УДК 004.056:061.68

Н.А. Деев

СТЕГАНОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ЭНЕРГЕТИЧЕСКОЙ И СТРУКТУРНОЙ СКРЫТНОСТИ

Рассматриваются методы защиты информации, основанные на сокрытии самого факта передачи данных, а также средства реализации этих методов в виде системы передачи двоичных сообщений с фазовой манипуляцией сигнала и псевдослучайной перестройкой рабочей частоты. Для передачи данных предлагается использовать фазовую манипуляцию, что обеспечивает затруднение процесса перехвата за счет расширения полосы частот передаваемого сигнала, и повышение помехоустойчивости приема на 3 дБ по сравнению с частотной манипуляцией. Коммутация компенсаторов контейнерных составляющих в каналах приема осуществляется в соответствии с синхронизированной псевдослучайной последовательностью, и за счет этого обеспечиваются обнаружение и эффективная оценка параметров узкополосных сигналов контейнерной составляющей с последующей компенсацией.

Введение

Надежная защита информации от несанкционированного доступа является актуальной, но не решенной в полном объеме проблемой. Одними из перспективных направлений защиты информации являются современные методы скремблирования и стеганографии. Слово *стеганография* в переводе с греческого буквально означает *тайнопись* (steganos – тайна, секрет; graphy – запись). Стеганография объединяет совокупность методов, основанных на различных принципах, которые обеспечивают сокрытие самого факта существования полезной информации в той или иной среде, а также средств реализации этих методов. Наряду с микрофотоснимками, невидимыми чернилами, условным расположением знаков к ней можно отнести средства связи с плавающими частотами, энергетической и структурной скрытностью [1].

В основе многих подходов к решению задач стеганографии лежит общая с криптографией методическая база, заложенная К.Э. Шенноном в теории тайнописи. Однако до сих пор теоретические основы стеганографии остаются практически не разработанными. Наблюдаемый в настоящее время интерес к стеганографии как совокупности методов сокрытия информации возник в большей мере благодаря интенсивному внедрению и широкому распространению средств вычислительной техники во все сферы деятельности человека. В рамках вычислительных сетей возникли достаточно широкие возможности по оперативному обмену различной информацией в виде текстов, программ, звука, изображений между любыми участниками сетевых сеансов независимо от их территориального размещения. Это позволяет активно использовать все преимущества, которые дают стеганографические методы защиты.

Стеганографические методы находят все большее применение в оборонной и коммерческой сферах деятельности в силу их легкой адаптируемости при решении задач защиты информации, а также отсутствия явно выраженных признаков средств защиты (например, криптографических), использование которых может быть ограничено или запрещено. Суть методов энергетической и структурной скрытности заключается в незначительной одновременной модификации целого ряда определенных битов контейнера при сокрытии одного бита информации. Существует несколько разновидностей метода. В наиболее распространенном варианте исходный сигнал модулируется высокочастотной псевдослучайной последовательностью $W(t)$, которая определена на области значений $\{-1,1\}$. Вследствие этого для передачи результата необходима большая (иногда более чем в 100 раз) полоса пропускания. Обычно последовательности $W(t)$ выбирают ортогональными к сигналу контейнера. Результирующий стегосигнал представляет собой суммарный сигнал контейнерной составляющей $V(t)$ и скрываемых данных $D(t)$:

$$S(t) = V(t) + \alpha \cdot D(t) \cdot W(t),$$

где α – коэффициент затухания, предназначенный для выбора оптимального уровня шума, который вносится данными.

Для извлечения скрытых данных $D(t)$ на принимающей стороне необходимо иметь ту же самую псевдослучайную импульсную последовательность $W(t)$, обеспечив ее синхронизацию со стегосигналом:

$$S(t)W(t) = V(t)W(t) + \alpha D(t).$$

В связи с этим данную псевдослучайную битовую последовательность обычно используют в качестве стегоключа.

В статье рассматривается система передачи с фазовой информационной манипуляцией сигнала и межбитовой псевдослучайной перестройкой рабочей частоты (ППРЧ). Контейнерной составляющей $V(t)$ в данном случае служат узкополосные ЧМ-сигналы, а скрываемые данные $D(t)$ передаются на фоне сигнала распределенными по диапазону и модулированными межсимвольной ППРЧ.

При точном воспроизведении псевдослучайной импульсной последовательности $W(t)$ в наибольшей степени удается осуществить подавление контейнерной составляющей $V(t)$. В случае, когда действует сумма сигналов контейнерной составляющей $V(t)$ и скрываемых данных $D(t)$ с различными спектрами, необходимо выделять из смеси каждую из них, оценивать, а затем вычитать из действующей смеси. Линейные фильтры для выделения сигналов контейнерной составляющей $V(t)$ и скрываемых данных $D(t)$ являются неэффективными для построения компенсаторов, поскольку при подавлении контейнерной составляющей $V(t)$ подавляется и часть спектральных составляющих широкополосного сигнала скрываемых данных $D(t)$. Поэтому целесообразно использовать нелинейные методы выделения и оценивания (фильтрации) параметров сигнала контейнерной составляющей $V(t)$, основанные на сочетании безынерционного нелинейного преобразования с линейной фильтрацией [2].

1. Структурные схемы формирования и обработки сигнала с межсимвольной ППРЧ

Схема формирования сигнала (рис.1, *а*) включает синтезатор частот (СЧ), вырабатывающего колебания с частотами $\omega_1, \ldots, \omega_м$; фазовые манипуляторы ($Ф_1 \ldots Ф_м$) (перемножители), обеспечивающие манипуляцию колебаний на 180° двоичными информационными символами, которые поступают от источника информации (ИИ). Генератор псевдослучайной последовательности чисел (ГПСП) через коммутатор (ком) осуществляет коммутацию колебаний (псевдослучайную перестройку рабочей частоты (ППРЧ)). На выходе формирователя образуется М-частотный сигнал $S(t, x, \vec{\beta})$, который можно представить в виде

$$S(t, x, \vec{\beta}) = \alpha_{\circ} \sum_{j=1}^{M} g_j \, rect\left[\left(t - jT_{П}\right) / T_{П}\right] \cdot X\left(t\right) \cos\left[\omega_j t + \beta_j\right] + V(t), \qquad (1)$$

где $rect = \left[\dfrac{t}{T_{П}}\right]$ – функция включения, $rect$ =1, если $t \in [0, T]$, или $rect$ =0, если $t \notin [0, T]$;

$T_{П}$ – длительность интервала с одной из частот ω_j;

M – количество частот ω_j, $j = \overline{1, M}$;

$V(t) = \sum_{j=1}^{M} y_j(t)$ – контейнерная составляющая, которая представляет собой сумму y_j узкополосных ЧМ-сигналов y_j, $j = \overline{1, M}$, действующих в узкополосных каналах;

g_j – значение псевдослучайной последовательности;

$X\left(t\right)$ – двоичная информационная последовательность;

β_j – начальная фаза колебания с частотой ω_j.

При таком формировании на каждой из M частот образуется фазоманипулированное колебание, амплитуда которого в зависимости от значения элемента g_j равна α_i или 0.

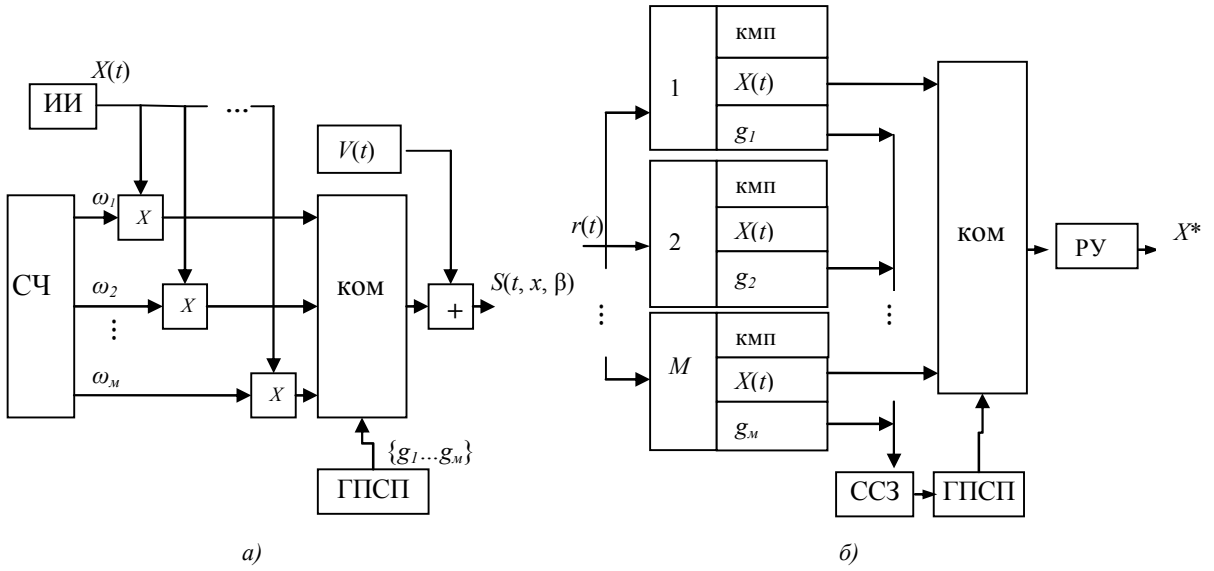


Рис. 1. Структурные схемы:
а) формирователя; *б)* устройства обработки сигнала с ППРЧ

При совпадении значения g_j с номером j-го частотного канала в течение интервала $T_п$ передается сигнал с фазовой информационной манипуляцией. Если период псевдослучайной последовательности чисел равен $MT_п$, то после активного интервала $T_п$ в j-м частотном канале образуется пауза длительностью $(M–1)T_п$. Количество информационных посылок в течение интервала $T_п$ определяется числом $K = T_п/T$, где T – длительность информационного символа.

На рис. 1, *б* показана обобщенная структурная схема устройства обработки сигналов с $ФМ_н$ и межбитовой ППРЧ, где $r(t)$ – сумма сигнала $S(t, x, \beta)$ и контейнерной составляющей $V(t)$. В каждом из M частотных каналов компенсатор (кмп) осуществляет оценку и компенсацию контейнерной составляющей. Схема синхронизации по задержке (ССЗ) управляет ГПСП, который обеспечивает синхронную с ППРЧ коммутацию информационных выходов частотных каналов. Решающее устройство (РУ) формирует оценку X^* информационных символов.

2. Алгоритмы компенсации контейнерной составляющей сигналов с ППРЧ

Оценка контейнерной составляющей (типа узкополосных ЧМ-сигналов $y_j(t)$) может быть существенно повышена за счет введения в каждый из каналов устройства обработки (УО) адаптивного компенсатора контейнерной составляющей (АКК). Процесс обнаружения контейнерной составляющей и оценки ее параметров осуществляется во время паузы в частотном канале. При этом сигнал не оказывает влияния на ошибки оценивания контейнерной составляющей, что обеспечивает существенное увеличение отношения информационного сигнала и контейнерной составляющей на выходе АКК, превышающее 0 дБ [3] (рис. 2).

Коммутация АКК в каналах приема осуществляется в соответствии с синхронизированной ПСП. Оценка амплитуды α^*_{ni} контейнерной составляющей производится в течение времени, пока полезный сигнал скрываемых данных $D(t)$ в i-м подканале отсутствует. Характеристика АКК i-го подканала определяется соотношением

$$Z_i(y_i) = k \cdot \frac{d\ell nW_y(y_i)}{dy_i}, \qquad (2)$$

где $W_y(y_i)$ – плотность распределения вероятности (ПРВ) мгновенных значений контейнерной составляющей ℓny_i.

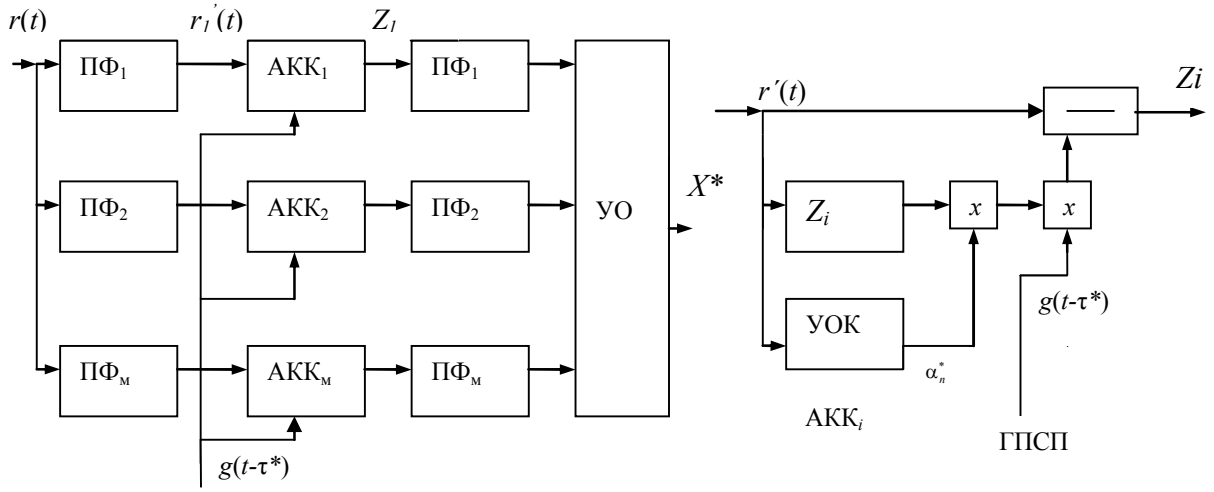


Рис. 2. Схема включения: *а)* устройство обработки АКК;
б) структура АКК$_i$ компенсации контейнерной составляющей *i*-го подканала

Во время включения *i*-го подканала $g_i = 1$ на вход вычитателя АКК поступает оценка контейнерной составляющей с амплитудой a^*_{ni}, сформированной на предыдущем интервале T_g. Полосовые фильтры (ПФ) на входе АКК обеспечивают селекцию контейнерной составляющей и исключают одновременное действие более одного ЧМ-сигнала в частотном канале. Выходные ПФ необходимы для подавления нечетных гармонических составляющих, образующихся в результате нелинейного преобразования контейнерной составляющей *sign*(*y*). Оценка амплитуды a^*_n контейнерной составляющей производится в устройстве оценки контейнерной составляющей (УОК). Компенсация контейнерной составляющей осуществляется сигналом $g(t - \tau^*)$ во время подключения частотного канала переключающим устройством (ПУ) от ГПСП приемника.

Если контейнерная составляющая представляет модулированное колебание (например, узкополосное частотно-модулированное), то ПРВ его мгновенных значений имеет бимодальный характер, что может быть учтено при построении нелинейного преобразователя. Оцененные узкополосные контейнерные составляющие компенсируются в вычитающем устройстве [4].

Рассмотрим пример построения компенсатора, задавшись конкретными статистическими характеристиками преобразуемых процессов. Примем ПРВ суммы контейнерных составляющих y_i и гауссовского шума n_{oi} в виде бимодальной функции, обусловленной действием контейнерного узкополосного ЧМ-сигнала с амплитудой a_i и шумовой составляющей с дисперсией σ_i^2:

$$W_y(y_{oi}) = C \exp\left[-\frac{1}{2\sigma_i^2}(y_{oi} - a_i sign(y_{oi})^2) \right], \tag{3}$$

где C – постоянная нормировки; σ_i^2 – дисперсия шумовой составляющей подканала.

В соответствии с выражениями (2) и (3) получим

$$Z_i(y_i) = k \cdot (y_i - a_i^* sign(y_i)). \tag{4}$$

Принимая независимыми сечения случайного процесса $\{r_{ij}\}, j=\overline{1,k}$, взятые с дискретом $\Delta t = T/k$, вычисляем логарифм отношения правдоподобия. На интервале *Тм* определяем максимально правдоподобную оценку контейнерной составляющей α_i^*:

$$\alpha_i^* = \frac{1}{T}\int_0^T |r_i(t)|dt . \tag{5}$$

Согласно (4) и (5) находим характеристику нелинейного преобразования $Z_{oi}(r)$ в *i*-м канале оценки контейнерной составляющей:

$$Z_{oi}(r_i) = \frac{1}{T}\int_0^T |r_i(t)|dt \cdot sign(r_i(t)) . \tag{6}$$

Характеристика $Z_{oi}(.)$ обеспечивает инвариантность преобразования к частоте контейнерной составляющей. Вместе с тем при клиппировании смеси $r_i(t)$ в спектре появляются составляющие на частотах $\varpi_i(2n-1), n \geq 2,3,\ldots$. Эти составляющие спектра на частотах вне полосы ПФ$_i$ подавляются (рис. 3), обеспечивая снижение ошибки оценивания контейнерной составляющей $y_i^*(t)$.

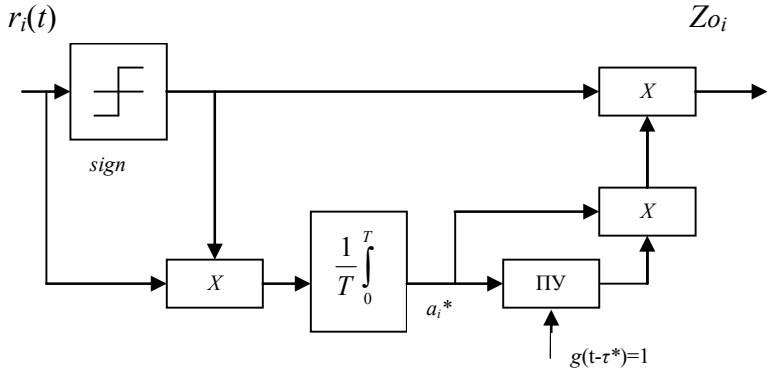


Рис. 3. Структурная схема нелинейного оценивателя
контейнерной составляющей *i*-го частотного подканала

Показателем качества компенсации может служить коэффициент подавления контейнерной составляющей μ^2 на выходе компенсатора (см. рис. 2, *б*):

$$\mu_i^2 = \frac{1+\alpha_i^2/\sigma_i^2}{1+\sigma_a^2/\sigma_i^2} , \tag{7}$$

где σ_i^2 – средняя мощность шумовой составляющей на выходе ПФ$_i$; σ_a^2 – дисперсия ошибки оценивания моды α_i, определяемая соотношением

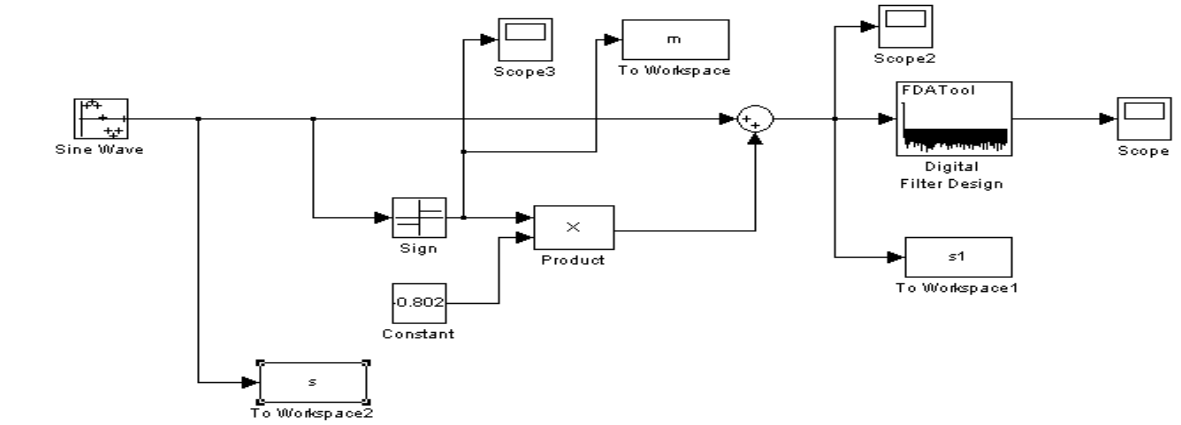
$$\sigma_a^2 \leq \sigma_i^2 2\tau_k / T . \tag{8}$$

Здесь τ_k – величина, зависящая от нормированной корреляционной функции $\rho(t_1 - t_2)$ процесса $y_i(t)$ и времени интегрирования T:

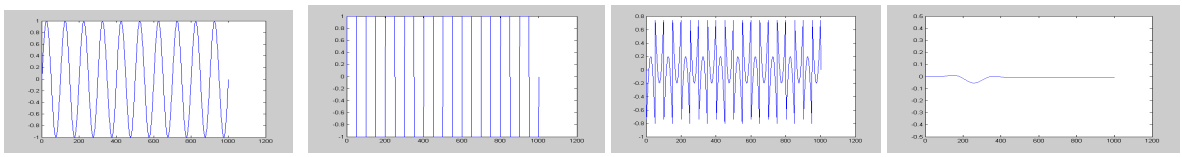
$$\tau_k = \int_0^T dt_1 \int_0^T \rho(t_1 - t_2)dt_2 \ . \qquad (9)$$

При относительно большом времени интегрирования $T >> \tau_k$ дисперсия σ_a^2 оценки моды может быть снижена до требуемой величины.

Разработанная система была смоделирована в среде MATLAB Simulink (рис. 4).



а)



б) *в)* *г)* *д)*

Рис. 4. Результаты компьютерного моделирования: *а)* структурная схема нелинейного оценивателя контейнерной составляющей частотного подканала; *б)* входной сигнал $U_{a0}(t)$; *в)* знаковая функция от сигнала $U_{sgn}(f)$; *г)* сигнал на выходе сумматора $U_{\Sigma}(t)$; *д)* сигнал на выходе фильтра $U_{a00}(t)$

Заключение

Для снижения ошибок воспроизведения контейнерной составляющей в полосе фильтрации могут быть использованы методы оценивания средней частоты ω_i контейнерной составляющей и адаптивная подстройка узкополосных фильтров, согласованных по полосе с шириной спектра контейнерной составляющей. Однако в этом случае требуется корректировать фазочастотную характеристику общего линейного компенсатора, что на практике может вызвать большие трудности. Компенсация узкополосных контейнерных составляющих в рассматриваемой системе позволяет снизить вероятность поражения спектральных составляющих широкополосного сигнала скрываемых данных $D(t)$. Предельная вероятность ошибки P_a на символ при использовании квадратурной обработки с накоплением оценки начальной фазы β_i, $i = 1, ..., M$ в каждом частотном канале определяется выражением

$$P_e = 1 - \Phi\left(\sqrt{q_o k}\right), \qquad (10)$$

где $\Phi(x) = \frac{1}{\sqrt{2\pi}} \cdot \int_{-\infty}^{x} \exp(\frac{-t^2}{2})dt$ – интеграл вероятности; q_0 – отношение сигнал/шум в канале, $k < 1$ – коэффициент, учитывающий потери за счет ошибок оценивания α_i^* и задержки τ^* псевдослучайной последовательности.

Список литературы

1. Чекатков, А.А. Методы и средства защиты информации / А.А. Чекатков, В.А. Хорошко. – М. : Юниор, 2003. – 594 с.

2. Варакин, Л.Е. Системы связи с шумоподобными сигналами / Л.Е. Варакин. – М. : Радио и связь, 1985. – 384 с.

3. Чердынцев, В.А. Подавление комплекса помех в каналах связи / В.А. Чердынцев, Н.А. Деев // Известия Белорусской инженерной академии. – 2002. – № 2. – С. 31–36.

4. Тихонов, В.И. Оптимальный прием сигналов / В.И. Тихонов. – М. : Радио и связь, 1983. – 512 с.

Поступила 17.04.08

Объединенный институт проблем
информатики НАН Беларуси,
Минск, Сурганова,6
e-mail: dna@newman.bas-net.by

M.A. Dzeyeu

STEGANOGRAPHICAL METHODS OF INFORMATION SECURITY ON THE BASIS OF ENERGY AND STRUCTURAL SECRECY

A system for binary message transfer with phase signal manipulation and pseudo-casual reorganization of working frequency is considered. It is suggested to use phase manipulation for data transfer that provides increase of a noise stability of reception on 3dB in comparison with frequency manipulation. In synchronism mode the receiver switches frequency channels to detect and effective rate to the parameters of intensive narrow-band interference with their subsequent indemnification. The compensating method based on allocation from the receiver working on an entrance of fluctuation of the most intensive interference and their subsequent indemnification is suggested.