Утверждение 6. $w_{\mathrm{maj}}[i] = f_{\mathrm{maj}}(w_1[i], w_2[i], w_3[i]), i = 1, 2, \ldots, k$, где w_1, w_2, w_3 — любые попарно различные векторы из W.

Замечание 3. Из утверждений 5 и 6 следует, что если мощность множества пиратов больше или равна 3, то злоумышленник всегда может построить ИН, не идентифицирующий никого.

Описаный способ построения ложного ИН назовём мажорирующей атакой. Эта атака — частный случай атаки сговором, характеризующийся строго определенным выбором вектора из $I(P) \setminus P$. Согласно предложенному методу идентификации, построение вектора w_{maj} является единственным способом для группы злоумышленников избежать ответственности в полном объеме, т. е. ни один их них не будет вычислен. В связи с этим дальнейшая задача состоит в разработке узконаправленного метода идентификации, противостоящего мажорирующей атаке.

ЛИТЕРАТУРА

1. *Грибунин В. Г., Оков И. Н., Туринцев И. В.* Цифровая стеганография. М.: Солон-Пресс, 2002.
2. *Стружков Р. С., Соловьёв Т. М., Черняк Р. И.* Цифровые водяные знаки, устойчивые к атаке сговором // Прикладная дискретная математика. Приложение. 2009. № 1. С. 56–59.

УДК 519.651

О ВЫЯВЛЕНИИ ФАКТА ЗАШУМЛЕНИЯ КОНЕЧНОЙ ЦЕПИ МАРКОВА С НЕИЗВЕСТНОЙ МАТРИЦЕЙ ПЕРЕХОДНЫХ ВЕРОЯТНОСТЕЙ

А. М. Шойтов

Задача выявления факта наличия вкраплений в случайных последовательностях исследована в целом ряде работ (см., например, [1 – 4]. При этом обычно предполагаются известными тип и параметры распределения исходной последовательности. Так, в [4] рассмотрена последовательность, полученная по полиномиальной схеме с известными вероятностями исходов, и установлено, что гарантированно обнаружить факт наличия независимых вкраплений возможно только в случае, когда объем вкраплений растет по порядку быстрее корня от длины исходной последовательности. Аналогичный факт установлен в [3] для последовательности, образующей простую цепь Маркова с известной матрицей переходных вероятностей. В тезисах приводится обобщение результата [3] на случай простой цепи Маркова с неизвестной матрицей переходных вероятностей.

Пусть $X = \{X_1, ..., X_n, ...\}$ — простая конечная неразложимая и ацикличная цепь Маркова с N исходами, которые, не ограничивая общности, будем обозначать числами $1, ..., N$, и фиксированной матрицей переходных вероятностей $\Pi = \|\pi_{a,b}\|_{N\times N}$. Соответственно определены стационарные вероятности цепи X, которые обозначим через $(\pi_1, ..., \pi_N)$.

Будем предполагать, что на множестве $A = \{1, ..., N\}$ задана последовательность независимых случайных преобразований $\Phi = \{\varphi_1, ..., \varphi_n, ...\}$, полученных по схеме серий (n — номер серии) так, что для всех $i \neq j$, $i, j = 1, ..., n, ...$, преобразования φ_i и φ_j независимы и каждое из них определяется одной матрицей переходных вероятностей $P = \|p_{a,b}\|_{N\times N}$ по правилу $\mathbf{P}\{\varphi_i(a) = b\} = p_{a,b}$, $i = 1, ..., n, ...$ Определим случайную

последовательность $Z = \{Z_1, ..., Z_n, ...\}$ следующим образом: $Z_i = \varphi_i(X_i)$, $i = 1, ..., n, ...$, и будем писать $Z = \Phi(X)$.

Относительно наблюдаемой последовательности Y алфавита A выдвигаются две сложные гипотезы H_0: $Y = X$ и H_1: $Y = \Phi(X)$. Причем при обеих гипотезах, в отличие от [3], будем предполагать, что матрица $\Pi = \|\pi_{a,b}\|_{N\times N}$ неизвестна, а матрица $P = \|p_{a,b}\|_{N\times N}$ также неизвестна, но удовлетворяет ограничению $\lim\limits_{n\to\infty} p_{a,a} = 1$, $a \in A$.

Определим статистику

$$\chi_n^2 = \sum_{a,b,c\in A} \frac{\left(\nu_{abc} - \nu_{ab}\nu_{bc}/\nu_b\right)^2}{\nu_{ab}\nu_{bc}/\nu_b},$$

где $\nu_{abc} = \sum\limits_{i=1}^{n} \mathbf{I}\{Y_i = a, Y_{i+1} = b, Y_{i+2} = c\}$; $\nu_{ab} = \sum\limits_{i=1}^{n} \mathbf{I}\{Y_i = a, Y_{i+1} = b\}$; $\nu_a = \sum\limits_{i=1}^{n} \mathbf{I}\{Y_i = a\}$, $a, b, c \in A$. Статистики типа χ_n^2 применяются для различения гипотез о порядке цепи Маркова (см., например, [5]). Известно, что при гипотезе H_0 при $n \to \infty$ распределение χ_n^2 сходится к распределению хи-квадрат с N степенями свободы.

При сделанных предположениях справедлива следующая теорема.

Теорема 1. Если при $n \to \infty$ матрица переходных вероятностей P преобразований Φ меняется так, что для некоторых $a, b, c \in A$ выполнено условие

$$\sqrt{n} \sum_{\substack{y\in A \\ y\neq b}} p_{y,b}\left(\pi_{b,c} - \pi_{y,c}\right)\left(\pi_y \pi_{a,b} - \pi_b \pi_{a,y}\right) \to \infty,$$

то статистический критерий различения гипотез H_0 и H_1 на основе статистики χ_n^2 является состоятельным.

Следствие 1. Если при $n \to \infty$ для всех $a \neq b$, $a, b \in A$, справедливы оценки $p_{a,b} = f(n)\big(1 + o(1)\big)$ и $\sqrt{n} f(n) \to \infty$, стационарное распределение $(\pi_1, ..., \pi_N)$ цепи X является равномерным и в матрице $\Pi = \|\pi_{a,b}\|_{N\times N}$ есть хотя бы два различных элемента, то критерий различения гипотез H_0 и H_1 на основе статистики χ_n^2 является состоятельным.

Замечание. Статистика χ_n^2 применима для различения гипотез H_0 и H_1 только в случае, когда известно, что последовательность X образует *простую* цепь Маркова.

ЛИТЕРАТУРА

1. *Иванов В. А.* Модели вкраплений в однородные случайные последовательности // Труды по дискретной математике. 2008. Т. 10. С. 18–34.
2. *Пономарев К. И.* Параметрическая модель вкрапления и ее статистический анализ // Дискретная математика. 2009. Т. 21. № 4. С. 148–157.
3. *Filler T., Ker A. D., Fridrich J.* The square root law of steganographic capacity for Markov covers // Proc. SPIE. 2009. V. 7254, 725408. P. 31–47.
4. *Ker A. D.* A capacity result for batch steganography // IEEE Signal Processing Letters. 2007. V. 14(8). P. 525–528.
5. *Ивченко Г. И., Глибоченко А. Ф., Иванов В. А., Медведев Ю. И.* Статистический анализ дискретных случайных последовательностей. М.: МИЭМ, 1984. 92 с.