УДК 004.415.24

В. К. Задирака, д-р физ.-мат. наук, профессор,
И. В. Швидченко, канд. физ.-мат. наук

Институт кибернетики им. В.М. Глушкова НАН Украины, г. Киев

ВЛИЯНИЕ КАЧЕСТВА ОЦЕНКИ ПОГРЕШНОСТИ ОКРУГЛЕНИЯ СТЕГАНОАЛГОРИТМА НА ЕГО СТОЙКОСТЬ

Обсуждается использование резервов оптимизации стеганоалгоритма для повышения его стойкости.

Ключевые слова: *стеганография, спектральный стеганоалгоритм, стеганостойкость, оценка погрешности округления, дискретное преобразование Фурье.*

Введение. В теории погрешностей вычислений исследование таких вопросов как использование (в зависимости от задачи) разных видов погрешностей и оценка их качества являются актуальными и малоисследованными задачами. Их важность проявляется при исследовании вопроса о возможности решения задачи с заданными характеристиками качества при данной информации о задаче и при определении не завышенных вычислительных ресурсов. На сегодняшний день актуальным является использование теории погрешностей как инструмента для нахождения параметров программы, позволяющих найти приближенное решение задачи с заданными значениями характеристик качества и конструирования соответствующей компьютерной технологии.

Теория погрешностей вместе с общей теорией оптимальных алгоритмов применяется при решении вопроса о разрешимости задачи с заданными значениями характеристик качества при данной информации о задаче или при доказательстве того факта, что такое решение не существует.

Поднятые вопросы являются актуальными при решении задач вычислительной и прикладной математики [1]. В этой статье мы попытаемся применить их для повышения стойкости алгоритмов решения задач компьютерной стеганографии, как улучшения результатов работ [2–4].

Аналитический обзор. В данной статье будет произведена попытка улучшить стеганостойкость спектральных алгоритмов внедрения информации [2–6], которые используют оценки погрешности округления быстрых ортогональных преобразований, за счет использования более общих и точных оценок. Рассматривается случай приближенного задания матрицы ортогонального преобразования, разные правила округления. Наряду с детерминированными априорными асимптотическими оценками рассматриваются также вероятностные оценки погрешности. Необходимо отметить, что детерминиро-

ванные оценки погрешности (даже и неулучшаемые), как правило, являются завышенными для практически решаемых задач, в то время как вероятностные оценки больше ориентированы на задачи средней сложности и лучше описывают поведение реальных погрешностей. Эти два факта — приближенное задание матрицы преобразования и вероятностные оценки погрешности округления, будем надеяться, дадут нам те резервы оптимизации вычислений, которые позволят повысить стеганостойкость спектральных алгоритмов.

Стеганография начала активно исследоваться и развиваться с появлением компьютерных технологий. Это новое направление научных исследований находится на стыке криптографии, теории информации, теории вероятностей и математической статистики, цифровой обработки сигналов и изображений, теории дискретных ортогональных преобразований и других дисциплин.

В общем случае информация, передаваемая по стеганоканалу, может быть искажена операциями обработки контейнера — так называемыми неумышленными атаками. Кроме легальных пользователей (отправителя и получателя), при эксплуатации стеганосистемы возможно наличие третьего участника информационного взаимодействия — нарушителя, осуществляющего умышленные атаки.

Если нарушитель имеет возможность только наблюдать информацию, передаваемую по каналу связи, без возможности ее изменить, то говорят, что мы имеем дело с пассивной атакой на стеганосистему. Если нарушитель имеет возможность модифицировать стеганоконтейнер с целью уничтожения внедренного в него сообщения, то говорят, что мы имеем дело с активной атакой на стеганосистему. И, наконец, если цель нарушителя — достоверная оценка секретного ключа, и как следствие — возможность выполнять функции легального пользователя, в частности генерировать фальшивые стеганоконтейнеры, то в таком случае говорят о злоумышленной атаке на стеганосистему.

Среди стеганосистем выделяют системы скрытой передачи данных, цифровых водяных знаков (ЦВЗ), идентификационных номеров (отпечатков пальцев) и заголовков.

Большинство используемых контейнеров зашумлены. По определению считается, что если нам удалось внедрить информацию в шумы, то мы имеем дело со стойким стеганоалгоритмом при пассивных атаках. Спектральные алгоритмы стеганографии [2] позволяют делать внедрение сообщения в спектр шума и поэтому являются стойкими. Приведенный ниже стеганоалгоритм позволяет не только внедрять сообщение в шумовую компоненту сигнала, но и делать это таким образом, что при этом величина изменения спектра стеганоконтейнера будет соизмерима с погрешностью округления стеганоалгоритма.

Если погрешность обработки, вызванная наличием погрешности округления стеганоалгоритма, меньше шума сигнала, получаем двойную стеганографическую защиту секретного сообщения: оно будет внедряться в те фрагменты контейнера, значение элементов которых не превышает уровня шума, точнее, на уровне погрешности округления стеганоалгоритма.

Эта идея построения стеганоалгоритма является оригинальной и на ее основе построен класс теоретически стойких стеганографических алгоритмов (нарушитель не в состоянии определить факт использования стеганосистемы, так как не существует способа отличить пустой контейнер от заполненного) [7].

Одним из инструментов, широко используемых при разработке стеганосистем, является спектральный анализ сигналов и изображений, дискретное преобразование Фурье (ДПФ), дискретное косинусное преобразование (ДКП), дискретное вейвлет-преобразование (ДВП) и быстрые алгоритмы их реализации.

Для одномерного сигнала $f(n), n = \overline{0, N-1}$ ДПФ $F(r)$ имеет вид

$$F(r) = \sum_{n=0}^{N-1} f(n) W^{nr}, \quad W = e^{-i\frac{2\pi}{N}}, r = \overline{0, N-1}. \tag{1}$$

Для восстановления $f(n)$ используется обратное дискретное преобразование Фурье (ОДПФ):

$$f(n) = \frac{1}{N} \sum_{r=0}^{N-1} F(r) W^{-nr}, \quad n = \overline{0, N-1}. \tag{2}$$

$F(r)$ можно разделить на действительную и мнимую части:

$$\mathrm{Re}(F(r)) = \sum_{n=0}^{N-1} f(n) \cos\left(2\pi \frac{rn}{N}\right),$$

$$\mathrm{Im}(F(r)) = \sum_{n=0}^{N-1} f(n) \sin\left(2\pi \frac{rn}{N}\right).$$

$F(r)$ можно также представить в виде амплитудного и фазового спектров:

$$\begin{gathered} \left|F(r)\right| = \sqrt{\mathrm{Re}^2(F(r)) + \mathrm{Im}^2(F(r))}, \\ \arg\left[F(r)\right] = arctg \frac{\mathrm{Im}(F(r))}{\mathrm{Re}(F(r))}, r = \overline{0, N-1}. \end{gathered} \tag{3}$$

При работе с изображениями используется двумерное ДПФ. Пусть $f(k,m)$ — изображение размером $N \times M$. ДПФ данного изображения имеет вид

$$F(r,d)=\sum_{k=0}^{N-1}\sum_{m=0}^{M-1} f(k,m)\cdot e^{-2\pi i\left(\frac{rk}{N}+\frac{dm}{M}\right)},$$
$$r=\overline{0,N-1};d=\overline{0,M-1}. \tag{4}$$

Восстанавливается изображение с помощью ОДПФ

$$f(k,m)=\frac{1}{NM}\sum_{r=0}^{N-1}\sum_{d=0}^{M-1} F(r,d)\cdot e^{2\pi i\left(\frac{rk}{N}+\frac{dm}{M}\right)},$$
$$k=\overline{0,N-1};m=\overline{0,M-1}. \tag{5}$$

Базовой операцией стеганоалгоритма является ДПФ, используемое в одномерном случае трижды [7]: два раза отправителем и один раз получателем. Стеганоалгоритм изображен на рис. 1.

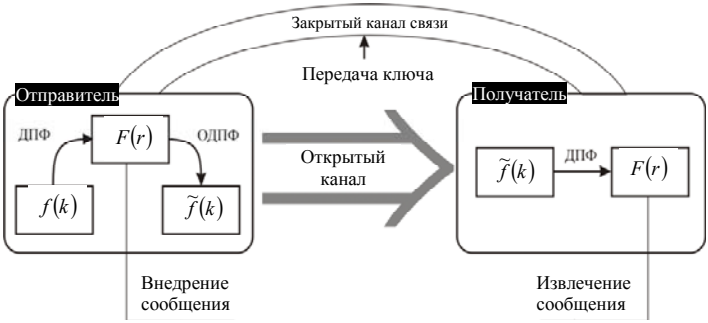

Рис. 1. *Общая структура спектральных алгоритмов на базе оценок погрешности округления*

Для уменьшения оценок сложности стеганоалгоритма и оценок погрешности округления для вычисления ДПФ будем использовать эффективную вычислительную процедуру быстрого преобразования Фурье (БПФ), которая вместо $O\left(N^2\right)$ комплексных операций сложения и умножения для стандартного метода, требует $O\left(N\log_2 N\right)$ таких операций. При этом отметим, что оценки снизу количества операций комплексного сложения $\left(Q^+\right)$ и умножения $\left(Q^*\right)$ вычисления ДПФ имеют вид [8]

$$Q^+ \geq \frac{N}{2}\log_2 N,$$
$$Q^* = O\left(N\right). \tag{6}$$

Коэффициент ускорения вычислений ДПФ $\left(K\right)$ стандартного алгоритма по отношению к БПФ имеет вид

$$K = \frac{N}{\log_2 N}. \tag{7}$$

Из (7) видно, что с ростом N K растет. Асимптотическую эффективность алгоритма БПФ можно сформулировать следующим образом: существует такое N_0, что для всех $N \geq N_0$ количество операций алгоритма БПФ составляет лишь 1% от количества операций стандартного метода.

Мы будем использовать ту модификацию алгоритма БПФ, которая минимизирует вычислительные затраты для вычисления тригонометрических функций и пересчета матрицы преобразования $\left[W^{rk}\right]$ $\left(W = e^{-i\frac{2\pi}{N}}\right)$, $r,k = \overline{0,N-1}$ [9]. Для этой модификации алгоритма БПФ (с предварительной заготовкой матрицы преобразования) A в работе [8] получены оценки его сложности по операциям умножения $Q_N^*(A)$ и «бабочек» $Q_N^0(A)$:

$$\begin{aligned} Q_N^*(A) &= \left[\frac{N\log_2 N}{2} - \frac{5}{3}N + 8\right], \\ Q_N^0(A) &= \left[\frac{N\log_2 N}{2} - \frac{13}{8}N + \frac{5}{8}\right]. \end{aligned} \tag{8}$$

Отметим, что в алгоритме A использовано его распараллеливание в зависимости от сложности «бабочки». Это дало возможность улучшить оценки сложности в сравнении с оценкой снизу для Q_N^+ (см. первую из оценок (6)).

Применение модификации алгоритма БПФ A особо эффективно при решении серии задач. Среди таких задач можно указать задачи двуключевой криптографии, компьютерной стеганографии, цифровой обработки сигналов и другие [5].

Как будет показано ниже, алгоритм БПФ не только существенно сокращает оценки сложности алгоритмов, вычисляющих ДПФ, но и соответствующие оценки погрешностей округления. В спектральном стеганоалгоритме оценки погрешности округления будут активно использоваться для выбора разрядов компонент спектра шума, в которые будет встраиваться передаваемое сообщение. Это является «изюминкой» стеганоалгоритма.

Пусть $fl(\cdot)$ обозначает результат вычисления выражения, стоящего в скобках в режиме с плавающей запятой. Имеют место сле-

дующие оценки эвклидовой нормы погрешности округления вычисления ДПФ F [10]:

- для стандартного алгоритма

$$\left\|\varepsilon^0\right\|_E < C\cdot(2N)^{\frac{3}{2}}; \tag{9}$$

- для БПФ при

$$N=\prod_{j=1}^{\gamma}N_j$$

$$\left\|\varepsilon^0\right\|_E < C\cdot\sum_{j=1}^{\gamma}\left(2N_j\right)^{\frac{3}{2}}; \tag{10}$$

- для БПФ при

$$N_1=N_2=\ldots=N_\gamma=2$$

$$\left\|\varepsilon^0\right\|_E < 8C\cdot\log_2 N, \tag{11}$$

где $\varepsilon^0 = fl(F)-F$, $C=1.06\cdot\|F\|_E\cdot 2^{-\tau}$, τ — количество двоичных разрядов у мантисс чисел при вычислении в режиме плавающей запятой.

В работе [3] подробно описан стеганоалгоритм, базирующийся на использовании оценок погрешности округления (10), (11) для одномерных и двумерных сигналов и результаты его тестирования для двух типов сигналов в одномерном случае и двумерного сигнала-контейнера. Кроме этого оценена пропускная способность созданного этой системой стеганоканала.

Резервы оптимизации стеганоалгоритма. Первый резерв оптимизации — это использование тех модификаций алгоритма БПФ (например, алгоритма A), которые максимально улучшают оценки сложности рассматриваемого стеганоалгоритма. Это и представление элементов матрицы преобразования в виде, не зависящем от N (от N зависит лишь число необходимых ранее заготовленных элементов матрицы $\frac{N}{2}$); это и сокращение информации о матрице в $2N$ раз; это и минимизация операций на поиск и выборку необходимого на данной итерации алгоритма элемента матрицы; это и распараллеливание алгоритма по сложности «бабочек» и другие.

Второй резерв состоит в использовании иных оценок погрешностей округления, которые учитывают:

- тот факт, что элементы матрицы преобразования, которые вычисляются, известны лишь приближенно;

- различные нормы вектора погрешностей округления;
- различные режимы вычислений (с плавающей или фиксированной запятой);
- различные способы округления (классический, отсечение и рандомизированный);
- кроме детерминированных также вероятностные оценки;
- многомерность цифрового контейнера.

Использование этого резерва оптимизации даст возможность приспособиться к реальной вычислительной ситуации и более точно определить номер разряда шумовой компоненты контейнера, в который будет произведено внедрение бита передаваемого сообщения, что позволит повысить стеганостойкость алгоритма.

Приведем некоторые из анонсированных оценок погрешностей округления.

В работе [11] приведены оценки для $\left\|\varepsilon^0\right\|_E$ и $\left\|\varepsilon^0\right\|_1$ в предположении, что элементы матрицы W вычислены приближенно:

$$fl(\sin(fl(\alpha))) = \sin(\alpha) + \delta \cdot \theta \cdot \varepsilon,$$

$$fl(\cos(fl(\alpha))) = \cos(\alpha) + \delta \cdot \theta \cdot \varepsilon,$$

где $\delta \geq 0$ — абсолютная константа, $-1 \leq \theta \leq 1$, $\varepsilon = 2^{-\tau}$; вычисления ведутся в режиме с плавающей запятой. Константа δ зависит от способа вычисления синусов и косинусов и их аргументов и не зависит от входных данных. Оценки при $N_1 = N_2 = ... = N_\gamma$ имеют вид

$$\left\|\varepsilon^0\right\|_E < \left[K(N,\delta)\cdot\varepsilon + O\left(\varepsilon^2\right)\right]\|F\|_E; \tag{12}$$

$$\left\|\varepsilon^0\right\|_1 < \left[\sqrt{N}\cdot K(N,\delta)\cdot\varepsilon + O\left(\varepsilon^2\right)\right]\frac{1}{\sqrt{N}}\|F\|_E, \tag{13}$$

где

$$K(N,\delta) = \sum_{i=1}^{\gamma}\alpha(N_i) + (\gamma - 1)(3 + 2\delta),$$

$$\alpha(N_i) = \begin{cases} \sqrt{2} & \text{при } N_i = 2; \\ 5 & \text{при } N_i = 4; \\ 2\sqrt{N_i(N_i + \delta)} & \text{в других случаях}. \end{cases}$$

Для алгоритмов БПФ с основаниями 2 и 4

$$K\left(2^\gamma, \delta\right) = \left(3 + \sqrt{2} + 2\delta\right)\gamma - (3 + 2\delta), \tag{14}$$

$$K\left(4^\gamma, \delta\right) = (8 + 2\delta)\gamma - (3 + 2\delta). \tag{15}$$

Рассмотрим теперь задачу оценки погрешности округления вычисления многомерного ДПФ:

$$F(r_1, r_2, ..., r_m) = \sum_{s_1} \sum_{s_2} ... \sum_{s_m} \exp\left(\frac{s_1 r_1}{N_1} + \frac{s_2 r_2}{N_2} + ... + \frac{s_m r_m}{N_m} \right) \times \tag{16}$$

$$\times f(s_1, s_2, ..., s_m), \quad s_i, r_i = \overline{0, N_i - 1}; \quad i = \overline{1, m}.$$

Пусть, по аналогии с одномерным случаем,

$$\varepsilon(r_1, r_2, ..., r_m) = fl\left(F(r_1, r_2, ..., r_m)\right) - F(r_1, r_2, ..., r_m);$$

$$\left\|\varepsilon\right\|_E = \left\{ \sum_{r_1} \sum_{r_2} ... \sum_{r_m} \left| \varepsilon\left(r_1, r_2, ..., r_m\right)^2 \right| \right\}^{\frac{1}{2}};$$

$$\left\|\varepsilon\right\|_1 = \max_{r_1, r_2, ..., r_m} \left| \varepsilon\left(r_1, r_2, ..., r_m\right) \right|.$$

Тогда

$$\left\|\varepsilon\right\|_E \le \left[\varepsilon \cdot \sum_{i=1}^{m} K\left(N_i, \delta\right) + O\left(\varepsilon^2\right) \right] \cdot \left\|F\right\|_E, \tag{17}$$

$$\left\|\varepsilon\right\|_1 \le \left[\varepsilon\left(N_1, N_2, ..., N_m\right)^{\frac{1}{2}} \sum_{i=1}^{m} K\left(N_i, \delta\right) + O\left(\varepsilon^2\right) \right] \frac{1}{\left(N_1, N_2, ..., N_m\right)^{\frac{1}{2}}} \left\|F\right\|_E. \tag{18}$$

В работах [12, 13] получены вероятностные оценки для отношения дисперсий погрешности округления и ДПФ для режимов вычислений с плавающей и фиксированной запятой и использовании рандомизированного правила округлений.

Для режима плавающей запятой и для случая, когда $f(n), n = \overline{0, N-1}$ — белый шум:

$$\frac{\sigma_{\varepsilon^0}^2}{\sigma_F^2} = 0,21 \cdot 2^{-2\tau} \cdot \gamma, \quad \left(N = 2^{\gamma}\right). \tag{19}$$

В случае, если используется правило округления — отсечение результатов, в правой части (19) будет не линейная зависимость от γ, а квадратичная.

Для режима фиксированной запятой в случае детерминированного сигнала

$$\left| f\left(n\right) \right| < \frac{1}{2}, n = \overline{0, N-1}$$

и рандомизированного правила округления имеет место следующая двусторонняя оценка

$$(\gamma - 2{,}5)c^2 \cdot 2^{-2\tau} \le \frac{\sigma^2_{\varepsilon^0}}{\sigma^2_F} \le 2^{\gamma+4} \cdot 2^{-2\tau} \cdot \frac{c^2}{\sqrt{K}},$$

где $K = \frac{1}{N}\sum_{n=0}^{N-1} |f(n)|^2$; $c = 0{,}3$ для округления; $c = 0{,}4$ для отсечения результатов операции.

Тестирование качества стеганоалгоритма с использованием резервов оптимизации. Самым тонким местом тестирования является выявление (на основе использования оценок погрешности округления стеганоалгоритма (17)–(19)) номера разряда пустого контейнера, в который нужно внедрять бит сообщения и определение качества стеганоалгоритма.

Предметом тестирования являются эффективные по быстродействию спектральные алгоритмы построения стеганоконтейнера на основе оценок погрешностей округления алгоритма БПФ с разными способами формирования ключа.

Цель тестирования — проверка качества оценок их основных характеристик: стеганостойкости, пропускной способности и быстродействия с целью выявления их зависимости от значений основных параметров алгоритмов и выявления областей их эффективного применения в задачах скрытой передачи информации.

Вычислительный эксперимент будет построен таким образом, чтобы продемонстрировать разные способы встраивания секретной информации в разного вида пустые цифровые контейнеры.

Опишем подробнее сам объект тестирования — спектральный стеганоалгоритм, который основывается на использовании оценок погрешности округления алгоритма БПФ.

Пусть наша задача — скрытая передача сообщения в некотором дискретном сигнале $f(k), k = \overline{0, N-1}$. При этом в качестве $f(k)$ возьмем сигнал вида:

$$f(k) = f_1(k) + n(k) = a_0 + \sum_{i=1}^{l} (a_i \cos \omega_i k + b_i \sin \omega_i k) + n(k), \quad (20)$$

где $n(k)$ — выборка шумовой компоненты сигнала $f(k), k = \overline{0, N-1}$ и известно, что в процессе передачи $f(k)$ подлежит спектральной обработке с использованием алгоритма БПФ.

В процессе вычисления на компьютере коэффициентов ДПФ сигнала возникают погрешности округления (см. соотношения (9)–(13), (17)–(19)), что приводит к несоответствию входного сигнала $f(k)$ с сигналом $f'(k)$, который получен из $f(k)$ после выполнения ДПФ и ОДПФ. Отсюда следует, что можно модифицировать разряды в отсчетах

сигнала таким образом, чтобы погрешность, которая возникает от встраивания сообщения, была соизмерима с погрешностью округления, которая возникает в процессе обработки сигнала (рис. 1). Выбор для встраивания последнего верного разряда позволит скрыть присутствие встроенной информации в стеганоконтейнере $\tilde{f}(k)$ ($\tilde{f}(k)$ получается из $f(k)$) после вычисления ДПФ, процедуры встраивания и ОДПФ).

Основной операцией спектрального стеганоалгоритма является ДПФ, оно используется трижды: два раза отправителем и один раз получателем.

Случайный сигнал (20) можно использовать в качестве пустого цифрового контейнера для передачи секретного сообщения.

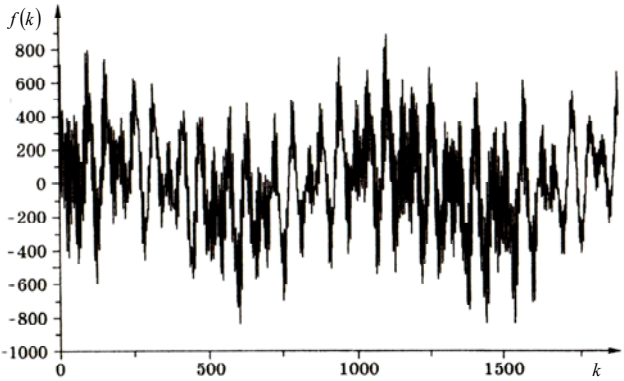

Рис. 2. *Пример случайного сигнала, который используется для передачи секретного сообщения*

Спектр зашумленного сигнала $f(k)$ состоит из главных и побочных лепестков.

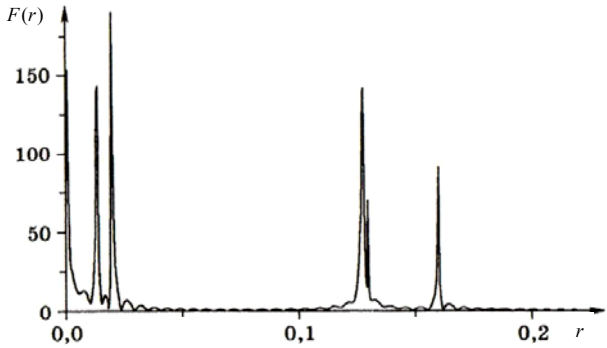

Рис. 3. *Амплитудный спектр сигнала*

Для встраивания сообщения используются побочные лепестки, которые соответствуют уровню шума и погрешности округления, так как встраивание в главные лепестки приводит к большой погрешности восстановления сигнала.

Необходимой процедурой является процедура формирования ключа. Для данного алгоритма это будет фиксация мест встраивания бит сообщения в спектр контейнера.

Обозначим секретное сообщение $y : y = (y_1, ..., y_p)$, а ключ $z : z = (z_1, ..., z_p)$.

Тогда для встраивания секретного сообщения в цифровой контейнер $f(k), k = \overline{0, N-1}$ можно использовать следующий алгоритм.

Используем алгоритм БПФ в качестве селективного преобразования [14] для селекции периодической компоненты с целью определения частот ω_j и приближенного значения амплитуд

$$a_0, a_j, b_j, r_j = \sqrt{a_j^2 + b_j^2}, j = \overline{1, l}.$$

Для минимизации погрешности восстановления сигнала $f(k)$ будем встраивать сообщение y в побочные лепестки спектра $F(r)$, амплитуды которых меньше, чем амплитуды выделенных пиков на заданное пороговое значение. Для этого воспользуемся соотношениями

$$\frac{r(w_j)}{r_{\max}} \le \xi, \tag{21}$$

$$\frac{a(w_j)}{a_{\max}} \le \xi, \tag{22}$$

$$\frac{b(w_j)}{b_{\max}} \le \xi, \ j = \overline{0, N-1}. \tag{23}$$

Внедрение бита y_i будем осуществлять в бит побочного лепестка на место, которое является предыдущим к первому верному биту $F(r)$ (относительно оценки апостериорной погрешности округления алгоритма БПФ).

Ключом является номер бита τ_k в который внедряются биты сообщения, а также p номеров j, для которых выполняется одно из соотношений (21–23). То есть общая длина ключа $k = p + 1$, а в случае, когда сообщение внедряется в действительную и мнимую части спектра $k = p + 2$.

Выводы. В работе показано, как применение более общих и точных оценок погрешности округления алгоритма БПФ может быть использовано для повышения стеганостойкости спектрального алгоритма.

Список использованной литературы:

1. Компьютерные технологии решения задач прикладной и вычислительной математики с заданными значениями характеристик качества / И. В. Сергиенко, В. К. Задирака, М. Д. Бабич и др. // Кибернетика и системный анализ. — 2006. — № 5. — С. 33–41.
2. Кошкина Н. В. Спектральные методы решения задач компьютерной стеганографии / Н. В. Кошкина, В. К. Задирака // Проблемы управления и информатики. — 2011. — № 4. — С. 132–151.
3. Оптимальні алгоритми обчислення інтегралів від швидкоосцилюючих функцій та їх застосування / І. В. Сергієнко, В. К. Задірака, О. М. Литвин та ін. — К. : Наукова думка, 2011. — Том 2. Застосування. — 348 с.
4. Current problems in information and computational technologies / M. Junisbekov at all. — Lublin : Politechnica Lubelska, 2012. — P. 61–98.
5. Задірака В. К. Комп'ютерна криптологія : підручник / В. К. Задірака, О. С. Олексюк. — К., 2002. — 504 с.
6. Стеганографічний алгоритм вкраплення інформації в зображення стійкий до стискання // Збірник наукових праць «Поступ в науку» міжнар. проблемно-наукової міжгалузевої конф. «Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління (ПНМК–2011)». — Бучач : Інститут менеджменту і аудиту. — № 7. — С. 166–170.
7. Задирака В. К. Спектральные алгоритмы компьютерной стеганографии / В. К. Задирака, С. С. Мельникова, Н. В. Бородавка // Искусственный интеллект. — 2002. — № 3. — С. 532–541.
8. Задирака В. К. Теория вычисления преобразования Фурье / В. К. Задирака. — К. : Наук. думка, 1983. – 216 с.
9. Задирака В. К. Об одной модификации алгоритма быстрого преобразования Фурье. В кн.: Вопросы оптимизации и организации вычислений / В. К. Задирака. — К. : О-во «Знание» УССР, 1973. — С. 13–19.
10. Gentleman W. M. Fast Fourier transform for fun and profit / W. M. Gentleman, G. Sande // A FIPS Proc. — 1966. — Vol. 29. — P. 563–578.
11. Ramos G. K. Roundoff error in multidimensional generalized discrete transform / G. K. Ramos // IEEE Circuits and Syst. — 1974. — Vol. 21. — P. 100–108.
12. Weinstein C. J. Roundoff noise in floating point fast Fourier transform computation / C. J. Weinstein // IEEE Trans. Audio and Electroacoust. — 1969. — Vol. 19. — № 2. — P. 209–215.
13. Welch P. O. A fixed point fast Fourier transform error analysis / P. O. Welch // IEEE Trans. Audio and Electroacoust. — Vol. 17. — № 2. — P. 151–157.
14. Серебренников М. Г. Выявление скрытых периодичностей / М. Г. Серебренников, А. А. Первозванский. — М. : Наука, 1965. — 224 с.

The use of steganography algorithm's optimization reserves for increasing of its security is discussed.

Key words: *steganography, spectral algorithm, steganographic security, round-off error estimation, discrete Fourier transformation.*

Отримано: 23.04.2015