2. *Wayner P.* Disappearing Cryptography, Second Edition — Information Hiding: Steganography and Watermarking. Elsevier, 2002. 413 p.
3. *Cox I., Miller M., Bloom J., et al.* Digital Watermarking and Steganography. Elsevier, 2008. 593 p.
4. *Cachin C.* An Information-Theoretic Model for Steganography // LNCS. 1998. V. 1525. P. 306–318.

УДК 681.511:3

СТЕГОСИСТЕМЫ ИДЕНТИФИКАЦИОННЫХ НОМЕРОВ, УСТОЙЧИВЫЕ К АТАКЕ СГОВОРОМ[1]

Т. М. Соловьёв, Р. И. Черняк

В связи с бурным развитием медиаиндустрии в настоящее время все более актуальной становится задача защиты интеллектуальной собственности от противоправных действий. Ежегодно медиапиратство наносит колоссальные убытки видео- и аудиоиндустриям. Основной статьей дохода кинокомпаний по-прежнему является прокат фильмов в кинотеатрах, в то время как современные сервисы IPTV, Internet TV и другие остаются в стороне. Такая ситуация во многом обуславливается высокими рисками утечки премьерного фильма и, как следствие, снижения интереса к нему у пользователей.

В настоящее время для защиты от копирования и несанкционированного использования медиаконтента широко применяется такой класс цифровых водяных знаков (ЦВЗ), как идентификационные номера (ИН).

ЦВЗ могут содержать некоторую информацию о собственнике материала или о месте и времени его производства.

В случае применение ИН в контейнер, предназначеный каждому пользователю, внедряется персональный номер, позволяющий контролировать дальнейший путь этого контейнера. Если пользователь окажется медиапиратом и начнет распространение своей копии, то идентификационный номер позволит быстро определить его.

Согласно терминологии, используемой в работе [1], множества ИН называются *стегосистемами идентификационных номеров*. При этом, помимо типичных атак для ЦВЗ, таких, как перекодирование, аффинные и другие преобразования, для стегосистем ИН существует очень опасная *атака сговором*.

Под атакой сговором понимается следующее. Злоумышленник побитно сравнивает имеющиеся у него копии некоторого медиаданного, содержащие различные ИН, и заключает, что биты, в которых сравниваемые данные различаются, суть биты ИН. Затем он устанавливает эти биты в некоторые значения так, чтобы полученный ИН, называемый *ложным*, не совпадал ни с одним из использованных при сравнении. При этом злоумышленник преследует одну из следующих целей: уничтожить ИН либо изменить его таким образом, чтобы он идентифицировал кого-то другого.

Данная работа является продолжением работы [2]. Предлагается решение для противостояния атаке сговором. Продолжается исследование структуры стегосистем идентификационных номеров, устойчивых к данной атаке. Определяется наиболее опасный случай атаки сговором — *мажорирующая атака*. Обсуждается проблема идентификации группы пиратов с помощью полученного ими ложного ИН.

[1]Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № П1010).

В работе [2] было показано, что для успешного противостояния атаке сговором необходимо использовать *допустимые* множества.

Определение 1. Множество $W_n \subset \{0,1\}^n$ (или W, если длина не существенна) называется допустимым, если каждому подмножеству $P \subseteq W_n$ взаимно-однозначно сопоставляется наименьший интервал $I(P)$, его покрывающий.

Далее интервал $I(P)$ будем называть *соответствующим* множеству P.

Замечание 1. В рамках решаемой задачи, достаточно ограничиться рассмотрением таких W_n, для которых $I(W_n) = \underbrace{- - \ldots -}_{n}$.

Некоторые свойства допустимых множеств

Свойство 1. Если W_n допустимое, то $|W_n| \leqslant n$.

Данное свойство налагает ограничение на количество пользователей системы. К примеру, для того чтобы обеспечить идентификационными номерами сеть из восьми миллионов пользователей, длина каждого из этих номеров должна быть не менее мегабайта. Такой объем дополнительного материала является существенным, и его дальнейшее увеличение может создавать проблемы на этапе внедрения.

Свойство 2. Все допустимые множества максимальной мощности ($|W_n| = n$) имеют вид $O_1(a)$, где $O_1(a) = \{x \in \{0,1\}^n : d_H(a,x) = 1\}$, $d_H(a,x)$ — расстояние по Хэммингу между векторами a и x.

Иными словами, любое допустимое множество максимальной мощности — это сфера радиуса один с некоторым вектором a в качестве центра.

Матричное представление стегосистем ИН

Рассмотрим допустимое множество W_n мощности k. Представим его в виде булевой матрицы $\|W\|_{k\times n}$, строками которой будут векторы из множества W_n. Матрицы, соответствующие допустимым множествам, будем называть допустимыми:

$$W_n = \begin{pmatrix} w_1[1] & w_1[2] & \ldots & w_1[n] \\ w_2[1] & w_2[2] & \ldots & w_2[n] \\ \vdots & \vdots & \ddots & \vdots \\ w_k[1] & w_k[2] & \ldots & w_k[n] \end{pmatrix}_{k\times n}.$$

Исходя из свойств 1 и 2, целесообразно рассматривать матрицы, для которых $k < n$.

Определим следующие операции над допустимыми матрицами:

1) перестановка столбцов и строк;
2) инверсия столбца;
3) удаление повторяющихся столбцов.

Утверждение 1. Применение операций 1–3 никак не влияет на свойство допустимости.

Определение 2. Матрицы A и A' назовем эквивалентными, если они могут быть получены друг из друга путем применения определенных выше операций.

Определение 3. Допустимые множества W и W' назовем эквивалентными, если соответствующие им допустимые матрицы эквивалентны.

Утверждение 2. В каждом классе эквивалентности существует матрица $W_n = (E_k A_{n-k})$, где

$$E_k = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}_{k \times k}, A = \|A\|_{k \times (n-k)}.$$

Определение 4. Множество W называется *сильно допустимым*, если удаление любого столбца в соответствующей ему матрице влечет потерю свойства допустимости.

Утверждение 3. Матрица, соответствующая любому сильно допустимому множеству, эквивалентна E_k.

Утверждение 4. Пусть W_n — допустимое множество. Тогда существует матрица $W'_n = (E_k A)$, эквивалентная матрице W_n, в котрой подматрица A не является допустимой.

Замечание 2. Из утверждений 2 – 4 следует, что свойство допустимости основывается на наличии подматрицы, эквивалентной единичной. Оставшаяся часть не влияет на допустимость и может быть выбрана произвольно.

Идентификация злоумышленников по ложному ИН

Рассмотрим сильно допустимое множество, заданное матрицей E_k. В каждом столбце этой матрицы все элементы, за исключением одного, равны нулю. Значит, единица в какой-либо компоненте ложного ИН может появиться в том и только в том случае, если соответствующий пользователь принимал участие в атаке сговором. В соответствии с этим, идентифицировать участников сговора по построенному ими ложному ИН возможно во всех случаях, кроме одного — когда ИН состоит из всех нулей. Наблюдая единицу в i-й компоненте ложного ИН, заключаем, что i-й пользователь участвовал в сговоре. При инвертировании i-го столбца в матрице E_k на злоумышленника укажет единственный ноль в i-м столбце. Покомпонентно просматривая ложный ИН, можно сделать вывод о степени вины каждого участника. Злоумышленниками окажутся пользователи с номерами i, такими, что $w'[i] = \overline{f}_{\text{maj}}(w_1[i], w_2[i], \dots, w_k[i])$, где w' — ложный ИН, а f_{maj} — мажоритарная функция.

Согласно утверждению 2, описанный способ идентификации злоумышленников может быть использован в любом допустимом множестве.

Мажорирующая атака

При использовании предложенного метода идентификации всегда существует ложный ИН, который не идентифицирует никого:

$$w[i] = f_{\text{maj}}(w_1[i], w_2[i], \dots, w_k[i]), i = 1, 2, \dots, k.$$

Далее будем обозначать его w_{maj}. Возникает закономерный вопрос: всегда ли злоумышленник может построить w_{maj} и существует ли стратегия, позволяющая строить именно его, а не какой-либо случайный вектор из интервала, соответствующего имеющимся у него ИН?

Утверждение 5. Если мощность множества пиратов P больше или равна 2, то w_{maj} принадлежит $I(P)$.

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