УДК 519.7+681.3

©2010. **В.Г. Скобелев, Н.А. Шереметьева**

АНАЛИЗ ХАРАКТЕРИСТИК КОНСТРУКТИВНОГО ПСЕВДОФРАКТАЛА

Решена задача анализа динамики построения черно-белого изображения конструктивного псевдофрактала на абстрактном экране размера $n \times n$. Разработан метод оценки количества пикселей, добавляемых в изображение псевдофрактала на каждой итерации процедуры его построения, а также метод оценки числа итераций при построении изображения псевдофрактала. Рассмотрена детализация предложенных методов для H-псевдофрактала.

Ключевые слова: *конструктивные псевдофракталы, абстрактный экран, шифры.*

Введение. В последнее время интенсивно развивается направление, связанное с применением хаотических динамических систем [1] при решении задач преобразования информации. Важным классом таких систем являются фракталы [2,3]. Наличие самоподобного (или почти самоподобного) множества делает весьма привлекательным применение фракталов при построении вычислительно стойких шифров. Предложенные в [4-7] шифры основаны на использовании динамического фрактала, который характеризуется тем, что его изображение в метрическом пространстве $\mathbf{R}^2$ строится в соответствии со следующей бесконечной рекурсивной процедурой:

$$\begin{cases} x_{n+1} = f_1(x_n, y_n) \\ y_{n+1} = f_2(x_n, y_n) \end{cases} \quad (n \in \mathbf{N}),$$

где f_i $(i = 1, 2)$ – целые или рациональные отображения.

Кроме динамических фракталов существует широкий класс конструктивных (или геометрических) фракталов, характеризуемых заданием двух множеств: основы и фрагмента (повторяющегося при каждом уменьшении масштаба). Известны, по крайней мере, три бесконечные рекурсивные процедуры построения изображения конструктивного фрактала:

1) метод решета, состоящий в том, что текущее состояние основы разбивается на части, подобные ее исходному состоянию; из каждого блока этого разбиения удаляются части, подобные фрагменту; а те точки основы, которые не удаляются в результате этой процедуры, образуют фрактал;

2) в предположении, что основа и фрагмент – ломаные линии (отрезки которых не пересекаются во внутренних точках), строится основа, а затем каждое звено заменяется ломаной, подобной фрагменту;

3) в предположении, что основа и фрагмент построены из отрезков, к каждой концевой точке (т.е. точке, не лежащей внутри ни одного из уже построенного отрезка), построенной на последней итерации, пристраивается подобная фрагменту фигура, повернутая на заданный угол.

Последняя процедура дает возможность при построении изображения конструктивного фрактала реализовать механизм случайности (за счет случайного выбора направления каждого поворота), что существенно расширяет множество конструктивных фракталов.

Если при построении изображения фрактала (динамического или конструктивного) ограничиться конечным числом итераций применяемой рекурсивной процедуры, то полученное изображение представляет собой псевдофрактал. Предложенная в [6,7] схема нестационарного поточного шифра использует именно псевдофракталы и состоит в следующем.

С помощью вычислений в кольце $\mathsf{Z}_{256} = (\mathbf{Z}_{256}, \oplus, \circ)$ (где $a \oplus b = a + b(mod\, 256)$, $a \circ b = ab(mod\, 256)$) строится семейство легко-вычислимых перестановок

$$\begin{cases} r_n = r_0 \oplus n \circ (\alpha_1^n \circ a_1 \ominus \alpha_2^n \circ a_2 \ominus \alpha_3^n \circ a_3) \\ g_n = g_0 \oplus n \circ (\alpha_2^n \circ a_2 \ominus \alpha_1^n \circ a_1 \ominus \alpha_3^n \circ a_3) \\ b_n = b_0 \oplus n \circ (\alpha_3^n \circ a_3 \ominus \alpha_1^n \circ a_1 \ominus \alpha_2^n \circ a_2) \end{cases} \tag{1}$$

множества $\mathbf{Z}_{256}^3$ ($\ominus$ – операция, обратная к $\oplus$). Очередной фрагмент исходной двоичной последовательности интерпретируется как 24-разрядный (т.е. цветной) bmp-файл. Шифрование состоит в изменении цвета (r_0, g_0, b_0) i-го пикселя ($i = 1, 2, \dots$) bmp-файла цветом (r_n, g_n, b_n), вычисленным в соответствии с (1) (параметры $\alpha_r, a_r \in \mathbf{Z}_{256}$ ($r = 1, 2, 3$) – секретный сеансовый ключ), где $n = \bigoplus_{j=1}^{i} n_j$, а n_j равно 1, если j-й пиксель экрана не содержит точку псевдофрактала и равно увеличенному на 1 номеру итерации, на которой этот пиксель становится точкой псевдофрактала, в противном случае. Отметим, что вычислительная стойкость обобщения семейства перестановок (1) на случай множества $\mathbf{Z}_{p^k}^m$ (p – простое число) исследована в [8], а соответствующее обобщение данного подхода к построению нестационарных поточных шифров систематически изложено в [9].

Вычислительная стойкость рассмотренного нестационарного поточного шифра существенно зависит от множества используемых псевдофракталов, черно-белые изображения которых представлены библиотекой массивов, каждый из которых содержит числа n_j ($j = 1, 2, \dots$), вычисленные для соответствующего псевдофрактала. Отсюда вытекает актуальность формального исследования структуры этих массивов, как неотъемлемой части математического анализа вычислительной стойкости рассмотренных шифров. Цель настоящей работы и состоит в разработке такого математического аппарата в случае, когда изображение конструктивного псевдофрактала строится в соответствии с третьей рекурсивной процедурой.

1. Постановка задачи. Длиной отрезка назовем количество содержащихся в нем пикселей. Предполагается, что:

1) изображение конструктивного псевдофрактала F строится на абстрактном экране размера $n \times n$ в соответствии с третьей рекурсивной процедурой, причем число итераций процедуры больше, чем 2;

2) все отрезки основы имеют длину h_1, а все отрезки фрагмента – длину h_2;

3) при добавлении части псевдофрактала F, подобной фрагменту, поворот не изменяет длину отрезка;

4) любая добавляемая часть псевдофрактала F имеет с уже построенной частью единственную общую точку – концевую точку, построенную на предыдущей итерации, к которой она пристраивается;

5) построение изображения завершается, если длина добавляемого отрезка не превосходит единицы.

В предположении, что основа размещается в центре экрана, а для каждой итерации, начиная с третьей, длина любого добавляемого отрезка определяется коэффициентом уменьшения ω $(0 < \omega < 1)$, оценим число итераций при построении изображения псевдофрактала F, а также количество элементов массива M_F, представляющего псевдофрактал F, имеющих одно и то же значение (такая характеристика является основой исследования динамики семейства перестановок (1) при псевдослучайном выборе очередного элемента массива M_F).

2. Основные результаты. Пусть основа состоит из m_1 отрезков, а фрагмент из m_2 отрезков. Обозначим через a_1 и a_2 количество пикселей основы и фрагмента, а через b_1 и b_2 количество концевых точек основы и фрагмента. Верхние и нижние оценки этих чисел определяются, соответственно, попарно непересекающимися отрезками и замощением плоскости треугольниками (возможно с одним висячим отрезком) и, поэтому, имеют следующий вид:

$$m_i h_i - 3\lfloor 0.5(m_i - 1)\rfloor - 1 + \mathtt{sign}(m_i - 2\lfloor 0.5 m_i\rfloor) \le a_i \le m_i h_i \ \ (i = 1, 2), \tag{2}$$

$$\lfloor 0.5(m_i + 1)\rfloor + 2 - \mathtt{sign}(m_i - 2\lfloor 0.5 m_i\rfloor) \le b_i \le 2m_i \ \ (i = 1, 2). \tag{3}$$

Пусть x_j $(j = 1, 2, \dots)$ – количество пикселей, добавляемых в изображение псевдофрактала F на j-й итерации.

Теорема 1. *При построении изображения псевдофрактала F на абстрактном экране размера $n \times n$ истинны неравенства:*

$$m_1 h_1 - 3\lfloor 0.5(m_1 - 1)\rfloor - 1 + \mathtt{sign}(m_1 - 2\lfloor 0.5 m_1\rfloor) \le x_1 \le m_1 h_1, \tag{4}$$

$$\begin{gathered} x_j \ge (\lfloor 0.5(m_1 + 1)\rfloor + 2 - \mathtt{sign}(m_1 - 2\lfloor 0.5 m_1\rfloor))(\lfloor 0.5(m_2 + 1)\rfloor + 2 - \\ -\mathtt{sign}(m_2 - 2\lfloor 0.5 m_2\rfloor) - 1)^{j-2}(m_2(\omega^{j-2} h_2 - S_{j-2}) - 3\lfloor 0.5(m_2 - 1)\rfloor + \\ +\mathtt{sign}(m_2 - 2\lfloor 0.5 m_2\rfloor) - 2), \end{gathered} \tag{5}$$

где $S_2 = 0$ и

$$S_{j-2} = \frac{1 - \omega^{j-2}}{1 - \omega} \ \ (j = 3, 4, \dots), \tag{6}$$

$$x_j \le 2m_1(2m_2)^{j-2}(m_2 \omega^{j-2} h_2 - 1) \ \ (j = 2, 3, \dots). \tag{7}$$

Доказательство. Рассмотрим 1-ю итерацию. Так как $x_1 = a_1$, то из (2) при $i = 1$ вытекают неравенства (4).

Рассмотрим 2-ю итерацию. Количество концевых точек, полученных на 1-й итерации, равно b_1, а каждый фрагмент добавляет $a_2 - 1$ пиксель. Следовательно, $x_2 = b_1(a_2 - 1)$. Воспользовавшись неравенствами (2) и (3), получим

$$(\lfloor 0.5(m_1+1)\rfloor + 2 - \mathtt{sign}(m_1 - 2\lfloor 0.5m_1\rfloor))(m_2h_2 - 3\lfloor 0.5(m_2-1)\rfloor +$$
$$+\mathtt{sign}(m_2 - 2\lfloor 0.5m_2\rfloor) - 2) \le x_2 \le 2m_1(m_2h_2 - 1),$$

т.е. неравенства (5) и (7) истинны при $j = 2$.

Рассмотрим j-ю итерацию ($j = 3, 4, \dots$). Длина l_j каждого отрезка добавляемой на j-й итерации фигуры, подобной фрагменту, определяется равенством

$$l_j = \lfloor \underbrace{\omega \lfloor \dots \lfloor \omega}_{j-2} h_2 \rfloor \dots \rfloor \rfloor. \tag{8}$$

Из (8) вытекает, что

$$\omega^{j-2}h_2 - S_{j-2} < l_j \le \omega^{j-2}h_2, \tag{9}$$

где S_{j-2} определяется равенством (6).

Из (2) и (9) вытекает, что на j-й итерации количество пикселей c_j, которые добавляет в изображение псевдофрактала F одна фигура, подобная фрагменту, удовлетворяет неравенствам

$$m_2(\omega^{j-2}h_2 - S_{j-2}) - 3\lfloor 0.5(m_2-1)\rfloor +$$
$$+\mathtt{sign}(m_2 - 2\lfloor 0.5m_2\rfloor) - 2 < c_j \le m_2\omega^{j-2}h_2 - 1. \tag{10}$$

Количество d_{j-1} концевых точек, добавленных на $(j-1)$-й итерации, удовлетворяет неравенствам

$$b_1(b_2-1)^{j-2} \le d_{j-1} \le b_1 b_2^{j-2} \ \ (j = 3, 4, \dots). \tag{11}$$

Из равенства $x_j = c_j d_{j-1}$ ($j = 3, 4, \dots$) и неравенств (10) и (11) вытекает, что

$$b_1(b_2-1)^{j-2}(m_2(\omega^{j-2}h_2 - S_{j-2}) - 3\lfloor 0.5(m_2-1)\rfloor +$$
$$+\mathtt{sign}(m_2 - 2\lfloor 0.5m_2\rfloor) - 2) < x_j \le b_1 b_2^{j-2}(m_2\omega^{j-2}h_2 - 1), \tag{12}$$

Воспользовавшись неравенствами (3) в (12), получим, что неравенства (5) и (7) истинны при $j = 3, 4, \dots$. $\square$

Следствие 1. *Для числа итераций построения изображения псевдофрактала F на абстрактном экране размера $n \times n$ истинны следующие неравенства*

$$(\ln^{-1}\omega)\ln\omega(3-2\omega)(h_2 - \omega h_2 + 1)^{-1} < j_0 \le (\ln^{-1}\omega)\ln 2\omega^2 h_2.$$

Доказательство. Так как процесс построения изображения псевдофрактала F завершается, когда длина отрезка, добавляемого на следующей итерации меньше, чем 2, то из (9) вытекает, что

$$\begin{cases} \omega^{j_0-1}h_2 - S_{j_0-1} < 2 \\ \omega^{j_0-2}h_2 \geq 2 \end{cases} \Leftrightarrow \begin{cases} \omega^{j_0-1}h_2 - \frac{1-\omega^{j_0-1}}{1-\omega} < 2 \\ \omega^{j_0-2}h_2 \geq 2 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} \omega^{j_0} < \omega(3-2\omega)(h_2 - \omega h_2 + 1)^{-1} \\ \omega^{j_0} \geq 2\omega^2 h_2 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} j_0 \ln\omega < \ln\omega(3-2\omega)(h_2 - \omega h_2 + 1)^{-1} \\ j_0 \ln\omega \geq \ln 2\omega^2 h_2 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} j_0 > (\ln^{-1}\omega)\ln\omega(3-2\omega)(h_2 - \omega h_2 + 1)^{-1} \\ j_0 \leq (\ln^{-1}\omega)\ln 2\omega^2 h_2 \end{cases}.$$

□

Рассмотрим применение полученных результатов при исследовании структуры псевдофрактала конкретного типа.

3. H-псевдофрактал. Зафиксируем число ω $(0 < \omega < 1)$ и такое число β $(0 < \beta < 0.5)$, что $\lfloor\omega\lfloor\omega\lfloor\beta n\rfloor\rfloor\rfloor \geq 1$. Определим H-псевдофрактал следующим образом:

1) основа – горизонтальный отрезок (т.е. $m_1 = 1$) длины $h_1 = \lfloor\beta n\rfloor$, размещенный в центре абстрактного экрана размера $n \times n$;

2) фрагмент – отрезок (т.е. $m_2 = 1$) длины $h_2 = \lfloor\omega\lfloor\beta n\rfloor\rfloor$;

3) число ω – коэффициент уменьшения при построении псевдофрактала;

4) j-я итерация $(j = 2, 3, \dots)$ рекурсивной процедуры состоит в том, что к концам каждого отрезка, построенного на предыдущей итерации добавляются два перпендикулярных ему отрезка, причем каждый добавляемый отрезок расположен так, что количество пикселей, расположенных с одной стороны от точки касания либо равно количеству пикселей с другой стороны от точки касания, либо эти количества пикселей отличаются на единицу.

Замечание 1. Если для добавляемого отрезка количества пикселей в частях, расположенных по разные стороны от точки касания отличаются на единицу, то для выбора меньшей части имеются две возможности: а) выбор осуществляется по заранее установленному правилу; б) выбор осуществляется с помощью генератора псевдослучайных чисел (т.е. вносится элемент псевдослучайности).

Теорема 2. *При построении изображения* H-*псевдофрактала на абстрактном экране размера* $n \times n$ *истинны неравенства*

$$\beta n - 1 < x_1 \leq \beta n, \tag{13}$$

$$2^{j-1}(\omega^{j-1}\beta n - T_{j-1} - 1) < x_j \leq 2^{j-1}(\omega^{j-1}\beta n - 1) \ \ (j = 2, 3, \dots), \tag{14}$$

где

$$T_{j-1} = \frac{1-\omega^{j-1}}{1-\omega} \ \ (j = 2, 3, \dots). \tag{15}$$

Доказательство. Так как $x_1 = h_1 = \lfloor \beta n \rfloor$, то неравенства (13) истинны.

Докажем, что истинны неравенства (14). Так как длина l_j $(j = 2, 3, \dots)$ отрезка, добавляемого на j-й итерации, определяется равенством

$$l_j = \underbrace{\lfloor \omega \lfloor \dots \lfloor \omega}_{j-2} \lfloor \omega \lfloor \beta n \rfloor \rfloor \rfloor \dots \rfloor \rfloor,$$

то

$$\omega^{j-1}\beta n - T_{j-1} < l_j \le \omega^{j-1}\beta n \ (j = 2, 3, \dots), \tag{16}$$

где T_{j-1} определено равенством (15).

Один пиксель добавляемого отрезка принадлежит отрезку, построенному на предыдущей итерации. Поэтому из (16) вытекает, что количество k_j пикселей, добавляемых в изображение Н-псевдофрактала одним отрезком, построенном на j-й итерации, удовлетворяет неравенствам

$$\omega^{j-1}\beta n - T_{j-1} - 1 < k_j \le \omega^{j-1}\beta n - 1 \ (j = 2, 3, \dots). \tag{17}$$

А так как число отрезков, добавляемых в изображение Н-псевдофрактала на j-й итерации $(j = 2, 3, \dots)$, равно 2^{j-1}, то из (17) вытекает, что неравенства (14) истинны. □

Следствие 2. *Для числа итераций построения изображения* Н*-псевдофрактала на абстрактном экране размера $n \times n$ истинны следующие неравенства*

$$(\ln^{-1}\omega)\ln(3 - 2\omega)(\beta n - \omega\beta n + 1)^{-1} < j_0 \le (\ln^{-1}\omega)\ln 2\omega(\beta n)^{-1}.$$

Доказательство. Так как процесс построения изображения Н-псевдофрактала завершается, когда длина отрезка, добавляемого на следующей итерации меньше, чем 2, то из (16) вытекает, что

$$\begin{cases} \omega^{j_0-1}\beta n \ge 2 \\ \omega^{j_0}\beta n - T_{j_0} < 2 \end{cases} \Leftrightarrow \begin{cases} \omega^{j_0} \ge 2\omega(\beta n)^{-1} \\ \omega^{j_0} < (3 - 2\omega)(\beta n - \omega\beta n + 1)^{-1} \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} j_0 \ln\omega \ge \ln 2\omega(\beta n)^{-1} \\ j_0 \ln\omega < \ln(3 - 2\omega)(\beta n - \omega\beta n + 1)^{-1} \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} j_0 \le (\ln^{-1}\omega)\ln 2\omega(\beta n)^{-1} \\ j_0 > (\ln^{-1}\omega)\ln(3 - 2\omega)(\beta n - \omega\beta n + 1)^{-1} \end{cases}.$$

□

Следствие 3. *При построении изображения* Н*-псевдофрактала на абстрактном экране размера $n \times n$ количество κ_j $(j = 1, \dots, j_0)$ пикселей изображения псевдофрактала, построенных в течение первых j итераций, удовлетворяет неравенствам*

$$\left(\beta n + \frac{1}{1-\omega}\right)\frac{1 - (2\omega)^j}{1 - 2\omega} -$$

$$-\left(1+\frac{1}{1-\omega}\right)(2^j-1)<\kappa_j\leq\beta n\frac{1-(2\omega)^j}{1-2\omega}-2^j+2\ \ (j=1,\ldots,j_0). \qquad (18)$$

Замечание 2. При $\omega=0.5$ для того, чтобы в (18) избавиться от неопределенности вида $\frac{0}{0}$ достаточно вычислить предел дроби по правилу Лопиталя.

Доказательство. Так как

$$\kappa_j=\sum_{r=1}^{j}x_r\ \ (j=1,\ldots,j_0),$$

то из (13)-(15) вытекает, что

$$\kappa_j\leq\beta n+\sum_{r=2}^{j}2^{r-1}(\omega^{r-1}\beta n-1)=\beta n\sum_{r=1}^{j}(2\omega)^{r-1}-\sum_{r=2}^{j}2^{r-1}=$$

$$=\beta n\frac{1-(2\omega)^j}{1-2\omega}-\frac{2^j-2}{2-1}=\beta n\frac{1-(2\omega)^j}{1-2\omega}-2^j+2.$$

$$\kappa_j>\beta n-1+\sum_{r=2}^{j}2^{r-1}(\omega^{r-1}\beta n-T_{r-1}-1)=$$

$$=\beta n\sum_{r=1}^{j}(2\omega)^{r-1}-\frac{1}{1-\omega}\left(\sum_{r=1}^{j}2^{r-1}-\sum_{r=1}^{j}(2\omega)^{r-1}\right)-\sum_{r=1}^{j}2^{r-1}=$$

$$=\beta n\frac{1-(2\omega)^j}{1-2\omega}-\frac{1}{1-\omega}\left(\frac{2^j-1}{2-1}-\frac{1-(2\omega)^j}{1-2\omega}\right)-\frac{2^j-1}{2-1}=$$

$$=\left(\beta n+\frac{1}{1-\omega}\right)\frac{1-(2\omega)^j}{1-2\omega}-\left(1+\frac{1}{1-\omega}\right)(2^j-1).$$

□

Заключение. В работе разработаны методы анализа динамики построения черно-белого изображения конструктивного псевдофрактала на абстрактном экране размера $n\times n$. Такие псевдофракталы могут использоваться для управления семействами легко вычислимых перестановок, применяемых в нестационарных поточных шифрах, разработанных в [6-9].

Развитая техника оценки количества пикселей, добавляемых в изображение псевдофрактала на каждой итерации процедуры его построения, а также оценки числа итераций при построении псевдофрактала необходима для анализа возможностей криптоаналитика при одной из наиболее сильных атак на секретный ключ (сеансовый или средней длительности) соответствующего шифра, предполагающей, что криптоаналитик имеет частичный доступ к библиотеке массивов, используемых для управления семействами легко вычислимых перестановок (т.е. может случайным образом просмотреть часть того или иного массива). Поэтому разработка техники сравнительного анализа структур этих массивов актуальна и представляет собой одно из возможных направлений исследований. Второе направление состоит в разработке методов выделения почти регулярных подмассивов (т.е. элементы которых достаточно точно описываются такими последовательностями, как арифметическая прогрессия). Третье направление состоит в построении алгебры массивов, предназначенной для динамической генерации множеств массивов, используемых в данном сеансе, из достаточно ограниченной стационарной библиотеки.

1. *Кузнецов С.П.* Динамический хаос. – М: Физматлит, 2001. – 296с.
2. *Турбин А.Ф., Працевитый Н.Ф.* Фрактальные множества, функции, распределения. – Киев: Наук. думка, 1992. – 208с.
3. *Морозов А.Д.* Введение в теорию фракталов. – Москва-Ижевск: Ин-т компьютерных исследований, 2002. – 160с.
4. *Турбин А.Ф.* Мультифрактальные методы сверхглубокой защиты информации // Фрактальний аналіз та суміжні питання. Київ: ІМ НАН України – НПУ ім. Драгоманова. – 1998. – № 1. – С. 27-33.
5. *Alia M.A., Samsydin A.B.* New key-exchange protocol based on Mandelbrot and Julia fractal sets // International Journal of Computer Science and Network Security. – 2007. – Vol. 7. – № 2. – P. 302-307.
6. *Зайцева Э.Е., Скобелев В.Г.* Шифр на основе отображения Мандельброта // Вестник Томского государственного университета. Приложение. – 2007. – № 23. – С. 107-113.
7. *Скобелев В.Г., Зайцева Э.Е.* Шифры на основе фракталов // Труды ИПММ НАНУ. – Т. 12. – 2006. – С. 63-68.
8. *Скобелев В.Г., Зайцева Э.Е.* Анализ класса легко вычислимых перестановок // Кибернетика и системный анализ – 2008. – № 5. – С. 12-24.
9. *Скобелев В.В., Скобелев В.Г.* Анализ шифрсистем. – Донецк: ИПММ НАНУ, 2009. – 479с.

V.G. Skobelev, N.A. Sheremetjeva

Analysis of characteristics for constuctive psevdo-fractal.

Problem of analysis of dynamics of design of black-and-white image of constructive pseudo-fractal onto abstract display of $(n \times n)$-size is resolved. It is proposed some method intended to estimate the number of picksels, that are added to pseudo-fractal image in each iteration and some method intended to estimate the number of iterations for the process of design of pseudo-fractal image. Proposed methods are worked in detail for H-pseudo-fractal.

Keywords: *onstructive pseudo-fractals, abstract display, ciphers.*

В.Г. Скобелєв, Н.А. Шереметьєва

Аналіз характеристик конструктивного псевдофрактала.

Розв'язано задачу побудови чорно-білого зображення конструктивного псевдофрактала на абстрактному екрані розміру $n \times n$. Розроблено метод оцінки кількості пікселів, які додаються до зображнення псевдофрактала на кожній ітерації процедури його побудови, а також метод оцінки кількості ітерацій при побудові зображення псевдофрактала. Розроблені методи деталізовано для H-псевдофрактала.

Ключові слова: *конструктивні псевдофрактали, абстрактний екран, шифри.*

Ин-т прикл. математики и механики НАН Украины, Донецк
`skbv@iamm.ac.donetsk.ua`

Получено 31.05.10