ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПЕРЕДАЧИ И ОБРАБОТКИ ИНФОРМАЦИИ И СИГНАЛОВ

УДК 681.3

МОДИФИКАЦИЯ СХЕМЫ РАЗДЕЛЕНИЯ ДАННЫХ АСМУТА-БЛУМА С ПРИМЕНЕНИЕМ МЕТОДА ФРАКТАЛЬНОЙ ГЕОМЕТРИИ

Кочеров Ю.Н., Червяков Н.И.
Северо-Кавказский федеральный университет, Ставрополь, РФ
E-mail: kocherov_yra@mail.ru

В статье рассмотрена схема разделения данных Асмута-Блума и ее модификация с применением фрактальной геометрии в качестве кодирующей функции, а также численный метод вычисления частей данных с применением модифицированной схемы разделения данных Асмута-Блума. Предложенная модификация позволяет одновременно разделять и кодировать изображение, не применяя дополнительных алгоритмов и, следовательно, не увеличивая вычислительную сложность.

Ключевые слова: пороговое разделение данных, Китайская теорема об остатках, схема Асмута-Блума, фрактальная геометрия

Введение

Хранение личной информации является важной составляющей жизни современного человека. С развитием облачных технологий для удаленного хранения данных, а также сетей для их передачи возрастает необходимость применения криптографических и некриптографических алгоритмов. Для надежного хранения информации и обеспечения распределенного доступа к ресурсам применяются схемы с разделением информации на части. В таких схемах получить доступ к ней можно, только собрав все ее части. В случае когда количество долей, достаточных для восстановления информации, отличается от общего количества частей, то применяются пороговые схемы разделения данных (СРД). Основоположниками порогового разделения данных являются А. Шамир [9] и Дж. Блэкли [10]. Позже были предложены схемы разделения данных, основанные на Китайской теореме об остатках (КТО), такие как схема Асмута-Блума [8] и схема Миньотта [11].

Основные критерии СРД – это совершенность, идеальность и вычислительная сложность. СРД, основанные на КТО, имеют меньшую вычислительную сложность по сравнению с другими схемами. Среди схем, основанных на КТО, совершенной и идеальной является схема Асмута-Блума [8]. СРД имеют также свои недостатки: они подвергаются как внутренним, так и внешним атакам [1]. Среди СРД, основанных на КТО, выявляется один общий недостаток – если данные меньше основания СОК, то они остаются неизменными, а в противном случае они меняют свой порядок.

На рис. 1 показано, как исходный синусоидальный сигнал (см. рис. 1*а*) подвергается модулярному делению по основанию 200 (см. рис. 1*б*) и по основанию 100 (см. рис. 1*в*). Из рис. 1 видно, что часть сигнала остается неизменной, а другая часть меняет свой порядок, но не изменяет форму. Например, применив СОК на изображении, часть его будет неизменна либо будут видны его «тени».

Введение в СОК. Схема разделения данных Асмута-Блума и ее модификация

Напомним, что СОК относится к непозиционным системам счисления, числа в которой представляются в базисе взаимнопростых чисел, называемых модулями $\beta = \{m_1,...,m_n\}$, $НОД(m_i, m_j) = 1$, для $i \neq j$. Произведение всех модулей СОК $P = \prod_{i=1}^{n} m_i$ называется динамическим диапазоном системы. В диапазоне $0 \le X < P$ любое целое число может быть представлено единственным образом в СОК в виде вектора $\{x_1, x_2, ..., x_n\}$, где $x_i = |X|_{m_i} = X \bmod m_i$.

Из вышесказанного можно сделать вывод, что для порогового разделения данных предпочтительнее использовать СРД Асмута-Блума, но необходимо применять дополнительные кодирующие преобразования. В схеме разделения данных Асмута-Блума разделение данных происходит по формуле $M'(\bmod p_n)$, $i = 1;2;3...\ n$

где $M' = M + qr$, qr – аддитивное смещение, которое добавляет шум в сигнал.

Так как пороговые схемы разделения данных подвергаются различным типам атак, например злоумышленник, прослушав линии связи, может восстановить информацию, то при использовании схемы Асмута-Блума он получит только M'. Для полного восстановления информации необходимо произвести вычитание $M = M' - qr$ где qr - постоянная константа в диапазоне $[0; p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k - 1]$. Для увеличения криптографических свойств константа qr должна изменяться. Величина q выбирается из условий $q > P$, где P – динамический диапазон СОК и $q > p_1 > p_2 > \ldots > p_n$, поэтому q величина постоянная. Значение r выбирается как случайное число из диапазона $\left[0; \frac{p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k}{q} - 1\right]$.

В статье предлагается подход к использованию фрактальных итерационных функций в качестве кодирующей функции. Данный подход отличается от обычных методов кодирования тем, что фрактальная последовательность используется в качестве сложной кодирующей функции [3]. При этом описание этой функции, достаточное для построения, является набором вещественных чисел, которые задают начальные условия итерационного процесса построения фрактальной последовательности [4]. Этот подход является вариантом гаммирования – процесса «наложения» гамма-последовательности на открытые данные, где в качестве гамма-последовательности используется фрактальная последовательность.

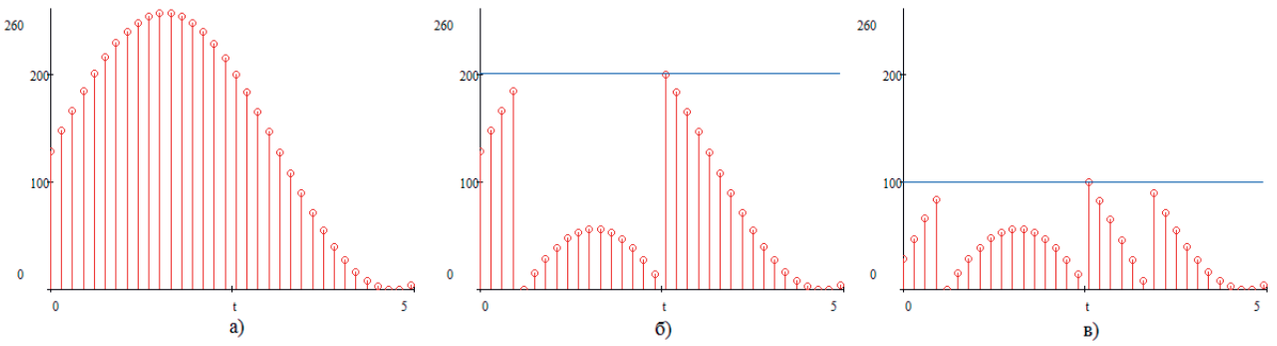


Рис. 1. Представление сигнала в СОК:
а) исходный сигнал, *б*) сигнал по модулю 200, *в*) сигнал по модулю 100

Основной проблемой средств защиты информации является порождение случайных последовательностей бит. Генераторы случайных последовательностей, используемые для общих целей, являются псевдослучайными генераторами [2]. Идея применения фракталов как псевдослучайных последовательностей исходит из предположения возможности описания поведения физических и природных систем с помощью фракталов [5].

Фракталы относятся к множествам с крайне нерегулярной разветвленной или изрезанной структурой. Теория фракталов рассматривает дробные меры вместо целочисленных и базируется на количественных показателях в виде дробных размерностей и соответствующих сигнатур. Фракталы характеризуют как топологию объектов, так и эволюцию динамических систем и связаны с их свойствами. Теория фракталов и нелинейность составляют геометрию хаоса. По своему содержанию контуры всех природных объектов суть динамические процессы, внезапно застывшие в физических формах и объединяющие в себе устойчивость и хаос [6].

Таким образом, применение «генераторов шума», основанных на фракталах, дает преимущество над традиционными системами псевдослучайных последовательностей. Другим достоинством генератора псевдослучайных чисел, основанного на фракталах, является то, что он имеет бесконечное количество состояний ЭВМ в отличие от классических генераторов псевдослучайных чисел.

В статье для построения фрактала применено множество Мандельброта. Множество Мандельброта является одним из самых известных фракталов, в том числе за пределами математики, благодаря своим цветным визуализациям. Его фрагменты не строго подобны исходному множеству, но при многократном увеличении определенные части все больше похожи друг на друга. Множество Мандельброта – это множество таких точек c на комплексной плоскости, для которых итерационная последовательность $z_{n+1} = z_n^2 + c$ при $z_0 = 0$ является ограниченной.

Последовательность может быть раскрыта для каждой точки c на комплексной плоскости следующим образом [7]:

$$c = x + i\,y\,;\quad z_0 = 0\,;$$
$$z_1 = z_0^2 + c = x + i\,y\,;\quad z_3 = z_2^2 + c\,;$$
$$z_2 = z_1^2 + c = (x + i\,y)^2 + x + i\,y =$$
$$= x^2 - y^2 + x + (2xy + y)i\,.$$

На рис. 2 слева представлен классический фрактал множества Мандельброта. Визуально внутри множества Мандельброта можно выделить бесконечное число элементарных фигур, причем самая большая в центре представляет собой кардиоиду. Пример увеличения множества фрактала представлен на рис. 2 справа.

Таким образом, применив фрактал в качестве случайной величины r, получим зашумленные части изображения. Рассмотрим алгоритм разделения информации на части с применим фрактала ее восстановления.

Изображение на ЭВМ имеет вид матрицы пикселей размерностью $m \times n$. В каждом ее элементе хранятся значения глубины цветов в палитре RGB (Red, Green, Blue) в диапазоне $[0; 255]$. Операторами $I_{x,y}$ и $F_{x,y}$, – где $0 < x < m$ и $0 < y < m$, обозначим матрицу исходного изображения и матрицу изображения фрактала, соответственно.

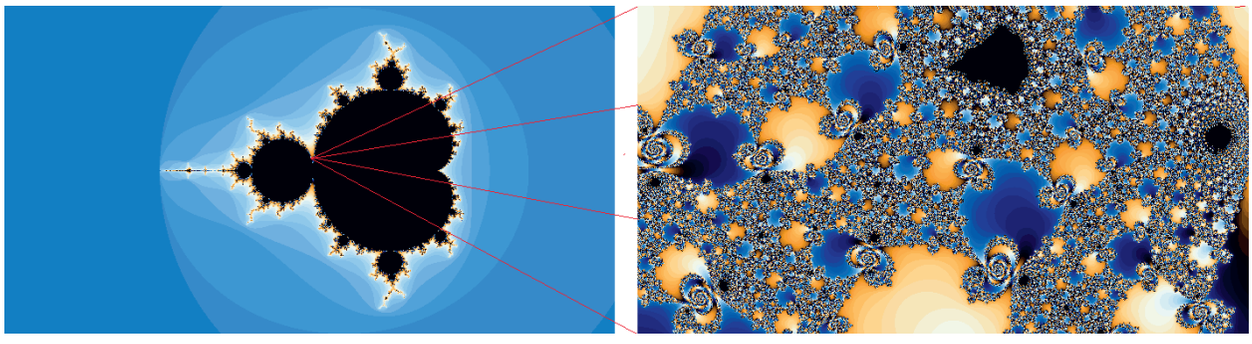


Рис. 2. Увеличение фрактала, соответствующего множеству Мандельброта

Таким образом алгоритм состоит из следующих действий.

1. Выбирается ряд чисел $q, p_1, p_2, ..., p_n$.
2. Вычисляется $I_{x,y}^{/} = I_{x,y} + q\,F_{x,y}$.
3. Вычисляются части данных $a_{x,y_i} = I_{x,y}^{/} \bmod p_i$.
4. Выполняется обратное преобразование из СОК в ПСС:

$$I_{x,y}^{/} = (a_{x,y_1}\ \ B_1 + a_{x,y_2}\ \ B_2 + ... + a_{x,y_n}\ \ B_n) \bmod P\,.$$

5. Вычисляется $I_{x,y} = I_{x,y}^{/} - q\,F_{x,y}$.

Схема разделения данных с применения фрактала представлена на рис. 3.

Применив для взлома метод «грубой силы», необходимо для каждой точки изображения перебрать все возможные комбинации. При использовании фрактала разрядностью 8 бит количество комбинаций $N = 2^n\,2^n\,2^n\,x\,y$, где x, y – разрешение изображения; n – глубина цвета изображения. Также достоинством данного метода

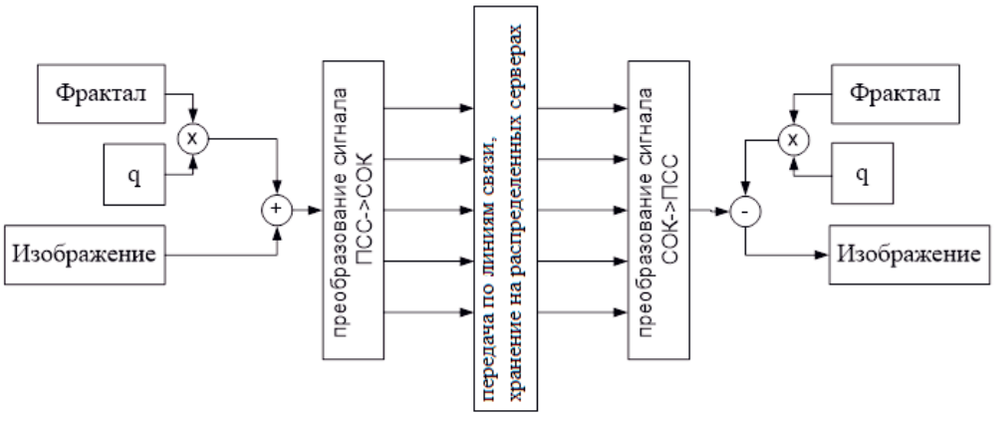


Рис. 3. Схема разделения изображения

является отсутствие необходимости хранить изображение фрактала или сгенерированные случайные числа, поскольку при восстановлении, зная схему раскраски фрактала и порядок его уравнения, числа могут быть сгенерированы заново.

Численный метод разделения информации с применением модифицированной схемы разделения данных Асмута-Блума

Для порогового разделения данных модифицированным методом Асмута-Блума необходимы две матрицы: A – матрица данных, F – матрица псевдослучайных чисел фрактала. Для простоты вычислений представим обе матрицы размерностью 3×3.

Рис. 4. Увеличение участка изображения

Необходимо заполнить массив данных и массив фрактала числами. Так как изображение – это матрица размерами $m \times n$, каждый пиксель которой представлен тремя цветами (красный, синий, зеленый), то путем увеличения рисунка (как это показано на рис. 4) и с помощью инструмента Paint можно получить значения нескольких пикселей и вычислить среднее арифметическое цветов RGB:

$$A = \begin{pmatrix} 100 & 50 & 30 \\ 20 & 150 & 70 \\ 40 & 200 & 80 \end{pmatrix};$$

$$F = \begin{pmatrix} 187 & 74 & 83 \\ 81 & 70 & 251 \\ 72 & 80 & 3 \end{pmatrix}.$$

Для вычислений возьмем следующий ряд модулей: $q = 257$, $p_1 = 547$, $p_2 = 557$, $p_3 = 563$, $p_4 = 569$, $p_5 = 571$. Проверим условие: $R = p_1\, p_2\, p_3 > q\, p_4\, p_5 = 71534277 > 83499043$.

Значения $q, p_1, p_2, p_3, p_4, p_5$ также упорядочены. Для вычисления частей данных необходимо массив F умножить на q:

$$F = q\,F = 257 \begin{pmatrix} 187 & 74 & 83 \\ 81 & 70 & 251 \\ 72 & 80 & 3 \end{pmatrix} =$$

$$= \begin{pmatrix} 48\,059 & 19\,018 & 21\,331 \\ 20\,817 & 17\,990 & 64\,507 \\ 18\,504 & 20\,560 & 771 \end{pmatrix}.$$

Далее необходимо поэлементно сложить значения в получившемся массиве и в массиве A:

$$A = \sum_{x=1}^{3} \sum_{y=0}^{3} \left(A_{x,y} + F_{x,y} \right) =$$

$$= \begin{pmatrix} 100 + 48059 & 50 + 19018 & 30 + 21331 \\ 20 + 20817 & 150 + 17990 & 70 + 64507 \\ 40 + 18504 & 200 + 20560 & 80 + 711 \end{pmatrix} =$$

$$= \begin{pmatrix} 48159 & 19018 & 21361 \\ 20837 & 18140 & 64577 \\ 18544 & 20760 & 7091 \end{pmatrix}.$$

Следующий шаг – это разделение данных, которое выполняется путем преобразования элементов массива A в СОК:

$$a = A_{x,y} \bmod(p_i) = A_{x,y} \bmod(547) =$$

$$= \begin{pmatrix} 23 & 420 & 28 \\ 51 & 89 & 31 \\ 493 & 521 & 527 \end{pmatrix};$$

$$b = A_{x,y} \bmod(p_i) = A_{x,y} \bmod(557) =$$

$$= \begin{pmatrix} 257 & 80 & 195 \\ 228 & 316 & 502 \\ 173 & 151 & 407 \end{pmatrix};$$

$$c = A_{x,y} \bmod(p_i) = A_{x,y} \bmod(563) =$$

$$= \begin{pmatrix} 304 & 439 & 530 \\ 6 & 124 & 395 \\ 528 & 492 & 335 \end{pmatrix};$$

$$d = A_{x,y} \bmod(p_i) = A_{x,y} \bmod(569) =$$

$$= \begin{pmatrix} 363 & 241 & 308 \\ 353 & 501 & 280 \\ 336 & 276 & 263 \end{pmatrix};$$

$$e = A_{x,y} \bmod(p_i) = A_{x,y} \bmod(571) =$$
$$= \begin{pmatrix} 195 & 175 & 234 \\ 281 & 439 & 54 \\ 272 & 204 & 239 \end{pmatrix}.$$

Массивы a,b,c,d,e – это части информации, и они распространяются среди пользователей. Для восстановления данных необходимо провести для массивов a,b,c,d,e обратное преобразование из СОК в ПСС. Выполнив данное преобразование, получим массив

$$A = \begin{pmatrix} 48159 & 19018 & 21361 \\ 20837 & 18140 & 64577 \\ 18544 & 20760 & 7091 \end{pmatrix}.$$

Далее из массива данных A необходимо поэлементно вычесть произведение $q\,F$:

$$A = \sum_{x=1}^{3}\sum_{y=0}^{3} A_{x,y} - F_{x,y} = \begin{pmatrix} -100+48059 & -50+19018 & -30+21331 \\ -20+20817 & -150+17990 & -70+64507 \\ -40+18504 & -200+20560 & -80+711 \end{pmatrix} = \begin{pmatrix} 100 & 50 & 30 \\ 20 & 150 & 70 \\ 40 & 200 & 80 \end{pmatrix}.$$

Блок-схема алгоритма разделения изображения на части приведена на рис. 5.

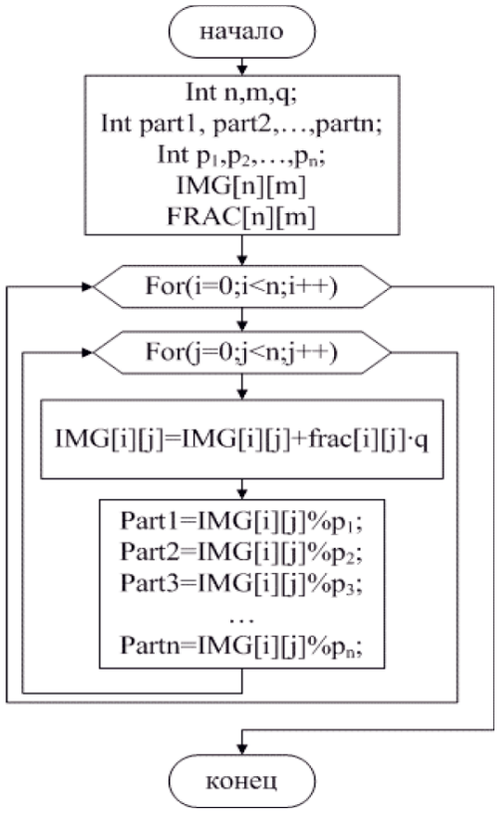


Рис. 5. Алгоритм вычисления частей данных модифицированным методом Асмута-Блума

В отличие от криптографических алгоритмов, таких как RSA, в котором вычислительная сложность равна $O[\log(n)^2]$, использование численного метода, основанного на модификации схемы Асмута-Блума с применением фрактальной геометрии, позволяет закодировать информацию, не увеличивая вычислительную сложность СРД.

Моделирование модифицированной схемы разделения данных Асмута-Блума с применением фрактальной геометрии

Рассмотрим пример реализации предложенного метода. Так как множество Мандельброта является бесконечной последовательностью, то увеличим его участок и в экспериментах будем использовать часть фрактала (см. рис. 7) для моделирования разделения изображения «Лена», показанного на рис. 7.

Применив схему, представленную на рис. 4, и алгоритм, представленный на рис. 6, а также используя набор модулей $p_1 = 547$, $p_2 = 557$, $p_3 = 563$, $p_4 = 569$, $p_5 = 571$, получим результаты, показанные на рис. 8.

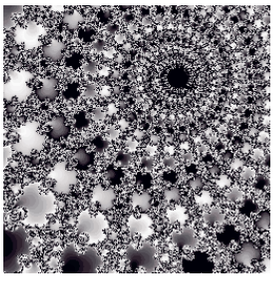


Рис. 6. Часть фрактала, используемого при моделировании

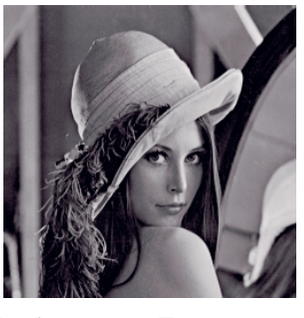
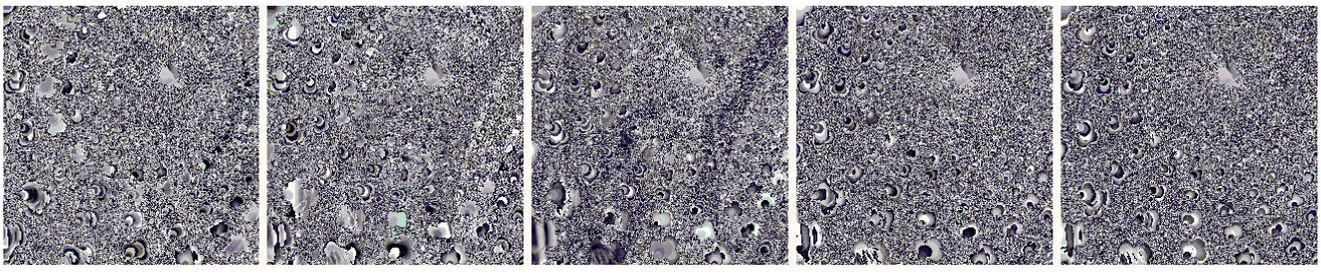


Рис. 7. Изображение «Лена», используемое при моделировании

Другим способом искажения изображения является наложение белого шума. Применив вместо фрактала белый шум, получим результаты, показанные на рис. 9.

Визуально сравнивая изображения, представленные на рис. 8 и рис. 9, можно сделать вывод, что применение фрактальной последовательности позволит более качественно иска-



а) *б*) *в*) *г*) *д*)

Рис. 8. Результаты работы модифицированной схемы разделения данных Асмута-Блума с применением фрактальной последовательности для набора модулей
а) 547; *б*) 557; *в*) 563; *г*) 569; *д*) 571

а) *б*) *в*) *г*) *д*)

Рис. 9. Результаты работы модифицированной схемы разделения данных Амсута-Блума с применением белого шума для набора модулей
а) 547; *б*) 557; *в*) 563; *г*) 569; *д*) 571

зить изображение, а следовательно, более надежно его хранить и обрабатывать.

Выводы

В статье разработан модифицированный метод разделения данных Асмута-Блума с применением фрактальной геометрии, где для генерации случайного числа r применяется псевдослучайная последовательность, генерируемая фракталом. Получение информации при атаке методом «грубой силы» потребует $N = 2^n\, 2^n\, 2^n\, x\, y$ комбинаций. Применение численного метода на основе разработанного алгоритма позволит разделять и кодировать изображение, одновременно не повышая вычислительную сложность алгоритма.

Литература

1. Кочеров Ю.Н., Червяков Н.И. Разработка помехоустойчивого метода разделения секрета на основе применения двухступенчатой системы остаточных классов // ИКТ. Т.11, №4, 2013. – С. 4-11.
2. Успенский В.А. Четыре алгоритмических лица случайности. М.: МЦНМО, 2006. – 48 с.
3. Кулешов С.В. Фрактальное шифрование // Труды СПИИРАН. 2:1 (2004). – С. 231-235.
4. Чумак О.В. Энтропии и фракталы в анализе данных. Москва – Ижевск: НИЦ «Регулярная и хаотическая динамика», Институт компьютерных исследований. 2011. – 164 с.
5. Фрактал и хаос в динамических системах. Основы теории. М.: Постмаркет, 2000. – 352 с.
6. Потапов А.А. Методы обработки сигналов и полей на основе теории фракталов // Труды Первой Всероссийской НК «Методы и средства обработки информации». Москва, октябрь 2003. М.: Изд. МГУ. 2003. – С. 559-565.
7. Морозов А.Д. Введение в теорию фракталов. Москва – Ижевск: Институт компьютерных исследований, 2002. – С. 82-108.
8. Asmuth C., Bloom J. A modular approach to key safeguarding // Information Theory, IEEE Transactions on. Vol. 29, Iss. 2, 1983. – P. 208-210. doi: 10.1109/TIT.1983.1056651.

9. Shamir A. How to share a secret // Communications of the ACM. New York City: ACM. Vol. 22, Iss. 11, 1979. – P. 612-613.
10. Blakley G.R. Safeguarding cryptographic keys // Proceedings of the 1979 AFIPS National Computer Conference. Monval, NJ, USA: AFIPS Press, 1979. – P. 313-317.
11. Mignotte M. How to Share a Secret // Lecture Notes in Computer Science. Vol. 149, 1983. – P. 371-375. doi: 10.1007/3-540-39466-4_27.

Получено 17.01.2017

Червяков Николай Иванович, д.т.н., профессор, Заслуженный деятель науки и техники РФ, заведующий Кафедрой прикладной математики и математического моделирования Северо-Кавказского федерального университета (СКФУ). Тел. (8-865) 226-60-14. E-mail: k-fmf-primath@stavsu.ru

Кочеров Юрий Николаевич, к.т.н., доцент Кафедры информационных систем, электропривода и автоматики Невинномысского технологического института (Филиала СКФУ). Тел. (8-865) 543-55-08; 8-918-866-91-93. E-mail: kocherov_yra@mail.ru

MODIFICATION OF ASMUT-BLUM DATA SHARING SCHEME USING THE FRACTAL GEOMETRY METHOD

Kocherov Y.N., Chervyakov N.I.
North-Caucasus Federal University, Stavropol, Russia Federation
E-mail: kocherov_yra@mail.ru

The paper presents schemes of information separation into parts, applied for reliable information storage and obtained of distributed access to resources. It is pointed out that data sharing schemes are subjected to internal and external threats and it can compromise data sharing scheme. The Asmut-Bloom data sharing scheme and its modification using the fractal geometry as a coding function and numerical method of pieces data calculation with the modified Asmut-Bloom data sharing scheme application is considered in the article. This modification allows to separate and encode the image simultaneously without using additional algorithms and, therefore, without increasing the computational complexity. A computer simulation of the proposed algorithm using white noise and fractal sequence as a coding function was carried out. Conclusions have been made.

Keywords: threshold data sharing, the Chinese remainder theorem, Asmut-Bloom scheme, fractal geometry

DOI: 10.18469/ikt.2017.15.1.01

Chervyakov Nikolai Ivanovich, North Caucasus Federal University; 1 Pushkin str., Stavropol 355009; the Head of Department of Applied Mathematics and Computer Science; Doctor of Technical Science, Professor. Tel.: +79054693412. E-mail: k-fmf-primath@stavsu.ru

Kocherov Yuri Nikolaevich, North Caucasus Federal University, Nevinnomyssk Technological Institute; 1 Gagarin srt., Nevinnomyssk, 357108, Stavropol region, Russian Federation; Associate Professor of the Departmetn of Information Systems, Electric Drive and Automation; PhD in Technical Science. Tel.: +79188669193. E-mail: kocherov_yra@mail.ru

References

1. Kocherov YU.N., Chervyakov N.I. Razrabotka pomekhoustojchivogo metoda razdeleniya sekreta na osnove primeneniya dvuhstupenchatoj sistemy ostatochnyh klassov [Development of an interference-free method of separation based on the two-level system of residual classes]. *Infokommunikacionnye tehnologii*, 2013, vol. 11, no. 4, pp. 4-11.
2. Uspenskij V.A. *Chetyre algoritmicheskih lica sluchajnosti* [Four algorithmic faces of chance]. Moscow, MCNMO Publ., 2006. 48 p.
3. Kuleshov S.V. Fraktal'noe shifrovanie [Fractal encryption]. *Trudy SPIIRAN*, 2004, no. 2, pp. 231-235.
4. Chumak O. V. *Entropii i fraktaly v analize dannyh* [Entropies and fractals in data analysis]. Moscow – Izhevsk, Institut komp'yuternyh issledovanij. 2011. 164 p.
5. *Fraktal i haos v dinamicheskih sistemah. Osnovy teorii* [Fractal and chaos in dynamic systems. Fundamentals of Theory]. Moscow, Postmarket Publ., 2000. 352 p.

6. Potapov A.A. Metody obrabotki signalov i polej na osnove teorii fraktalov [Methods for processing signals and fields based on the theory of fractals]. *Trudy Pervoj Vserossijskoj NK «Metody i sredstva obrabotki informacii»*, Moscow, MGU Publ., 2003, pp. 559-565.
7. Morozov A.D. *Vvedenie v teoriyu fraktalov* [Introduction to the theory of fractals]. Moscow – Izhevsk, Institut komp'yuternyh issledovanij, 2002, pp. 82-108.
8. Asmuth S., Bloom J. A modular approach to key safeguarding. *Information Theory, IEEE Transactions on*, 1983, vol. 29, no. 2, pp. 208-210. doi: 10.1109/TIT.1983.1056651.
9. Shamir A. How to share a secret. *Communications of the ACM*, New York City: ACM, 1979, vol. 22, no. 11, pp. 612-613.
10. Blakley G.R. *Safeguarding cryptographic keys. Proceedings of the 1979 AFIPS National Computer Conference*, Monval, NJ, USA, AFIPS Press, 1979, pp. 313-317.
11. Mignotte M. How to Share a Secret. *Lecture Notes in Computer Science*, 1983, vol. 149, pp. 371-375. doi: 10.1007/3-540-39466-4_27.

Received 17.01.2017

УДК 621.395

МЕТОД СЖАТИЯ РЕЧЕВЫХ ДАННЫХ БЕЗ ПАУЗ НА ОСНОВЕ ОПТИМАЛЬНОГО КВАНТОВАНИЯ ПО УРОВНЮ КОЭФФИЦИЕНТОВ РАЗЛОЖЕНИЯ ОТРЕЗКОВ РЕЧЕВЫХ СИГНАЛОВ ПО СОБСТВЕННЫМ ВЕКТОРАМ СУБПОЛОСНЫХ МАТРИЦ

Жиляков Е.Г., Белов С.П., Белов Ал.С., Белов Ан.С., Медведева А.А.
Белгородский государственный национальный исследовательский университет, Белгород, РФ

В работе предложен метод сжатия речевых данных без пауз на основе оптимального квантования по уровню коэффициентов разложения отрезков речевых сигналов по собственным векторам субполосных матриц из *m*-информационных частотных интервалов с применением кодовых книг квазиоптимальных квантователей, применение которого позволяет в зависимости от величины разрядности исходных отсчетов указанных сигналов обеспечить коэффициент сжатия до 12 раз.

Ключевые слова: отрезок речевого сигнала, речевые данные, распределение энергии, субполосная матрица, собственные векторы субполосной матрицы, информационные частотные интервалы, кодовые книги квазиоптимальных квантователей, коэффициент сжатия

Постановка задачи

Проблема уменьшения объемов битовых представлений речевых данных при их хранении и передаче рассматривается в работах многих авторов, особенно специалистов в области телекоммуникаций, что подтверждается результатами анализа научно-технической литературы [1-4].

При этом отмечаются два основных аспекта: необходимость обнаружения с последующим их кодированием пауз, возникающих между отдельными словами и в режиме диалога занимающих до 60% длительности исходных звукозаписей, и сокращение объемов битовых представлений собственно звуков речи без пауз. Существующие методы сжатия звуков речи без пауз с использованием грубого квантования по уровню основываются на психоакустической модели, что приводит к необходимости применения так называемых субполосных преобразований отрезков (векторов) отсчетов речевых сигналов, позволяющих получить другие векторы, подвекторы которых отражают частотные свойства исходного вектора в выбранных диапазонах оси частот. Именно компоненты этих подвекторов подвергаются квантованию по уровню с различными шагами, чем достигается учет частотно-избирательных свойств человеческого слуха. В настоящее время для субполосного преобразования принято использовать процедуру прореживания выходных последовательностей КИХ-фильтров (фильтров с конечной импульсной характеристикой), настроенных на соответствующие участки оси частот. Такая процедура субполосного преобразования не является оптимальной в смысле минимума погрешностей аппроксимации спектров исходных векторов в выбранных частотных диапазонах, что приводит к увеличению погрешностей восстановления данных по квантованным значениям