О МЕТОДАХ СТЕГАНОГРАФИИ, ОСНОВАННЫХ НА РАЗЛОЖЕНИИ КОНТЕЙНЕРА ПО ОРТОНОРМИРОВАННОМУ БАЗИСУ

Д. П. Глиндзич

Пусть $\widetilde{x} = (\widetilde{x}_1,...,\widetilde{x}_N)^T \in R^N$ – реализация случайного процесса, представленная в виде последовательности N его отсчетов, которые предлагается использовать как контейнер [1;2]. Без потери общности полагаем:

$$E\{\widetilde{x}\} = 0_N, \quad E\{\widetilde{x}\widetilde{x}^T\} = \Sigma, \quad |\widetilde{x}_i| < C, i = \overline{1,N}.$$

Проведем «равномерное» квантование отсчетов $\widetilde{x}_i, \quad i = \overline{1,N}$, для хранения их с использованием n битов памяти:

$$h := \frac{C}{2^{n-1}}, \quad x_i = \left[\frac{\widetilde{x}_i}{h}\right], i = \overline{1,N}.$$

Обозначим через $x = (x_1,...,x_N)^T, \quad x_i \in \{-2^{n-1}+1,...,0,...,2^{n-1}-1\} = A$, $i = \overline{1,N}$, квантованную реализацию случайного процесса. Будем рассматривать x как блок для встраивания скрытого сообщения, считая, что он имеет необходимый для этого размер.

Пусть задана плотность распределения вероятностей случайного вектора $\widetilde{x} = (\widetilde{x}_1,...,\widetilde{x}_N)^T \in R^N$. Обозначим ее как $\widetilde{p}_{(\widetilde{x}_1,...,\widetilde{x}_N)}(z_1,...,z_N)$, тогда справедлива следующая

Лемма 1. Дискретное распределение вероятностей квантованного блока имеет вид:

$$p_{x_1,...,x_N}(k_1,...,k_N) = P\{x = (k_1,...,k_N)^T\} = \int_{hk_1}^{h(k_1+1)} ... \int_{hk_N}^{h(k_N+1)} \widetilde{p}_{\widetilde{x}_1,...,\widetilde{x}_N}(z_1,...,z_N)dz_1...dz_N,$$

$$k_1,...,k_N \in A, \quad \sum_{k_1,...,k_N \in A} p_{x_1,...,x_N}(k_1,...,k_N) = 1.$$

Пусть в пространстве R^N задан ортонормированный базис $\{\psi_1,...,\psi_N\}$, тогда однозначно определяется вектор $y = (y_1,...,y_N)^T$ коэффициентов разложения x по этому базису:

$$y = \Psi^T x, \quad \Psi = (\psi_1 \vdots \psi_2 \vdots ... \vdots \psi_N) = \begin{pmatrix} \psi_{11}\ \psi_{12} \cdots \psi_{1N} \\ \psi_{21}\ \psi_{22} \cdots \psi_{2N} \\ \cdots \\ \psi_{N1}\ \psi_{N2} \cdots \psi_{NN} \end{pmatrix}.$$

Пусть встраивание скрытого сообщения $m = (m_1,...,m_M) \in R^M$, $1 \le M < N$, осуществляется путем замены *(N-M)* коэффициентов разложения x по $\{\psi_i\}_{i=1}^N$. Для определенности будем полагать, что m встраивается за счет замены последних *N-M* коэффициентов $y_{N-M},...,y_N$, $y_i \in R, i \in \{1,2,...,N\}$ на соответствующие отсчеты $m_1,...,m_M$. Обозначим измененный вектор коэффициентов $y^* = (y_1, y_2,...y_{N-M}, m_1,...,m_M)^T$. Стеганограмма x^* вычисляется по формуле:

$$x^* = \Psi y^*, \quad x^* \in R^N.$$

Необходимо подчеркнуть, что в общем случае полученная стеганограмма x^* не будет иметь целочисленных отсчетов.

Пусть сообщение $(m_1,...,m_M)$ − случайный вектор и известно его распределение вероятностей:

$$\hat{q}_{m_1,...,m_M}(l_1,...,l_M) = P\{m = (l_1,...,l_M)^T\}.$$

Обозначим $p^*_{x_1,...,x_N}(k_1,...,k_N) = P\{x^* = (k_1,...,k_N)^T\}$ − распределение вероятностей стеганограммы. Справедлива следующая теорема:

Теорема 1. Распределение вероятностей стеганограммы имеет вид:

$$p^*_{x_1,...,x_N}(k_1,...,k_N) = q_{y_1,...,y_{N-M}}(\psi_1^T k,...,\psi_{N-M}^T k) \cdot \hat{q}_{m_1,...,m_M}(\psi_{N-M+1}^T k,...,\psi_N^T k),$$

$$k = (k_1,...,k_N)^T \in A^N, \quad \sum_{k_1,...,k_N \in A} p^*_{x_1,...,x_N}(k_1,...,k_N) = 1.$$

Для использования описанного выше метода скрытой передачи информации в цифровых каналах связи необходимо, чтобы стеганограмма x^* имела отсчеты из множества целых чисел. Пусть $X \subseteq N_0^N$ – множество сообщений, передаваемых по цифровому каналу связи (т.е. контейнеров и стеганограмм) и $Y \subseteq R^N$ – множество коэффициентов разложения контейнеров $x = (x_1,...,x_N)^T \in X$ по ортонормированному базису

$$\{\psi_1,...,\psi_N\},\ \psi_i = \left(\psi_{1i}, \psi_{2i}, \ldots, \psi_{Ni}\right)^T \in R^N,\ i \in \{1,2,...,N\}.$$

Рассмотрим метод встраивания скрываемых данных $m = (m_1,...,m_M)$, имеющих целые отсчеты, в коэффициенты $y = (y_1,...,y_N)^T \in Y$ так, чтобы стеганограмма $x^* = \Psi y^*$ принадлежала множеству *X*. Для этого специальным образом строится отображение $G_\Psi : X \to Y \cap Z^N$, обладаю-

щее свойством сюръективности. Тогда можно утверждать, что при встраивании скрываемого сообщения в коэффициенты $z = G_\Psi(x)$ разложения по ортонормированному базису Ψ, получаемые стеганограммы будут иметь целочисленные отсчеты.

Рассмотрим данный метод встраивания в случае, когда в качестве ортонормированного базиса $\{\psi_1,...,\psi_N\}$ выбирается базис Карунена-Лоэва, который определяется при решении задачи на собственные значения:

$$\Sigma\psi_i = \nu_i\psi_i, i \in \{1,2,...,N\},$$

где Σ − ковариационная матрица, которая может быть выражена через ковариационную функцию исходного случайного процесса. Тогда относительная среднеквадратичная ошибка аппроксимации исходного сообщения *x* при встраивании скрытого сообщения будет равна:

$$\delta_M = \frac{\nu_{M+1} + ... + \nu_N}{\nu_1 + ... + \nu_N}.$$

Алгоритм:

- По заданному контейнеру $x = (x_1,...,x_N)^T \in X$ находим параметры преобразования G_Ψ.
- Находим вектор квантованных коэффициентов $(z_1, z_2,..., z_N)^T = G_\Psi(x)$.
- Осуществляем встраивание скрываемых данных в компоненты z, т.е. строим вектор $z^* = (z_1,..., z_{N-M}, m_1,..., m_M) \in Y \cap Z^N$.
- Вычисляем стеганограмму $x^* = G_\Psi^{-1}(z^*)$, которая в силу сюръективности используемого отображения будет иметь целые коэффициенты

Литература

1. Аграновский А. В., Девянин П. Н., Хади Р. А., Черемушкин А. В. Основы компьютерной стеганографии / М.: Радио и связь. 2003.
2. *Грибунин В. Г., Оков И. Н., Туринцев И. В.* Цифровая стеганография / М.:СОЛОН-пресс. 2002