

О.А. ГОМЦЯН

ОБОБЩЕННАЯ КОНЦЕПЦИЯ КАСКАДНОГО КОДИРОВАНИЯ В ЦИФРОВЫХ СИСТЕМАХ ОБРАБОТКИ ИНФОРМАЦИИ

Исследованы новые кодовые конструкции и цифровые методы модуляции, совместно применяемые в различных цифровых системах обработки информации. Известные преимущества цифровых систем обработки информации выдвигают на первый план способы защиты данных от несанкционированного доступа (НСД) и улучшения помехоустойчивости с использованием современных кодовых схем. Эти две основные задачи породили большое количество решений и применений, начиная с простейших кодов до современных сложных турбоконструкций и др. В дополнительном исследовании нуждаются также сигнально-кодовые конструкции, а также их взаимодействие с многокаскадными кодами. Помехоустойчивое кодирование в сочетании с аналого-цифровым преобразованием, перемежением и удачными кодами передачи является эффективным средством для повышения качества записи и передачи информации по различным каналам. Шифрование и сжатие предоставляют дополнительную защиту каналов связи от НСД.

Ключевые слова: каскадное кодирование, аналого-цифровое преобразование, сжатие, шифрование, помехоустойчивое кодирование, перемежение, линейное кодирование.

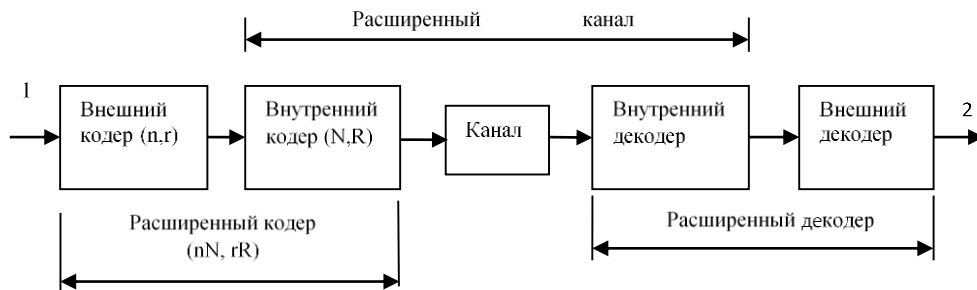
Введение. В современных цифровых системах обработки информации широкое применение получили различные методы кодирования. В общем случае при кодировании осуществляется преобразование одной цифровой информации в другую как в передатчике, так и в приемнике. Такие преобразования обычно преследуют различные цели, например, устранение избыточности, содержащейся в информации, или специальное введение избыточности при помехоустойчивом кодировании, или шифрование информации и т.д.

Отметим, что помехоустойчивое кодирование, кроме всего прочего, позволило создать современные цифровые системы записи-воспроизведения информации с огромной памятью, такие как жесткие диски, DVD, CD-ROM и др. При этом степень сложности реализации кодирующих-декодирующих устройств за счет помехоустойчивого кодирования очень мала по сравнению с выигрышем за счет высокой плотности записи.

С другой стороны, из теоремы Шеннона для канала с шумами известно, что повышение пропускной способности канала может быть достигнуто за счет увеличения длины кода, что, в свою очередь, повышает его эффективность. Однако при этом резко возрастает сложность кода, и особенно это относится к алгоритмам декодирования, т.е. практическая реализация длинных кодов затруднительна.

Постановка задачи. Для решения этой проблемы были разработаны так называемые коды-произведения или итеративные коды [1]. При этом результирующий код произвольной размерности формируется при помощи последовательных преобразований произвольного количества соответствующих образующих (составляющих) кодов. Основные параметры результирующего кода (длина, количество информационных символов и минимальное кодовое расстояние) получаются произведением соответствующих параметров составляющих кодов [1].

Модификацией итеративных кодов являются каскадные коды, предложенные Форни в работе [2]. Здесь рассмотрена уже ставшая классической двухступенчатая (двухкаскадная) схема кодирования-декодирования, как это показано на рис.1.



1 - источник сообщения; 2 - получатель сообщения;
 n - длина внешнего кода; N - длина внутреннего кода;
 nN - длина результирующего кода;
 r - скорость внешнего кодера; R - скорость внутреннего кодера;
 rR - скорость результирующего кода

Рис. 1. Схема каскадного кодирования по Форни

В работе [2] в качестве внешнего кода предлагается всегда использовать корректирующий код Рида-Соломона (РС), а в качестве внутреннего – рассмотрены как сверточный помехоустойчивый код, так и код Боуза-Чоудхури-Хоквингема (БЧХ).

Как видно из рис.1, кодовые слова на выходе предыдущего каскада используются как входные информационные символы для следующего каскада и т.д. Поскольку каждый кодер – это отдельное устройство, то в результате удастся упростить техническую реализацию каждого более короткого кода по сравнению с однокаскадным кодированием, конечно, при большой длине общего кода.

Отметим, что в случае многоступенчатой схемы кодирования скорость результирующего кода R равна произведению скоростей кодов r_i , используемых на разных ступенях.

Следующей модификацией этой схемы является включение перемежителя-деперемежителя между внутренним и внешним кодерами, что обеспечивает

преобразование пачек цифровых ошибок в одиночные, которые вносит внешний кодек, а также нестационарность помехи.

В современной интерпретации внешний кодек часто называется кодером источника, а внутренний кодек - кодером канала. Различные структурные схемы методов кодирования, модуляции и уплотнения приведены в [3,4].

Предлагаемая схема. Следует отметить, что как в вышеперечисленных, так и в многочисленных других работах почти нет сведений о структуре кодеков источника и канала, что приводит к трудностям в вопросе анализа и разработки систем передачи информации. Поэтому нами разработана и предложена наиболее развернутая и полная модель методов каскадного кодирования для современных систем обработки информации, показанная на рис. 2 [5-8].

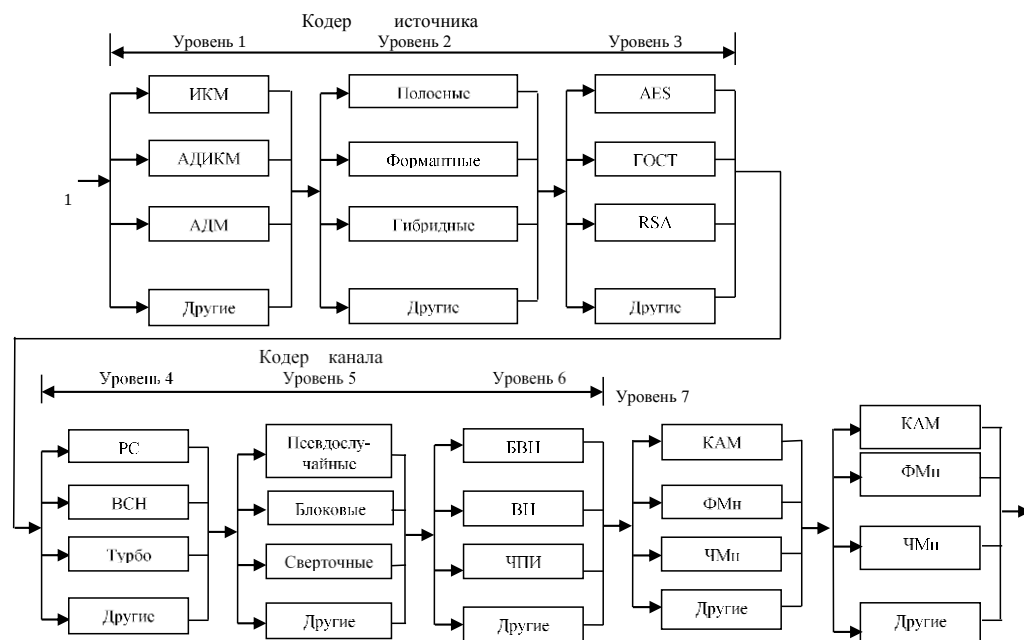


Рис. 2. Обобщенная модель каскадного кодирования

Здесь источник сообщений 1 вырабатывает мультимедийную информацию (речь, музыка, изображение, текст и т.п.), которая далее преобразуется в цифровой формат на уровне 1 с помощью аналого-цифрового преобразователя (АЦП). Наиболее распространенные виды АЦП – это импульсно-кодовая модуляция (ИКМ) со скоростью 64 кбит/с, адаптивная дифференциальная ИКМ (АДИКМ) со скоростью 32 кбит/с, адаптивная дельта-модуляция (АДМ) и дельта-сигма-модуляция (ДСМ) со скоростью 16...32 кбит/с. Для одного канала такие скорости передачи достаточно высокие, и, кроме того, они могут перегружать сети связи. Поэтому на уровне 2 обычно используются вокодеры и гибридные кодеры для понижения

этих скоростей до значений 3...8 *кбит/с*. Классическими видами вокодеров являются формантные, полосные, ортогональные. Однако в последние годы появились и применяются вокодеры с линейным предсказанием типа LPC (Linear Predictive Coding) и др. Лучшие результаты в смысле качества передаваемой информации обеспечивают современные гибридные кодеры, такие как ACELP (Algebraic Code-Excited Linear Prediction), LTP-LPC (Long-Term Prediction-LPC), RPE-LPC (Regular Pulse Excitation-LPC) и др.

Дальнейшим этапом преобразования может служить шифрование (криптография) с целью защиты системы от несанкционированного доступа (НСД), осуществляемое на уровне 3. Существует множество стандартов и алгоритмов шифрования, среди которых можно выделить AES (Advanced Encryption Standard), RSA (Rivest, Shamir, Adleman), ГОСТ и др. Основные задачи шифрования - обеспечение аутентификации и конфиденциальности связи. При этом конфиденциальность означает предотвращение утечки информации из линии связи, например, путем подслушивания; аутентификация же, наоборот, не допускает ввода ложной информации несанкционированными лицами в канал связи.

Уровни 1,2,3 могут быть объединены в кодер источника.

Кодер канала представлен также в виде трех уровней: помехоустойчивое кодирование, перемежение (интерливинг-interleaving) и линейное кодирование, которые обеспечивают эффективную передачу информации по каналу связи, где цифровой сигнал подвергается различного рода искажениям и ошибкам.

Цифровые ошибки исправляются на уровне 4 с помощью таких корректирующих кодов, как коды Рида-Соломона, БЧХ, Турбо и др.

Часто ошибки, возникающие в линии связи, группируются в пакеты (пачки), и поэтому для их преобразования в одиночные используется так называемое перемежение на уровне 5. Последовательное соединение корректирующего кодера и перемежителя является эффективной системой для устранения пачек ошибок.

На уровне 6 осуществляется линейное кодирование, при котором удается решить такие проблемы, как согласование характеристик цифрового сигнала с линией связи, передача информации о синхросигнале и др. Существуют различные форматы линейных кодов или кодов передачи, такие как без возврата к нулю (БВН), с возвратом к нулю (ВН), манчестерские, с чередованием полярности импульсов (ЧПИ) и др. В общем случае при линейном кодировании производится преобразование типа $mBnV$, где m и n – целые числа, а B – означает бинарный. При этом в коде БВН происходит переход к биимпульсному формату с целью устранения постоянной составляющей. Например, самое распространенное преобразование 1B2B известно под названием кода Манчестера. Другие популярные преобразования – 5B6B или 64B66B и т.д.

Последним этапом преобразования (уровень 7) является модуляция, с помощью которой осуществляется переход в область радиочастот. Здесь могут

использоваться квадратурная амплитудная модуляция (КАМ), фазовая манипуляция (ФМн), частотная манипуляция (ЧМн) и др.

Отметим, что эти методы кодирования используются в различных сочетаниях в современных цифровых системах передачи, обработки и хранения информации. Например, в среднескоростных каналах сети Intelsat применяется двухкаскадная схема кодирования, где в качестве внешнего кода выбран один из (126,112), (225,205), (219,201) или (194,178) модифицированных кодов РС. Внутренний код - это сверточный код с возможными скоростями $r=1/2$; $3/4$ или $7/8$. Тип модуляции – квадратурная фазовая манипуляция КФМн-4 [9]. Или другой пример: в стандарте широкополосного доступа IEEE 802.16-2004 рекомендуется использовать каскадное кодирование в формате Рид-Соломон – сверточный код, а тип модуляции - двоичная ФМн, КАМ или КФМн [10]. Наконец, в стандарте GSM используются следующие методы кодирования и модуляции: уровень 1 - ИКМ со скоростью 64 кбит/с; уровень 2- ACELP-EFR (Enhanced Full Rate) гибридный кодер со скоростью 12,2 кбит/с; уровень 4 - сверточный корректирующий код; уровень 5 – блочный перемежитель и шифратор A5; уровень 6 – код передачи БВН; уровень 7 – гауссовская ЧМн с минимальным частотным сдвигом.

Основываясь на этой концепции, с помощью программного комплекса MATLAB нами исследована новая четырехкаскадная схема, в которую входят следующие составляющие: уровень 1 - дельта-кодер; уровень 4 - кодер Рида-Соломона; уровень 5 - сверточный, спиральный и матричный интерливеры; уровень 7 - КАМ-64; канал связи с аддитивным белым гауссовским шумом (АБГШ) [11-13].

Заключение. Предложена многоуровневая модель каскадного кодирования, которая включает в себя все известные на сегодняшний день методы кодирования и позволяет, варьируя ими, создавать различные новые сложные кодовые схемы.

СПИСОК ЛИТЕРАТУРЫ

1. Элайес П. Кодирование для двух каналов с шумами // Теория передачи сообщений.- М.: Иностранная литература, 1957.- С.114-138.
2. Форми Д. Каскадные коды/ Пер. с англ. В.В. Зяблова и О.В. Попова; Под ред. С.И. Самойленко.- М.: Мир, 1970.- 207 с.
3. Скляр Бернард. Цифровая связь. Теоретические основы и практическое применение. - 2-е изд./ Пер. с англ.- М.: Изд. дом “Вильямс”, 2003.- 1104 с.
4. Simon M.K., Hinedi S.H., Lingsey W.C. Digital Communication Techniques. Englewood Cliffs.- New Jersey: PTR Prentice Hall, 1995.- 888 p.
5. Gomtsyan H.A. Computer simulation of cascade codes for CDMA systems // Proc. of Second International Symposium of Trans Black Sea. Region on Applied Electromagnetism.- Xanthi, Greece, 2000, June.- P.105.

6. **Гомцяц О.А.** Методы кодирования в цифровых системах передачи информации // Сборник материалов Годичной научной конференции ГИУА.- Ереван, 2001.- Т. 2.- С. 446-447.
7. **Gomtsyan H.A.** Encoding Methods for the Fiber Optical Communication and Storage Systems // 5th International Conference on Transparent Optical Networks –ICTON 2003, Conference Proceedings.- Poland, 2003, June 29-July 3.- We.P.13.-P.133 - 136.
8. **Gomtsyan H.A.** Generalized model of the digital communication systems // Материалы Тринадцатой Межрегиональной конференции “Обработка сигналов в системах телефонной связи и вещания”. - Пушкинские горы-Москва, 2004. - С.79-81.
9. **Камнев В.Е., Черкасов В.В., Чечин Г.В.** Спутниковые сети связи: Уч. пособие.- М.: Альпина Паблишер, 2004.- 536 с.
10. **Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.В.** Широкополосные беспроводные сети передачи информации.- М.: Техносфера, 2005.- 592 с.
11. **Гомцяц О.А., Бадалян Б.Ф.** Сложные кодирующие системы // Известия НАН РА и ГИУА. Серия Техн.наук.- 2009.- Т.62, N4.- С. 451-455.
12. **Гомцяц О.А., Бадалян Б.Ф.** Об одном способе построения составного кода // Вестник ГИУА (Политехник): Сборник научных и методических статей.- Ереван, 2010.- Т.2, N1.- С.194-198.
13. **Бадалян Б.Ф., Гомцяц О.А.** Эффективные системы помехоустойчивого кодирования для цифровой связи //Вестник ГИУА (Политехник): Сборник научных статей.- Ереван, 2012.- Часть 1.- С. 216-220.

Национальный политехнический университет Армении. Материал поступил в редакцию 02.10.2015.

Հ.Ա. ԳՈՄՅԱՆ

ԻՆՖՈՐՄԱՑԻԱՅԻ ՄՇԱԿՄԱՆ ԹՎԱՅԻՆ ՀԱՄԱԿԱՐԳԵՐՈՒՄ ԿԱՄԿԱՂԱՅԻՆ ԿՈՂԱՎՈՐՄԱՆ ԸՆՀԱՆՐԱՅՎԱԾ ՀԱՅԵՑԱԿԱՐԳ

Հետազոտվել են կոդային նոր կառուցվածքների և մոդուլյացիայի բազմազան մեթոդները, որոնք համատեղ օգտագործվում են ինֆորմացիայի մշակման տարբեր թվային համակարգերում: Ինֆորմացիայի մշակման թվային համակարգերի հայտնի առավելություններն առաջին պլան են մղում անթույլատրելի մուտքից տվյալների պաշտպանության միջոցները և խանգարումակայունության բարելավումը ժամանակակից կոդային սխեմաների օգտագործմամբ: Այս երկու հիմնական խնդիրներն առաջացրել են լուծումների և գործածության մեծ քանակություն՝ սկսած պարզագույն կոդերից մինչև ժամանակակից բարդ տուրբոկառուցվածքներ և այլն: Լրացուցիչ հետազոտման կարիք ունեն ազդանշանակողային կառուցվածքները, ինչպես նաև դրանց փոխադրությունը բազմակասկադային կոդերի հետ: Խանգարումակայուն կոդավորումը, անալոգա-թվային ձևափոխման և փոխանցման հաջող կոդերի հետ համադրված, շատ արդյունավետ է ձայնագրման որակի բարձրացման և տարբեր կապուղիներով ինֆորմացիայի հաղորդման համար: Ծածկագրումը և սեղմումը ապահովում են կապի ուղիների լրացուցիչ պաշտպանությունը չարտոնագրված մուտքից:

Առանցքային բառեր. կասկադային կոդավորում, անալոգա-թվային ձևափոխում, սեղմում, ծածկագրում, աղմկակայուն կոդավորում, միախառնում, գծային կոդավորում:

H.A. GOMTSYAN

**A GENERALIZED CONCEPT OF STAGE CODING IN DIGITAL SYSTEMS OF
INFORMATION PROCESSING**

New code structures and different modulation techniques used together in different digital information processing systems are investigated. The known advantages of digital processing systems promote the methods of data protection from unauthorized access and improvement of the noise immunity, using modern coding schemes. The two main tasks spawned a large number of solutions and applications, starting with the simplest codes to modern complex turbo constructions, etc. The signal-code constructions, as well as their interaction with multistage codes also require additional studies. Noiseless coding combined with analog – to - digital conversion, interleaving and successful transmission codes is very effective to improve the quality of recording and transmitting information on different channels. Encryption and compression provide additional protection channels against unauthorized access.

Keywords: concatenated coding, analog-to-digital conversion, compression, encryption, error correction coding, interleaving, line coding.