ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 19 МАТЕМАТИКИ Выпуск 5
2012

Ф. К. Алиев, **А. В. Зайцева**, **И. В. Костенюк** (Москва, ТВП, МГТУ). **Элементы энтропийного подхода в стеганографии.**

Напомним [3], что обобщенно *встраивание* (*внедрение*) сообщения m (представленного в виде двоичной конечной последовательности длины l) в стеганографический контейнер (из n пикселей (в случае изображений или видеосигналов) или сэмплов (в случае аудиосигналов)) после или на этапе выполнения квантования стандартным алгоритмом сжатия цифрового мультимедийного сигнала осуществляется в соответствии с правилом, суть которого заключается в изменении квантованных коэффициентов (являющихся целыми числами) $g_1, g_2, \ldots, g_n$ и получении новых квантованных коэффициентов $\widetilde{g}_1, \widetilde{g}_2, \ldots, \widetilde{g}_n$, являющихся такими целыми числами, что для некоторой функции H_k от n переменных (заранее выбранной из множества функций $\{H_k | k \in K\}$, являющегося структурной компонентой стеганографического алгоритма с пространством ключей K), $H_k : \underbrace{Z \times Z \times \cdots \times Z}_{n \text{ раз}} \to \underbrace{\{0,1\} \times \{0,1\} \times \cdots \times \{0,1\}}_{l \text{ раз}}$, справедливо соотношение $H_k(\widetilde{g}_1, \widetilde{g}_2, \ldots, \widetilde{g}_n) = m$, где Z — множество целых чисел, $\times$ – знак декартова произведения множеств.

Извлечение сообщения m из стеганограммы осуществляется путем выбора по ключу $k \in K$ функции H_k и вычисления значения m функции H_k на наборе целых чисел $\widetilde{g}_1, \widetilde{g}_2, \ldots, \widetilde{g}_n$: $m = H_k(\widetilde{g}_1, \widetilde{g}_2, \ldots, \widetilde{g}_n)$.

Дополнительно будем полагать выполненным еще следующее:

a) для внедрения в контейнер одного элемента $m_s \in \{0,1\}$ (где $s \in \{1, 2, \ldots, l\}$) двоичного сообщения $m = (m_1, m_2, \ldots, m_l)$ используется τ элементов контейнера и, следовательно, для скрытия всего сообщения m используется $n = \tau l$ элементов контейнера;

b) элементы множества функций $\{H_k |\, k \in K\}$, являющегося структурной компонентой стеганографического алгоритма с пространством ключей K, устроены таким образом, что для любого $k \in K$ существует такой набор функций $\{H_{kj} |\, j \in \mathbf{N}\}$, что $H_{kj} : \underbrace{Z \times Z \times \cdots \times Z}_{\tau \text{ раз}} \to \{0,1\}$ для любого числа $j \in \mathbf{N}$ и справедливы равенства: $m = H_k(\widetilde{g}_1, \widetilde{g}_2, \ldots, \widetilde{g}_n) = (H_{k1}(\widetilde{g}_{i_1}, \widetilde{g}_{i_2}, \ldots, \widetilde{g}_{i_\tau}) \;\; H_{k2}(\widetilde{g}_{i_{\tau+1}}, \widetilde{g}_{i_{\tau+2}}, \ldots, \widetilde{g}_{i_{2\tau}}) \;\; \ldots \;\; H_{kl}(\widetilde{g}_{i_{(l-1)\tau+1}}, \widetilde{g}_{i_{(l-1)\tau+2}}, \ldots, \widetilde{g}_{i_{l\tau}}))$, где $H_{k1}(\widetilde{g}_{i_1}, \widetilde{g}_{i_2}, \ldots, \widetilde{g}_{i_\tau}) = m_1$, $H_{k2}(\widetilde{g}_{i_{\tau+1}}, \widetilde{g}_{i_{\tau+2}}, \ldots, \widetilde{g}_{i_{2\tau}}) = m_2$, $\ldots$, $H_{kl}(\widetilde{g}_{i_{(l-1)\tau+1}}, \widetilde{g}_{i_{(l-1)\tau+2}}, \ldots, \widetilde{g}_{i_{l\tau}}) = m_l$ и $(\widetilde{g}_{i_1}, \widetilde{g}_{i_2}, \ldots, \widetilde{g}_{i_n})$ — некоторая перестановка множества элементов $(\widetilde{g}_1, \widetilde{g}_2, \ldots, \widetilde{g}_n)$, $(i_1, i_2, \ldots, i_n)$ — перестановка множества чисел $(1, 2, \ldots, n)$, зависящая от выбранного ключа $k \in K$;

c) для любого $k \in K$ и для любого $j \in \mathbf{N}$ существует такая булева функция $f_{kj}(x_1, x_2, \ldots, x_\tau)$ от τ переменных $x_1, x_2, \ldots, x_\tau$, что для любых целых чисел $a_1, a_2, \ldots, a_\tau$ справедливо равенство $H_{kj}(a_1, a_2, \ldots, a_\tau) = f_{kj}(b_1, b_2, \ldots, b_\tau)$, где $b_r = 0$, если a_r — четное число, или $b_r = 1$, если a_r — нечетное число, $r \in \{1, 2, \ldots, \tau\}$.

Очевидно, что при выполнении вышеуказанных дополнительных условий число искажений (изменений), внесенных в контейнер в процессе внедрения в него сообщения m, равно арифметической сумме чисел искажений, внесенных в контейнер при внедрении каждого бита данного сообщения.

Если, например, положить, что для любого $k \in K$ и для любого $j \in \mathbf{N}$

$$H_{kj}(a_1, a_2, \ldots, a_\tau) = \begin{cases} 0, & \text{если} \quad \sum_{r=1}^{\tau} a_r \text{ — четное число,} \\ 1, & \text{если} \quad \sum_{r=1}^{\tau} a_r \text{ — нечетное число,} \end{cases}$$

то справедливо равенство $f_{kj}(x_1, x_2, \ldots, x_\tau) = x_1 \oplus x_2 \oplus \cdots \oplus x_\tau$, где $\oplus$ — знак операции сложения по модулю 2. В этом случае для внедрения в контейнер элемента $m_s \in \{0, 1\}$ (где $s \in \{1, 2, \ldots, l\}$) сообщения m по ключу генерируются соответствующие номера элементов и выбираются сами элементы $g_{i_{(s-1)\tau+1}}, g_{i_{(s-1)\tau+2}}, \ldots, g_{i_{s\tau}}$ контейнера. При этом достаточно изменение не более одного из них для получения таких элементов $\widetilde{g}_{i_{(s-1)\tau+1}}, \widetilde{g}_{i_{(s-1)\tau+2}}, \ldots, \widetilde{g}_{i_{s\tau}}$, что $H_{ks}(\widetilde{g}_{i_{(s-1)\tau+1}}, \widetilde{g}_{i_{(s-1)\tau+2}}, \ldots, \widetilde{g}_{i_{s\tau}}) = m_s$. Действительно, если $m_s = 0$ и $\sum_{w=1}^{\tau} g_{i_{(s-1)\tau+w}}$ равна четному числу, то при внедрении не производятся никакие изменения, т. е. набор $(\widetilde{g}_{i_{(s-1)\tau+1}}, \widetilde{g}_{i_{(s-1)\tau+2}}, \ldots, \widetilde{g}_{i_{s\tau}})$ совпадает с набором $(g_{i_{(s-1)\tau+1}}, g_{i_{(s-1)\tau+2}}, \ldots, g_{i_{s\tau}})$ с учетом порядка. Если же $\sum_{w=1}^{\tau} g_{i_{(s-1)\tau+w}}$ равна нечетному числу, то при внедрении производится изменение одного из элементов $g_{i_{(s-1)\tau+1}}, g_{i_{(s-1)\tau+2}}, \ldots, g_{i_{s\tau}}$ путем прибавления или вычитания единицы в сторону, противоположную направлению операции округления стандартом сжатия при получении этого элемента. И в результате сумма полученных элементов $\widetilde{g}_{i_{(s-1)\tau+1}}, \widetilde{g}_{i_{(s-1)\tau+2}}, \ldots, \widetilde{g}_{i_{s\tau}})$ становится равной четному числу.

Аналогично, если $m_s = 1$ и $\sum_{q=w}^{\tau} g_{i_{(s-1)\tau+w}}$ равна нечетному числу, то при внедрении не производятся никакие изменения, т. е. набор $(\widetilde{g}_{i_{(s-1)\tau+1}}, \widetilde{g}_{i_{(s-1)\tau+2}}, \ldots, \widetilde{g}_{i_{s\tau}})$ совпадает с набором $(g_{i_{(s-1)\tau+1}}, g_{i_{(s-1)\tau+2}}, \ldots, g_{i_{s\tau}})$ с учетом порядка. Если же $\sum_{w=1}^{\tau} g_{i_{(s-1)\tau+w}}$ равна четному числу, то при внедрении производится изменение одного из элементов $g_{i_{(s-1)\tau+1}}, g_{i_{(s-1)\tau+2}}, \ldots, g_{i_{s\tau}}$ путем прибавления или вычитания единицы в сторону, противоположную направлению операции округления стандартом сжатия при получении этого элемента. И в результате сумма полученных элементов $\widetilde{g}_{i_{(s-1)\tau+1}}, \widetilde{g}_{i_{(s-1)\tau+2}}, \ldots, \widetilde{g}_{i_{s\tau}})$ становится равной нечетному числу.

Очевидно, функцию H_{ks} можно заменить на булеву функцию f_{ks}, используя соответственно вместо наборов $g_{i_{(s-1)\tau+1}}, g_{i_{(s-1)\tau+2}}, \ldots, g_{i_{s\tau}}$ и $\widetilde{g}_{i_{(s-1)\tau+1}}, \widetilde{g}_{i_{(s-1)\tau+2}}, \ldots, \widetilde{g}_{i_{s\tau}})$ элементов контейнера соответственно их наборы битов четности $b_{i_{(s-1)\tau+1}}, b_{i_{(s-1)\tau+2}}, \ldots, b_{i_{s\tau}}$ и $\widetilde{b}_{i_{(s-1)\tau+1}}, \widetilde{b}_{i_{(s-1)\tau+2}}, \ldots, \widetilde{b}_{i_{s\tau}})$ при внедрении и извлечении элемента m_s. Данное обстоятельство дает возможность вычислить важные с теоретической и практической точек зрения характеристики случайной величины $\xi(m)$, равной минимальному числу искажений, вносимых в контейнер в результате внедрения в него сообщения m. Действительно, предположим, что биты четности элементов пустого контейнера могут быть представлены как результат работы источника, который генерирует 0 и 1 по-тактно по схеме независимых испытаний с одной и той же вероятностью 0,5. А сообщение m — результат работы источника, который генерирует 0 и 1 по-тактно по схеме независимых испытаний соответственно с вероятностями p и q, где $p \geqslant 0$, $q \geqslant 0$, $p + q = 1$. Тогда, например, для математического ожидания $\mathbf{M}\,\xi(m)$ случайной величины $\xi(m)$ справедлива цепочка равенств $\mathbf{M}\,\xi(m) = \sum_{s=1}^{l} \mathbf{M}\,\xi(m_s) = \sum_{s=1}^{l}(0 \cdot \mathbf{P}\{\xi(m_s) = 0\} + 1 \cdot \mathbf{P}\{\xi(m_s) = 1\}) = 0,5\,l$, где $\mathbf{M}\,\xi(m_s)$ — математическое ожидание случайной величины $\xi(m_s)$, равной минимальному числу искажений, вносимых в контейнер при внедрении элемента m_s сообщения m, $s \in \{1, 2, \ldots, l\}$. Таким образом, при внедрении в контейнер одного бита сообщения, подлежащего скрытию, допускается в среднем 0,5 искажений (изменений). Отсюда следует, что если для любого $k \in K$ и для любого $s \in \{1, 2, \ldots, l\}$ булева функция f_{ks} задается равенством $f_{ks} = x_1 \oplus x_2 \oplus \cdots \oplus x_\tau$, то значение математического ожидания $\mathbf{M}\,\xi(m)$ случайной величины $\xi(m)$, равной минимальному числу искажений, вносимых в контейнер в результате внедрения в него произвольного двоичного сообщения m, не зависит от значений чисел p и q, т. е. не зависит от вероятностных параметров источника сообщений, подлежащих скрытию. Однако очевидна возможность уменьшения значения $\mathbf{M}\,\xi(m)$ путем учета значений вероятностных параметров p и q источника сообщений за счет выбора подходящих булевых функций f_{ks}, $k \in K$, $s \in \{1,2,\ldots,l\}$. Так, например, если $\mathbf{P}\{m_s = 0\} = p > q = \mathbf{P}\{m_s = 1\}$, то имеются основания предположить, что значение $\mathbf{M}\,\xi(m)$ может быть меньше, чем полученное выше значение 0,5 l, если булевы функции f_{ks}, $k \in K$, $s \in \{1,2,\ldots,l\}$, будут принимать значение 0 на большем числе двоичных наборов, чем значение 1. Однако это предположение требует соответствующего исследования для своего обоснования, так как при таком неравномерном делении двоичных наборов по значениям 0 и 1 булевых функций f_{ks}, $k \in K$, $s \in \{1,2,\ldots,l\}$, может оказаться недостаточным изменение не более одного элемента из $g_{i_{(s-1)\tau+1}}, g_{i_{(s-1)\tau+2}}, \ldots, g_{i_{s\tau}}$ для получения требуемого набора $\widetilde{g}_{i_{(s-1)\tau+1}}, \widetilde{g}_{i_{(s-1)\tau+2}}, \ldots, \widetilde{g}_{i_{s\tau}}$. Могут иметь место ситуации, требующие изменения двух и более элементов. В связи с этим имеет смысл выписать общее выражение для математического ожидания $\mathbf{M}\,\xi(m)$ случайной величины $\xi(m)$, равной минимальному числу искажений (изменений) элементов контейнера при внедрении в $n = \tau$ элементов контейнера сообщения m из одного бита, сгенерированного источником сообщений с параметрами p и q. Для упрощения записи далее индексы булевой функции f_{k1} будем опускать и писать просто f. Обозначим V_2^n множество двоичных векторов с n координатами $(n \in \mathbf{N})$, т. е. $V_2^n = \{(\alpha_1, \alpha_2, \ldots, \alpha_n) \,|\, \alpha_i \in \{0,1\}$, $i = 1,2,\ldots,n$, положим $A = \{v \in V_2^n \,|\, f(v) = 1\}$ и $B = \{v \in V_2^n \,|\, f(v) = 0\}$. С учетом этого можно указать, что множества A и B содержат соответственно такие системы подмножеств $\{A_1, A_2, \ldots, A_n\}$ и $\{B_1, B_2, \ldots, B_n\}$, что:

1) при $i \neq j$ справедливы равенства $A_i \cap A_j = \varnothing$, $B_i \cap B_j = \varnothing$;

2) $A_1 \cup A_2 \cup \cdots \cup A_n = A$, $B_1 \cup B_2 \cup \cdots \cup B_n = B$;

3) для любого $k \in \{1,2,\ldots,n\}$ множество векторов A_k таково, что если $A_k \neq \varnothing$, то каждый вектор $a^{(k)} \in A_k$ обладает тем свойством, что при инвертировании любых его координат в количестве меньшем, чем k, и неизменности остальных координат получается вектор, принадлежащий множеству A; но существует набор ровно из k координат вектора $a^{(k)}$, при инвертировании которых и неизменности остальных координат получается вектор, принадлежащий множеству B;

4) для любого $k \in \{1,2,\ldots,n\}$ множество векторов B_k таково, что если $B_k \neq \varnothing$, то каждый вектор $b^{(k)} \in B_k$ обладает тем свойством, что при инвертировании любых его координат в количестве меньшем, чем k, и неизменности остальных координат получается вектор, принадлежащий множеству B; но существует набор ровно из k координат вектора $b^{(k)}$, при инвертировании которых и неизменности остальных координат получается вектор, принадлежащий множеству A.

Тогда для математического ожидания $\mathbf{M}\,\xi(m)$ случайной величины $\xi(m)$, равной минимальному числу искажений (изменений) элементов контейнера при внедрении в n элементов контейнера сообщения m из одного бита, сгенерированного источником сообщений с параметрами p и q, верна цепочка равенств $\mathbf{M}\,\xi(m) = \mathbf{P}\{\xi(m) = 0\} \sum_{i=1}^{n} i\,\mathbf{P}\{v \in A_i\} + \mathbf{P}\{\xi(m) = 1\} \sum_{i=1}^{n} i\,\mathbf{P}\{v \in B_i\} = p\,2^{-n} \sum_{i=1}^{n} i\,y_i + q 2^{-n} \sum_{i=1}^{n} i\,z_i$, где $y_i = |A_i|$, $z_i = |B_i|$, $i = 1,2,\ldots,n$, v — вектор, состоящий из битов четности элементов контейнера, в которые внедряется сообщение.

Стеганографический метод, в котором внедрение в контейнер сообщения, подлежащего скрытию, оптимизируется с позиции уменьшения математического ожидания минимального числа искажений (изменений) элементов контейнера на один бит внедряемой информации путем учета и использования вероятностно-статистических характеристик источника сообщений назовем *энтропийным стеганографическим методом*, а соответствующие стеганографические алгоритмы — *энтропийными стеганографическими алгоритмами.*

Следует отметить имеющуюся здесь определенную аналогию с теорией кодирования, где термин «энтропия» широко используется в разделе «кодирование источников сообщений». И в этой теории с помощью понятия энтропии источника, отражающего

его вероятностно-статистические характеристики, предсказывается наилучшее сжатие информации, т. е. наименьшее в среднем число бит, необходимое для представления кодируемого сообщения, сгенерированного источником. Соответствующие процедуры кодирования называют *энтропийными.* Примером такого кодирования является кодирование Хаффмана [1].

При фиксированном источнике сообщений (т. е. при фиксированных значениях параметров p и q) и фиксированном числе $n \in \mathbf{N}$ энтропийный стеганографический метод назовем *оптимальным энтропийным стеганографическим методом* (а соответствующий алгоритм — *оптимальным энтропийным стеганографическим алгоритмом*), если при данном методе математическое ожидание минимального числа искажений (изменений) при внедрении двоичного сообщения, состоящего из одного бита m (сгенерированного источником) в n элементов контейнера, равно $\min \mathbf{M}\,\xi(m)$, где минимум берется по всевозможным функциям $f \in F_2^n$, F_2^n — множество всех двоичных функций от n переменных.

Таким образом, задача разработки оптимального энтропийного стеганографического алгоритма при фиксированном источнике сообщений (т. е. при фиксированных значениях параметров p и q) является задачей комбинаторной оптимизации [2] в силу конечности множеств F_2^n и V_2^n.

Оптимальный энтропийный стеганографический алгоритм внедрения информации в контейнер может быть получен путем перебора всех возможных разбиений множества V_2^n на два подмножества A и B с определением в них чисел $y_i = |A_i|$, $z_i = |B_i|$, $i = 1, 2, \ldots, n$, что само по себе является громоздкой процедурой, применимой лишь для небольших значений параметра n. По этой причине имеет смысл направить усилия на разработку не обязательно оптимальных, но приемлемых с практических позиций энтропийных стеганографических алгоритмов, допускающих существенно меньшие, чем 0,5, значения математического ожидания минимального числа искажений (изменений) при внедрении двоичного сообщения, состоящего из одного бита m (сгенерированного источником), в n элементов контейнера. Такие алгоритмы будем называть *субоптимальными энтропийными стеганографическими алгоритмами.* Различные варианты разработанных субоптимальных алгоритмов могут затем детально исследоваться для определения степени их близости к оптимальному алгоритму и определения лучшего из них.

СПИСОК ЛИТЕРАТУРЫ

1. *Вернер М.* Основы кодирования. М.: Техносфера, 2006, 288 с.
2. *Пападимитриу Х.*, *Стайглиц К.* Комбинаторная оптимизация. Алгоритмы и сложность. М.: Мир, 1985, 512 с.
3. *Fridrich J.* Steganography in Digital Media. Cambridge: Cambridge University Press, 2010.