УДК 621.391

К.С. Васюта, С.А. Щербинин

Харьковский университет Воздушных Сил имени Ивана Кожедуба, Харьков

МЕТОД СКРЫТОЙ ПЕРЕДАЧИ БИНАРНОЙ ИНФОРМАЦИИ НА ОСНОВЕ ПРИМЕНЕНИЯ ЛИНЕЙНОПРЕОБРАЗОВАННОГО СТОХАСТИЧЕСКОГО ПРОЦЕССА "СКОЛЬЗЯЩЕГО СРЕДНЕГО"

В работе проанализировано возможность использования линейнопреобразованного стохастического процесса "модели скользящего среднего" для повышения скрытности передачи бинарной информации. Предложен метод оценки показателей модели, а так же приведен график зависимости вероятности правильной оценки бита информации от отношения сигнал/шум на входе приемника.

Ключевые слова: *скользящее среднее, коэффициент автокорреляции, скрытность.*

Введение

Для увеличения помехоустойчивости, скрытности и защиты от несанкционированного доступа в последнее время все большее количество ученых обращает свои взгляды к сигналам на стохастической основе. Достоинством данного вида сигналов является их широкополосность, что в свою очередь характеризует их высокую помехозащищенность, адаптивность к реальной эфирной обстановке, низкий уровень мощности "шумоподности" сигнала, экономное использование частотного ресурса, сложности перехвата и постановки прицельных помех.

В стохастических системах связи информация кодируется посредством временной позиционно-импульсной модуляции, т.е. "импульсное радио". Один информационный бит кодируется последовательностью многих импульсов. Время смещения не превышает четверти длительности импульса [1].

Недавно было предложено передавать бинарную информацию путем манипуляции показателя Херста фрактального "цветного" Гауссовского шума [2]. Однако данный вид передачи информации имеет ряд недостатков, к которым можно отнести вычислительную сложность и малый диапазон изменений аттракторов фазового портрета при постоянном законе распределения порождающего процесса. Для устранения данных недостатков, авторами предложен более простой метод передачи информации, за счет манипуляции параметрами модели скользящего среднего. Данная модель обладает малой вычислительной сложностью, а так же большим количеством видов аттракторов фазового портрета при изменении ее параметров.

Целью работы является анализ свойств стохастического процесса на основе модели скользящего среднего, а также формирование метода повышения скрытности и помехоустойчивости передачи бинарной информации за счет манипуляции параметрами модели скользящего среднего.

Изложение основного материала

Для моделирования финансовых временных рядов, которые зачастую имеют случайный характер, уже давно применяются несколько типов линейнопреобразованных моделей стохастического процессов с кратковременной памятью [3]:

1. Авторегрессионный процесс (AR).
2. Процесс скользящего среднего (MA).
3. Авторегрессионный процесс скользящего среднего (ARMA).

Каждый из этих процессов имеет ряд улучшенных вариантов. Однако для простоты в данной статье мы рассмотрим только процесс скользящего среднего (Moving Average). Модель скользящего среднего q - порядка записывается как MA(q) и имеет вид:

$$X_t = \sum_{j=1}^{q} b_j \xi_{t-j}, \qquad (1)$$

где ξ_t – белый гауссовский шум с нулевым математическим ожиданием и единичной дисперсией, b_j – параметр модели.

Также в модель иногда добавляют константу a. Однако для того, что бы упростить дальнейшие вычисления поставим условие, что константа $a = 0$, а в процессе моделирования будем использовать процесс скользящего среднего первого порядка MA(1) который имеет следующий вид:

$$X_t = \xi_t - b\xi_{t-1}.$$

Временная реализация, фазовый портрет и частотный спектр порождающего процесса ξ_t (белый шум с нулевым математическим ожиданием и единичной дисперсией) представлен на рис. 1.

Для анализа свойств MA было проведено моделирование с разными значениями параметра модели (рис. 2). Из рисунка видно, что при смени знака параметра процесс скользящего среднего меняет характер своего поведения в фазовой плоскости с персистентного на антиперсистентный.

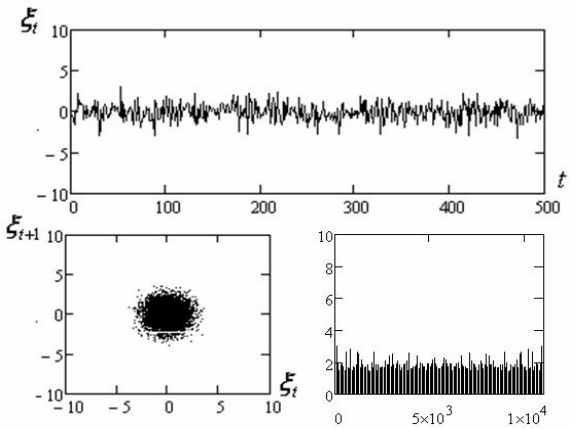
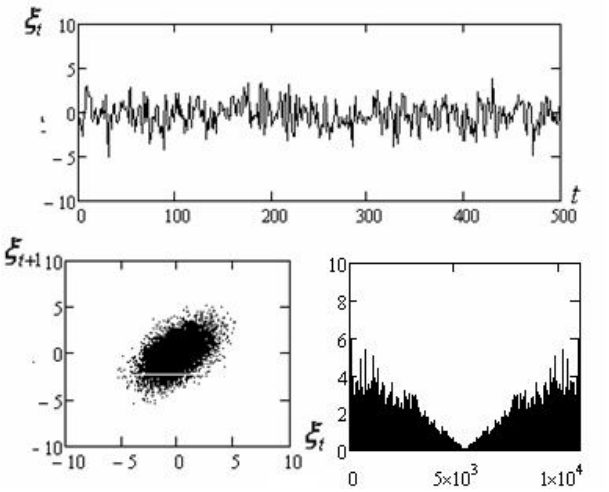
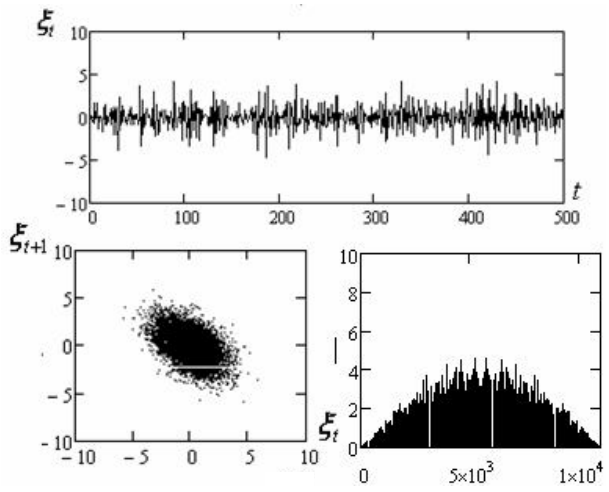


Рис. 1. Временная реализация, фазовый портрет и частотный спектр порождающего процесса



а



б

Рис. 2. Временная реализация, фазовый портрет и спектр процесса а) при b=-1 б) при b=1

Проведя внесение бинарной последовательности (рис. 3) методом, предложенным в [2]. Получаем временную реализацию и фазовый портрет, представленный на рис. 4.

Из рисунка видно, что скрытность такой системы передачи информации будет обеспечиваться визуальным сходством передаваемой реализации и ее фазового портрета с белым Гауссовским шумом, а так же будет не различима в частотной области (рис. 1).

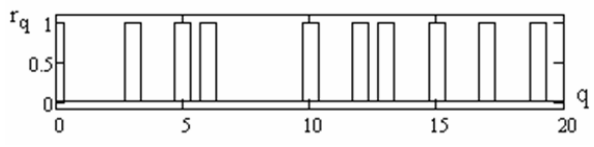


Рис. 3. Бинарное сообщение

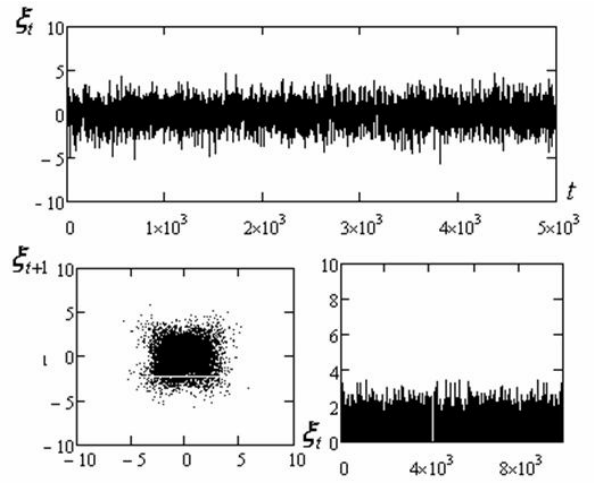


Рис. 4. Временная реализация, фазовый портрет и частотный спектр сигнала на входе приемника

Декодирование принятой информации.

Важной задачей является правильное восстановление передаваемой информации.

Для решения этой задачи мы воспользуемся оценкой параметра МА [4].

В соответствии с определением белого шума ошибка ξ_t характеризуется следующими свойствами:

$$M[\xi_t] = 0,\ D(\xi_t) = \sigma_\xi^2 = \text{const};$$

$$\gamma_j = M[\xi_t, \xi_{t-1}] = \begin{cases} \sigma_\xi^2, & j = 0 \\ 0, & j \neq 0 \end{cases}. \qquad (2)$$

Вследствие этого и автокорреляционная функция белого шума имеет очень простую форму

$$\rho_j^{(\xi)} = 1,\ j = 0;\ \rho_j^{(\xi)} = 0,\ j \neq 0. \qquad (3)$$

С учетом свойств ошибки ξ_t несложно построить автокорреляционную функцию модели MA(q), определяемой выражением (1). Ее коэффициент ковариации j-го порядка определяется следующим образом:

$$\gamma_j = M\left[\left(\xi_t - b_1\xi_{t-1...} - b_q\xi_{t-q}\right)\times \right.$$
$$\left.\times\left(\xi_{t-j} - b_1\xi_{t-1-j...} - b_q\xi_{t-q-j}\right)\right]. \qquad (4)$$

При j=0 выражение (4) представляет собой дисперсию процесса X_t, которая в силу свойства (2) выражается через коэффициенты модели MA(q) b_j, $j = 1, 2, \ldots, q$ и дисперсию ошибки σ_ξ^2 следующим образом:

$$\gamma_0 = \sigma_\gamma^2 = \left(1 + b_1^2 + \ldots + b_q^2\right)\sigma_\xi^2. \qquad (5)$$

Для $j = 1$ из (5) получим, что первый коэффициент ковариации определяется выражением

$$\gamma = \left(-b_1 + b_1 b_2 + \ldots + b_{q-1} b_q\right)\sigma_\xi^2.$$

Для произвольного j имеем

$$\gamma_j = \begin{cases} \left(-b_1 + b_1 b_2 + \ldots + b_{q-1} b_q\right)\sigma_\xi^2, \; j = 1,2,\ldots q; \\ 0, \qquad j > q. \end{cases} \qquad (6)$$

Из соотношения (6) вытекает, что автокорреляционная функция модели MA(q) стремится к нулю после задержки на q.

С учетом выражений (5) и (6) несложно также заметить, что коэффициенты автокорреляции модели скользящего среднего q-го порядка определяются через ее параметры b_j, $j = 1,2,\ldots,q$ таким образом:

$$\rho_j = \begin{cases} \dfrac{-b_j + b_1 b_{j+1} + \ldots + b_{q-j} b_q}{1 + b_1^2 + \ldots b_q^2}, j = 1,2,\ldots,q; \\ 0, \qquad j > q. \end{cases} \qquad (7)$$

Система из q уравнений (7), сформированных для $j = 1,2,\ldots,q$ служить основой для получения оценок $b1, b2, \ldots, b_q$ неизвестных параметров модели MA(q).

Однако в отличие от уравнений Юла-Уокера эта система нелинейная и ее решение требует использования специальных итеративных процедур. Однако с учетом принятого нами условия, что в процессе моделирования мы имеем дело только с MA(1).

Из (5) следует, что дисперсии процесса σ_X^2 и ошибки этой модели σ_ξ^2 связаны следующим соотношением:

$$\sigma_X^2 = \left(1 + b_1^2\right)\sigma_\xi^2,$$

а ее единственный отличный от нуля первый коэффициент автокорреляции выражается через коэффициент модели как

$$\rho_1 = -\frac{b_1}{1 + b_1^2}. \qquad (8)$$

Из соотношения (1.8) несложно получаем квадратическое уравнение относительно оценки b_1 неизвестного параметра

$$b_1^2 + \frac{b_1}{r_1} + 1 = 0, \qquad (9)$$

где r_1 – оценка коэффициента автокорреляции первого порядка процесса X_t, то есть ρ_1.

В свою очередь, из (9) следует, что существуют два решения этого уравнения, связанные между собой следующим соотношением:

$$b_{1,1} \cdot b_{1,2} = 1, b_{1,1} = \frac{1}{b_{1,2}}.$$

Условию стационарности процесса X_t удовлетворяет только решение b по абсолютной величине меньшее единицы. Оно может быть получено из следующего выражения:

$$b_1 = \frac{\frac{-1}{r_1} \pm \sqrt{\left(\frac{1}{r_1}\right)^2 - 4}}{2}, \qquad (10)$$

при условии, что

$$\left(\frac{1}{r_1}\right)^2 - 4 \geq 0 \Rightarrow |r_1| \leq 0,5. \qquad (11)$$

Из (11) следует, что модели скользящего среднего первого порядка могут применяться только для описания процессов с автокорреляционной функцией, обрывающейся после первой задержки и коэффициентом автокорреляции по абсолютной величине не превышающим $0,5$.

В полученном уравнении (10) иметься только одна неизвестная это коэффициента автокорреляции. Для ее вычисления воспользуемся формулой для вычисления коэффициента автокорреляции первого порядка.

$$r_1 = \frac{\sum_{t-2}^{n}\left(X_t - \overline{X}_1\right)\left(X_{t-1} - \overline{X}_2\right)}{\sqrt{\sum_{t=2}^{n}\left(X_t - \overline{X}_1\right)^2 \sum_{t=2}^{n}\left(X_{t-1} - \overline{X}_2\right)^2}},$$

где $\overline{X}_1 = \dfrac{\sum_{t=2}^{n} X_t}{n-1}$, $\overline{X}_2 = \dfrac{\sum_{t=2}^{n} X_{t-1}}{n-1}$.

Используя выше изложенный математический аппарат для оценки параметра модели скользящего среднего при разных значениях сигнал/шум на входе приемника.

Был построен график зависимости вероятности правильной оценки $P_{\vec{r}}(L,q) = 1 - P_{\text{ерг.}\vec{r}}(L,q)$ сообщения $\vec{r}$ от количества элементов L бинарного сообщения и отношения сигнал/шум на входе приемника $q = \sigma_S^2 / \sigma_n^2$, рис. 5.

Величина $P_{\text{ерг.}\vec{r}} = d_H(\vec{r}, \hat{\vec{r}})/Q$ 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 её оценкой $\hat{\vec{r}}$ к общему числу L ее элементов (рис. 5). Из графика видно, что данный вид внесения бинарной информации дает возможность обеспечить заданное качество восстановления $P_{\vec{r}} \geq 0,95$ при отношении сигнал/шум на входе приемника $q \geq 0.13$.

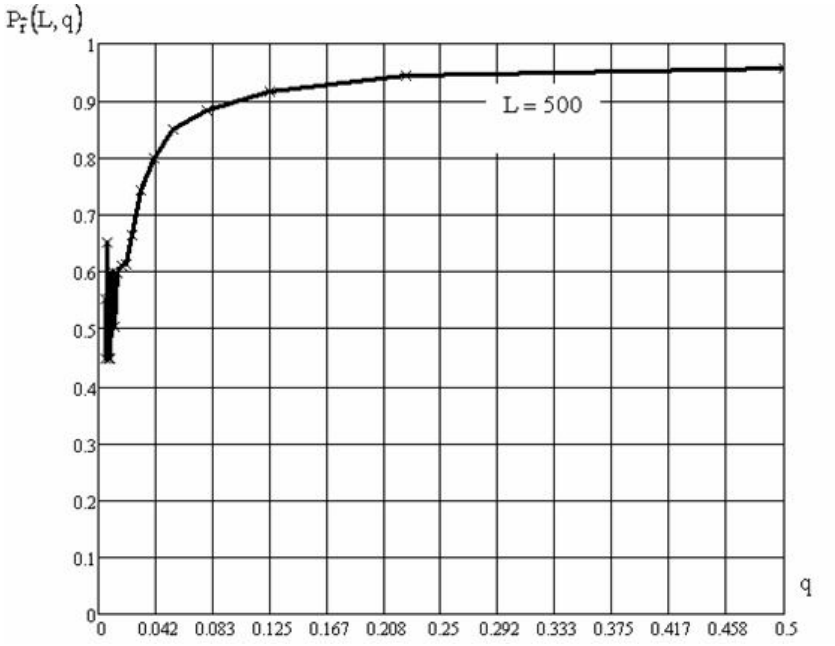


Рис. 5. Зависимости вероятности правильной оценки от отношения сигнал/шум на входе приемника

Выводы

Таким образом, для повышения скрытности передачи информации предложен новый метод внесения информации, который обеспечивают форму аттрактора информационного сообщения схожую с аттрактором бело шума, чем повышается стойкость информации к перехвату несанкционированным пользователем.

Также предложен метод декодирования принятого сообщения обеспечивающий заданную помехозащищенность принимаемого сигнала с вероятностью правильного восстановления $P_{\tilde{i}} \geq 0,95$ при отношении сигнал/шум на входе приемника $q \geq 0.13$.

В дальнейшем авторами будет исследована возможность применения других моделей стохастических процессов в качестве несущих для скрытой передачи бинарной информации.

Список литературы

1. PulsON Technology. Time Modulated Ultra-Wideband for Wireless Applications. – Time Domain Corporation, 2000.

2. Васюта К.С. Манипуляции показателя Херста фрактального "цветного" Гауссовского шума / К.С. Васюта // Системи обробки інформації. – 2010. – № 6 (87). – С. 62-65.

3. Петерс Эдгар Э. Фрактальный анализ финансовых рынков / Едгар Э. Петерс. – М.: Интрернет-Трейдинг, 2004. –81 с.

4. Тихомиров Н.П. Эконометрика / Н.П. Тихомиров, Е.Ю. Дорохина. – М.: Изд-во Рос. экон. акад., 2002. – 640 с.

Поступила в редколлегию 23.01.2014

Рецензент: д-р техн. наук, проф. В.Д. Карлов, Харьковский университет Воздушных Сил им. Ивана Кожедуба, Харьков.

МЕТОД СКРИТОЇ ПЕРЕДАЧІ БІНАРНОЇ ІНФОРМАЦІЇ НА ОСНОВІ ВИКОРИСТАННЯ ЛІНІЙНО ПЕРЕТВОРЕНОГО СТОХАСТИЧНОГО ПРОЦЕСУ "СЕРЕДНЬОГО КОВЗАННЯ"

К.С. Васюта, С.О. Щербінін

В роботі проаналізована можливість використання лінійно перетвореного стохастичного процесу "середнього ковзання" для підвищення прихованості передачі бінарної інформації. Запропоновано метод оцінки показника моделі, а також приведений графік залежності ймовірності правильної оцінки біта інформації від відношення сигнал/шум на вході приймача.

Ключові слова: *середнє ковзання, коефіцієнт автокореляції, прихованість.*

THE METHOD OF HIDDEN TRANSMISSION OF BINARY INFORMATION BASED ON USING LINEAR TRANSDUCED STOCHASTIC PROCESS OF MOVING AVERAGE

K.S. Vasyuta, S.A. Shcherbinin

The possibility of using linear transduced stochastic process of "moving average model" to improve transmission secrecy of binary information is analyzed in the paper. A method for esti-mating model parameters is proposed, as well as a plot of the probability of the correct estimation of information bit from the signal/noise ratio at the receiver input is given.

Keywords: *moving average, autocorrelation coefficient, secrecy.*