УДК 621.391.037.3

И.Ю. Давыдов, Д.А. Козлов, С.В. Шахтанов, М.Ю. Шибаева

ПЕРЕСТАНОВОЧНОЕ ДЕКОДИРОВАНИЕ В СИСТЕМЕ КОМБИНАЦИЙ КОДОВЫХ КОНСТРУКЦИЙ ПРИ ОЦЕНКЕ БИОМЕТРИЧЕСКИХ ДАННЫХ

Давыдов Иван Юрьевич, *окончил магистратуру Ульяновского государственного технического университета по направлению «Телекоммуникационные технологии и системы связи», аспирант кафедры «Телекоммуникации» УлГТУ. Имеет статьи в области помехоустойчивого кодирования и защиты информации. [e-mail: 1Davydov2i@gmail.com].*

Козлов Денис Александрович, *окончил Ульяновский институт гражданской авиации им. главного маршала авиации Б.П. Бугаева, аспирант кафедры «Обеспечение авиационной безопасности» УИ ГА. Начальник центра транспортной (авиационной) безопасности (Ульяновск). Имеет статьи в области авиационной безопасности. [e-mail: peccab@mail.ru].*

Шахтанов Сергей Валентинович, *окончил Ленинградское Высшее Военное Инженерное училище связи, старший преподаватель кафедры «Инфокоммуникационные технологии и системы связи» Нижегородского государственного инженерно-экономического университета. Имеет публикации в области помехоустойчивого кодирования и защиты информации. [e-mail: r155p@bk.ru].*

Шибаева Мария Юрьевна, *окончила факультет информационных технологий и систем связи НГИЭУ, магистрант кафедры «Инфокоммуникационные технологии и системы связи» НГИЭУ. Имеет публикации в области помехоустойчивого кодирования и защиты информации. [e-mail: shibaevamarya@yandex.ru].*

Аннотация

Современные телекоммуникационные системы и средства защиты данных от помех естественного и антропогенного характера в виде избыточных кодов все активнее используются в различных приложениях, связанных с обработкой биометрических данных. Большой объем публикаций в этой предметной области посвящен кодам с малой плотностью проверок на четность, полярным кодам (ПК), турбокодам с итеративными преобразованиями данных, реализующих алгоритм «распространения доверия». Указанные кодовые конструкции обеспечивают требуемые вероятностные характеристики, но процедура декодирования таких кодов занимает большие временные интервалы, что неприемлемо с точки зрения длительности цикла управления биометрическими данными в системах, критичных к временным задержкам. В работе предлагается использовать принцип перестановочного декодирования (ПД), который применяется к систематическим блоковым кодам. Указанный метод позволяет в полной мере использовать корректирующие возможности избыточных кодов, но в классической трактовке требует громоздких матричных вычислений, что не позволяет использовать положительные свойства метода по исправлению ошибок. Сложность вычислительного процесса оказывается избыточно высокой. Поэтому для снижения отрицательного эффекта в системе ПД предлагается использовать когнитивный принцип обработки данных на канальном уровне, что существенно снижает сложность реализации декодера и обеспечивает применение ПД в системах управления биометрическими данными субъектов, например, при автоматизации процессов обеспечения транспортной безопасности. Особое внимание уделено комбинации кодов в формате каскадного кодирования. Впервые дается описание подобной схемы применительно к ПК и недвоичным кодам Рида-Соломона (РС).

Ключевые слова: мягкое решение символа, перестановочное декодирование, когнитивная карта декодера, каскадное кодирование.

doi: 10.35752/1991-2927-2019-2-56-85-92

PERMUTATION DECODING IN THE SYSTEM OF COMBINATIONS CODE DESIGNS IN THE EVALUATION OF BIOMETRIC DATA

Ivan Iurevich Davydov, *graduated with a Master degree from Ulyanovsk State Technical University in Telecommunication Technologies and Communication Systems; a postgraduate student of the Department of*

Telecommunications of Ulyanovsk State Technical University; an author of articles in the field of error-proof coding and information security. e-mail: 1Davydov2i@gmail.com.

Denis Aleksandrovich Kozlov, *graduated from the Ulyanovsk Institute of Civil Aviation; Head of Ulyanovsk Transport (Aviation) Security Center; a postgraduate student of the Department of Aviation Security Assurance at the Ulyanovsk Institute of Civil Aviation named after Chief Air Marshal B.P. Bugaev; an author of articles in the field of aviation security. e-mail: peccab@mail.ru.*

Sergei Valentinovich Shakhtanov, *graduated from the Leningrad Higher Military Engineering School of Communications; Senior Lecturer of the Department of Infocommunication Technologies and Communication Systems at the Nizhny Novgorod State University of Engineering and Economics; an author of publications in the field of error-proof coding and information protection. e-mail: r155p@bk.ru.*

Mariia Iurevna Shibaeva, *graduated from the Faculty of Information Technologies and Communication Systems at the Nizhny Novgorod State University of Engineering and Economics; Master's Degree Student of the Department of Infocommunication Technologies and Communication Systems at the Nizhny Novgorod State University of Engineering and Economics; an author of publications in the field of error-proof coding and information protection. e-mail: shibaevamarya@yandex.ru.*

Abstract

State-of-the-art telecommunication systems and means of data protection against natural and anthropogenic interference in the form of redundant codes are increasingly used in various applications related to the processing of biometric data. A large volume of publications in this subject area is devoted to codes with a low density of parity checks, polar codes, turbocodes with iterative data transformations that implement the algorithm of "belief propagation". These code constructions provide the required probabilistic characteristics but the procedure of decoding such codes takes long time intervals, which is unacceptable in terms of the duration of the cycle of biometric data management in systems critical to time delays. The paper proposes to use the principle of permutation decoding (PD), which is applied to systematic block codes. This method allows to fully use the corrective capabilities of redundant codes but in the classical interpretation requires cumbersome matrix calculations, which does not allow to use the positive properties of the method for error correction. The complexity of the computational process is excessively high. Therefore, to reduce the negative effect in the PD system, it is proposed to use the cognitive principle of data processing at the channel level, which significantly reduces the complexity of the decoder implementation and ensures the use of PD in the control systems of biometric data of subjects, for example, in the automation of transport security processes. Special attention is paid to the combination of codes in the format of cascade coding. For the first time, a description of such a scheme is given for polar codes and non-binary Reed-Solomon (RS) codes.

Key words: soft symbol solution, permutation decoding, cognitive map decoder, concatenated code.

Введение

Объективной основой интеллектуализации многих перспективных информационных и технологических процессов является совершенствование процедуры управления при их реализации в реальном масштабе времени. Последнее обстоятельство требует поиска путей сокращения цикла управления, внедрения принципов когнитивной адаптации и искусственного интеллекта. Широкое применение в таких системах каналов для связи управляющего объекта с объектом (объектами) управления требует безусловного использования средств помехоустойчивого кодирования с целью защиты команд управления от воздействия различного рода деструктивных факторов. Становится очевидным, что жесткие требования к длительности цикла управления не позволяют использовать в полной мере для достижения указанной цели ряд положений теории помехоустойчивого кодирования, например, в виде систем турбокодирования и итеративных преобразований данных. На этом фоне возникает проблема эффективного применения коротких помехоустойчивых кодов с максимальным использованием введенной в такой код избыточности и быстрой идентификацией команд управления. Решение подобной задачи носит актуальный характер при обработке данных в системе высокоскоростных когерентных сетей при их согласовании с возможностями процессоров оконечных устройств. Анализ показал, что в наибольшей степени решению указанных задач соответствует метод перестановочного декодирования (ПД) систематических кодов при модификации его математической модели с использованием концепции когнитивной обработки данных. Принцип ПД может быть использован в системах каскадного кодирования, при этом на внутренней ступени декодирования данных продуктивно использовать полярные коды (ПК), для которых в качестве мягких решений применяются коэффициенты Бхаттачария [1].

Цель работы – разработка производительных алгоритмов декодирования помехоустойчивых кодов на базе когнитивной метафоры в системе оценки биометрических данных.

Биометрические данные как основа автоматизации контроля пассажиропотока

Повышение угроз террористических актов обострило недоверие многих государств к международным паспортам на бумажных носителях. Это привело к разработке национальных биометрических стандартов, которые ориентированы на дублирование органолептической биометрии автоматизированным биометрическим контролем личности. Ряд государств выступили с инициативой создания нового поколения биометрических паспортов с радиочитаемой микросхемой, где должны находиться биометрические данные проверяемого человека [2, 3]. При этом предполагается, что подлинность биометрических данных в микросхеме паспорта гарантируются совпадением их номера с номером в паспорте и электронной цифровой подписью под данными. На данный момент считается, что подделать электронную цифровую подпись намного сложнее, чем создать фальшивый бланк паспорта с присутствующими в нем элементами защиты.

Поэтому совершенствование организации пассажиропотоков на уровне авиакомпаний и аэропортов тесно связано с внедрением комплексных автоматизированных решений на базе новой концепции цифровой идентификации авиапассажиров по биометрическим параметрам: по лицевому изображению с временем бесконтактной идентификации $T_{ли}$, по голосу с временем контроля $T_{г}$ и отпечаткам пальцев с временем $T_{оп}$, учитывающим контакт субъекта с контроллером. Основные преимущества применения предлагаемой концепции заключаются в следующем: повышение пропускной способности точек контроля транспортной системы, сокращение количества обслуживающего персонала на них, повышение эффективности обеспечения транспортной (авиационной) безопасности. Конечно, предпочтение отдается оценке лицевого изображения, поскольку всегда выполняется условие $T_{ли} << T_{г} < T_{оп}$. Вместе с тем, основной проблемой внедряемой концепции является постоянная изменчивость биометрических характеристик пассажиров, которая может породить возникновение ошибок в идентификации, не зависящих от непреднамеренных действий владельцев или преднамеренных действий со стороны потенциального нарушителя. Для повышения надежности функционирования комплексов персональной идентификации пассажиров в части исправления представленных ошибок, наиболее подходящим является использование помехоустойчивого кодирования. Это связано с тем, что использование контроля лицевого изображения не требует получения собственно изображения, а содержит параметры между критическими точкам лица субъекта, и такие методы позволяют в значительной степени повысить достоверность принимаемой информации. Некоторые результаты использования алгоритмов помехоустойчивого кодирования в системах биометрической идентификации представлены в работе [3].

Вместе с тем в открытой печати практически отсутствует информация о путях модернизации и совершенствовании комплексов (систем) персональной идентификации пассажиров в части повышения надежности посредством разработки и модификации методов и алгоритмов обработки, хранения и ввода-вывода информации.

Проблема идентификации состоит из двух этапов. Этап регистрации, на котором записываются данные пользователя, их сжатие и сохранение, например, параметры отпечатков пальцев или захвата некоторых важных особенностей лица субъекта. На этапе идентификации, наблюдения отпечаток пальца или отпечатки нескольких пальцев, параметры лица субъекта сравниваются с сохраненной информацией в базе данных. После чего дается утвердительный ответ, а в случае сомнений осуществляется контроль субъекта по дополнительным параметрам. При этом оценка параметров лица осуществляется бесконтактным методом, что способствует увеличению общей пропускной способности системы контроля. Это особенно важно для крупных транспортных узлов, включая аэропорты. И именно по этой причине повышение скорости обработки данных в таких системах имеет принципиальное значение.

Алгоритм ПД и его свойства

Классический метод ПД систематических избыточных кодов описан в работе [4]. Более поздние интерпретации математической модели этого метода даны в работах [5–8]. Алгоритмическое представление указанного способа заключается в том, что передатчик использует систематический избыточный (n,k)-код, где n – общая длина кодовой комбинации, а k – число информационных разрядов в ней. Порождающая матрица кода $\mathbf{G}$ с единичной матрицей слева. В ходе передачи произвольного вектора такого кода $V_{n,k}$ по каналу с аддитивным белым гауссовским шумом на него накладывается вектор помех e_n. Приемник принимает вектор вида $V_{re} = V_{n,k} \oplus e_n$, где символ $\oplus$ означает операцию сложения по модулю два. Задачей приемника является идентификация вектора e_n и выделение из вектора V_{re} команды управления с вероятностью ее правильного восстановления P_r. В системе ПД для решения подобной задачи необходимы три этапа обработки принятых данных.

Во-первых, на длине вектора V_{re} в системе мягкого декодирования среди n символов необходимо выделить, по крайней мере, k надежных символов. Для этого используются целочисленные мягкие решения символов (МРС) λ_i, где $i = \overline{1,n}$ – нумераторы симво-

лов вектора V_{re}, а $\lambda = \overline{0,7}$ – МРС по Витерби [4]. Далее массив символов длины n сортируется в порядке убывания значений λ_i, используя, например, метод пузырька с наименьшим значением λ_i справа, а между исходной, случайной последовательностью нумераторов МРС и их упорядоченной последовательностью фиксируется биекция в виде перестановочной матрицы $\mathbf{P}$. Далее по наиболее надежным k' (левым) символам упорядоченного массива формируется новый информационный вектор $V_{k'}$ [5]. Сложность реализации данного этапа декодирования обычно оценивается как $O(n^2)$.

Во-вторых, на основе матрицы $\mathbf{P}$ осуществляется перестановка столбцов порождающей матрицы $\mathbf{G}$ исходного (основного) кода с образованием переставленной матрицы $\mathbf{G}'$. В матрице $\mathbf{G}'$ выделяются первые k столбцов, совокупность которых образует квадратную матрицу $\mathbf{Q}$, для которой последовательно отыскиваются определитель Δ, матрица миноров, транспонированная матрица миноров и обратная матрица $\mathbf{Q}^{-1}$. Умножая $\mathbf{Q}^{-1} \times \mathbf{G}' = \mathbf{G}'_{\mathbf{sis}}$, получают порождающую матрицу эквивалентного кода в систематической форме. Сложность реализации второго этапа декодирования из-за наличия матричных вычислений представляется как $O(n^3)$.

На третьем, заключительном этапе, осуществляется кодирование вектора $V_{k'}$ путем умножения его на матрицу $\mathbf{G}'_{\mathbf{sis}}$ с образованием вектора эквивалентного кода V_{eq}. После этого нумераторы вектора V_{eq}, а вместе с ними и символы, путем умножения на матрицу $\mathbf{P}^{\mathbf{T}}$ приводятся к канонической последовательности $\overline{V}_{eq}$, и, выполняя $V_{re} \oplus \overline{V}_{eq} = e_n$, находят вектор ошибок, исказивший переданный вектор $V_{n,k}$.

Становится очевидным, что последовательное выполнение описанных шагов алгоритма в реальной системе обработки данных для каждого принятого вектора становится серьезной вычислительной нагрузкой для процессора приемника, поэтому классический вариант рассматриваемого метода практического применения не нашел. Однако асимптотические характеристики ПД оказываются достаточно привлекательными. В работе [8] показано, что по критерию энергетического выигрыша кода (ЭВК) метод ПД для двоичных кодов является лучшим, а для недвоичных избыточных кодов позволяет полностью использовать введенную в код избыточность.

Приведенный анализ показывает, что целевая функция $F\{\bullet\}$ алгоритма ПД содержит несколько стохастических параметров и единственную детерминированную компоненту. Суть целевой функции можно представить следующим образом:

$$F\{\bullet\} = \begin{cases} \{V_k\} \oplus e(h), \\ \{P_n\}, \end{cases}$$

где $\{V_k\}$ – множество случайных векторов, составляющих суть команды управления, а e_h – вероятность появления векторов помех длины n как функции отношения «сигнал-шум» при $h = E_b / N_0$, действующих на элементы множества $\{V_k\}$. К детерминированной составляющей целесообразно отнести множество перестановок $\{P_n\}$, формирующихся на втором этапе реализации ПД. Принципиально такие перестановки могут быть вычислены заранее (в процессе обучения декодера), и результаты вычисления матриц вида $\mathbf{G}'_{\mathbf{sis}}$ могут быть зафиксированы в памяти декодера, по сути, в его когнитивной карте. В этом случае сложный в реализационном отношении второй этап алгоритма ПД однозначно теряет свое негативное значение в реализации процедуры ПД [9, 10].

Модель перестановочного декодера с когнитивной метафорой

Принципиальной разницы между алгоритмами ПД двоичных и недвоичных кодов нет. Исключение составляет процедура оценки определителя Δ матрицы $\mathbf{Q}$ в ходе реализации второго шага алгоритма. Поскольку двоичные коды не являются максимально декодируемыми, то для ряда перестановок столбцов порождающей матрицы $\mathbf{G}$ может оказаться, что $\Delta = 0$ [9]. Следовательно, для такой перестановки создать эквивалентный код не представляется возможным и необходима новая корректировка значений МРС по первому этапу. Исследования показали, что подобная ситуация для двоичных кодов характерна для 20% перестановок от их общего числа [9]. Для недвоичных кодов, например, кодов РС в выполнении подобной проверки нет необходимости (такие коды максимально декодируемы). Отмеченная общность алгоритмов двоичных и недвоичных групповых систематических кодов указывает на возможность их применения в системах с каскадным кодированием. Дело в том, что формирование МРС в непрерывном канале связи не всегда обеспечивает достоверные оценки. В общем случае такие оценки позволяют повысить достоверность обрабатываемых данных, но существование вероятности ошибочной регистрации МРС с высоким значением является значимой. Каскадная схема использует алгебраические методы обработки жестких решений на внутренней ступени декодирования, поэтому принудительное формирование стираний для внешнего кода оказывается более эффективным. Именно этот принцип целесообразно применять при использовании ПК [1, 3]. Достаточно ясно этот эффект описан в работе [11]. В этой же работе установлено, что при сохранении номеров позиций в перестановках k надежных и $(n-k)$ ненадежных символов следует на первом шаге

переставлять строки эталонной матрицы, а на втором шаге – столбцы этой новой матрицы. Следуя принципам когнитивной обработки данных, декодер, получив, например, кортеж значений надежных символов для первых k символов принятой комбинации и оставшихся $(n-k)$ менее надежных символов формирует матрицу $\mathbf{G}'$, исходя из структуры эталонной матрицы. Тут же доказано, что структура эталонной матрицы в силу линейности исследуемых кодов несет в себе информацию о всех перестановках выделенной группы k надежных символов, что позволяет существенно сократить объем когнитивной карты декодера (ККД). Если оценивается код длины $n = 7$, то всего эталонных матриц для такого декодера будет равно $7! = 5040$. Объем памяти ККД должен быть достаточно велик. Но с учетом результатов работы [11] объем карты снижается до значения 35 эталонных матриц, а с учетом вскрытых в указанной работе циклических свойств перестановок символов отдельной кодовой комбинации объем памяти ККД необходимо рассчитывать всего на 5 эталонных матриц. Таким образом, замена сложного вычислительного процесса на память вполне оправдана, при этом для быстрого поиска требуемой эталонной матрицы необходимо лексикографическая организации ККД. Пример такой организации для кода (неважно двоичного или недвоичного) длины $n = 7$ приведен в таблице 1.

Верхний ряд данных каждой ячейки таблицы 1 представляет каноническую форму номеров надежных оценок и соответствующий ей номер эталонной матрицы $\mathbf{G}^{\mathbf{i}}_{\mathbf{sis}}$, образ которой необходимо извлечь из памяти ККД. Нижний ряд каждой ячейки содержит номера строк надежных символов и номера столбцов ненадежных символов, которые необходимо присвоить извлеченной из памяти эталонной матрицы с номером i.

Пусть, например, сортировка надежных символов привела к последовательности (6 2 7) и некоторой последовательности ненадежных символов вида (3 5 1 4). Тогда

$$\mathbf{G}^{\mathbf{2}}_{\mathbf{sis}} = \begin{matrix} \alpha^1 & \alpha^3 & \alpha^1 & \alpha^0 & 6 \\ \alpha^6 & \alpha^2 & \alpha^2 & \alpha^0 & 7 \\ \alpha^4 & \alpha^4 & \alpha^5 & \alpha^0 & 2 \\ 3 & 4 & 5 & 1 & \end{matrix} \Rightarrow$$

$$\Rightarrow \begin{matrix} \alpha^1 & \alpha^3 & \alpha^1 & \alpha^0 & 6 \\ \alpha^4 & \alpha^4 & \alpha^5 & \alpha^0 & 2 \\ \alpha^6 & \alpha^2 & \alpha^2 & \alpha^0 & 7 \\ 3 & 4 & 5 & 1 & \end{matrix} \Rightarrow$$

$$\Rightarrow \begin{matrix} \alpha^1 & \alpha^1 & \alpha^0 & \alpha^3 & 6 \\ \alpha^4 & \alpha^5 & \alpha^0 & \alpha^4 & 2 \\ \alpha^6 & \alpha^2 & \alpha^0 & \alpha^2 & 7 \\ 3 & 5 & 1 & 4 & \end{matrix}.$$

Канонический вид первой последовательности дает (2 6 7). Из таблицы 1 становится ясно, что следует обрабатывать эталонную матрицу 2 с нумерацией строк (6 7 2) и нумерацией столбцов (3 4 5 1) с последующей их перестановкой, как показано выше. Становится очевидным, что для поиска эталонной матрицы декодер не выполняет арифметических операций в полях Галуа (для недвоичных кодов), а реализует тривиальную процедуру копирования и адресного переноса данных. В последнем случае число таких операций всегда будет

Таблица 1

Лексикографическая структура ККД

123 – 1	**124 – 2**	**125 – 3**	**126 – 4**	**127 – 1**
123 – 4567	124 – 5673	125 – 6734	126 – 7345	712 – 3456
134 – 1	**135 – 5**	**136 – 5**	**137 – 2**	**145 – 3**
341 – 2567	135 – 6724	613 – 4572	713 – 4562	451 – 2367
146 – 5	**147 – 3**	**156 – 2**	**157 – 4**	**167 – 1**
461 – 2357	714 – 5623	561 – 2347	715 – 6234	671 – 2345
234 – 1	**235 – 2**	**236 – 3**	**237 – 4**	**245 – 4**
234 – 5671	235 – 6714	236 – 7145	237 – 1456	452 – 3671
246 – 5	**247 – 5**	**256 – 3**	**257 – 5**	**267 – 2**
246 – 7135	724 – 5613	562 – 3471	572 – 3461	672 – 3451
345 – 1	**346 – 2**	**347 – 3**	**356 – 4**	**357 – 5**
345 – 6712	346 – 7125	347 – 1256	563 – 4712	357 – 1246
367 – 3	**456 – 1**	**457 – 2**	**467 – 4**	**567 – 1**
673 – 4512	456 – 7123	457 – 1236	674 – 5123	567 – 1234

равно длине кодового вектора n. В таблице 2 приводится оценка получаемого при этом выигрыша.

В таблице 3 приведены сравнительные данные по временным интервалам, необходимым для получения порождающих матриц эквивалентных кодов применительно к возможностям ПЛИС типа «ALTERA» с тактовой частотой $5 \cdot 10^7$ Гц, длительностью такта $2 \cdot 10^{-8}$ с и объемом внутренней памяти 2 Мб.

Преимущества предлагаемого метода очевидны особенно для кодов с различной корректирующей способностью при фиксированной длине кодового вектора.

Модель перестановочного декодера в системе ПК

Рассматриваемая структура ПК является типичным представителем класса блоковых кодов. Для определения возможностей таких кодов по коррекции ошибок необходимо оценить их граничные параметры. В случае линейного кода при фиксированной длине комбинации N и числе информационных разрядов K можно получить значения верхней и нижней границ для наибольшего минимального расстояния. В качестве верхней границы целесообразно использовать границу Бхаттачария, которая определяется на основе знания условных выходных распределений. В работе [1] было показано, что в случае двоичного симметричного канала (ДСК) граница Бхаттачария равна $Z = \sqrt{4 \cdot P \cdot (1-P)}$, где P – условное входное распределение. Применив неравенство Шварца к этому выражению, получим верхнюю и нижнюю границы для параметра Бхаттачария, которые равны $0 \le Z \le 1$. Для канала с двоичным входом последнее выражение примет вид [1]:

$$P_E < M \cdot \exp\left(-N\left[\ln 2 - \ln\left(1+z\right)\right]\right), \quad (1)$$

где M – число кодовых векторов в ансамбле. При этом для линейных кодов, используемых в этом классе каналов, вероятность ошибки определена без учета ансамбля сигналов (использовано в качестве ограничения по сумме). При этом

$$P_E \le \sum_K^M \exp\left(w_K \ln Z\right),$$

где w_K – веса ненулевых кодовых слов. При равенстве $M = N$ для всех $N = 2^K$ существует ортогональный код такой, что $w_K = N/2$, при всех $K \ne 1$. В этом случае получаем границу

$$P_E < M \cdot \exp\left(-N\left(-\ln Z^{0,5}\right)\right). \quad (2)$$

Легко заметить, что показатель экспоненты в выражении (2) больше, чем в (1), т. е.

$$-0,5 \cdot \ln Z \ge \ln 2 - \ln\left(1+z\right) \text{ при } 0 \le Z \le 1.$$

В этом случае неравенство выполняется тогда и только тогда, когда $Z = 1$. Из выражений (1) и (2) видно, что параметр $Z = 0$ описывает каналы без шума. С увеличением шума параметр Z монотонно возрастает. Канал становится бесполезным при $Z = 1$ [1]. Таким образом, при конструировании линейных кодов целесообразно рассматривать ансамбль кодовых векторов, вычленяя «плохие» кодовые комбинации.

Целью применения ПК является создание такой решающей схемы, при которой $Z(P) \to 0$, тем самым вероятность ошибочного приема также стремится к «0». Концепция формирования ПК построена на базе ядра Арикана. Ядром Арикана называют матрицу вида:

$$\boldsymbol{F} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

Таблица 2

Оценка выигрыша по числу операций в условиях применения когнитивной карты

Число арифметических операций при реализации классического подхода			
Код PC (7,3,5)	Код PC (15,5,11)	Код PC (15,9,7)	Код PC (15,13,3)
336	2410	2912994	68584334026
Число операций при реализации предлагаемого метода			
7	15	15	15
Выигрыш в 48 раз	Выигрыш в 1,6*10^2 раза	Выигрыш в 1,9*10^6 раза	Выигрыш в 4,6*10^9 раза

Таблица 3

Временные интервалы получения конечного результата

Классический подход			
Код PC (7,3,5)	Код PC (15,5,11)	Код PC (15,9,7)	Код PC (15,13,3)
$\approx 6,7 \cdot 10^{-6}$ с	$\approx 4,8 \cdot 10^{-5}$ с	$\approx 5,8 \cdot 10^{-2}$ с	$\approx 1,7 \cdot 10^{3}$ с
Предлагаемый метод			
$\approx 1,4 \cdot 10^{-8}$ с	$\approx 3,0 \cdot 10^{-7}$ с	$\approx 3,0 \cdot 10^{-7}$ с	$\approx 3,0 \cdot 10^{-7}$ с

а через величину $\boldsymbol{F}^{\otimes \boldsymbol{m}}$ обозначают ее m-ю кронекеровскую степень, в основе которой лежит кронекеровское (прямое) произведение матриц [1]. Для получения требуемого выходного вектора необходимо произвести преобразование последовательности таким образом, чтобы номер новой позиции i-го элемента получился как обратная запись числа i, т. е. полярное представление. Например, $1_{10} \equiv 0001_2 \to 1000_2 \equiv 8_{10}$. Таким образом, для получения соответствующей матрицы необходимо ввести матрицу перестановок B_N. Результирующая матрица $\boldsymbol{G}_N$ определяется выражением $\boldsymbol{G}_N = \boldsymbol{B}_N \cdot \boldsymbol{F}^{\otimes \boldsymbol{m}}$. Для осуществления операции поляризации необходимо произвести трансформацию скалярного канала в векторный канал, отождествляя его с функцией плотности условной вероятности выходного символа [1]. Это достигается за счет создания копий ДСК, как представлено на рисунке 1.

Рекурсия начинается с 0-го уровня ($n = 0$) посредством применения только одного экземпляра P, которому ставится в соответствие $P_0 = P$. На первом уровне рекурсии схема сочетает в себе две независимых копии P_0, тем самым мы получаем канал P_1 с вероятностью пере$^{\text{ходов}}$ $P_1\left(y_0 \middle| y_1 \middle| u_0, u_1\right) = P\left(y_0 \middle| u_0 \otimes u_1\right) \cdot P\left(y_1 \middle| u_1\right)$.

Матрица $\boldsymbol{F}^{\otimes \boldsymbol{m}}$ получается посредством прямого произведения матриц $\boldsymbol{F}$. Длина блока N определяется кронекеровской степенью $m \to 2^m$. То есть при $m = 1$ матрица $\boldsymbol{F}^{\otimes 1}$ равна ядру Арикана, при $m = 2$ и $m = 3$ имеем $\boldsymbol{F}^{\otimes 2}$ и $\boldsymbol{F}^{\otimes 3}$ соответственно. При значении $N \to \infty$ каналы P_i^{n-1} будут либо полностью бесшумные, либо полностью ненадежные.

В связи с этим информационные символы u_i, передаваемые по каналам с низким уровнем достоверности, можно считать всегда фиксированными («замороженными»). Рассмотрим принцип фиксации каналов на основе матрицы $\boldsymbol{F}^{\otimes 3}$. Строкам матрицы $\boldsymbol{F}^{\otimes 3}$ с весом $w < 4$ поставим в соответствие каналы с фиксированными значениями, равными нулю, на основе правила Рида-Маллера, как представлено на рисунке 2. Необходимо обратить внимание, что модифицированная матрица $\boldsymbol{F}_{\boldsymbol{nfr}}^{\otimes 3}$ степени $m = 3$ образуется из строк матрицы $\boldsymbol{F}^{\otimes 3}$ с весом $\boldsymbol{w} \geq 4$. Таким образом, мы переходим из пространства $2M$ в пространство M, поставив данным каналам в соответствие нулевое значение (коды с выбрасыванием). Это позволяет уменьшить вероятность ошибки для систем передачи данных. Однако стоит отметить, что для корректной оценки кодового вектора, как отмечалось ранее, целесообразно использовать границу Бхаттачария.

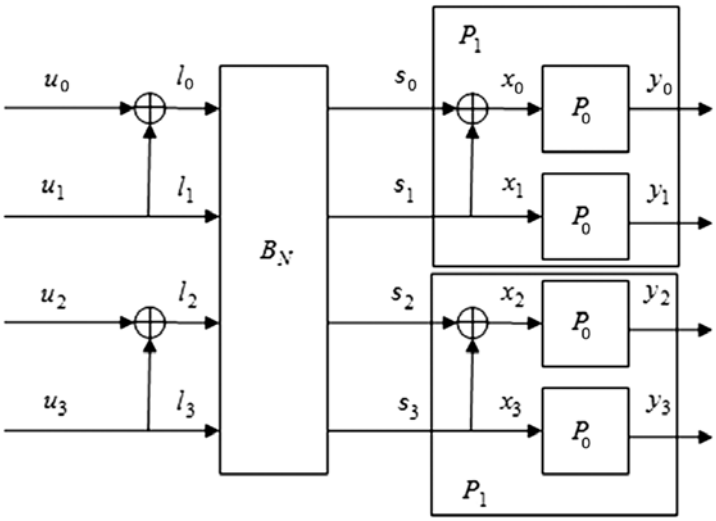

Рис. 1. Рекурсивный способ формирования кодового вектора

$$\boldsymbol{F}^{\otimes 3} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix},$$

$$x = [u_0\ u_1\ u_2\ u_3\ u_4\ u_5\ u_6\ u_7]\boldsymbol{B}_N \cdot \boldsymbol{F}^{\otimes 3},$$

$$x = [0\ 0\ 0\ u_3\ 0\ u_5\ u_6\ u_7]\boldsymbol{B}_N \cdot \boldsymbol{F}^{\otimes 3}.$$

u_0 замороженные y_0
u_1 замороженные y_1
u_2 замороженные y_2
u_3 данные y_3
u_4 замороженные y_4
u_5 данные y_5
u_6 данные y_6
u_7 данные y_7

Рис. 2. Принцип фиксации зашумленных каналов

Для матрицы $\boldsymbol{G}_N = \boldsymbol{B}_N \cdot \boldsymbol{F}^{\otimes \boldsymbol{m}}$ ранговый вектор равен Z_{N-1} = (0,996; 0,88; 0,81; 0;32; 0,68; 0,191; 0,121; 0,004). Заметно, что приведенные оценки характеризуют надежность принятых символов и являются аналогом значений МРС, вырабатываемых за счет оценки параметров сигнала на физическом уровне. Применение коэффициентов Бхаттачария с целью оценки надежности принятых битов в условиях смены параметров непрерывного канала связи подлежит безусловному дальнейшему изучению.

Заключение

ПД является разновидностью мягкого декодирования блоковых помехоустойчивых кодов. Оно основано на вычислении для каждого кодового вектора, переданного по каналу с ошибками, некоторого вектора эквивалентного кода, образующегося за счет последовательного ранжирования мягких решений и создания по наиболее надежным из них однозначной биекции принятому вектору. На этой основе вырабатывается вектор эквивалентного кода.

Применение ПК не противоречит принципам ПД и может быть успешно использовано в системах биометрической идентификации субъектов.

Основные трудности при реализации классического алгоритма ПД заключаются в преобразованиях матриц на предмет выявления свойства невырожденности переставленной матрицы кода и приведения такой матрицы к систематической форме.

В работе вскрыты закономерности матричных преобразований, характерных для групповых избыточных кодов, применение которых существенно сокращает сложность реализации декодера.

Основой подобной реализации является создание когнитивной карты декодера в канонической форме, которая позволяет выполнить вычисление эквивалентного кода по заранее подготовленному шаблону.

Использование метода позволяет существенно снизить вероятность ошибочного приема кодового вектора за счет исправления стираний за пределами метрики Хэмминга. Это позволяет повысить эффективность схем каскадного кодирования и получить в системе обмена данными дополнительный ЭВК.

СПИСОК ЛИТЕРАТУРЫ

1. Гладких А.А., Климов Р.В., Чилихин Н.Ю. Методы эффективного декодирования избыточных кодов и их современные приложения. – Ульяновск : УлГТУ, 2016. – 258 с.

2. An Introduction to Biometric Authentication Systems / Wayman, James Jain, Anil Maltoni, Davide Maio, Dario. 2005. pp. 1–20.

3. Linghui Zhon. Polar Codes for Identification Systems, Degree project in electrical engineering, Second Cycle, 30 credits Stockholm, Sweden. 2018. P. 55

4. MacWilliams F.J. Permutation Decoding of Systematic Codes // Bell System Tech. J. 1964. No 43. pp. 485–505.

5. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки : пер. с англ. / под ред. Р.Л. Добрушина, С.И. Самойленко. – М. : Мир, 1976. – 594 с.

6. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / пер. с англ. В.Б. Афанасьева. – М. : Техносфера, 2005. – 320 с.

7. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М. : Вильямс, 2003. – 1104 с.

8. Гладких А.А. Основы теории мягкого декодирования избыточных кодов в стирающем канале связи. – Ульяновск : УлГТУ, 2010. – 379 с.

9. Гладких А.А. Перестановочное декодирование как инструмент повышения энергетической эффективности систем обмена данными // Электросвязь. – 2017. – № 8. – С. 52–56.

10. Гладких А.А., Ал Тамими Т.Ф.Х. Концепция когнитивной обработки данных в системе перестановочного декодирования недвоичного избыточного кода // Электросвязь. – 2018. – № 9. – С. 69–74.

11. Гладких А.А., Наместников С.М., Пчелин Н.А. Эффективное перестановочное декодирование двоичных блоковых избыточных кодов // Автоматизация процессов управления. – 2017. – № 1 (47). – С. 67–74.

REFERENCES

1. Gladkikh A.A., Klimov R.V., Chilikhin N.Iu. *Metody effektivnogo dekodirovaniia izbytochnykh kodov i ikh sovremennye prilozheniia* [Methods for Effective Decoding of Redundant Codes and Its State-Of-The-Art Applications]. Ulyanovsk, UlSTU Publ., 2016. 258 p.

2. James Wayman, Anil Jain, Davide Maltoni, Dario Maio. *An Introduction to Biometric Authentication Systems.* 2005. pp. 1–20.

3. Linghui Zhon. *Polar Codes for Identification Systems. Degree Project in Electrical Engineering.* Stockholm, Sweden, 2018. 55 p.

4. MacWilliams F.J. Permutation Decoding of Systematic Codes. *Bell System Tech. J.,* 1964, no. 43, pp. 485–505.

5. Piterson U., Ueldon E. *Kody, ispravliaiushchie oshibki.* Per. s angl. Pod red. R.L. Dobrushina, S.I. Samoilenko [Error Correcting Codes. transl. from Engl., edited by R.L. Dobrushin, S.I. Samoilenko]. Moscow, Mir Publ., 1976. 594 p.

6. Morelos-Saragosa R. *Iskusstvo pomekhoustoichivogo kodirovaniia. Metody, algoritmy, primenenie.* Per. s angl. V.B. Afanaseva [The Art of Error Correcting Coding. Methods, Algorithms, Application. Translated from Engl. by V.B. Afanasev]. Moscow, Tekhnosfera Publ., 2005. 320 p.

7. Sklar B. *Tsifrovaia sviaz. Teoreticheskie osnovy i prakticheskoe primenenie* [Digital Communication. Fundamentals and Applications]. Moscow, Williams, 2003. 1104 p.

8. Gladkikh A.A. *Osnovy teorii miagkogo dekodirovaniia izbytochnykh kodov v stiraiushchem kanale sviazi* [Foundations of the Theory of Soft-Decision Decoding of Redundant Codes in Erasure Communication Channels]. Ulyanovsk, UlSTU Publ., 2010. 379 p.

9. Gladkikh A.A. Perestanovochnoe dekodirovanie kak instrument povysheniia energeticheskoi effektivnosti sistem obmena dannymi [Permutation Decoding as a Tool to Improve the Energy Efficiency of Data Exchange Systems]. *Elektrosviaz* [Electrosvyaz Magazine], 2017, no. 8, pp. 52–56.

10. Gladkikh A.A., Al Tameemi T.F.H. Kontseptsiia kognitivnoi obrabotki dannykh v sisteme perestanovochnogo dekodirovaniia nedvoichnogo izbytochnogo koda [The Concept of Cognitive Data Processing in the System of Permutation Decoding of Non-Binary Redundant Code]. *Elektrosviaz* [Electrosvyaz Magazine], 2018, no. 9, pp. 69–74.

11. Gladkikh A.A., Namestnikov S.M., Pchelin N.A. Effektivnoe perestanovochnoe dekodirovanie dvoichnykh blokovykh izbytochnykh kodov [Efficient Permutation Decoding of Binary Block Redundant Codes]. *Avtomatizatsiia protsessov upravleniia* [Automation of Control Processes], 2017, no. 1 (47), pp. 67–74.