

УДК 621.391

К.С. Васюта, С.А. Щербинин

Харьковский университет Воздушных Сил им. Ивана Кожедуба, Харьков

СКРЫТАЯ ПЕРЕДАЧА ЦИФРОВОЙ ИНФОРМАЦИИ ПУТЕМ ВАРИАЦИИ ПАРАМЕТРОВ СЛУЧАЙНЫХ ПРОЦЕССОВ С УСТОЙЧИВЫМИ РАСПРЕДЕЛЕНИЯМИ

В работе исследована возможность применения случайных процессов с α -стабильными распределениями для скрытой передачи цифровой информации путем вариации свойств их распределений. Проведен анализ свойств таких процессов при изменении плотности распределения случайной величины в зависимости от вариации параметров распределения α и показателя сдвига закона распределения β . Показана малая чувствительность BDS статистики к обнаружению случайных процессов с одинаковым законом распределения случайной величины и разными параметрами сдвига.

Ключевые слова: скрытность, бинарное сообщение, хаотическая последовательность, α -стабильные распределения.

Введение

Использование случайных и хаотических сигналов для скрытой передачи цифровой (бинарной) информации является одним из перспективных направлений в современных средствах конфиденциальной связи [1], так как они позволяют передавать сигналы трудно отличимые от шума, как визуально, так и в рамках спектрального и корреляционного анализа, а также обладают свойствами широкополосных сигналов. В работах [2, 3] показано, что при обработке наблюдений в информационно-измерительных системах радио и оптического диапазонов длин волн оправдано использование моделей сигналов и шумов с мультифрактальной структурой в псевдофазовом пространстве. Эти модели описывают негауссовские случайные процессы и поля со статистически зависимыми значениями. Очевидно ожидать, что использование случайных процессов с усложненным видом аттрактора (фазового портрета) будет уменьшать степень их структурированности и увеличивать их скрытность при обнаружения и правильной классификации. Под скрытностью далее будем понимать способность системы передачи данных (связи) обеспечивать сохранение втайне от несанкционированного наблюдателя факт передачи информации [4].

В работе [5] показано, что, применяя манипуляции показателя Херста в ядре преобразования порождающих (исходных) процессов по закону бинарного сообщения, возможно, осуществлять скрытую передачу бинарной информации. Ниже в работе используя такой подход, предлагается новый метод скрытой передачи цифровой (бинарной) информации, основанный на манипуляции по закону бинарного сообщения параметров случайных процессов с α -стабильными распределениями.

Целью данной работы является анализ свойств α -стабильных распределений и их чувстви-

тельности к вариации параметров закона распределения, а также исследование возможности скрытой передачи цифровых сообщений путем применения α -стабильных распределений.

Результаты исследований

Для численного анализа альфа стабильных распределений в работе [6] предложен численный метод, который характеризует монофрактальные и мультифрактальные свойства линейно преобразованных случайных процессов. Однако в этой работе не дано практических рекомендаций использования случайных сигналов с мультифрактальной структурой аттракторов для скрытой передачи бинарных сообщений.

Трудность изучения свойств альфа стабильных распределений связана с отсутствием в общем случае аналитических выражений, описывающих плотности распределения. Такие выражения имеются лишь для следующих четырех параметров $\alpha, \beta, \gamma, \lambda$ - которыми однозначно можно задать устойчивые распределения [7]:

а) $\alpha = 2$, остальные параметры произвольные. Этот случай соответствует семейству нормальных распределений:

$$g(x, 2, \beta, \gamma, \lambda) = (4 \cdot \pi)^{-1/2} \cdot \exp\left\{-\frac{(x - \gamma)^2}{2\beta} \cdot \lambda\right\}.$$

б) $\alpha = 1$, $\beta = 0$, параметры γ и λ произвольны. Этот случай соответствует семейству распределений Коши:

$$g(x, 2, 0, \gamma, \lambda) = \frac{\lambda}{\pi} \left(\lambda^2 + (x - \gamma)^2 \right)^{-1}.$$

в) $\alpha = 1/2$, $\beta = 1$, параметры γ и λ произвольны. Соответствующее множество устойчивых законов называется распределение Леви, плотность которых имеет вид:

$$g\left(x, \frac{1}{2}, 1, \gamma, \lambda\right) = \begin{cases} \frac{\lambda}{2\sqrt{\pi}} x^{-\frac{3}{2}} \exp\left(-\frac{\lambda^2}{4(x-\gamma)}\right), & \text{если } x > \gamma \\ 0, & \text{если } x \leq \gamma \end{cases}$$

г) $\alpha = 1/2$, $\beta = -1$, параметры γ и λ произвольны. В этом случае плотности устойчивых законов имеют простую связь с плотностями распределений из семейства Леви:

$$g\left(x, \frac{1}{2}, -1, \gamma, \lambda\right) = g\left(-x, \frac{1}{2}, 1, -\gamma, \lambda\right)$$

На рис. 1 приведены графики плотности распределения случайной величины.

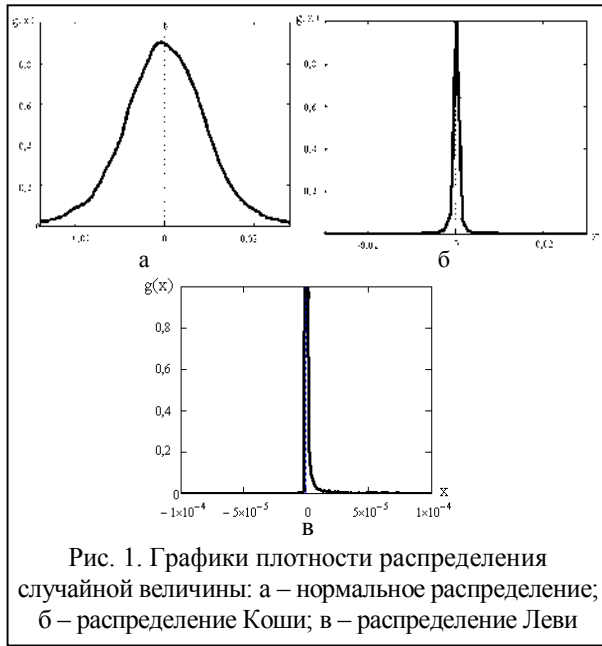


Рис. 1. Графики плотности распределения случайной величины: а – нормальное распределение; б – распределение Коши; в – распределение Леви

α -стабильное распределение описывает целый класс распределений, в который среди прочих входят и нормальный закон распределения и закон распределения Коши. Характеристическая функция процесса описывается следующим выражением [8]:

$$\Phi(t) = \begin{cases} e^{i\delta t - |\delta t|^\alpha (1 - i\beta \frac{t}{|t|} \operatorname{tg} \frac{\pi\alpha}{2})}, & \alpha \neq 1; \\ e^{i\delta t - |\delta t| (1 - i\beta \frac{2t}{\pi|t|} \ln|t|)}, & \alpha = 1, \end{cases}$$

где α -экспоненциальная характеристика стационарности ($0 < \alpha \leq 2$); β - коэффициент симметрии ($-1 \leq \beta \leq 1$), δ - параметр положения. При $\alpha = 2$ и $\beta = 0$ выражение описывает нормальный закон распределения, а при $\alpha = 1$ и $\beta = 0$ - распределение Коши. Для генерации случайных величин с α -стабильным распределением можно использовать выражение [8]:

для $\alpha \neq 1$:

$$\xi = S_{\alpha, \beta} \frac{\sin\{\alpha(V + B_{\alpha, \beta})\}}{\{\cos(V)\}^{1/\alpha}} \left[\frac{\cos\{V - \alpha(V + B_{\alpha, \beta})\}}{W} \right]^{1-\alpha}$$

где $S_{\alpha, \beta} = \left\{ 1 + \beta^2 \tan^2\left(\frac{\pi\alpha}{2}\right) \right\}^{1/(2\alpha)}$,

$$B_{\alpha, \beta} = \frac{\arctan\left(\beta \tan \frac{\pi\alpha}{2}\right)}{\alpha},$$

для $\alpha = 1$:

$$\xi = \frac{2}{\pi} \left\{ \left(\frac{\pi}{2} + \beta V \right) \tan V - \beta \ln \left(\frac{\frac{2}{\pi} W \cos V}{\frac{2}{\pi} + \beta V} \right) \right\},$$

где V - случайная величина, сформированная на интервале $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$, W - экспоненциальная случайная величина с единичной дисперсией. На рис. 2 приведена временная реализация порождающего случайного процесса Коши и соответствующий ей фазовый портрет.

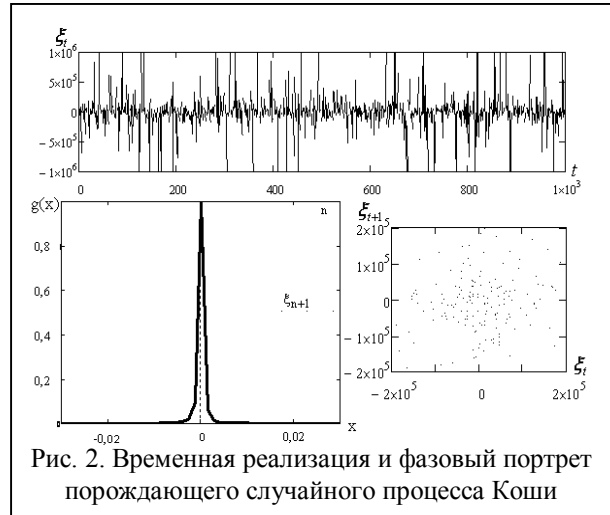


Рис. 2. Временная реализация и фазовый портрет порождающего случайного процесса Коши

Проанализируем свойство α -стабильных распределений используя BDS статистику. На рис. 3 представлен график зависимости среднего значения BDS статистики от изменения параметра α .

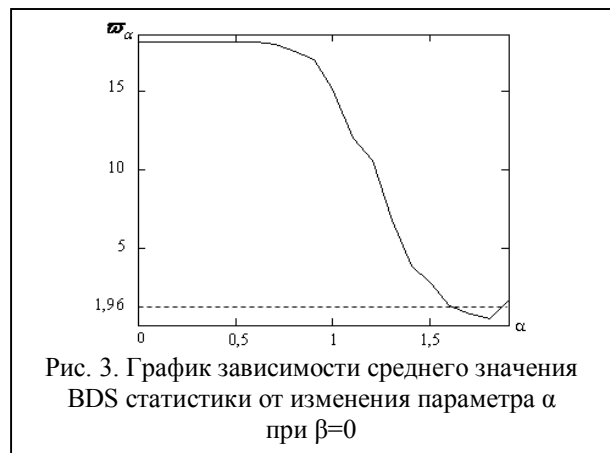


Рис. 3. График зависимости среднего значения BDS статистики от изменения параметра α при $\beta = 0$

Из рисунка видно, что значения BDS статистики на интервале $0 \leq \alpha < 1$ значительно не меняются, а на интервале $1 > \alpha \geq 2$ резко снижаются. Таким

образом, найбільш значимість для дальшого аналізу представляє інтервал $1 > \alpha \geq 2$, оскільки дає можливість в дальшому на основі BDS статистики здійснювати оцінку скритності пропонуваного методу передачі інформації.

На рис. 4 приведені графіки законів розподілення при різних значеннях параметра α .

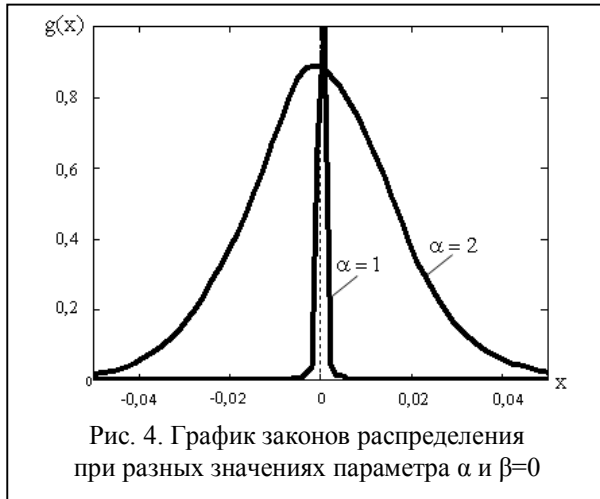


Рис. 4. Графік законів розподілення при різних значеннях параметра α і $\beta=0$

Из рисунка видно, что от величины параметра α существенно зависит закон распределения.

Поскольку параметр α описывает только симметричные относительно нулевого значения законы распределения то очевидным является необходимость исследовать поведения законов распределения случайной величины при разных значениях показателя сдвига β . При фиксированных значениях параметра α параметр β характеризует величину и направление асимметрии стандартного устойчивого закона.

На рис. 5 иллюстрируется, как влияет изменение значения параметра β на закон распределения случайного процесса.

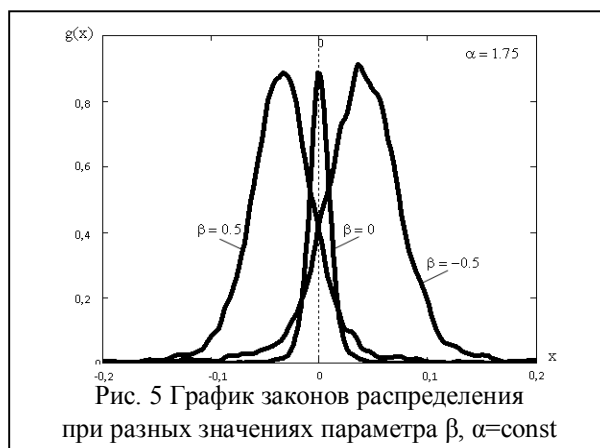


Рис. 5. Графік законів розподілення при різних значеннях параметра β , $\alpha=const$

Опираясь на результаты работы [9] проанализируем скрытность передачи цифровой информации через оценку среднего значения BDS статистики от изменения параметров α и β (рис. 6). Из рисунка видно, что значения BDS статистики при вариации показателем сдвига β изменяются не значительно.

А при вариациях значений параметра α меняется существенно. Это говорит о том, что для передачи бинарных сообщений целесообразней использовать манипуляцию параметра β .

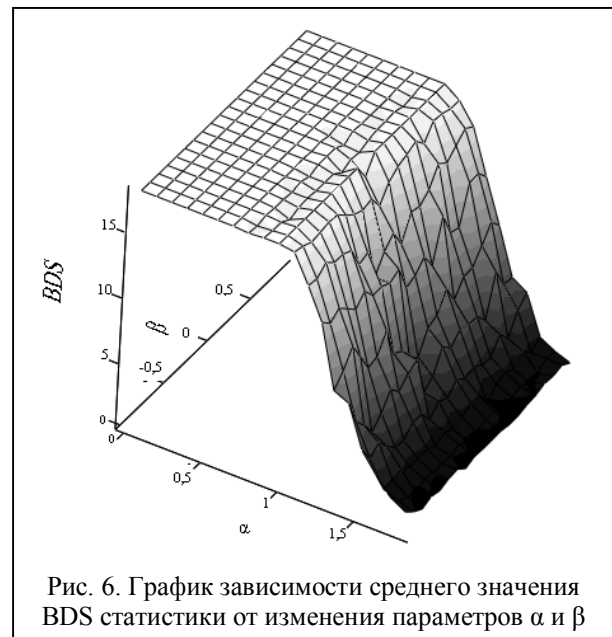


Рис. 6. Графік залежності середнього значення BDS статистики від змін параметрів α і β

На рис. 7 приведен метод скритої передачі бинарного повідомлення шляхом маніпуляції параметра α .

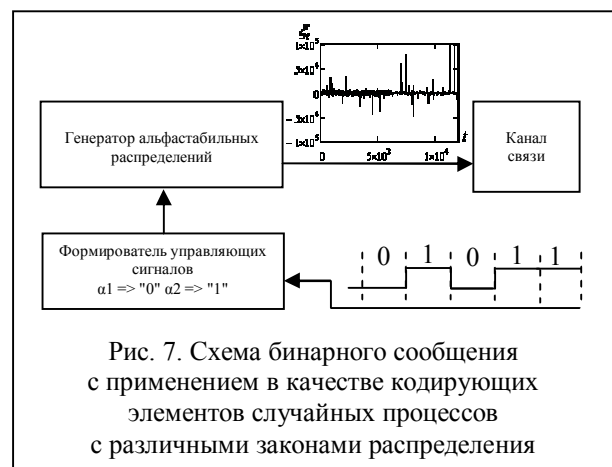


Рис. 7. Схема бінарної передачі з використанням елементів випадкових процесів з різними законами розподілення

На рис.8 приведені закони розподілення, часові діаграми та фазові портрети відповідні "0" (рис.8, а), передачі "1" (рис.8, б) та інформаційному повідомленню на виході передатчика (рис.8, в). Из рис.8 видно, что сигнал на выходе имеет сложную шумоподобную форму во времени, а так же закон распределения и фазовый портрет близкий к нормальному белому шуму. Увеличение разрядов бинарного сообщения в соответствии с центральной предельной теоремой приводит вид распределения случайной величины выходного сигнала к нормальному закону распределения, вследствие чего, сигнал на выходе, будет восприниматься несанкционированным наблюдателем как шум наблюдения. Это в

сою очередь значительно увеличивает скрытность факта передачи цифрового сообщения.

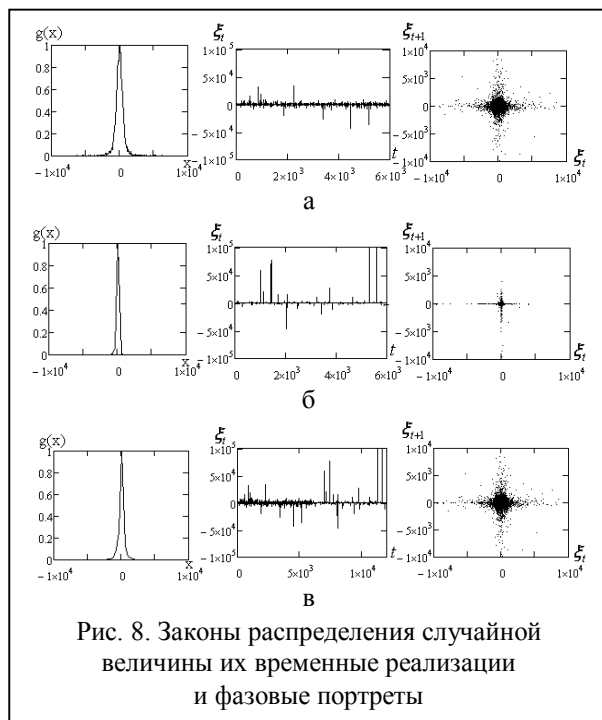


Рис. 8. Законы распределения случайной величины их временные реализации и фазовые портреты

Выводы

Таким образом, для повышения скрытности передачи цифровой информации возможно использование моделей случайных мульти и моно фрактальных процессов. Такие процессы могут быть сформированы путем манипуляции параметров законов распределения.

Вариация показателя сдвига β позволяет расширить возможности скрытой передачи цифровых сообщений.

В дальнейших работах авторами будет изложен алгоритм восстановления цифровых сообщений.

Список литературы

1. Парфенов В.И. Анализ систем передачи информации, основанной на манипуляции статистическими характеристиками случайного процесса / В.И. Парфенов, Е.В. Сергеева. – Киев.: Изв. Вузов. Радиоэлектроника – 2010. – Т. 53, № 3. – С. 42-49.
2. Марков Е.П. Фрактальная модель космических оптико-электронных изображений / Е.П. Марков // Исследование земли из космоса. – 1996. – № 1. – С. 56-61.
3. Stephen M. Signal Modeling with Self-similar α -Stable Processes: The Fractional Levy Stable Motion Model / Stephen M., Kogon and Dimitris, G.Manolakis // IEEE TRANSACTIONS ON SIGNAL PROCESSING.- VOL. 44.- №4.- APRIL 1996. – P. 1006-1010.
4. ГОСТ В 23609-86 (СТ А СЭВ 0217-86). 1986.
5. Парфенов В.И. Исследование системы передачи информации, основанной на манипуляции параметром Херста (метод Хигучи) стохастического процесс / В.И. Парфенов, Е.В. Сергеева, А.В. Новиков // Теория и техника радиосвязи. – 2009. – С. 5-12.
6. Васюта К.С. Анализ свойств α -стабильных (мультифрактальных) процессов в псевдофазовом пространстве с использованием BDS статистики / К.С. Васюта // Всеукр. межвед. науч.-техн. сб. – 2010. – Вып. 160. – С. 132-136.
7. Золотарев В.М. Математика, кибернетика. Устойчивые законы и их применение / В.М. Золотарев. – М: Знание, 1984. – С. 30-35.
8. Szymon Borak, Wolfgang Hardle, Rafal Weron. Stable Distributions. // SFB 649 Discussion Paper 2005-008. – P.28.
9. 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.

Поступила в редколлегию 6.12.2012

Рецензент: д-р техн. наук, проф. А.В. Лемешко, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ПРИХОВАНА ПЕРЕДАЧА ЦИФРОВОЇ ІНФОРМАЦІЇ ЗА РАХУНОК ВАРІАЦІЇ ПАРАМЕТРІВ ВИПАДКОВИХ ПРОЦЕСІВ ІЗ СТІЙКИМИ РОЗПОДІЛАМИ

К.С. Васюта, С.О. Щербінін

У роботі досліджено можливість застосування випадкових процесів з α -стабільними розподілами для прихованої передачі цифрової інформації за рахунок варіації властивостей їх розподілів. Проведено аналіз властивостей таких процесів при зміні щільності розподілу випадкової величини в залежності від варіації параметрів розподілу α та показника зсуву закону розподілу β . Показано малу чутливість BDS статистики до виявлення випадкових процесів з однако- вим законом розподілу випадкової величини та різними параметрами зсуву.

Ключові слова: прихованість, бінарне повідомлення, хаотична послідовність, α -стабільні розподіли.

HIDDEN TRANSMISSION OF DIGITAL INFORMATION BY THE VARIATION OF PARAMETERS OF RANDOM PROCESSES WITH STABLE DISTRIBUTIONS

K.S. Vasyuta, S.A. Shcherbinin

Possibility of using random processes with α -stable distributions for the hidden transmission of digital information by the variation of their distributions properties is researched in this paper. The properties of such processes with the change of density of random quantity distribution depending on variation of distribution parameters α and shear index of distribution law β are analyzed. Weak sensitivity of BDS statistics for random processes with identical distribution law of random quantity and different shear parameters is shown.

Keywords: security, binary message, chaotic sequence, α -stable distributions.