УДК 621.391

К.С. Васюта

Харьковский университет Воздушных Сил им. Ивана Кожедуба, Харьков

МЕТОД ПЕРЕДАЧИ ИНФОРМАЦИИ, ОСНОВАННЫЙ НА МАНИПУЛЯЦИИ ПОКАЗАТЕЛЯ ХЕРСТА ФРАКТАЛЬНОГО (“ЦВЕТНОГО”) ГАУССОВСКОГО ШУМА

Предложена и исследована перспективная система скрытой передачи информации в цифровых широкополосных каналах связи, основанная на манипуляции “цвета шума” случайного процесса. Приведены алгоритм внесения бинарного сообщения в линейно преобразованную случайную последовательность с ядром Мандельброта и алгоритм восстановления бинарного сообщения. Анализируются ошибки восстановления бинарного сообщения, обусловленные его длительностью и отношением сигнал/шум.

Ключевые слова: *скрытность, фрактальный шум, бинарное сообщение, показатель Херста, преобразование Мандельброта, ошибки восстановления, шум наблюдения.*

Введение

Использование случайных и хаотических сигналов для скрытной передачи информации является одним из перспективных направлений в современных средствах конфиденциальной связи [1], так как они обеспечивает работу системы связи «под шум». По сравнению с традиционными (шумоподобными) сигналами хаотические сигналы обладают рядом преимуществ [2].

Однако, как выяснилось, в последнее время и этот класс сигналов не удовлетворяет требованиям скрытности в полной мере, так как их аттракторы структурированы достаточно просто и легко отличимы от аттракторов случайных процессов с независимыми и одинаково распределенными значениями. В то же время свойства некоторых случайных процессов с зависимыми значениями оказываются весьма чувствительными к вариациям их параметров. Заметим, что в результате манипуляции их характеристик (параметров) при несанкционированном доступе к информации у наблюдаемого процесса сохраняется вид однородного широкополосного шума.

Например, изменение показателя Херста фрактального гауссовского шума влияет на его "цвет" [3]. Очевидно, что это свойство может быть использовано для скрытной передачи бинарных сообщений.

Под скрытностью далее будем понимать способность системы связи обеспечивать сохранение в тайне от несанкционированного потребителя факт передачи информации [4].

Целью данной работы является анализ возможности скрытной передачи бинарного сообщения с использованием фрактального ("цветного") шума, полученного линейным преобразованием белого гауссовского шума $\xi(t)$ с нулевым математическим ожиданием и единичной дисперсией, заданным ядром Мандельброта. Параметр ядра H – показатель Херста – манипулируется бинарным сообщением. По наблюдению цветного шума на фоне белого гауссовского шума необходимо восстановить моменты изменения параметра H и его значения, что будет соответствовать последовательности элементов бинарного сообщения.

Результаты исследований

При моделировании фрактального шума используем приближенное выражение, которое в дискретные моменты времени t имеет вид: [5]:

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

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

На рис. 2, 3 показано влияние параметра H на цвет шума и его характер. При $H = 0,1$ имеем "розовый" шум и антиперсистентный характер фрактального шума, а при $H = 0,9$ получаем "черный" шум и персистентный его характер.

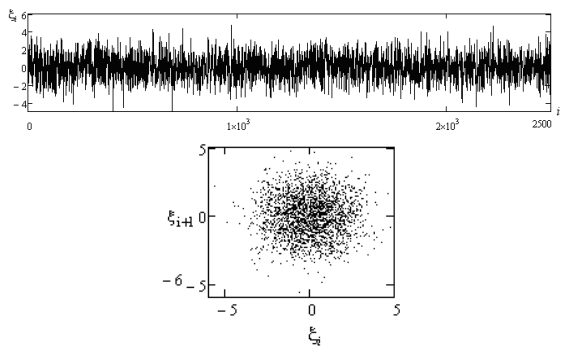

Рис. 1. Белый гауссовский шум ($H = 0,5$) и его фазовый портрет

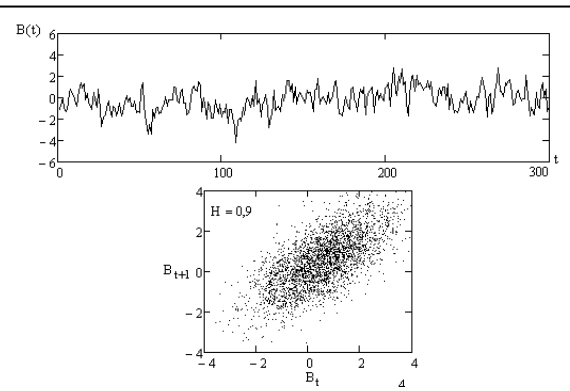

Рис. 2. Персистентный процесс (черный шум – $H = 0,9$) и его фазовый портрет

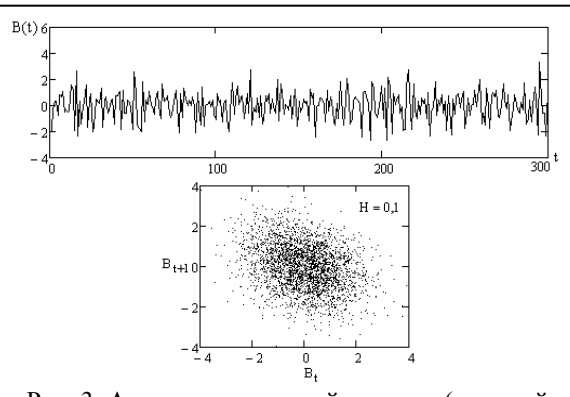

Рис. 3. Антиперсистентный процесс (розовый шум – $H = 0,1$) и его фазовый портрет

Для примера 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. 4).

На рис. 5 приведена реализация информационной последовательности $S_i\ {}_{i=0}^{t}$, полученной в результате манипуляции параметра H. Для передачи

одного элемента (бита) сообщения r_q использовано $T_{bit} = 100$ отсчетов несущей последовательности $S_i \Big|_{i=0}^{t}$ ($r_q = 0 \to 100$ значений $S(t;0,1;n)$, $r_q = 1 \to$ 100 значений $S(t;0,9;n)$).

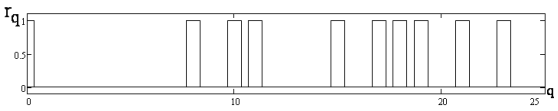

Рис. 4. Бинарное сообщение $\vec{r}$

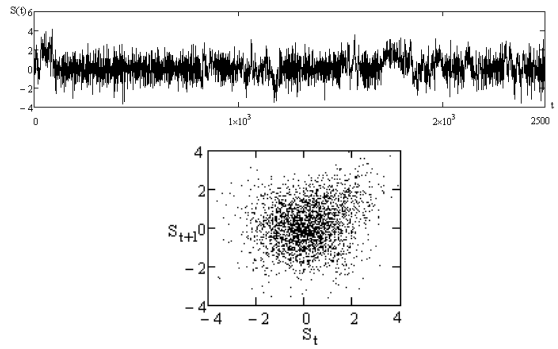

Рис. 5. Информационная последовательность, сформированная манипуляцией H, и ее фазовый портрет

Из рис. 5 видно, что скрытность такой системы передачи информации будет обеспечиваться визуальным сходством передаваемой реализации и ее фазового портрета с белым гауссовским шумом (рис. 1).

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. Необходимо по наблюдению $y_i \Big|_{i=0}^{t}$ восстановить сообщение $\vec{r} = (r_1, ..., r_L)$.

Поскольку в качестве порождающего использован случайный процесс, то на приемной стороне невозможно сформировать реализацию ожидаемого сигнала (фрактального шума). В этом случае для восстановления элемента бинарного сообщения выполним оценку параметра Херста фрактального шума, используя для этого метод максимального правдоподобия. 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.

Воспользуемся спектральным представлением логарифма функции максимального правдоподобия, которое в предположении, что размер мелких деталей спектра мощности процесса $y(t, \varepsilon, H)$ гораздо меньше характерного масштаба его изменения, имеет вид [6]:

$$G(H, \sigma_s^2) = \ln p(\tilde{y}(\omega) \mid H, \sigma_s^2) =$$

$$= -T \frac{1}{2\pi} \int_{-\infty}^{\infty} \left[\frac{|\tilde{y}(\omega)|^2}{\tilde{R}_y(\omega, H, \sigma_s^2)} + \ln \tilde{R}_y(\omega, H, \sigma_s^2) \right] d\omega, \quad (2)$$

где

$$R_y(\tau, \varepsilon) = \frac{\sigma_s^2 \varepsilon^{2H-2}}{2} \left(\left(\frac{\tau}{\varepsilon} + 1 \right)^{2H} + \left(\frac{\tau}{\varepsilon} - 1 \right)^{2H} - 2 \left(\frac{\tau}{\varepsilon} \right)^{2H} \right) +$$

$+\sigma_n^2 R_n(\tau)$ – автокорреляционная функция приращения наблюдения.

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}. Вид этой функции в случае, когда оценка $\hat{\sigma}_n^2$ получена по 256-ти значениям спектра наблюдаемого сигнала и отношении сигнал/шум $q = \sigma_s^2 / \sigma_n^2 = 5$ показан на рис. 6. Функция имеет минимальное значение при $\hat{H} = 0.91$, которое принимается за максимально правдоподобную оценку истинного значения параметра равного $H = 0,0$. Функция $G(H, \hat{\sigma}_s^2)$ строилась с шагом дискретизации $\Delta H = 0,01$ и $\varepsilon = 1$.

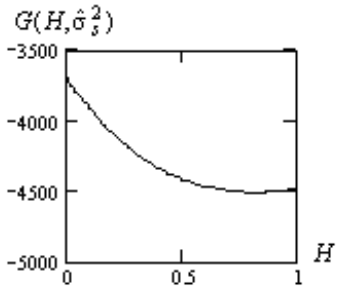

Рис. 6. Функции максимального правдоподобия $G(H, \sigma_s^2)$

Оценка элемента сообщения сводится к оценке значения H на интервале T_{bit} и проверке гипотезы о наличии или отсутствии в восстановленном сообщении $\hat{\vec{r}}$ на заданном интервале символа “0” или “1”, а качество оценки определяется значением вероятности правильного принятия решения. На рис. 7 представлено восстановленное бинарное сообщение с тремя ошибками при отношении сигнал/шум на входе приемника $q = \sigma_S^2 / \sigma_n^2 = 10$. На рис. 8 представлены зависимости вероятности правильной оценки $P_{\vec{r}}(L,q) = 1 - P_{err.\vec{r}}(L,q)$ от количества элементов L бинарного сообщения и отношения сигнал/шум на входе приемника $q = \sigma_S^2 / \sigma_n^2$.

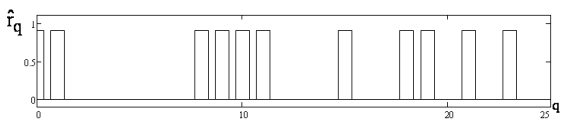

Рис. 7. Восстановленное бинарное сообщение $\hat{\vec{r}}$

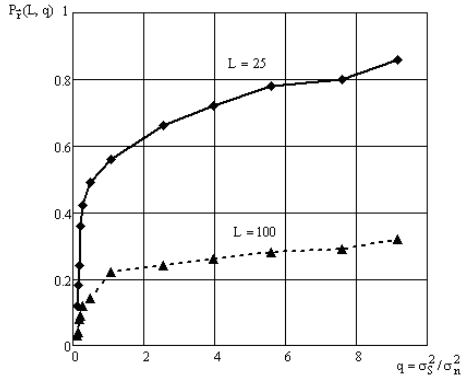

Рис. 8. Зависимости вероятности правильной оценки от количества элементов L бинарного сообщения и отношения сигнал/шум на входе приемника

Величина $P_{err.\vec{r}} = d_H(\vec{r}, \hat{\vec{r}}) / L$ определяет долю ошибок в оценках элементов сообщения и равна отношению расстояния Хемминга $d_H(\vec{r}, \hat{\vec{r}})$ между передаваемой бинарной последовательностью $\vec{r}$ и еѐ оценкой $\hat{\vec{r}}$ к общему числу L ее элементов. Количество символов в бинарном сообщении фиксировано и принималось при моделировании равным $L = 25$ $L = 100$, а длина выборки t (наблюдения) принималась равно $t = 2{,}5 \cdot 10^3$ и $t = 10^4$.

Из рис. 8 видно, что рост числа элементов сообщения порождает большее количество ошибок восстановления при фиксировано выборке. Предложенный метод требует для обеспечения заданного качества восстановления $P_{\vec{r}} \geq 0{,}95$ отношения сигнал/шум на входе приемника $q \geq 10$.

Выводы

Таким образом, опираясь на визуальные, энергетические и корреляционные свойства фрактальных шумовых сигналов можно надеяться на повышение их скрытности при передаче информации основанной на манипуляции параметра Херста. Для обеспечения высокого качества восстановления ($P_{\vec{r}} \geq 0{,}95$) сообщения по наблюдению требуются отношения сигнал/шум на входе приемника $q > 10$.

Список литературы

1. Парфенов В.И. Анализ систем передачи информации, основанной на манипуляции статистическими характеристиками случайного процесса / В.И. Парфенов, Е.В. Сергеева. – К.: Изв. Вузов. Радиоэлектроника. – 2010. – Т.53, №3. – С. 42-49.

2. Дмитриев А.С. Динамический хаос: новые носители информации для систем связи / А.С. Дмитриев, А.И. Панас. – М.: Физматлит, 2002. – 252 с.

3. Васюта К.С. Анализ эвристических моделей информационных систем на хаотической несущей / К.С. Васюта // Радиотехника: межвед. научно-техн. сборник. – Х., 2009. – № 156. – С. 17-22.

4. ГОСТ В 23609-86 (СТ А СЭВ 0217-86). 1986.

5. Федер Е. Фракталы / Е. Федер. – М.: Мир, 1991. – 261 с.

6. Васюта К.С. Эффективность статистически оптимальной оценки показателя Херста обобщенного фрактального гауссовского процесса, искаженного белым шумом / К.С. Васюта, А.В. Шаповалов, В.И. Сторожев. – К.: НТУ «КПИ». – 2010. – № 7(53). – С. 1-6.

Поступила в редколлегию 14.07.2010

Рецензент: д-р техн. наук, доцент А.В. Потий, Харьковский университет Воздушных Сил им. Ивана Кожедуба, Харьков.

МЕТОД ПЕРЕДАЧІ ІНФОРМАЦІЇ, ЯКИЙ ЗАСНОВАНО НА МАНІПУЛЯЦІЇ ПОКАЗНИКА ХЕРСТА ФРАКТАЛЬНОГО (“КОЛЬОРОВОГО”) ГАУССОВСЬКОГО ШУМУ

К.С. Васюта

Запропоновано і досліджено перспективну систему прихованої передачі інформації в цифрових широкосмугових каналах зв'язку, засновану на маніпуляції “кольору шуму” випадкового процесу. Приведено алгоритм внесення бінарного повідомлення в лінійно перетворену випадкову послідовність з ядром Мандельброта і алгоритм відновлення бінарного повідомлення. Аналізуються помилки відновлення бінарного повідомлення, що обумовлені його тривалістю і відношенням сигнал/шум.

Ключові слова: *скритність, фрактальний шум, бінарне повідомлення, показник Херста, перетворення Мандельброта, помилки відновлення, шум спостереження.*

METHOD OF INFORMATION TRANSFER, BASED ON MANIPULATION OF INDEX OF HEARST FRACTAL (“COLORED”) GAUSSIAN NOISE

K.S. Vasyuta

Offered and investigational the perspective system of the hidden information transfer in the digital ducting of connection, based on manipulation of “color of noise” of casual process. Resulted algorithm of bringing of binary report in an arc wise regenerate casual sequence with the kernel of Mandelbrot and algorithm of renewal of binary report. The errors of renewal of binary report, conditioned by his duration and relation signal-to-noise, are analyses.

Keywords: *secrecy, fractal noise, binary report, index of Hearst, transformation of Mandelbrot, errors of renewal, noise of supervision.*