

Math-Net.Ru

Общероссийский математический портал

Ю. С. Харин, Е. В. Вечерко, Статистическое оценивание параметров модели вкраплений в двоичную цепь Маркова, *Дискрет. матем.*, 2013, том 25, выпуск 2, 135–148

<https://www.mathnet.ru/dm1241>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<https://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 216.73.216.37

14 декабря 2025 г., 19:35:40



Статистическое оценивание параметров модели вкраплений в двоичную цепь Маркова

© 2013 г. Ю. С. Харин, Е. В. Вечерко

В статье рассматриваются математические модели вкраплений в двоичную цепь Маркова, возникающие в задачах стеганографии. Построены и исследованы статистические оценки модельных параметров, основанные на частотных статистиках и выборочных корреляциях. Разработан полиномиальный алгоритм вычисления функции правдоподобия, на основе которого построены оценки максимального правдоподобия. Представлены результаты компьютерных экспериментов.

1. Введение

В настоящее время стеганография стремительно развивается и используется при решении задач защиты информации [1, 4, 3, 6, 5, 2, 7, 8]. Несмотря на большое число публикаций, в литературе недостаточно внимания уделено теоретическим аспектам стеганографической защиты информации. Вероятностно-статистические аспекты стеганографии мало изучены, поэтому проблема построения и анализа математических моделей вкраплений (встраивания сообщений в контейнеры) актуальна [7, 9].

В качестве математических моделей контейнеров в стеганографии могут использоваться двоичные случайные последовательности и случайные поля. Использование схемы независимых испытаний Бернулли в качестве модели контейнера позволяет построить статистические критерии обнаружения вкраплений [7] и теоретически оценить их мощности. Однако эта модель не учитывает существующих зависимостей в реальных статистических данных, используемых в качестве контейнеров. В данной статье используется обобщение модели из [7] – марковская модель зависимости.

Целью данной статьи является исследование вероятностных свойств и статистическое оценивание параметров для моделей двоичной цепи Маркова с вкраплениями.

Статья имеет следующую структуру. В разделе 2 дается обоснование марковской модели вкраплений и двух ее частных случаев: классической модели побитового вкрапления и новой модели q -блочного вкрапления. Раздел 3 содержит результаты по вероятностным распределениям s -грамм и статистическим оценкам параметров на основе этих распределений для модели побитового вкрапления. Раздел 4 посвящен оценкам максимального правдоподобия параметров для модели побитового вкрапления, а раздел 5 – для модели блочного вкрапления. В разделе 6 теоретические результаты иллюстрируются результатами компьютерных экспериментов.

2. Математические модели цепи Маркова с вкраплениями

Введем обозначения: $V = \{0, 1\}$ – двоичный алфавит, V_T – пространство двоичных T -мерных векторов, \mathbb{N} – множество натуральных чисел, $I\{A\}$ – индикатор события A , $u_{t_1}^{t_2} = (u_{t_1}, \dots, u_{t_2}) \in V_{t_2-t_1+1}$ ($t_1, t_2 \in \mathbb{N}$, $t_1 \leq t_2$) – двоичная строка из $t_2 - t_1 + 1$ символов, $w(\cdot)$ – вес Хемминга, $\mathfrak{L}\{\xi\}$ – закон распределения вероятностей случайной величины ξ , $\mathfrak{B}(\theta)$ – закон распределения вероятностей Бернулли с параметром $\theta \in [0, 1]$: $\mathbf{P}\{\xi = 1\} = 1 - \mathbf{P}\{\xi = 0\} = \theta$.

Будем предполагать, что контейнер для встраивания сообщения есть двоичная последовательность $x_1^T = (x_1, x_2, \dots, x_T) \in V_T$, $x_t \in V$, $t = 1, \dots, T$, являющаяся однородной двоичной цепью Маркова 1-го порядка с матрицей вероятностей одношаговых переходов $P = (p_{v_0, v_1})$, $v_0, v_1 \in V$:

$$P = P(\varepsilon) = \frac{1}{2} \begin{pmatrix} 1 + \varepsilon & 1 - \varepsilon \\ 1 - \varepsilon & 1 + \varepsilon \end{pmatrix},$$

$$p_{v_0, v_1} = \mathbf{P}\{x_{t+1} = v_1 | x_t = v_0\} = \frac{1}{2}(1 + (-1)^{v_0 + v_1} \varepsilon), \quad |\varepsilon| < 1. \quad (1)$$

Здесь ε – параметр модели: случай $\varepsilon = 0$ соответствует схеме независимых испытаний и исследован в [7]; случай $\varepsilon > 0$ учитывает зависимость типа притяжения, $\varepsilon < 0$ – зависимость типа отталкивания. Отметим, что цепь Маркова (2) удовлетворяет условиям эргодичности [10] и имеет равномерное стационарное распределение вероятностей $\pi = (1/2, 1/2)$. Далее будем полагать, что цепь Маркова (2) является стационарной, то есть ее начальное распределение совпадает с π .

Отметим, что представленная модель контейнера достаточно хорошо согласуется с реальными статистическими данными. Например, при анализе 10^2 случайно выбранных 512×512 изображений в градациях серого из базы данных [8] установлено, что $|\mathbf{P}\{x_t = 1\} - \frac{1}{2}| \leq 0.0021$, а оценка для параметра ε равна 0.07.

Обычно до встраивания в контейнер сообщение подвергается криптографическому преобразованию [11], устраняющему статистическую избыточность, поэтому далее полагаем, что сообщение $\xi_1^M = (\xi_1, \dots, \xi_M) \in V_M$, $M \leq T$, является последовательностью M независимых случайных величин Бернулли:

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

На практике, как правило ([11]), $\{\xi_t\}$ имеет симметричное распределение вероятностей: $\theta_1 = \theta_0 = 1/2$.

Стегослуж $\gamma_1^T = (\gamma_1, \dots, \gamma_T) \in V_T$, определяет моменты времени, в которые биты сообщения ξ_1^M вкрапляются в последовательность x_1^T . Так как V – двоичный алфавит, то распространенные в стеганографии методы вкрапления информации “LSB replacement” и “ ± 1 embedding” [12] тождественны и имеют вид:

$$Y_t = \gamma_t \xi_{\tau_t} + (1 - \gamma_t) x_t = \begin{cases} x_t, & \text{если } \gamma_t = 0, \\ \xi_{\tau_t}, & \text{если } \gamma_t = 1, \end{cases} \quad (3)$$

где $Y_1^T = (Y_1, \dots, Y_T)$ – случайная стегопоследовательность, содержащая сообщение, $\tau_t = \sum_{j=1}^t \gamma_j \leq M$ при $\gamma_t = 1$ определяет номер бита сообщения ξ_{τ_t} для вкрапления в момент времени t .

Будем полагать, что стегоключ (ключевая последовательность) $\gamma_1^T = (\gamma_1, \dots, \gamma_T)$ есть последовательность независимых случайных величин, имеющих бернуллиевский закон распределения вероятностей:

$$\mathfrak{L}\{\gamma_t\} = \mathfrak{B}(\delta), \quad \mathbf{P}\{\gamma_t = 1\} = 1 - \mathbf{P}\{\gamma_t = 0\} = \delta, \quad t = 1, \dots, T. \quad (4)$$

Введем в рассмотрение еще одну специальную q -блочную модель стегоключа ($q \in \mathbb{N}$) при $T = Kq$, которая при $q = 1$ совпадает с (4). Для этого вначале разобьем последовательность x_1^T на блоки длины $q > 1$ ($T = Kq$, $K \in \mathbb{N}$): $x_{(1)} = x_1^q, x_{(2)} = x_{q+1}^{2q}, \dots, x_{(K)} = x_{(K-1)q+1}^{Kq}$. Введем вспомогательные независимые случайные величины $\zeta_k \in V$, $\mathfrak{L}\{\zeta_k\} = \mathfrak{B}(\delta)$, $k = 1, \dots, K$, которые отвечают за выбор блоков $\{x_{(k)}\}$ для вкрапления сообщения: если $\zeta_k = 1$, то в один из наудачу выбранных битов блока $x_{(k)}$ вкрапляется один бит сообщения, иначе вкрапление не производится. Сразу же отметим, что для такой модели стегоключа максимальная пропускная способность стegosистемы уменьшается до $K = T/q$ бит. В дальнейшем будем рассматривать случай $q = 2$ (случай $q > 2$ исследуется аналогично).

При $q = 2$ стегоключ γ_1^T состоит из независимых пар:

$$(\gamma_{2k-1}, \gamma_{2k}) = \begin{cases} (0, 0), & \text{если } \zeta_k = 0, \\ (0, 1), & \text{если } \zeta_k = 1, \eta_{\tau_k} = 0, \\ (1, 0), & \text{если } \zeta_k = 1, \eta_{\tau_k} = 1, \end{cases} \quad k = 1, \dots, K, \quad (5)$$

где $\{\eta_k\}$ – независимые двоичные случайные величины с распределением вероятностей $\mathfrak{L}\{\eta_k\} = \mathfrak{B}(1/2)$, $\tau_k = \sum_{j=1}^k \zeta_j$. Отметим, что при таком построении стегоключей мощность множества всевозможных стегоключей уменьшается до $3^{T/2} < 2^T$. С учетом (5) для условных вероятностей $q_{t,u_0,u_1} = \mathbf{P}\{\gamma_t = u_1 | \gamma_{t-1} = u_0\}$, $u_0, u_1 \in V$, справедливы соотношения

$$q_{2k-1,u_0,u_1} = \begin{pmatrix} 1 - \delta/2 & \delta/2 \\ 1 - \delta/2 & \delta/2 \end{pmatrix}_{u_0,u_1}, \quad q_{2k,u_0,u_1} = \begin{pmatrix} 1 - \delta(2 - \delta)^{-1} & \delta(2 - \delta)^{-1} \\ 1 & 0 \end{pmatrix}_{u_0,u_1}. \quad (6)$$

Здесь учтено, что по построению γ_{2k-1} и γ_{2k-2} независимы.

Случайные последовательности $\{x_t\}$, $\{\xi_t\}$, $\{\gamma_t\}$ предполагаются независимыми в совокупности.

Заметим, что с практической точки зрения наибольшего внимания в рамках рассматриваемой здесь марковской модели вкрапления (2)–(5) заслуживает наиболее трудный для стегоаналитика случай $\theta_0 = \theta_1 = 1/2$ в (2), так как в этом случае при вкраплении одномерное распределение вероятностей не искажается: $\mathbf{P}\{x_t = 1\} = \mathbf{P}\{x_t = 0\} = \mathbf{P}\{\xi_t = 1\} = \mathbf{P}\{\xi_t = 0\} = 1/2$, $t = 1, 2, \dots, T$.

3. Распределения вероятностей s -грамм и основанные на них оценки параметров ε, δ для модели побитового вкрапления

Рассмотрим s -мерные распределения стегопоследовательности $\{Y_t\}$ ($s \in \mathbb{N}$):

$$p_{v_0, \dots, v_{s-1}}^{(s)} = \mathbf{P}\{Y_t = v_0, \dots, Y_{t+s-1} = v_{s-1}\} = \mathbf{P}\{Y_t^{t+s-1} = v_0^{s-1}\} \in V, \quad t \in \mathbb{N}.$$

Воспользуемся известным вспомогательным утверждением [13].

Лемма 1. Если $P = \frac{1}{2} \begin{pmatrix} 1 + \varepsilon & 1 - \varepsilon \\ 1 - \varepsilon & 1 + \varepsilon \end{pmatrix}$, $|\varepsilon| \leq 1$, то для любого натурального $k \in \mathbb{N}$ справедливо соотношение

$$P^k = \frac{1}{2} \begin{pmatrix} 1 + \varepsilon^k & 1 - \varepsilon^k \\ 1 - \varepsilon^k & 1 + \varepsilon^k \end{pmatrix}, (P^k)_{v_0, v_1} = \frac{1}{2}(1 + (-1)^{v_0 + v_1} \varepsilon^k), \quad v_0, v_1 \in V. \quad (7)$$

Теорема 1. Если имеет место модель побитового вкрапления (2)-(4), то для s -мерных распределений вероятностей стегопоследовательности $\{Y_t\}$ при $s \in \{1, 2, 3\}$ справедливы формулы

$$p_{v_0}^{(1)} = (1 - \delta)/2 + \delta\theta_{v_0}, \quad (8)$$

$$p_{v_0, v_1}^{(2)} = (1 - \delta)^2 p_{v_0, v_1}/2 + \delta(1 - \delta)(\theta_{v_1} + \theta_{v_0})/2 + \delta^2 \theta_{v_0} \theta_{v_1}, \quad (9)$$

$$p_{v_0, v_1, v_2}^{(3)} = (1 - \delta)^3 p_{v_0, v_1, v_2}/2 + \delta(1 - \delta)^2 (\theta_{v_0} p_{v_1, v_2} + \theta_{v_1} (P^2)_{v_0, v_2} + \theta_{v_2} p_{v_0, v_1})/2 + \\ + \delta^2 (1 - \delta) (\theta_{v_0} \theta_{v_1} + \theta_{v_0} \theta_{v_2} + \theta_{v_1} \theta_{v_2})/2 + \delta^3 \theta_{v_0} \theta_{v_1} \theta_{v_2}, \quad v_0, v_1, v_2 \in V. \quad (10)$$

Доказательство. По формуле полной вероятности с учетом (2)-(4) и независимости последовательностей $\{x_t\}$, $\{\xi_t\}$, $\{\gamma_t\}$ имеем цепочку равенств:

$$p_{v_0, v_1}^{(2)} = \mathbf{P}\{Y_t = 1, Y_{t+1} = 1\} = \\ = \mathbf{P}\{\gamma_t = 0, \gamma_{t+1} = 0\} \mathbf{P}\{x_t = v_0, x_{t+1} = v_1 | \gamma_t = 0, \gamma_{t+1} = 0\} + \\ + \mathbf{P}\{\gamma_t = 0, \gamma_{t+1} = 1\} \mathbf{P}\{x_t = v_0, \xi_{t+1} = v_1 | \gamma_t = 0, \gamma_{t+1} = 1\} + \\ + \mathbf{P}\{\gamma_t = 1, \gamma_{t+1} = 0\} \mathbf{P}\{\xi_{t+1} = v_0, x_{t+1} = v_1 | \gamma_t = 1, \gamma_{t+1} = 0\} + \\ + \mathbf{P}\{\gamma_t = 1, \gamma_{t+1} = 1\} \mathbf{P}\{\xi_{t+1} = v_0, \xi_{t+2} = v_1 | \gamma_t = 1, \gamma_{t+1} = 1\} = \\ = (1 - \delta)^2 p_{v_0, v_1}/2 + \delta(1 - \delta)(\theta_{v_1} + \theta_{v_0})/2 + \delta^2 \theta_{v_0} \theta_{v_1},$$

что совпадает с (9). Просуммировав по компоненте $v_1 \in V$, получаем: $p_{v_0}^{(1)} = \sum_{v_1=0}^1 p_{v_0, v_1}^{(2)} = (1 - \delta)^2/2 + \delta(1 - \delta)(1/2 + \theta_{v_0}) + \delta^2 \theta_{v_0} = (1 - \delta)/2 + \delta\theta_{v_0}$, что совпадает с (8).

Соотношение (10) выводится аналогично.

Заметим, что если $\theta_0 = \theta_1 = 1/2$, то $p_v^{(1)}$ не зависит от $v \in V$: $p_0^{(1)} = p_1^{(1)} = 1/2$. Это означает, что одномерное распределение вероятностей стегопоследовательности $\{Y_t\}$ не несет никакой информации о параметрах модели ε, δ . Отметим еще, что стегопоследовательность $\{Y_t\}$ при $\delta > 0$, вообще говоря, не является цепью Маркова 1-го порядка, так как в общем случае в силу (8)-(10) нарушается марковское свойство: $p_{v_0, v_1, v_2}^{(3)} \neq p_{v_0, v_1}^{(2)} \cdot p_{v_1, v_2}^{(2)} / p_{v_1}^{(1)}$.

Будем далее рассматривать наиболее трудный для стегоаналитика случай, когда одномерные распределения вероятностей контейнера и сообщения совпадают: $\theta_0 = \theta_1 = 1/2$. Тогда согласно (9) двумерное ($s = 2$) распределение вероятностей стегопоследовательности $\{Y_t\}$ имеет вид $p_{v_0, v_1}^{(2)} = (1 - \delta)^2(1 + (-1)^{v_0 + v_1} \varepsilon)/4 + \delta(2 - \delta)/4$, и для определения ε, δ по $\{p_{v_0, v_1}^{(2)}\}$ имеем систему уравнений:

$$\begin{cases} p_{0,0}^{(2)} = p_{1,1}^{(2)} = 1/4 + (1 - \delta)^2 \varepsilon/4, \\ p_{0,1}^{(2)} = p_{1,0}^{(2)} = 1/4 - (1 - \delta)^2 \varepsilon/4. \end{cases} \quad (11)$$

Обозначим через $f_{v_0 \dots v_{s-1}} = \sum_{t=1}^{T-s+1} I\{Y_t^{t+s-1} = v_0^{s-1}\}$ абсолютную частоту s -граммы, $(v_0, \dots, v_{s-1}) \in V_s$. Из (11) при известном $\delta < 1$ получаем подстановочную (plug-in) оценку параметра ε , являющуюся функцией частот биграмм $\{f_{v_0 v_1}\}$ при $s = 2$:

$$\hat{\varepsilon} = g_0 \left(\frac{f_{00}}{T-1}, \frac{f_{11}}{T-1}, \frac{f_{01}}{T-1}, \frac{f_{10}}{T-1} \right) = \frac{f_{00} + f_{11} - f_{01} - f_{10}}{(1-\delta)^2(T-1)}. \quad (12)$$

Теорема 2. Для модели вкраплений (2)-(4) при $\delta < 1$ статистика (12) является несмещенной и состоятельной при $T \rightarrow \infty$ оценкой параметра модели ε : $\mathbf{E}\{\hat{\varepsilon}\} = \varepsilon$, $\hat{\varepsilon} \xrightarrow{P} \varepsilon$.

Доказательство. В силу (9) для модели (2)-(4) имеем:

$$\mathbf{E}\{f_{v_0 v_1}\} = (T-1)p_{v_0 v_1}^{(2)} = (T-1)(1 + (-1)^{v_0+v_1}(1-\delta)^2\varepsilon)/4. \quad (13)$$

Из (13) следует, что оценка $\hat{\varepsilon}$ является несмещенной:

$$\mathbf{E}\{\hat{\varepsilon}\} = \mathbf{E} \left\{ \frac{f_{00} + f_{11} - f_{01} - f_{10}}{(1-\delta)^2(T-1)} \right\} = \frac{(T-1)(2 + 2(1-\delta)^2\varepsilon - (2 - 2(1-\delta)^2\varepsilon))}{4(1-\delta)^2(T-1)} = \varepsilon.$$

В силу принятых обозначений, группируя слагаемые, получаем:

$$\begin{aligned} \mathbf{E}\{f_{11}^2\} &= \sum_{t, t'=1}^{T-1} \mathbf{P}\{Y_t = Y_{t+1} = Y_{t'} = Y_{t'+1} = 1\} = (T-1)\mathbf{P}\{Y_t = Y_{t+1} = 1\} + \\ &+ 2(T-2)\mathbf{P}\{Y_t = Y_{t+1} = Y_{t+2} = 1\} + 2 \sum_{\tau=2}^{T-2} (T-1-\tau)\mathbf{P}\{Y_t = Y_{t+1} = Y_{t+\tau} = Y_{t+\tau+1} = 1\}. \end{aligned}$$

С учетом модели (2)-(4) при $\tau \geq 2$ находим:

$$\begin{aligned} \mathbf{P}\{Y_t = Y_{t+1} = Y_{t+\tau} = Y_{t+\tau+1} = 1\} &= \\ &= \sum_{u_0, \dots, u_3 \in V_4} \mathbf{P}\{\gamma_t = u_0, \gamma_{t+1} = u_1, \gamma_{t+\tau} = u_2, \gamma_{t+\tau+1} = u_3\} \times \\ &\times \mathbf{P}\{Y_t = Y_{t+1} = Y_{t+\tau} = Y_{t+\tau+1} = 1 | \gamma_t = u_0, \gamma_{t+1} = u_1, \gamma_{t+\tau} = u_2, \gamma_{t+\tau+1} = u_3\} = \\ &= (1-\delta)^4(1+2\varepsilon+\varepsilon^2+\varepsilon^{\tau-1}+2\varepsilon^\tau+\varepsilon^{\tau+1})/16 + 2\delta(1-\delta)^3(2+2\varepsilon+\varepsilon^2+\varepsilon^{\tau-1}+2\varepsilon^\tau+\varepsilon^{\tau+1})/16 + \\ &\quad \delta^2(1-\delta)^2(6+2\varepsilon+\varepsilon^{\tau-1}+2\varepsilon^\tau+\varepsilon^{\tau+1})/16 + 4\delta^3(1-\delta)/16 + \delta^4/16 = \\ &= (1+2\varepsilon(1-\delta)^2+\varepsilon^2(1-\delta)^4+(1+\varepsilon)^2(1-\delta)^2\varepsilon^{\tau-1})/16 = \\ &= (1+\varepsilon(1-\delta)^2)^2/16 + (1+\varepsilon)^2(1-\delta)^2\varepsilon^{\tau-1}/16. \end{aligned}$$

Учитывая (13), проверим выполнение достаточного условия Маркова закона больших чисел [14]:

$$\begin{aligned} \mathbf{D}\{f_{11}\}/(T-1)^2 &= \mathbf{E}\{f_{11}^2\}/(T-1)^2 - \mathbf{E}^2\{f_{11}\}/(T-1)^2 = \mathbf{E}\{f_{11}^2\}/(T-1)^2 - (p_{11}^{(2)})^2 = \\ &= \mathbf{P}\{Y_t = Y_{t+1} = 1\}/(T-1) + 2(T-1)^{-2} \left((T-2)\mathbf{P}\{Y_t = Y_{t+1} = Y_{t+2} = 1\} + \right. \\ &\quad \left. + (p_{11}^{(2)})^2 \sum_{\tau=2}^{T-2} (T-1-\tau) + (1+\varepsilon)^2(1-\delta)^2 \sum_{\tau=2}^{T-2} (T-1-\tau)\varepsilon^{\tau-1}/16 \right) - (p_{11}^{(2)})^2 \xrightarrow{T \rightarrow \infty} 0. \end{aligned}$$

Следовательно, $f_{11}/(T-1) \xrightarrow{P} p_{11}^{(2)}$. Аналогично можно показать, что $f_{v_0 v_1}/(T-1) \xrightarrow{P} p_{v_0 v_1}^{(2)}$ при всех $v_0, v_1 \in V$. Тогда из свойства непрерывности функции $g_0(z_1, z_2, z_3, z_4)$, входящей в (12), и свойств функциональных преобразований случайных последовательностей [14] следует, что оценка $\hat{\varepsilon}$ состоятельна.

Из (10) при $s = 3$ имеем: $p_{v_0, v_1, v_2}^{(3)} = 1/8 + (1 - \delta)^2((-1)^{v_1}((-1)^{v_0} + (-1)^{v_2}) + (-1)^{v_0+v_2}\varepsilon)/8$. Тогда для определения ε, δ по $\{p_{v_0, v_1, v_2}^{(3)}\}$ можно составить систему уравнений

$$\begin{cases} p_{0,0,0}^{(3)} = p_{1,1,1}^{(3)} = 1/8 + (1 - \delta)^2(2 + \varepsilon)\varepsilon/8, \\ p_{0,1,0}^{(3)} = p_{1,0,1}^{(3)} = 1/8 + (1 - \delta)^2(-2 + \varepsilon)\varepsilon/8, \\ p_{0,0,1}^{(3)} = p_{1,1,0}^{(3)} = p_{0,1,1}^{(3)} = p_{1,0,0}^{(3)} = 1/8 - (1 - \delta)^2\varepsilon^2/8. \end{cases} \quad (14)$$

Из системы уравнений (14) следует соотношение

$$(1 - \delta)^2 = (f_{000} + f_{111} + f_{010} + f_{101} - f_{001} - f_{110} - f_{011} - f_{100})/\varepsilon^2(T - 2). \quad (15)$$

Подставляя сюда оценку $\hat{\varepsilon}$, определяемую (12), и учитывая ограничение: $\delta \in [0, 1]$, получаем статистическую оценку для δ :

$$\begin{aligned} \hat{\delta} &= 1 - \sqrt{\max\{0, \min\{1, g_1\}\}}, \\ g_1 &= \frac{(f_{00} + f_{11} - f_{01} - f_{10})^2(T - 2)}{(f_{000} + f_{111} + f_{010} + f_{101} - f_{001} - f_{110} - f_{011} - f_{100})(T - 1)^2}. \end{aligned} \quad (16)$$

Теорема 3. Для модели вкраплений (2)-(4) статистика (16) является состоятельной при $T \rightarrow \infty$ оценкой параметра модели δ : $\hat{\delta} \xrightarrow{P} \delta$.

Доказательство. Проводится аналогично доказательству теоремы 2.

Исследуем теперь корреляционные свойства стегопоследовательности $\{Y_t\}$.

Теорема 4. Если имеет место модель побитового вкрапления (2)-(4) и $\theta_0 = \theta_1 = 1/2$, то корреляционная функция ρ_l стегопоследовательности $\{Y_t\}$ имеет вид

$$\rho_l = \text{Corr}\{Y_t, Y_{t+l}\} = (1 - \delta)^2\varepsilon^{|l|}, \quad l = \pm 1, \pm 2, \dots \quad (17)$$

Доказательство. Для модели (2)-(4) в силу (8) имеем: $\mathbf{E}\{Y_t\} = \mathbf{P}\{Y_t = 1\} = 1/2$, $\mathbf{D}\{Y_t\} = 1/4$. С учетом леммы 1 и доказательства теоремы 1 справедливо соотношение

$$\begin{aligned} \mathbf{E}\{Y_t Y_{t+l}\} &= \mathbf{P}\{Y_t = 1, Y_{t+l} = 1\} = \\ &= (1 - \delta)^2(1 + \varepsilon^{|l|})/4 + \delta(1 - \delta)\theta_1 + \delta^2\theta_1^2 = (1 - \delta)^2\varepsilon^{|l|}/4 + 1/4. \end{aligned}$$

Подставляя эти выражения в $\rho_l = (\mathbf{E}\{Y_t Y_{t+l}\} - \mathbf{E}^2\{Y_t\})/\mathbf{D}\{Y_t\}$, получаем (17).

Следствие 1. В условиях теоремы 4 оценки параметров ε, δ , основанные на корреляциях (17), имеют вид

$$\hat{\varepsilon} = \min\{1, \max\{-1, \hat{\rho}_2/\hat{\rho}_1\}\}, \quad \hat{\delta} = 1 - \sqrt{\max\{0, \min\{1, \hat{\rho}_1^2/\hat{\rho}_2\}\}}, \quad (18)$$

где $\hat{\rho}_l = \frac{4}{T-1} \sum_{t=1}^{T-l} I\{Y_t = 1\}I\{Y_{t+l} = 1\} - 1$ - выборочная корреляционная функция.

Следствие 2. В условиях теоремы 4 статистики (18) являются состоятельными при $T \rightarrow \infty$ оценками параметров модели ε, δ .

Доказательство. Аналогично доказательству теоремы 3.

4. Оценки максимального правдоподобия параметров ε, δ для модели побитового вкрапления

По наблюдаемой стегопоследовательности $y_1^T = (y_1, \dots, y_T) \in V_T$ построим функцию правдоподобия.

Разобьем множество V_t двоичных t -мерных векторов на $t + 1$ непересекающихся подмножеств:

$$V_t = \Gamma_0^{(t)} \cup \Gamma_1^{(t)} \cup \dots \cup \Gamma_t^{(t)}, \quad (19)$$

где

$$\begin{aligned} \Gamma_0^{(t)} &= \{u_1^t \in V_t : u_t = 1\}, \\ \Gamma_1^{(t)} &= \{u_1^t \in V_t : u_t = u_{t-1} = 0\}, \\ \Gamma_j^{(t)} &= \{u_1^t \in V_t : u_t = 0, u_{t-1} = \dots = u_{t-j+1} = 1, u_{t-j} = 0\}, \quad 1 < j < t, \\ \Gamma_t^{(t)} &= \{u_1^t \in V_t : u_t = 0, u_{t-1} = \dots = u_1 = 1\}. \end{aligned} \quad (20)$$

Разбиение (19), (20) порождает разбиение всевозможных траекторий фрагментов ключевой последовательности $\gamma_1^t = u_1^t \in V_t$ (см. рис. 1).

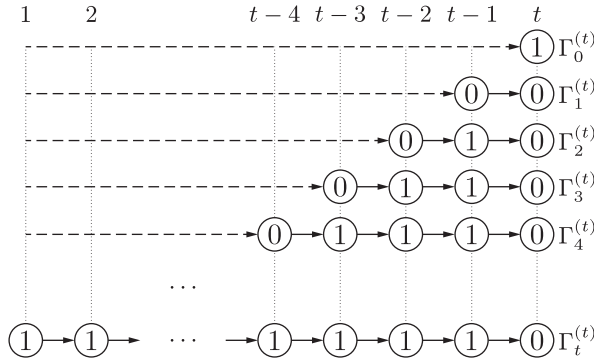


Рис. 1. Разбиение траекторий γ_1^t ; штриховая стрелка — произвольная траектория.

Используя разбиение (19),(20), определим функции двоичных переменных $u_1^t \in V_t$, $y_1^t \in V_t$ ($t \geq 1$):

$$\varphi_t(u_1^t, y_1^t) = \begin{cases} \theta_{y_t}, & u_1^t \in \Gamma_0^{(t)}, \\ \frac{1}{2}(1 + (-1)^{y_{t-j} + y_t} \varepsilon^j), & u_1^t \in \Gamma_j^{(t)}, \quad 1 \leq j < t, \\ \frac{1}{2}, & u_1^t \in \Gamma_t^{(t)}. \end{cases} \quad (21)$$

Теорема 5. Если имеет место модель побитового вкрапления (2)–(4), то функция правдоподобия $L(\varepsilon, \delta; y_1^T)$ для наблюдаемой стегопоследовательности $y_1^T \in V_T$ имеет вид:

$$L(\varepsilon, \delta; y_1^T) = \mathbf{P}\{Y_1^T = y_1^T\} = \sum_{u_1^T \in V_T} \delta^{w(u_1^T)} (1 - \delta)^{T - w(u_1^T)} \prod_{t=1}^T \varphi_t(u_1^t, y_1^t). \quad (22)$$

Доказательство. С учетом (3), (4) и принятых обозначений имеем:

$$\begin{aligned} L(\varepsilon, \delta; y_1^T) &= \mathbf{P}\{Y_1^T = y_1^T\} = \sum_{u_1^T \in V_T} \mathbf{P}\{\gamma_1^T = u_1^T\} L_{u_1, \dots, u_T}(\varepsilon; y_1^T) = \\ &= \sum_{u_1^T \in V_T} \delta^{w(u_1^T)} (1 - \delta)^{T-w(u_1^T)} L_{u_1, \dots, u_T}(\varepsilon; y_1^T) = \mathbf{E}\{L_{\gamma_1, \dots, \gamma_T}(\varepsilon; y_1^T)\}, \end{aligned}$$

где $L_{u_1, \dots, u_T}(\varepsilon; y_1^T) = \mathbf{P}\{Y_1^T = y_1^T | \gamma_1^T = u_1^T\}$ – условная функция правдоподобия (при условии, что стегоключ $\gamma_1^T = u_1^T \in V_T$):

$$\begin{aligned} L_{u_1, \dots, u_T}(\varepsilon; y_1^T) &= \mathbf{P}\{Y_1 = y_1 | \gamma_1 = u_1\} \mathbf{P}\{Y_2 = y_2 | Y_1 = y_1, \gamma_1^2 = u_1^2\} \times \dots \\ &\quad \dots \times \mathbf{P}\{Y_T = y_T | Y_1^{T-1} = y_1^{T-1}, \gamma_1^T = u_1^T\} = \\ &= \mathbf{P}\{Y_1 = y_1 | \gamma_1 = u_1\} \prod_{t=2}^T \mathbf{P}\{Y_t = y_t | Y_1^{t-1} = y_1^{t-1}, \gamma_1^t = u_1^t\}. \end{aligned}$$

Первый сомножитель в правой части этого равенства в силу (2)-(4) и независимости ξ_1, γ_1 равен

$$\mathbf{P}\{Y_1 = y_1 | \gamma_1 = u_1\} = \begin{cases} \mathbf{P}\{\xi_1 = y_1 | \gamma_1 = 1\} = \theta_{y_1}, & u_1 = 1, \\ \mathbf{P}\{x_1 = y_1 | \gamma_1 = 0\} = 1/2, & u_1 = 0. \end{cases}$$

Во втором сомножителе, используя лемму 1, обозначения (19)-(21), независимость $\{x_t\}$, $\{\gamma_t\}$ и $\{\xi_t\}$, получаем для $t \geq 2$:

$$\begin{aligned} \mathbf{P}\{Y_t = y_t | Y_1^{t-1} = y_1^{t-1}, \gamma_1^t = u_1^t\} &= \varphi_t(u_1^t, y_1^t) = \\ &= \begin{cases} \mathbf{P}\{\xi_t = y_t | Y_1^{t-1} = y_1^{t-1}, \gamma_t = 1, \gamma_1^{t-1} = u_1^{t-1}\}, & u_1^t \in \Gamma_0^{(t)}, \\ \mathbf{P}\{x_t = y_t | \xi_{t-j+1}^{t-1} = y_{t-j+1}^{t-1}, x_{t-j} = y_{t-j}, Y_1^{t-j-1} = y_1^{t-j-1}, \gamma_1^t = u_1^t\}, & u_1^t \in \Gamma_j^{(t)}, 1 \leq j < t, \\ \mathbf{P}\{x_t = y_t | \xi_1^{t-1} = y_1^{t-1}, \gamma_t = 0, \gamma_{t-1} = \dots = \gamma_1 = 1\}, & u_1^t \in \Gamma_t^{(t)}. \end{cases} \end{aligned}$$

Объединяя эти выражения, приходим к (22).

Следствие 3. Оценки максимального правдоподобия (МП-оценки) $\hat{\varepsilon}, \hat{\delta}$ параметров ε, δ определяются как решение экстремальной задачи

$$L(\varepsilon, \delta; y_1^T) = \mathbf{E}\{L_{\gamma_1, \dots, \gamma_T}(\varepsilon; y_1^T)\} \rightarrow \max_{\varepsilon \in (-1, 1), \delta \in [0, 1]}. \quad (23)$$

Следствие 4. В частном случае отсутствия вкраплений ($\delta = 0, \gamma_t \equiv 0$) МП-оценка параметра ε совпадает с ранее полученной частотной оценкой (12):

$$\hat{\varepsilon}_0 = \frac{f_{00} + f_{11} - f_{01} - f_{10}}{T - 1}; \quad (24)$$

эта оценка является несмещенной и при $T \rightarrow \infty$, $\varepsilon \in (-1, 1)$, имеет асимптотически нормальное распределение вероятностей: $\mathfrak{L}\{\sqrt{T-1}(\hat{\varepsilon}_0 - \varepsilon)\} \rightarrow N(0, 1 - \varepsilon^2)$.

Доказательство. МП-оценка находится максимизацией логарифмической функции правдоподобия:

$$\begin{aligned} l(\varepsilon, 0; y_1^T) &\stackrel{\text{def}}{=} \log L(\varepsilon, 0; y_1^T) = \log L_{0,\dots,0}(\varepsilon; y_1^T) = \log \mathbf{P}\{Y_1^T = y_1^T | \gamma_1 = 0, \dots, \gamma_T = 0\} = \\ &= \log \mathbf{P}\{x_1^T = y_1^T\} = \log \pi_{y_1} + \sum_{t=2}^T \log p_{y_{t-1}, y_t} = \log \pi_{y_1} + \sum_{v_0, v_1=0}^1 f_{v_0 v_1} \log p_{v_0, v_1}(\varepsilon) = \\ &= -\log 2 + (f_{00} + f_{11}) \log(1 + \varepsilon) + (f_{01} + f_{10}) \log(1 - \varepsilon) - (T - 1) \log 2 \rightarrow \max_{\varepsilon \in (-1, 1)}. \end{aligned}$$

Из уравнения $l'(\varepsilon, 0; y_1^T) = 0$ получаем единственное решение (24), которое соответствует точке максимума.

Несмещенность оценки следует из теоремы 2 при $\delta = 0$.

Используя теоремы о функциональных преобразованиях асимптотически нормальных статистик из [14], получаем, что оценка $\hat{\varepsilon}$ асимптотически нормальна при $T \rightarrow \infty$ и что $1 - \varepsilon^2$ является асимптотической дисперсией этой оценки.

Из-за существенной нелинейности решение экстремальной задачи (23) возможно только численными методами (например, методом табулирования $L(\varepsilon, \delta; y_1^T)$ на сетке или методом градиентного спуска), требующими вычисления функции правдоподобия для заданной последовательности точек. Согласно определению (22), вычисление одного значения функции правдоподобия $L(\varepsilon, \delta; y_1^T)$ при фиксированных параметрах ε, δ имеет вычислительную сложность порядка $O(T2^T)$, т. е. экспоненциальную сложность относительно длины стегапоследовательности.

Отметим, что для численной оценки функции правдоподобия можно применить метод Монте-Карло: $\tilde{L}(\varepsilon, \delta, K; y_1^T) = \frac{1}{K} \sum_{k=1}^K L_{u_1^{(k)}, \dots, u_T^{(k)}}(\varepsilon; y_1^T)$, где K – число имитаций, $(u_1^{(k)}, \dots, u_T^{(k)}) \in V_T - k$ -я реализация стегаключа γ_1^T , $\mathbf{P}\{\gamma = (u_1^{(k)}, \dots, u_T^{(k)})\} = \delta \sum_{t=1}^T u_t^{(k)} (1 - \delta)^{T - \sum_{t=1}^T u_t^{(k)}}$. Вычислительная сложность этого алгоритма имеет порядок $O(KT)$. При этом имеет место случайная ошибка вычисления значения функции правдоподобия, для которой среднеквадратическое отклонение имеет порядок $O(1/\sqrt{K})$.

5. Оценивание параметров ε, δ для модели блочного вкрапления

Использование модели блочного вкрапления (2)-(3), (5) позволяет построить алгоритмы вычисления функции правдоподобия и оценок максимального правдоподобия $\hat{\varepsilon}, \hat{\delta}$, имеющие полиномиальную относительно длины стегапоследовательности T сложность.

Лемма 2. Если имеет место блочная модель (5) ключевой последовательности $\{\gamma_t\}$, то при $t > 3$

$$\mathbf{P} \left\{ \gamma_1^t \in \bigcup_{j>3} \Gamma_j^{(t)} \right\} = 0, \quad (25)$$

и стегапоследовательность $\{Y_t\}$, определяемая (2)-(3), при фиксированной последовательности $\{\gamma_t\}$ является управляемой цепью Маркова условного порядка

$s_t \in \{0, 1, 2, 3\}$, причем порядок s_t зависит от ключевой последовательности $\{\gamma_t\}$:

$$s_t = j, \text{ если } u_1^t \in \Gamma_j^{(t)}. \quad (26)$$

Доказательство. Соотношение (25) вытекает из (5) и обозначений (20). Для доказательства (26) достаточно проверить марковское свойство последовательности Y_t при фиксированной управляющей последовательности γ_t аналогично ходу доказательства теоремы 5:

$$\begin{aligned} \mathbf{P}\{Y_t = y_t | Y_1^{t-1} = y_1^{t-1}, \gamma_1^t = u_1^t\} &= p_{y_{t-3}, y_{t-2}, y_{t-1}, y_t}(u_{t-3}^t) = \\ &= \begin{cases} \theta_{y_t}, & u_1^t \in \Gamma_0^{(t)}, \\ \frac{1}{2}(1 + (-1)^{y_{t-j} + y_t} \varepsilon^j), & u_1^t \in \Gamma_j^{(t)}, 1 \leq j \leq 3. \end{cases} \end{aligned} \quad (27)$$

Следствие 5. Если $\theta_0 = \theta_1 = 1/2$, то 8×2 — матрица усредненных по γ_{t-3}^t вероятностей одношаговых переходов управляемой цепи Маркова 3-го порядка имеет вид

$$\bar{P}_t = (\bar{p}_{y_{t-3}, y_{t-2}, y_{t-1}, y_t}) = \begin{cases} \begin{pmatrix} CA_{2k} & 1_8 - CA_{2k} \end{pmatrix}, & t = 2k, k \in \mathbb{N}, \\ \begin{pmatrix} CA_{2k-1} & 1_8 - CA_{2k-1} \end{pmatrix}, & t = 2k-1, k \in \mathbb{N}, \end{cases} \quad (28)$$

где $1_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}'$,

$$\begin{aligned} A_{2k} &= \begin{pmatrix} 1/2 \\ \varepsilon(1-\delta)/2 \\ \varepsilon^2\delta(1-\delta/2)/4 \\ \varepsilon^3\delta^2/8 \end{pmatrix}, & C &= \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & -1 \end{pmatrix}. \\ A_{2k-1} &= \begin{pmatrix} 1/2 \\ \varepsilon(1-\delta+\delta^2/4)/2 \\ \varepsilon^2\delta(1-\delta/2)/4 \\ 0 \end{pmatrix}, \end{aligned}$$

Доказательство. Имеем по определению:

$$\bar{p}_{y_{t-3}, y_{t-2}, y_{t-1}, y_t} = \sum_{j=0}^3 \mathbf{P}\{\gamma_1^t \in \Gamma_j^{(t)}\} p_{y_{t-3}, y_{t-2}, y_{t-1}, y_t}(u_{t-3}^t).$$

Подставляя сюда (27) и следующие из (5) значения вероятностей

$$\mathbf{P}\{\gamma_1^{2k} \in \Gamma_j^{(2k)}\} = \begin{cases} \frac{\delta}{2}, & j = 0, \\ 1 - \delta, & j = 1, \\ \delta \frac{1-\delta}{2}, & j = 2, \\ \frac{\delta^2}{4}, & j = 3, \end{cases} \quad \mathbf{P}\{\gamma_1^{2k-1} \in \Gamma_j^{(2k-1)}\} = \begin{cases} \frac{\delta}{2}, & j = 0, \\ 1 - \delta + \frac{\delta^2}{4}, & j = 1, \\ \delta \frac{1-\delta}{2}, & j = 2, \\ 0, & j = 3, \end{cases}$$

получаем (28).

Заметим, что аналогично (12), (16) соотношение (28) удобно использовать при построении частотных оценок параметров ε, δ для блочной модели (5) ключевой последовательности $\{\gamma_t\}$.

Используя лемму 2, построим полиномиальный относительно T алгоритм вычисления функции правдоподобия для блочной модели стежокляча (5), основанный на алгоритме “Forward” [16].

Для этого вначале аналогично (22) построим функцию правдоподобия для блочной модели стежокляча (5):

$$L(\varepsilon, \delta; y_1^T) = \sum_{u_1^T \in V_T} I\{b_2(u_1^T) = 0\} (1 - \delta)^{b_0(u_1^T)} (\delta/2)^{b_1(u_1^T)} \prod_{t=1}^T \varphi_t(u_1^t, y_1^t), \quad (29)$$

где $b_k(u_1^T) = \sum_{t=1}^{T/2} I\{w(u_{2t-1}, u_{2t}) = k\}$, $k \in \{0, 1, 2\}$.

Заметим, что согласно лемме 2 в сумме (29) исключаются слагаемые, для которых $u_1^t \in \bigcup_{j>3} \Gamma_j^{(t)}$, поэтому функция $\varphi_t(u_1^t, y_1^t) = p_{y_{t-3}, y_{t-2}, y_{t-1}, y_t}(u_{t-3}^t)$ фактически зависит только от u_{t-3}^t, y_{t-3}^t .

Пусть $r \in \mathbb{N}$ – вспомогательный параметр, $\alpha_t(u_0, \dots, u_{r-1}) = \mathbf{P}\{Y_1 = y_1, \dots, Y_t = y_t, \gamma_{t-r+1} = u_0, \dots, \gamma_t = u_{r-1}\}$, $t > r$, – это вероятность наблюдения последовательности y_1, \dots, y_t до момента времени t и состояний стежокляча u_0, \dots, u_{r-1} в моменты времени $t - r + 1, \dots, t$.

Теорема 6. Если имеет место модель блочного вкрапления (2)-(3), (5), $r \geq 3$, то для $\alpha_t(u_0, \dots, u_{r-1})$, при $t = r + 1, r + 2, \dots, T$ справедливо рекуррентное соотношение

$$\alpha_t(u_0, \dots, u_{r-1}) = q_{t, u_{r-2}, u_{r-1}} \sum_{u_{-1} \in V} \alpha_{t-1}(u_{-1}, \dots, u_{r-2}) p_{y_{t-3}, y_{t-2}, y_{t-1}, y_t}(u_{r-4}^{r-1}), \quad (30)$$

где $\{q_{t, i, j}\}$ определяются формулой (6).

Доказательство. По построению $\gamma_t, \gamma_{t'}$ зависимы лишь тогда, когда они принадлежат одному и тому же блоку, т.е. $t = 2k - 1, t' = 2k$ или $t = 2k, t' = 2k - 1$ при некотором $k \in \mathbb{N}$, поэтому с учетом (5) по формуле полной вероятности имеем:

$$\begin{aligned} \alpha_t(u_0, \dots, u_{r-1}) &= \mathbf{P}\{Y_1^t = y_1^t, \gamma_{t-r+1} = u_0, \dots, \gamma_t = u_{r-1}\} = \\ &= \sum_{u_{-1} \in V} \mathbf{P}\{Y_1^t = y_1^t, \gamma_{t-r} = u_{-1}, \gamma_{t-r+1} = u_0, \dots, \gamma_t = u_{r-1}\} = \\ &= \sum_{u_{-1} \in V} \mathbf{P}\{Y_1^{t-1} = y_1^{t-1}, \gamma_{t-r} = u_{-1}, \gamma_{t-r+1} = u_0, \dots, \gamma_{t-1} = u_{r-2}\} \times \\ &\times \mathbf{P}\{\gamma_t = u_{r-1} | Y_1^{t-1} = y_1^{t-1}, \gamma_{t-r} = u_{-1}, \gamma_{t-r+1} = u_0, \dots, \gamma_{t-1} = u_{r-2}\} \times \\ &\times \mathbf{P}\{Y_t = y_t | Y_1^{t-1} = y_1^{t-1}, \gamma_{t-r} = u_{-1}, \gamma_{t-r+1} = u_0, \dots, \gamma_t = u_{r-1}\} = \\ &= \sum_{u_{-1} \in V} \alpha_{t-1}(u_{-1}, u_0, \dots, u_{r-2}) \mathbf{P}\{\gamma_t = u_{r-1} | \gamma_{t-1} = u_{r-2}\} \times \\ &\times \mathbf{P}\{Y_t = y_t | Y_1^{t-1} = y_1^{t-1}, \gamma_{t-r} = u_{-1}, \gamma_{t-r+1} = u_0, \dots, \gamma_t = u_{r-1}\}. \end{aligned}$$

В силу 2 справедливо соотношение

$$\mathbf{P}\{Y_t = y_t | Y_1^{t-1} = y_1^{t-1}, \gamma_{t-r} = u_{-1}, \dots, \gamma_t = u_{r-1}\} = p_{y_{t-3}, y_{t-2}, y_{t-1}, y_t}(u_{r-4}^{r-1}).$$

В результате получаем (30).

Начальные вероятности $\alpha_t(u_0, \dots, u_{t-1})$ при $t = 1, \dots, r$ имеют вид

$$\begin{aligned}\alpha_1(u_0) &= q_{1,0,u_0} \varphi_1(u_0, y_1), \\ \alpha_t(u_0, \dots, u_{t-1}) &= \alpha_{t-1}(u_1, \dots, u_{t-1}) q_{t,u_{t-2},u_{t-1}} \varphi_t(u_0^{t-1}, y_0^{t-1}), \quad 2 \leq t \leq r.\end{aligned}\quad (31)$$

Следствие 6. Функция правдоподобия $L(\varepsilon, \delta; y_1^T)$, определяемая (29), допускает следующий алгоритм вычисления при $r \geq 3$:

$$L(\varepsilon, \delta; y_1^T) = \sum_{u_0^{r-1} \in V_r} \alpha_T(u_0, \dots, u_{r-1}), \quad (32)$$

где вероятности $\{\alpha_t\}$ вычисляются рекуррентно по $t = 1, \dots, T$ согласно (30), (31). Вычислительная сложность этого алгоритма имеет порядок $O(T2^r)$.

Доказательство. Используя определение и введенные обозначения, получаем

$$\begin{aligned}L(\varepsilon, \delta; y_1^T) &= \mathbf{P}\{Y_1^T = y_1^T\} = \\ &= \sum_{u_0^{r-1} \in V_r} \mathbf{P}\{Y_1^T = y_1^T, \gamma_{T-r+1}^T = u_0^{r-1}\} = \sum_{u_0^{r-1} \in V_r} \alpha_T(u_0, \dots, u_{r-1}),\end{aligned}$$

что совпадает с (32). Вычислительная сложность алгоритма (30)-(32) относительно T определяется вычислительной сложностью рекурсии (30), (31) и имеет порядок $O(T2^r)$.

Как видно из следствия 6, вычислительная сложность растет с ростом r , поэтому на практике целесообразно использовать минимальное значение $r = 3$.

Заметим, что при больших t значения α_t могут выходить из диапазона чисел, представимых в формате с плавающей точкой, поэтому необходима процедура нормировки аналогично [16]. Для каждого $t = 1, \dots, T$ вычисляются значения $\alpha_t(u_0, \dots, u_{r-1})$, $u_0, \dots, u_{r-1} \in V$, и далее умножаются на нормировочный коэффициент $c_t = 1 / \sum_{u_0^{r-1} \in V_r} \alpha_t(u_0, \dots, u_{r-1})$. В результате получаем, что логарифмическая функция правдоподобия $\log L(\varepsilon, \delta; y_1^T)$ имеет вид:

$$\log L(\varepsilon, \delta; y_1^T) = - \sum_{t=1}^T \log c_t. \quad (33)$$

Разработанный алгоритм (30)-(32) вычисления функции правдоподобия $L(\varepsilon, \delta; y_1^T)$ реализован и оттестирован в компьютерных экспериментах.

6. Результаты компьютерных экспериментов

Для иллюстрации состоятельности построенных в разделах 3-5 статистических оценок параметров для двух марковских моделей вкраплений проведены две серии компьютерных экспериментов.

В первой серии экспериментов для модели побитового вкрапления (2)-(4) методом Монте-Карло вычислены среднеквадратические ошибки $v\{\hat{\varepsilon}\} = 1/K \sum_{k=1}^K (\hat{\varepsilon}^{(k)} - \varepsilon)^2$, $v\{\hat{\delta}\} = 1/K \sum_{k=1}^K (\hat{\delta}^{(k)} - \delta)^2$ оценивания параметров модели на основе частотных статистик (16), (12) и выборочных корреляций (18) при следующих значениях параметров: $\varepsilon = 0.3$, $\delta = 0.15$, число прогонов $K = 10^3$. На рис. 2,3

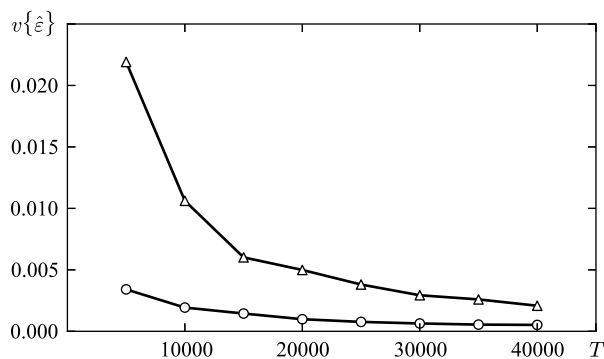


Рис. 2. Зависимость $v\{\hat{\varepsilon}\}$ от длины T при $\varepsilon = 0.3$, $\delta = 0.15$, $K = 10^3$

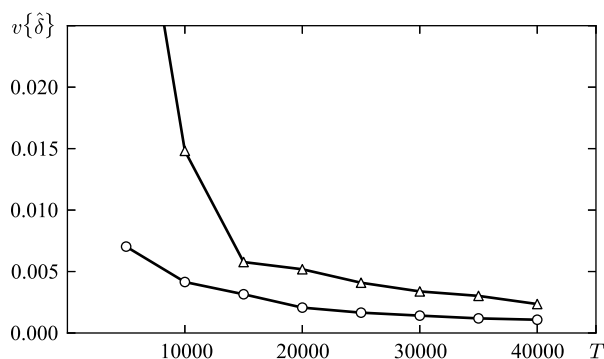


Рис. 3. Зависимость $v\{\hat{\delta}\}$ от длины T при $\varepsilon = 0.3$, $\delta = 0.15$, $K = 10^3$

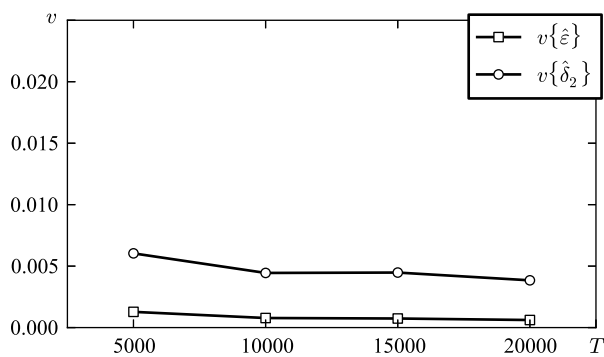


Рис. 4. Зависимость $v\{\hat{\varepsilon}\}$, $v\{\hat{\delta}\}$ от длины T при $\varepsilon = 0.3$, $\delta = 0.3$, $K = 10^2$

изображены графики зависимостей $v\{\hat{\varepsilon}\}$, $v\{\hat{\delta}\}$ от длины стегопоследовательности T . Кружками отмечены графики для частотных оценок (16), (12), треугольниками – оценок на основе выборочных корреляций (18).

Во второй серии экспериментов для модели блочного вкрапления (2)-(3), (5) вычислены среднеквадратические ошибки $v\{\hat{\varepsilon}\}$, $v\{\hat{\delta}\}$ МП-оценок параметров модели на основе полиномиального алгоритма (30)-(32) при следующих значениях параметров: $\varepsilon = 0.3$, $\delta = 0.3$, $K = 10^2$; построение МП-оценок осуществлялось табулированием функции $L(\varepsilon, \delta)$ на решетке: $\varepsilon, \delta \in \{0.20, 0.21, \dots, 0.40\}$. На рис. 4 изображены графики зависимостей $v\{\hat{\varepsilon}\}$, $v\{\hat{\delta}\}$ от длины стегапоследовательности T .

Авторы благодарны А.М. Зубкову за вопросы и замечания, способствовавшие улучшению данной статьи.

Список литературы

1. Sullivan K., Madhow U., Chandrasekaran S., Manjunath B., Steganalysis of spread spectrum data hiding exploiting cover memory. *SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VII* (2005) **5681**, 38–46.
2. Fridrich J., Pevny T., Kodovsky J., Statistically undetectable JPEG steganography: Dead ends, challenges, and opportunities. *Proc. 9-th ACM Multimedia Security Workshop* (2007) 3–14.
3. Pevny T., Bas P., Fridrich J., Steganalysis by subtractive pixel adjacency matrix. *Proc. 11-th ACM Multimedia Security Workshop* (2009) 75–84.
4. Shi Y. Q., Chen C., Chen W., A Markov process based approach to effective attacking JPEG steganography. *Lect. Notes Comput. Sci.* (2006) **4437**, 249–264.
5. Харин Ю. С., Вечерко Е. В., О некоторых задачах статистической проверки гипотез в стеганографии. *Вестн НАН Беларуси. Сер. физ.-мат. наук* (2010) **4**, 5–12.
6. Kharin Yu. S., Vecherko E. V., On statistical hypotheses testing of embedding. *Proc. 9-th Int. Conf. Computer Data Analysis and Modeling* (2010) **2**, 26–29.
7. Пономарев К. И., Параметрическая модель вкрапления и ее статистический анализ. *Дискретная математика* (2009) **21**, №4, 148–157.
8. Bas P., Filler T., Pevny T., Break Our Steganographic System – the ins and outs of organizing BOSS. *Proc. Inf. Hiding Conf.* (2011).
9. Зубков А. М., Датчики псевдослучайных чисел и их применения. *Сб.: Труды II Междунар. научн. конф. "Математика безопасности информационных технологий"* (2003) 200–206.
10. Кемени Дж., Снелл Дж., Конечные цепи Маркова (1982).
11. Харин Ю. С., Берник В. И., Матвеев Г. В., Агиевич С. В., *Математические и компьютерные основы криптологии*. Новое знание, 2003.
12. Sharp T., An Implementation of Key-Based Digital Signal Steganography. *Lect. Notes Comput. Sci.* (2001), №2137.
13. Ивченко Г. И., Медведев Ю. И., *Математическая статистика*. Высшая школа, Москва, 1984.
14. Боровков А. А., *Математическая статистика*. Наука, Москва, 1984.
15. Billingsley P., Statistical methods in Markov chains. *Ann. Math. Statist* (1961) **32**, №1, 12–40.
16. Rabiner L. R., A tutorial on hidden Markov models and selected applications in speech recognition. *Proc. of the IEEE* (1989) **77**, №2, 257–286.

Статья поступила 11.09.2012.