МЕТОД ЭФФЕКТИВНОЙ КОРРЕКТИРОВКИ ИСКАЖЕНИЙ ГИСТОГРАММЫ КОНТЕЙНЕРА ПРИ СТЕГОКОДИРОВАНИИ

Е. О. Волкорез

Задача скрытой передачи данных посредством мультимедиа контейнера, часто сводится к встраиванию данных в бинарную последовательность. Например, в последовательность младших бит квантованных коэффициентов дискретного косинусного преобразования JPEG изображения. Проблема эффективного встраивания данных в последовательность впервые была рассмотрена в статье [1] и в дальнейшем была сведена к конструированию кодов [2,3].

Основное условие скрытой передачи данных – стойкость к обнаружению факта передачи данных. На данный момент, наиболее действенные методы обнаружения скрытых данных базируются на анализе гистограммы контейнера.

Существует несколько подходов, позволяющих скрыть искажения гистограммы. Один из них заключается в изменении гистограммы таким образом, что она «похожа» на гистограмму изображения без встроенных данных. Другой подход опирается на корректировку искажений гистограммы – использование одной части контейнера для встраивания данных, а другой части для компенсации возникших искажений гистограммы.

В статье предложен метод, основанный на применении свойств кодов Хэмминга, и обладающий двумя основными преимуществами:

- не требуется выделение части контейнера для корректировки искажений контейнера, что увеличивает пропускную способность;
- увеличивается эффективность корректировки искажений гистограммы, т.е. корректировка существенно меньше искажает контейнер.

Задача встраивания данных заключается в такой модификации контейнера – последовательности $x = \{x_i\}_{i=1}^{N} \in B^N$, что из модифицированной последовательности $\tilde{x} = \{x_i\}_{i=1}^{N} \in B^N$ может быть однозначно извлечена последовательность данных $y = \{y_i\}_{i=1}^{M} \in B^M$, где B – поле вычетов по модулю 2.

Рассмотрим два алгоритма встраивания в контейнер $x = \{x_i\}_{i=1}^{N}$: корректирующий искажения, и стандартный, не производящий коррекцию. Для корректирующего алгоритма будут использованы те же обозначения, что и для стандартного, но с правым верхним индексом *c*.

Определение. Эффективность корректировки:

$$c := \frac{|\tilde{x}^c - x| - |\tilde{x} - x|}{\Delta},$$

где Δ – модуль разницы частот единиц в последовательностях $\tilde{x}^c$ и $\tilde{x}$.

Пусть исходная последовательность разбита на блоки, а корректирующий глобальный алгоритм заключается в применении к каждому из блоков стандартного или корректирующего локального алгоритма. Если p_i^c – доля ошибок, корректируемых с эффективностью c_i, где $i = 1,...,r$, то эффективность глобального алгоритма выражается через эффективность локальных:

$$c = \sum_{i=1,...,r} c_i \, p_i^c .$$

В таком случае глобальный корректирующий алгоритм заключается в применении корректирующего алгоритма в первую очередь к блокам с наилучшим значением эффективности.

Рассмотрим алгоритм встраивания данных $d \in B^m$ в вектор $b \in B^n$, где $n = 2^m - 1, m \in Z^+$. Определим синдром вектора b по формуле:

$$s(b) = \sum_{i=1}^{n} B(i) b_i , \qquad (1)$$

где $B(i)$ – бинарное представление числа i. Встраивание данных – поиск такого вектора $\tilde{b}$, что $s(\tilde{b}) = d$. Стандартный алгоритм встраивания изменяет максимум один элемент b согласно формулам:

$$\tilde{b} = b - e_0^{\,s,d}, \qquad (2)$$

$$e_{0,i}^{s,d} = \delta_{i,Z^+(s-d)}, i = \overline{1,n}, \qquad (3)$$

где $Z^+(s-d)$ - представление бинарного вектора $s-d$ целым положительным числом, $\delta_{i,j}$ – символ Кронекера. Корректирующий алгоритм допускает изменение двух элементов вектора b, что позволяет выбрать лучший из нескольких вариантов его модификации:

$$\tilde{b} = b - e_{j_o}^{\,s,d}, \qquad (4)$$

$$e_{j,i}^{s,d} = \delta_{i,j} + \delta_{i,Z^+(s-d-B(j))}, \; j = \overline{0,n}, i = \overline{1,n} \qquad (5)$$

где $j_0 \in [0,n]$ – число определяющее лучший вариант модификации (4).

В силу равенства $j = Z^+(s-d-B(Z^+(s-d-B(j))))$ для всех $j = 0,...,n$ справедливо соотношение:

$$e_j^{s,d} = e_{Z^+(s-d-B(j))}^{s,d}. \qquad (6)$$

Поэтому, если $s \neq d$, то существует $\frac{n+1}{2} = 2^{m-1}$ различных вариантов изменения вектора b. Если $s = d$, то $e_j^{s,d} = 0$ для всех j. Из (6) также следует, что стандартный алгоритм является частным случаем корректирующего при $j = 0$ и $j = Z^+(s-d)$.

Утверждение 1. Алгоритм (4),(5) корректен, т.е. любого $j_0 \in [0,n]$ верно равенство:

$$s(\tilde{b}) = d.$$

Пусть цель корректирующего алгоритма – уменьшение числа единиц. Тогда параметр j_0 определяется следующим образом:

$$j_0 = \min\left\{ k \in [0,n] \;\middle|\; b_k + b_{z^+(s-d-B(k))} = \max_{j=0,...,n} (b_j + b_{Z^+(s-d-B(j))}) \right\}, \qquad (7)$$

где величина b_0 полагается равной 0, а операции сложения над компонентами вектора b выполняются как над целыми числами. Число исправляемых рассматриваемым блоком b искажений равно:

$$\Delta^b = (1-\delta_{s,d}) \max\left(0, 2(b_{j_0} + b_{Z^+(s-d-B(j_0))} - b_{Z^+(s-d)}) - 1\right).$$

Таким образом, Δ^b может принимать значения 0,1,3. Если $\Delta^b = 0$, то согласно (7), $j_0 = 0$ и корректирующий алгоритм сводится к стандартному. Если $\Delta^b > 0$ корректирующий алгоритм модифицирует два элемента вектора b с эффективностью корректировки $c^b = (\Delta^b)^{-1}$.

Пусть вектор (b,d) – случайная величина. Введем обозначения:

$$a_{i,j} = \{(b,d) \mid b_{Z^+(s-d)} = i, b_{j_0} + b_{Z^+(s-d-B(j_0))} = j\},$$

$$a_i = \{(b,d) \mid b_{Z^+(s-d)} = i\},$$

$$p(a_{i,j} \mid s \neq d) = p_{i,j},$$

где $i, j \in \{0,1,2\}$ и $i \leq j$. Очевидно, что $p(a_i \mid s \neq d) = p_i, i = 0,1$.

Утверждение 2. Если элементы векторов b и d независимы, одинаково распределены и $P(b_i = 1) = p_1$, $P(d_i) = 0.5$, то

$$p_{0,0} = p_0{}^n,\ p_{i,2} = p_i(1-(1-p_1^2)^{\frac{n-1}{2}}),$$

$$p_{1,1} = p_1(1-p_1^2)^{\frac{n-1}{2}},\ p_{0,1} = p_0(1-p_1^2)^{\frac{n-1}{2}} - p_0^n.$$

Утверждение 3. Пусть ξ - изменение доли нулей в результате встраивания данных в блок. В условиях утверждения 2 верны равенства:

$$E(\xi) = (2(1-P_2) + p_1P_2 - p_0^n)p_{s\neq d},$$

$$D(\xi) = 4p_0P_2(1-P_2) + p_0^n(1-p_0^n) + p_1P_2(1-p_1P_2) + p_0^n(2p_1P_2 + 4(1-P_2)),$$

где $P_2 = (1-p_1^2)^{(n-1)/2}$, $p_{s\neq d} = P(s \neq d)$.

Рассмотрим использование локального алгоритма встраивания (4), (5) в глобальном алгоритме. Обозначим через n_i и $n_{i,j}$ – число блоков (b,d), принадлежащих множествам a_i и $a_{i,j}$ соответственно.

Утверждение 4. Пусть глобальный алгоритм корректирует только уменьшение числа 0, причем модифицируется минимально возможное число элементов. Тогда число элементов контейнера, дополнительно модифицированных в результате корректировки, определяется формулой:

$$\begin{cases} 0 & ,если\ \ n_0 \le n_1, \\ (n_0 - n_1)/3 & ,если\ \ n_0 \in]n_1, n_1 + 3n_{02}], \\ n_0 - n_1 - 2n_{02} & ,если\ \ n_0 \in]n_1 + 3n_{02}, n_1 + 3n_{02} + n_{01} + n_{12}], \\ n_{01} + n_{02} + n_{12} & ,если\ \ n_0 > n_1 + 3n_{02} + n_{01} + n_{12}, \end{cases}$$

а уменьшение числа нулей в результате корректировки:

$$\begin{cases} 0 & ,если\ \ n_0 \le n_1 + 3n_{02} + n_{01} + n_{12}, \\ n_0 - n_1 - n_{01} - 3n_{02} - n_{12} & ,если\ \ n_0 > n_1 + 3n_{02} + n_{01} + n_{12}. \end{cases}$$

Утверждение 5. Пусть доля нулей в последовательность $x = \{x_i\}_{i=1}^N$ равна p_0, а вероятности появления всех конфигураций нулей и единиц равны. Элементы последовательности данных независимы и равномерно распределены. Если процесс встраивания происходит только согласно (4),(5),(7), для изменения доли η нулей всего контейнера верны равенства:

$$E(L^{-1}\eta) = \mu + 0(L^{-1}),\quad D(L^{-0.5}\eta) = \sigma + s + 0(L^{-1}),$$

где $s \in R$.

Следствие. Величина $L^{-1}\eta$ сходится по вероятности к μ при $L \to \infty$.

Литература

1. *Crandall R.*: Some notes on steganography, 1998.
2. *Bierbrauer J., Fridrich J.*: Constructing good covering codes for applications in steg-

anography. Transactions on Data Hiding and Multimedia Security III, LNCS 4920 pp. 1–22, Berlin, 2008.
3. *Zhang W., Li S.*: Steganographic codes a new problem in coding theory, 2002.

НЕПАРАМЕТРИЧЕСКАЯ МОДЕЛЬ ДИНАМИКИ ВРЕМЕННОЙ СТРУКТУРЫ И РЫНОЧНАЯ ЦЕНА РИСКА ПРОЦЕНТНОЙ СТАВКИ

Е. В. Гладкая

Современная теория цен активов позволяет определять стоимости широкого круга контрактов со случайными платежами в будущем, когда задана модель изменения ситуации на рынке. Разработано много моделей для описания рыночных показателей, включая цены акций и реальные доходности инвестиций. Чаще всего для определения стоимости опционов и других финансовых производных необходимо использовать непрерывно-временные модели динамики краткосрочных безрисковых процентных ставок r_t в реальном масштабе времени.

Однако, представляя способы определения цен актива, когда модель основной переменной задана, теория не формулирует правил, как выбирать ту модель, которая является наиболее подходящей для определения цены. Предложено много параметрических моделей динамики краткосрочных процентных ставок. Вместе с тем эмпирическое тестирование этих моделей привело к разноречивым результатам: одни тесты подтверждают адекватность модели, другие нет. Поэтому в последнее время стали популярными непараметрические методы, позволяющие конструировать модели, не навязывая ей структуру и значения параметров, создающих ограничения динамики моделируемой переменной.

В этой статье используется именно такая методика [1], которая не предполагает использования каких-либо предположений о функциях дрейфа μ или диффузии σ, когда обе эти функции оцениваются непараметрически по данным, наблюдаемым дискретно через определенные временные интервалы длительностью Δ. Процедура, которая может быть использована и в многомерной постановке, предполагает конструирование семейства приближений к функциям дрейфа и диффузии. Эти приближения поточечно сходятся к μ и σ со скоростью Δ^k, где k – произвольное положительное число. В статье рассматривается эффективность этих приближений для некоторых обычно используемых параметрических моделей процентной ставки и найдено, что для ежедневных данных даже простейшая модель дает приближение первого порядка, почти неотличимое от истинной функции, для широкого диапазона значений параметров. При уменьшении частоты получения выборочных значений