ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 22 МАТЕМАТИКИ Выпуск 5
2015

Ю. Е. Рябинин (Краснодар, КВВУ)**. Повышение пропускной способности стеганографического канала связи методами модулярной арифметики.**

Открытый характер фактов передачи зашифрованных данных в информационно-телекоммуникационных системах общего пользования легко обнаруживается злоумышленником с помощью современных методов анализа трафика, что приводит к возможности реализации угрозы нарушения целостности передаваемых данных. Для устранения этой уязвимости могут быть использованы методы стеганографии [1]. Однако стеганографические каналы связи (СКС) характеризуются низкой пропускной способностью, под которой понимается максимальный средний объем информации передаваемой по данному каналу в единицу времени. Определим вектор $\vec{C}_i$ символов исходных зашифрованных данных (криптограмму), предназначенных для передачи по СКС:

$$\vec{C}_i = [\underbrace{a_{i,0} \quad a_{i,1} \quad \cdots \quad a_{i,j_1-1}}_{\vec{c}_{i,1}} \quad \underbrace{a_{i,j_1} \quad \cdots \quad a_{i,j_2-1}}_{\vec{c}_{i,2}} \quad \underbrace{a_{i,j_{k-1}} \quad \cdots \quad a_{i,j_k-1}}_{\vec{c}_{i,k}}]$$

для $\sum_{s=0}^{k-1} j_s$ цифр $a_{i,j_s} \in \{0,1\}$. Тогда, $\vec{C}_i$ можно представить: $\vec{C}_i = [\vec{c}_{i,1}\vec{c}_{i,2}\cdots\vec{c}_{i,k}]$.

Пусть $c_{i,1}, c_{i,2}, \ldots, c_{i,k}$ — целые неотрицательные числа, такие что: $0 \leqslant c_{i,1} = \sum_{s=0}^{l-1} a_{i,s}2^s < 2^l$, где $l = 1, 2, \ldots, j_k$.

Примем набор попарно простых модулей $p_1, p_2, \ldots, p_k$, где $2^l < p_k < 2^{l+1}$. Тогда числа $c_{i,1}, c_{i,2}, \ldots, c_{i,k}$ можно объявить наименьшими неотрицательными вычетами некоторого числа X_i. Согласно [2] любое число $X_i \geqslant 0$ однозначно представляется последовательностью $X_i = (c_1, c_2, \ldots, c_k)$, где $c_i = X_i \bmod p_i$; $i = 1, 2, \ldots, k$, при $0 \leqslant X_i < P$, где $P = \prod_{i=1}^{k} p_i$.

Тогда система сравнений: $X_i \equiv c_1 \bmod p_1$; $X_i \equiv c_2 \bmod p_2$; $\ldots$; $X_i \equiv c_i \bmod p_k$ имеет единственное решение X_i, если выполнены вышеуказанные условия.

Таким образом, криптограмма $\vec{C}_i$ в результате деконкатенации (разделение цепочек двоичных цифр) разбивается на равные части $\vec{c}_{i,1}$, $\vec{c}_{i,2}$, $\ldots$, $\vec{c}_{i,k}$, которые сопоставляются символам модулярного кода (МК), то есть являются вычетами некоторого числа X_i. Для повышения достоверности передаваемой информации выполняется операция расширения полученного МК путем введения избыточных оснований $p_{k+1}, \ldots, p_{k+r}$ и получения избыточных вычетов $c_{k+1} = X_i \bmod p_{k+1}, \ldots, c_{k+r} = X_i \bmod p_{k+r}$. Будем предполагать, что $p_1 < p_2 < \cdots < p_k < p_{k+1} < \cdots < p_{k+r}$.

В стегокодере по заданному алгоритму и ключу K выполняется встраивание вычета c_i в контейнер T_i в соответствии со следующими зависимостями стеганографического преобразования в общем виде [3]: $T^* = F(T, K, X); C = D(T^*, K)$, где T — множество контейнеров-оригиналов; X — множество секретных сообщений; K — множество секретных ключей; F, D — функции прямого и обратного стеганографических преобразований соответственно; T^* — множество контейнеров-результатов.

Таким образом, представление вектора $\vec{X}_i = [\vec{c}_{i,1}\ \vec{c}_{i,2}\ \cdots\ \vec{c}_{i,k}\ \vec{c}_{i,k+1} \cdots \vec{c}_{i,k+r}]$ в расширенном МК позволяет обнаруживать и исправлять ошибки в целях повышения устойчивости стеганографической системы [2], где под q-кратной ошибкой понимается произвольное искажение q вычетов c_i. И представление в МК позволяет встраивать вычеты $(c_{i,k+r})$ в «многоформатном» режиме (встраивание информации в различные виды контейнеров (фото, видео, звук и т. д.)), что способствует повышению пропускной способности СКС.

СПИСОК ЛИТЕРАТУРЫ

1. *Рябинин Ю. Е.*, *Финько О. А.* Устойчивая к атакам стеганографическая система в расширенном модулярном коде. — Изв. ЮФУ. Технические науки. Таганрог, 2014, № 2(151), с. 167–174.
2. *Акушский И. Я.*, *Юдицкий Д. И.* Модулярная арифметика в остаточных классах. М.: Сов. Радио, 1968, 440 с.
3. *Грибунин В. Г.*, *Оков И. Н.*, *Туринцев И. В.* Цифровая стеганография. М.: Солон-Пресс, 2009, 260 с.