APPLICATION OF BROADBAND SIGNALS AT THE REMOTE MANAGEMENT OF THE RADIO SET ON LONG DISTANCE CHANNELS

Nazarov S.N., Pjatakov A.I.

In work ways of the decision of a problem of shortage of transmission capacity to radio networks of a decameter range, including military-oriented are analyzed. The present work is devoted development of algorithm of performance of the adaptive radio communication systems with simultaneous transmission to one channel of reports of information and control instructions mode of operations a radio set, and also a procedure of an estimation of parameters broadband the signals used for carrying over of control instructions.

It is offered, for magnifying of transmission capacity of the channel, a service information operating mode of operations by a radio set to transmit not mixed up with information blocks, and simultaneously, in a common strip of the channel. For service information carrying over to use broadband signals.

Keywords: *control instruction, signal spectral concentration, noise level.*

Назаров Сергей Николаевич, к.т.н., доцент, докторант Кафедры «Телекоммуникации» Ульяновского государственного технического университета. Тел. (8-842) 243-54-00; 8-903-338-34-72. E-mail: art3456@rambler.ru

Пятаков Анатолий Иванович, к.т.н., главный специалист ФНПЦ ОАО НПО «Марс». Тел. (8-842) 239-80-59. E-mail: art3456@rambler.ru

ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ И БЕЗОПАСНОСТЬ ОБОРУДОВАНИЯ

УДК 519.72, 621.391

МОДЕЛИРОВАНИЕ КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ЭНТРОПИЕЙ ЕСТЕСТВЕННЫХ И ИСКУССТВЕННЫХ БИОМЕТРИЧЕСКИХ ЯЗЫКОВ

Иванов А.И., Майоров А.В., Надеев Д.Н., Фунтиков В.А.

Показано, что функция изменения показателя энтропии естественных и искусственных языков однозначно связана с параметрами высокоразмерной матрицы корреляционного связывания случайных кодов. Для любого из естественных или искусственных языков может быть построен соответствующий генератор случайных последовательностей, одновременно воспроизводящий и упорядоченную матрицу парных корреляций языка, и его экспоненту снижения энтропии по мере роста размерности наблюдателя.

Ключевые слова: моделирование, биометрические коды, энтропия, высокоразмерная корреляционная матрица.

Введение

Задача моделирования естественных и искусственных языков возникает во многих практических приложениях. Традиционно этим занимались криптоаналитики и лингвисты [1-2]. Новым направлением науки, использующим языковые модели, является биометрия [3]. Высоконадежные нейросетевые преобразователи биометрия-код, выполненные по требованиям отечественного стандарта [4], при их тестировании ведут себя как источники некоторого биометрического языка, порождая сильно связанные между собой кодовые последовательности. Естественно, что эти последовательности можно исследовать через вычисление их энтропии и плотности распределения значений парных коэффициентов корреляции [5-6]. При исследовании влияния многомерных статистик той или иной кодовой последовательности на ее функцию энтропии необходимо уметь моделировать эти кодовые последовательности с разными уровнями корреляционных связей.

Генерирование случайных кодов с равномерной корреляционной матрицей

Примитивным решением задачи является пренебрежение корреляционными связями. В этом случае для генерирования случайных кодов можно использовать достаточное число независимых генераторов случайного «белого» шума. Пойдем на заведомую избыточность описания и будем считать, что система из n независимых случайных генераторов данных $x_{i,j}$ порождается путем псевдоумножения вектора их данных на единичную корреляционную матрицу в соответствии с формулой (1).

Очевидно, что псевдоумножение на единичную матрицу ничего не дает, и данные на выходе останутся независимыми. Корреляционная матрица выходной последовательности кодов оказывается единичной.

Легко показать, что если нули в матрице формулы (1) заменить на некоторое постоянное число $a < 1$, то входные и выходные данные системы будут существенно различаться. Входные данные останутся независимыми, а выходные данные будут зависимыми. При этом все коэффициенты, находящиеся вне корреляционной матрицы, оказываются одинаковыми (2).

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \times \begin{bmatrix} x_{1,i} \\ x_{2.i} \\ \cdots \\ x_{n,i} \end{bmatrix} = \begin{bmatrix} x_{1,i} \\ x_{2.i} \\ \cdots \\ x_{n,i} \end{bmatrix} \Rightarrow \quad R = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \qquad (1)$$

$$\begin{bmatrix} 1 & a & \cdots & a \\ a & 1 & \cdots & a \\ \cdots & \cdots & \cdots & \cdots \\ a & a & \cdots & 1 \end{bmatrix} \times \begin{bmatrix} x_{1,i} \\ x_{2.i} \\ \cdots \\ x_{n,i} \end{bmatrix} = \begin{bmatrix} y_{1,i} \\ y_{2.i} \\ \cdots \\ y_{n,i} \end{bmatrix} \Rightarrow \quad R = \begin{bmatrix} 1 & r & \cdots & r \\ r & 1 & \cdots & r \\ \cdots & \cdots & \cdots & \cdots \\ r & r & \cdots & 1 \end{bmatrix} \qquad (2)$$

Номограмма зависимости значения параметра a связывающей матрицы от значения параметра r корреляционных матриц размерностью 2; 4; 8; 16; 32; 64; 128 и 256 приведена на рис. 1.

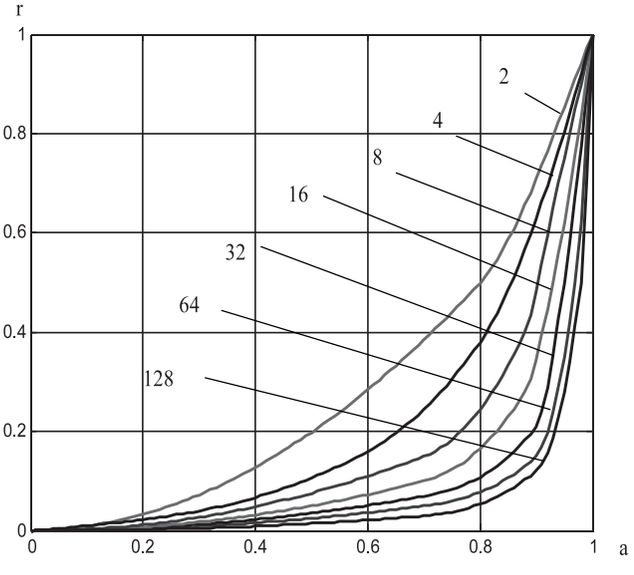

Рис. 1. Номограмма связи параметров a и r для разных размерностей генераторов зависимых данных

Из рис. 1 видно, что с повышением размерности задачи моделирования зависимость параметра a связывающей матрицы с коэффициентами корреляции становится все более и более нелинейной. По мере роста размерности задачи кривая связи $r(a)$ все более и более сильно прижимается к горизонтальной и вертикальной осям координат.

Генерирование случайных кодов, воспроизводящих статистики синтетических языков преобразователей биометрия-код

Генерирование кодов с равномерной корреляционной матрицей плохо отражает реальные данные биометрических кодов. В связи с этим для большей реалистичности данных необходимо выбирать коэффициенты a случайными, причем желательно использовать два случайных генератора нормальных данных с одинаковыми среднеквадратическими отклонениями и симметричными математическими ожиданиями a и $-a$. Пример распределения значений подобных генераторов приведен на рис. 2.

При моделировании зависимых выходных кодов биометрических преобразователей связывающая матрица может быть как симметричной, так и асимметричной. Естественно, что более удобными для моделирования являются симметричные связывающие матрицы. Они формируются путем случайного выбора данных двух генераторов и подстановки этих данных в верхнюю часть матрицы, далее нижняя часть матрицы заполняется зеркальным отражением верхней части матрицы.

Пример распределения значений парных коэффициентов корреляции, соответствующий распределению значений симметричной связывающей матрицы, полученных от генераторов случайных данных с распределениями, показанными на рис. 2, приводится на рис. 3.

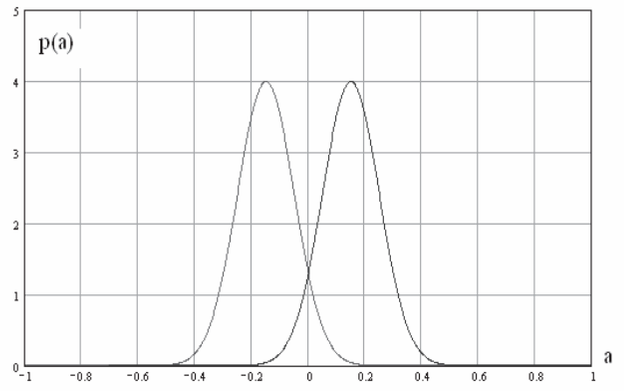

Рис. 2. Пример распределения значений двух генераторов случайных значений параметра *a* и *-a*, позволяющих получать случайные значения элементов связывающей данные матрицы

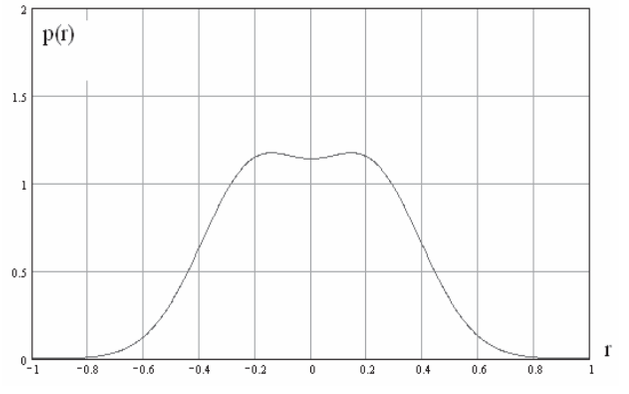

Рис. 3. Распределение значений парных коэффициентов корреляции, полученное при использовании данных двух симметричных генераторов параметра *a* связывающей матрицы

Предложенный выше подход к имитации биометрических кодов конструктивен, так как позволяет добиваться любых распределений парных коэффициентов корреляции воспроизводимой кодовой последовательности, подбирая (регулируя) всего два параметра двух генераторов (их математическое ожидание и среднеквадратическое отклонение). Если пытаться решить туже самую задачу, пользуясь классическим подходом Шалыгина [7], то решить задачу для матриц высокой размерности не удается. Предлагаемый подход позволяет решать задачу для матриц очень высокой размерности: 32; 64; 128; 256; 512 и 1024. При этом значительных вычислительных затрат не требуется, а задача вычисления высокоразмерной матрицы параметров моделирования оказывается устойчивой.

Описанный выше подход к моделированию разработан с ориентацией на имитацию искусственных биометрических языков, являющихся откликами обученных нейросетевых преобразователей биометрия-код, выполненных по требованиям ГОСТ Р 52633-2006. Именно для этого класса устройств характерны матрицы корреляционных парных связей, имеющих случайный характер (параметры соответствующей корреляционной матрицы вне ее диагонали случайны).

Генерация кодов, воспроизводящих энтропию и корреляции естественных языков

Необходимо отметить, что описанный выше подход к моделированию кодовых последовательностей неприменим к естественным языкам (например, русскому языку или английскому языку). Проведенные исследования показали, что для естественных языков характерны корреляционные матрицы взаимосвязи со случайными знаками коэффициентов парной корреляции и далеко не случайным значением их модулей. Все естественные языки имеют модули коэффициентов корреляции, монотонно убывающие по мере удаления положения коэффициента от диагонали корреляционной матрицы. В связи с тем, что модули коэффициентов корреляции связаны монотонными функциями с параметрами *a* (см. рис. 1), модули параметров связывающей матрицы будут также уменьшаться по мере удаления их от диагонали связывающей матрицы *a* в формуле (2).

Очевидно, что рассчитать модули корреляционной матрицы кодов естественного языка нетрудно. На рис. 4 приведены соответствующие функции убывания модулей коэффициентов парной корреляции для русского, английского и татарского языков при использовании однобайтной кодировки.

Так как функции убывания модулей коэффициентов корреляции естественных языков известны, по ним легко можно восстановить значение модулей элементов связывающей матрицы *a* выражения (2). Переход от модулей коэффициентов корреляции к параметрам связывающей матрицы *a* осуществляется путем применения номограммы (рис. 1). Таким способом удается получать кодовые последовательности, полностью эквивалентные по их энтропии русскому, татарскому, английскому или любому другому естественному языку.

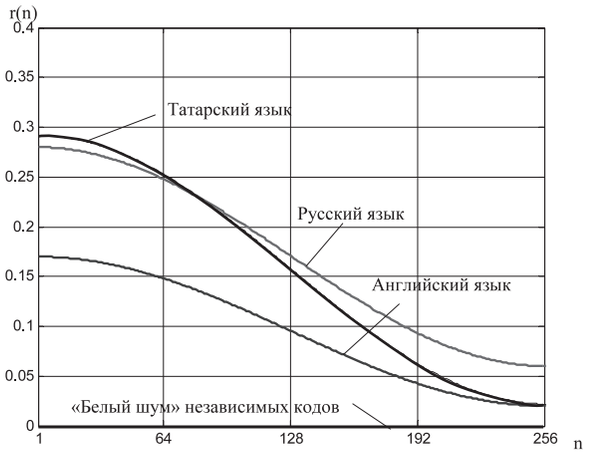

Рис. 4. Зависимость модулей коэффициентов корреляции естественных языков от расстояния до диагонали корреляционной матрицы

Примеры убывающих функций относительной энтропии (энтропии, приходящейся на один бит кода) для естественных языков и постоянная функция относительной энтропии белого шума приведены на рис. 5.

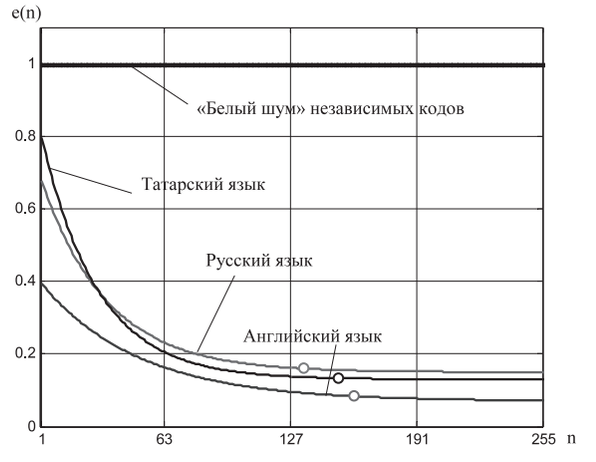

Рис. 5. Убывание относительной энтропии кодовых последовательностей русского, английского и татарского естественных языков

Из рис. 5 видно, что идеальный «белый шум» всегда обладает максимально возможной энтропией. Энтропия русского языка перестает изменяться для групп с числом букв более 17 (число бит $n = 17 \cdot 8 = 136$). Как следствие, показатель экспоненты относительной энтропии русского языка составляет 17/3 = 6,4 буквы (45,3 бита).

Для английского языка стабильный участок начинается после 22 буквы (показатель затухания экспоненты составляет 7,1 буквы, или 56,8 бита). Для татарского языка изменение относительной энтропии прекращается для расстояний в 20 и более букв.

Исходя из приведенных данных, должны выбираться размерности генераторов имитационных кодов того или иного естественного языка. Так, для имитаторов кодов русского языка необходимо использовать в формуле (2) связывающие матрицы размерностью 136 параметров (17 знаков в 8-битной кодировке). При этом каждый такт работы 136-мерного генератора будет давать 136-битный кодовый пакет. Практика показала, что при генерации каждого из таких последовательных пакетов знаки элементов связывающей матрицы должны выбираться случайно. В итоге получается кодовая последовательность, хорошо воспроизводящая плотность распределения парных коэффициентов побитной корреляции кодов русского языка.

Для татарского языка приходится увеличивать размерность связывающей матрицы до 160 одновременно учитываемых параметров. Английский язык требует еще большего увеличения размерности связывающей матрицы – до 176 одновременно учитываемых параметров.

Заключение

Изложенный в данной статье подход к моделированию естественных и искусственных языков позволяет относительно малыми вычислительными ресурсами воспроизводить кодовые последовательности любой длины. При этом размерность связывающих матриц может составлять 136; 160; 176; 256; 512 и 1024 параметра. Технические ограничения, обусловленные применением классического подхода к моделированию [7], снимаются. Вычислительная сложность предложенных в данной статье процедур имитационного моделирования оказывается линейно связана с размерностью решаемой задачи. То есть удается снизить кубический рост сложности вычислений, характерный для классики [7], до линейной, что делает задачу легко реализуемой на практике.

Литература

1. Яглом А.М., Яглом И.М. Вероятность и информация. М.: Дом Книги, 2007. – 512 с.
2. Bell T.C., Cleary J.G., Witten I.H. Text compression. Prentice Hall, Englewood Cliffs, New Jersey 07632, 1990. – 320 p.
3. Малыгин А.Ю., Волчихин В.И., Иванов А.И., Фунтиков В.А. Быстрые алгоритмы тестирования нейросетевых механизмов биометрико-криптографической защиты информации. Пенза: Изд. ПГУ, 2006. – 161 с.
4. ГОСТ Р 52633-2006. Защита информации. Техника защиты информации. Требования

к средствам высоконадежной биометрической аутентификации.
5. Надеев Д.Н. Моделирование биномиального зависимого закона распределения значений вероятностей ошибок нейросетевых преобразователей для высоконадежной биометрической защиты // Вопросы защиты информации. №3, 2008. – С. 31-35.
6. Надеев Д.Н., Иванов А.И. Модуль-нормальная связь коэффициентов парной корреляции со стойкостью нейросетевой защиты // Вопросы защиты информации. №3, 2008. – С. 35-38.
7. Шалыгин А.С., Палагин Ю.И. Прикладные методы статистического моделирования. Л.: Машиностроение, 1986. – 320 с.

CODE CHAINS MODELLING WITH ENTROPY NETURAL AND SYNTETIC LANGUAGE

Ivanov A.I., Mayorov A.V., Nadeev D.N., Funtikov V.A.

It is shown, that changing entropy of natural and synthetic languages function is unambiguously concerned with parameters of hi-dimension correlation matrix of random code chains. For any natural or synthetic languages can be constructed the generator of random sequences reproducing sorting pair-correlation matrix of language and its exponent of lowering entropy, when spectator dimension is growth.

Keywords: *modeling, biometric codes, entropy, hi-dimension correlation matrix.*

Иванов Александр Иванович, д.т.н., доцент, начальник Лаборатории нейросетевых и биометрических технологий ФГУП «ПНИЭИ» (г. Пенза). Тел. (8-841) 259-33-10.
Майоров Александр Викторович, инженер ФГУП «ПНИЭИ». Тел. 8-906-397-24-27. E-mail: sasha.maiorov@mail.ru
Надеев Дамир Наилевич, к.т.н., м.н.с. ФГУП «ПНИЭИ». Тел. (8-841) 259-33-10.
Фунтиков Вячеслав Александрович, к.т.н., генеральный директор ФГУП «ПНИЭИ». Тел. (8412) 59-33-10.

УДК 681.3

АЛГОРИТМ ЦИФРОВОЙ ПОДПИСИ НА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Бабенко М.Г., Стрекалов Ю.А., Червяков Н.И.

В статье проанализированы существующие алгоритмы цифровой подписи на эллиптической кривой. Выработаны требования для построения алгоритма цифровой подписи на эллиптической кривой над кольцом Z_q, все вычисления в которой производятся с использованием системы остаточных классов.

Ключевые слова: эллиптическая кривая, цифровая подпись, криптосистемы, поля Галуа, система остаточных классов, дискретный логарифм, сингулярные и несингулярные кривые.

Введение. Постановка задачи

Эллиптические кривые над конечными полями – один из самых перспективных инструментов для построения криптографических алгоритмов [1]. Это обусловлено тем, что эллиптическая кривая обеспечивает максимально возможную для криптосистемы с открытым ключом стойкость на один бит размера задачи [2]. Эллиптическая кривая E над простым полем F_p, где $p > 3$, задана уравнением в форме Вейерштрассе

$$E(F_p): y^2 = x^3 + ax + b, \text{ где } 4a^3 + 27b^2 \neq 0. \quad (1)$$

Решение уравнения (1) совместно с бесконечно удаленной точкой задает множество точек эллиптической кривой.

Алгоритм формирования цифровой подписи на эллиптической кривой состоит из двух этапов:

1. Сжатие текста M до размера поля с помощью однонаправленной хеш-функции $h(M)$.

2. Шифрование $h(M)$ с помощью секретного ключа отправителя на эллиптической кривой.

Первый этап формирования цифровой подписи – алгоритмы вычисления хеш-функций по SHA, ГОСТ Р34.11-94 и др. – в данной статье мы рассматривать не будем.

Проанализируем второй этап формирования цифровой подписи – шифрование $h(M)$ с ис-