грешностью порядка 10^{-8} . Однако при этом в подинтегральных функциях (8) появляется логарифмическая особенность. Для более точного их вычисления используются квадратурные формулы Гаусса с соответствующими весами, что в совокупности с (9) позволяет добиться приемлемой точности.

Для решения системы (7) применяется метод исключения Гаусса. Аналогично определяются граничные значения $q^{(1)}$. По известному решению на границе явным образом находятся значения потенциала внутри области

$$-\pi u_i^{(1)} = \sum_{j=1}^N w_{ij} u_{j-1/2}^{(1)} - \sum_{j=1}^N v_{ij} q_{j-1/2}^{(1)},$$

где $u_{j-1/2}^{(1)}$ и $q_{j-1/2}^{(1)}$ – известные значения потенциала и потока на границе, $u_i^{(1)}$ – искомое значение внутри области. Аналогичным способом определяется потенциал $u^{(2)}(\xi)$ в любой точке $\xi = (x, y)$ вне капли.

Преимущество метода граничных элементов для данной задачи над распространенным в настоящее время методом конечных элементов заключается в том, что он не требует введения сетки ни внутри капли, ни во внешней бесконечной области, а условие на бесконечности (4) выполняется точно.

Проведенный вычислительный эксперимент показал, что полученные результаты точно отражают структуру магнитного поля.

Литература

1. Береснев С. А. Комбинированный метод граничных и конечных элементов решения сопряженной задачи магнитостатики //61 конференция студентов и аспирантов БГУ. Мн., 2004.
2. Бреббия К., Теллес Ж., Вроубел Л. Методы граничных элементов/ Пер. с англ. Л. Г. Корнейчука; Под ред. И. Г. Григолюка. М.: Мир, 1987. 524 с.
3. Абрамовиц М., Стиган И. Справочник по специальным функциям М.:Наука, 1979.

ВЕРОЯТНОСТНЫЙ АНАЛИЗ LSB-МЕТОДА СТЕГАНОГРАФИИ ДЛЯ АУДИОСИГНАЛОВ

Д. П. Глиндзич

В данной работе рассматривается метод встраивания скрытого сообщения в наименее значащие биты элементов контейнера (LSB)[1]. Решаются задачи вычисления распределений вероятностей отсчетов и значений их битов и минимизации различия между распределениями вероятностей отсчетов контейнера и стеганограммы.

1. РАСПРЕДЕЛЕНИЕ ВЕРОЯТНОСТЕЙ ОТСЧЕТОВ СТЕГАНОГРАММ

Рассмотрим в качестве контейнера стационарный случайный процесс $\delta_t^0 \in R$ с дискретным временем $t \in N$. Пусть A – амплитуда процесса (полагаем, что $0 \leq x_t^0 < A$). Проведем процедуру равномерного квантования δ_t^0 на $M = 2^m$ уровней, в результате получим случайный процесс δ_t . Пусть задано значение $L \leq m, L \in N$. Осуществим двоичное разложение числа x_t и представим его в виде двоичного m -вектора:

$$X_t = \begin{pmatrix} x_{tm} \\ x_{t2} \\ \vdots \\ x_{t1} \end{pmatrix} = \begin{pmatrix} X_t^{(2)} \\ \text{---} \\ X_t^{(1)} \end{pmatrix}, \quad X_t \in \{0, 1\}^m, X_t^{(2)} \in \{0, 1\}^{m-L}, X_t^{(1)} \in \{0, 1\}^L, \quad t \in N.$$

Обозначим:

$$p_{tk} = P\{x_t = k\}, \quad k = 0, \dots, M-1, \quad \sum_{k=0}^{M-1} p_{tk} = 1,$$

$$p_{tk}^{(1)} = P\{\langle X_t^{(1)} \rangle = k\}, \quad k = 0, \dots, 2^L - 1, \quad \sum_{k=0}^{2^L-1} p_{tk}^{(1)} = 1, \quad \langle X_t \rangle = x_{t1} + 2x_{t2} + \dots + 2^{m-1}x_{tm}.$$

Утверждение 1. Пусть x_t^0 - гауссовский стационарный случайный процесс с одномерным распределением $N(\mu, \sigma^2)$. Тогда

$$p_{tk}^{(1)} = \sum_{i=0}^{2^{m-L}-1} \left[\Phi\left(\frac{(2^L i + k + 1)h - \mu}{\sigma}\right) - \Phi\left(\frac{(2^L i + k)h - \mu}{\sigma}\right) \right], \quad k = \overline{0, 2^L - 1},$$

$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{t^2}{2}} dt$ – функция распределения нормального закона.

Согласно LSB-методу [1], в m -мерном двоичном ряде X_t заменим L -мерные подвекторы младших битов $X_t^{(1)}$ на скрытое сообщение $\hat{X}_t^{(1)}$ с распределением вероятностей

$$\hat{p}_{tk}^{(1)} = P\{\langle \hat{X}_t^{(1)} \rangle = k\}, \quad k = \overline{0, 2^L - 1}, \quad \sum_{k=0}^{2^L-1} \hat{p}_{tk}^{(1)} = 1.$$

Полученный временной ряд называется [1], [2] стеганограммой:

$$X_t^* = \begin{pmatrix} X_t^{(2)} \\ \text{---} \\ \hat{X}_t^{(1)} \end{pmatrix} \in \{0, 1\}^m.$$

Утверждение 2. Пусть $p_{tk}^* = P\{< X_t^* >= k\}$, $k = \overline{0, 2^m - 1}$, $\sum_{k=0}^{2^m-1} p_{tk}^* = 1$ –

распределение вероятностей стеганограммы, $\hat{p}_{tk}^{(1)}$, p_{tk} – известные распределения вероятностей скрытого сообщения и контейнера соответственно. Тогда если X_t и $\hat{X}_t^{(1)}$ независимы, то

$$p_{tk}^* = \hat{p}_{tk^{(1)}}^{(1)} \cdot \sum_{j=0}^{2^L-1} p_{t, 2^L k^{(2)} + j}, \quad k = \overline{0, 2^m - 1}, \quad k^{(2)} = \left\lfloor \frac{k}{2^L} \right\rfloor, \quad k^{(1)} = k - 2^L k^{(2)}.$$

2. РАСПРЕДЕЛЕНИЯ ВЕРОЯТНОСТЕЙ БИТОВ ОТСЧЕТОВ СТЕГАНОГРАММ И КОНТЕЙНЕРОВ

Найдем распределения вероятностей случайных битов для процессов X_t и X_t^* . Обозначим:

$$p_{tk}^n = P\{x_{tn} = k\}, \quad k \in \{0, 1\}, \quad X_t = \begin{pmatrix} x_{tm} \\ \dots \\ x_{t1} \end{pmatrix}, \quad \sum_{k=0}^1 p_{tk}^n = 1, \quad n = \overline{1, m}.$$

Утверждение 3. Распределение вероятностей случайных битов контейнера X_t определяется формулой

$$p_{tk}^n = \sum_{j=0}^{2^{m-n}-1} \sum_{i=2^{n-1}k}^{2^{n+k-1}-1} p_{t, 2^n \cdot j + i}, \quad k \in \{0, 1\}, \quad n \in \{1, 2, \dots, m\}.$$

Следствие 1. Распределение вероятностей случайных битов стеганограммы X_t^* определяется формулой

$$p_{tk}^{*n} = \sum_{j=0}^{2^{m-n}-1} \sum_{i=2^{n-1}k}^{2^{n+k-1}-1} \hat{p}_{t, (2^n j + i)^{(1)}}^{(1)} \cdot \sum_{h=0}^{2^L-1} p_{t, 2^L (2^n j + i)^{(2)} + h}, \quad k \in \{0, 1\}, \quad n \in \{1, 2, \dots, m\},$$

$$(2^n j + i)^{(2)} = \left\lfloor \frac{2^n j + i}{2^L} \right\rfloor, \quad (2^n j + i)^{(1)} = 2^n j + i - 2^L (2^n j + i)^{(2)},$$

$\hat{p}_{tk}^{(1)} = P\{< \hat{X}_t^{(1)} >= k\}$, $k = \overline{0, 2^L - 1}$ – распределение вероятностей скрытого сообщения.

Следствие 2. Пусть x_t^0 – гауссовский стационарный случайный процесс с одномерным распределением $N(\mu, \sigma^2)$ и $\hat{p}_{tk}^{(1)} = P\{< \hat{X}_t^{(1)} >= k\}$, $k = \overline{0, 2^L - 1}$ – распределение вероятностей скрытого сообщения $\hat{X}_t^{(1)}$. Тогда распределение вероятностей битов стеганограммы X_t^* имеет вид:

$$p_{tk}^{*n} = \sum_{j=0}^{2^{m-n}-1} \sum_{i=2^{n-1}k}^{2^{n+k}-1} \hat{p}_{t(2^n j+i)^{(1)}}^{(1)} \left[\Phi \left(\frac{2^L ((2^n j+i)^{(2)} + 1)h - \mu}{\sigma} \right) - \Phi \left(\frac{2^L (2^n j+i)^{(2)} h - \mu}{\sigma} \right) \right],$$

$$(2^n j+i)^{(2)} = \left\lfloor \frac{2^n j+i}{2^L} \right\rfloor, \quad (2^n j+i)^{(1)} = 2^n j+i - 2^L (2^n j+i)^{(2)}, \quad k \in \{0,1\}, n \in \{1,2,\dots,m\}.$$

3. ЗАДАЧИ МИНИМИЗАЦИИ РАЗЛИЧИЯ МЕЖДУ РАСПРЕДЕЛЕНИЯМИ ВЕРОЯТНОСТЕЙ ЗНАЧЕНИЙ КОНТЕЙНЕРА И СТЕГАНОГРАММЫ

Для повышения стойкости стegosистемы необходимо обеспечить минимальное различие между распределениями вероятностей контейнера и стеганограммы [2]. Осуществим минимизацию различия между вероятностными распределениями исходного контейнера X_t и стеганограммы X_t^* за счет преобразования скрытого сообщения $\hat{X}_t^{(1)}$.

Рассмотрим $p_{tk}^* = P\{< X_t^* > = k\}$, $k = \overline{0, 2^m - 1}$, как функцию от распределения вероятностей скрытого сообщения $\hat{X}_t^{(1)}$, т.е.

$$p_{tk}^* = p_{tk}^*(\hat{p}_{tk^{(1)}}^{(1)}) = \hat{p}_{tk^{(1)}}^{(1)} \cdot \sum_{j=0}^{2^L-1} p_{t2^L k^{(2)}+j}, \quad k = \overline{0, 2^m - 1}.$$

Пусть $(j_0, \dots, j_{2^L-1})$ – перестановка последовательности чисел $(0, 1, \dots, 2^L - 1)$. Рассмотрим задачу минимизации различия между распределениями X_t и X_t^* по всем перестановкам:

$$\sum_{k=0}^{2^m-1} |p_{tk} - p_{tk}^*(\hat{p}_{tj_k^{(1)}}^{(1)})| \rightarrow \left(\min_{(j_0, \dots, j_{2^L-1})} \right),$$

или, что равносильно:

$$\sum_{k=0}^{2^m-1} |p_{tk} - \hat{p}_{tj_k^{(1)}}^{(1)} \cdot \sum_{j=0}^{2^L-1} p_{t2^L k^{(2)}+j}| \rightarrow \left(\min_{(j_0, \dots, j_{2^L-1})} \right), \quad k^{(2)} = \left\lfloor \frac{k}{2^L} \right\rfloor, \quad k^{(1)} = k - 2^L k^{(2)}. \quad (1)$$

Пусть $(j_0^*, \dots, j_{2^L-1}^*)$ – перестановка, минимизирующая (1). Осуществим «перекодировку» исходного скрытого сообщения:

$$f(\hat{X}_t^{(1)}) = \begin{pmatrix} \tilde{x}_{tL} \\ \dots \\ \tilde{x}_{t1} \end{pmatrix}, \quad \tilde{x}_{ti} = \frac{j_{<\hat{X}_t^{(1)}>}^*}{2^{i-1}} - 2 \cdot \left\lfloor \frac{j_{<\hat{X}_t^{(1)}>}^*}{2^i} \right\rfloor, \quad i = \overline{1, L}.$$

С уменьшением суммы $\sum_{k=0}^{2^m-1} |p_{tk} - p_{tk}^*(\hat{p}_{tj_k^{(1)}}^{(1)})|$ стойкость используемой стegosистемы повышается.

Для минимизации различия между распределениями вероятностей значений n -ых битов X_t и X_t^* , $n = \overline{1, m}$ решается задача:

$$\left| \sum_{j=0}^{2^{m-n}-1} \sum_{i=0}^{2^{n-1}-1} \left(p_{t \cdot 2^n \cdot j + i} - \hat{p}_{t \cdot j_{(2^n \cdot j + i)}^{(1)}} \cdot \sum_{h=0}^{2^L-1} p_{t \cdot 2^L \cdot (2^n + i)^{(2)} + h} \right) \right| +$$

$$+ \left| \sum_{j=0}^{2^{m-n}-1} \sum_{i=2^{n-1}}^{2^n-1} \left(p_{t \cdot 2^n \cdot j + i} - \hat{p}_{t \cdot j_{(2^n \cdot j + i)}^{(1)}} \cdot \sum_{h=0}^{2^L-1} p_{t \cdot 2^L \cdot (2^n + i)^{(2)} + h} \right) \right| \rightarrow \min_{(j_0, \dots, j_{2^L-1})}.$$

4. ЧИСЛОВЫЕ РЕЗУЛЬТАТЫ

Проверим гипотезы о совпадении теоретических распределений вероятностей p_{tk}^n , $n \in \{1, \dots, 8\}$, $k \in \{0, 1\}$, гауссовского случайного процесса с распределениями вероятностей значений n -ых битов $x_t \in \{0, 1, \dots, 255\}$, $t = 0, \dots, N$, $N = 100$. Результаты тестов приведены в следующей таблице.

Таблица

P-значения тестов

n(bit №)	1	2	3	4	5	6	7	8
p_n	0,7365	0,8799	0,7365	0,6464	0,7990	0,7992	0,7993	0,9998

$$p_n = 1 - F_{\chi_{\nu-1}^2}(\chi_n^2), \chi_n^2 = N \left[\frac{(\hat{p}_0^n - p_0^n)^2}{p_0^n} + \frac{(\hat{p}_1^n - p_1^n)^2}{p_1^n} \right], F_{\chi_\nu^2}(x) = \int_0^x \frac{x^{\nu/2-1} e^{-x/2}}{2^{\nu/2} \Gamma(\nu/2)} dx, \nu = 2$$

$\hat{p}_0^n, \hat{p}_1^n = 1 - \hat{p}_0^n$ – оценки распределения вероятностей n -го бита.

Литература

1. Аграновский А. В., Девянин П. Н., Хади Р. А., Черемушкин А. В. Основы компьютерной стеганографии. – М.: Радио и связь, 2003.
2. Барсуков В. С., Романцев А. П. Компьютерная стеганография // Специальная техника. 1998. № 4–5.

ТАНДЕМ МНОГОЛИНЕЙНЫХ СИСТЕМ МАССОВОГО ОБСЛУЖИВАНИЯ С УПРАВЛЯЕМЫМ ДОСТУПОМ

С. А. Дудин

1. ВВЕДЕНИЕ

Многолинейная система массового обслуживания (СМО) типа M|M|N|0 со времен А. К. Эрланга (начало 20-го века) являлась адекват-