УДК 004.056.5: 518

Кобозева А.А., Борисенко И.И.

СТЕГАНОГРАФИЧЕСКИЙ SS-МЕТОД, ИСПОЛЬЗУЮЩИЙ МОДУЛИРУЮЩИЙ СИГНАЛ СПЕЦИАЛЬНОГО ВИДА

В статье предлагается новый стеганографический SS-метод, работающий в пространственной области. В качестве модулирующего сигнала используется собственный вектор автокорреляционной матрицы контейнера, отвечающий наименьшему собственному значению, позволяющий обеспечить максимальное значение отношения «сигнал-шум». Приводятся результаты вычислительного эксперимента.

1. Введение

Среди методов защиты информации, разработка и совершенствование которых является чрезвычайно актуальной задачей на современном этапе развития общества в целом и научных исследований в частности, важное место занимают методы компьютерной стеганографии [1,2], при использовании которых секретное сообщение, или дополнительная информация (ДИ), погружается в некоторый объект, или основное сообщение (ОС), не привлекающий внимания, который затем открыто пересылается адресату по каналу связи или хранится в таком виде. Процесс погружения ДИ в ОС, или контейнер, будем называть *стегопреобразованием* ОС, а результат погружения – *стегосообщением*.

Одним из основных требований, выдвигаемых к любому стеганографическому методу, является требование его стойкости к различным возмущающим воздействиям. Для обеспечения высокой помехоустойчивости и затруднения процесса перехвата в технике связи используются методы расширения спектра [1], суть которых заключается в расширении полосы частот сигнала более, чем это необходимо для передачи реальной информации, посредством кода, который не зависит от передаваемых данных. Применение широкополосных методов в стеганографии (SS-методов (Spread-Spectrum)) значительно затрудняет обнаружение ДИ и ее удаление: секретное сообщение «растворяется» во всем объеме контейнера, в силу чего при потере сигнала в некоторых полосах частот, в других присутствует достаточно информации для ее восстановления. Таким образом, SS-методы являются достаточно устойчивыми к случайным и преднамеренным искажениям [1].

Целью настоящей работы является создание нового стеганографического SS-метода на основании классической непрерывной модели связи [3], использующего для погружения модулирующий сигнал специального вида и осуществляющего погружение ДИ в пространственной области. Применяемый кодовый сигнал должен обеспечить высокую помехоустойчивость метода, являясь оптимальным в смысле максимизации отношения «сигнал-шум» (ОСШ), где ДИ и ОС рассматриваются как сигнал и составная часть шума соответственно.

2. Предпосылки

Рассмотрим классическую непрерывную модель связи [3]. Сигнал $Abs(t)$, где $b \in \{-1,1\}$, $A > 0$, $s(t)$ - функция, определяющая форму сигнала, передается в течение промежутка времени $[0,T]$. Получаемый на приемном пункте сигнал имеет вид:

$$r(t) = Abs(t) + z(t), \quad (1)$$

где $z(t)$ - независимая случайная помеха. Задача – восстановить b.

Будем считать, что рассматриваемая помеха имеет нулевое среднее, и $z(t)$ можно разложить в ряд на отрезке $[0,T]$ по некоторой ортонормальной системе функций $\Phi_i(t),\ i=1,2,...$ [4] (например, многочленам Лежандра, Чебышева с весовыми коэффициентами и др. [5]):

$$z(t)=\sum_{i=1}^{\infty} a_i\Phi_i(t)=\lim_{N\to\infty}\sum_{i=1}^{N} a_i\Phi_i(t)\,, \tag{2}$$

где $$a_i=\int_0^T z(t)\Phi_i(t)dt\,, \tag{3}$$

т.е. являются проекциями $z(t)$ на соответствующие функции $\Phi_i(t),\ i=1,2,...$ Множество ортонормированных функций $\{\Phi_i(t)\}_{i=1}^{\infty}$ должно удовлетворять условию некоррелированности этих проекций $z(t)$ [3,4]:

$$M[<\Phi_i(t),z(t)><\Phi_j(t),z(t)>]=M[\int_0^T\int_0^T\Phi_i(\tau)z(\tau)\Phi_j(t)z(t)dtd\tau]=\lambda_j\delta_{ij} \tag{4}$$

где $M[\bullet]$ - математическое ожидание, $<\bullet,\bullet>$- скалярное произведение аргументов, δ_{ij} - символ Кронекера. Обозначая $R_z(t,\tau)=M[z(t)z(\tau)]$, переходя от двойного интеграла к повторному [6], получим интегральное уравнение, эквивалентное (4):

$$\int_0^T\Phi_j(t)(\int_0^T R_z(t,\tau)\Phi_i(\tau)d\tau)dt=\lambda_j\delta_{ij}\,,$$

решение которого, очевидно, удовлетворяет условию:

$$\int_0^T R_z(t,\tau)\Phi_i(\tau)d\tau=\lambda_i\Phi_i(t)\,. \tag{5}$$

Поскольку решение интегрального уравнения (5) связано с трудностями, переходят к эквивалентному дискретному представлению этого уравнения [3] и пользуются далее для его решения методами вычислительной линейной алгебры [7].

Предположим, что функции множества $\{\Phi_i(t)\}_{i=1}^{\infty}$ и $z(t)$ могут быть хорошо приближены линейными комбинациями некоторого конечного множества ортонормальных базисных функций

$$\{\psi_n(t)\},\quad n=1,...,N \tag{6}$$

на $[0,T]$, т.е. $\Phi_i(t),\ i=1,2,...$ удовлетворяют сотношениям $\max_{t\in[0,T]}\left|\Phi_i(t)-\sum_{n=1}^{N}\phi_{in}\psi_n(t)\right|\approx 0,\ i=1,2,\ldots,$ где $\phi_{in},\ n=1,2,...,N$, - коэффициенты

соответствующих линейных комбинаций. Тогда $\Phi_i(t),\ i=1,2,...$ могут быть представлены в виде

$$\Phi_i(t)=\sum_{n=1}^{N}\phi_{in}\psi_n(t), \tag{7}$$

Подставляя (7) в (5), получим:

$$\lambda_i\sum_{n=1}^{N}\phi_{in}\psi_n(t)=\int_0^T R_z(t,\tau)\sum_{n=1}^{N}\phi_{in}\psi_n(\tau)d\tau\ . \tag{8}$$

Умножая равенство (8) на $\psi_k(t)$ и интегрируя результат на $[0,T]$, учитывая ортонормированность системы функций (6), получим:

$$\lambda_i\phi_{ik}=\sum_{n=1}^{N}\phi_{in}\int_0^T\int_0^T R_z(t,\tau)\psi_k(t)\psi_n(\tau)dtd\tau=\sum_{n=1}^{N}r_{kn}\phi_{in}\ , \tag{9}$$

где $r_{kn}=\int_0^T\int_0^T R_z(t,\tau)\psi_k(t)\psi_n(\tau)dtd\tau$. Если обозначить проекции сигнала $z(t)$ на функции множества $\{\psi_i(t)\}_{i=1}^N$ как $Z_j=\int_0^T z(t)\psi_j(t)dt,\ j=\overline{1,N}$, то

$$r_{kn}=M[\int_0^T\int_0^T z(t)z(\tau)\psi_k(t)\psi_n(\tau)dtd\tau]=M[Z_kZ_n]\,.$$

Тогда (9), полученное из интегрального уравнения (5), превращается в стандартную задачу о собственных значениях (СЗ):

$$M[ZZ^T]\phi_i=R\phi_i=\lambda_i\phi_i \tag{10}$$

где $\phi_i=(\phi_{i1},...,\phi_{in})^T$, $Z=(Z_1,...,Z_N)^T$ [3,4].

По полученному сигналу $r(t)=Abs(t)+z(t)$ строится вектор $\bar{r}=Ab\bar{s}+\bar{z}$, где $i-$ые компоненты векторов $\bar{r},\bar{s},\bar{z}$, $i=\overline{1,N}$, представляют собой проекции соответствующих сигналов $r(t),s(t),z(t)$ на собственные функции помехи $\Phi_i(t)$, $i=\overline{1,N}$. Если предположить, что $z(t)$ имеет распределение Гаусса, то декодирование b заключается в следующем [4]:

$$b=sign\left(\sum_{i=1}^{N}\frac{\bar{s}_i\bar{r}_i}{\lambda_i}\right). \tag{11}$$

Такой метод декодирования называется обеляющей фильтрацией [3]. Как известно, среди всех линейных фильтров вектор $\bar{c}$ с компонентами $\bar{c}_i=\bar{s}_i/\lambda_i,\ i=\overline{1,N}$, максимизирует ОСШ (SNR), определяемое как

$$SNR = \frac{M\left[\left(b\sum_{i=1}^{N}\frac{\bar{s}_i^{2}}{\lambda_i}\right)^2\right]}{M\left[\left(\sum_{i=1}^{N}\frac{\bar{s}_i\bar{z}_i}{\lambda_i}\right)^2\right]} = \sum_{i=1}^{N}\frac{\bar{s}_i^{2}}{\lambda_i} \qquad (12)$$

Значение SNR, как следует из (12), определяется компонентами вектора $\bar{s}$ и будет максимальным в случае, когда в качестве $s(t)$ используется $\Phi_N(t)$ [3], (т.е. вектор $\bar{s}$ отвечает собственному вектору (СВ) матрицы R, соответствующему минимальному СЗ) .

3. Новый стеганографический метод, основанный на расширении спектра секретного сообщения

Пусть секретное сообщение, подлежащее погружению в ОС, – бинарная последовательность, элементы которой принадлежат множеству $\{-1,1\}$. Для пересылки одного бита b ДИ в качестве контейнера используется сигнал $x(t)$, трактуемый как гауссовский шум. Рассмотрим аддитивный метод погружения ДИ, основанный на расширении спектра секретного сообщения, в виде [8]:

$$y(t) = Abs(t) + x(t) + \bar{\bar{n}},$$

где $A > 0$ - параметр погружения, $s(t)$ - расширяющий (или кодовый) сигнал, который не зависит от передаваемой информации, $\bar{\bar{n}}$ - аддитивный белый гауссовский шум (заметим, что аддитивный белый гауссовский шум является подходящей моделью для ошибок квантования, возмущающих воздействий при пересылке в канале связи и (или) атак на стегосообщение [8]). Здесь в качестве полезного сигнала выступает $Abs(t)$. Введение $\bar{\bar{n}}$ учитывает возможность возмущающих воздействий при пересылке стегосообщения по каналу связи.

Рассмотрим подробнее возможность конкретного выбора множества функций $\{\psi_i(t)\}_{i=1}^{N}$ (6).

Пусть $0 = t_1 < t_2 < ... < t_{N+1} = T$ - разбиение сегмента $[0,T]$ на частичные сегменты равной длины Δt. Для $\Phi_i(t)$, которые по предположению удовлетворяют соотношениям (2), (4), построим интерполяционные сплайны $L_0^{(i)}(t)$ нулевой степени [9], полагая точки $(t_k, \Phi_i(t_k)), \quad k = \overline{1,N}$, узлами интерполяции. Поскольку $\{\Phi_i(t)\}_{i=1}^{\infty}$ является ортонормальной системой функций, для которой выполняется (2), то $\Phi_i(t)$ предполагаются интегрируемыми на $[0,T]$. Тогда можно утверждать [9], что выбрав достаточное количество узлов, ошибку интерполяции можно сделать сколь угодно малой, т.е.

$$\Phi_i(t) \approx L_0^{(i)}(t), t \in [0,T]. \quad (13)$$

С каждым частичным сегментом $[t_i, t_{i+1}], i = \overline{1,N}$ свяжем базисную функцию $\psi_i(t)$, определенную на $[0,T]$ следующим образом:

$$\psi_i(t) = \begin{cases} 1, & если \quad t \in [t_i, t_{i+1}], \\ 0, & если \quad t \notin [t_i, t_{i+1}] \end{cases}, \quad i = \overline{1,N}. \quad (14)$$

Заметим, что все функции множества $\{\psi_i(t)\}_{i=1}^N$ попарно ортогональны. Фактически, каждая из функций $\psi_i(t)$ является масштабирующей функцией, используемой при кратномасштабном анализе на основе вейвлетов Хаара [10]. Кроме того, система функций $\{\psi_i(t)\}_{i=1}^N$ является ортонормированной с весовым коэффициентом $1/\Delta t$. Тогда, учитывая (13), и определяя функции конечного базиса по формулам (14), формула (7) принимает вид:

$$\Phi_i(t) = \sum_{n=1}^{N} \Phi_i(t_n)\psi_n(t), \quad (15)$$

При подстановке (15) в уравнение (5), умножения полученного равенства на $\psi_k(t)/\Delta t$ и интегрирования результата на сегменте $[0,T]$, получим:

$$\lambda_i \Phi_i(t_k) = \frac{1}{\Delta t}\sum_{n=1}^{N} \Phi_i(t_n) \int_0^T \int_0^T R_z(t,\tau)\psi_k(t)\psi_n(\tau)dtd\tau = \sum_{n=1}^{N} \frac{1}{\Delta t} r_{kn}\Phi_i(t_n).$$

Рассмотрим проекции сигнала $z(t)$ на функции (14) множества $\{\psi_i(t)\}_{i=1}^N$, воспользовавшись для вычисления интеграла формулой левых прямоугольников [11]:

$$Z_j = \int_0^T z(t)\psi_j(t)dt = \int_{t_j}^{t_{j+1}} z(t)dt \approx z(t_j)\Delta t, \; j = \overline{1,N}, \quad (16)$$

причем, если $z(t)$ интегрируема на рассматриваемом сегменте $[0,T]$, погрешность полученного приближения за счет увеличения количества частичных сегментов можно сделать сколь угодно малой [6].

Пусть сигнал $z(t)$ подвергается равномерной дискретизации и квантованию, результатом чего становится вектор $\overline{Z} = (\overline{Z}_1, ..., \overline{Z}_N)^T$, где $\overline{Z}_i, i = \overline{1,N}$, это значение $z(t_i)$ после квантования в точках $0 = t_1 < ... < t_N = T$, Δt - длина каждого частичного сегмента. Не ограничивая общности, будем считать, что $\Delta t = 1$. Матрицу R в формуле (10), учитывая (16), представим в виде:

$$R = M[\overline{Z}\overline{Z}^T]. \quad (17)$$

Тогда собственным функциям $\Phi_i(t)$ уравнения (5) будут отвечать собственные вектора $\phi_i = (\Phi_i(t_1),..., \Phi_i(t_N))^T$ матрицы R, координаты которых являются ординатами узлов интерполяции $\Phi_i(t)$. Конечно, таким образом мы сможем восстановить лишь первые N функций множества $\{\Phi_i(t)\}_{i=1}^{\infty}$, однако, из необходимого условия сходимости ряда (2) [6] будет вытекать, что $\lim\limits_{i\to\infty} a_i = 0$ (a_i определяются в соответствии с (3)), а значит вклад $\Phi_i(t)$ в сигнал $z(t)$ при достаточно больших i становится бесконечно малым.

Проектируя полученный на приемном пункте сигнал (1) на функции $\{\Phi_i(t)\}_{i=1}^{N}$, получим вектор $\overline{Y} = Ab\overline{S} + \overline{Z}$. Взяв в качестве кодового сигнала $s(t) = \Phi_N(t)$ для максимизации ОСШ, получим, что вектор $\overline{S} = (0,0,...,0,1)^T$, а формула (11) для декодирования, учитывая неотрицательность собственных значений матрицы R, примет вид:

$$b = sign\left(\sum_{i=1}^{N} \frac{\overline{s}_i \overline{y}_i}{\lambda_i}\right) = sign\frac{\overline{y}_N}{\lambda_N} = sign\langle \overline{Y}, \phi_N \rangle . \qquad (18)$$

Пусть в качестве ОС используется изображение в градациях серого, матрицу которого обозначим F. Стандартным образом изображение разбивается на блоки $F_1,..., F_K$ малой размерности n [12] (например, $n = 8$), каждый из которых используется для переноса одного бита ДИ, представляющей из себя бинарную последовательность $b_1,...,b_K$, $b_i \in \{-1,1\}$, $i = \overline{1,K}$. Перед встраиванием ДИ каждый блок F_i разворачивается в вектор $\overline{Z}_i$ длины n^2, используемый для построения матрицы R размерности $n^2 \times n^2$ в соответствии с (17), приобретающей вид:

$$R = M[\overline{Z}\overline{Z}^T] = \frac{1}{K}\sum_{i=1}^{K} \overline{Z}_i \overline{Z}_i^T .$$

Заметим, что матрица R является симметричной:

$$R^T = \frac{1}{K}\left(\sum_{i=1}^{K} \overline{Z}_i \overline{Z}_i^T\right)^T = R$$

и положительно полуопределенной:

$$x^T R x = \frac{1}{K} x^T \left(\sum_{i=1}^{K} \overline{Z}_i \overline{Z}_i^T\right) x = \frac{1}{K}\sum_{i=1}^{K} x^T \overline{Z}_i \overline{Z}_i^T x = \frac{1}{K}\sum_{i=1}^{K} (\overline{Z}_i^T x)^T (\overline{Z}_i^T x) \geq 0$$

для $\forall x$, где x - вектор размерности n^2, а значит все СЗ матрицы R являются неотрицательными [7].

Погружение бита b_i ДИ произведем в пространственной области каждого блока в соответствии с формулой:

$$\overline{Y}_i = Ab_i\overline{S} + \overline{Z}_i + \overline{\overline{n}}_i, \quad i = \overline{1,K}, \tag{19}$$

при этом $\left\|\overline{S}\right\| = 1$, $\overline{\overline{n}}_i$ - аддитивный гауссовский шум, отвечающий i-му блоку ОС. Для максимизации ОСШ и, как следствие, повышения помехоустойчивости метода, в соответствии с выводами, сделанными выше, в качестве кодового сигнала для каждого блока ОС рассмотрим СВ, отвечающий наименьшему собственному значению R.

Итогом погружения ДИ в соответствии с (19), является присутствие энергии секретного сигнала во всех частотных диапазонах стегосообщения, что делает секретный сигнал с расширенным спектром стойким к внесению помех, а информацию, погруженную в ОС, стойкой к возмущающим воздействиям. Различные атаки на систему связи могут устранить энергию секретного сигнала из некоторых участков спектра, но в других полосах остается достаточное количество данных для восстановления информации.

Декодирование ДИ из стегосообщения, подвергшегося возможным возмущающим воздействиям, осуществляется в соответствии с формулой (18), применяемой для каждого блока, на которые стегосообщение разбивается предварительно перед осуществлением декодирования. Блоки разбиения отвечают соответствующим блокам контейнера при погружении ДИ.

4. Результаты вычислительного эксперимента

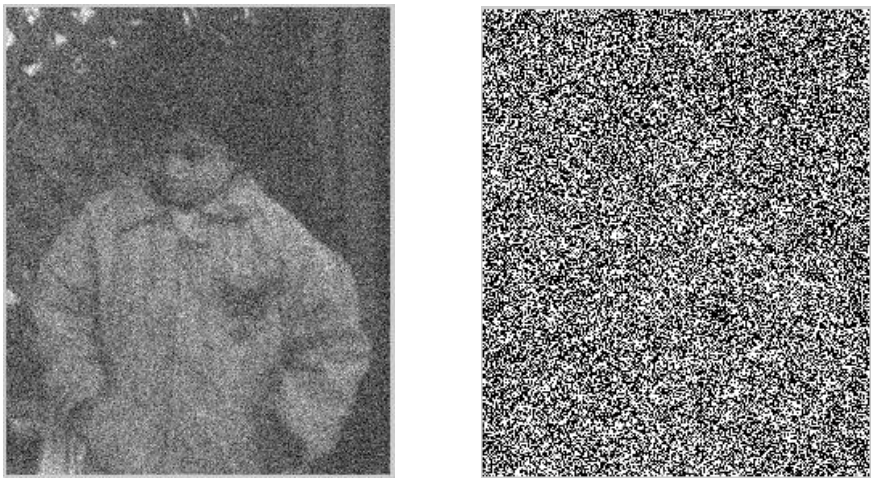
Целью вычислительного эксперимента, проводимого в среде MATLAB, была практическая реализация нового стеганографического метода, названного OPTIMA, для оценки его реальной помехоустойчивости, а также сравнение основных характеристик алгоритма с SS-алгоритмом, предложенным в [8] (ниже этот алгоритм будем называть GPM). Алгоритм GPM был выбран неслучайно: здесь также используется оптимальный с точки зрения максимизации ОСШ кодовый сигнал, но погружение и декодирование ДИ производится GPM в частотной области.

Рис.1. – Изображение POUT

Стеганогафические методы, использующие для сокрытия данных не пространственную, а частотную область, традиционно считаются более стойкими к разнообразным возмущениям [1,2,13]. На взгляд авторов настоящей статьи, такое утверждение не совсем оправдано. Подтверждением этому служат результаты вычислительного эксперимента, приведенные ниже, для демонстрации которых используется изображение POUT.TIF (рис.1).

В ходе эксперимента случайным образом было сформировано бинарное секретное сообщение, длина которого равна количеству блоков размерности 8×8, на которые предварительно было разбито изображение-контейнер. Погружение одной и той же ДИ производилось при разных значениях параметра A (1) стеганографическими алгоритмами OPTIMA и GPM. После погружения ДИ в ОС, на стегосообщения накладывался аддитивный гауссовский шум с нулевым математическим ожиданием и различными значениями дисперсии σ_n^2 (для

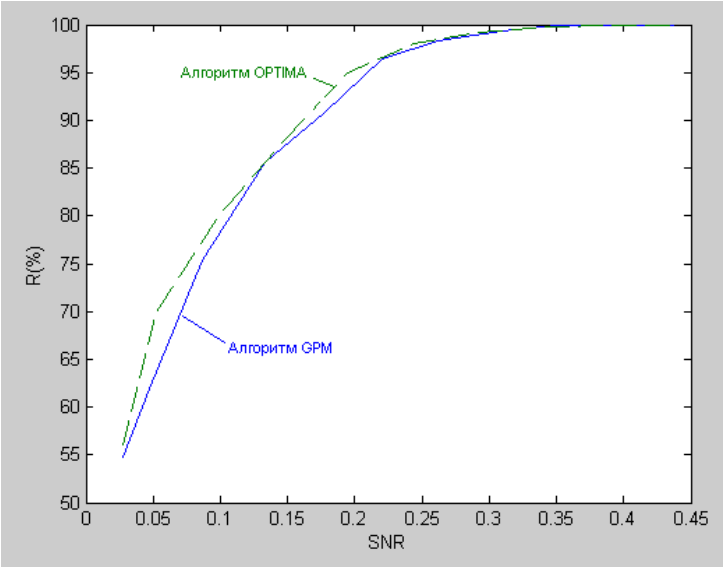
иллюстрации величины шума на рис.2 представлены результаты таких наложений на ОС) при помощи программы IMNOISE. Заметим, что параметры шума намеренно



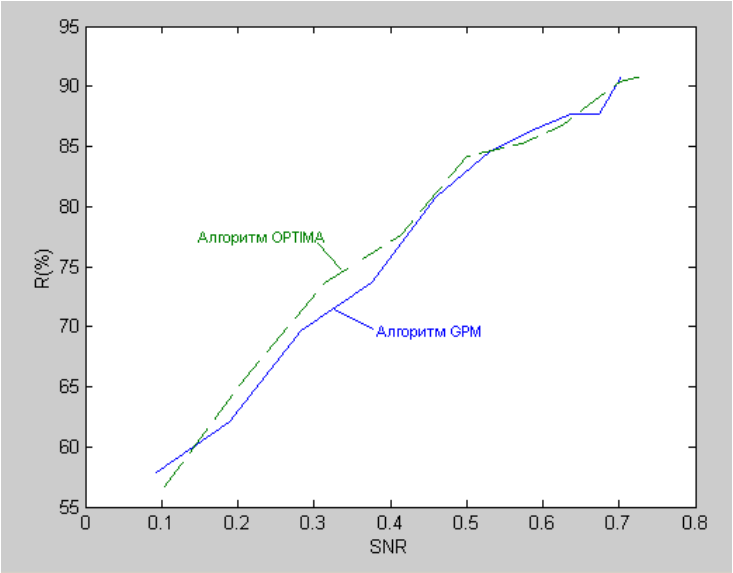
а б

Рис.2. – Контейнер POUT.TIF, возмущенный аддитивным гауссовским шумом с дисперсией: а – 0.01; б - 3

выбирались так, чтобы обеспечить значительное возмущение стегосообщения. Декодирование ДИ производилось из возмущенных стегосообщений в соответствии с формулой (18). Результаты эксперимента отражены в виде графиков зависимости объема восстановленной ДИ, выраженного в процентах, от величины SNR (12), представленных на рис.3. Для одного и того же значения SNR величины параметра A в OPTIMA и GPM будут отличаться друг от друга, но результаты декодирования ДИ, а значит и помехоустойчивость методов, как видно из графиков, – практически одинаковы, хотя области работы алгоритмов различные. За счет выбора параметра



а



б

Рис.3. – Графики зависимости объема восстановленной ДИ от значения SNR при различных дисперсиях шума, накладываемого на стегосообщения: а - $\sigma_n^2 = 0.01$; б - $\sigma_n^2 = 3$

A при использовании предложенного в работе алгоритма OPTIMA, в пространственной области погружения могут быть достигнуты результаты, аналогичные результатам, получаемым алгоритмом GPM в частотной области. Однако, переход в частотную область требует дополнительных вычислительных затрат (в частности, для GPM - построения коэффициентов ДКП) по сравнению с работой непосредственно с коэффициентами матрицы контейнера. Это позволяет утверждать, что алгоритм OPTIMA, обеспечивая как и GPM максимальное значение ОСШ, и обладая аналогичной помехоустойчивостью, имеет бесспорное преимущество в вычислительном смысле.

5. Заключение

В работе на базе классической непрерывной модели связи разработан теоретически и реализован практически новый помехоустойчивый стеганографический SS-алгоритм OPTIMA, использующий в качестве кодового сигнала оптимальный с точки зрения максимизации ОСШ линейный фильтр, являющийся собственным вектором автокорелляционной матрицы контейнера, отвечающий ее наименьшему собственному значению. Предложенный метод, осуществляя погружение и декодирование ДИ в пространственной области, обладает значительным преимуществом в вычислительном смысле перед SS-алгоритмом GPM, также использующим оптимальный с точки зрения максимизации ОСШ кодовый сигнал, но работающим в частотной области. Накладные затраты в OPTIMA отвечают решению задачи о нахождении спектра и собственных векторов матрицы размерности 64×64, и не зависят от размерности матрицы контейнера, являясь постоянной величиной.

Список литературы

1. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. – К.: Юниор, 2003. - 501 с.

2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – К.: МК – Пресс, 2006.- 288 с.
3. C. Rose, S. Ulukus, and R. D. Yates. Wireless Systems and Interference Avoidance,- IEEE Trans. Wireless Commun., vol.1, no. 7, pp. 415-428, Jul. 2002.
4. H. L. Van Trees. Detection, Estimation and Modulation Theory. Part I. New York: Wiley, 2001.
5. И.С. Гоноровский. Радиотехнические цепи и сигналы. - М.: «Радио и связь», 1986. - 513 с.
6. Г.М. Фихтенгольц Курс дифференциального и интегрального исчисления. – М. Наука, 1969.
7. Деммель Дж. Вычислительная линейная алгебра. – М.: Мир, 2001. - 430 с.
8. M. Gkizeli, D. A. Pados, M. J. Medley. Optimal Signature Design for Spread-Spectrum Steganography.- IEEE Trans. On Image Processing, vol.16, no.2, Feb. 2007.
9. Каханер Д., Моулер К., Нэш С. Численные методы и программное обеспечение. – М.: Мир, 2001. – 575 с.
10. Уэлстид С. Фракталы и вейвлеты для сжатия изображений в действии. – М.: «Триумф», 2003.-320 с.
11. Бахвалов Н.С., Жидков Н.П., Кобельков Г.М. Численные методы.- М.: БИНОМ. Лаборатория знаний, 2006 г.-636 с.
12. Гонсалес Р., Вудс Р. Цифровая обработка изображений.- М.: Техносфера, 2005.- 1072 с.
13. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография.-М.: Солон-Пресс, 2002.-272с.

Вісник Східноукраїнського національного університету ім. Володимира Даля, №5(111), 2007,ч.1, с.24-32.