1 Математическая модель вкраплений на основе схемы независимых испытаний

Контейнер представляет собой последовательность случайных величин распределенных по закону Бернулли с параметром p:

$$\mathcal{L}x_t = Bi(1,p), x_i \in V = 0,1, i = \overline{1,T}; \tag{1}$$

Вкрапляемое сообщение имеет вид:

$$\mathcal{L}m_t = Bi(1,\theta), m_i \in V = 0,1, i = \overline{1,\tau}; \tag{2}$$

Ключ γ_t определяет момент времени вкрапления i-того бита сообщения в исходный контейнер:

$$\mathcal{L}\gamma_t = Bi(1,\delta), \gamma_i \in V = 0,1, i = \overline{1,T}; \tag{3}$$

Вкрапление битов m_t производится по правилу, заданному следующим функциональным преобразованием:

$$y_t = (1-\gamma_t)x_t + \gamma_t m_{\tau_t}; \tag{4}$$

Лемма 1.1. *Для модели (1)-(4)*

$$P\{y_t = 1\} = (1-\delta)p + \delta\theta; \tag{5}$$

$$P\{y_t = 0\} = (1-\delta)(1-p) + \delta(1-\theta); \tag{6}$$

Доказательство. Воспользуемся формулой полной вероятности:
$P\{y_t = 1\} = P\{(1-\gamma_t)x_t + \gamma_t m_{\tau_t} = 1\} = \sum_{j\in V} P\{y_t = 1, \gamma_t = j\} = \sum_{j\in V} P\{\gamma_t = j\}P\{y_t = 1|\gamma_t = j\} = (1-\delta)P\{x_=1, \gamma_t = 0\} + \delta P\{m_{\tau_t} = 1, \gamma_t = 1\} = (1-\delta)p + \delta\theta;$
Тогда:
$P\{y_t = 0\} = 1 - P\{y_t = 1\} = (1-\delta)(1-p) + \delta(1-\theta);$ □

$$h = \frac{H(y_1,...,y_t)}{T} = \frac{TH(y_1)}{T} = H(y_1); \tag{7}$$

Воспользуемся леммой 1.1:
$h = -P\{y_t = 1\}\log_2 P(y_t = 1) - P\{y_t = 0\}\log_2 P(y_t = 0) = -((1-\delta)p + \delta\theta)\log_2((1-\delta)p + \delta\theta) - ((1-\delta)(1-p) + \delta(1-\theta))\log_2((1-\delta)(1-p) + \delta(1-\theta)).$

2 Математическая модель вкраплений в двоичную стационарную марковскую последовательность 1-го порядка и ее свойства

Рассмотрим модель (1)-(4).

Пусть контейнер (1) пердставляет собой цепь Маркова 1-го порядка с вектором распределения вероятностей $\pi = (\frac{1}{2}, \frac{1}{2})$ и матрицей вероятностей одношаговых переходов

$$P(\varepsilon) = \frac{1}{2}\binom{1+\varepsilon, 1-\varepsilon}{1-\varepsilon, 1+\varepsilon}, |\varepsilon| < 1, \varepsilon \neq 0. \quad (8)$$

Лемма 2.1. *Для модели (1)-(4) с условием (8):*

$$P\{y_{t-1} = 1, y_t = 1\} = \frac{1}{4}(1+\varepsilon)(1-\delta)^2 + \theta\delta(1-\delta) + \theta^2\delta^2; \quad (9)$$

$$P\{y_{t-1} = 1, y_t = 0\} = \frac{1}{4}(1-\varepsilon)(1-\delta)^2 + \frac{1}{2}\delta(1-\delta) + \theta(1-\theta)\delta^2; \quad (10)$$

$$P\{y_{t-1} = 0, y_t = 1\} = \frac{1}{4}(1-\varepsilon)(1-\delta)^2 + \frac{1}{2}\delta(1-\delta) + \theta(1-\theta)\delta^2; \quad (11)$$

$$P\{y_{t-1} = 0, y_t = 0\} = \frac{1}{4}(1+\varepsilon)(1-\delta)^2 + \delta(1-\theta)(1-\delta) + \delta^2(1-\theta)^2. \quad (12)$$

Доказательство. Рассмотрим биграмм: $\{y_{t-1}, y_t\}$
$(a_1, a_2) \in \{0,1\}, P\{y_{t-1} = a_1, y_t = a_2\} = \sum_{(b_1,b_2)\in\{0,1\}^2} P\{y_{t-1} = b_1, y_t = b_2, \gamma_{t-1} = a_1, \gamma_t = a_2\} = \sum_{(b_1,b_2)\in\{0,1\}^2} P\{y_{t-1} = b_1, y_t = b_2 | \gamma_{t-1} = a_1, \gamma_t = a_2\} P\{\gamma_{t-1} = a_1, \gamma_t = a_2\}$.
Для (9):
$\sum_{(b_1,b_2)\in\{0,1\}^2} P\{y_{t-1} = b_1, y_t = b_2 | \gamma_{t-1} = a_1, \gamma_t = a_2\} P\{\gamma_{t-1} = a_1, \gamma_t = a_2\} = \frac{1}{2} \cdot \frac{1}{2}(1+\varepsilon)(1-\delta)^2 + \theta\delta(1-\theta) + \theta^2\delta^2$.
Для случаев (10)-(12) доказывается аналогично. □

Для формул (9)-(12) справедливо условие нормировки:
$\sum_{(a_1,a_2)\in\{0,1\}^2} P\{y_{t-1} = a_1, y_t = a_2\} = 1$.
Далее полагаем, что $\theta = \frac{1}{2}$.
Тогда:

$$P\{y_{t-1} = 1, y_t = 1\} = P\{y_{t-1} = 0, y_t = 0\} = \delta^2\frac{\varepsilon}{4} - \delta\frac{\varepsilon}{2} + \frac{1+\varepsilon}{4}; \quad (13)$$

$$P\{y_{t-1} = 1, y_t = 0\} = P\{y_{t-1} = 0, y_t = 1\} = -\delta^2\frac{\varepsilon}{4} + \delta\frac{\varepsilon}{2} + \frac{1-\varepsilon}{4}. \quad (14)$$

Определение 2.1. *[1] Дискретный стационарный источник называется марковским источником порядка m, если для любого l(l>m) и любой последовательности $c_l = (a_{i_1}, ..., a_{i_l})$ выполняется: $P\{a_{i_l} | a_{i_{l-1}}, ..., a_{i_1}\} = P\{a_{i_l} | a_{i_{l-1}}, ..., a_{i_{l-m+1}}\}$.*

Определение 2.2. *[1] Величина: $H^{(k)} = \sum_{\{c_k\}} P\{a_{i_1}, ..., a_{i_k}\} \log P\{a_{i_k} | a_{i_{k-1}} ..., a_{i_1}\}$ называется шаговой энтропией марковского источника порядка k.*

Введем понятие энтропии на знак для l-граммы:

$$H_l(\delta) = -\frac{1}{l} \sum_{(a_1,...,a_l)\in\{0,1\}} P\{y_{t-l} = a_1, ..., y_{t-1} = a_l\} \log P\{y_{t-l} = a_1, ..., y_{t-1} = a_l\}. \quad (15)$$

При $\delta = 0$ стегоконтейнер y совпадает с контейнером x, тогда:

$$H_l(0) = -\frac{1}{l}(H\{x_1\} + (l-1)H\{x_2|x_1\}); \tag{16}$$

$$\lim_{l\to\infty} H_l(0) = \lim_{l\to\infty} -\frac{1}{l}(H\{x_1\} + (l-1)H\{x_2|x_1\}) = H\{x_2|x_1\}. \tag{17}$$

Рассмотрим случайную величину $\xi \in B = \{b_1, ..., b_m\}$, заданную на вероятностном пространстве $(\Omega, \mathcal{F}, \mathcal{P})$, $P\{\xi = b_i\} = p_i$.

Определение 2.3. *[1] Величина*

$$I\{b_i\} = -\log p_i \tag{18}$$

называется собственной информацией, содержащейся в исходе $b_i \in B$.

Велиина $I\{b_i\}$ изменяется от нуля в случае реализации достоверного исхода до бесконечности, когда $p(b_i) = p_i \to 0$. Величину $I\{b_i\}$ можно интерпретировать как априорную неопределённость события $\{\xi = b_i\}$.

Случайная величина $I\{\xi\}$ имеет математическое ожидание

$$EI\{\xi\} = -\sum_{b_i\in B} p_i \log p_i. \tag{19}$$

Определение 2.4. *Величина $EI\{\xi\}$ называется средней собственной информацией.*

Средняя собственная информация равна энтропии: $EI\{\xi\} = H\{\xi\}$.

Для представления функции логарифма воспользуемся формулой Маклорена первого порядка:

$$f(\delta) = f(\delta_0) + (\delta - \delta_0)f'(\delta_0) + o((\delta - \delta_0)^2). \tag{20}$$

Для краткости, в обозначении функции log будем использовать основание b.

Согласно (20) в точке $\delta = 0$ справедливо асимптотическое разложение 1-го порядка:

$$\begin{gathered}\log_b(a_0(\varepsilon) + \delta a_1(\varepsilon) + \delta^2 a_2(\varepsilon) + o(\delta^2)) = \\ = \log a_0(\varepsilon) + \delta \left(\log(a_0(\varepsilon) + \delta a_1(\varepsilon) + \delta^2 a_2(\varepsilon) + o(\delta^2))\right)'|_{\delta=0} + o(\delta) = \\ = \log a_0(\varepsilon) + \delta \frac{1}{\ln b}\frac{a_1(\varepsilon)}{a_0(\varepsilon)} + o(\delta).\end{gathered}$$

Учитывая (20), найдем асимптотические выражения при $\delta \to 0$ для собственной информации $I\{y_{t-1} = i_1, y_t = i_2\}, i_1, i_2 \in \{0, 1\}$:

$$\begin{gathered}I\{y_{t-1} = 0, y_t = 0\} = I\{y_{t-1} = 1, y_t = 1\} = -\log(\frac{1}{4}(1+\varepsilon)(1-\delta)^2 + \frac{1}{2}\delta(1-\delta) + \frac{1}{4}\delta^2) = \\ = -\log\frac{1+\varepsilon}{4} + \delta\frac{1}{\ln b}\frac{2\varepsilon}{1+\varepsilon} + o(\delta); \\ I\{y_{t-1} = 0, y_t = 1\} = I\{y_{t-1} = 1, y_t = 0\} = -\log(\frac{1}{4}(1-\varepsilon)(1-\delta)^2 + \frac{1}{2}\delta(1-\delta) + \frac{1}{4})\delta^2) = \\ = -\log\frac{1-\varepsilon}{4} - \delta\frac{1}{\ln b}\frac{2\varepsilon}{1-\varepsilon} + o(\delta).\end{gathered}$$

Лемма 2.2. *Если имеет место монобитная модель вкраплений (1)-(4), то для энтропии при $l = 2$ справедливо асимптотическое разложение 1-го порядка*

$$H_2(\delta) = H_2(0) + 2\delta\varepsilon\log\frac{1+\varepsilon}{1-\varepsilon} + O(\delta^2). \tag{21}$$

Доказательство. $H_2(\delta) = -(P\{y_{t-1}=0, y_t=0\}\log(P\{y_{t-1}=0, y_t=0\}) + P\{y_{t-1}=0, y_t=1\}\log(P\{y_{t-1}=0, y_t=1\}) + P\{y_{t-1}=1, y_t=0\}\log(P\{y_{t-1}=1, y_t=0\}) + P\{y_{t-1}=1, y_t=1\}\log(P\{y_{t-1}=1, y_t=1\})) = -2(P\{y_{t-1}=0, y_t=0\}\log(P\{y_{t-1}=0, y_t=0\}) + P\{y_{t-1}=0, y_t=0\}\log(P\{y_{t-1}=0, y_t=1\})) = -2((\delta^2\frac{\varepsilon}{4} - \delta\frac{\varepsilon}{2} + \frac{1+\varepsilon}{4})(-\log(\frac{1+\varepsilon}{4}) + \delta\frac{1}{\ln b}\cdot\frac{2\varepsilon}{1+\varepsilon} + o(\delta^2)) + (-\delta^2\frac{\varepsilon}{4} + \delta\frac{\varepsilon}{2} + \frac{1-\varepsilon}{4})(-\log(\frac{1-\varepsilon}{4}) - \delta\frac{1}{\ln b}\cdot\frac{2\varepsilon}{1-\varepsilon} + o(\delta^2))) = \frac{1}{2}(-(1+\varepsilon)\log(\frac{1+\varepsilon}{4}) - (1-\varepsilon)\log(\frac{1-\varepsilon}{4}) + 2\delta\varepsilon\log(\frac{1+\varepsilon}{1-\varepsilon}))) + O(\delta^2) = H_2(0) + 2\delta\varepsilon\log(\frac{1+\varepsilon}{1-\varepsilon}))) + O(\delta^2).$ □

Определение 2.5. *[1] Величина* $\lim_{k\to\infty} H^{(k)} = \lim_{k\to\infty} H_k = H_\infty \geqslant 0$ *называется энтропий марковского источника, где* H_k *- энтропия на знак.*

Рассмотрим условные вероятности появления трехграммы $(0,0,0)$ при условии всевозможных стегоключей.

$P\{y_{i-1}=0, y_i=0, y_{i+1}=0\} = (1-\delta)^3 P\{y_{i-1}=0, y_i=0, y_{i+1}=0|\gamma_{i-1}=0, \gamma_i=0, \gamma_{i+1}=0\} +$
$+\,\delta(1-\delta)^2(P\{y_{i-1}=0, y_i=0, y_{i+1}=0|\gamma_{i-1}=1, \gamma_i=0, \gamma_{i+1}=0\} + P\{y_{i-1}=0, y_i=0, y_{i+1}=0|\gamma_{i-1}=0, \gamma_i=1, \gamma_{i+1}=0\} + P\{y_{i-1}=0, y_i=0, y_{i+1}=0|\gamma_{i-1}=0, \gamma_i=0, \gamma_{i+1}=1\}) +$
$+\,\delta^2(1-\delta)(P\{y_{i-1}=0, y_i=0, y_{i+1}=0|\gamma_{i-1}=1, \gamma_i=1, \gamma_{i+1}=0\} + P\{y_{i-1}=0, y_i=0, y_{i+1}=0|\gamma_{i-1}=0, \gamma_i=1, \gamma_{i+1}=1\} + P\{y_{i-1}=0, y_i=0, y_{i+1}=0|\gamma_{i-1}=1, \gamma_i=0, \gamma_{i+1}=1\}) +$
$+\,\delta^3(P\{y_{i-1}=0, y_i=0, y_{i+1}=0|\gamma_{i-1}=1, \gamma_i=1, \gamma_{i+1}=1\}).$

$P\{y_{i-1}=0, y_i=0, y_{i+1}=0|\gamma_1=0, \gamma_2=0, \gamma_3=0\} = P\{x_{i-1}=0, x_i=0, x_{i+1}=0\} = P\{x_{i-1}=0\}P\{x_i=0, x_{i+1}=0|x_{i-1}=0\} = P\{x_{i-1}=0\}P\{x_i=0\}P\{x_{i+1}=0|x_i=0\} = \frac{1}{2}\cdot\frac{1}{2}(1+\varepsilon)\cdot\frac{1}{2}(1+\varepsilon) = \frac{1}{8}(1+\varepsilon)^2;$

$P\{y_{i-1}=0, y_i=0, y_{i+1}=0|\gamma_1=1, \gamma_2=0, \gamma_3=0\} = P\{\xi=0, x_i=0, x_{i+1}=0\} = P\{\xi=0\}P\{x_i=0, x_{i+1}=0\} = P\{\xi=0\}P\{x_i=0\}P\{x_{i+1}=0|x_i=0\} = \frac{1}{2}\cdot\frac{1}{2}(1+\varepsilon)\cdot\frac{1}{2} = \frac{1}{8}(1+\varepsilon);$

$P\{y_{i-1}=0, y_i=0, y_{i+1}=0|\gamma_1=0, \gamma_2=1, \gamma_3=0\} = P\{x_{i-1}=0, \xi=0, x_{i+1}=0\} = P\{\xi=0\}P\{x_{i-1}=0, x_{i+1}=0\} = \frac{1}{2}\cdot\frac{1}{2}\cdot\frac{1}{2}(1+\varepsilon^2) = \frac{1}{8}(1+\varepsilon^2);$

$P\{y_{i-1}=0, y_i=0, y_{i+1}=0|\gamma_1=0, \gamma_2=0, \gamma_3=1\} = P\{x_{i-1}=0, x_i=0, \xi=0\} = P\{\xi=0\}P\{x_{i-1}=0, x_i=0\} = \frac{1}{2}\cdot\frac{1}{2}\cdot\frac{1}{2}(1+\varepsilon) = \frac{1}{8}(1+\varepsilon);$

$P\{y_{i-1}=0, y_i=0, y_{i+1}=0|\gamma_1=0, \gamma_2=1, \gamma_3=1\} = P\{y_{i-1}=0, y_i=0, y_{i+1}=0|\gamma_1=1, \gamma_2=0, \gamma_3=1\} = P\{y_{i-1}=0, y_i=0, y_{i+1}=0|\gamma_1=1, \gamma_2=1, \gamma_3=0\} = P\{y_{i-1}=0, y_i=0, y_{i+1}=0|\gamma_1=1, \gamma_2=1, \gamma_3=1\} = P\{\xi=0, \xi=0, \xi=0\} = P\{\xi=1\}P\{x_{i-1}=1\}P\{x_i=0\} = \frac{1}{2}\cdot\frac{1}{2}\cdot\frac{1}{2} = \frac{1}{8};$

$P\{y_{i-1}=0, y_i=0, y_{i+1}=0\} = \frac{1}{8}\big(\varepsilon(\varepsilon+2)\delta^2 - 2\varepsilon(\varepsilon+1)\delta + (1+\varepsilon)^2\big).$

Найдем вероятности появления всевозможных трехграмм в стегоконтейнере $\{y_t\}$:

$$P\{y_{i-1}=1, y_i=1, y_{i+1}=1\} = P\{y_{i-1}=0, y_i=0, y_{i+1}=0\} = \\ = \frac{1}{8}\big(\varepsilon(\varepsilon+2)\delta^2 - 2\varepsilon(\varepsilon+2)\delta + (1+\varepsilon)^2\big),$$
$$P\{y_{i-1}=1, y_i=1, y_{i+1}=0\} = P\{y_{i-1}=0, y_i=0, y_{i+1}=1\} = P\{y_{i-1}=0, y_i=1, y_{i+1}=1\} = \\ = P\{y_{i-1}=1, y_i=0, y_{i+1}=0\} = \frac{1}{8}\big(-\varepsilon^2\delta^2 + 2\varepsilon^2\delta - \varepsilon^2 + 1\big),$$
$$P\{y_{i-1}=1, y_i=0, y_{i+1}=1\} = P\{y_{i-1}=0, y_i=1, y_{i+1}=0\} = \\ = \frac{1}{8}\big(\varepsilon(\varepsilon-2)\delta^2 - 2\varepsilon(\varepsilon-2)\delta + (1-\varepsilon)^2\big).$$

Теорема 2.1. *Если имеет место монобитная модель вкраплений (1)-(4) , то для энтропии при $l = 3$ справедливо асимптотическое разложение 1-го порядка:*

$$H_3(\delta) = H_3(0) + 2\varepsilon\delta \log \frac{1+\varepsilon}{1-\varepsilon} + O(\delta^2); \tag{22}$$

собственная информация имеет вид:

$$I\{y_{i-1} = 0, y_i = 0, y_{i+1} = 0\} = -\log \frac{(1+\varepsilon)^2}{8} + \delta \frac{1}{\ln b} \cdot \frac{2\varepsilon^2 + 4\varepsilon}{(1+\varepsilon)^2} + O(\delta^2),$$

$$I\{y_{i-1} = 1, y_i = 0, y_{i+1} = 0\} = I\{y_{i-1} = 0, y_i = 0, y_{i+1} = 1\} =$$

$$= -\log \frac{1-\varepsilon^2}{8} - \delta \frac{1}{\ln b} \cdot \frac{2\varepsilon^2}{1-\varepsilon^2} + O(\delta^2),$$

$$I\{y_{i-1} = 0, y_i = 1, y_{i+1} = 0\} = -\log \frac{(1-\varepsilon)^2}{8} + \delta \frac{1}{\ln b} \cdot \frac{2\varepsilon^2 - 4\varepsilon}{(1-\varepsilon)^2} + O(\delta^2);$$

$I\{y_{i-1} = j_1, y_i = j_2, y_{i+1} = j_3\} = I\{y_{i-1} = 1 - j_1, y_i = 1 - j_2, y_{i+1} = 1 - j_3\},\ j_1, j_2, j_3 \in \{0, 1\}.$

Доказательство. Подставляя в (20) найденные выражения для вероятностей трехграмм, получим асимптотические выражения для собственной информации.

Используя выражения для собственной информации, получим: $H_3(\delta) = -2(\frac{1}{8}\big(\varepsilon(\varepsilon+2)\delta^2 - 2\varepsilon(\varepsilon+2)\delta + (1+\varepsilon)^2\big)(\log(\frac{(1+\varepsilon)^2}{8}) + \delta\frac{1}{\ln b} \cdot \frac{-2\varepsilon^2-4\varepsilon}{(1+\varepsilon)^2}) + 2\frac{1}{8}\big(-\varepsilon^2\delta^2 + 2\varepsilon^2\delta - \varepsilon^2 + 1\big)(\log(\frac{1-\varepsilon^2}{8}) + \delta\frac{1}{\ln b} \cdot \frac{2\varepsilon^2}{1-\varepsilon^2}) + \frac{1}{8}\big(\varepsilon(\varepsilon-2)\delta^2 - 2\varepsilon(2+\varepsilon)\delta + (1-\varepsilon)^2\big)(\log(\frac{(1-\varepsilon)^2}{8}) + \delta\frac{1}{\ln b} \cdot \frac{-2\varepsilon^2+4\varepsilon}{(1-\varepsilon)^2})) + O(\delta^2) = -((1-\varepsilon)\log(1-\varepsilon) + (1+\varepsilon)\log(1+\varepsilon) + \log(\frac{1}{8}) + 2\varepsilon\delta\log\frac{1-\varepsilon}{1+\varepsilon}) + O(\delta^2) = H_3(0) - 2\varepsilon\delta\log\frac{1-\varepsilon}{1+\varepsilon} + O(\delta^2).$ □

Рассмотрим условные вероятности появления четырехграммы $(0,0,0,0)$ при условии всевозможных стегоключей.

$P\{y_{i-1} = 0, y_i = 0, y_{i+1} = 0, y_{i+2} = 0\} = (1-\delta)^4 P\{y_{i-1} = 0, y_i = 0, y_{i+1} = 0, y_{i+2} = 0|\gamma_{i-1} = 0, \gamma_i = 0, \gamma_{i+1} = 0, \gamma_{i+2} = 0\} + \delta(1-\delta)^3\Big(P\{y_{i-1} = 0, y_i = 0, y_{i+1} = 0, y_{i+2} = 0|\gamma_{i-1} = 0, \gamma_i = 0, \gamma_{i+1} = 0, \gamma_{i+2} = 1\} + P\{y_{i-1} = 0, y_i = 0, y_{i+1} = 0, y_{i+2} = 0|\gamma_{i-1} = 0, \gamma_i = 0, \gamma_{i+1} = 1, \gamma_{i+2} = 0\} + P\{y_{i-1} = 0, y_i = 0, y_{i+1} = 0, y_{i+2} = 0|\gamma_{i-1} = 0, \gamma_i = 1, \gamma_{i+1} = 0, \gamma_{i+2} = 0\} + P\{y_{i-1} = 0, y_i = 0, y_{i+1} = 0, y_{i+2} = 0|\gamma_{i-1} = 1, \gamma_i = 0, \gamma_{i+1} = 0, \gamma_{i+2} = 0\}\Big) + \delta^2(1-\delta)^2\Big(P\{y_{i-1} = 0, y_i = 0, y_{i+1} = 0, y_{i+2} = 0|\gamma_{i-1} = 0, \gamma_i = 0, \gamma_{i+1} = 1, \gamma_{i+2} = 1\} + P\{y_{i-1} = 0, y_i = 0, y_{i+1} = 0, y_{i+2} = 0|\gamma_{i-1} = 0, \gamma_i = 1, \gamma_{i+1} = 1, \gamma_{i+2} = 0\} + P\{y_{i-1} = 0, y_i = 0, y_{i+1} = 0, y_{i+2} = 0|\gamma_{i-1} = 1, \gamma_i = 1, \gamma_{i+1} = 0, \gamma_{i+2} = 0\} + P\{y_{i-1} = 0, y_i = 0, y_{i+1} = 0, y_{i+2} = 0|\gamma_{i-1} = 1, \gamma_i = 0, \gamma_{i+1} = 1, \gamma_{i+2} = 0\} + P\{y_{i-1} = 0, y_i = 0, y_{i+1} = 0, y_{i+2} = 0|\gamma_{i-1} = 0, \gamma_i = 1, \gamma_{i+1} = 0, \gamma_{i+2} = 1\} + P\{y_{i-1} = 0, y_i = 0, y_{i+1} = 0, y_{i+2} = 0|\gamma_{i-1} = 1, \gamma_i = 0, \gamma_{i+1} = 0, \gamma_{i+2} = 1\}\Big) + \delta^3(1-\delta)\Big(P\{y_{i-1} = 0, y_i = 0, y_{i+1} = 0, y_{i+2} = 0|\gamma_{i-1} = 0, \gamma_i = 1, \gamma_{i+1} = 1, \gamma_{i+2} = 1\} + P\{y_{i-1} = 0, y_i = 0, y_{i+1} = 0, y_{i+2} = 0|\gamma_{i-1} = 1, \gamma_i = 0, \gamma_{i+1} = 1, \gamma_{i+2} = 1\} + P\{y_{i-1} = 0, y_i = 0, y_{i+1} = 0, y_{i+2} = 0|\gamma_{i-1} = 1, \gamma_i = 1, \gamma_{i+1} = 0, \gamma_{i+2} = 1\} + P\{y_{i-1} = 0, y_i = 0, y_{i+1} = 0, y_{i+2} = 0|\gamma_{i-1} = 1, \gamma_i = 1, \gamma_{i+1} = 1, \gamma_{i+2} = 0\}\Big) + \delta^4(P\{y_{i-1} = 0, y_i = 0, y_{i+1} = 0, y_{i+2} = 0|\gamma_{i-1} = 1, \gamma_i = 1, \gamma_{i+1} = 1, \gamma_{i+2} = 1\}).$

$P\{y_{i-1} = 0, y_i = 0, y_{i+1} = 0, y_{i+2} = 0|\gamma_{i-1} = 0, \gamma_i = 0, \gamma_{i+1} = 0, \gamma_{i+2} = 0\} = \frac{(1+\varepsilon)^3}{16};$

$P\{y_{i-1} = 0, y_i = 0, y_{i+1} = 0, y_{i+2} = 0|\gamma_{i-1} = 1, \gamma_i = 0, \gamma_{i+1} = 0, \gamma_{i+2} = 0\} = P\{y_{i-1} = 0, y_i = 0, y_{i+1} = 0, y_{i+2} = 0|\gamma_{i-1} = 0, \gamma_i = 0, \gamma_{i+1} = 0, \gamma_{i+2} = 1\} = \frac{(1+\varepsilon)^2}{16};$

$P\{y_{i-1}=0, y_i=0, y_{i+1}=0, y_{i+2}=0|\gamma_{i-1}=0, \gamma_i=1, \gamma_{i+1}=0, \gamma_{i+2}=0\} = P\{y_{i-1}=0, y_i=0, y_{i+1}=0, y_{i+2}=0|\gamma_{i-1}=0, \gamma_i=0, \gamma_{i+1}=1, \gamma_{i+2}=0\} = \frac{(1+\varepsilon)(1+\varepsilon^2)}{16}$;

$P\{y_{i-1}=0, y_i=0, y_{i+1}=0, y_{i+2}=0|\gamma_{i-1}=1, \gamma_i=1, \gamma_{i+1}=0, \gamma_{i+2}=0\} = P\{y_{i-1}=0, y_i=0, y_{i+1}=0, y_{i+2}=0|\gamma_{i-1}=0, \gamma_i=0, \gamma_{i+1}=0, \gamma_{i+2}=1\} = P\{y_{i-1}=0, y_i=0, y_{i+1}=0, y_{i+2}=0|\gamma_{i-1}=1, \gamma_i=0, \gamma_{i+1}=0, \gamma_{i+2}=1\} = P\{y_{i-1}=0, y_i=0, y_{i+1}=0, y_{i+2}=0|\gamma_{i-1}=0, \gamma_i=0, \gamma_{i+1}=1, \gamma_{i+2}=1\} = \frac{1+\varepsilon}{16}$;

$P\{y_{i-1}=0, y_i=0, y_{i+1}=0, y_{i+2}=0|\gamma_{i-1}=0, \gamma_i=1, \gamma_{i+1}=0, \gamma_{i+2}=1\} = P\{y_{i-1}=0, y_i=0, y_{i+1}=0, y_{i+2}=0|\gamma_{i-1}=1, \gamma_i=0, \gamma_{i+1}=1, \gamma_{i+2}=0\} = \frac{1+\varepsilon^2}{16}$;

$P\{y_{i-1}=0, y_i=0, y_{i+1}=0, y_{i+2}=0|\gamma_{i-1}=1, \gamma_i=1, \gamma_{i+1}=1, \gamma_{i+2}=0\} = P\{y_{i-1}=0, y_i=0, y_{i+1}=0, y_{i+2}=0|\gamma_{i-1}=1, \gamma_i=1, \gamma_{i+1}=0, \gamma_{i+2}=1\} = P\{y_{i-1}=0, y_i=0, y_{i+1}=0, y_{i+2}=0|\gamma_{i-1}=1, \gamma_i=0, \gamma_{i+1}=1, \gamma_{i+2}=1\} = P\{y_{i-1}=0, y_i=0, y_{i+1}=0, y_{i+2}=0|\gamma_{i-1}=0, \gamma_i=1, \gamma_{i+1}=1, \gamma_{i+2} = P\{y_{i-1}=0, y_i=0, y_{i+1}=0, y_{i+2}=0|\gamma_{i-1}=1, \gamma_i=1, \gamma_{i+1}=1, \gamma_{i+2}=1\} = \frac{1}{16}$;

$P\{y_{i-1}=0, y_i=0, y_{i+1}=0, y_{i+2}=0\} = P\{y_{i-1}=1, y_i=1, y_{i+1}=1, y_{i+2}=1\} = \frac{1}{16}\big(\delta^4\varepsilon^2+\delta^3(-4\varepsilon^2)+\delta^2(\varepsilon^3+8\varepsilon^2+3\varepsilon)+\delta(-2\varepsilon^3-8\varepsilon^2-6\varepsilon)+\varepsilon^3+3\varepsilon^2+3\varepsilon+1\big)$.
Найдем вероятности появления всевозможных четырехграмм в стегоконтейнере $\{y_t\}$:

$$P\{y_{i-1}=0, y_i=0, y_{i+1}=0, y_{i+2}=1\} = P\{y_{i-1}=1, y_i=1, y_{i+1}=1, y_{i+2}=0\} =$$
$$= P\{y_{i-1}=1, y_i=0, y_{i+1}=0, y_{i+2}=0\} = P\{y_{i-1}=0, y_i=1, y_{i+1}=1, y_{i+2}=1\} =$$
$$= \tfrac{1}{16}\big(\delta^4(-\varepsilon^2)+\delta^3\cdot 4\varepsilon^2+\delta^2(-\varepsilon^3-6\varepsilon^2+\varepsilon)+\delta(2\varepsilon^3+4\varepsilon^2-2\varepsilon)-\varepsilon^3-\varepsilon^2+\varepsilon+1\big);$$
$$P\{y_{i-1}=0, y_i=1, y_{i+1}=0, y_{i+2}=0\} = P\{y_{i-1}=1, y_i=0, y_{i+1}=1, y_{i+2}=1\} =$$
$$= P\{y_{i-1}=0, y_i=0, y_{i+1}=1, y_{i+2}=0\} = P\{y_{i-1}=1, y_i=1, y_{i+1}=0, y_{i+2}=1\} =$$
$$= \tfrac{1}{16}\big(\delta^4(-\varepsilon^2)+\delta^3\cdot 4\varepsilon^2+\delta^2(\varepsilon^3-6\varepsilon^2-\varepsilon)+\delta(-2\varepsilon^3+4\varepsilon^2+2\varepsilon)+\varepsilon^3-\varepsilon^2-\varepsilon+1\big);$$
$$P\{y_{i-1}=0, y_i=0, y_{i+1}=1, y_{i+2}=1\} = P\{y_{i-1}=1, y_i=1, y_{i+1}=0, y_{i+2}=0\} =$$
$$= \tfrac{1}{16}\big(\delta^4\varepsilon^2+\delta^3(-4\varepsilon^2)+\delta^2(-\varepsilon^3+4\varepsilon^2+\varepsilon)+\delta(2\varepsilon^3-2\varepsilon)-\varepsilon^3-\varepsilon^2+\varepsilon+1\big);$$
$$P\{y_{i-1}=0, y_i=1, y_{i+1}=1, y_{i+2}=0\} = P\{y_{i-1}=1, y_i=0, y_{i+1}=0, y_{i+2}=1\} =$$
$$= \tfrac{1}{16}\big(\delta^4\varepsilon^2+\delta^3(-4\varepsilon^2)+\delta^2(\varepsilon^3+4\varepsilon^2-\varepsilon)+\delta(-2\varepsilon^3+2\varepsilon)+\varepsilon^3-\varepsilon^2-\varepsilon+1\big);$$
$$P\{y_{i-1}=1, y_i=0, y_{i+1}=1, y_{i+2}=0\} = P\{y_{i-1}=0, y_i=1, y_{i+1}=0, y_{i+2}=1\} =$$
$$= \tfrac{1}{16}\big(\delta^4\varepsilon^2+\delta^3(-4\varepsilon^2)+\delta^2(-\varepsilon^3+8\varepsilon^2-3\varepsilon)+\delta(2\varepsilon^3-8\varepsilon^2+6\varepsilon)-\varepsilon^3+3\varepsilon^2-3\varepsilon+1\big).$$

Теорема 2.2. *Если имеет место монобитная модель вкраплений (1)-(4) , то для энтропии при $l=4$ справедливо асимптотическое разложение 1-го порядка:*

$$H_4(\delta) = H_4(0) + \frac{24\varepsilon\delta}{16}\log\frac{1+\varepsilon}{1-\varepsilon} + O(\delta^2); \tag{23}$$

собственная информация имеет вид:

$$
\begin{aligned}
&I\{y_{i-1}=0,y_i=0,y_{i+1}=0,y_{i+2}=0\}=I\{y_{i-1}=1,y_i=1,y_{i+1}=1,y_{i+2}=1\}=\\
&=-\left(\log\frac{(1+\varepsilon)^3}{16}+\delta\frac{-2\varepsilon^3-8\varepsilon^2-6\varepsilon}{(1+\varepsilon)^3\ln b}\right)+O(\delta^2);\\
&I\{y_{i-1}=0,y_i=0,y_{i+1}=0,y_{i+2}=1\}=I\{y_{i-1}=1,y_i=1,y_{i+1}=1,y_{i+2}=0\}=\\
&=I\{y_{i-1}=1,y_i=0,y_{i+1}=0,y_{i+2}=0\}=I\{y_{i-1}=0,y_i=1,y_{i+1}=1,y_{i+2}=1\}=\\
&=-\left(\log\frac{(1-\varepsilon)(1+\varepsilon)^2}{16}+\delta\frac{2\varepsilon^3+4\varepsilon^2-2\varepsilon}{(1-\varepsilon)(1+\varepsilon)^2\ln b}\right)+O(\delta^2);\\
&I\{y_{i-1}=0,y_i=0,y_{i+1}=1,y_{i+2}=0\}=I\{y_{i-1}=1,y_i=1,y_{i+1}=0,y_{i+2}=1\}=\\
&=I\{y_{i-1}=0,y_i=1,y_{i+1}=0,y_{i+2}=0\}=I\{y_{i-1}=1,y_i=0,y_{i+1}=1,y_{i+2}=1\}=\\
&=-\left(\log\frac{(1-\varepsilon)^2(1+\varepsilon)}{16}+\delta\frac{-2\varepsilon^3+4\varepsilon^2+2\varepsilon}{(1-\varepsilon)^2(1+\varepsilon)\ln b}\right)+O(\delta^2);\\
&I\{y_{i-1}=0,y_i=0,y_{i+1}=1,y_{i+2}=1\}=I\{y_{i-1}=1,y_i=1,y_{i+1}=0,y_{i+2}=0\}=\\
&=-\left(\log\frac{(1-\varepsilon)(1+\varepsilon)^2}{16}+\delta\frac{2\varepsilon^3-2\varepsilon}{(1-\varepsilon)(1+\varepsilon)^2\ln b}\right)+O(\delta^2);\\
&I\{y_{i-1}=0,y_i=1,y_{i+1}=1,y_{i+2}=0\}=I\{y_{i-1}=1,y_i=0,y_{i+1}=0,y_{i+2}=1\}=\\
&=-\left(\log\frac{(1-\varepsilon)^2(1+\varepsilon)}{16}+\delta\frac{-2\varepsilon^3+2\varepsilon}{(1-\varepsilon)^2(1+\varepsilon)\ln b}\right)+O(\delta^2);\\
&I\{y_{i-1}=1,y_i=0,y_{i+1}=1,y_{i+2}=0\}=I\{y_{i-1}=0,y_i=1,y_{i+1}=0,y_{i+2}=1\}=\\
&=-\left(\log\frac{(1-\varepsilon)^3}{16}+\delta\frac{2\varepsilon^3-8\varepsilon^2+6\varepsilon}{(1-\varepsilon)^3\ln b}\right)+O(\delta^2).
\end{aligned}
$$

Доказательство. Подставляя в (20) найденные выражения для вероятностей четырех-грамм, получим асимптотические выражения для собственной информации.
Используя выражения для собственной информации, получим:

$H_4(\delta)=-2\Bigg(\frac{1}{16}\big(\delta^4\varepsilon^2+\delta^3(-4\varepsilon^2)+\delta^2(\varepsilon^3+8\varepsilon^2+3\varepsilon)+\delta(-2\varepsilon^3-8\varepsilon^2-6\varepsilon)+\varepsilon^3+3\varepsilon^2+3\varepsilon+1\big)\big(\log\frac{(1+\varepsilon)^3}{16}+\delta\frac{-2\varepsilon^3-8\varepsilon^2-6\varepsilon}{(1+\varepsilon)^3\ln b}+O(\delta^2)\big)+2\frac{1}{16}\big(\delta^4(-\varepsilon^2)+\delta^3\cdot4\varepsilon^2+\delta^2(-\varepsilon^3-6\varepsilon^2+\varepsilon)+\delta(2\varepsilon^3+4\varepsilon^2-2\varepsilon)-\varepsilon^3-\varepsilon^2+\varepsilon+1\big)\big(\log\frac{(1-\varepsilon)(1+\varepsilon)^2}{16}+\delta\frac{2\varepsilon^3+4\varepsilon^2-2\varepsilon}{(1-\varepsilon)(1+\varepsilon)^2\ln b}+O(\delta^2)\big)+2\frac{1}{16}\big(\delta^4(-\varepsilon^2)+\delta^3\cdot4\varepsilon^2+\delta^2(\varepsilon^3-6\varepsilon^2-\varepsilon)+\delta(-2\varepsilon^3+4\varepsilon^2+2\varepsilon)+\varepsilon^3-\varepsilon^2-\varepsilon+1\big)\big(\log\frac{(1-\varepsilon)^2(1+\varepsilon)}{16}+\delta\frac{-2\varepsilon^3+4\varepsilon^2+2\varepsilon}{(1-\varepsilon)^2(1+\varepsilon)\ln b}+O(\delta^2)\big)+\frac{1}{16}\big(\delta^4\varepsilon^2+\delta^3(-4\varepsilon^2)+\delta^2(-\varepsilon^3+4\varepsilon^2+\varepsilon)+\delta(2\varepsilon^3-2\varepsilon)-\varepsilon^3-\varepsilon^2+\varepsilon+1\big)\big(log\frac{(1-\varepsilon)(1+\varepsilon)^2}{16}+\delta\frac{2\varepsilon^3-2\varepsilon}{(1-\varepsilon)(1+\varepsilon)^2\ln b}+O(\delta^2)\big)+\frac{1}{16}\big(\delta^4\varepsilon^2+\delta^3(-4\varepsilon^2)+\delta^2(\varepsilon^3+4\varepsilon^2-\varepsilon)+\delta(-2\varepsilon^3+2\varepsilon)+\varepsilon^3-\varepsilon^2-\varepsilon+1\big)\big(\log\frac{(1-\varepsilon)^2(1+\varepsilon)}{16}+\delta\frac{-2\varepsilon^3+2\varepsilon}{(1-\varepsilon)^2(1+\varepsilon)\ln b}+O(\delta^2)\big)+\frac{1}{16}\big(\delta^4\varepsilon^2+\delta^3(-4\varepsilon^2)+\delta^2(-\varepsilon^3+8\varepsilon^2-3\varepsilon)+\delta(2\varepsilon^3-8\varepsilon^2+6\varepsilon)-\varepsilon^3+3\varepsilon^2-3\varepsilon+1\big)\big(\log\frac{(1-\varepsilon)^3}{16}+\delta\frac{2\varepsilon^3-8\varepsilon^2+6\varepsilon}{(1-\varepsilon)^3\ln b}+O(\delta^2)\big)\Bigg)=\frac{(1+\varepsilon)^3}{16}\log\frac{(1+\varepsilon)^3}{16}+3\frac{(1+\varepsilon)^2(1-\varepsilon)}{16}\log\frac{(1+\varepsilon)^2(1-\varepsilon)}{16}+3\frac{(1+\varepsilon)(1-\varepsilon)^2}{16}\log\frac{(1+\varepsilon)(1-\varepsilon)^2}{16}+\frac{(1-\varepsilon)^3}{16}\log\frac{(1-\varepsilon)^3}{16}+\frac{24\varepsilon\delta}{16}\log\frac{1+\varepsilon}{1-\varepsilon}+O(\delta^2)=H_4(0)+\frac{24\varepsilon\delta}{16}\log\frac{1+\varepsilon}{1-\varepsilon}+O(\delta^2).$ □

Оценим остаточный член для асимптотического выражения энтропии биграммы:

$$r_n(\delta)=\frac{f^{(n+1)}(\overline{\delta})}{(n+1)!}(\delta-\delta_0),\overline{\delta}\in[\delta_0,\delta]. \tag{24}$$

Для асимптотического разложения 1-го порядка при $\delta_0=0$ остаточный член имеет вид:

$$r_n(\delta)=\frac{f''(\overline{\delta})}{2}\delta,\overline{\delta}\in[0,\delta]. \tag{25}$$

$(\log(P_{00}))'' = \frac{-2\varepsilon(\delta^2\varepsilon-2\delta\varepsilon+\varepsilon-1)}{\ln b(\delta^2\varepsilon-2\delta\varepsilon+\varepsilon+1)^2}$;
$(\log(P_{01}))'' = \frac{-2\varepsilon(\delta^2\varepsilon-2\delta\varepsilon+\varepsilon+1)}{\ln b(\delta^2\varepsilon-2\delta\varepsilon+\varepsilon-1)^2}$;
Тогда остаточный член для $\log(P_{00}) = \log(P_{11})$ равен:
$r_{n_{00}}(\delta) = \frac{\delta}{2} \cdot \frac{-2\varepsilon(\delta^2\varepsilon-2\delta\varepsilon+\varepsilon-1)}{\ln b(\delta^2\varepsilon-2\delta\varepsilon+\varepsilon+1)^2}|_{\delta=\overline{\delta}}$
Остаточный член для $\log(P_{10}) = \log(P_{01})$ равен:
$r_{n_{10}}(\delta) = \frac{\delta}{2} \cdot \frac{-2\varepsilon(\delta^2\varepsilon-2\delta\varepsilon+\varepsilon+1)}{\ln b(\delta^2\varepsilon-2\delta\varepsilon+\varepsilon-1)^2}|_{\delta=\overline{\delta}}$
Тогда остаточный член для энтропиии будет равен:
$R_n(\delta) = -2(P_{00}r_{n_{00}}(\delta) + P_{10}r_{n_{01}}(\delta)) = -2\big((\delta^2\frac{\varepsilon}{4} - \delta\frac{\varepsilon}{2} + \frac{1+\varepsilon}{4})(\frac{\delta}{2} \cdot \frac{-2\varepsilon(\delta^2\varepsilon-2\delta\varepsilon+\varepsilon-1)}{\ln b(\delta^2\varepsilon-2\delta\varepsilon+\varepsilon+1)^2}|_{\delta=\overline{\delta}}) + (-\delta^2\frac{\varepsilon}{4} + \delta\frac{\varepsilon}{2} + \frac{1-\varepsilon}{4})(\frac{\delta}{2} \cdot \frac{-2\varepsilon(\delta^2\varepsilon-2\delta\varepsilon+\varepsilon+1)}{\ln b(\delta^2\varepsilon-2\delta\varepsilon+\varepsilon-1)^2}|_{\delta=\overline{\delta}})\big)$

3 Компьютерные эксперименты

На рисунках 1.2, 1.3, 1.4 изображены зависимости остаточных членов $H_2(\delta) - H_2^{as}(\delta)$, $H_4(\delta) - H_4^{as}(\delta)$, $H_4(\delta) - H_4^{as}(\delta)$ соответственно от величины доли вкрапления δ. Из графика видно, что при меньшей доле вкрапления разница между асимптотическим выражением и точным значение энтропии стремится к нулю.

Список литературы

[1] А. А. Духин: Теория информации - М.: "Гелиос АРВ 2007.

[2] А.В. Аграновский, А. В. Балакин: Стеганография, цифровые водяные знаки о стегоанализ - М.: Вузовская книга, 2009.

[3] В. Г. Грибунин, И. Н. Оков, И. В. Туринцев: Цифровая стеганография - М.: Солон-Прессб, 2002.

[4] Н. П. Варновский, Е. А. Голубев, О. А. Логачев: Современные направления стеганографии. Математика и безопасность информационных технологий. Материалы конференции в МГУ 28-29 октября 2004 г., МЦМНО, М., 2005, с. 32-64.

[5] Ю. С. Харин [и др.]: Криптология - Минск: БГУ, 2013.

[6] Ю. С. Харин, Е. В. Вечерко "Статистическое оценивание параметров модели вкраплений в двоичную цепь Маркова Дискрет. матем., 25:2 (2013), 135-148.