

01;06.3;07;09

## Передача информации с использованием маскирующих хаотических колебаний

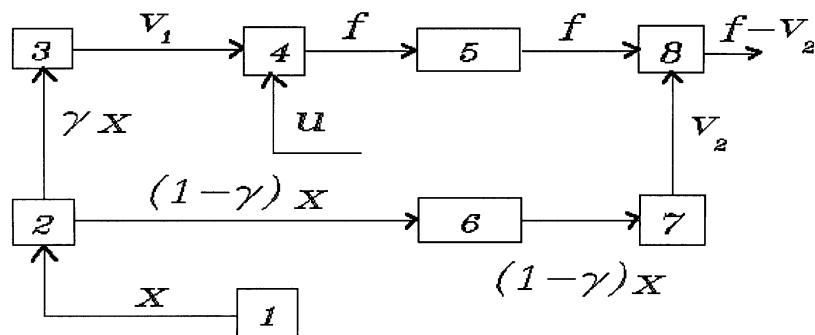
© Э.В. Кальянов, В.В. Григорьянц

Институт радиотехники и электроники РАН, Фрязинская часть

Поступило в Редакцию 1 июня 2000 г.

Рассмотрена схема скрытой связи применительно к кабельным и волоконно-оптическим системам. Численными методами проведен анализ двухканальной схемы, основанной на кодировании хаотического сигнала, используемого для маскировки передаваемой информации.

В настоящее время активно исследуются возможности использования хаотических колебаний для маскировки передаваемой информации. Привлекательным достоинством такой маскировки является потенциально большая ее эффективность по сравнению с известными способами, основанными на различных методах кодирования [1]. В литературе описано несколько систем скрытой связи, использующих явление хаотической синхронизации [2–9]. Однако практическая реализация таких систем сталкивается с трудностями выделения полезного сигнала в приемнике. Это обусловлено тем, что синхронизируемая динамическая приемная система должна генерировать хаотические колебания, которые с большой степенью точности идентичны передаваемым. Последнее делает такую систему связи трудно реализуемой. Это приводит к необходимости поиска других способов передачи информационных сигналов с использованием достоинств хаотических колебаний. В настоящей работе рассматривается система скрытой связи, в которой выделение информационного сигнала из хаоса не связано с обеспечением идентичности колебаний двух генераторов путем синхронизации. При этом предлагается использовать не один, как обычно, а два канала связи. Это хотя и усложняет линию связи, но делает реальным осуществление маскировки информационного сигнала различными сложными внешними колебаниями, в том числе и хаотическими. Такие линии особенно перспективны в волоконно-оптических системах, так как они обладают



**Рис. 1.** Схема передачи информации при использовании хаотических колебаний: 1–4 — элементы передатчика; 5, 6 — элементы двухканальной линии связи; 7, 8 — элементы приемника.

рекордно малыми потерями и практически нулевой дисперсией, а также малыми габаритами многоволоконных кабелей.

Один из вариантов схемы передачи скрытой информации при использовании сложных колебаний для маскировки информационного сигнала иллюстрируется блок-схемой рис. 1. Она содержит передатчик из элементов 1–4, двоянный передающий тракт связи (линии 5 и 6) и приемное устройство из элементов 7 и 8. Маскирующий сигнал  $x(t)$  формируется автостохастическим генератором 1. Этот сигнал разделяется на два канала в устройстве 2. В одном канале часть этих колебаний ( $\gamma x(t)$ , где  $\gamma$  — постоянный коэффициент, причем  $\gamma < 1$ ) проходит через кодирующее устройство 3 и приобретает вид  $v_1(t)$ . Этот сигнал суммируется с информационным сигналом  $u(t)$  в сумматоре 4 и результирующие колебания поступают в линию передачи 5 в виде  $f(t)$  ( $f(t) = v_1(t) + u(t)$ ). В линию передачи 6 подается вторая часть хаотических колебаний генератора 1, равная  $(1 - \gamma)x(t)$ . После прохождения линии 6 эти колебания поступают в приемнике на кодирующее устройство 7, аналогичное устройству 3, и преобразуются в колебания  $v_2(t)$ . Полезный сигнал выделяется в вычитающем устройстве 8 так, что информационный сигнал в приемнике определяется разностью  $f(t) - v_2(t)$ .

В рассматриваемом способе передачи информации степень ее искажения определяется лишь степенью неидентичности кодирующих устройств. Сигнал на выходе вычитающего устройства воспроизводит входной сигнал при идентичных кодирующих устройствах и равных сигналах после разветвления (при  $\gamma = 0.5$ ), так как в этом случае  $v_1(t) = v_2(t)$ . При  $\gamma \neq 0.5$  для воспроизведения информационного сигнала можно использовать различные компенсирующие устройства.

Следует отметить, что достоинством рис. 1 является то, что в качестве маскирующих колебаний могут использоваться не только колебания, формируемые динамическими системами (хаотические или сложные, например, многочастотные), но и шумовые колебания, формируемые любыми источниками шума.

При анализе работы схемы рис. 1 целесообразно в качестве маскирующего сигнала выбрать колебания, формируемые динамической системой с хаотическим поведением. При этом могут быть использованы различные источники хаотических колебаний [2–4]. В качестве генератора таких колебаний удобно использовать источник, описываемый уравнениями Рёсслера [10]

$$\begin{aligned}\dot{x} &= -y - z, \\ \dot{y} &= x + \alpha y, \\ \dot{z} &= -\beta z + xy + \delta.\end{aligned}\tag{1}$$

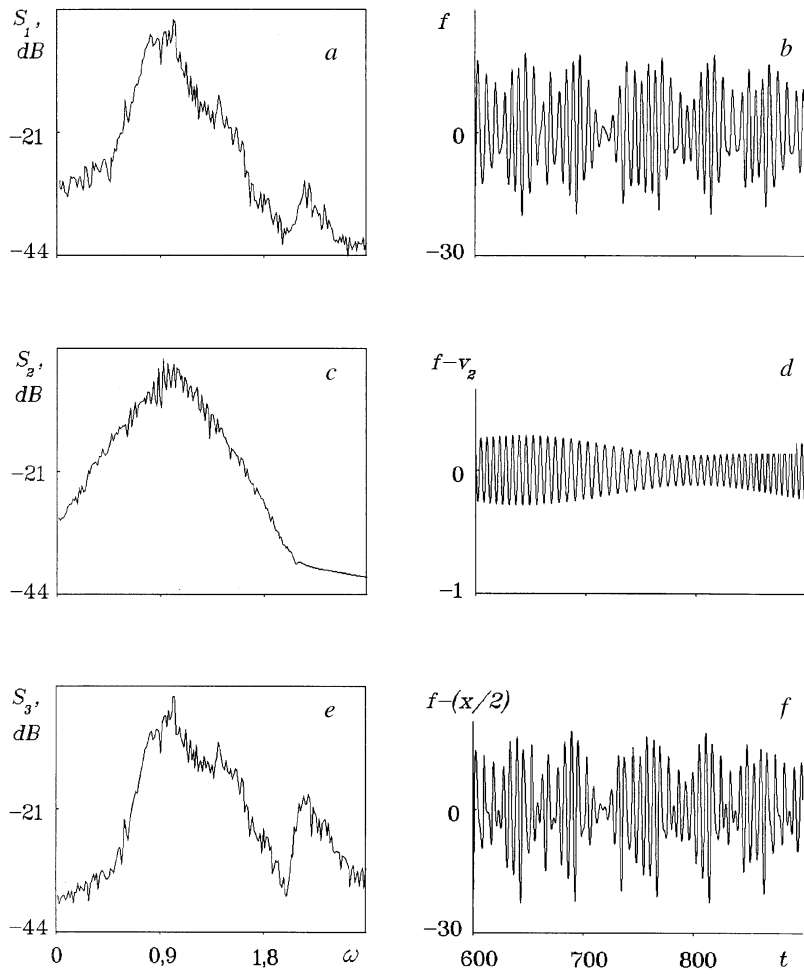
Решение  $x(t)$  этой системы нелинейных дифференциальных уравнений при  $\alpha = 0.3$ ,  $\beta = 8.5$ ,  $\delta = 0.4$  является хаотическим. Спектр колебаний при этом не содержит регулярных составляющих.

Информационный сигнал  $u(t)$  представим в виде гармонического колебания, модулированного по амплитуде и частоте:

$$u = A_0(1 + M \cos \Omega t) \cos[(\omega_0 + m \cos \Omega t)t],\tag{2}$$

где  $A_0$ ,  $\omega_0$  — амплитуда и частота гармонического сигнала;  $M$ ,  $m$ ,  $\Omega$  — коэффициент амплитудной модуляции, индекс частотной модуляции и частота модуляции соответственно.

В качестве относительно простых кодирующих устройств 3 и 6 можно использовать фильтры второго порядка. В этом случае колебания



**Рис. 2.** Спектры мощности ( $a$ ,  $c$ ,  $e$ ) и соответствующие им фрагменты реализаций ( $b$ ,  $d$ ,  $f$ ).

$v_1(t)$  на входе фильтра 3 при колебаниях на его входе  $\gamma x(t)$  являются решением следующего дифференциального уравнения:

$$\ddot{v}_1 + (\omega_1/Q_1)\dot{v}_1 + \omega_1^2(v_1 - \gamma x) = 0, \quad (3a)$$

где  $\omega_1, Q_1$  — резонансная частота и добротность фильтра. Аналогично колебания  $v_2(t)$  на выходе фильтра 7, имеющего резонансную частоту  $\omega_2$  и добротность  $Q_2$ , описываются уравнением

$$\ddot{v}_2 + (\omega_2/Q_2)\dot{v}_2 + \omega_2^2[v_2 - (1 - \gamma)x] = 0. \quad (3b)$$

Соотношения (1)–(3) определяют математическую модель, описывающую работу рассматриваемой схемы передачи информации. На рис. 2 приведены результаты численного анализа математической модели. Спектры рассчитаны для случая хаотических колебаний  $x(t)$  ( $\alpha = 0.3, \beta = 8.5, \delta = 0.4$ ). Параметры в соотношениях (2) и (3) полагались равными следующим величинам:  $A_0 = 0.2, M = 0.1, m = 0.01, \omega_0 = 1, \Omega = 0.02, \omega_1 = \omega_2 = 1, Q_1 = Q_2 = 4, \gamma = 0.5$ .

На рис. 2, *a* показан спектр  $S_1$  колебаний  $f(t)$ , распространяющихся в линии 5. Практически этот спектр не отличается от спектра хаотических колебаний  $v_1(t)$ , так как амплитуда колебаний информационного сигнала  $u(t)$  значительно меньше (на два порядка) максимальных выбросов хаотического колебательного процесса  $v_1(t)$ . На рис. 2, *b* показан фрагмент реализации, рассчитанный при тех же параметрах, что и спектр  $S_1$ . Спектр колебаний информационного сигнала  $S_2$  на входе вычитающего устройства 8 при одинаковых фильтрах иллюстрируется рис. 2, *c*. Он не отличается от спектра информационного сигнала на входе сумматора в передающем устройстве. Соответствующая реализация показана на рис. 2, *d*. При этом спектр разности колебательных процессов  $f(t)$  и  $(1 - \gamma)x(t)$  в линиях передачи ( $S_3$ , рис. 2, *e*) и соответствующая ему реализация колебаний (рис. 2, *f*) отображают хаотический характер колебаний. Это свидетельствует о невозможности выделения информационного сигнала при несанкционированном доступе.

Проведенный анализ свидетельствует о потенциальной эффективности использования двухканальной системы связи для передачи конфиденциальной информации. Как уже отмечалось, в рассматриваемом способе передачи информации для маскировки могут использоваться не только сигналы, формируемые динамическими системами с хаотическим поведением, но и шумовые сигналы.

Следует отметить, что на работоспособности рассмотренной системы на практике может отрицательно сказываться неидентичность кодирующих устройств и связанных каналов, а также временная нестабильность их характеристик. Именно поэтому наиболее перспективно применение рассмотренного в статье метода передачи конфиденциальной информации при использовании волоконно-оптических линий связи.

Работа выполнена при поддержке РФФИ (грант 98-02-16722).

## Список литературы

- [1] *Варакин Л.Е.* Системы связи с шумоподобными сигналами. М.: Радио и связь. 1985.
- [2] *Волковский А.Р., Рульков Н.Ф.* // Письма в ЖТФ. 1993. Т. 19. В. 3. С. 72–77.
- [3] *Colet P., Roy R.* // Optics Lett. 1994. V. 19. N 24. P. 2056–2059.
- [4] *Матросов И.И.* // Письма в ЖТФ. 1996. Т. 22. В. 23. С. 4–8.
- [5] *Шалфеев В.Д., Осипов Г.В., Козлов А.К., Волковский А.Р.* // Зарубежная радиоэлектроника. Успехи современной радиоэлектроники. 1997. № 10. С. 27–49.
- [6] *Percord L.M., Carroll T.L., Johnson G.A., Mar D.J., Heagy J.F.* // Chaos. 1997. V. 7. N 4. P. 520–543.
- [7] *Кальянов Э.В.* // Письма в ЖТФ. 1997. Т. 23. В. 14. С. 66–71.
- [8] *Van Wiggeren G.D., Roy R.* // Phys. Rev. Lett. 1998. V. 81. N 16. P. 3547–3550.
- [9] *Кальянов Э.В.* // Радиотехника и электроника. 1998. Т. 43. № 2. С. 206–217.
- [10] *Rossier O.E.* // Phys. Lett. 1976. V. 57A. N 5. P. 397–398.