}T(1-\varepsilon)^2\right)'$ has an asymptotic normal distribution $\mathcal{N}_2((0,0)', \Sigma_0)$, where

$$\Sigma_0 = (1-\varepsilon^2)\begin{pmatrix} \frac{1}{4} & \frac{1-\varepsilon}{4} \\ \frac{1-\varepsilon}{4} & \frac{(5-3\varepsilon)(1-\varepsilon)}{16} \end{pmatrix}. \tag{21}$$

In Fig. 1 the region $\mathcal{D}_{1,2}$ for the case $\varepsilon > 0$ is marked by the '+' sign. Such a form of the domain follows from the asymptotical normality of the bivariate statistics $(\mathcal{B}_{T,1}, \mathcal{B}_{T,2})$ and from expressions (18). To calculate the probability of the first kind error, we use the linear transform of the region $\mathcal{D}_{1,2}$. We apply the matrix $\Sigma_0^{-\frac{1}{2}}$ to the unit vectors $(1,0), (0,1) \in \mathcal{R}^2$ and construct the Gram matrix:

$$\begin{gathered}u_1 = \Sigma_0^{-\frac{1}{2}}(1,0)',\ u_2 = \Sigma_0^{-\frac{1}{2}}(0,1)', \\ \begin{pmatrix} u_1'u_1 & u_1'u_2 \\ u_1'u_2 & u_2'u_2 \end{pmatrix} = \Sigma_0^{-1} = \frac{2^6}{(1-\varepsilon^2)^2}\begin{pmatrix} \frac{(5-3\varepsilon)(1-\varepsilon)}{16} & -\frac{1-\varepsilon}{4} \\ -\frac{1-\varepsilon}{4} & \frac{1}{4} \end{pmatrix}.\end{gathered}$$

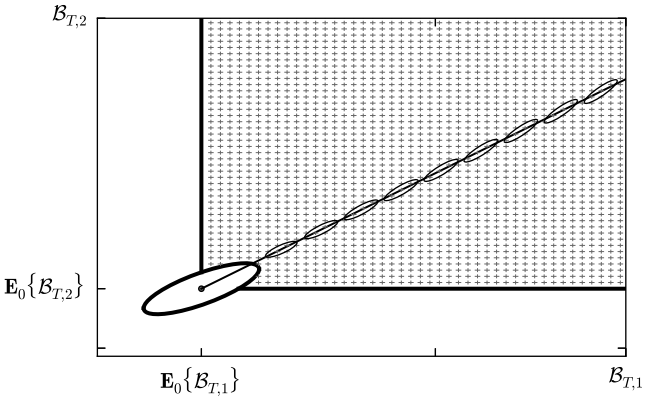

Figure 1. The region $\mathcal{D}_{1,2}$ for $\varepsilon > 0$ and the scattering ellipses for $\delta \in [0, 1]$.

The angle ϕ between the vectors u_1 and u_2 is expressed in terms of the coefficient of correlation:

$$\phi = \arccos\left(\frac{u_1' u_2}{|u_1||u_2|}\right) = \pi - \arccos\left(\operatorname{corr}_0\{\mathcal{B}_{T,1}, \mathcal{B}_{T,2}\}\right) = \pi - \arccos\left(2\sqrt{\tfrac{1-\varepsilon}{5-3\varepsilon}}\right).$$

Because of the joint asymptotic normality of statistics (17), the random variable

$$Q_{1,2} = \frac{1}{T}\begin{pmatrix} \mathcal{B}_{T,1} - \mu_{0,1} \\ \mathcal{B}_{T,2} - \mu_{0,1}^2 \end{pmatrix}' \Sigma_0^{-1} \begin{pmatrix} \mathcal{B}_{T,1} - \mu_{0,1} \\ \mathcal{B}_{T,2} - \mu_{0,1}^2 \end{pmatrix}$$

has an asymptotically exponential distribution with the parameter $1/2$ as $T \to \infty$. Hence, from the equation

$$\mathbf{P}_0\{(\mathcal{B}_{T,1}, \mathcal{B}_{T,2}) \in \mathcal{D}_{1,2}\} = \mathbf{P}_0\{Q_{1,2} \geq c\}\frac{\phi}{2\pi} = \frac{(\pi - \arccos(2\sqrt{\frac{1-\varepsilon}{5-3\varepsilon}}))}{2\pi e^{c/2}} = \alpha$$

we find $c = \dfrac{2^6}{(1-\varepsilon^2)^2}\, c_{1,2}$ (the ellipse equation in Fig. 1: $Q_{1,2} = c$). The case $\varepsilon < 0$ is considered similarly with $u_1 = \Sigma_0^{-\frac{1}{2}}(-1, 0)'$, $u_2 = \Sigma_0^{-\frac{1}{2}}(0, -1)'$. □

Lemma 3. *Under the* $(1, 1)$*-model of embedding and the alternative* H_1 *the random variables* z_t, z_s *are independent if* $|t - s| \geq 2$*, the random variables* $z_t, z_s z_{s+1}$ *are independent if* $|t - s| \geq 2$*, and the random variables* $z_t z_{t+1}, z_s z_{s+1}$ *are independent if* $|t - s| \geq 3$.

Proof. Let us consider the random variables z_t, z_{t+k}, $k \geq 2$, and find the expectation $\mathbf{E}_\delta\{z_t z_{t+k}\}$, $k \geq 2$:

$$\begin{aligned}
\mathbf{E}_\delta\{z_t z_{t+k}\} &= \mathbf{P}_\delta\{z_t z_{t+k} = 1\} = 2\mathbf{P}_\delta\{Y_t = 0, Y_{t+1} = 1, Y_{t+k} = 0, Y_{t+k+1} = 1\} + \\
&\quad + 2\mathbf{P}_\delta\{Y_t = 0, Y_{t+1} = 1, Y_{t+k} = 1, Y_{t+k+1} = 0\} = \\
&= 2\sum_{u \in V_4} \mathbf{P}_\delta\{(Y_t, Y_{t+1}, Y_{t+k}, Y_{t+k+1}) = (0,1,0,1), (\gamma_t, \gamma_{t+1}, \gamma_{t+k}, \gamma_{t+k+1}) = u\} + \\
&\quad + 2\sum_{u \in V_4} \mathbf{P}_\delta\{(Y_t, Y_{t+1}, Y_{t+k}, Y_{t+k+1}) = (0,1,1,0), (\gamma_t, \gamma_{t+1}, \gamma_{t+k}, \gamma_{t+k+1}) = u\} = \\
&= \tfrac{2}{16}\sum_{c \in \{1,-1\}} \big((1-\delta)^4(1-\varepsilon)^2(1 - c\varepsilon^{k-1}) + \delta(1-\delta)^3(2(1-\varepsilon)(1 - c\varepsilon^{k-1}) + 2(1-\varepsilon)(1 + c\varepsilon^k)) + \\
&\quad + \delta^2(1-\delta)^2(6 - 2\varepsilon - c\varepsilon^{k-1} + 2c\varepsilon^k - c\varepsilon^{k+1}) + 4\delta^3(1-\delta) + \delta^4\big) = \left(\tfrac{1}{2}(1 - \varepsilon(1-\delta)^2)\right)^2 = (\mathbf{E}_\delta\{z_t\})^2.
\end{aligned}$$

Since the random variables z_t, z_{t+k} are binary and since $\operatorname{cov}_\delta\{z_t, z_{t+k}\} = 0$ for $k \geq 2$, then such variables are independent. A similar argument shows that the random variables $z_t, z_s z_{s+1}$ are independent if $|t - s| \geq 2$ and that the random variables $z_t z_{t+1}, z_s z_{s+1}$ are independent if $|t - s| \geq 3$. □

Now we will employ Lemma 3 to find asymptotic expressions for the first and second moments of the bivariate statistics $(\mathcal{B}_{T,1}, \mathcal{B}_{T,2})$ under the alternative $H_{1,\delta}$. The first-order moments were found in (18). In the course of the proof of Theorem 1 it was shown that

$$\mathbf{D}_\delta\{\mathcal{B}_{T,1}\} = T\tfrac{1}{4}(1-(1-\delta)^2\varepsilon^2(1-6\delta+3\delta^2))(1+o(1)),\ T\to\infty.$$

In view of Lemma 3 we have, as $T\to\infty$,

$$\begin{gathered}
\operatorname{cov}_\delta\{\mathcal{B}_{T,1},\mathcal{B}_{T,2}\} = \sum\nolimits_{t,s=1}^{T-2}\operatorname{cov}_\delta\{z_t, z_s z_{s+1}\} = \\
= (T-2)\operatorname{cov}_\delta\{z_t, z_t z_{t+1}\} + (T-3)\operatorname{cov}_\delta\{z_t, z_{t+1}z_{t+2}\} + \\
+(T-3)\operatorname{cov}_\delta\{z_t, z_{t-1}z_t\} + (T-4)\operatorname{cov}_\delta\{z_t, z_{t-2}z_{t-1}\} = \\
= 2T(\operatorname{cov}_\delta\{z_t, z_t z_{t+1}\} + \operatorname{cov}_\delta\{z_t, z_{t+1}z_{t+2}\})(1+o(1)), \\
\operatorname{cov}_\delta\{z_t, z_t z_{t+1}\} = \mathbf{P}_\delta\{z_t z_{t+1}=1\}(1-\mathbf{P}_\delta\{z_t=1\}) = \\
= \tfrac{1}{4}(1-(1-\delta)^2\varepsilon(2-\varepsilon))(1-\tfrac{1}{2}(1-(1-\delta)^2\varepsilon)) = \\
= \tfrac{1}{8}(1-(1-\delta)^2\varepsilon(1-\varepsilon)-(1-\delta)^4\varepsilon^2(2-\varepsilon)), \\
\operatorname{cov}_\delta\{z_t, z_{t+1}z_{t+2}\} = \mathbf{P}_\delta\{z_t z_{t+1}z_{t+2}=1\} - \mathbf{P}_\delta\{z_t=1\}\mathbf{P}_\delta\{z_{t+1}z_{t+2}=1\}.
\end{gathered}$$

Using the law of total probability, we find, for the model of embedding (1, 1),

$$\begin{gathered}
\mathbf{P}_\delta\{z_t z_{t+1}z_{t+2}=1\} = 2\mathbf{P}_\delta\{Y_t=0, Y_{t+1}=1, Y_{t+2}=0, Y_{t+3}=1\} = \\
= 2\sum_{u\in V_4}\mathbf{P}_\delta\{Y_t=0, Y_{t+1}=1, Y_{t+2}=0, Y_{t+3}=1, \gamma_t^{t+3}=u\} = \\
= \tfrac{1}{8}(1-(1-\delta)^2\varepsilon(3-2\varepsilon+\varepsilon^2)+(1-\delta)^4\varepsilon^2),
\end{gathered}$$

$$\begin{gathered}
\operatorname{cov}_\delta\{z_t, z_{t+1}z_{t+2}\} = \mathbf{P}_\delta\{z_t z_{t+1}z_{t+2}=1\} - \mathbf{P}_\delta\{z_t=1\}\mathbf{P}_\delta\{z_{t+1}z_{t+2}=1\} = \\
= \mathbf{P}_\delta\{z_t z_{t+1}z_{t+2}=1\} - \tfrac{1}{8}(1-(1-\delta)^2\varepsilon(3-\varepsilon)+(1-\delta)^4\varepsilon^2(2-\varepsilon)) = \\
= \tfrac{1}{8}(1-\delta)^2\delta(2-\delta)\varepsilon^2(1-\varepsilon).
\end{gathered}$$

We thus have

$$\operatorname{cov}_\delta\{\mathcal{B}_{T,1},\mathcal{B}_{T,2}\} = T\tfrac{1}{4}(1-(1-\delta)^2\varepsilon(1-\varepsilon)^2-(1-\delta)^4\varepsilon^2(3-2\varepsilon))(1+o(1)).$$

Using Lemma 3 as $T\to\infty$ we find the variance $\mathbf{D}_\delta\{\mathcal{B}_{T,2}\}$:

$$\begin{gathered}
\mathbf{D}_\delta\{\mathcal{B}_{T,2}\} = (T-2)\mathbf{D}_\delta\{z_t z_{t+1}\} + 2(T-3)\operatorname{cov}_\delta\{z_t z_{t+1}, z_{t+1}z_{t+2}\} + \\
+2(T-4)\operatorname{cov}_\delta\{z_t z_{t+1}, z_{t+2}z_{t+3}\}, \\
\mathbf{D}_\delta\{z_t z_{t+1}\} = \mathbf{P}_\delta\{z_t z_{t+1}=1\}(1-\mathbf{P}_\delta\{z_t z_{t+1}=1\} = \\
= \tfrac{1}{16}(1-(1-\delta)^2\varepsilon(2-\varepsilon))(3+(1-\delta)^2\varepsilon(2-\varepsilon)), \\
\operatorname{cov}_\delta\{z_t z_{t+1}, z_{t+1}z_{t+2}\} = \mathbf{P}_\delta\{z_t z_{t+1}z_{t+2}=1\} - (\mathbf{P}_\delta\{z_t z_{t+1}=1\})^2 = \\
= \tfrac{1}{16}(1-(1-\delta)^2 2\varepsilon(1-\varepsilon+\varepsilon^2)-(1-\delta)^4\varepsilon^2(2-4\varepsilon+\varepsilon^2)), \\
\operatorname{cov}_\delta\{z_t z_{t+1}, z_{t+2}z_{t+3}\} = \mathbf{P}_\delta\{z_t z_{t+1}z_{t+2}z_{t+3}=1\} - (\mathbf{P}_\delta\{z_t z_{t+1}=1\})^2.
\end{gathered}$$

A similar argument as for $\mathbf{P}_\delta\{z_t z_{t+1}z_{t+2}=1\}$ shows that

$$\begin{gathered}
\mathbf{P}_\delta\{z_t z_{t+1}z_{t+2}z_{t+3}=1\} = 2\mathbf{P}_\delta\{Y_t=0, Y_{t+1}=1, Y_{t+2}=0, Y_{t+3}=1, Y_{t+4}=0\} = \\
= 2\sum_{u\in V_5}\mathbf{P}_\delta\{Y_t=0, Y_{t+1}=1, Y_{t+2}=0, Y_{t+3}=1, Y_{t+4}=0, \gamma_t^{t+4}=u\} = \\
= \tfrac{1}{16}(1-(1-\delta)^2(\varepsilon(4+\delta^3)-3\varepsilon^2(2-2\delta+\delta^2)+\varepsilon^3(4-4\delta+2\delta^2-\delta^3)-\varepsilon^4)), \\
\operatorname{cov}_\delta\{z_t z_{t+1}, z_{t+2}z_{t+3}\} = \tfrac{1}{16}(1-\delta)^2\delta\varepsilon(1-\varepsilon)(-\delta^2+\varepsilon(2-\delta-\delta^2)-\varepsilon^2(2-\delta)).
\end{gathered}$$

As a result, we have

$$\mathbf{D}_\delta\{\mathcal{B}_{T,2}\} = T\tfrac{1}{16}(5-(1-\delta)^2(2(4+\delta^3)\varepsilon+2(1-10\delta+5\delta^2)\varepsilon^2- \\ -2(4-16\delta+8\delta^2+\delta^3)\varepsilon^3+(3-10\delta+\delta^2)\varepsilon^4))(1+o(1)).$$

Using the strong mixing property [10], one may show that under the alternative $H_{1,\delta}$ the distribution of the random vector

$$\frac{1}{\sqrt{T}}\left(\mathcal{B}_{T,1}-\tfrac{1}{2}T(1-(1-\delta)^2\varepsilon),\mathcal{B}_{T,2}-\tfrac{1}{4}T(1-(1-\delta)^2\varepsilon(2-\varepsilon))\right)'$$

as $T\to\infty$ is asymptotically normal $\mathcal{N}_2((0,0)',\Sigma_1)$ with zero mean and covariance matrix $\Sigma_1=(\sigma_{1,ij})$, $i,j=1,2$, where

$$\sigma_{1,00}=\tfrac{1}{4}(1-(1-\delta)^2\varepsilon^2(1-6\delta+3\delta^2)), \\ \sigma_{1,01}=\sigma_{1,10}=\tfrac{1}{4}(1-(1-\delta)^2\varepsilon(1-\varepsilon)^2-(1-\delta)^4\varepsilon^2(3-2\varepsilon)), \\ \sigma_{1,11}=\tfrac{1}{16}(5-(1-\delta)^2(2(4+\delta^3)\varepsilon+2(1-10\delta+5\delta^2)\varepsilon^2- \\ -2(4-16\delta+8\delta^2+\delta^3)\varepsilon^3+(3-10\delta+\delta^2)\varepsilon^4)).$$

Unfortunately, for the test (19) based on the short runs statistics we have not succeed to obtain an explicit expression for the power and to examine it, because the covariance matrix depends on δ. This dependence is illustrated in Fig. 1, which depicts the scattering ellipses (corresponding to the asymptotic matrices) when the parameter δ is increasing from 0 to 1. The following important property of the asymptotically normal distribution of the random vector (17) under the alternative $H_{1,\delta}$ is worth pointing out: with δ changing from 0 to 1 the centre of the asymptotically normal distribution of the bivariate statistics $(\mathcal{B}_{T,1},\mathcal{B}_{T,2})$ always lies on the line

$$\begin{cases} b_1=\tfrac{1}{2}T\varepsilon\Delta+\tfrac{1}{2}T(1-\varepsilon), \\ b_2=\tfrac{1}{4}T\varepsilon(2-\varepsilon)\Delta+\tfrac{1}{4}T(1-\varepsilon)^2, \end{cases} \quad \Delta=\delta(2-\delta). \tag{22}$$

Taking into account the property (22), we construct a statistical test for the hypotheses $H_{0,\varepsilon}$, H_1 based on the statistics obtained as the orthogonal projection of the statistics $(\mathcal{B}_{T,1},\mathcal{B}_{T,2})$ on the line (22). Such a test for $\varepsilon>0$ is given by the critical region

$$\mathcal{X}_{1\alpha}^{\mathfrak{h}+}=\{y_1^T:\ \mathcal{B}_{T,1}+\tfrac{1}{2}(2-\varepsilon)\mathcal{B}_{T,2}\ge\tfrac{1}{2}T(1-\varepsilon)+\tfrac{1}{8}T(1-\varepsilon)^2(2-\varepsilon)-t_\alpha\sqrt{Td_{\mathfrak{h}}}\}, \tag{23}$$

$$d_{\mathfrak{h}}=2^{-6}(1-\varepsilon^2)(68-100\varepsilon+65\varepsilon^2-20\varepsilon^3+3\varepsilon^4).$$

Theorem 5. *Let the model of embedding (4) hold and let $\varepsilon>0$. Then, as $T\to\infty$, the asymptotic size of test (23) for the hypotheses $H_{0,\varepsilon}$, H_1 based on the projection of the short runs statistics*

$$\mathfrak{h}=\mathcal{B}_{T,1}-\tfrac{1}{2}T(1-\varepsilon)+\tfrac{1}{2}(2-\varepsilon)(\mathcal{B}_{T,2}-\tfrac{1}{4}T(1-\varepsilon)^2) \tag{24}$$

coincides with the significance level $\alpha\in(0,1)$. The asymptotic power of this test for the $(1,1)$-model of embedding and for the family of contiguous alternatives $H_{1,\delta}:\ \{\delta=\frac{\rho}{\sqrt{T}}\}$ is as follows:

$$W_1^{\mathfrak{h}+}\to\Phi\left(t_\alpha+\frac{\rho\varepsilon(1+\frac{1}{4}(2-\varepsilon)^2)}{\sqrt{d_{\mathfrak{h}}}}\right),\ T\to\infty. \tag{25}$$

Proof. The angle between the line (22) and the b_2-axis is $\phi=\arctan(\frac{1}{2}(2-\varepsilon))$, and hence, the orthogonal projection of the point $(\mathcal{B}_{T,1},\mathcal{B}_{T,2})$ on this line is given by

$$(\mathcal{B}_{T,1}-\tfrac{1}{2}T(1-\varepsilon))\cos\phi+(\mathcal{B}_{T,1}-\tfrac{1}{2}T(1-\varepsilon))\sin\phi.$$

Multiplying this expression by $\operatorname{cosec}\phi$, we get the random variable $\mathfrak{h}$, which, according to (21), has the asymptotically normal distribution $\mathcal{N}_1(0, d_{\mathfrak{h}})$ under the hypothesis $H_{0,\varepsilon}$. Hence, $\mathbf{P}_0\{\mathscr{X}_{1\alpha}^{\mathfrak{h}+}\} \to \alpha$ as $T \to \infty$.

Let us find the power of test (23) as $T \to \infty$ for contiguous alternatives of the form indicated in the theorem. We have

$$\begin{aligned} W_1^{\mathfrak{h}+} &= \mathbf{P}_\delta\{\mathcal{B}_{T,1} + \tfrac{1}{2}(2-\varepsilon)\mathcal{B}_{T,2} \geq \tfrac{1}{2}T(1-\varepsilon) + \tfrac{1}{8}T(1-\varepsilon)^2(2-\varepsilon) - t_\alpha\sqrt{Td_{\mathfrak{h}}}\} \\ &= \mathbf{P}_\delta\{\mathcal{B}_{T,1} + \tfrac{1}{2}(2-\varepsilon)\mathcal{B}_{T,2} - \mathbf{E}_\delta\{\mathcal{B}_{T,1}\} - \tfrac{1}{2}(2-\varepsilon)\mathbf{E}_\delta\{\mathcal{B}_{T,2}\} \leq \\ &\leq \tfrac{1}{2}T\delta(2-\delta)\varepsilon + \tfrac{1}{8}T\delta(2-\delta)\varepsilon(2-\varepsilon)^2 + t_\alpha\sqrt{Td_{\mathfrak{h}}}\} \to \\ &\to \Phi\left(\lim \frac{\tfrac{1}{2}T\delta(2-\delta)\varepsilon + \tfrac{1}{8}T\delta(2-\delta)\varepsilon(2-\varepsilon)^2 + t_\alpha\sqrt{Td_{\mathfrak{h}}}\}}{\sqrt{T(\sigma_{1,00} + \tfrac{1}{4}(2-\varepsilon)^2\sigma_{1,11} + (2-\varepsilon)\sigma_{1,01})}}\right). \end{aligned}$$

Substituting $\delta = \dfrac{\rho}{\sqrt{T}}$ in this expression as $T \to \infty$, we find that

$$W_1^{\mathfrak{h}+} \to \Phi\left(\lim \frac{\sqrt{T}\rho\varepsilon + \tfrac{1}{4}\sqrt{T}\rho\varepsilon(2-\varepsilon)^2 + t_\alpha\sqrt{Td_{\mathfrak{h}}} + \mathcal{O}(1)}{\sqrt{T\left(d_{\mathfrak{h}} + \mathcal{O}\left(\frac{1}{\sqrt{T}}\right)\right)}}\right) \to \Phi\left(t_\alpha + \frac{\rho\varepsilon(1 + \frac{1}{4}(2-\varepsilon)^2)}{\sqrt{d_{\mathfrak{h}}}}\right).$$

□

4 Embedding detection on the basis of the likelihood ratio statistics

Let us now consider the case when the parameter ε in (1) is unknown and separated from the zero: $\varepsilon_0 \leq |\varepsilon| < 1$, where $\varepsilon_0 > 0$ is the known boundary value.

We construct the likelihood function for the observed stego-sequence $y_1^T \in V_T$. Following [5], we partition the set V_t of binary t-dimensional vectors into $t+1$ disjoint subsets,

$$V_t = \Gamma_0^{(t)} \cup \Gamma_1^{(t)} \cup \ldots \cup \Gamma_t^{(t)}, \tag{26}$$

where

$$\begin{aligned} \Gamma_0^{(t)} &= \{u_1^t \in V_t : u_t = 1\}, \\ \Gamma_1^{(t)} &= \{u_1^t \in V_t : u_{t-1} = u_t = 0\}, \\ \Gamma_j^{(t)} &= \{u_1^t \in V_t : u_{t-j} = 0, u_{t-j+1} = \ldots = u_{t-1} = 1, u_t = 0\},\ 1<j<t, \\ \Gamma_t^{(t)} &= \{u_1^t \in V_t : u_1 = \ldots = u_{t-1} = u_t = 1\}. \end{aligned} \tag{27}$$

The partition (26), (27) generates the partition of all possible trajectories of fragments of the key sequence $\gamma_1^t = u_1^t \in V_t$.

Lemma 4. *The likelihood function for the (q,r)-block model of embedding is as follows*

$$L(\varepsilon,\delta) = \mathbf{P}_\delta\{Y_1^T = y_1^T\} = 2^{-T} \sum_{u_1^T \in \Gamma^{(q,r)}} (1-\delta)^{b_0(u_1^T)} (\delta/C_q^r)^{b_r(u_1^T)} \prod_{t=1}^{T} \varphi_t(u_1^t, y_1^t),$$

where

$$\varphi_t(u_1^t, y_1^t) = \begin{cases} 1, & u_1^t \in \Gamma_0^{(t)}, \\ 1 + (-1)^{y_{t-j}+y_t}\varepsilon^j, & u_1^t \in \Gamma_j^{(t)},\ 1 \leq j < t, \\ 1, & u_1^t \in \Gamma_t^{(t)}. \end{cases}$$

The proof is similar to that of Theorem 5 for the q-block model of embedding in [5].

To test the hypotheses H_0, H_1 on the existence of embeddings we now construct the statistical likelihood ratio test [12]. The statistics λ_T of this test for the hypotheses $H_0,\ H_1$ takes the form

$$\lambda_T = \lambda_T(y_1^T) = -2\ln\frac{L(\hat{\varepsilon},0)}{\max\{L(\hat{\varepsilon}_1,\hat{\delta}_1), L(\hat{\varepsilon},0)\}} \geq 0, \tag{28}$$

where $\hat{\varepsilon}$, $(\hat{\varepsilon}_1, \hat{\delta}_1)$ are the maximum-likelihood estimates, which were constructed in [5] under the hypotheses H_0 and H_1 respectively. The statistics (28) introduced above is equivalent to the likelihood ratio statistics

$$\frac{\sup\limits_{|\varepsilon|<1,\delta>0}\mathbf{P}_\delta\{y_1,\dots,y_T\}}{\sup\limits_{|\varepsilon|<1}\mathbf{P}_0\{y_1,\dots,y_T\}}.$$

Besides, according to [5],

$$\arg\max_{|\varepsilon|<1,\delta>0}\mathbf{P}_\delta\{y_1,\dots,y_T\} = (\hat{\varepsilon}_1,\hat{\delta}_1),\ \arg\max_{|\varepsilon|<1}\mathbf{P}_0\{y_1,\dots,y_T\} = \hat{\varepsilon}.$$

The statistical test of size $\alpha \in (0,1)$ based on the statistics λ_T is defined by the critical region

$$\mathscr{X}_{1\alpha}^{\lambda} = \{y_1^T \in V_T :\ \lambda_T \geq \lambda_\alpha\}, \tag{29}$$

where $\lambda_\alpha > 0$ is the solution of the equation

$$\sup_{\varepsilon_0\leq|\varepsilon|<1}\mathbf{P}_0\{\lambda_T \geq \lambda\} = \sup_{\varepsilon_0\leq|\varepsilon|<1}(1 - F_0(\varepsilon,T,\lambda_T)) = \alpha. \tag{30}$$

Here, $F_0(\varepsilon,T,\lambda_T)$ is the distribution function of the statistics (28) under the null hypothesis H_0.

To estimate the value of λ_α satisfying (30), we use the Monte Carlo method: we model M_0 samples of a Markov chain of length T with the parameter ε_0. For each sample we calculate the value of the statistics by (28). Let $\lambda^{(1)},\dots,\lambda^{(M_0)}$ be the calculated values. Then λ_α can be estimated by the sample quantile of level $1-\alpha$:

$$\hat{\lambda}_\alpha = \lambda_{([(1-\alpha)M_0])}; \tag{31}$$

the accuracy of this estimate increases with $M_0 \to \infty$. So, the statistical tests (29) for the embedding existence assumes the form:

$$\text{the hypothesis } H_0 \text{ (respectively, } H_1\text{) is adopted if } p \geq \alpha\ (p < \alpha),$$
$$p = \frac{1}{M_0+1}\left(1 + \sum_{i=1}^{M_0} I\{\lambda^{(i)} > \lambda_T\}\right).$$

The available asymptotic properties of the likelihood ratio test [12, 13] may be used under the regularity conditions [12] guaranteeing the existence, uniqueness, and asymptotic normality of the maximum likelihood estimates of the parameters ε and δ.

Theorem 6. *Under the model of embedding* (4)*, as $T \to \infty$ the test of asymptotic significance level $\alpha \in (0,1)$ based on the likelihood ratio statistics for the composite null hypothesis is given by the critical region* (29) *with the threshold $\lambda_\alpha = \chi^2_{1-\alpha,1}$; that is,*

$$\mathbf{P}_0\{\mathscr{X}_{1\alpha}^{\lambda}\} = \mathbf{P}_0\{\lambda_T \geq \chi^2_{1-\alpha,1}\} \to \alpha.$$

This test is consistent under fixed alternatives $\delta = \delta_1 > 0$:

$$W_1^{\lambda} = \mathbf{P}_\delta\{\mathscr{X}_{1\alpha}^{\lambda}\} \to 1.$$

The proof follows the argument of [13] with the use of the central limit theorem for weakly dependent random variables [10].

5 Statistical estimation of embeddings points

If the alternative H_1 is adopted, then there arises the problem of estimation of points of embeddings—these being the time instants $t \in \{1, \dots, T\}$ at which in accordance with (4) a bit of the sequence $\{x_t\}$ is replaced by a bit of the hidden message $\{\xi_t\}$.

Theorem 7. *Let $\gamma_1^T = (\gamma_1, \dots, \gamma_T) \in \Gamma^{(q,r)}$ be the key sequence corresponding to the (q, r)-model of embedding, $y_1^T \in V_T$ be the observed stego-sequence, $\hat{\gamma}_1^T = f(y_1^T)$ is some statistical estimate of the key sequence γ_1^T based on observations y_1^T. The minimum of the error probability in estimating the stego-key*

$$\mathbf{P}_\delta\{\hat{\gamma}_1^T \neq \gamma_1^T\} \to \min$$

is attained for the statistics

$$\hat{\gamma}_1^{T*} = \arg \max_{u_1^T \in \Gamma^{(q,r)}} \mathbf{P}_\delta\{\gamma_1^T = u_1^T | Y_1^T = y_1^T\}, \tag{32}$$

which maximizes the a posteriori probability of the stego-key. The minimum of error probability is as follows:

$$\begin{aligned} r^*(\varepsilon, \delta, T) &= \min_{f(\cdot)} \mathbf{P}_\delta\{\hat{\gamma}_1^T \neq \gamma_1^T\} = \\ &= 1 - \sum_{y_1^T \in V_T} \mathbf{P}_\delta\{Y_1^T = y_1^T\} \max_{u_1^T \in \Gamma^{(q,r)}} \mathbf{P}_\delta\{\gamma_1^T = u_1^T | Y_1^T = y_1^T\}. \end{aligned} \tag{33}$$

Proof. We choose an arbitrary statistics

$$\hat{\gamma}_1^T = f(Y_1^T) : V_T \to \Gamma^{(q,r)}, \tag{34}$$

and calculate for it the corresponding error probability for the estimate of the true stego-key $\gamma_1^T \in \Gamma^{(q,r)}$:

$$r(f; \varepsilon, \delta, T) = \mathbf{P}_\delta\{\hat{\gamma}_1^T \neq \gamma_1^T\} = 1 - \mathbf{P}_\delta\{\hat{\gamma}_1^T = \gamma_1^T\}.$$

After equivalent transformations, using (34) and the rlaw of total probability, we find that

$$\begin{aligned} r(f; \varepsilon, \delta, T) &= 1 - \sum_{u_1^T \in \Gamma^{(q,r)}} \mathbf{P}_\delta\{\hat{\gamma}_1^T = \gamma_1^T, \gamma_1^T = u_1^T\} = 1 - \sum_{u_1^T \in \Gamma^{(q,r)}} \sum_{y_1^T \in V_T} \mathbf{P}_\delta\{f(Y_1^T) = \gamma_1^T, \gamma_1^T = u_1^T, Y_1^T = y_1^T\} = \\ &= 1 - \sum_{y_1^T \in V_T} \sum_{u_1^T \in \Gamma^{(q,r)}} \mathbf{P}_\delta\{Y_1^T = y_1^T\} \mathbf{P}_\delta\{\gamma_1^T = u_1^T | Y_1^T = y_1^T\} \times \mathbf{P}_\delta\{f(Y_1^T) = \gamma_1^T | \gamma_1^T = u_1^T, Y_1^T = y_1^T\} = \\ &= 1 - \sum_{y_1^T \in V_T} \mathbf{P}_\delta\{Y_1^T = y_1^T\} \sum_{u_1^T \in \Gamma^{(q,r)}} I\{f(y_1^T) = u_1^T\} \mathbf{P}_\delta\{\gamma_1^T = u_1^T | Y_1^T = y_1^T\}. \end{aligned} \tag{35}$$

Minimizing this expression in $f(\cdot)$ and using (34), we obtain the optimal function $f(\cdot)$ in the form

$$f^*(y_1^T) = \arg \max_{u_1^T \in \Gamma^{(q,r)}} \mathbf{P}_\delta\{\gamma_1^T = u_1^T | Y_1^T = y_1^T\}, \tag{36}$$

which agrees with the statistics (32).

Substituting (36) into (35), we get (33). □

The estimate (32) by the maximum a posteriori probability criterion admits the following equivalent representation, which is convenient for its evaluation:

$$\hat{\gamma}_1^{T*} = \arg \max_{u_1^T \in \Gamma^{(q,r)}} \mathbf{P}_\delta\{\gamma_1^T = u_1^T | Y_1^T = y_1^T\} = \arg \max_{u_1^T \in \Gamma^{(q,r)}} \mathbf{P}_\delta\{\gamma_1^T = u_1^T, Y_1^T = y_1^T\}. \tag{37}$$

The solution of problem (37) for the (q, r)-block model of embedding by the exhaustive search has a computational complexity $O(T(1 + C_q^r)^{T/q})$. Let us find a polynomial algorithm for solving this problem on the basis of the classical Viterbi algorithm [14].

We set

$$\mathfrak{s}_t(u_{t-c},\dots,u_t) = \max_{u_1,\dots,u_{t-c-1}\in V} \log \mathbf{P}_\delta\{Y_1^t = y_1^t, \gamma_1 = u_1,\dots,\gamma_t = u_t\},$$
$$c = \max\{2r+1, q-1\}.$$

The initial values of $\mathfrak{s}_t(u_1,\dots,u_t)$ with $t = 1,\dots,c$ are as follows:

$$\begin{aligned}\mathfrak{s}_1(u_1) &= \log\varphi_1(u_1,y_1) + \log \mathbf{P}_\delta\{\gamma_1 = u_1\},\\ \mathfrak{s}_t(u_1,\dots,u_t) &= \mathfrak{s}_{t-1}(u_1,\dots,u_{t-1}) + \log\varphi_t(u_1^t, y_1^t) +\\ &\quad + \log \mathbf{P}_\delta\{\gamma_t = u_t|\gamma_{t-1} = u_{t-1},\dots,\gamma_1 = u_1\},\ 2\le t\le c;\end{aligned} \tag{38}$$

here, $\varphi_t(\cdot)$ is the same as in Lemma 4.

Theorem 8. *Under the (q,r)-block model of embedding (4), $q > r$, the recurrence relation*

$$\begin{aligned}&\mathfrak{s}_t(u_{t-c},\dots,u_t) =\\ &= \max_{u_{t-c-1}\in V} \mathfrak{s}_{t-1}(u_{t-c-1},u_{t-c},\dots,u_{t-1}) + \log \mathfrak{f}_t(u_{t-2r-1}^t, y_{t-2r-1}^t) +\\ &\quad + \log \mathbf{P}_\delta\{\gamma_t = u_t|\gamma_{t-1} = u_{t-1},\dots,\gamma_{t-c} = u_{t-c}\}\end{aligned} \tag{39}$$

holds for $\mathfrak{s}_t(u_{t-c},\dots,u_t)$ with $t > c$, where

$$\mathfrak{f}_t(u_{t-2r-1}^t, y_{t-2r-1}^t) = \begin{cases} \frac{1}{2},\ u_1^t \in \Gamma_0^{(t)},\\ \frac{1}{2}(1+(-1)^{y_{t-j}+y_t}\varepsilon^j),\ u_1^t\in\Gamma_j^{(t)},\ 1\le j\le 2r+1.\end{cases}$$

Proof. In the case $q \le 2r+2$ we have

$$\begin{aligned}\mathfrak{s}_t(u_{t-2r-1},\dots,u_t) &= \max_{u_1,\dots,u_{t-2r-2}\in V} \log \mathbf{P}_\delta\{Y_1^t = y_1^t, \gamma_1 = u_1,\dots,\gamma_t = u_t\} =\\ &= \max_{u_1,\dots,u_{t-2r-2}\in V} \log \mathbf{P}_\delta\{Y_1^{t-1} = y_1^{t-1}, Y_t = y_t, \gamma_1 = u_1,\dots,\gamma_{t-1} = u_{t-1}, \gamma_t = u_t\} =\\ &= \max_{u_1,\dots,u_{t-2r-2}\in V} \log \mathbf{P}_\delta\{Y_1^{t-1} = y_1^{t-1}, \gamma_1 = u_1,\dots,\gamma_{t-1} = u_{t-1}\} +\\ &\quad + \log \mathbf{P}_\delta\{\gamma_t = u_t|\gamma_1 = u_1,\dots,\gamma_{t-1} = u_{t-1}\} +\\ &\quad + \log \mathbf{P}_\delta\{Y_t = y_t \mid Y_1^{t-1} = y_1^{t-1}, \gamma_1 = u_1,\dots,\gamma_t = u_t\}.\end{aligned}$$

The case $q > 2r+2$ is dealt with similarly. Combining these cases, we arrive at (39). □

Corollary 1. *Under the hypotheses of Theorem 8 the estimate $\hat\gamma_1^T = (\hat\gamma_1,\dots,\hat\gamma_T)$ of the stego-key by the maximum a posteriori probability criterion is as follows*

$$\begin{aligned}&(\hat\gamma_{T-c},\dots,\hat\gamma_T) = \arg\max_{u_{T-c},\dots,u_T\in V} \mathfrak{s}_T(u_{T-c},\dots,u_T),\\ &\hat\gamma_t = \arg\max_{v\in V} \mathfrak{s}_{t+c}(v,\hat\gamma_{t+1},\dots,\hat\gamma_{t+c}),\ t = T-c-1,\dots,1.\end{aligned} \tag{40}$$

Proof. The estimate $\hat\gamma_1^T = (\hat\gamma_1,\dots,\hat\gamma_T)$ of the stego-key is obtained as the reverse execution of the algorithm for finding $\max_{u_{T-c},\dots,u_T\in V} \mathfrak{s}_T$ by (38), (39). □

The algorithm of the estimation of embedding points (the forward run (38), (39), the backward run (40)) has a numerical complexity $O(2^c + (T-c)2^{2c+2})$.

Having estimate the embedding points γ_1^T by (40), one can construct an estimate $\hat\xi$ of the message itself:

$$\hat\xi_\tau = y_{t_\tau},\quad \text{where}\quad t_\tau = \min_{t\in\{1,\dots,T\}}\{t : \sum_{k=1}^t \hat\gamma_k = \tau\},\ \tau = 1,\dots,w(\hat\gamma_1^T).$$

6 Results of computer experiments

We give the results of three series of computer experiments using simulated data.

Series 1. The initial Markov sequence (1) of length $T = 10^4$ with the parameter $\varepsilon = 0.13$ was simulated. For $q = r = 1$, the key Bernoulli sequence was simulated using (3) with various values of the parameter $\delta \in [0, 1]$, the stego-sequence y_1^T was constructed by (4). Figure 2 depicts the total number of runs statistics B_T versus the fraction of embeddings δ. Circles mark the values of the statistics $\frac{1}{T-1}B_T$ for the sequence y_1^T thus constructed with the corresponding fraction of embeddings δ, the solid line shows the graph for the mean value $\frac{1}{T-1}\mathbf{E}_\delta\{B_T\}$.

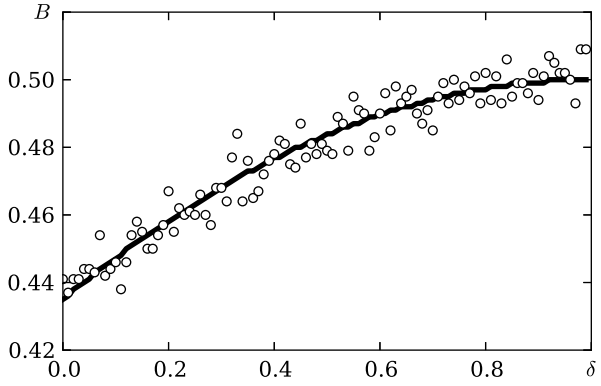

Figure 2. The total number of runs statistics B_T versus the fraction of embeddings δ.

Series 2. As in Series 1, the Monte Carlo method with the number of replications $M_1 = 2^8$ was used to construct estimates of powers for the tests (7), (23) under the hypotheses $H_{0,\varepsilon}$, H_1 with known cover sequence parameter $\varepsilon = 0.48$; the length $T = 2^{13}$, the significance level $\alpha = 0.05$, and the fraction of embeddings $\delta \in \{0.005, 0.01, 0.015, 0.02, 0.025, 0.03, 0.04, 0.05, 0.06, 0.07\}$.

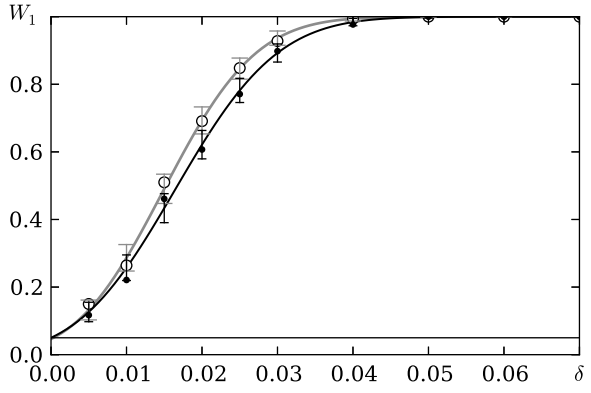

Figure 3. Powers of the tests $\mathscr{X}_{1\alpha}^{B+}$, $\mathscr{X}_{1\alpha}^{\hbar+}$ versus the fraction of embeddings δ.

Figure 3 shows graphically the powers of the statistical tests (7), (23) versus the fraction of the embeddings δ. The black solid line depicts the theoretical curve of the test power (7) based on the total number of runs statistics, the grey solid line shows the theoretical curve of the test power (23) based on the projection of short runs statistics, the black circles correspond to estimates of the powers of test (7), the white circles

show estimates of the powers of test (23). The 95%-confidence intervals for the powers of tests (7) and (23) are shown in grey and black, respectively.

It is seen from the graph that test (23) based on the short runs statistics is more powerful than test (7) based on the total number of runs statistics. Numerical experiments show that for small values ε the powers of tests (7) and (23) are practically the same.

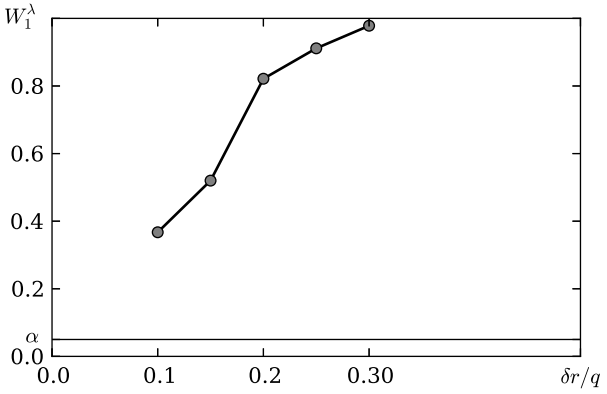

Figure 4. Power of the test $\mathscr{X}_{1\alpha}^{\lambda}$ versus the fraction of embeddings $\delta r/q$.

Series 3. For the block model of embedding with $q = 2$, $r = 1$, the Monte Carlo method was used to find the threshold estimates $\hat{\lambda}_\alpha$ by (31) and the power of the statistical test (29) based of the likelihood ratio with the model parameters $\varepsilon = 0.12$; the length $T = 2^{18}$, and the significance level $\alpha = 0.05$. The threshold estimate was calculated with the number of replications $M_0 = 500$, the estimates of powers were calculated with the number of replications $M_\lambda = 250, 100, 200, 150, 100$ and the fraction of the actual embedding $\delta r/q = \delta/2$, which equals 0.10, 0.15, 0.20, 0.25, 0.30, respectively. Figure 4 shows the graph of the power estimates for the test $\mathscr{X}_{1\alpha}^{\lambda}$ versus the fraction of the actual embedding $\delta/2$.

Computer experiments demonstrate the efficiency of the statistical test thus constructed for the embedding detection and the agreement between theoretical and experimental results.

In conclusion, we note that embeddings may also be detected using small-parametric models of high-order Markov chains [15].

Acknowledgment: The authors are grateful to A. M. Zubkov for suggesting to study the runs statistics for the embedding detection and to the referees for comments and advices.

References

[1] Ponomarev K. I., "A parametric model of embedding and its statistical analysis", *Discrete Math. Appl.*, **19**:6 (2009), 587–596.
[2] Ponomarev K. I., "On one statistical model of steganography", *Discrete Math. Appl.*, **19**:3 (2009), 329–336.
[3] Ker A., "A capacity result for batch steganography", *IEEE Signal Process. Lett.*, **14**:8 (2007), 525–528.
[4] Shoytov A.M., "On the fact of detecting the noise in finite Markov chain with an unknown transition probability matrix", Prikl. Diskr. Mat., 2010, № Supplement № 3, 44–45 (in Russian).
[5] Kharin Yu. S., Vecherko E. V., "Statistical estimation of parameters for binary Markov chain models with embeddings", *Discrete Math. Appl.*, **23**:2 (2013), 153–169.
[6] Zubkov A. M., "Pseudorandom number generatgors and its applications", Proc. II Int. Sci. Conf. "Mathematics and security of information technologies", 2003, 200–206.
[7] Kemeny J. G., Snell J. L., *Finite Markov chains*, Van Nostrand, 1960.
[8] Ivanov V.A., "Models of inclusions into homogeneous random sequences", Tr. Diskr. Mat., **10** (2008), 18–34 (in Russian).

[9] *A statistical test suite for random and pseudorandom number generators for cryptographic applicatiions: NIST Special Publication 800-22 Rev. 1a.*, Nat. Inst. Stand. Technol., 2010.
[10] Doukhan P., *Mixing: properties and examples*, Springer-Verlag, 1994.
[11] Kharin Yu. S., Voloshko V. A., "Robust estimation of AR coefficients under simultaneously influencing outliers and missing values", *J. Statist. Plan. Infer.*, **141**:9 (2011), 3276-3288.
[12] Ivchenko G. I., Medvedev Yu. I., *Mathematical statistics*, Vysshaya shkola, Moscow, 1984 (in Russian).
[13] Wald A., "Tests of statistical hypotheses concerning several parameters when the number of observations is large", Trans. Amer. Math. Soc., **54**:3 (1943), 426–482.
[14] Rabiner L. R., "A tutorial on hidden Markov models and selected applications in speech recognition", Proc. IEEE, **77**:2 (1989), 257–286.
[15] Kharin Yu. S., Petlitskiy A. I., "A Markov chain of order s with r partial connections and statistical inference on its parameters", *Discrete Math. Appl.*, **17**:3 (2007), 295–317.