УДК 621.391

А.В. Гопиенко, Ю.В. Куц, Е.В. Монченко

Национальный авиационный университет, Киев

ФОРМИРОВАНИЕ ПОТАЙНЫХ КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ В КОМПЬЮТЕРИЗИРОВАННЫХ ИЗМЕРИТЕЛЬНЫХ СИСТЕМАХ

В статье рассмотрен способ формирования потайных каналов для организации скрытого информационного обмена по каналам измерительных систем, использующих для передачи открытой информации фазоманипулированные сигналы. Способ является одним из возможных вариантов реализации фазового метода стеганографии.

Ключевые слова: *фазовая стеганография, фазоманипулированный сигнал, потайной канал.*

Введение

Своевременное получение и доставка потребителю достоверной измерительной информации является необходимым условием надежной работы технических систем различного назначения, точного управления сложными технологическими и социальными процессами, принятия правильных управленческих решений. Современные измерительные системы (включая информационно-измерительные, контрольно-измерительные и диагностико-измерительные) представляют собой сложные, распределенные в пространстве технические комплексы, включающие не только измерительное, но и коммуникационное и компьютерное оборудование, сетевые и информационно-измерительные технологии передачи измерительной информации по открытым каналам. Вместе с возрастающими функциональными возможностями подобных систем такая интеграция несет в себе потенциальную угрозу умышленного искажения данных, что может привести к ошибкам при принятии решений с тяжелыми и плохо прогнозируемыми последствиями. Поэтому возникает задача скрытой передачи по открытым каналам наиболее важной, конфиденциальной части измерительной информации. Актуальность и злободневность вопросов защиты информации в информационно-измерительных системах (ИИС) обсуждалась, например, в работе [1].

Одним из эффективных способов передачи конфиденциальной информации в измерительных системах является создание и использование потайных или стеганографических каналов, под которыми понимают нестандартные способы передачи информации по легальным каналам.

На сегодня известно значительное число различных способов организации потайных каналов передачи данных. Например, в работе [2] рассмотрена возможность создания таких каналов путем перераспределения информационного ресурса открытого канала передачи цифровых данных между ним и потайным каналом путем выделения определенной части младших бит аудиоинформации для скрытой передачи данных. Выбор младших бит происходит с помощью специального секретного ключа, известного источнику и приемнику информации, а частота их использования не должна приводить к заметному искажению передаваемого аудиосигнала.

В целом, анализ публикаций в данной предметной области свидетельствует о том, что наиболее часто рассматриваются вопросы защиты информации, которые реализуются на высших уровнях модели взаимодействия открытых систем. В то же время концепция многоуровневой защиты информации предполагает использование методов защиты данных на всех уровнях, включая физический.

В работе [3] для скрытой передачи данных авторами предложен способ, основанный на модификации частотно-фазовой области сигнала-контейнера. Для достижения поставленной цели используется модулирование параметров гармонических несущих локализованными во времени сигналами-сообщениями с уровнем значительно меньшим уровня несущей. Суть предложенного способа состоит в том, что фаза гармонической несущей модулируется сообщением на интервалах времени, сопоставимых с ее периодом, а выделение сообщения осуществляется по результатам анализа фазовой (амплитудной) характеристики принятого сигнала-контейнера.

Цель статьи – исследовать возможность формирования потайного канала передачи информации в открытых коммуникационных каналах измерительных информационных систем с фазовой манипуляцией за счет незначительного изменения фазовых характеристик несущего сигнала.

Основной материал

Постановка задачи. Информационный обмен в открытом канале измерительной системы осуществляется с помощью сигналов двоичной фазовой манипуляции ФМ-2. Для передачи цифр двоичного кода используются радиоимпульсы вида

$$\begin{aligned} "0" &\rightarrow u_0(t) = U_0 \sin 2\pi ft, \quad t \in [t_н, t_н + T_c); \\ "1" &\rightarrow u_1(t) = U_0 \sin(2\pi ft + \pi), \quad t \in [t_н, t_н + T_c), \end{aligned} \tag{1}$$

где U_0, f – соответственно амплитуда и частота гармонического сигнала; $t_н, T_c$ – соответственно момент начала и длительность передачи одного канального символа (одной двоичной цифры).

Открытое сообщение – контейнер, представляет собой случайную последовательность детерминированных канальных символов (1), отображающих передаваемый цифровой сигнал и следующих через интервал T_c.

Каждый j-й бит s_j закрытого сообщения встраивается в контейнер в виде незначительного искажения фазовой характеристики сигнала (1) на величину $\psi(t)$ на всем интервале передачи одного канального символа $[t_н, t_н + T_c)$ или его части $[t'_н, t'_н + T'_c) \subseteq [t_н, t_н + T_c)$:

$$\begin{aligned} u_0(t) &= \sin\left(2\pi f t + \psi(t)\right), \quad t \in [t_н, t_н + T_c); \\ u_1(t) &= \sin\left(2\pi f t + \pi + \psi(t)\right), \quad t \in [t_н, t_н + T_c), \end{aligned} \tag{2}$$

где

$$\psi(t) = \begin{cases} 0, & s_j = 0, \\ \dfrac{\pi}{k}, & s_j = 1, \ t \in [t'_н, t'_н + T'_c). \end{cases} \tag{3}$$

Параметр $k > 1$ определяет уровень скрытности потайного канала.

Для передачи стегосигнала (2) используется открытый канал связи с постоянными параметрами. В канале действует аддитивный гауссовский шум (соотношение сигнал/шум по мощности не менее 100).

Необходимо проанализировать процесс выделения скрытого сообщения в предложенном фазовом методе стеганографии.

Решение задачи. В основу решения поставленной задачи положены полученные в [3] результаты. В этой работе показана принципиальная возможность использования гармонических несущих, модулированных сигналами с частотой модуляции, соизмеримой с частотой несущей и на интервалах времени соизмеримых с её периодом для передачи скрытых сообщений. Такой способ скрытой передачи реализуется следующим образом. Контейнером для передачи скрытого сообщения служит гармоническая несущая. Встраивание сообщения осуществляется путем модулирования параметров несущего сигнала на последовательности интервалов времени сопоставимых с его периодом. Сформированный таким образом стегосигнал передается через канал связи на приемник. Принятый стегосигнал подвергается преобразованию Гильберта (ПГ) с целью определения его амплитудной и фазовой характеристик [4]. Полученное сообщение выделяется на основе анализа разности соответствующих характеристик (фазовых или амплитудных) заполненного и пустого контейнеров.

Рассмотрим более подробно основные этапы формирования потайного канала.

1. Формирование стегосигнала. Встраивание скрытого сообщения осуществляется следующим образом. В предлагаемом техническом решении каждый канальный символ фазоманипулированного сигнала используется для передачи одного бита открытого сообщения или синхросигнала. Последний свидетельствует о начале/завершении одного байта переданных данных или всего сообщения в целом. При такой организации стегосигнала фазоманипулированный сигнал может быть использован для синхронизации приема каждого бита в переданном скрытом сообщении. Информационные и синхросигналы имеют различные полярности, что необходимо для их разделения. Встраивание в стегосигнал каждого ненулевого бита информации осуществляется путём замены соответствующего канального символа на его модифицированный в соответствии с (2) прототип.

2. Анализ стегосигнала и выделение сообщения. Принятый сигнал представляется аддитивной смесью сигнала-контейнера и гауссовского шума n(t) вида

$$y(t) = \sum_{i=1}^{M} u_i(t) + n(t), \quad t \in [t_н, \ t_н + MT_c), \tag{4}$$

где M – количество принятых канальных символов, $u_i(t)$ – i-й канальный символ вида (2) с учетом его затухания в канале передачи данных.

Сигнал (4) сегментируется на канальные символы $y_i(t), \ t \in [t_н + (i-1)T_c, \ t_н + iT_c)$. Для каждого выделенного сегмента выполняется преобразование Гильберта $\hat{y}_i(t) = \mathbf{H}[(y_i(t)]$, где $\mathbf{H}$ – оператор преобразования Гильберта, и определяется дробная часть фазовой характеристики.

$$\begin{aligned} \tilde{\varphi}_i(t) &= \operatorname{arctg}\left(\hat{y}_i(t)/y_i(t)\right) + \\ &+ (\pi/2)\cdot\left[2 - (1 + \operatorname{sign} y_i(t))\operatorname{sign}\hat{y}_i(t)\right], \quad \tilde{\varphi}_i \in [0, 2\pi), \end{aligned} \tag{5}$$

где $\operatorname{sign}(\cdot)$ – знаковая функция.

Развернутую на интервале $[t_н + (i-1)T_c, \ t_н + iT_c)$ фазовую характеристику канального символа определяют как функцию

$$\tilde{\Phi}_i(t) = \tilde{\varphi}_i(t) + \mathbf{L}[\tilde{\varphi}_i(t)]2\pi, \tag{6}$$

где $\mathbf{L}[\cdot]$ – оператор ступенчатой функции, необходимой для устранения скачков $\tilde{\varphi}_i(t)$.

Оценка i-го бита сообщения формируется с учетом того, что фазовая характеристика сигнала-контейнера без сообщения является линейной функцией времени, а частота f несущей известна или может быть измерена с высокой точностью

$$\tilde{\psi}_i(t) = \tilde{\Phi}_i(t) - 2\pi f t, \ t \in [t_н + (i-1)T_c, \ t_н + iT_c). \tag{7}$$

Определив функции $\tilde{\psi}_i(t)$ для всех $i = \overline{1, M}$ и выделив синхроимпульсы можно восстановить переданное сообщение.

Скрытность передачи будем оценивать по вносимым в каждый канальный символ стегосигнала

искажениям как среднюю за время передачи одного канального символа мощность разностного сигнала – канальных символов сигнала-контейнера $y_{i,1}(t)$ для $s_j = 1$ и $y_{i,0}(t)$ для $s_j = 0$ (что соответствует канальному символу без сообщения)

$$P = \frac{1}{T_c} \int_{t_н+(i-1)T_c}^{t_н+iT_c} \left(y_{i,1}(t) - y_{i,0}(t)\right)^2 dt \qquad (8)$$

или ее нормированное значение (коэффициент скрытности)

$$k_{ск} = \int_{t_н+(i-1)T_c}^{t_н+iT_c} \left(y_{i,1}(t) - y_{i,0}(t)\right)^2 dt \Big/ \int_{t_н+(i-1)T_c}^{t_н+iT_c} y_{i,0}^2(t) dt . \qquad (9)$$

Результаты моделирования. Моделирование задачи скрытой передачи сообщения выполнялось в системе Matlab для следующих исходных данных.

Мгновенные значения канальных символов сигнала-контейнера (1) формировались в дискретные моменты времени $jT_д$, $j = \overline{1, N}$ и имели следующие характеристики: $U = 1$; частота $fT_д = 10^{-2}$, где $T_д$ – период дискретизации сигналов; объем выборки $N = 1000$. Длительность канального символа выбрана равной длительности периода несущей, т.е. $T_c = T$.

Принятый сигнал представлялся аддитивной моделью (4), в которой шум $n(t)$ задавался как реализация случайной гауссовской величины с нулевым математическим ожиданием и среднеквадратическим значением $\sigma = 0,05$. Передаваемое закрытое сообщение ввиде байта цифровых данных $S_з = (01100100)_2$ встраивалось в сигнал-контейнер, соответствующий открытому сообщению $S_o = (01001111)_2$. Параметр $k = 10\pi$, а модификация фазы в соответствие с (3) выполнялась в последних полупериодах канальных символов, причем для передачи информационных бит выбрано $\psi = \pi/k = 0,1$ рад, а для синхросигналов $\psi = -0,1$ рад.

На рис. 1 представлено встраиваемое сообщение $S_з$ и соответствующая функция $\psi[j]$ (рис. 1, а), а так же открытое сообщение S_o и стегосигнал со встроенным сообщением (рис. 1, б) и, для сравнения, пустой контейнер (рис. 1, в). Графики на рис. 1, а, б визуально практически неразличимы, как неразличимы и их спектры, что и обеспечивает скрытность передачи сообщения. Коэффициент скрытности (9) для сформированного стегосигнала с заданными параметрами не превышает величины 0,005.

Закрытое сообщение объемом 1 байт (рис. 1, а) выделено слева и справа синхроимпульсами, которые отличаются от информационных бит полярностью. Вес каждого бита определяется номером канального символа в интервале между двумя смежными синхроимпульсами. Каждый бит передается в течение одного периода несущей, соответственно каждый 9-ый период является синхронизирующим (определяющим начало очередного байта данных). Дополнительная служебная информация, например, о начале передачи нового сообщения, может задаваться установленной последовательностью любого числа отрицательных модулирующих импульсов в функции $\psi[j]$.

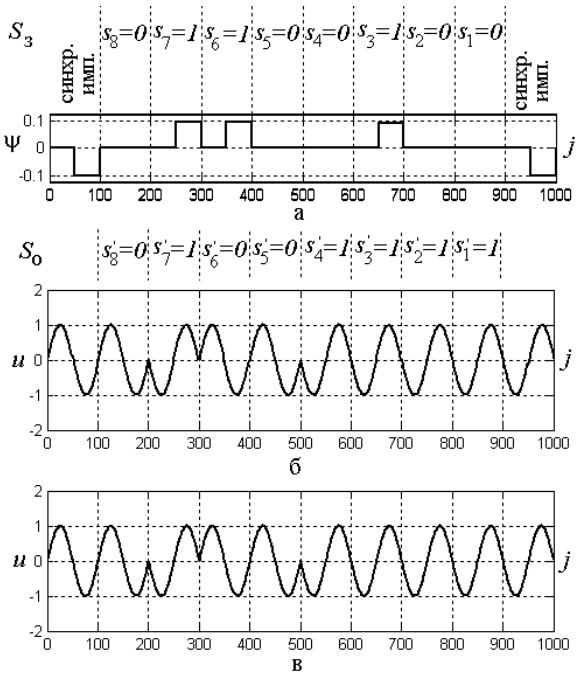

Рис. 1. Встраиваемое сообщение S_3 и соответствующая функция

Аддитивная смесь стегосигнала и гауссовского шума (стегосигнал на стороне приёма), из которой необходимо извлечь скрытое сообщение, приведена на рис. 2.

Обработка стегосигнала выполнялась отдельно для каждого канального символа. На рис. 3, в качестве примера, представлены оценки функций $\tilde{\psi}_2[j]$ и $\tilde{\psi}_{синхр}[j]$, рассчитанных по формуле (7) соответственно для второго бита s_2 и синхроимпульса (рис. 3 а, в, кривые 1) и их цифровые копии $\hat{\psi}_2(t)$ и $\hat{\psi}_{синхр}(t)$, полученные после выполнения медианной фильтрации (рис. 3 а, в, кривые 2) и операции компарирования (рис. 3 б, г).

Для повышения уровня скрытности встраиваемое сообщение может быть предварительно зашифровано.

Из проведенного анализа предложенного способа получения, передачи и восстановления скрытых сообщений можно сделать вывод о том, что он может быть использован для формирования потайных каналов передачи информации в измерительных системах, в которых открытый информационный обмен организован на основе использования фазоманипулированных сигналов.

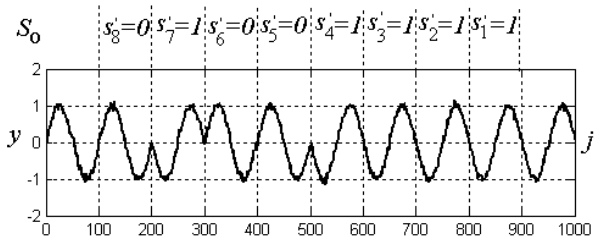

Рис. 2. Аддитивная смесь стегосигнала и гауссовского шума

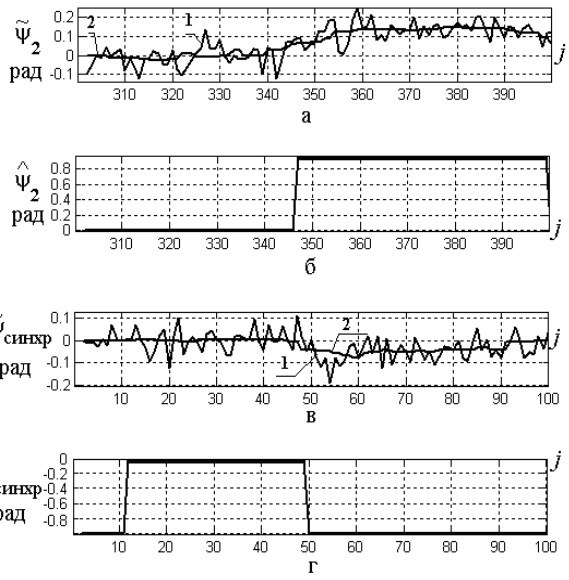

Рис. 3. Оценки функций

Следует отметить, что устойчивость работы потайного канала передачи данных существенно зависит от уровня шумов канала и возможных преднамеренных его искажений. В целом создание потайных каналов связано с поиском некоторого компромисса между допустимым уровнем искажения статистических свойств информационного сигнала, его спектральных и энергетических характеристик, помехоустойчивости и надежности передачи информации. С целью повышения помехоустойчивости приема стегосигнала представляется целесообразным выполнить анализ эффективности корреляционной обработки фазовых характеристик сигналов.

Выводы

Задача организации потайных каналов передачи информации занимает существенное место в общей проблеме информационной безопасности. Применение методов защиты информации на физическом уровне обеспечивает дополнительную степень защищенности информационного обмена в измерительных системах. Рассмотренный способ создания потайных каналов является одним из возможных вариантов реализации фазового метода стеганографии, использующим в качестве контейнеров фазоманипулированные сигналы, практически не требует дополнительных затрат энергии на передачу конфиденциальной информации. Показана возможность формирования потайного канала передачи информации за счет незначительного изменения фазовых характеристик сигнала-контейнера. Выделение скрытого сообщения базируется на использовании фазовых характеристик сигналов открытого канала, получаемых с помощью преобразования Гильберта.

Повышение помехозащищенности потайного канала и его устойчивости к влиянию преднамеренных искажений возможно за счет применения корреляционной обработки фазовых характеристик сигналов, что требует дальнейших исследований.

Список литературы

1. Исаев А.Б. Современные технические методы и средства защиты информации: учеб. пособие / А.Б. Исаев. – М.: РУДН, 2008. – 253 с.: ил.

2. Пузыренко О.Ю. Комп'ютерні системи стеганографічної обробки і захисту інформації у цифровому звуковому мовленні: автореферат дис. ... канд. техн. наук / О.Ю. Пузиренко. – К., 2012. – 20 с.

3. Пат. 51344 UA, МПК H04K 1/00. Спосіб прихованого передавання інформації / Куц Ю.В., Гопієнко А.В., Монченко О.В.; власник Нац. авіац. ун-т. – № u2010 01022; заявл. 01.02.2010; опубл. 12.07.2010, Бюл. № 13.

4. Куц Ю. В. Статистична фазометрія / Ю.В. Куц, Л.М. Щербак. – Тернопіль: В-во Терноп. технологіч. ун-ту, 2009. – 383 с.

Поступила в редколлегию 16.02.2012

Рецензент: д-р техн. наук проф. Л.М. Щербак, Национальный авиационный университет, Киев.

ФОРМУВАННЯ ПОТАЙНИХ КАНАЛІВ ПЕРЕДАЧІ ІНФОРМАЦІЇ В КОМП'ЮТЕРИЗОВАНИХ ВИМІРЮВАЛЬНИХ СИСТЕМАХ

А.В. Гопієнко, Ю.В. Куц, О.В. Монченко

В статті розглянутий спосіб формування потайних каналів організації прихованого інформаційного обміну по каналах вимірювальних систем, що використовують для передачі відкритої інформації фазоманіпульовані сигнали. Спосіб є одним з можливих варіантів реалізації фазового методу стеганографії.

Ключові слова: *фазова стеганографія, фазоманіпульований сигнал, таємний канал.*

FORMING OF SECRET CHANNELS OF INFORMATION TRANSFER IN COMPUTER MEASURING SYSTEMS

A.V. Gopienko, Yu.V. Kuts, O.V. Monchenko

In the article the method of forming of the secret channels is considered for the hidden information transfer in channels of the measurings systems, using phase-manipulated signals for an opened information transfer. A method is one of possible variants of realization of phase method of steganographion.

Keywords*: phase steganographion, phase-mamipulation signal, secret channel.*