УДК 621.396

Контроль фрактальной размерности динамического хаоса

Г.А. Валюк, А.В. Кондрашов, В.В. Перепеловский

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

Аннотация: рассмотрен инновационный метод преобразования псевдослучайной последовательности, основанной на системе уравнений Лоренца, с возможность управления значением фрактальной размерности. Решена задача оценки хаотичности и повышения фрактальной размерности для ограниченной последовательности изолированных псевдослучайных чисел (ИПСП). Под ИПСП понимается последовательность, элементы которой, разделены промежутками, в которых нет возможных псевдослучайных чисел (ПСЧ). Данные последовательности могут применяться для вторичного использования каналов связи, например, в стеганографии для выбора пикселя в фотографических изображениях. Измерение фрактальной размерности выполнялось методом сечения Пуанкаре. Управление фрактальной размерностью основано на методе нечетко заданного масштабирования.

Ключевые слова: вторичное использование каналов связи, детерминированный хаос, изолированные псевдослучайные числа, случайные числа, нечеткие множества, криптография, стеганография, FIPS-140, уравнения Лоренца.

1. Введение

Широкое применение последовательности псевдослучайных чисел, генерацию которых осуществляют специализированные алгоритмы, нашли в области шифрования [1]. В ряде работ исследовались возможности получения ПСП целых чисел [2,3]. В работе [4] выполнен анализ получения псевдослучайных последовательностей изолированных натуральных чисел (ИПСП). Такого рода последовательности применимы для выбора элементов множеств, нумеруемых целыми числами, например, при выборе пикселя в шифровании фотографических изображений. Однако этим спектр применения не ограничивается и для различных сфер деятельности требуются последовательности различной степени сложности в таких ситуациях появляется необходимость в использовании алгоритмов, позволяющих управлять значением фрактальной размерности.

В данной работе проведен численный анализ фрактальной размерности ИПСП на основе метода сечения Пуанкаре. Показана возможность увеличения фрактальной размерности решений уравнения Лоренца в режиме динамического хаоса.

2. Понятие ИПСП

Под последовательностью изолированных псевдослучайных чисел понимается последовательность, элементы которой, удалены одни от другого на промежутки R, в которых нет возможных псевдослучайных чисел. Параметр R будем называть радиусом изоляции. Под ограниченностью ИПСП понимается существование такого числа (min), которое определяет область наиболее вероятных значений ИПСП снизу, и существование такого числа (max), которое определяет область наиболее вероятных значений ИПСП сверху.

Процесс получения ИПСП изображенный на рис. 2 включает в себя три этапа, которым соответствует три различные последовательности. На первом этап требуется

получить ПСП, как результат решения N уравнений Лоренца -$\left\{\alpha_i^{(m)}\right\}$, где $m \in [0,1,..]$ - номер сета, под сетом будем понимать множество решений полученное за один шаг метода Эйлера; $i \in [1,2,...,3N]$ - номер ПСЧ в одном сете. Большинство элементов последовательности $\left\{\alpha_i^{(m)}\right\}$ находиться на расстояниях меньших R. $\left\{\beta_i^{(m_0)}\right\}$ - последовательность принадлежащая множеству вещественных чисел, большинство элементов этой последовательности находиться на расстоянии дальше R, т.е. являются изолированными элементами последовательности . $\left\{Q_i^{(m_0)}\right\}$ - последовательность, все элементы которой изолированы и принадлежат множеству натуральных чисел. Особенность финального этапа состоит в процессе задание мягких границ масштабирования множества $\left\{\beta_i^{(m_0)}\right\}$.

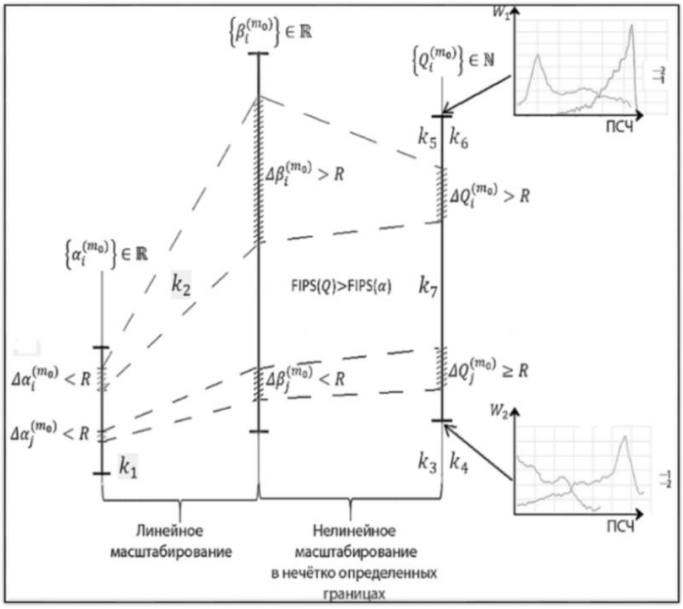

Рисунок 1. Преобразование псевдослучайной последовательности, основанной на системах уравнений Лоренца в ИПСП.

3. Численный анализ, фрактальная размерность ИПСП

Проведем оценку влияния преобразования ПСП в ИПСП опираясь на статистические тесты, а также значение фрактальной размерности.

В качестве набора статистических тестов был выбран алгоритм FIPS-140[5,6], поскольку он позволяет оценить надежность последовательности для дальнейшего ее применения в области шифрования данных и в некоторой степени ее хаотичность. Наиболее наглядных из набора является “Poker test”, результат которого для прохождения теста должен укладываться в диапазон от 1.03 до 57.4. По результатам проверки исходная ПСП получила 554, а ИПСП при двух различных распределениях максимальных и минимальных значений получила 13.29 и 12.89 соответственно. Основываясь на норме, которая согласно постулатам Голомба составляет 16.01, делаем вывод, что применение представленного в пункте 2 преобразования позволяет получить пригодную для использования в области шифрования псевдослучайную последовательность изолированных натуральных чисел.

Одним из главных параметров, используемых при работе со странными аттракторами является значение фрактальной размерности системы. Если рассматривать последовательность, получаемую системой уравнений Лоренца, то

значение фрактальной размерности составит 2.,06 [7]. На рис. 2 показано отображение Пуанкаре, выбор сечения проходит путем нахождения плоскости, которой соответствует максимальное число её пересечений с фазовой траекторией системы. Для аттрактора Лоренца справедливо правило, по которому значение размерности всего аттрактора равняется размерности полученной для отображения Пуанкаре с прибавление единицы. В результате расчета фрактальная размерность сечения составила 1.06, следовательно, размерность аттрактора 2.06.

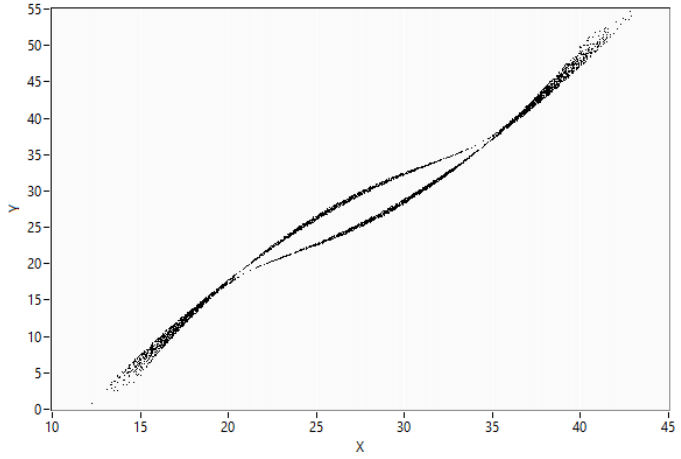

Рисунок 2. Отображение Пуанкаре аттрактора Лоренца. Фрактальная размерность отображения составляет 1.06.

В задачах пакетной передачи данных, требуется большее число ПСЧ [8]. Стоит учитывать тот факт, что для шифрования одного символа необходимо использовать 8 бит. Одним из способов решения такой задачи является использования нескольких систем уравнений динамического хаоса с различными коэффициентами и начальными условиями [9]. В таком случае целесообразно провести оценку влияния числа систем, используемых при генерации ПСП, на значение фрактальной размерности. По произведенным расчетам сделан вывод, что изменение числа систем Лоренца не оказывает влияния на значение фрактальной размерности, полученной ПСП, а именно во всех случаях фрактальная размерность равна 2.06.

Сделав вывод о том, что число используемых систем не оказывает влияние, можно оценить, влияние преобразования ПСП в ИПСП в нечетко заданных границах. Полученное сечение Пуанкаре для псевдослучайной последовательности изолированных натуральных чисел показано на рис. 3.

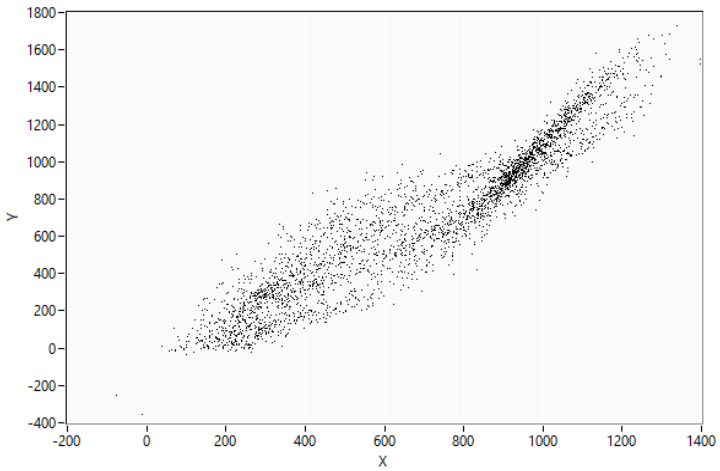

Рисунок 3. Отображение Пуанкаре, полученное для ИПСП. Фрактальная размерность отображения составляет 1,75.

В результате расчета значения фрактальной размерности для сечения Пуанкаре было получено значение 1.75. В таком случае значение размерности аттрактора составляет 2.75. Сравнив значения фрактальной размерности, полученные для ИПСП и исходной ПСП, а именно 2.75 и 2.06 соответственно, делаем вывод о повышении хаотичности системы в результате преобразования исходной последовательности в псевдослучайную последовательность изолированных натуральных чисел. Наиболее весомый вклад в повышение фрактальной размерности вносит масштабирование в нечетко заданных границах, которое так же позволяет управлять значение фрактальной размерности.

3. Заключение

Решена задача по реализации алгоритма для преобразования ПСП в ИПСП с возможность повышения и дальнейшего управления фрактальной размерностью системы. Значения фрактальной размерности, полученные для ИПСП и исходной ПСП равны 2.75 и 2.06 соответственно, что говорит о повышении хаотичности системы в результате преобразования исходной последовательности в псевдослучайную последовательность изолированных натуральных чисел. Преобразование позволило не только повысить хаотичность, но и получить хорошие результаты при прохождении статистических тестов FIPS-140, это означает, что полученную ИПСП можно надежно применять для шифрования данных.

Список литературы

1. Ünal Ç. et al. The design and implementation of hybrid RSA algorithm using a novel chaos based RNG // Chaos, Solitons & Fractals. – 2017. – Т. 104. – С. 655 – 667.
2. Lynnyk V. et al. Pseudo random number generator based on the generalized Lorenz chaotic system // IFAC-PapersOnLine. – 2015. –Т. 48. – С. 257 – 261.
3. Aleksandra V. et al. Adaptive chaotic maps and their application to pseudo-random numbers generation // Chaos, Solitons & Fractals. – 2020. – Т. 133. – С. 109615.
4. Валюк Г. А. и др. Масштабирование псевдослучайных последовательностей в нечетко определенных границах // Электроника и микроэлектроника СВЧ. – 2020. – Т. 1. – № 1. – С. 72-75.
5. NIST. Security requirements for cryptographic modules, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf>; 2002.
6. NIST. Security requirements for cryptographic modules, <2002.https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf>; 2019.
7. Divakar V. The fractal property of the Lorenz attractor // Physica D. – 2003. – Т. 190. – С. 115 – 128.
8. Гребенев М. С. и др. Передача двоичных данных на хаотически сформированных несущих частотах. // Известия высших учебных заведений России. Радиоэлектроника. – 2018. – Т. 5. – С. 5 – 12.
9. Kondrashov A. V. et al. Application of hyper-chaotic Lorenz system for data transmission» // Journal of Physics: Conference Series. – 2019. – Т. 1400. – С. 044033.