ФРАКТАЛЫ И ЗАЩИТА ИНФОРМАЦИИ

А.Ю. Лабинский, кандидат технических наук, доцент;
А.В. Ильин.
Санкт-Петербургский университет ГПС МЧС России

Рассмотрены возможности использования теории фракталов для защиты информации. Приведены основные особенности классических фракталов и возможности фрактального подхода для кодирования информации и создания фрактальных систем связи.

Ключевые слова: фрактал, самоподобие, кодирование информации, моделирование

FRACTALS AND INFORMATION PROTECTION

A.Yu. Labinskiy; A.V. Ilyin.
Saint-Petersburg university of State fire service of EMERCOM of Russia

This article presents the special feature of fractals theory for information protection. Presents the possibility of the classical fractals for information encode and development the fractals connection systems.

Keywords: fractal, self-similarity, information encode, modelling

Деятельность органов управления МЧС России происходит в сложной обстановке воздействия различных факторов. При этом особую важность приобретают вопросы защиты информации. Сфера высоких технологий не оставляет без внимания это направление обеспечения устойчивого функционирования современных систем управления. Современный подход к решению вопросов защиты информации заключается в использовании фрактальной концепции, которая заняла прочное место во многих областях естествознания, но только в последнее время она стала очевидной для актуальных задач защиты информации и создании защищенных систем связи. В основе такого применения теории фракталов лежат принципиально новые методы фрактального разбиения и геометрического кодирования информации, а также использования в качестве носителей информации помехозащищенных сигналов с фрактальными спектрами.

Фракталы. Основные понятия

Многие природные системы настолько сложны и нерегулярны, что использование известных объектов классической геометрии для их моделирования представляется безнадежным. Это такие объекты, как, например, модель горного хребта или крона дерева. Часто наблюдается в природе бесконечное повторение одного и того же узора, увеличенного или уменьшенного во много раз. Это относится как к структуре горного хребта, так и к кроне дерева. Так проявляется характерное для фракталов свойство самоподобия.

Шведский ученый Бенуа Мандельброт в 1975 г. ввел в употребление термин «фрактал», основываясь на теории фрактальной (дробной) размерности немецкого ученого Ф. Хаусдорфа, предложенной в 1919 г.

Рассмотрим так называемые «классические фракталы» [1]. Разделим отрезок прямой на N равных частей. Тогда каждую часть можно считать копией всего отрезка, уменьшенной в 1/R раз. Очевидно, что данные модели N и R связаны соотношением: $N*R=1$. Если квадрат разбить на N квадратов с площадью, в $1/R^2$ раз меньше исходной, то соотношение между N и R будет иметь вид: $N*R^2=1$. Если куб разбить на N равных объемов, в $1/R^3$ раз меньше исходного объема, то соотношение между N и R будет иметь вид: $N*R^3=1$. Здесь R – коэффициент подобия.

Размерность подобия D объекта во всех рассмотренных выше случаях появляется как степень числа R, а именно: $N*R^D=1$. В этих случаях размерность D является целым числом. Если размерность D является не целой, а дробной (фрактальной), то получаемое множество объектов называют самоподобным фракталом.

Величину фрактальной (дробной) размерности можно найти из выражения: D=log(N)/log(1/R). Здесь логарифм может быть по любому положительному основанию, отличному от единицы (десятичный, натуральный и т.п.).

Более общий тип самоподобных фракталов является объединением непересекающихся подмножеств, полученных масштабированием оригинала, но коэффициенты подобия уже не обязательно одни и те же для всех подмножеств.

1. Снежинка Г. Коха.

Граница снежинки, придуманной Г. Кохом в 1904 г., описывается кривой, составленной из трех одинаковых фракталов размерности:

$$N=4,\ R=1/3,\ D=\log(4)/\log(3)\approx 1{,}2618.$$

Каждая треть снежинки строится итеративно, начиная с одной из сторон равностороннего треугольника (рис. 1).

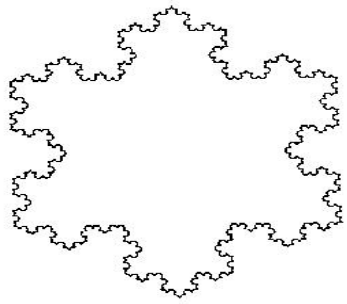

Рис. 1

2. Ковер В. Серпинского.

Еще один пример простого самоподобного фрактала – ковер В. Серпинского (польский математик Вацлав Серпинский, 1915 г.). Ковер представляет собой объединение N=3 существенно непересекающихся уменьшенных в два раза копий. Коэффициент подобия R=1/2, размерность фрактала D=log(3)/log(2)≈1,585. Суммарная площадь треугольных частей, выкинутых при построении, в точности равна площади исходного треугольника (рис. 2).

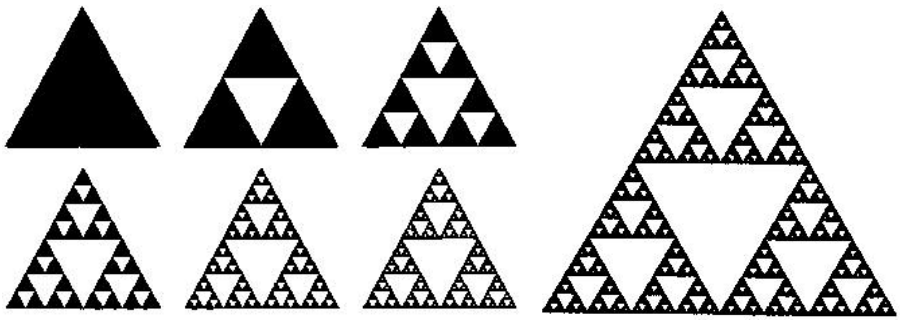

Рис. 2

3. Губка К. Менгера (рис. 3).

Рис. 3

Пример трехмерного аналога ковров, называемых губками, является губкой немецкого математика Карла Менгера. Это самоподобный фрактал с N=20 и R=1/3. Его размерность равна: D=log(20)/log(3)≈2,7268.

Теория итерированных функций является составной частью общей теории динамических систем. Замечательным свойством алгоритмов, основанных на теории систем итерированных функций, является то, что их результат, называемый аттрактором, не зависит от выбора начального множества или начальной точки. В общем случае для построения системы итерированных функций нужно использовать совокупность сжимающих отображений вида: T_1 с коэффициентом сжатия $S_1<1$; T_2 с коэффициентом сжатия $S_2<1$; T_m с коэффициентом сжатия $S_m<1$, действующих в n-мерном пространстве.

Таким образом, системой итерированных функций (СИФ) называют совокупность отображений вместе с итерационной схемой: E_0 – компактное произвольное множество, $E_1=T(E_0)$, $E_2=T(E_1)$,…., $E_n=T(E_{n-1})$.

Основная задача теории СИФ – выяснить, когда СИФ порождает предельное множество E: $E=Lim_{n\to\infty}E_n$. Если предел существует, то множество E называют аттрактором СИФ, причем аттрактор часто оказывается фрактальным множеством.

Имеется два подхода к реализации СИФ: детерминированный алгоритм (ДСИФ) и рандомизированный алгоритм (РСИФ). ДСИФ требует хранения и обработки сравнительно больших массивов информации. В РСИФ нет необходимости хранить большие массивы данных в памяти, но для получения изображения приемлемого качества требуются тысячи точек (пикселов).

Процесс построения ковра В. Серпинского с использованием алгоритма ДСИФ представлен на рис. 4.

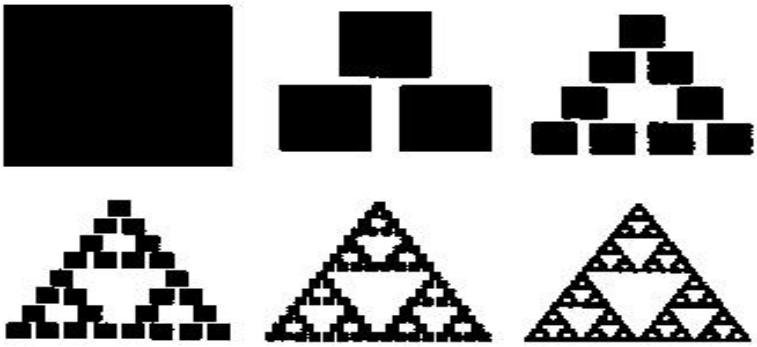

Рис. 4

Для вывода достаточно качественных фрактальных изображений необходимо создание графического окна с размерами не менее 256*256 пикселей. Когда размер изображения зафиксирован, нужно произвести преобразование мировых координат в экранные и найти эквиваленты аффинных отображений для заданного графического окна.

В процессе расчетов с использованием ДСИФ какая-либо точка изображения может выйти за пределы заданного графического окна, что может привести к аварийной остановке программы. Поэтому в процессе вычислений нужно проверять координаты новых точек изображения.

Фракталы широко используются в различных отраслях науки и техники. В физике фракталы естественным образом возникают при моделировании нелинейных процессов, таких как турбулентное течение жидкости, сложные процессы диффузии-адсорбции, пламя, облака и тому подобное. Фракталы используются при моделировании пористых материалов, например, в нефтехимии. В биологии они применяются для моделирования популяций и для описания систем внутренних органов (система кровеносных сосудов). После создания кривой Г. Коха было предложено использовать ее при вычислении протяженности береговой линии.

Радиотехника. Фрактальные антенны [2].

Использование фрактальной геометрии при проектировании антенных устройств было впервые применено американским инженером Натаном Коэном, который тогда жил в центре г. Бостона, где была запрещена установка внешних антенн на здания. Коэн Н. вырезал из алюминиевой фольги фигуру в форме кривой Г. Коха и наклеил ее на лист бумаги, затем присоединил к приемнику. Коэн Н. основал собственную компанию и наладил серийный выпуск фрактальных антенн.

Информатика. Сжатие изображений [3].

Существуют алгоритмы сжатия изображения с помощью фракталов. Они основаны на идее о том, что вместо самого изображения можно хранить сжимающее отображение, для которого это изображение (или некоторое близкое к нему) является неподвижной точкой. Один из вариантов данного алгоритма был использован фирмой Microsoft при издании своей энциклопедии, но большого распространения эти алгоритмы не получили.

Компьютерная графика [4].

Фракталы широко применяются в компьютерной графике для построения изображений природных объектов, таких как деревья, кусты, горные ландшафты, поверхности морей и так далее. Существует множество программ, служащих для генерации фрактальных изображений.

Экономика и финансы [5].

Алмазов А.А. в своей книге «Фрактальная теория. Как поменять взгляд на рынки» предложил способ использования фракталов при анализе биржевых котировок, в частности – на рынке Форекс.

Фракталы. Защита информации

Децентрализованные сети [6].

Система назначения IP-адресов в децентрализованной сети Интернет использует принцип фрактального сжатия информации для компактного сохранения информации об узлах сети. Каждый узел такой сети хранит всего 4 Кб информации о состоянии соседних узлов, при этом любой новый узел подключается к общей сети без необходимости в центральном регулировании раздачи IP-адресов, что, например, характерно для сети Интернет. Таким образом, принцип фрактального сжатия информации гарантирует полностью децентрализованную, а, следовательно, максимально устойчивую работу всей сети.

Кодирование информации [7].

Кодирование информации, основанное на выделении фракталов (самоподобных элементов). Фрактальное разбиение и геометрическое кодирование при защите конфиденциальности информации – новый подход к созданию методов шифрования информации, позволяющий создать быстродействующие аппаратные кодеры и декодеры.

Предложены методы кодирования информации в информационно-управляющих системах с применением теории фракталов, основанные на возможности использования геометрического кодирования символьной информации. Эти методы дают новый подход обеспечения конфиденциальности информации.

Фрактальные системы связи [8].

Фрактальные системы связи (ФСС) используют в качестве носителей информации помехозащищенные сигналы с фрактальными спектрами. Фрактальными являются такие сигналы, спектры которых имеют самоподобную структуру, задаваемую множеством Г. Кантора.

Разработанная система предназначена для передачи информации как по кабельным линиям с помощью фрактальных видеосигналов, так и по эфиру, с использованием несущей частоты, промодулированной сигналами с фрактальными спектрами различных видов. Разработаны передатчик (генератор), приемник и антенное оборудование, предназначенные для использования в ФСС.

Становление теории фракталов – яркий пример развития нового направления науки, основанного как на достижениях в абстрактной области математики, так и на прикладных исследованиях в различных областях, в том числе в области защиты информации. Новые идеи и методы позволяют использовать в целях защиты информации такие новые системы и технологии, как децентрализованные сети с фрактальным сжатием информации, фрактальное разбиение и геометрическое кодирование информации и фрактальные системы связи.

Литература

1. Кроновер Р. Фракталы и хаос в динамических системах. М.: Техносфера, 2006.

2. Гарднер М. От мозаик Пенроуза к надежным шифрам. М.: Мир, 1993.

3. Кренкель Э.Т. Сжатие сигналов с применением теории фракталов. М.: ТУСИ, 1996.

4. Шредер М. Фракталы, хаос, степенные законы. М.: Мир, 2000.

5. Алмазов А.А. Фрактальная теория. Как поменять взгляд на рынки. М.: МФА, 2005.

6. Гуляев Ю.В., Никитов С.А., Матвеев Е.Н. Фракталы в новых средах передачи информации. М.: МФТИ, 2003.

7. Агафонов Т.Б. Защита ценной информации в компьютерных сетях // Автоматизированные системы контроля и управления. 2009. Вып. 6.

8. Болотов В.Н. Фрактальная система связи // Журнал технической физики. 2008. Вып. 9.