эксперименты. Оценивается параметр θ, в предположении, что значение σ известно. Использованы следующие значения параметров: $\theta = -0.3$, $\sigma = 1$, $c_t \equiv 0$, $T = 300$. При вычислении значений функции (3) – (5), входящих в (6), суммирование по k проводится от 1 до $k_{\max}$.

Таблица 1

Результаты компьютерных экспериментов

			kmax=2		kmax=6	
№	МНК	Ошибка	ОМП	Ошибка	ОМП	Ошибка
1	0.17639	0.47639	-0.345856	0.045856	-0.30225	0.002252
2	0.190799	0.490799	-0.333964	0.033964	-0.26261	0.037387
3	0.155476	0.455476	-0.389459	0.089459	-0.37559	0.075586
4	0.149382	0.449382	-0.427117	0.127117	-0.40333	0.103333
5	0.195661	0.495661	-0.383514	0.083514	-0.3518	0.051802
6	0.151674	0.451674	-0.417207	0.117207	-0.3855	0.085495
7	0.178645	0.478645	-0.365676	0.065676	-0.31018	0.01018
8	0.154852	0.454852	-0.433063	0.133063	-0.40333	0.103333
9	0.164298	0.464298	-0.341892	0.041892	-0.29036	0.00964
10	0.166816	0.466816	-0.294324	0.005676	-0.24874	0.051261
среднее	**0.168399**	**0.468399**	**-0.37625**	**0.077508**	**-0.33337**	**0.053027**

Результаты экспериментов приведены в таблице 1. Как видно из таблицы 1, метод максимального правдоподобия, в отличие от метода наименьших квадратов, используемого на практике, дает приемлемые результаты. Также отметим, что с ростом числа слагаемых в (3) – (5) точность оценивания по методу максимального правдоподобия увеличивается.

Литература

1. *Бокс Дж., Дженкинс Г.* Анализ временных рядов. Прогноз и управление. М. 1974.
2. *Андерсон Т.* Статистический анализ временных рядов. М. 1976.
3. *Харин Ю. С.* Оптимальность и робастность в статистическом прогнозировании. Мн., 2008.
4. *Park J. W., Genton M. G., Ghosh S. K.* Censored time series analysis with autoregressive moving average models // The Canadian journal of statistics. 2007. Vol. 35. № 1. P. 151–168.

ВЕРОЯТНОСТНО-СТАТИСТИЧЕСКОЕ МОДЕЛИРОВАНИЕ В СТЕГАНОГРАФИИ

Е. В. Вечерко

ВВЕДЕНИЕ

В настоящее время стеганография стремительно развивается и используется при решении задач защиты информации и авторских прав [1–5].

Вероятностно-статистические вопросы стеганографии являются недостаточно проработанными, в частности, актуальна проблема построения и анализа адекватных математических моделей контейнеров, используемых для скрытия (“вкрапления” [4]) защищаемой информации.

Метод LSB, заключающийся в использовании наименее значимых бит цифровых представлений контейнеров для встраивания защищаемой информации [1,3], является одним из наиболее распространенных в стеганографии методов, который применяется для различных форматов контейнеров. В [2] предложен метод, основанный на статистическом анализе пар значений, которые изменяются при встраивании информации.

В статье исследуются вероятностно-статистические свойства LSB-метода.

ВЕРОЯТНОСТНЫЕ МОДЕЛИ И СВОЙСТВА СТЕГОКОНТЕЙНЕРОВ

Введем обозначения: $V=\{0,1\}$, $V_N=\{J=(j_k): j_k\in V, k=1,\ldots,N\}$ - множество 2^N двоичных N-векторов; $A=\{0,1,\ldots,2^N-1\}$ - множество из 2^N элементов; L - закон распределения вероятностей; $Bi(k,p)$ - биномиальный закон распределения с параметрами k,p; $\delta_{i,j}$ - символ Кронекера. Математическую модель контейнера в достаточно общем случае можно представить последовательностью N-мерных двоичных случайных векторов-столбцов $x_1,x_2,\ldots,x_n$:

$$x_t=(x_{t1},x_{t2},\ldots,x_{tN})'\in V_N,\ t=1,\ldots,n,$$

где n определяет размер контейнера. Двоичный вектор $x_t\in V_N$ будем отождествлять с числом $<x_t>=x_{t1}+2^1x_{t2}+\ldots+2^{N-1}x_{tN},\ <x_t>\in A$.

Рассмотрим наиболее распространенный LSB-метод встраивания сообщения в наименее значимый 1-ый бит, причем механизм встраивания – “чисто случайный” [3,4]:

$$\tilde{x}_{t1}=\xi_t m_{\tau_t}+(1-\xi_t)x_{t1}=\begin{cases}x_{t1}, \xi_t=0,\\ m_{\tau_t}, \xi_t=1\end{cases},\ \tilde{x}_{tk}=x_{tk},\ k=2,\ldots,N, \qquad (1)$$

$$L\{\xi_t\}=Bi(1,\beta),\ \tau_t=\tau_t(\xi_1,\ldots,\xi_t)=\sum_{i=1}^{t}\xi_i,\ t=1,\ldots,n, \qquad (2)$$

где $\tilde{x}_t=(\tilde{x}_{t1},\ldots,\tilde{x}_{tN})'\in V_N$ - контейнер, содержащий встроенное сообщение, называемый стегоконтейнером; ξ_t- последовательность независимых в совокупности случайных величин Бернулли, $P\{\xi_t=1\}=1-P\{\xi_t=0\}=\beta$,

определяющая механизм встраивания сообщения; $\beta \in [0,1]$ – доля встроенных в контейнер бит сообщения; $m_t \in V$ – встраиваемое сообщение. Случайные последовательности $\{x_t\}$, $\{\xi_t\}$, $\{m_t\}$ являются взаимно независимыми.

Введем случайную величину η=\{число бит, в которых $\tilde{x}_t \neq x_t$\}:

$$\eta = \sum_{i=1}^{n} I\{\tilde{x}_t \neq x_t\}, \ \eta \in \{0,\ldots,n\}.$$

Следующая теорема позволяет установить точное распределение вероятностей стегоконтейнера x_t *и* случайной величины η.

Терема 1. Пусть $x_t \in V_N$ - последовательность одинаково распределенных двоичных случайных векторов с независимыми компонентами x_{t1}, $m_t \in V$ - двоичная случайная последовательность, представляющая собой встраиваемое сообщение, $P\{m_t = 1\} = 1 - P\{m_t = 0\} = p_1$, а стегоконтейнер $\tilde{x}_t$ строится согласно (1), (2). Тогда, если $\pi = (\pi_i)$ есть распределение вероятностей x_t: $\pi_i = P\{< x_t >= i\}$, $i \in A$, то распределение вероятностей стегоконтейнера $\tilde{x}_t$ и случайной величины η имеют вид:

$$\tilde{\pi}_{<J>} = P\{<\tilde{x}_t>=<J>\} = P\{\tilde{x}_t = J\} = (1-\beta)\pi_{<J>} + \beta p_1^{j_1}(1-p_1)^{1-j_1}\sum_{v=0}^{1}\pi_{<J>-j_1+v},$$

$$L\{\eta\} = \mathcal{B}i(n, \beta(1 - p_1 - \sum_{i=0}^{2^{N-1}-1}\pi_{2i} + 2p_1\sum_{i=0}^{2^{N-1}-1}\pi_{2i})). \tag{3}$$

На практике обычно имеют дело с большими выборками, поэтому вместо точных формул удобно использовать их асимптотический при $n \to \infty$ вариант:

$$L\{\eta\} \xrightarrow[n\to\infty]{} \mathcal{N}(np, np(1-p)),$$

где $p = \beta(1 - p_1 - \sum_{i=0}^{2^{N-1}-1}\pi_{2i} + 2p_1\sum_{i=0}^{2^{N-1}-1}\pi_{2i})$; $\mathcal{N}(a,D)$ - нормальный закон распределения вероятностей с параметрами a, D.

Введем в рассмотрение функционал, характеризующий указанное свойство:

$$\Delta_1(\tilde{\pi}) = \sum_{k=0}^{2^{N-1}-1}\sum_{v=0}^{1}(\tilde{\pi}_{2k+v} - c_k)^2 \geq 0, \ \ c_k = \frac{1}{2}\sum_{v=0}^{1}\tilde{\pi}_{2k+v}.$$

Следствие 1. В условиях теоремы 1, если $p_1 = 1/2$, то

$$\Delta_1(\tilde{\pi}) = (1-\beta)^2 \Delta_1(\pi).$$

Следствие 2. В условиях следствия 2, если $\beta = 1$, то $\Delta_1(\tilde{\pi}) = 0$, а если, вдобавок, $\{x_t\}$ – независимые случайные векторы, то

$$\hat{\Delta}_1 = \Delta_1(\hat{\tilde{\pi}}) \xrightarrow[n\to\infty]{P} 0,$$

где $\hat{\tilde{\pi}}$ - статистическая оценка распределения вероятностей $\tilde{\pi}$ стего-контейнера по наблюдаемой реализации $\tilde{x}_1, \ldots, \tilde{x}_n$:

$$\hat{\tilde{\pi}}_i = v_i / n, \;\; v_i = \sum_{t=1}^{n} \delta_{<\tilde{x}_t>,i}, \;\; i \in A.$$

Рассмотрим более сложную модель контейнера, учитывающую марковскую зависимость в последовательности $\{x_t\}$ двоичных N-векторов.

Терема 2. Пусть x_t – стационарная цепь Маркова с пространством состояний V_N, стационарным распределением вероятностей $\pi = (\pi_i)$ и матрицей вероятностей одношаговых переходов $P = (p_{ij})$, $m_t \in V$ – последовательность независимых случайных величин, представляющая собой встраиваемое сообщение, $P\{m_t = 1\} = 1 - P\{m_t = 0\} = p_1$, а стегоконтейнер $\tilde{x}_t$ строится согласно (1), (2). Тогда для двумерного распределения вероятностей $\tilde{\pi}_{<J>,<K>} = P\{\tilde{x}_{t-1} = J, \tilde{x}_t = K\}$, $J, K \in V_N$, стегоконтейнера $\tilde{x}_t$ справедливо выражение:

$$\tilde{\pi}_{<J>,<K>} = (1-\beta)^2 \pi_{<J>} p_{<J>,<K>} + \beta^2 p_1^{j_1+k_1} (1-p_1)^{2-(j_1+k_1)} \sum_{v,h=0}^{1} \pi_{<J>-j_1+v} p_{<J>-j_1+v,<K>-k_1+h} +$$

$$+\beta(1-\beta)\Big(p_1^{k_1}(1-p_1)^{1-k_1} \sum_{v=0}^{1} \pi_{<J>} p_{<J>,<K>-k_1+v} + p_1^{j_1}(1-p_1)^{1-j_1} \sum_{v=0}^{1} \pi_{<J>-j_1+v} p_{<J>-j_1+v,<K>}\Big).$$

Следствие 4. Если $\beta = 1, p_1 = 1/2$, то

$$\hat{\Delta}_2 = \Delta_2(\{\hat{\tilde{\pi}}_{<J>,<K>}\}) = \sum_{k=0}^{2^{N-1}-1} \sum_{l=0}^{2^{N-1}-1} \sum_{v_1,v_2=0}^{1} (\hat{\tilde{\pi}}_{2k+v_1,2l+v_2} - \hat{c}_{k,l})^2 \xrightarrow[n\to\infty]{P} 0,$$

где $\hat{\tilde{\pi}}_{i,j} = \sum_{t=2}^{n} \delta_{<\tilde{x}_{t-1}>,i} \cdot \delta_{<\tilde{x}_t>,j} / (n-1)$, $i, j \in A$, $\hat{c}_{k,l} = \sum_{v_1,v_2=0}^{1} \hat{\tilde{\pi}}_{2k+v_1,2l+v_2} / 4$.

Рассмотрим более общий случай, когда сообщение встраивается в N_1 наименее значимых бит. Обозначим: $N = N_1 + N_2$, $1 \le N_1 \le N$, $m_\tau = (m_{\tau 1}, \ldots, m_{\tau N_1}) \in V_{N_1}$, $J = (J_{(1)'}, J_{(2)'})' \in V_N, J_{(1)} \in V_{N_1}$, $\tilde{x}_t = (\tilde{x}_{t(1)'}, \tilde{x}_{t(2)'})'$, $\tilde{x}_{t(1)} \in V_{N_1}, \tilde{x}_{t(2)} \in V_{N-N_1}$. Стегоконтейнер $\tilde{x}_t$ строится согласно обобщению (1):

$$\tilde{x}_{t(2)} = x_{t(2)}, \;\; \tilde{x}_{t(1)} = \xi_t m_{\tau_t} + (1-\xi_t)x_{t(1)} = \begin{cases} x_{t(1)}, \xi_t = 0, \\ m_{\tau_t}, \xi_t = 1 \end{cases}, \;\; t = 1,\ldots,n, \qquad (4)$$

где случайные величины $\{\xi_t\}$ и функция τ_t определены в (2). Теорема 3 допускает следующее обобщение на случай $N_1 > 1$.

Терема 3. Пусть x_t - стационарная цепь Маркова с пространством состояний V_N, стационарным распределением вероятностей $\pi = (\pi_i)$ и матрицей вероятностей одношаговых переходов $P = (p_{ij})$, $m_t \in V_{N_1}$ – последовательность независимых случайных векторов, представляющая собой встраиваемое сообщение, $P\{m_t = J_{(1)}\} = p_{<J_{(1)}>}$, $J_{(1)} \in V_{N_1}$, а стегоконтейнер строится согласно (4). Тогда для двумерного распределения вероятностей $\tilde{\pi}_{<J>,<K>} = P\{\tilde{x}_{t-1} = J, \tilde{x}_t = K\}$, $J, K \in V_N$, стегоконтейнера $\tilde{x}_t$ справедливо выражение:

$$\tilde{\pi}_{<J>,<K>} = (1-\beta)^2 \pi_{<J>} p_{<J>,<K>} + \beta^2 p_{<J_{(1)}>} p_{<K_{(1)}>} \sum_{v,h=0}^{2^{N_1}-1} \pi_{2^{N_1}<J_{(2)}>+v} p_{2^{N_1}<J_{(2)}>+v, 2^{N_1}<K_{(2)}>+h} +$$

$$+\beta(1-\beta)\Big(p_{<K_{(1)}>} \sum_{v=0}^{2^{N_1}-1} \pi_{<J>} p_{<J>,2^{N_1}<K_{(2)}>+v} + p_{<J_{(1)}>} \sum_{v=0}^{2^{N_1}-1} \pi_{2^{N_1}<J_{(2)}>+v} p_{2^{N_1}<J_{(2)}>+v,<K>}\Big).$$

Литература

1. *Anderson R. J.* Stretching the Limits of Steganography. LNCS. Vol. 1174. London: Springer-Verlag, 1996.
2. *Westfeld, A., Pfitzmann A.* Attacks on Steganographic Systems. LNCS. Vol. 1768. Springer-Verlag, 2000.
3. *Грибунин В. Г.* Цифровая стеганография. М.: Солон-Пресс. 2002.
4. *Пономарев К. И.* // Параметрическая модель вкрапления и ее статистический анализ. Дискретная математика. 2009. Том 21.
5. *Вечерко Е. В., Харин Ю. С.* // О некоторых задачах статистической проверки гипотез в стеганографии. Материалы международной конференции Информационные системы и технологии. Минск. 2009. С. 14–18.

ВЫДЕЛЕНИЕ СРЕДНИХ ЛИНИЙ ОБЪЕКТОВ НА ТРЕХМЕРНЫХ МЕДИЦИНСКИХ ИЗОБРАЖЕНИЯХ

Д. А. Гончаров

ВВЕДЕНИЕ

Выделение средних линий объектов является важным этапом в обработке изображений для последующих вычислений различных (линейных, площадных, объемных) характеристик объекта, а также описания и рас-