09

Шифрование информации при использовании хаотических решений детерминированных уравнений

© Г.Н. Кальянов, Э.В. Кальянов

Институт радиотехники и электроники РАН (Фрязинский филиал)
E-mail: erast@ms.ire.rssi.ru

Поступило в Редакцию 14 июля 2005 г.

Предложен новый метод шифрования графической информации, основанный на хаотическом изменении цвета каждого символа изображения. Приведены результаты исследования хаотической системы, а также результаты применения псевдослучайной последовательности чисел, формируемых на основе ее решений, к шифрованию и дешифрованию цветного графического изображения.

При шифровании в основном исследуются телекоммуникационные технологии, основанные на использовании различных способов кодирования матриц. Наряду с использованием сложных регулярных закономерностей для кодирования матриц рассматривалась возможность применения нерегулярных процессов [1]. При этом для перестановки элементов матрицы использован стандартный генератор псевдослучайных чисел.

Наряду с тем что при применении модели матрицы возможно восстановление потерь „голографическим“ методом, в принципе, при перестановке элементов матрицы возможно и вскрытие шифра, хотя в ряде случаев это очень сложно. В то же время с помощью псевдослучайных генераторов можно получать довольно стойкие криптосистемы, если осуществлять не перестановку элементов матрицы, а изменение цвета элементов, формирующих изображение. При этом в качестве генераторов псевдослучайных сигналов, как представляется, весьма подходят генераторы с хаотической динамикой, и особенно искусственно сконструированные [2–7]. Они предпочтительны тем, что хаос, описываемый их уравнениями (при относительной простоте записи), может быть более развитым.

В данной работе рассматривается новый способ шифрования информации, основанный на хаотическом изменении цвета символов, форми-

рующих изображение. Для генерирования псевдослучайной последовательности чисел используются оригинальные уравнения, имеющие вид

$$dx/dt = \alpha(y - x),\ dy/dt = x(z - \beta),\ dz/dt = \gamma - xy, \qquad (1)$$

где α, β, γ — положительные коэффициенты. Эти уравнения описывают искусственно сконструированную автоколебательную систему. Особенностью решений этих уравнений как системы, обладающей хаотической динамикой, является высокая чувствительность к изменению параметров. Именно это затрудняет несанкционированное дешифрование при использовании для кодирования информации детерминированного хаоса.

Для иллюстрации „чувствительности“ используемой системы к изменению параметров проведем сравнение колебаний двух автономных систем, каждая из которых описывается уравнениями (1), отличаясь индексами $i (i = 1, 2)$ при переменных и положительных коэффициентах. В этом случае

$$\begin{aligned} dx_1/dt &= \alpha_1(y_1 - x_1), \quad dx_2/dt = \alpha_2(y_2 - x_2), \\ dy_1/dt &= x_1(z_1 - \beta_1), \quad dy_2/dt = x_2(z_2 - \beta_2), \\ dz_1/dt &= \gamma_1 - x_1y_1, \quad dz_2/dt = \gamma_2 - x_2y_2. \end{aligned} \qquad (2)$$

На рис. 1 представлены фрагменты реализаций разностных колебаний $x_1(t) - x_2(t)$ при незначительном различии параметров α_1 и α_2; при этом $\alpha_1 = 1$, $\beta_1 = \beta_2 = 0.8$, $\gamma_1 = \gamma_2 = 1.2$. Значения коэффициента α_2 равны 1.1 (a) и 1.01 (b) и 1.000001 (c). Начальные условия для всех переменных во всех случаях равны 0.1.

Структура разностных колебаний свидетельствует о нарастающем различии сравниваемых хаотических процессов даже при небольшом изменении одного из параметров. При малой разнице параметров α_1 и α_2 $(\alpha_1 - \alpha_2 = 0.01)$ разностные колебания возникают с заметной задержкой, которая увеличивается с уменьшением величины $\alpha_1 - \alpha_2$ (c). В случае рис. $1, b$ задержка занимает интервал времени $t \in$ [0,20], а в случае рис. $1, c$ — интервал времени $t \in$ [0,52]. Эту задержку (ее условно можно рассматривать как „переходный“ процесс) легко устранить путем исключения начального участка реализации. Это необходимо при кодировании информации.

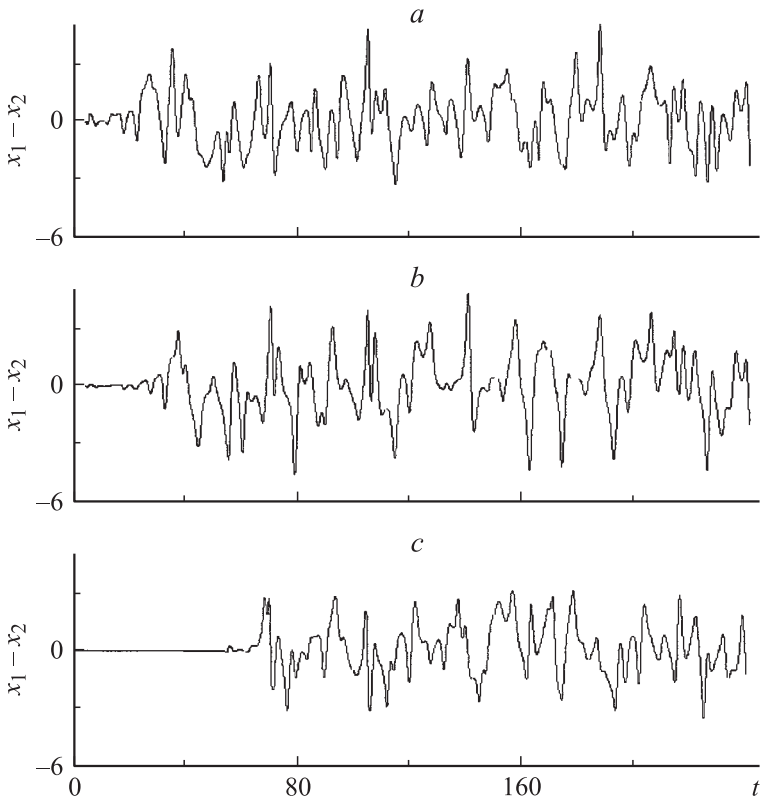

Рис. 1. Фрагменты реализаций разностных колебаний.

Использование хаотических решений рассмотренной системы уравнений позволяет создать достаточно сложный шифр, который не поддается раскрытию, если не воспроизведены точные значения начальных условий и параметров динамической системы, при которых выполнялось решение уравнений.

Подмешивание всевдослучайной последовательности чисел, получаемой на основе решения хаотических уравнений, как уже отмечалось, целесообразно осуществлять так, чтобы происходило хаотическое изменение их палитры цвета. Это является основой разработанной программы (на языке C++ Builder), обеспечивающей шифрование и

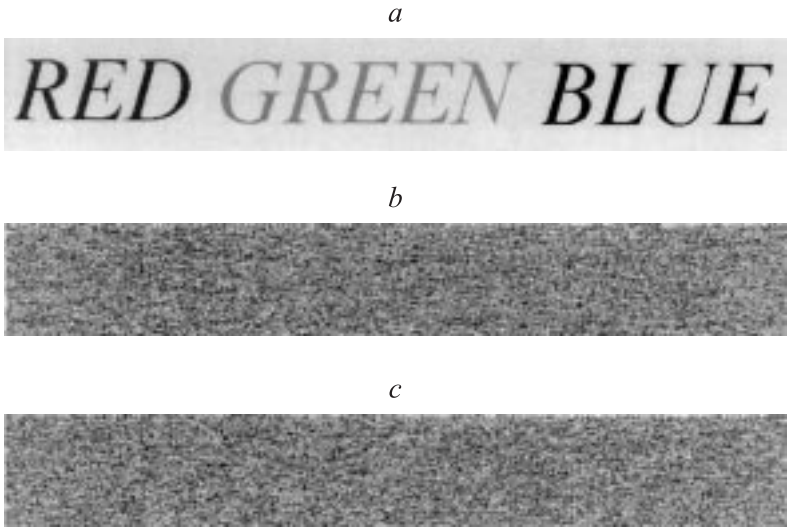

Рис. 2. Изображение рисунка в незашифрованном (a) и зашифрованном (b) виде, а также его изображение при неправильном дешифровании (c), когда при точном введении параметров α и β ($\alpha = 1.123456789123456$, $\beta = 0.8$) параметр γ задан значением $\gamma = 1.200000000000001$.

дешифрование с использованием системы с хаотической динамикой. Преобразование графической матрицы осуществляется путем присвоения каждому символу, формирующему изображение, нового цвета в соответствии не только с хаотическими решениями дифференциальных уравнений, но и с его исходной палитрой цвета. В этом случае выполняется условие, при котором индекс нового цвета пикселя равен исходному индексу цвета пикселя плюс дополнительный индекс цвета пикселя, определяемый решением хаотических дифференциальных уравнений. При этом каждый символ графической матрицы последовательно преобразуется в одном и том же стековом блоке памяти. При дешифровании используется аналогичный алгоритм преобразований. Отличие заключается в том, что при формировании палитры цвета осуществляется вычитание псевдослучайной последовательности чисел, формируемых на основе решений тех же уравнений, которые использовались при шифровании.

Для иллюстрации процессов шифрования и дешифрования использовалась цветная матрица 24 бита в виде графического изображения. На рис. 2, *a* при использовании многоцветной матрицы приведены изображения слов, показанные для наглядности в трех цветах (на желтом фоне), когда каждое слово записано цветом, соответствующим его смыслу (например, слово „*RED*“ — красным цветом). Хотя изображение на рис. 2, *a* получено в цвете, оно распечатано на принтере как черно-белое. Поэтому изменение цвета пикселей на этом рисунке (а также на рис. 2, *b*, *c*) отображается тональностью серого. Изображения слов, представленных на рис. 2, *a*, после процедуры преобразования в зашифрованной матрице принимают вид, иллюстрируемый рис. 2, *b*. Зашифрованное изображение отображает хорошее (хаотическое) перемешивание цветов (в представленном виде — тональности серого) пикселей, так что исходная информация надежно замаскирована.

При шифровании в случае рис. 2, *b* в уравнениях (1) при $\beta = 0.8$ заданы (для примера) следующие значения варьируемых параметров: $\alpha = 1.123456789123456$, $\gamma = 1.2$. При санкционированном дешифровании рис. 2, *b*, когда параметры α, β, γ введены с абсолютной точностью, рис. 2, *a* воспроизводится без изменения. В случаях малейших ошибок хотя бы по одному параметру (например, при несанкционированном входе), дешифрование оказывается невозможным. Даже при ошибке в определении одного из параметров, составляющей 10^{-15} (рис. 2, *c*), вид матрицы остается подобным рисунку, показанному на рис. 2, *b*; при этом распределение цвета пикселей, естественно, иное.

Проведенные исследования шифрования и дешифрования свидетельствуют о том, что при кодировании цвета символов, формирующих изображение, могут быть использованы псевдослучайные последовательности целых чисел, являющихся результатом решений нелинейных дифференциальных уравнений с хаотической динамикой, описывающих модели искусственно сконструированных систем.

При шифровании с помощью последовательности псевдослучайных чисел использование изменения цвета символов, формирующих изображение, позволяет обеспечить его надежную маскировку. Учитывая устойчивость шифра, информацию, зашифрованную рассмотренным способом, можно передавать по открытым каналам, в том числе по электронной почте и путем излучения, а также хранить в архивах со свободным доступом. При этом маскировка информации при ее передаче по открытым каналам не хуже, чем ее маскировка при передаче излучаемыми хаотическими колебаниями в случаях, описанных в [8–13].

Работа выполнена при поддержке РФФИ (проект № 04–02–16536).

Список литературы

[1] *Колесов В.В., Залогин Н.Н., Воронцов Г.М.* // РЭ. 2002. Т. 47. № 5. С. 583–588.
[2] *Гарел Д., Гарел О.* Колебательные химические реакции / Пер. с англ. М.: Мир, 1986. 148 с.
[3] *Rossler O.E.* // Phys. Lett. 1976. V. A57. N 5. P. 397, 398.
[4] *Sprott J.C.* // Phys. Rev. 1994. V. E50. N 2. P. 647–650.
[5] *Кислов В.Я., Кислов В.В.* // РЭ. 1997. Т. 42. № 8. С. 962–973.
[6] *Кальянов Э.В.* // Письма в ЖТФ. 2004. Т. 30. В. 13. С. 45–50.
[7] *Кальянов Э.В.* // Письма в ЖТФ. 2004. Т. 30. В. 15. С. 30–34.
[8] *Сиото К.М., Oppenheim A.V.* // Phys. Rev. Lett. 1993. V. 71. N 1. P. 65–68.
[9] *Матросов И.И.* // Письма в ЖТФ. 1996. Т. 22. В. 23. С. 4–8.
[10] *Дмитриев А.С., Кузьмин Л.В.* // Письма в ЖТФ. 1999. Т. 25. В. 16. С. 71–77.
[11] *Кальянов Э.В.* // Письма в ЖТФ. 2001. Т. 27. В. 16. С. 1–9.
[12] *Пономаренко В.И., Прохоров М.Д.* // Письма в ЖТФ. 2002. Т. 28. В. 16. С. 37–43.
[13] *Дмитриев А.С., Кяргинский Б.Е., Панас А.И.* и др. // Письма в ЖТФ. 2003. Т. 29. В. 2. С. 70–76.