НАУКОВО-ТЕХНІЧНИЙ ЖУРНАЛ „ЗАХИСТ ІНФОРМАЦІЇ" №2, 2005

УДК 681.5.015: 004.056.57 Маракова И.И., Мараков О.А.

ИСПОЛЬЗОВАНИЕ ПЕРЦЕПЦИОННОЙ МОДЕЛИ ПРИ ПОСТРОЕНИИ УСТРОЙСТВА ФОРМИРОВАНИЯ СТЕГОСИГНА СИСТЕМЫ С ЦИФРОВЫМИ ВОДЯНЫМИ ЗНАКАМИ

Задача разработчика системы с цифровыми водяными знаками (ЦВЗ) заключается в построении в общем случае при нескольких информационных битах ЦВЗ таких устройства формирования стегосигнала (УФС), кодера, детектора, декодера ЦВЗ, которые при заданном значении ложного детектирования ЦВЗ P_{fa} минимизировали бы значение вероятности пропуска ЦВЗ P_m и неправильного декодирования P_e при выполнении требования надежного восприятия стегосигнала или незаметности изменения основного покрывающего сообщения (ОПС). Условие допустимих скажений ОПП при формировании стегасообщения с учетом выполнений требований надежного восприятия $\|S-C\| = \sqrt{E(\sum_{\bar{n}\in A_N} w^2(n))} \le \rho$, $c(\bar{n}) \in C$, $w(\bar{n}) \in W$, где ρ —некоторая метрика искажений ОПП C после формирования стегосигнала S. Реализовать данное требование возможно на основе использования психофизических особенностей органов восприятия человека при погружении ЦВЗ, т.е. с учетом ПМ. Однако необходимо формализовать положения ПМ с учетом особенностей рассматриваемого приложения идентификации и верификации цифровых сообщений на основе технологий ЦВЗ.

Целью настоящий работы является разработка метода построения УФС системы с ЦВЗ с учетом ПМ, обеспечивающего минимальное различие при сравнении экспертом стегообраза и оригинала. Системы с ЦВЗ, которые автоматически контролируют незаметность ЦВЗ, несомненно, можно выделить в подгруппу систем с адаптивным управлением надежности восприятия стегосигнала.

Адаптация систем с цифровыми водяными знаками с учетом перцепционной модели

Прежде всего, необходимо отметить, что незаметность ЦВЗ нельзя рассматривать как бинарное событие. ЦВЗ могут иметь высокую или низкую заметность: малое или большое значение вероятности того, что они настолько будут искажать ОПС, что изменения станут заметны зрительно или на слух. При этом довольно заманчивым представляется автоматизировать оценку заметности ЦВЗ, т.е. свойство, определяемое органами восприятия человека, сделать обнаруживаемым автоматически без непосредственного участия человека. Основой алгоритмов автоматического контроля незаметности является использование особенностей визуальной и аудиовосприимчивости человека.

Надежность восприятия стегообраза определяется степенью различия с исходным ОПС. Однако как для видео-, так и для аудиосигналов существует понятие качества. При всей сложности определения данного понятия можно сказать, что оно является мерой притягательности. Стегообразам систем с ЦВЗ присущи оба свойства: и надежность восприятия и качество. Для большинства практических приложений систем с ЦВЗ надежность восприятия является более важным свойством.

Основными признаками аудиовосприимчивости являются частота и громкость, а видеовосприимчивости — пространственная частота (проявление тех или иных форм и фигур в изображении, чем меньше фигуры, тем больше частота), яркость и цвет. В общем случае ПМ основывается на учете эффектов маскировки и слияния, обусловленных особенностями визуальной и аудиовосприимчивости человека. Данные свойства находятся в прямой зависимости от органов слуха и зрения человека. С учетом различных признаков визуальной и аудиовосприимчивости человека необходимо отдельно определить особенности учета ПМ при ОПС в виде аудиосигналов и изображений. Отбор положений ПМ при построении УФС требует решения компромисса между ожидаемым эффектом (незаметности ЦВЗ) и сложностью практической реализации УФС и системы в целом.

1.1. Основные покрывающие сообщения в виде аудиосигналов

Реакция восприимчивости человека к аудиосигналам находятся в определенной зависимости от частоты [1]. Тестирование показало, что чувствительность человека к изменению громкости повышается на СЧ, а на ВЧ и НЧ чувствительность к переходам уменьшается (рис. 1). Для учета зависимости порога слышимости от частоты при построении систем с ЦВЗ и ОПС в виде аудиосигналов необходимо оценивать и учитывать параметр порога слышимости звука

$$DP = 20\log\frac{P}{P_o}, \qquad (1)$$

где P — давление источника звука в паскалях, $P_o = 20$ пск — учитывает звуковой фон.

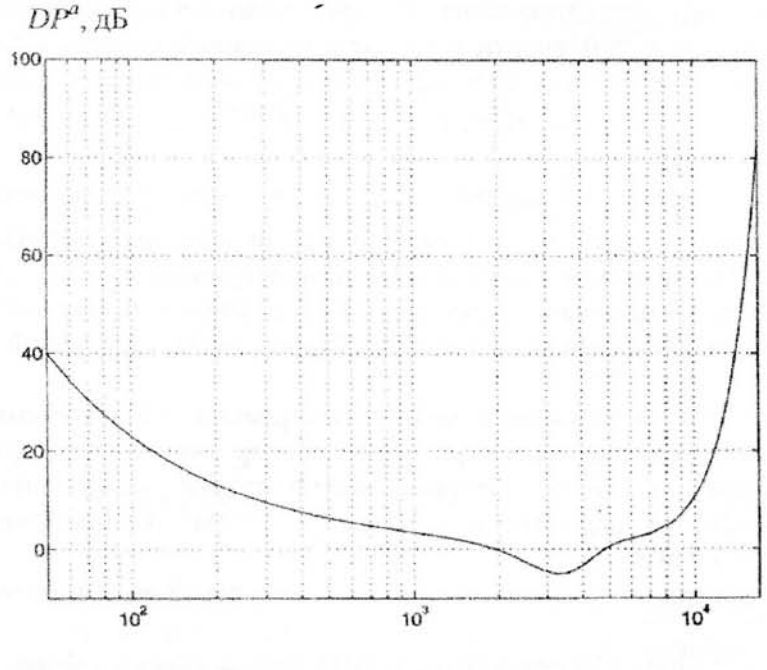

Рис. 1. Зависимость абсолютного порога слышимости DP^a в дБ от частоты звука f, Гц

Полученный эмпири- чески график иллюстрирует наивысшую чувствительность на 3 кГц, которая ухудшается к очень низким (20 Гц) и особенно очень высоким частотам (20 кГц) (рис. 2.7). Таким образом, учитывая, что вносимые при погружении ЦВЗ измене ния ОПС будут менее заметны на высоких уровнях громкости и в зависимости от частотного диапазона, представляется возможным осуществлять частотную маскировку по громкости, что является первой компонентой комплексного учета ПМ для обеспечения незаметности ЦВЗ (более громкие фрагменты ОПС предпочтительнее для погружения ЦВЗ, т.к. изменения будут менее заметны).

После анализа абсолютного уровня слышимости необходимо выполнить анализ относительного уровня слышимости, т.е. с учетом эффектов маскировки. Для того чтобы получить порог относительной слышимости прежде всего необходимо представить сигнал в виде окон или фреймов в соответствии со спектральной моделью слуховой системы человека [2]. Эмпирически получено, что в некотором приближении «канал» слухового восприятия можно моделировать линейкой фильтров с перекрывающимися частотными характеристиками разными полосами пропускания [1, 2].. Если рассмотреть узкополосный источник шума на минимально слышимом уровне громкости и его полосу увеличивать, то при достижении некоторого значения увеличиваемой полосы пропускания первоначального уровня громкости будет не достаточно для слышимости. Таким образом, после

разделения ОПС на M фреймов C_m, m=1,… M, перехода в частотную область, например, на основе ДПФ полученные частотные коэффициенты анализируются с точки зрения наличия частотных критических полос, т.е. выявляются частотные полосы, определяются энергетические параметры и характер каждой полосы (шум или тон). Порог относительной слышимости для каждого окна/фрейма является функцией энергии и зависит от характера фрейма (шум или тон). Порог слышимости зависит не только от уровня энергии в текущей частотной полосе, но и от уровня энергии в соседних полосах. Итак, при определении порога относительного уровня слышимости для каждой частотной составляющей ОПС необходимо: определить энергию для каждой критической полосы; определить «мнимую» энергию в каждой критической полосе, обусловленную влиянием соседних полос; определить характер полосы (шум или тон); определить порог маскировки.

Энергия в каждой критической полосе:

$$\Psi(r) = \sum_{f_{\min}}^{f_{\max}} |c(f)|, \qquad (2)$$

где $f_{\min}$, $f_{\max}$ — минимальная и максимальная частоты критической полосы r;

r — номер критической полосы;

$|c(f)|$ — амплитуды гармоник спектра в рассматриваемой критической полосе для исследуемого аудиосигнала.

Распределение энергии по критическим полосам моделируется основной мембранной функцией распространения

$$RF(r) = 15{,}81 + 7{,}5(r + 0{,}474) - 17{,}5\sqrt{1 + (r + 0{,}474)^2} \ . \qquad (3)$$

Полная энергия в некоторой критической полосе

$$\Psi_{\Sigma}(r) = \sum_{r'=r-r_0}^{r+r_1} \Psi(r - r')RF(r') \ , \qquad (4)$$

где r_o, r_1 — номера соседних критических полос, для которых (2.25) превышает заданный порог.

С другой стороны, если две тоновые составляющие звучат одновременно, то одна может стать не различимой, если их частоты находятся в одной критической полосе и $DP_1 < DP_2$. Кроме того, если частотная составляющая попадает в полосу, удаленную от центральной частоты полосы более, чем на 20 %, то ее амплитуда резко уменьшается [1]. Вместо использования таблицы допускается аналитическая оценка критической полосы $\Delta_{кр}(f) = 25 + 75\left[1 + 1.4\left(10^{-3} f\right)^2\right]^{0,69}$.

Свойства чувствительности и маскировки могут использоваться как составляющие ПМ при погружении ЦВЗ на одной частоте. Если же ЦВЗ являются коррелированным процессом и содержат несколько частотных составляющих, то анализ необходимо выполнять на всех частотах ЦВЗ. Характеристика, называемая слиянием, оценивается статистическим параметром, который называется нормой Минковского [1]:

$$L_d(\mathrm{C}\ ,\mathrm{S}) = \left(\sum_i \left|P(i)^d\right|\right)^{\frac{1}{d}} \ , \qquad (5)$$

где $P(i)$ — вероятность того, что эксперт заметит разницу при оценке по определенным параметрам, фрагментам, i= 1,… I — число отличий ОПС и стегосообщений;

d=1÷4 — рекомендуемая константа [1].

При анализе эффекта маскировки необходимо разделять маскировку тоновой составляющей шумом (рис. 2,а) и маскировку шума тоновой составляющей (рис. 2,б). Возможна так же маскировка одного узкополосного шума другим, что, однако, весьма трудно оценить количественно и потому данный эффект ПМ не будет учитываться.

Таким образом, эффект маскировки зависит не только от энергии в критической

полосе, но и от спектральной меры монотонности

$$SM = 10\log_{10}\left[\frac{\left[\prod_{r=1}^{r=r\max}\Psi_{\Sigma}(r)\right]^{\frac{1}{r_{\max}}}}{\frac{1}{r_{\max}}\sum_{r=1}^{r=r_{\max}}\Psi_{\Sigma}(r)}\right]=\frac{\mu_g}{\mu_a}, \text{ дБ}, \qquad (6)$$

где μ_g, μ_a — геометрическая и алгебраическая меры спектральной плотности критических полос [1].

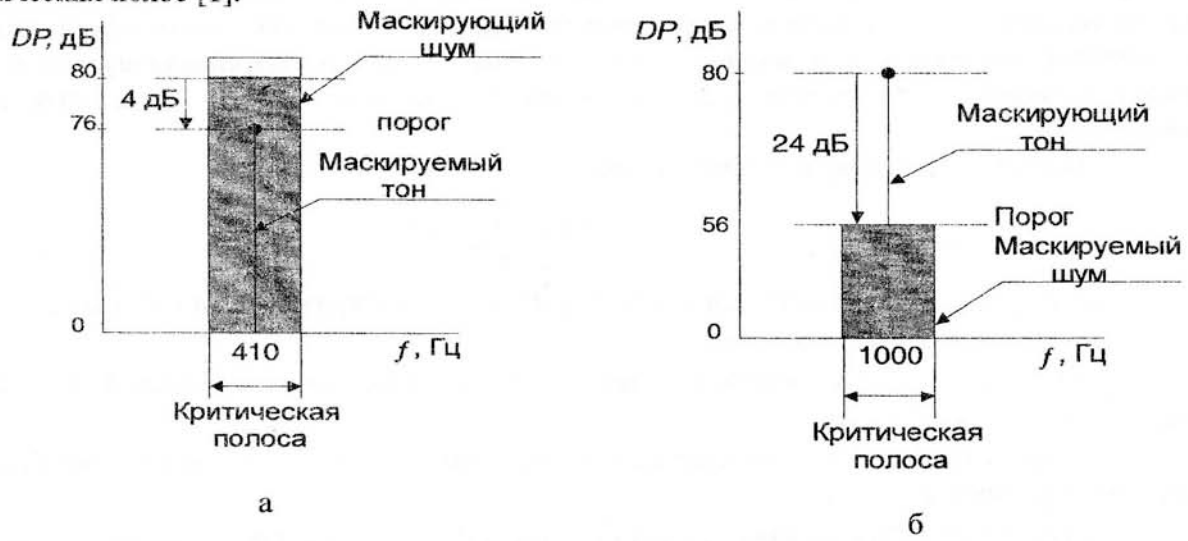

Рис. 2. Пример эффекта маскировки за счет чувствительности к окружению тональной составляющей шумом (а), шума тональной составляющей (б)

На основе спектральной меры монотонности можно оценить коэффициент тональности:

$$\alpha_T = \min\left(\frac{SM}{-60},\ 1\right). \qquad (6)$$

Если $\alpha_T = 1$, то составляющая является тональной, если меньше, то шумом. Эмпирически показано, что порог маскировки критической полосы в дБ можно оценить формулой $t(r) = 10\log_{10} IF(r) - \{\alpha_T(14{,}5 + r) + (1 - \alpha_T)5{,}5\}$ или в паскалях $t(r) = 10^{O(r)\frac{r}{10}}$, где $O(r) = \{\alpha_T(14{,}5 + r) + (1 - \alpha_T)5{,}5\}$ — эмпирическая формула оценки контраста. Для принятия решения о том, насколько какая либо частота внутри критической полосы может быть изменена значение порога $t(r)$ в паскалях нормализуется $t_n(r) = \frac{t(r)}{N_{fr}}$, где N_{fr} — число гармоник в критической полосе. Модель погружения ЦВЗ с автоматическим обеспечением незаметности на основании контроля энергетического порога (анализ чувствительности) весьма проста. Однако наилучшего результата следует ожидать при комплексном учете составляющих ПМ: чувствительности, маскировки и слияния, т.е. оценки (1) - (6).

Построение системы с цифровыми водяными знаками с учетом перцепционной модели

С учетом особенностей аудиовосприимчивости человека одним из основных методов анализа аудиосигналов является кратковременный спектральный анализ. Фрагмент аудиосигнала длительностью 10 с при частоте дискретизации в соответствии с теоремой Котельникова 22,05 кГц содержит около 220500 дискретов. Погружение ЦВЗ можно осуществлять как во временной, так и в частотной области. Переход в частотную область позволит облегчить учет ПМ при погружении ЦВЗ. При разделении на окна обработки (фреймы) длительностью 2048 отсчетов ДПФ выполняется для каждого фрейма, т.е.

$DFT(c(n)) = c(k) = \sum_{k=0}^{N-1} c(n)\exp(-2\pi nkj/N)$, K=2048, $n = 1,\ldots N$, N=$N_{фр}$=2048. В качестве ЦВЗ используется ПСП $w(n) = \{\pm\alpha\}$, где $\alpha > 0$, $\alpha = 0{,}5 \div 2$ дБ. Поскольку фазовые компоненты спектра ДПФ содержат больше перцепционной информации и поэтому их изменения в большей степени отразятся на надежности восприятия стегосигнала, то погружение ЦВЗ в фазовые компоненты ДПФ ОПС обеспечит большую надежность стегосистемы. Возможны следующие алгоритмы формирования стегосигнала:

$$s(n) = c(n) + w(n),\ n \in A_N, \tag{7}$$

$$s(k) = c(k) + w(k),\ k \in A_N, \tag{8}$$

$$arctgs(k) = arctg\{\sum_{n=0}^{N-1} c(n)\sin(2\pi nkj/N) / \sum_{n=0}^{N-1} c(n)c\cos(2\pi nkj/N) + w(k),\ k \in A_N. \tag{9}$$

Перед погружением ЦВЗ в видеширокополосной псевдослучайной последовательности, распределенной по всему фрейму, определялась дисперсия фрейма ОПС σ_{Fc}^2 и в случае $\sigma_{Fc}^2 \le 0{,}1\sigma_c^2$ фрейм не использовался для формирования стегосигнала, как не пригодный с точки зрения обеспечения надежности восприятия. Однако для аудио-сигналов наличие таких «тихих» фреймов не превышало 1-5 %. Длина ЦВЗ задавалась в соответствии с [3]. Косвенная оценка надежности восприятия стегосигнала основана на оценке параметров отношений сигнал/шум после формирования стегосигнала η_w и после воздействия аддитивного шума (процедуры перезаписи) η_α, причем, $\eta = \eta_w / \eta_\alpha$. При переходе в частотную область кроме выбора фрейма с наиболее широким спектром и дисперсией σ_{Fc}^2 погружение осуществлялось в СЧ и НЧ составляющие с адаптацией по амплитуде ЦВЗ (рис. 3).

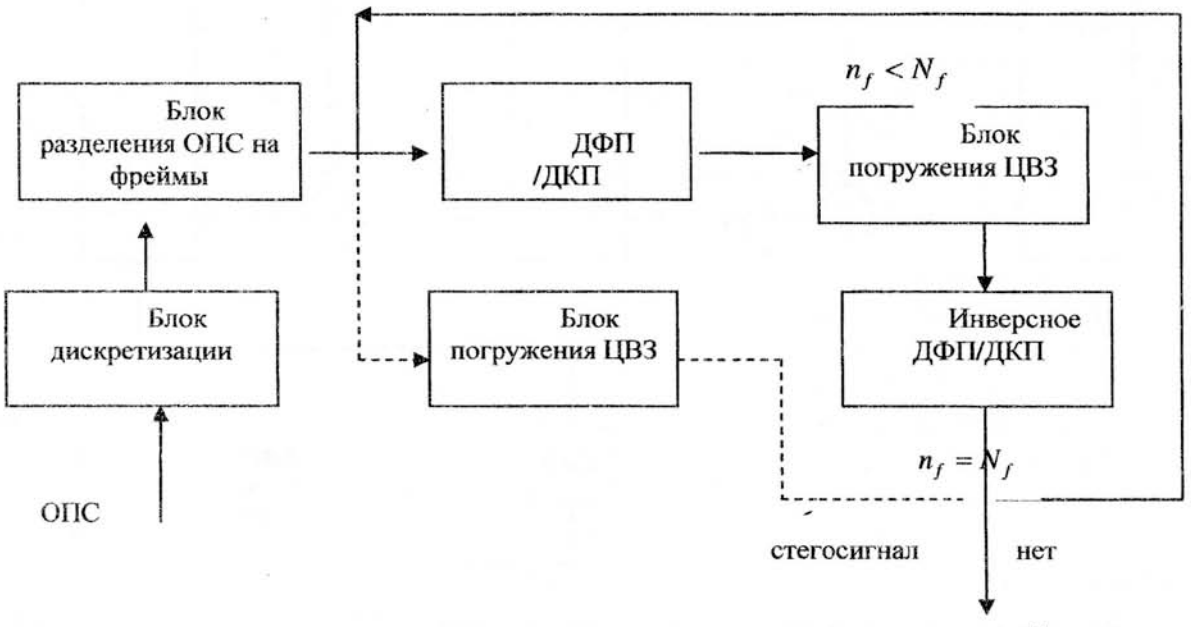

Рис. 3. Блок схема формирования стегосигнала

Результаты имитационного моделирования продемонстрировали удовлетворительное совпадение с данными аналитических исследований системы с ЦВЗ на основе детектора, не использующего при детектировании ЦВЗ знаний о ОПС [3]. Однако при $\sigma_w^2 \geq 0{,}2\sigma_c^2$ надежность восприятия стегасигнала при экспертной оценке оставляла желать лучшего. В реальных системах погружение цифровых водяных знаков должно осуществляться с учетом ПМ (рис. 4). Для учета эффектов чувствительности и маскировки в общем случае коррелированных ЦВЗ необходимо выполнять для каждой частотной составляющей ДФП/ДКП ЦВЗ. При анализе эффекта маскировки необходимо отдельно рассматривать маскировку тона шумом, шума тоном. Многократный расчет (1) - (6) весьма громоздкий. Формирование стегосообщения с учетом критерия порога маскировки в критических частотных полосах при ЦВЗ с параметрами N=1000, $\alpha = 0{,}025\sigma_c$ продемонстрировало приемлемую надежность восприятия, но при отсутствии атак десинхронизацией.

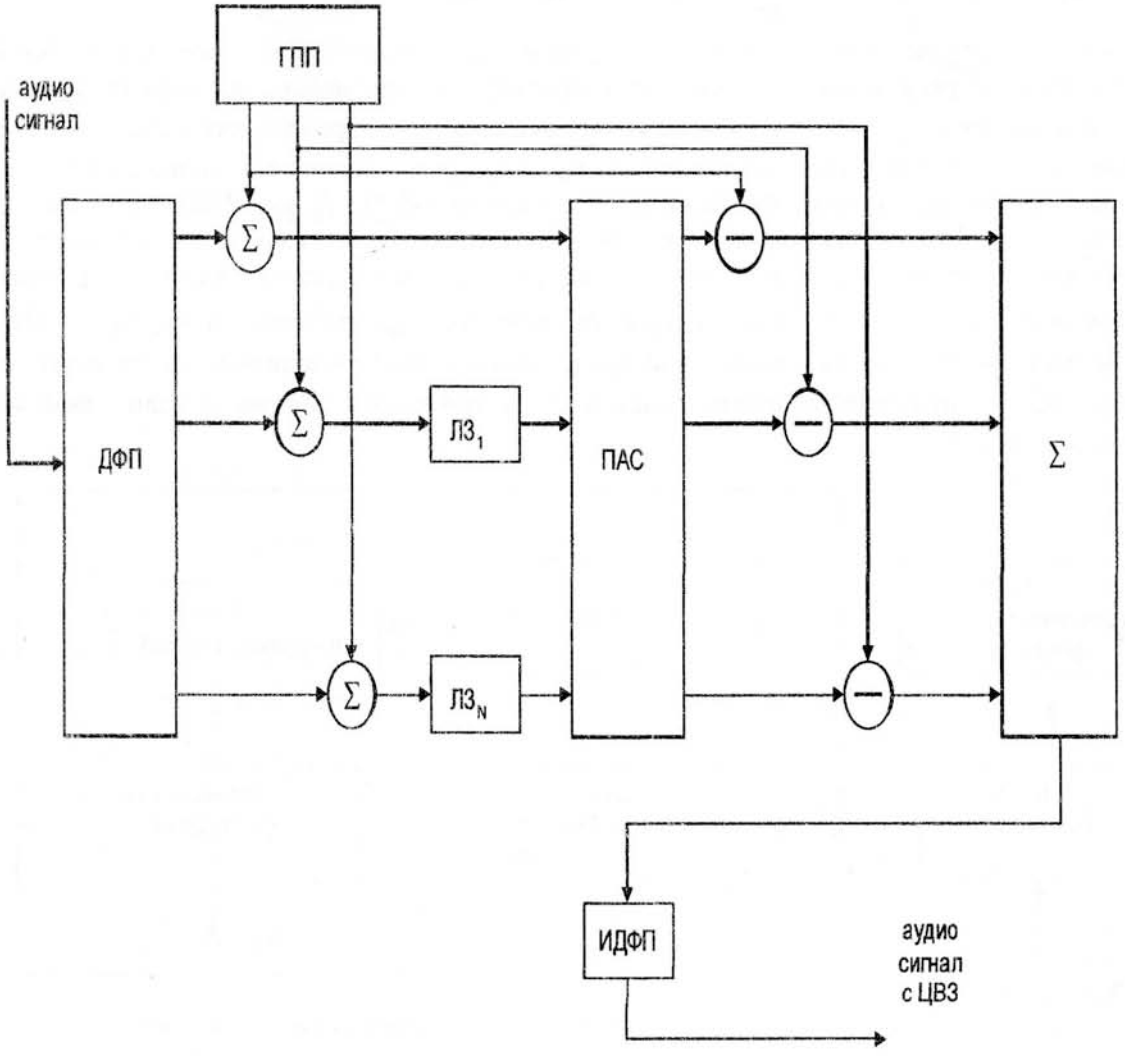

Рис. 4. Схема формирования стегосообщения с учетом ПМ:

ГПП – генератор ПСП $\{\pm\alpha\}$; ИДФП – инверсное ДФП; $ЛЗ_n$ – линия задержки на n тактов; ПАС – перцепционный анализатор спектра

Выводы

Использование даже выборочных положений ПМ при формировании стегосигнала при ОПС в виде аудиосигнала позволяет повысить эффективность системы с ЦВЗ, а именно, при заданном уровне эффективности детектирования ЦВЗ, например $P_{fa} = P_m = 10^{-3}$

представляется возможным уменьшить требуемую длину ЦВЗ более, чем на порядок. Улучшается экспертная оценка надежности восприятия аудиосигнала на выходе УФС. Однако для более серьезных выводов, безусловно, требуется проведения большого объема экспериментальных исследований и оценки (5) для представительного набора ОПС, получения соответствующих статистических данных.

Список литературы:

1. *Painter T., Spanias A.* Perceptual Coding of Digital Audio // Proceedings of the IEEE.— 2000. — Vol. 88(4). — P. 413—451.

2. *Moore B. C. J.* Masking in the human auditory system // Collected Papers on Digital Audio Bit-Rate Reduction. — 1996. —P. 9—19.

3. *Маракова І.І., Комендантов І.І.* Дослідження систем з цифровими водяними знаками при основному покриваючому повідомленні у виді аудіосигналу // Наукові праці ОНАЗ – 2004. – Вип. 2. – С. 40 – 46.

Поступила 1.12.2004г.

УДК 519.6:519.712.3:510.52

Зінченко Я.В.

МЕТОДИ ЗМЕНШЕННЯ ЧАСУ РЕАЛІЗАЦІЇ ОПЕРАЦІЇ МНОЖЕННЯ НАДВЕЛИКИХ ЧИСЕЛ ДЛЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

У більшості асиметричних криптографічних систем захисту інформації при шифруванні, дешифруванні і генерації ключів основною є операція модулярного зведення в ступінь, яка являє собою багаторазове виконання операції множення за модулем простого числа чи добутку простих чисел. З метою забезпечення необхідної практичної криптостійкості зазначених систем, розмірності модулів для них вибираються рівними 512…2048 бітам і більше. Оскільки ж процесори сучасних універсальних ПЕОМ не спеціалізовані на багаторозрядну арифметику, то обчислення ними добутків надвеликих чисел "стовпчиком" (складність цього традиційного методу порядку m^2, де m – довжина числа в бітах) вимагає істотних часових витрат, що обумовлює низьку швидкість роботи програмних реалізацій асиметричних криптосистем.

Одним з основних рішень проблеми підвищення швидкодії програмних реалізацій асиметричних криптосистем є застосування спеціальних методів множення надвеликих чисел [1]. На сьогоднішній день розроблена досить велика кількість таких методів, кожен з яких має свою область ефективного застосування в залежності від області значень m, моделі обчислень, програмної чи апаратної реалізації. Усі ці методи є рекурсивними і засновані на зведенні множення m-розрядних чисел до послідовності множень чисел з меншою кількістю розрядів. При їх практичній реалізації m-розрядні двійкові числа, що перемножуються, наприклад u і v, представляються як масиви l-бітних слів $(u_1, u_2, u_3, \ldots, u_K)$ та $(v_1, v_2, v_3, \ldots, v_K)$, де K – кількість l-бітних блоків у числах. Довжина блоку дорівнює розрядності процесора використовуваної ЕОМ.

Асимптотично найшвидшим з відомих методів є метод Шенхаге-Штрассена [1, 2]. Він заснований на ідеї використання теореми про дискретну згортку двох функцій і дозволяє помножити два m-розрядних двійкових числа за $m \log m \log\log m$ кроків (бітових операцій). Оскільки дискретна згортка дає основний внесок в оцінку складності методу, то для ефективного її обчислення використовується алгоритм швидкого перетворення Фур'є (ШПФ). Однак, використання для обчислення добутків надвеликих чисел алгоритму ШПФ