МОДИФИЦИРОВАННЫЙ СИНГУЛЯРНЫЙ СПЕКТРАЛЬНЫЙ АНАЛИЗ ЗАШИФРОВАННОЙ НА ОСНОВЕ ДИНАМИЧЕСКОГО ХАОСА ИНФОРМАЦИИ

А. В. Сидоренко, И. В. Шакинко

Белорусский государственный университет
Минск, Беларусь
E-mail: sidorenkoA@yandex.ru

Определены показатели выходных последовательностей зашифрованной на основе динамического хаоса информации при использовании разработанного метода модифицированного сингулярного спектрального анализа.

Проведен сравнительный анализ результатов, полученных сингулярным спектральным анализом и модифицированным методом.

Установлено, что режимы шифрования CBC и CFB подходят для использования в алгоритме шифрования на основе динамического хаоса, в отличие от режимов OFB и ECB.

Ключевые слова: сингулярный спектральный анализ, динамический хаос, шифрование, уровень вклада главных компонент, вейвлет-анализ.

Введение

Современные информационные технологии находят все более широкое применение в телекоммуникационных системах. Актуальной становится задача разработки и внедрения надежных методов и средств в области защиты информации для обеспечения ее целостности и конфиденциальности [1].

Использование динамического хаоса при шифровании данных предъявляет новые требования к обеспечению надежности, качественности шифра.

Существенным является обеспечение хаотического режима алгоритма на основе динамического хаоса при шифровании данных. Для оценки хаотичности в некоторых работах применяются показатели Ляпунова. Однако при использовании, например, логистического отображения вычисление показателей Ляпунова недостаточно точно либо не охватывает «окна прозрачности», где динамическая система является детерминированной.

Ввиду того, что выходные последовательности, зашифрованные на основе динамического хаоса, являются не стационарными, для их обработки возможно использование метода сингулярного спектрального анализа (ССА) [2]. Но поскольку периодические процессы в исследуемых временных рядах сами не стационарны, то применение одного метода ССА для выделения детерминированных составляющих оказывается недостаточным [3]. В связи с этим возникает необходимость поиска других методов оценки хаотичности поведения динамической системы.

Схема шифрования на основе динамического хаоса

Основой схемы алгоритма шифрования является сеть Фейстеля, которая представляет собой определенную многократно повторяющуюся структуру, называемую ячейкой Фейстеля. При переходе от одной ячейки к другой меняется секретный

ключ. В нашей работе число итераций *z* изменялось от 64 до 1024. Для формирования нового итерационного ключа применялось «пилообразное» хаотическое отображение $F(x) = (Ax) \bmod (M - 1)$, где A – параметр отображения, M – мощность. В данной работе использовались четыре режима шифрования: электронная кодовая книга ECB (Electronic Code Book), сцепление блоков шифра CBC (Cipher Block Chaining), обратная связь по шифртексту CFB (Cipher Feed Back), обратная связь по выходу OFB (Output Feed Back). Режимы шифрования используются для модификации процесса шифрования так, чтобы результат шифрования каждого блока был уникальным вне зависимости от шифруемых данных и не позволял сделать какие-либо выводы об их структуре [4].

Алгоритм модифицированного сингулярного спектрального анализа

На основе вейвлет-преобразования и сингулярного спектрального анализа разработан собственный метод модифицированного сингулярного спектрального анализа. Алгоритм метода включает следующие этапы.

1. Вычисление вейвлет-коэффициентов. Пусть сообщение *s* представлено в виде последовательности N отсчетов $\{s_k\}$. Тогда непрерывное вейвлет-преобразование можно записать следующим образом [5]:

$$W_s(a,b) = \sqrt{a}\Delta t \sum_{k=n}^{n+[aN]+1} s_k \overline{c_k(a,b)}, \qquad (1)$$

где

$$c_k(a,b) = \Psi\left(\frac{k+1}{a} - \frac{b}{a\Delta t}\right) - \Psi\left(\frac{k}{a} - \frac{b}{a\Delta t}\right), \qquad (2)$$

Δt – шаг дискретизации, b – параметр сдвига вейвлета, a – масштабный коэффициент, $\Psi(t)$ – первообразная выбранного вейвлета с компактным носителем на промежутке [0, *N*], $n = b/\Delta t$.

Для отделения трендовой составляющей сигнала и выявления детерминированных составляющих к полученным вейвлет-коэффициентам применяется операция «модуль».

2. Формирование многомерного ряда. При значении масштабного коэффициента $a = a_0$, вейвлет-коэффициенты $W_s(a_0, b)$ можно рассматривать как одномерный временной ряд *x*. На основе данного ряда формируется матрица *X*. В качестве первой строки матрицы X используется M (число компонент) значений ряда, начиная с первого члена. В качестве второй строки матрицы используются значения, начиная с x_2 до x_{M+1}. Последнюю строку матрицы с номером $k = N - M + 1$ образуют последние M элементов ряда *x*.

3. Сингулярное разложение выборочной ковариационной матрицы.

Вычисляется матрица $V = (1/k)XX^T$. Определяются собственные числа и собственные вектора матрицы *V*, т. е. ее разложение $V = P\Lambda P^T$, где Λ – диагональная матрица собственных чисел, а P – ортогональная матрица собственных векторов матрицы *V*.

4. Определение уровней вклада главных компонент и построение фазовых диаграмм. Используя диагональную матрицу собственных чисел, вычисляются уровни вклада главных компонент:

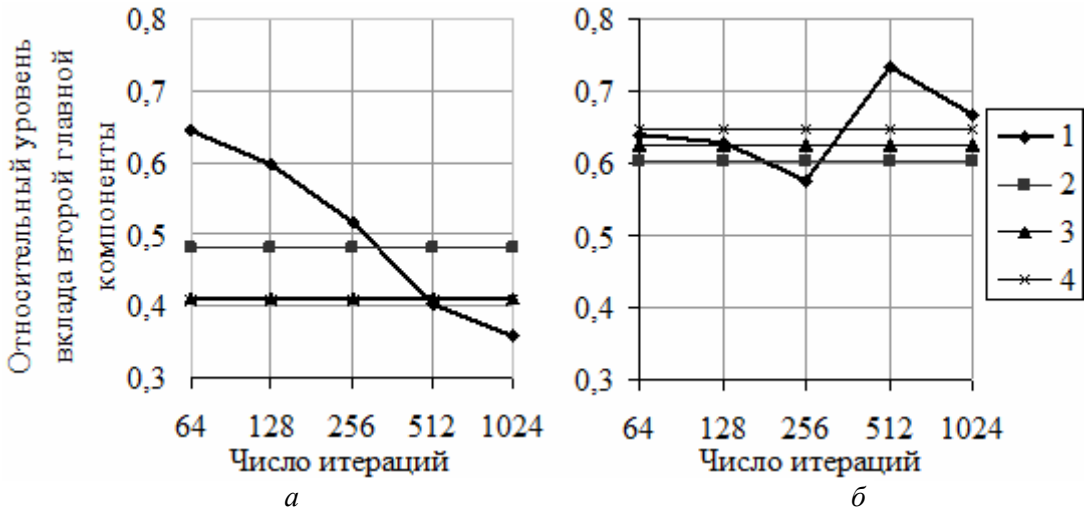
$$\beta_j = (\lambda_j / \sum_{i=1}^{M} \lambda_i) * 100\% . \quad (3)$$

На основе полученных собственных векторов строятся фазовые диаграммы, представляющие собой изображения, образованные последовательным соединением точек на координатной плоскости. На этой плоскости координаты i-ой точки задаются парой чисел (x_i, y_i), где x_i – i-ое значение первого выбранного для построения собственного вектора, y_i – i-ое значение второго выбранного для построения собственного вектора.

Результаты и их обсуждение

Анализу подвергались реализации зашифрованных сообщений длиной N = 10 000, число компонент, на которые велось разложение, выбиралось M = 1000. Использовался вейвлет Добеши пятого порядка.

На рис. 1 приводятся графики, построенные по данным, полученным при обработке зашифрованных сообщений методом сингулярного спектрального анализа и методом модифицированного сингулярного спектрального анализа (значение масштабного коэффициента $a = 0{,}7$).



а *б*

Рис. 1. График зависимости относительного уровня вклада второй главной компоненты от числа итераций при использовании модифицированного сингулярного спектрального анализа (*а*) и сингулярного спектрального анализа (*б*) для зашифрованных сообщений при помощи: алгоритма шифрования на основе динамического хаоса (режим СВС) (*1*); алгоритма des (режим OFB) (*2*); алгоритма aes в режимах OFB (*3*) и СВС (*4*)

Относительные уровни вклада второй главной компоненты, полученные модифицированным методом и сингулярным спектральным анализом для зашифрованных сообщений при помощи алгоритма на основе динамического хаоса при числе итераций, большем 512, отличаются более чем на 45 %. Стоит отметить, что для стандартных шифров данный показатель составляет более 20 %.

На основании экспериментальных данных установлено, что наибольшее отличие между уровнями вклада главных компонент, полученными для открытого текста и зашифрованных сообщений на основе динамического хаоса при использовании режима OFB наблюдается при значении масштабного коэффициента *a,* равном 0,8, с

проведением процедуры «центрирование». Результаты представлены в табл. 1. При сравнении с сингулярным спектральным анализом модифицированный метод дает большее отличие между уровнями вклада второй главной компоненты открытого текста и зашифрованных сообщений на основе динамического хаоса при использовании режима OFB (более 18 % практически для всех рассматриваемых значениях итераций).

Таблица 1

Относительный уровень вклада второй главной компоненты зашифрованных сообщений при помощи алгоритма шифрования на основе динамического хаоса с использованием режима OFB

	Число итераций				
	64	128	256	512	1024
CCA	10,835	10,329	10,311	10,250	9,989
Модифицированный CCA	13,236	14,500	16,452	13,373	8,597

Для анализа алгоритмов шифрования на основе динамического хаоса при использовании режимов CFB и ECB было выбрано значение масштабного коэффициента *a*, равное 0,7. Полученные результаты приведены в табл. 2.

Как следует из полученных экспериментальных данных, относительный уровень вклада второй главной компоненты для случая использования CFB лежит в пределах от 0,39 до 0,49, что примерно соответствует результатам, полученным для алгоритма шифрования на основе динамического хаоса в режиме CBC (при числе итераций, большем 256) и алгоритмов des и aes. Для алгоритма шифрования на основе динамического хаоса в режиме ECB данный показатель лежит в пределах от 3,5 до 4, что свидетельствует о высоком уровне детерминизма в зашифрованных сообщениях.

Таблица 2

Относительный уровень вклада второй главной компоненты зашифрованных сообщений при помощи алгоритма шифрования на основе динамического хаоса с использованием режимов CFB и ECB

Режим шифрования	Число итераций				
	64	128	256	512	1024
CFB	0,487	0,396	0,397	0,458	0,429
ECB	3,696	3,252	4,012	3,556	3,892

Визуально для выявления детерминированных составляющих в исследуемых реализациях используется построение фазовых диаграмм (рис. 2). Для фазовых диаграмм, полученных для зашифрованных сообщений на основе динамического хаоса при применении режимов шифрования CBC и CFB, наблюдается «зашумленность». Данные фазовые диаграммы схожи по общей форме и структуре с построенными фазовыми диаграммами для алгоритмов aes и des. При использовании режимов OFB и ECB в фазовых диаграммах наблюдается высокая структурированность. Это также указывает на высокую степень детерминизма в зашифрованных сообщениях.

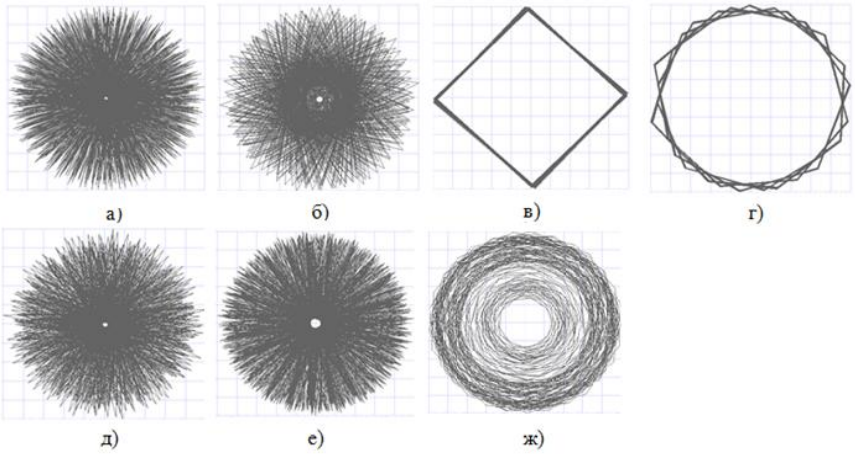


Рис. 2. Фазовые диаграммы пар собственных векторов с номерами 2 и 3, построенные для: зашифрованных сообщений при помощи алгоритма шифрования на основе динамического хаоса с использованием режимов CBC (*а*), CFB (*б*), ECB (*в*), OFB (*г*); алгоритма aes (*д*); алгоритма des (*е*); открытого текста (*ж*)

Выводы

Метод модифицированного сингулярного спектрального анализа позволяет проанализировать количественно (по уровню главных компонент) и качественно (в виде фазовых диаграмм) выходные последовательности алгоритма шифрования на основе динамического хаоса. Применение модифицированного метода позволяет выявить более чем на 20 % различия в показателях уровня вклада главных компонент входных и выходных последовательностей. Из фазовых диаграмм и результатов расчета уровня вклада второй главной компоненты можно заключить, что подходящими для шифрования являются алгоритмы на основе динамического хаоса с применением режимов шифрования CBC и CFB, в отличие от ECB и OFB, при применении которых выходные последовательности алгоритмов шифрования на основе динамического хаоса обладают значительной степенью детерминизма.

Библиографические ссылки

1. *Андреев В. В., Сапожникова Ю. В., Фомичев А. И.* Детерминированный хаос и кодирование информации // Прикладная информатика. 2009. № 6 (24). С. 80–85.
2. *Сидоренко А. В., Шакинко И. В., Мулярчик К. С.* О преобразовании методом сингулярного спектрального анализа зашифрованных на основе динамического хаоса последовательностей // Вестн. БГУ. Сер.1. 2012. № 3. С. 44–50.
3. *Борог, В. В., Крянев А. В., Удумян Д. К.* Комбинированный метод выявления скрытых аномалий в хаотических временных процессах // Фундаментальные физико-математические проблемы и моделирование технико-технологических систем. М. : Янус-К, 2009. В. 12. С. 536–546.
4. Основы криптографии. А. П. Алферов [и др.] М. : Гелиос АРВ, 2005.
5. *Смоленцев Н. К.* Основы теории вейвлетов. Вейвлеты в Matlab. М. : ДМКПресс, 2005.