Министерство образования и науки Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

.

Кафедра компьютерной физики и метаматериалов
на базе Саратовского филиала
Института радиотехники и электроники
им. В. А. Котельникова РАН

ОТОБРАЖЕНИЕ ПЕКАРЯ: ТРАЕКТОРНЫЕ ОСОБЕННОСТИ И ПРИМЕНЕНИЕ В КРИПТОГРАФИИ

Автореферат
выпускной квалификационной бакалаврской работы
по направлению 03.03.02 «Физика»
студента 4 курса 432 группы
физического факультета
Семенова Антона Александровича

Научный руководитель –
д. ф.-м. н., профессор В. М. Аникин

Заведующий кафедрой –
д. ф.-м. н., профессор В. М. Аникин

Саратов 2018

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуализация проблемы. Разработка новых криптографических алгоритмов ведется постоянно в целях повышения надежности защиты пересылаемой по компьютерным цепям информации от несанкционированного доступа. Одним из направлений криптографии является хаотическая криптография, основанная, в частности, на использовании в процессе кодирования информации свойств хаотических отображений.

Основная идея кодирования информации на базе хаотических отображений заключается в получении кода для передаваемой единицы информации в результате определенного числа повторений итераций отображения. В рассматривается двумерное отображение – отображение пекаря; название отображению дал Эберхард Хопф, который отметил что повторные итерации отображения напоминают приготовление слоеного теста.

Целью выпускной квалификационной работы является аналитическое и численное выявление траекторных особенностей двумерного дискретного, сохраняющего меру отображения пекаря, способствующие его использованию в криптографических схемах. Под траекторными особенностями отображения пекаря мы будем понимать его обратимость, возможность соотнесения с авторегрессионной системой, циклические траектории отображения.

Задачи. Изучение и трактовка траекторных свойств отображения пекаря, а также построение алгоритм его использования как ядра хаотической схемы кодирования информации для защиты от несанкционированного доступа к ней.

Структура работы. Работа включает введение, три главы, заключение, список использованных источников.

СОДЕРЖАНИЕ РАБОТЫ

В главе 1 изучаются трансформационные особенности отображения пекаря. Вводится система разностных уравнений, определяющая отображение, отмечается свойство хаотического перемешивания, представление итераций в двоичной системе; рассчитываются периодические орбиты отобра-

жения пекаря, демонстрируется «зеркальная» обратимость отображения пекаря.

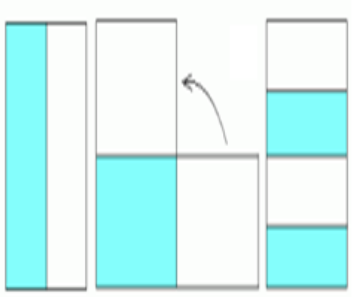
В главе 2 на базе свойств отображения, рассмотренных в главе 2, предлагается алгоритм кодирования информации на базе отображения пекаря, его компьютерная реализация и статистический анализ. В главе 3 выводится уравнение Фробениуса-Перрона и находится его решение относительно инвариантной плотности этого отображения.

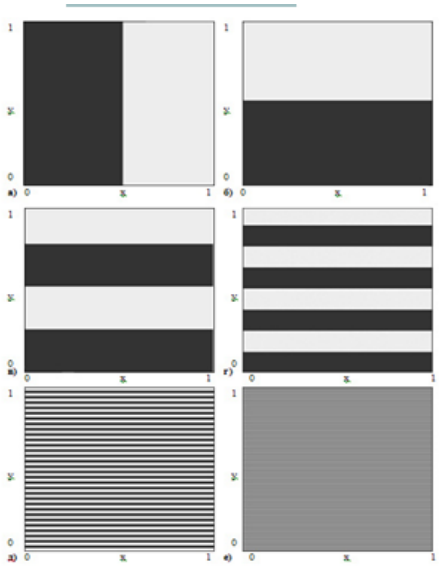
Отображение пекаря

$$x_{n+1} = 2x_n, \quad y_{n+1} = \frac{y_n}{2}, \qquad 0 \le x_n < 1/2$$

$$x_{n+1} = 2x_n - 1, \quad y_{n+1} = \frac{y_n + 1}{2}, \quad 1/2 \le x_n \le 1.$$

Перемешивание при первых двух итерациях отображения пекаря





Отражение процесса перемешивания в процессе итераций отображения пекаря

Отображение пекаря в двоичной записи

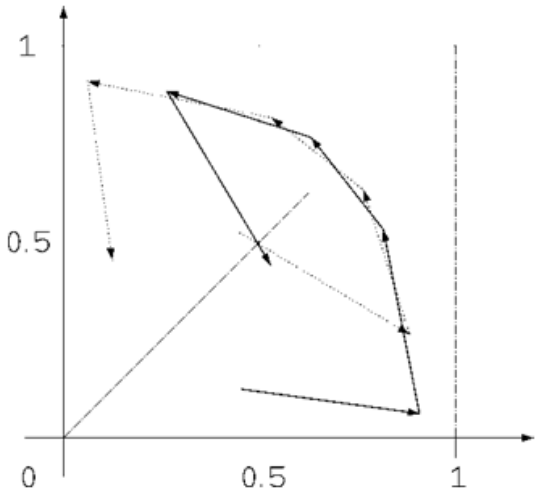
$$x_{n+1} = 2x_n \mod 1 = \{2x_n\}, \; 0 \le x_n \le 1. \qquad y_{n+1} = \frac{1}{2}y_n + \frac{1}{2}\lfloor 2x_n \rfloor$$

$$x_0 = 0.\beta_1\beta_2\ldots\beta_n\ldots = \sum_{p=1}^{\infty}\frac{\beta_p}{2^p} \qquad y_0 = 0.\gamma_1\gamma_2\ldots\gamma_n\ldots = \sum_{p=1}^{\infty}\frac{\gamma_p}{2^p}$$

$$x_n = \{2^n x_0\} = \sum_{p=1}^{\infty}\frac{\beta_{n+p}}{2^p} \qquad y_{n+1} = \frac{y_n}{2} + \frac{1}{2}\beta_{n+1}$$

$$y_n = \frac{1}{2^n}y_0 + \frac{1}{2^{n+1}} \otimes \beta_n = \sum_{p=1}^{\infty}\frac{\gamma_p}{2^{p+n}} + \sum_{p=0}^{n}\frac{\beta_p}{2^{n+1-p}} = 0.\beta_n\beta_{n-1}\beta_{n-2}\ldots\beta_2\beta_1\gamma_1\gamma_2\ldots$$

Обратимость отображения пекаря



$$x_n = \{Gx_{n+1}\}$$

$$y_n = \frac{y_{n+1} + \beta_{n+1}}{G}.$$

Графическое представление прямых (сплошная жирная линия) и обратных (пунктирная светлая линия) итераций отображения пекаря: начальная и конечная точки симметричны относительно диагонали квадрата

Особенности схемы кодирования сообщений на основе отображения пекаря определяются выше свойствами этого отображения. Во-первых, отображение обладает, по существу, единственной компонентой, «ответственной» за хаос (это сдвиг Бернулли, реализуемый по координате *x*). Во-вторых, инвариантным распределением отображения является равномерное распределение. Названные два свойства ценны для процесса шифрования дискретного сигнала. На стадии расшифровки переданного сообщения оказывается незаменимым такое свойство отображения, как его обратимость.

Полезную информацию мы передаем начальному значению по координате *y*. В принципе, в качестве другой координаты – координаты $x_0^{(k)}$ можно взять любое значение, равномерным образом выбранное из единичного интервала. Если теперь осуществить процесс итераций на основе отображения пекаря, состоящий из $m^{(k)}$ шагов, то оба начальных значения $(x_0^{(k)}, y_0^{(k)} = s_k)$, естественно, претерпят соответствующие изменения, причем траектория точки будет заполнять единичный квадрат. При этом эта траектория в среднем не будет посещать различные области квадрата с примерно одинаковой веро-

ятностью. Остановив процесс итераций через $m^{(k)}$ шагов, переходим к преобразованиям следующей пары координат $(x_0^{(k+1)}, y_0^{(k+1)} = s_{k+1})$, осуществляемой в процессе $m^{(k+1)}$ шагов. Данная процедура повторяется n раз, по числу дискретных отсчетов в шифруемой последовательности. В силу обратимости отображения в указанном выше смысле, зная количество проделанных итераций, можно восстановить каждую стартовую пару.

ЗАКЛЮЧЕНИЕ

Среди двумерных отображений, сохраняющих площадь, особая роль принадлежит так называемому «отображению пекаря» (baker transformation). Введенное впервые в 1934 г. Э. Хопфом, это отображение стало классическим образцом эргодического (обладающего инвариантной плотностью) и перемешивающего (имеющего инвариантную плотность пределом нестационарных распределений – решений оператора Перрона–Фробениуса) отображения. Интересны приложения отображения пекаря к конкретным задачам моделирования, возникающим в естественных науках. С помощью цепочки связанных отображений пекаря моделировались такие физико-химические процессы, как изомеризация (три связанных отображения пекаря), диффузия и хаотическое рассеяние (бесконечная цепочка отображений пекаря), явление перемежаемости, хаотическая адвекция в двухкомпонентных авто- каталитических химических реакциях. Свое применение отображение пекаря (в ряду некоторых других двумерных отображений) нашло в послед- нее время при решении криптографических задач. Связано это с тем, что благодаря свойству перемешиваемости отображение пекаря в процессе итераций быстро нивелируют особенности полезного дискретного и квантованного сигнала, который выступает в качестве начального значения для «сжимающей» координаты этого преобразования. Двумерное распределение при этом, в силу ярко выраженных хаотических свойств «растягивающей» (бернуллиевой) компоненты отображения, «релаксирует» к равномерному. Конкретно эти свойства находят отражение в следующих заключениях:

1. «Сжимающая координата y_n на каждом шаге итераций выражается двоичной дробью, первыми n разрядами которой являются записанные в об-

ратном порядке n первых разрядов стартового значения x_0 «растягивающей» координаты, а последующие позиции занимают двоичные разряды стартового значения y_0.

2. С каждой итерацией, последовательность разрядов, отвечающих y_0, в представлении для y_n сдвигается вправо на одну позицию.

3. В асимптотике (при $n \to \infty$) главную роль в формировании значения y_n играют первые n разрядов начального значения x_0; «ценность» (значимость) же разрядов начального значения y_0 самой «сжимающей» координаты в представлении y_n «утрачивается».

4. Установившийся стационарный режим пары (x_n, y_n) можно принимать как стационарный режим авторегрессионной системы, не зависящий от распределения начального условия y_0.

На основе статистического анализа результатов кодирования числовой информации на базе отображения пекаря можно сделать следующие выводы:

1) равномерность численных значений выходного сигнала зависит от числа итераций, что может быть связано с наличием машинных ошибок округления результатов и переходом на периодические орбиты;

2) для исключения эффектов машинной арифметики может быть предложено использование иных модификаций отображения пекаря – вместо двоичного сдвига Бернулли, согласно которому изменяется координата x , использовать иные кусочно-линейные отображения (с различным числом и направлением ветвей при сохранении модуля тангенса наклонов этих ветвей);

3) с той же целью может быть предложена разработка алгоритмов по принципам безошибочной машинной арифметики (работа с целыми числами) [18];

4) таким образом, дальнейшее исследование алгоритма кодирования числовой информации на базе двумерного консервативного перемешивающего отображения пекаря представляется целесообразным.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Табор М.* Хаос и интегрируемость в нелинейной динамике. М. : Эдиториал УРСС. 2001. 320 с.

2. *Аникин В. М., Голубенцев А. Ф.* Аналитические модели детерминированного хаоса. М. : ФИЗМАТЛИТ, 2007. 328 с.

3. *Хопф Э.* Эргодическая теория // УМН. 1949. Т. 4, вып. 1 (29). С. 113–182.

4. *Голубенцев А. Ф., Аникин В. М., Ноянова С. А.* Модификация отображения пекаря: особенности асимптотического поведения // Изв. вузов. Прикладная нелинейная динамика. 2004. Т. 12, № 3. С. 45 – 57.

5. *Аникин В.М., Василенко Л.П., Ремизов А.С., Чебаненко С.В.* Алгоритм шифрования произвольных данных на основе трехмерного аналога хаотического отображения «Кот Арнольда» // Компьютерные науки и информационные технологии: Материалы межд. научной конф. Саратов, Россия, 1-4 июля 2012 г. Саратов: Издат. Центр «Наука», 2012. С. 29-31.

6. *Аникин В.М., Ноянова С.А., Чебаненко С.В.* Кодирование информации на базе отображения пекаря // Гетеромагнитная электроника. 2012. Вып. 12. С. 52 – 60.

7. *Gaspard P.* Diffusion, Effusion and Chaotic Scattering: An Exactly Solvable Liovillia Dynamics // J. Stat. Phys.1992.Vol 68, Nos 5/6. Pp. 673-747.

8. Kaufman Z., Szépfalusy P. Transient chaos and critical states in generalized baker map // J. Stat. Phys. 2000. V. 101. Nos. 1/2. Pp. 107-124.

9. Toroczkai Z., Károlyi, Péntek Á., Tél T. Autocatalytic reactions in systems with hyperbolic mixing exact results for active Baker map // J. Phys. A: Math. Gen. 2001. V. 34. Pp. 5215-5235.

10. Chernoff D. F., Barrow J. D. Chaos in the Mixmaster Universe // Phys. Rev. Letters. 1983. V.50. No. 2. Pp. 134-137.

11. Tracy M. M., Scott A. J. The classical limit for a class of quantum baker's maps // J. Phys. A: Math. Gen. 2002. V. 35. Pp. 8341-8360.

12. Годунов С.К., Антонов А.Г., Кирилюк О.П., Костин В.И. Гарантированная точность решения систем линейных уравнений в евклидовых пространствах. – Новосибирск: Наука, 1988.

13. *Рабинер Л., Гоулд Б.* Теория и применение цифровой обработки сигналов. М. : Мир, 1978. 848 с.

14. *Морозов А. В., Пирожков М. А.* Отображение пекаря и его траектории // Актуальные проблемы гуманитарных и естественных наук. 2017. № 4–6. С. 7–13.

15. *Lasota A., Mackey M.C.* Probabilistic properties of deterministic systems. Cambridge: Cambridge University Press, 1985.

16. *Аникин В. М., Аркадакский С.С., Ремизов А. С.* Несамосопряженные операторы в хаотической динамике. Саратов: Изд-во Сарат. ун-та, 2015. 96 с.

17. *Грегори Р., Кришнамурти Е.* Безошибочные вычисления. Методы и приложения. М. : Мир, 1988. 208 с.