УДК 621.391

ОСОБЕННОСТИ ПОСТРОЕНИЯ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ РАДИОСВЯЗИ

К.С. Васюта,
С.В. Озеров, А.Н. Королюк
Харьковский университет Воздушных Сил им. Ивана Кожедуба

Abstract *- The successful solution to protect information from unauthorized access plays a large role in increasing stealth radio system and, as a consequence, its vitality. Now for the task involved cryptography and steganography. Application only cryptography does not completely solve the problem of data security observer, since the presence of an encrypted message attracts cryptanalysts. Hiding the same of the transfer of confidential data through the communication channel is a problem of steganography. By steganographic method to hide information in radio communication systems include the use of broadband (noise-like) signals. The work under the "noise" when the reconnaissance unit can not detect (save) the transmitted signal due to the similarity of the signal with a random process in the visual, correlation and spectral analysis.*

At the moment, promising are the communication system using chaotic sequences as information carriers. Noise-like (working under the "noise") and self-synchronization systems based on chaos and give them the potential benefits over traditional spread spectrum systems, based on a pseudo-random sequences. However, this class of signals is not met in full secrecy, as their attractors structured and easily distinguishable from the attractors of random processes with independent and identically distributed values. Accordingly, for the solution of the secure data transmission in a communication channel is inappropriate to use harmonic carrier and chaotic signals with simple attractor, as their attractors structured and easily classified in phase space. To ensure the secrecy of the operation of radio systems are useful complex chaotic signals that the visual, spectral, correlation and nonlinear analysis to be indistinguishable from white noise.

Анотація *– Аналізуються відмінності між криптографічними і стеганографічними методами передачі інформації в системах радіозв'язку. Проілюстровані властивості різних типів сигналів з позиції прихованої передачі інформації і показано можливість їх застосування для стеганографічних методів прихованої передачі повідомлень. Запропоновані нові підходи приховування інформації в стеганографічних системах радіозв'язку для передачі даних. Запропонована узагальнена структурна схема системи стеганографічного радіозв'язку.*

Аннотация *– Анализируются различия между криптографическими и стеганографическими методами передачи информации в системах радиосвязи. Проиллюстрированы свойства разных типов сигналов с позиции скрытой передачи информации и показана возможность их применения для стеганографических методов скрытой передачи сообщений. Предложены новые подходы скрытия информации в стеганографических системах радиосвязи для передачи данных. Предложена обобщённая структурная схема системы стеганографической радиосвязи.*

Введение

Известно, что успешное решение задачи по защите информации от несанкционированного доступа играет большую роль в повышении скрытности системы радиосвязи и, как следствие, её живучести. В настоящее время для решения этой задачи привлекаются криптография и стеганография. Криптографическая защита информации предполагает лишь изменение (шифрование) сообщения с целью скрытия смысла передаваемой информации для стороннего наблюдателя (обеспечение информационной скрытности). Однако применение лишь криптографии не решает полностью проблему защиты информации от несанкционированного наблюдателя,

поскольку наличие шифрованного сообщения привлекает внимание криптоаналитиков. Скрытие же самого факта передачи конфиденциальных данных по каналу связи является задачей стеганографии [1]. Иначе говоря, под скрытием передачи информации следует подразумевать не только невозможность ее обнаружения в перехваченном сообщении, но и скрытие самого факта передачи сообщения по каналу связи. Поэтому применение стеганографических методов скрытия информации является актуальным при передаче, обработке и хранении информации.

В дальнейшем под скрытностью систем радиосвязи будем понимать [1, 2] способность противостоять мерам радиотехнической разведки: обнаружению сигнала и определению его структуры на основе оценки ряда его параметров без учета возможности раскрытия смысла информации. В качестве критерия скрытности можно принять величину $p_{скр} = 1 - p_р$, которая определяется вероятностью разведки $p_р = p_{обн} p_{стр}$, характеризуемой вероятностью правильного обнаружения сигнала $p_{обн}$ и вероятностью раскрытия его структуры $p_{стр}$.

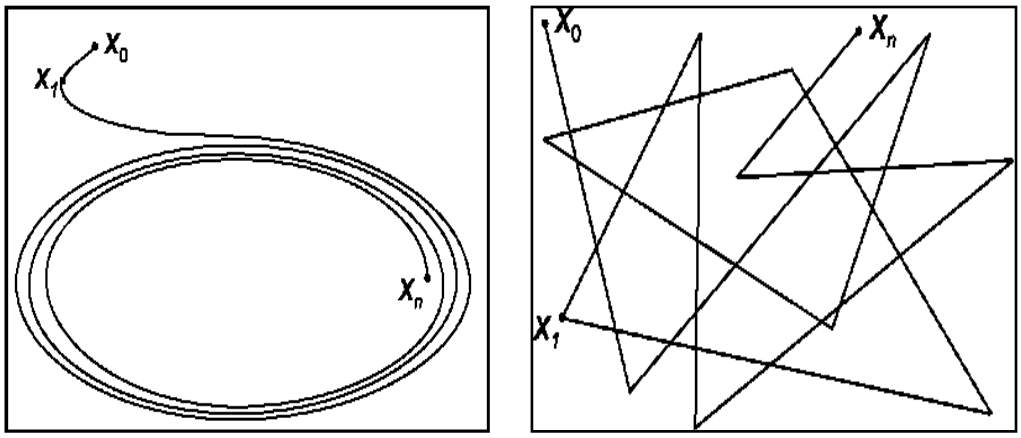
Традиционно для обнаружения детерминированных сигналов с неизвестной "формой" и случайных процессов используют энергетические обнаружители (радиометры), базирующиеся на χ^2 - статистике. В качестве признака процесса используется его энергия. Фактически оптимальный обнаружитель представляет собой измеритель мощности процесса, позволяющий выявлять энергетические приращения над мощностью шумов при наличии сигнала в анализируемом диапазоне частот. В то же время понятие "форма" процесса можно рассматривать как лингвистическую характеристику, которую можно формализовать, пользуясь, например, следующей цепочкой: "форма" процесса → структурированность аттрактора процесса → зависимость значений процесса → критерий зависимости (динамический или статистический) → мера зависимости (например, динамические инварианты: показатели Ляпунова, корреляционная размерность или энтропия). Корреляционной размерностью можно характеризовать структурированность аттрактора, связанного с анализируемым процессом. Например, случайный I.I.D (independent and identically distributed) процесс неструктурирован, его аттрактор полностью "заполняет" пространство вложения, а корреляционная размерность совпадает с его размерностью. Различия в "наполняемости" фазового пространства аттракторами случайного и детерминированных процессов и, как следствие, в зависимостях корреляционной размерности от размерности пространства вложения подсказывают еще один способ классификации наблюдений, а также решения задачи анализа скрытности сигналов, наблюдаемых на фоне шума.

Целью работы является развитие стеганографических методов скрытой передачи информации в системах радиосвязи.

I. Основная часть

Под стеганографической системой следует понимать совокупность средств и методов, которые используются с целью формирования скрытого (незаметного) ка-

нала передачи информации. Процесс скрытия данных в таких системах отличается от операции шифрования. Его целью является не ограничение или регламентирование доступа к сигналу (файлу-контейнеру), а в значительной степени гарантия того, что встроенные данные останутся необнаруженными и неподлежащими восстановлению [1]. Принципиальное различие стеганографической и криптографической систем, как показано в работе [2], состоит в том, что стеганосистема может иметь дробную размерность, меньшую, чем число независимых переменных системы, а в криптографических системах стараются использовать все пространство с максимальной целой размерностью (см. рис. 1).



а) б)

Рис. 1. Фазовые портреты стеганографической (хаотической) (а) и криптографической (б) систем

Исходя из анализа работ [3, 4], при построении стеганосистемы должны учитываться следующие требования:

– скрытие факта передачи информации для стороннего наблюдателя;

– обеспечение необходимой пропускной способности (что особенно актуально для скрытой передачи данных);

– обеспечение аутентичности и целостности конфиденциальной информации для авторизированного пользователя;

– обнаружение скрытого сообщения сторонним наблюдателем не должно позволить последнему извлечь его до тех пор, пока принцип формирования сигнала («ключа») сохраняется в тайне.

Стеганографические методы скрытия информации широко применяются в автоматизированных системах управления (компьютерная стеганография). В работе [3] показано, что компьютерная стеганография используется для решения следующих задач:

– защита конфиденциальной информации от несанкционированного доступа;

– защита авторского права на интеллектуальную собственность;

– преодоление систем мониторинга и управления сетевыми ресурсами;

– создание скрытых от законного пользователя каналов утечки информации.

Методы компьютерной стеганографии реализуются путем встраивания сооб-

щения в текст, изображения, аудиосигналы, видеоизображения, основываясь на ключевых принципах, изложенных в [3]. Например, файлы, которые не требуют абсолютной точности (файлы с изображением, звуковой информацией и т. д.), могут быть изменены без потери их функциональности, в то время как органы чувств человека неспособны различать незначительные изменения в модифицированных таким образом файлах.

Не менее актуальным направлением применения стеганографических методов скрытия информации является повышение скрытности систем радиосвязи. В современных радиосистемах используются следующие методы скрытия информации в канале передачи данных:

– накопление информации и дискретной ее передачи за короткие интервалы времени (до нескольких миллисекунд);

– накопление информации за достаточно продолжительное время с последующей передачей в назначенное время или при получении внешней команды;

– периодическая или хаотичная перестройка частоты канала излучения;

– использование широкополосных (шумоподобных) сигналов, когда энергия сигнала распределена в широкой полосе частот, и сигнал не имеет ярко выраженного превышения над шумами (работа под «шум»);

– выбор частоты излучения рядом с сильными источниками легальных сигналов, которые перегружают приемные тракты разведывательной аппаратуры, при недостаточном динамическом диапазоне или маскируются спектром легального сигнала при недостаточно низких фазовых шумах радиотрактов разведывательных комплексов;

– маскировка под стандартные каналы связи и/или работа узкополосных излучений внутри спектра легальных широкополосных сигналов;

– использование стандартных каналов связи, таких как GSM, CDMA, WiFi, BlueTooth.

Используемые методы могут комбинироваться друг с другом. Так, например, использование сигналов со сверхширокой полосой занимаемых частот может комбинироваться с методом накопления информации и дискретной ее передачей.

К стеганографическим методам скрытия информации в радиосвязи можно отнести использование широкополосных (шумоподобных) сигналов, т.е. работу под “шум”, когда разведывательный приемник не может обнаружить (накопить) передаваемый сигнал из-за схожести сигнала со случайным процессом при визуальном, корреляционном и спектральном анализах. Обобщенную структурную схему такой стеганографической системы связи можно представить в виде, показанном на рис. 2.

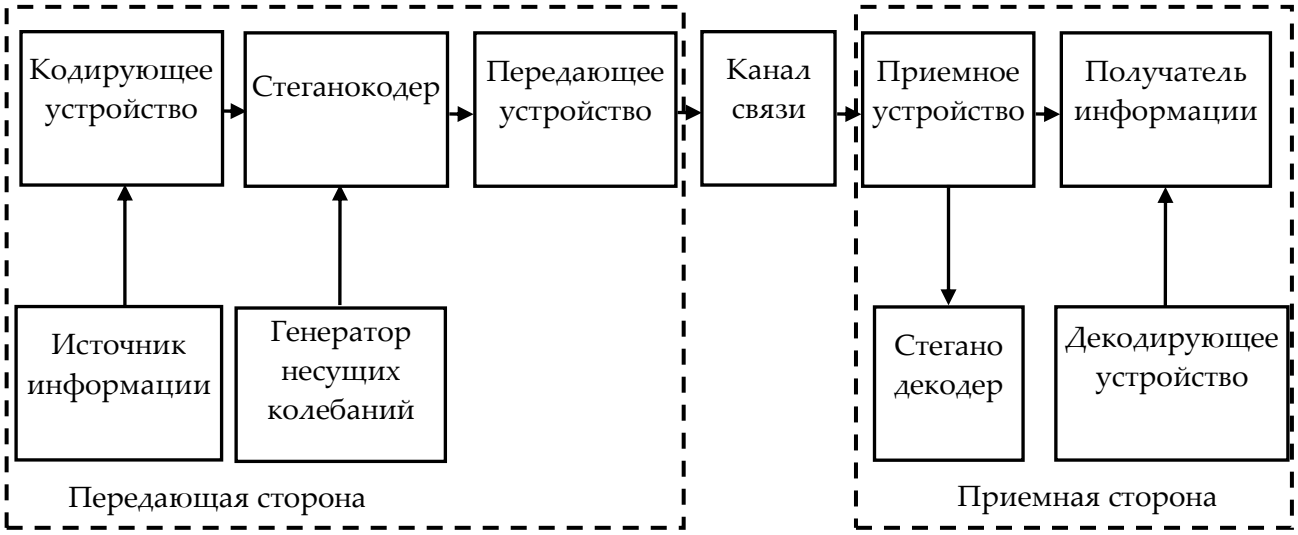


Рис. 2. Обобщенная структурная схема стеганосистемы связи

Выбор несущего сигнала (контейнера) – один из наиболее ответственных факторов, который учитывается при проектировании стеганографической системы связи. Это положение объясняется прежде всего тем, что "формой" сигнала определяются такие важнейшие функции, как кодирование и модуляция, в свою очередь, намечаются структура и функциональная схема всего передающего устройства. На сложность приемного устройства форма сигнала также оказывает решающее влияние. Таким образом, от выбора формы сигнала зависит, по существу, структура всей системы, следовательно, – и ее основные характеристики (скрытность, сложность, надежность и т.д.).

Ниже проанализируем (с позиции скрытности для несанкционированного наблюдателя) такие виды сложных сигналов (детерминированный – фазокодоманипулированный (ФКМ) сигнал, хаотический, описываемый полиномом Чебышева, случайный процесс – шум), которые могут быть использованы при реализации стеганографической передачи данных в системе радиосвязи.

Одним из наиболее используемым в системах радиосвязи для скрытия информации является ФКМ-сигнал. Преимущества при использовании ФКМ-сигналов в широкополосных системах связи следующие [5]:

– конфиденциальность передачи информации, так как сигнал кодируется, а распределение мощности в широкой полосе частот уменьшает возможность его обнаружения;

– устойчивость к организованным помехам, так как корреляционная обработка в приемнике уменьшает относительный уровень организованной помехи;

– возможность одновременного доступа для нескольких абонентов, поскольку одну и ту же полосу спектра могут иметь несколько сигналов, если их коды не коррелированы.

ФКМ-сигнал можно представить последовательностью импульсов с длительностью τ_u, амплитудой U, каждый из которых определяется аналитическим выражением:

$$u(t) = \begin{cases} 0, t < -\tau_u / 2 \\ U \cos \omega_0 t, -\tau_u / 2 \le t \le \tau_u, \\ 0, t > \tau_u / 2 \end{cases} \quad (1)$$

При этом в качестве первичных сигналов, как правило, используются сигналы с кодом Баркера, так как в их автокорреляционных функциях реализуется наименьший уровень боковых лепестков. Временная реализация, фазовый портрет и энергетический спектр ФКМ-импульса с семиэлементным кодом Баркера приведены на рис. 3. Из рисунка следует что, применение ФКМ-сигнала не удовлетворяет требованиям стеганографической передачи данных, так как энергетический спектр не имеет равномерного распределения, а фазовый портрет имеет ярко выраженную структурную зависимость. Следует отметить важное замечание – применение сложных кодов для скрытия, прежде всего, смысла передаваемой информации обеспечивает лишь структурную и информационную скрытность. Скрытие же самого факта передачи информации не происходит из-за применения гармонической несущей, которая легко обнаруживается (правильно классифицируется) современными методами нелинейного анализа.

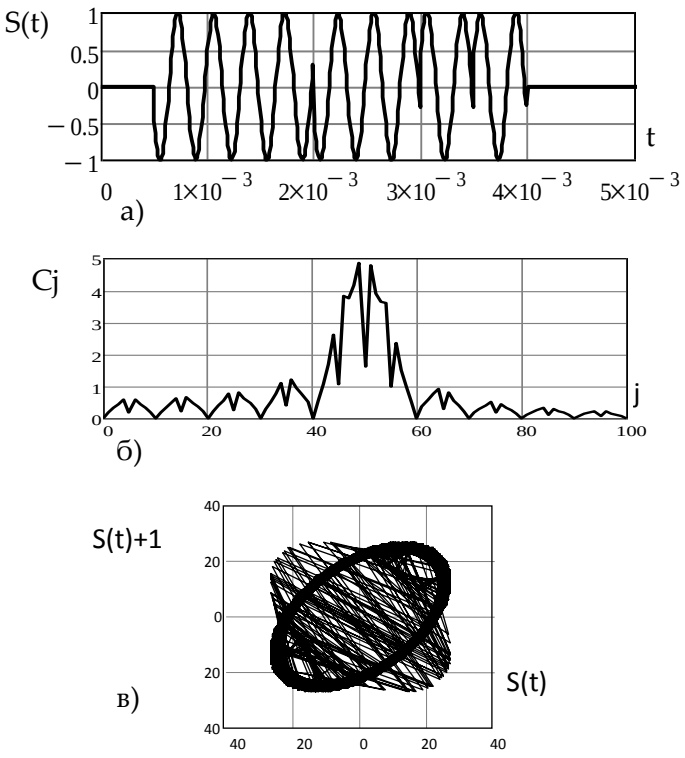


Рис. 3. Временная реализация ФКМ-импульса (а), энергетический спектр (б), фазовый портрет (в)

Исходя из этого, в последнее время получили широкое распространение системы связи, использующие хаотические колебания и хаотические последовательности в качестве носителей информации. Использование динамического хаоса в системах передачи информации позволяет получить следующие преимущества [6]:

– хаотические процессы можно получать при помощи достаточно простых динамических систем, при этом можно создавать большое число различных закрытых каналов связи, что способствует увеличению степени конфиденциальности;

– возможность самосинхронизации приемника и передатчика и потенциально большую информационную емкость хаотических систем связи;

– скорость передачи можно повысить за счет использования нескольких информационных параметров хаотического генератора;

– возможность получения разнообразных методов подмешивания сообщения в хаотический сигнал.

Шумоподобность (работа под «шум») и самосинхронизируемость систем, основанных на хаосе, дают им потенциальные преимущества над традиционными системами с расширением спектра, базирующимися на псевдослучайных последовательностях. Кроме того, они позволяют получить более простую аппаратную реализацию с большей энергетической скрытностью [6], более высокую скорость операций [7, 8]. *Для* анализа использована хаотическая последовательность Чебышева, аналитическое выражение которой имеет вид:

$$x_{n+1} = 4(x_n)^3 - 3x_n. \qquad (2)$$

Временная реализация, фазовый портрет и энергетический спектр хаотической последовательности Чебышева приведены на рис. 4. Как показано на рисунке, по сравнению с ФКМ-сигналом, см. рис. 3, хаотические сигналы обладают энергетическим спектром, подобным случайному процессу (рис. 5).

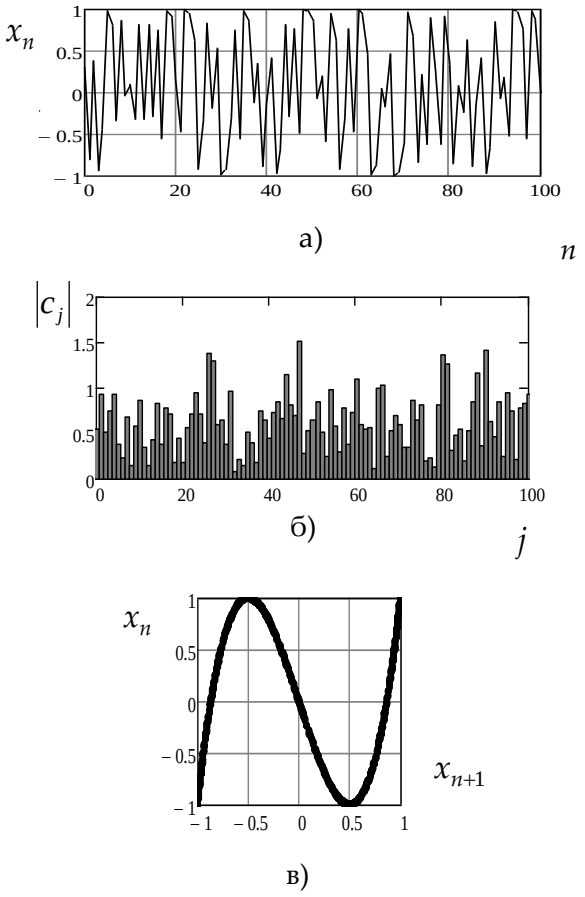


Рис. 4. Временная реализация хаотической последовательности (а), энергетический спектр (б), фазовый портрет (в)

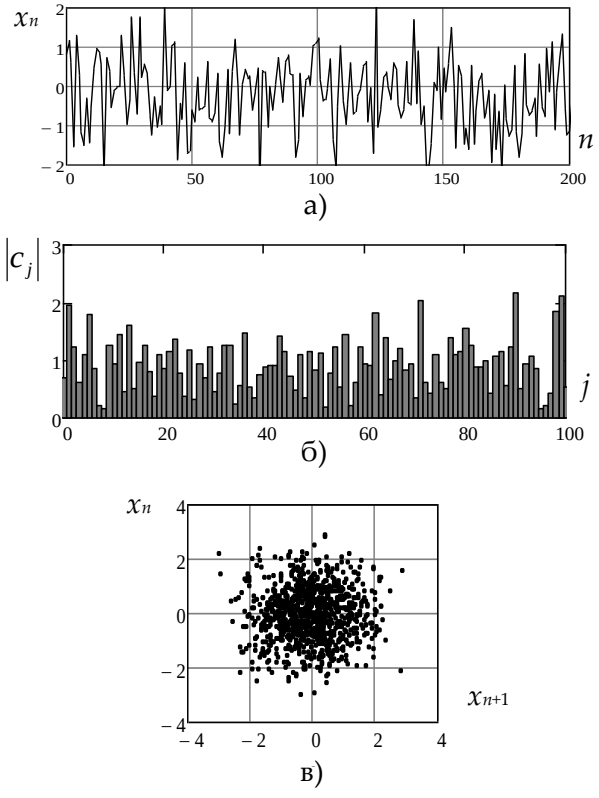


Рис. 5. Временная реализация белого гауссовкого шума (а), энергетический спектр (б), фазовый портрет (в)

Однако и этот класс сигналов не удовлетворяет требованиям скрытности в полной мере, так как их аттракторы структурированы и легко отличимы от аттракторов случайных процессов с независимыми и одинаково распределенными значениями [8]. Поэтому, с позиции стеганографии, наиболее применимы для скрытой передачи сообщений случайные фрактальные процессы с зависимыми значениями, которые оказываются весьма чувствительными к вариациям их параметров. Например, изменение показателя Херста (коэффициента самоподобия) фрактального гауссовского шума влияет на его «цвет» [7-9] и может быть применено для скрытой передачи бинарных сообщений. При моделировании фрактального шума использовано приближенное выражение [10], которое в дискретные моменты времени t имеет вид:

$$S(t,H,n) \approx \frac{n^{-\frac{1}{2}}}{\Gamma\left(H+\frac{1}{2}\right)}\left[\sum_{i=0}^{[n\cdot(t+1)]-1}\left((t+1)-\frac{i}{n}\right)^{H-\frac{1}{2}}\xi_i - \left[\sum_{i=0}^{tn-1}\left(t-\frac{i}{n}\right)^{H-\frac{1}{2}}\xi_i\right]\right], \quad (3)$$

где ξ_i – значение порождающего процесса в дискретные моменты времени i, (см. рис. 5); n – параметр ядра, задающий конечное разрешение; H – показатель Херста (коэффициент самоподобия), принимающий значение из интервала [0, 1].

Для примера рассмотрим подход скрытой передачи бинарного сообщения в стеганографическом канале радиосвязи. Предположим, что q-му элементу r_q бинарного сообщения $\vec{r} = (r_1,...,r_L)$ (L – число его элементов), принимающего значение $r_q = 0$, ставится в соответствие параметр $H = 0{,}1$, а для $r_q = 1$ – значение $H = 0{,}9$ (рис. 6).

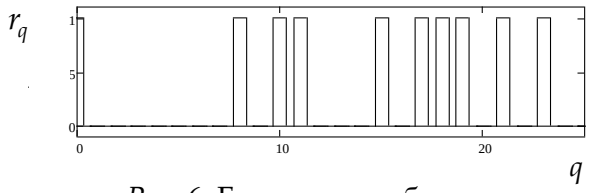


Рис. 6. Бинарное сообщение r

На рис. 7 приведена реализация информационной последовательности $\{S_i\}_{i=0}^{t}$, полученной в результате манипуляции параметра H. Из рис. 7 следует, что скрытность такой системы передачи информации будет обеспечиваться визуальным сходством передаваемой реализации и ее фазового портрета с белым гауссовским шумом (рис. 5). Таким образом, опираясь на энергетические свойства сигнала, его визуальное, спектральное, корреляционное и динамическое сходство с белым шумом можно говорить о высокой скрытности передачи информации в радиосвязи.

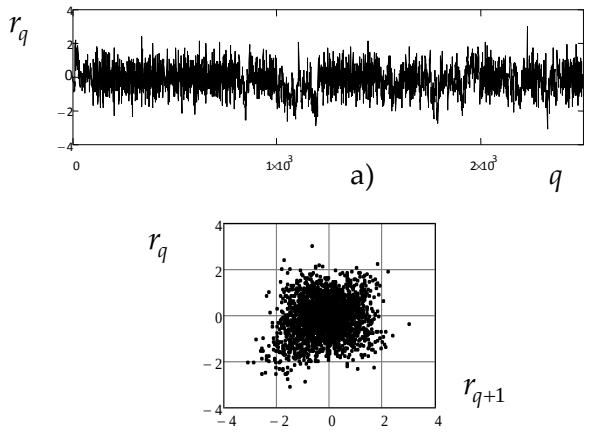


Рис. 7. Информационное сообщение, сформированное манипуляцией H (а), и его фазовый портрет (б)

На рис. 8 представлена синтезированная структурная схема системы радиосвязи для скрытной передачи бинарной информации, основанной на манипуляции «цветом» шума [9].

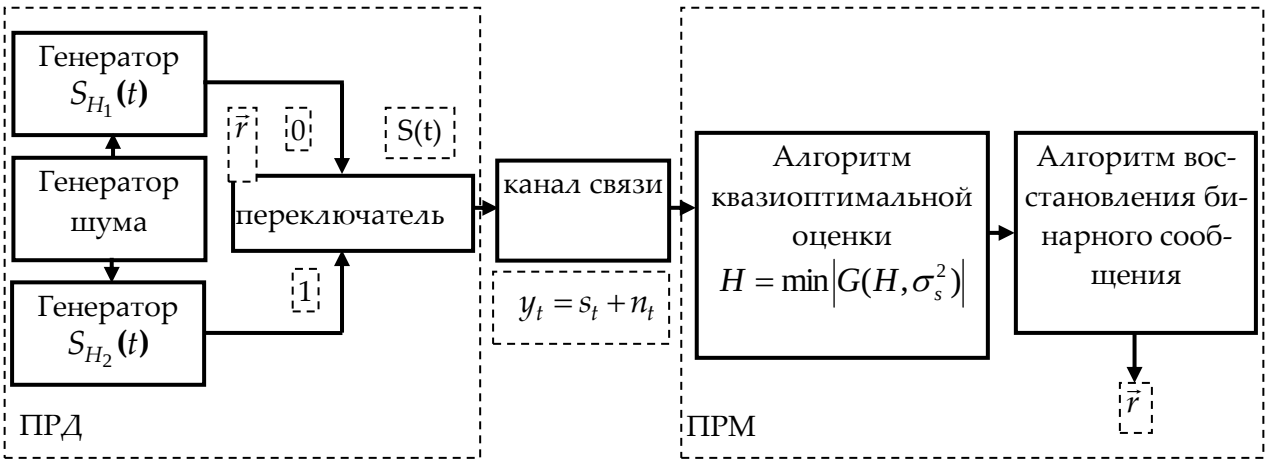


Рис. 8. Структурная схема системы радиосвязи для скрытной передачи бинарной информации, основанной на манипуляции «цвета» шума

На приемной стороне наблюдается аддитивная смесь $y_i = s_i + n_i$ фрактального шума s_i и белого гауссовского шума n_i с нулевым математическим ожиданием и дисперсией σ_n^2. В приемном устройстве по наблюдению $\{y_i\}_{i=0}^{t}$ восстанавливается сообщение $\vec{r} = (r_1,...,r_L)$ путем квазиоптимальной оценки параметра Херста $\hat{\hat{H}} = \mathbf{min}\left|G(H,\sigma_s^2)\right|$ фрактального шума на основе метода максимально правдоподобного оценивания.

В общем случае можно предполагать, что дисперсия шума наблюдения также неизвестна. Тогда требуется дать статистически оптимальные оценки параметров H и σ_n^2 по данным $y(t, \varepsilon, H)$, здесь ε - приращение текущего момента времени. Статистически квазиоптимальная оценка H определяется как минимальное значение функции максимального правдоподобия $G(H, \sigma_s^2)$ в плоскости (H, σ_s^2) на интервале времени T_{bit}. Таким образом, опираясь на визуальные, энергетические и корреляционные свойства фрактальных шумовых сигналов можно говорить о повышении их скрытности при передаче информации.

Как известно, несанкционированный наблюдатель рассматривает стеганосистему как источник информации. В процессе анализа он обращается к статистическим свойствам стеганоданных и пытается восстановить стеганоалгоритм (параметры данных). В идеальных стеганосистемах данные не отличаются от случайных последовательностей и не содержат никакой информации для несанкционированного наблюдателя. Соответственно, чем выше непредсказуемость (энтропия) системы, тем сложнее стороннему наблюдателю выявить стеганоалгоритм. Например, используя показатель экспоненты Ляпунова [11], можно получить первую количественную информацию о том, как быстро теряется способность предсказывать поведение системы с течением времени. Более точную оценку дает энтропия Колмогорова-Синая [2]. Согласно [12] энтропия равна нулю для регулярных систем (ФКМ-сигнал), положительна для хаотических последовательностей, бесконечна для случайных процессов (рис. 9).

Рис. 9. Шкала показателя непредсказуемости

Следовательно, в стеганографических системах радиосвязи, с точки зрения оценки энтропии, предпочтительнее использовать сложные хаотические и фрактальные шумовые сигналы.

Заключение

Таким образом, в работе изложены новые подходы для стеганографической передачи информации в системах радиосвязи за счет использования сложных шумо-

подобных сигналов в качестве стеганоконтейнера (несущей). Проведен сравнительный анализ известных сложных сигналов с позиции скрытой передачи информации. Показано, что для решения задачи скрытой передачи информации в канале связи нецелесообразно использовать гармонические несущие и хаотические сигналы с простым аттрактором, так как их аттракторы структурированы и легко классифицируется на фазовой плоскости. Для обеспечения скрытности функционирования систем радиосвязи целесообразно применять сложные хаотические сигналы и фрактальные шумы, которые при визуальном, спектральном, корреляционном и нелинейном анализах будут неотличимы от белого шума.

Список литературы:

1. *Конахович Г.Ф., Пузыренко А.Ю.* Компьютерная стеганография. Теория и практика. – К.: "МК-Пресс", 2006. – 288 с.

2. *Птицын Н.* Приложение теории детерминированного хаоса в криптографии. – М.: МГТУ им. Баумана, 2002. – 80с.

3. Основи комп'ютерної стеганографії: Навчальний посібник для студентів і аспірантів./ *В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук.* – Вінниця: ВДТУ, 2003. – 143 с.

4. *Грибунин В.Г., Оков В.Н., Туринцев И.В.* Цифровая стеганография. – М.: Солон-пресс, 2002. – 272 с.

5. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. Пер. с англ. – М: Издательский дом Вильямс, 2003. – 1104 с.

6. Использование BDS-статистики для оценки скрытности сигнала, полученного перемешиванием хаотической несущей / *П. Ю. Костенко, К. С. Васюта, А. Н. Барсуков [и др.]* // Известия вузов. Радиоэлектроника. — 2010. — № 5 (53). — С. 41—45.

7. *Васюта К.С.* Новый подход к оценке параметров хаотических сигналов, наблюдаемых на фоне шума, с использованием "нелинейной динамической статистики" [Электронный ресурс] // Проблеми телекомунікацій. – 2010. – № 1 (1). – С. 109 – 114. – Режим доступа к журн.: http://pt.journal.kh.ua/2010/1/1/101_vasyuta_chaotic.pdf.

8. *Васюта К.С.* Анализ эвристических моделей информационных систем на хаотической несущей // Радиотехника. – 2009. – Вып. 156. – С. 17– 22.

9. *Васюта К. С.* Метод передачи информации, основанный на манипуляции показателя Херста фрактального ("цветного") гауссовского шума // Системи обробки інформації. – 2010. — № 6(87). — С. 62—65.

10. *Федер Е.* Фракталы. – М: Мир, 1991. – 261 с.

11. *Синай Я.Г.* Современные проблемы эргодической теории. – М: ФИЗМАТЛИТ, 1995. – 208 с.

12. *Boffetta G., Cencini M., Falcioni M.* Predictability**:** A Way to Characterize Complexity // Physics Reports, 2002. – Vol. 356. – No. 6. – P. 367-474.