

УДК 621.391

П.Ю. Костенко, А.Н. Барсуков, С.И. Сивашенко, К.С. Васюта

Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков

ВОССТАНОВЛЕНИЕ БИНАРНОГО СООБЩЕНИЯ, МАСКИРУЕМОГО ХАОТИЧЕСКИМ ПРОЦЕССОМ МАККЕЯ-ГЛАССА, МЕТОДОМ РЕГУЛЯРИЗАЦИИ

Анализируются ошибки восстановления бинарного сообщения маскируемого хаотическим процессом, генерируемым динамической системой с запаздыванием, обусловленные несогласованным выбором параметра регуляризации, длительности элемента бинарного сообщения и отношения сигнал/шум. Приведены численные результаты эффективности восстановления.

маскировка, бинарное сообщение, хаотический процесс, шум, восстановление, регуляризация

Введение

Задача маскировки сообщения хаотическим процессом, генерируемым нелинейной динамической системой с запаздыванием привлекает к себе большое внимание [1, 2] в связи с актуальностью скрытной и конфиденциальной передачей информации. Специфика данной задачи обусловлена чувствительностью известных эвристических алгоритмов [3, 4] восстановления сообщения к шуму, помехам в канале связи и параметрам хаотического процесса. В результате возникает большое число ошибок при декодировании сообщения. Уменьшение влияния одного из источни-

ков ошибок восстановления, обусловленного неустойчивым вычислением производной наблюдаемого сигнала, с использованием метода регуляризации производной рассмотрено в [5]. Была показана возможность уменьшения (в среднем в пять раз) отношения сигнала к шуму, при сохранении вероятности правильного восстановления бинарного сообщения и ее зависимость от параметра регуляризации.

Также наряду с регуляризацией производной наблюдения был исследован вклад фильтрации наблюдения в эффективность алгоритма восстановления сообщения. Результаты исследований показали,

что дополнительная обработка (фильтрация) наблюдения существенно не влияет на устойчивость алгоритма восстановления сообщения, а ошибки восстановления уменьшаются незначительно.

Однако за рамками этих исследований остались вопросы, связанные с анализом влияния длительности элементов бинарной последовательности, а также неточности задания параметров передаваемого хаотического процесса на качество восстановления сообщения при различных значениях параметра регуляризации.

В данной работе исследуются характеристики устойчивости (вероятности правильного восстановления) алгоритма восстановления бинарного сообщения маскируемого хаотическим процессом, генерируемым динамической системой Маккея-Гласса при вариациях параметра регуляризации и длительности элементарного символа сообщения в отсутствии и при наличии шумов наблюдения.

Результаты исследований

Рассмотрим передающую систему с запаздыванием, описываемую нелинейным дифференциальным уравнением Маккея-Гласса первого порядка в которой подмешивание информационного сообщения $i(t)$ осуществляется добавлением его к параметру b :

$$\dot{f}(t) = -[b + ci(t)]f(t) + \frac{af(t - \tau)}{1 + (f(t - \tau))^{10}}. \quad (1)$$

При значениях параметров $a = 0,2$, $b = 0,1$, $c = -0,06$, $\tau = 100$ реализуется хаотический режим ее колебаний. Сообщение описывается бинарной последовательностью $i(t) = r_{[t/T_r]}^{(p)}$ ($p = 1, 2$), представленной в алфавите $R = (0, 1)$. В пределах длительности T_r её элементов $i(t) = r_{[t/T_r]}^{(1)} = 0$ или $i(t) = r_{[t/T_r]}^{(2)} = 1$. Число элементов Q на интервале наблюдения T_ξ маскирующего хаотического процесса равно целой части отношения $[T_\xi / T_r]$. Требуется восстановить сообщения $i(t)$ по наблюдению $\xi(t) = f(t, i(t)) + n(t)$, представляющему аддитивную смесь передаваемого хаотического сигнала $f(t, i(t))$ с дисперсией σ_f^2 и белого гауссовского шума $n(t)$ с нулевым математическим ожиданием и дисперсией σ_n^2 . Предложенный алгоритм восстановления сообщения с использованием метода регуляризации, при условии, что параметры хаотической системы известны, позволяет получить выражение для оценки сообщения в явном виде [6]:

$$\hat{f}(t) = \left[\left[\left\{ \frac{a\xi(t - \tau)}{1 + (\xi(t - \tau))^{10}} - R_\alpha \xi(t) \right\} \frac{1}{\xi(t)} \right] - b \right] c^{-1}. \quad (2)$$

В этом выражении R_α – искомый регуляризатор производной наблюдаемого сигнала,

$$R_\alpha f(x) = \int_{|x-y| \leq \alpha} \frac{d}{dx} A_\alpha(x, y) f(y) dy,$$

где $A_\alpha(x, y)$ – усредняющее ядро (функция двух переменных) выбранное в виде:

$$A_\alpha(x, y) = \begin{cases} \left\{ \int_{-\alpha}^{\alpha} \exp \left[\frac{\eta^2}{(\eta^2 - \alpha^2)} \right] d\eta \right\}^{-1} \exp \left\{ \frac{(x-y)^2}{(x-y)^2 - \alpha^2} \right\}; & |x-y| < \alpha; \\ 0 & |x-y| \geq \alpha, \end{cases}$$

а α – параметр регуляризации.

Известно, что суммарная ошибка восстановления состоит из методической ошибки (ошибки регуляризации) и ошибки обусловленной шумом наблюдения. Вклад обеих ошибок неравнозначен и когда выбором параметров удастся уменьшить одну из компонент, вторая проявляет тенденцию к увеличению. Компромисс (минимум суммарной ошибки) достигается, при определенных значениях параметра регуляризации и отношения сигнал/шум. Ниже исследуем ошибки восстановления, обусловленные независим выбором параметра регуляризации и длительности элемента бинарного сообщения как в отсутствии та и в присутствии шумов.

Оценка элемента сообщения сводится к проверке гипотезы о наличии или отсутствии в восстановленном сообщении $\hat{f}(t)$ на заданном интервале символа “0” или “1”, а качество оценки определяется значением вероятности правильного принятия решения. На рис. 1 представлены зависимости вероятности правильной оценки $P_\alpha(L) = 1 - P_{err,\alpha}(L)$ бинарного сообщения в отсутствие шума от величины $L = K / z_\delta$.

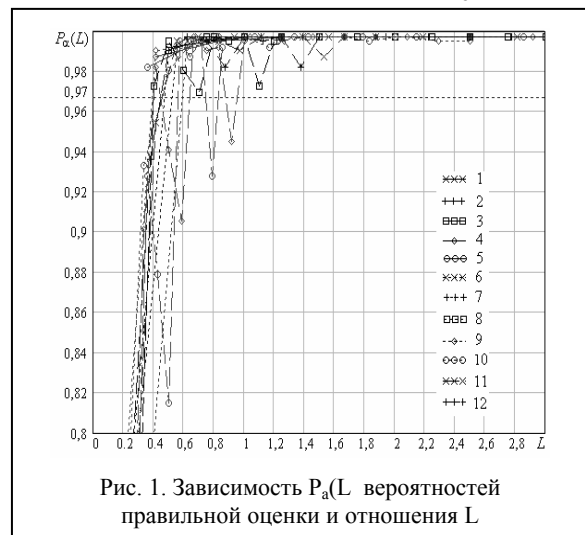


Рис. 1. Зависимость $P_\alpha(L)$ вероятностей правильной оценки и отношения L

Ее значение определяется отношением числа K отсчетов наблюдаемого сигнала в элементе бинарного сообщения к числу его отсчетов $z_\delta = 2b/h$, попадающих в интервал, 2α на котором задается весовая функция. Здесь h – шаг дискретизации хао-

тического процесса. При этом $\bar{b} \in (0,2, \dots, 3,5)$, а длительность элементарного символа принимает значения $K_1 = 50, K_2 = 100, \dots, K_{12} = 600$ (кривые 1–12). Например, при $L = 5$ числе отсчетов в элементарном символе наблюдаемого сигнала в 5 раз больше числа отсчетов выделяемой весовой функцией. Величина $P_{\text{err.}\alpha} = d_H(\bar{b})/Q$ определяет долю ошибок в оценках элементов сообщения и равна отношению расстояния Хемминга $d_H(i(t), \hat{f}_\alpha(t))$ между передаваемой бинарной последовательностью $i(t)$ и её оценкой $\hat{f}_\alpha(t)$ к общему числу Q ее элементов. Количество символов в бинарном сообщении фиксировано и равно $Q = 400$.

Заметим, что $L \geq 1$ вероятность правильной оценки информационного сообщения во всем диапазоне изменения \bar{b} выше уровня 0,97, что свидетельствует о приемлемой методической ошибке. С увеличением значения L качество восстановления $i(t)$ улучшается, и при $L \geq 2$ все кривые близки к уровню определяющему вероятность $P_\alpha(L) \approx 1$.

Результаты расчета вероятности правильной оценки $P_\delta(\alpha)$ бинарного сообщения в присутствии шума различного уровня иллюстрирует рис.2.

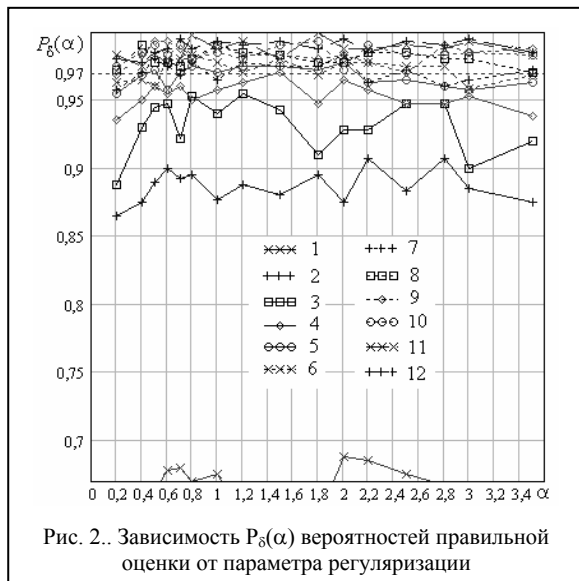


Рис. 2. Зависимость $P_\delta(\alpha)$ вероятностей правильной оценки от параметра регуляризации

Параметр регуляризации \bar{b} принимает значения из интервала $(0,2 - 3,5)$, а отношения сигнал/шуму $\delta = \sigma_f / \sigma_n$ соответственно $d_1 = 1, d_2 = 5, d_3 = 10, d_4 = 15, d_5 = 20, d_6 = 25, d_7 = 30, d_8 = 40, d_9 = 50, d_{10} = 60, d_{11} = 70, d_{12} = 80$ кривые (1–12) с длительностью элементарного символа $K = 500$.

В анализируемом интервале качественное восстановление $i(t)$ ($P_\delta(\alpha) \geq 0,97$) наблюдается при значениях d , которым соответствуют кривые (9–12). С увеличением уровня шума восстановление с заданным качеством ($P_\delta(\alpha) \geq 0,97$) наблюда-

ется в меньшем интервале возможных значений \bar{b} (кривые (5–8)), которые группируются вокруг $\bar{b} \approx 1,5$. По мере увеличения уровня шума подобная тенденция сохраняется до полной потери необходимого качества восстановления сообщения (кривые (1–3)).

Результаты расчета вероятности правильной оценки бинарного сообщения $P_\alpha(\delta)$ при различных значениях δ и параметре регуляризации ($\alpha_1 = 0,2, \alpha_2 = 0,4, \alpha_3 = 0,5, \alpha_4 = 0,6, \alpha_5 = 0,7, \alpha_6 = 0,8, \alpha_7 = 1, \alpha_8 = 1,2, \alpha_9 = 1,5, \alpha_{10} = 2, \alpha_{11} = 2,5, \alpha_{12} = 3$) иллюстрируются соответствующими кривыми (1–12) рис. 3.

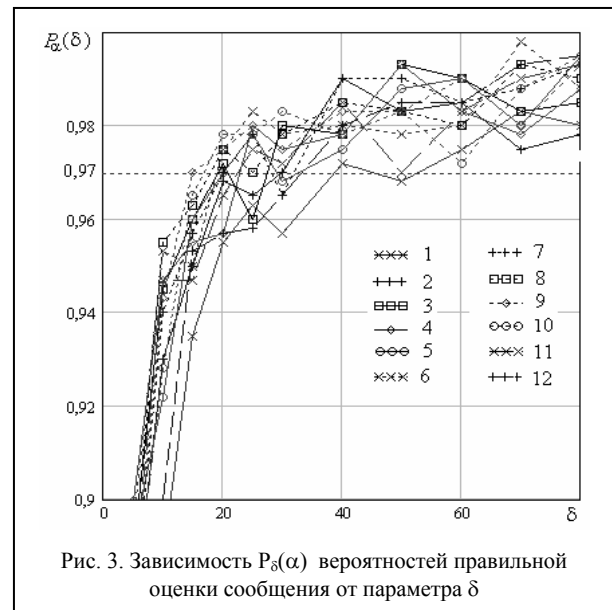
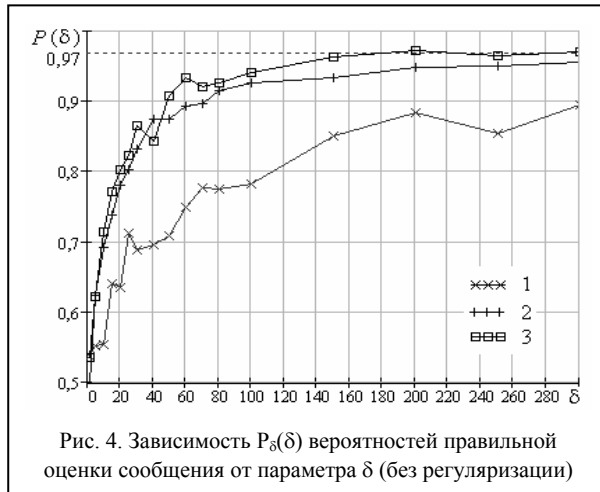


Рис. 3. Зависимость $P_\delta(\alpha)$ вероятностей правильной оценки сообщения от параметра δ

Легко заметить, что только при $\alpha_9 = 1,5$ и $d \geq 15$ качество восстановления удовлетворяет заданному требованию – $P_\alpha(\delta) \geq 0,97$. По мере увеличения d эта вероятность увеличивается для всех рассматриваемых значений параметра регуляризации и его выбор становится менее критичным.

Кривые (1–3) (рис. 4) описывают качество восстановления бинарного сообщения при различных значениях δ и параметре длительности T_f элемента сообщения, принимающего значения: $K_1 = 300, K_2 = 400$ и $K_3 = 500$ с использованием алгоритма (2) в котором производная наблюдения находилась численными методами без регуляризации.

Сравнительный анализ кривых рис.3 и аналогичных зависимостей $P(\delta)$ представленных на рис.4, показывает, что для обеспечения одинаковых значений $P_\alpha = P = 0,97$ требуется, в среднем, в девять раз меньшее значение параметра δ , чем при использовании алгоритма без регуляризации, что подтверждает эффективность предложенного алгоритма восстановления бинарного сообщения.



Заклучение

В результате проведенного исследования определены допустимые, с точки зрения суммарной ошибки восстановления бинарного сообщения, значения параметра регуляризации при различных требованиях к параметрам сообщения и уровню шума. Показано, что учет влияния параметра регуляризации на методическую ошибку позволяет определить допустимые границы его изменения и дальнейшее уточнение при наличии помех в наблюдении. Во всех рассмотренных случаях для качественного восстановления число отсчетов наблюдения должно быть больше числа отсчетов попадающих в интервал определения весовой функции принимающей

участие в формировании регуляризованного значения производной наблюдения.

Список литературы

1. V.B. Ryabov, P.V. Usik, D.M. Vavriv. *Chaotic Masking without Synchronization*. Радиофизика и астрономия, 1997, т.2, № 4, стр. 473-479.
2. В.И. Пономарев, М.Д. Прохоров. Кодирование и извлечение информации, замаскированной хаотическим сигналом системы с запаздыванием. Радиотехника и электроника, 2004. том 49, №9, с. 1098-1104.
3. Э.В. Кальянов. Передача информации через радиоканал с использованием маскирующих колебаний. Письма в ЖТФ, 2001, том 27, вып. 1.
4. С.Е. Фалькович, П.Ю. Костенко. Основы статистической теории радиотехнических систем. Учеб. пособие. – Харьков: Нац. аэрокосмический ун-т «Харьк. авиац. ин-т», 2005. – 390 с.
5. Костенко П.Ю., Барсуков А.Н., Антонов А.В., Хаотическая маскировка бинарного сообщения и его восстановление без синхронизации устойчивое к шуму наблюдению. Современные проблемы радиотехники и телекоммуникаций РТ-2007: Тез доклад. 3-я Междунар. конфер. 16 по 21 апреля 2007. Севастополь, 2007 г. С. 67.
6. В.В. Васин. Об устойчивом вычислении производной в пространстве $C(-\infty, \infty)$. Ж. вычисл. матем. и матем. физ., 1973, 13, №6, 1383-1389.

Рецензент: д-р техн. наук проф. Г.В. Алешин, Харьковский университет Воздушных Сил Украины, Харьков.